SONICWALL®

# SonicOS 8

# TZ80

## Getting Started Guide

# Contents

1

# Overview

The next-generation SonicWall TZ Series is powered by SonicCoreX and SonicOS and is designed to provide higher threat prevention performance. This document provides an overall process for configuring and deploying a typical TZ Series firewall. It serves as a template to describe common usage and configuration. Your deployment may vary depending on the features and related products that you choose to implement in your environment. Other documents and details are available at the Technical Documentation portal.

Topics in this section include:

- Using this Document
- Hardware Deployment Requirements
- TZ80 Description

## Using this Document

This document has been redesigned to provide a summary of an end-to-end deployment and configuration. It offers a brief overview of the necessary steps and refers to other guides for more detailed information when needed. The document begins by explaining how to connect to and prepare the firewall. Following that, it outlines the best practices for enabling features for a typical TZ Series use case.

| **Preparing and Connecting the Firewall** | |
|---|---|
| **Prerequisites** | Describes those chores that need to be done before you start configuring your firewall. See Prerequisites |
| **Preparing the Firewall** | Summarizes the steps to run the setup wizard, diagnose connectivity issues, configure the LAN settings, and update the firmware. See Preparing the Firewall |
| **Configuring Features and Options** | |
| **Zones and Policies** | Overview of security zones and their implementation in SonicOS is provided. The concept of grouping interfaces into logical entities for easier management and consistent policy application is explained, along with information about predefined security zones, default zone settings, and access rules. For more information on Zones refer to SonicOS 8 Objects Guide and Policies refer to SonicOS 8 Rules and Policies Administration Guide for Classic Mode. See Zones and Policies |

| | |
|---|---|
| **Using Capture ATP and RTDMI** | Describes the Capture ATP, a security solution that uses a multi-engine sandbox and Real-Time Deep Memory Inspection™ (RTDMI) to detect and stop Zero-day threats in real time. It shares threat intelligence across platforms and highly detects previously unknown threats, analyzing over 100,000 malware samples and events daily. For more information on Capture ATP refer to SonicOS 8 Capture ATP Administration Guide. See Using Capture ATP and RTDMI |
| **Security Services** | The SonicOS 8 framework provides various security services such as Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Geo-IP filtering, Botnet Filter, Application Control, and Content Filtering. These services can be used together to enhance environmental protection. For more information on Security Services refer to SonicOS 8 Security Services Administration Guide. |
| **SNMP** | SNMP (Simple Network Management Protocol) is a network protocol used with the User Datagram Protocol (UDP) to monitor the status of the SonicWall Security Appliance and receive notifications of critical events on the network. The SonicWall Security Appliance supports SNMP v1/v2c/v3 and most Management Information Base II (MIB-II) groups, except *egp* and *at*. SNMPv3 enhances security by authenticating and encrypting packets. For information on SNMP refer to SonicOS 8 Firewall Administration Guide |
| **Email Automation Setup and Tuning** | Automate email dispatch for log and alert management, including recipient addresses, manual or automatic sending, dispatch frequency, and email format. Additionally, automate email audit records, health check notifications, mail server settings, and FTP log automation, while identifying similarities between email and FTP log automation processes. For information on Email Automation Setup and Tuning refer to SonicOS 8 Device Log Administration Guide. See Email Automation Setup and Tuning |
| **User Authentication** | Describes how to set up user authentication, user reporting, and session tracking on a network firewall. It covers LDAP authentication, user status monitoring, and the use of Single Sign-On (SSO) for better visibility into user activities. It also discusses alternative methods for implementing SSO, such as using SonicWall's agents and the Directory Services Connector for integrating with directory services. For information on user authentication refer to SonicOS 8 Users Administration Guide. See User Authentication |
| **Syslog Setup** | The syslog server is a centralized system for logging. It collects error and system logs in one place and coordinates system events across multiple systems. The logs can then be sent to a SIEM/XDR platform for a Security Operations Center (SOC) to monitor. For information on syslog setup refer to SonicOS 8 Device Log Administration Guide. See Syslog Setup |
| **DPI-SSL** | DPI-SSL decrypts and inspects encrypted internet traffic, enhancing security and preventing data leakage for HTTPS and other SSL/TLS-based traffic. It can be deployed in Client DPI-SSL and Server DPI-SSL scenarios. For information on DPI-SSL refer to SonicOS 8 DPI SSL Administration Guide. See DPI-SSL |
| **AppFlow Reporting and Monitoring** | AppFlow feature helps manage firewall flow reporting and statistics in various formats. It allows users to effectively monitor and assess firewall performance. For information on AppFlow reporting and monitoring refer to SonicOS 8 AppFlow Device Administration Guide and SonicOS 8 Monitor Guide. See AppFlow Reporting and Monitoring |

# Hardware Deployment Requirements

Before configuring the TZ80 for operation, ensure that all physical connections are complete as described in the Quick Start Guide. It includes topics for:

- Package Contents
- Front and Back Panel
- Mounting options
- Connecting power
- Connecting interfaces
- Setup and Registration
    - Local management
    - Cloud management
    - SonicExpress Application

Once these tasks are complete you can begin configuring the TZ80 to operate in your environment.

# TZ80 Description

The SonicWall TZ80 firewall is a subscription-based appliance designed for small offices and home offices. It offers high-security efficacy at a low total cost of ownership, providing flexibility to meet changing security needs, rapid time-to-value, and a strong security posture. With best-in-class threat protection throughput, the TZ80 firewall delivers a strong return on investment.

Businesses can also transition from enabling basic secure connectivity to advanced protection, matching their growth requirements. The firewall supports Zero Trust Access by integrating Cloud Secure Edge and enabling authenticated access to private resources behind the firewall. TZ80 also drives quick onboarding and ease of use via zero-touch provisioning and simplified management.

The TZ80 requires one of two licenses to be operational:

- **Secure Connect** enables secure network connectivity and is common for use cases where VPN terminates at headquarters. It includes device management; 7-day alerting; firewall features such as Network Address Translation (NAT), Access Control List (ACL), High Availability (HA), Virtual Private Network (VPN), Software-Defined Wide Area Network (SD-WAN), advanced routing and 8x5 technical support service.
- **Advanced Protection Security Service (APSS)** enables device management; 7-day reporting and analytics that can extend to 30, 90, or 365 days; security services; firewall features such as NAT, ACL, HA, VPN, SD-WAN, and advanced routing and 8x5 technical support service.

# Unsupported Features

The unsupported features in TZ 80 firewall are:

- NTP server configuration
- Updating time
  **NOTE:** Because accurate internal time is critical for logging and reporting, the TZ80 automatically retrieves and updates its internal clock from a well-established SonicWall time source.
- Manual Keyset Download/Upload
- Manual Signature Download/Upload
- Closed Network
- Capture Client
- Switch Integration

2

# Prerequisites

Necessary tasks that must be completed prior to beginning the setup of your firewall.

**Topics:**

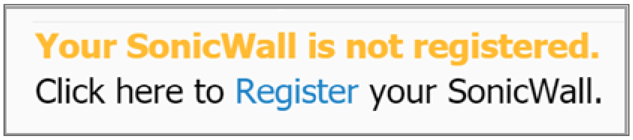
- Registering a TZ Firewall
- System Requirements
- Operational Environment
- Determining the WAN Type

## Registering a TZ Firewall

Registration is an important part of the setup process and is necessary in order to receive the benefits of SonicWall security services, firmware updates, and technical support.

***To register the appliance from SonicOS:***

1. Point your browser to the appliance LAN IP address (default https://192.168.168.168) and log in using the administrator credentials.
2. Click **Register** in the top banner or on the **MONITOR | Current Status > System Status** page under **Security Services**.

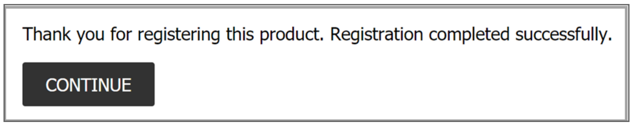


Your SonicWall is not registered.
Click here to Register your SonicWall.

ⓘ **TIP:** Registering the appliance from SonicOS requires that DNS Server settings are configured on the WAN (X1) interface.

3. Log in using your MySonicWall account name and password. If you do not have a MySonicWall account, go to http://www.mysonicwall.com to create an account. MySonicWall directly obtains the necessary information from the appliance. When finished, a message appears indicating that the registration is complete.

4. Click **CONTINUE**.



Thank you for registering this product. Registration completed successfully.

# License Expiry for TZ 80 Firewall

This section provides an overview of the different operational modes and functionalities of a firewall based on its licensing status. It covers unregistered devices, active licenses, and expired licenses. The firewall offers various features during the 30-day, 60-day, and 90-day grace periods that follow a license expiration. Some of the key features include configuration mode, packet forwarding capabilities, registration requirements, feature availability, system reset options, user interface (UI) and command-line interface (CLI) notifications, and administrative privileges.

| **Unregistered Device** | **Active License** | **Expired License** | | |
|---|---|---|---|---|
| | | **30-day Grace Period** | **60-day Grace Period** | **90-day Grace Period** |
| The firewall will be in configuration mode. | The firewall will be in configuration mode. | The firewall will be in configuration mode. | The firewall will be in non-configuration mode. | The firewall will be in non-configuration mode. |
| Packet Forwarding is not allowed. | The firewall allows end-to-end functionality to be performed. | A banner or message is displayed in the firewall UI and CLI to prompt license renewal during the 30-day grace period. | A banner or message is displayed in the firewall UI and CLI to prompt license renewal during the 60-day grace period. | A banner or message is displayed in the firewall UI and CLI to prompt license renewal during the 90-day grace period. |
| Successful registration requires valid MSW credentials. | Firewall features that require a license can be configured. | Firewall features that require a license can be configured, except for security services. | Firewall configuration is not allowed. | Firewall configuration is not allowed. |
| License data not available. | Licensed features are fully operational in the firewall. | Licensed features are fully operational in the firewall, except for security services. | Restart and restore factory defaults are permitted via the UI, CLI, or API. | Restart and restore factory defaults are permitted via the UI, CLI, or API. |

| Unregistered Device | Active License | Expired License | | |
|---|---|---|---|---|
| The banner and message are displayed in the Firewall UI and CLI. | Licensed features are configurable accordingly to user privilege | Licensed features are configurable accordingly to user privilege, except for security services. | Safemode is allowed. | Safemode is allowed. |
| | Licensed features function according to user privileges. | Licensed features function according to user privileges, except for security services. | Packets forwarding is allowed. | Packets forwarding is not allowed. |
| | Packets forwarding is allowed. | Packets forwarding is allowed. | The backup of firewall settings to both local and cloud storage is not allowed. | The backup of firewall settings to both local and cloud storage is not allowed. |
| | Multiple users are allowed to log in with full administrator privileges. | Multiple users are allowed to log in with full administrator privileges. | Upgrading the firmware is not allowed. | Upgrading the firmware is not allowed. |
| | | End to End functionality is allowed, except for security services. | EXP/TSR/Logs and Packet Capture is allowed. | EXP/TSR/Logs and Packet Capture is allowed. |

# System Requirements

Before beginning the setup process, verify that you have the following:

- An internet connection
- A web browser supporting Java Script and HTTP uploads

The following clients and platforms are supported for SonicOS:

| Client | Version | Notes |
|---|---|---|
| Windows 10 | • Version 22H2<br>• Version 21H2 | x86, x64 and arm64 |
| Windows 11 | • Version 24H2 | x64 and arm64 |

| Client | Version | Notes |
|---|---|---|
| macOS | • Sequoia (15)<br>• Sonoma (14) | arm64 |
| Linux | • Kernel level 6.X<br>• Ubunt 24 & above<br>• Fedora 40 | x86, x64 and arm64 |
| iOS (iPhone/iPad) | • Version 18.x<br>• Version 17.x | |
| Android | • Version 14.x<br>• Version 13.x | |
| Chrome OS | • Version 129 and higher | |

The following browsers are supported for SonicOS management:

| Browser | Version |
|---|---|
| Chrome | Version 129.0 or later |
| Edge | Version 129.0 or later |
| Firefox | Version 129.0 or later |
| Safari (running on non-Windows machines) | Version 18.0 or later |
| Opera | Version 113.0 or later |

# Operational Environment

The following environmental components are required to operate a SonicWall firewall:

- **Management workstation**: Any IT environment management workstation.
- **Remote Logging**: Audit Server supporting syslog protocol with an IPsec peer supporting IKEv2 and ESP.
- **Management Console**: Any computer that provides a supported browser to access the administrative interface via HTTPS and a direct serial connection providing administrative CLI access.
- **VPN Gateway**: VPN connections via IPSec.
- **WAN/internet**: External IP interface.
- **LAN/Internal**: Internal IP interface.

# Determining the WAN Type

Before setting up your SonicWall appliance, you must first identify the type of WAN connection used in your setup. SonicWall supports the following connection types:

- **Static**-Configures the appliance for a network that uses static IP addresses.
- **DHCP**-Configures the appliance to request IP settings from a DHCP server on the internet.
- **PPPoE**-Point-to-Point Protocol over Ethernet (PPPoE) is typically used with a DSL modem. If your ISP requires desktop software with a username and password, select NAT with PPPoE mode.
- **PPTP**-Point-to-Point Tunneling Protocol (PPTP) is used to connect to a remote server. PPTP typically supports older Microsoft Windows implementations that require tunneling connectivity.
- **L2TP**-Layer 2 Tunneling Protocol (L2TP) is used to transmit Layer 2 data over IP or other Layer 3 routed networks. Internet Service Providers (ISPs) often use it to enable virtual private networks (VPNs) for customers over the internet. It does not encrypt network traffic itself. ***If L2TP is not available in the Setup Wizard, you can configure it later in the SonicOS management interface***.
- **Wire Mode (2-Port Wire)**-Inserts the appliance into the network using two paired interfaces. Available Wire Mode types include Bypass, Inspect, and Secure. Bypass mode allows for quick and non-disruptive insertion into the data path. Inspect mode extends Bypass mode with traffic inspection for classification and flow reporting. Secure mode provides full SonicWall ReAssembly-Free Deep Packet Inspection™ (RF-DPI) and control of network traffic.

  Secure Mode also 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. If Wire Mode is not available in the Setup Wizard, you can configure it later in the SonicOS management interface.

  > ⓘ **NOTE:** When operating in Wire Mode, the firewall's 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.

- Tap Mode (1-Port Tap)-Using a single interface, the firewall connects to and receives mirrored packets from an adjacent switch SPAN port. Similar to Inspect mode in Wire Mode, but with a single port and not in the physical path of traffic. ***If Tap Mode is not available in the Setup Wizard, you can configure it later in the SonicOS management interface***.

For more information about WAN types including Wire Mode, Tap Mode, L2TP, and others, refer to the *SonicOS 8 Administration* documentation or online Help available at the Technical Documentation portal.

3

# Preparing the Firewall

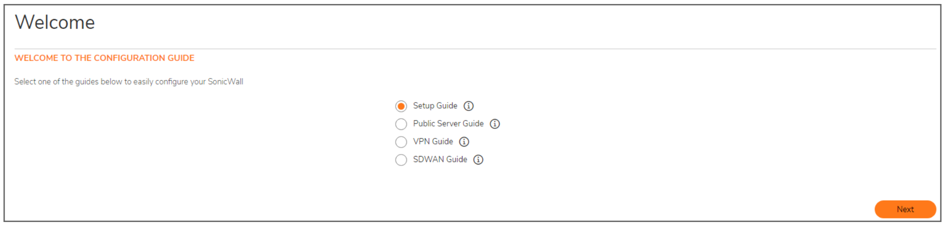
Outlines the procedure for initiating the setup wizard, identifying connectivity problems, adjusting the LAN settings, and upgrading the firmware.

**Topics:**

- Running the Setup Wizard
- Testing and Troubleshooting Connectivity
- Uploading the Latest Firmware

## Running the Setup Wizard

1. Navigate to https://192.168.168.168 in your web browser.
2. Click the wizard icon and select **Setup Guide** option.



Welcome

WELCOME TO THE CONFIGURATION GUIDE

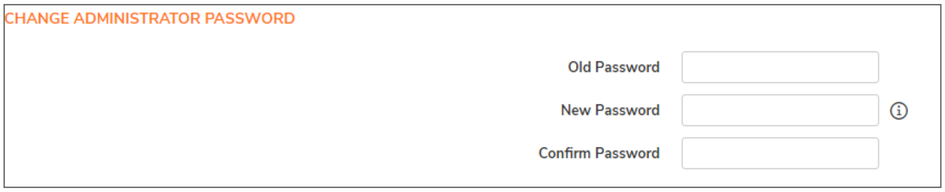
Select one of the guides below to easily configure your SonicWall

● Setup Guide ⓘ
○ Public Server Guide ⓘ
○ VPN Guide ⓘ
○ SDWAN Guide ⓘ

   The ***SonicOS Setup Guide*** opens.

3. Click **NEXT** and follow the prompts in the **Setup Guide**.
4. On the **Password / Time Zone** screen, enter log in with the default credentials; On successful login using the default password, you are then prompted to change the password.
   - **Old Password**
   - **New Password**
   - **Confirm Password**

ⓘ **NOTE:** The default password must be changed at the time of your first log in to the new password to be used for future login attempts.



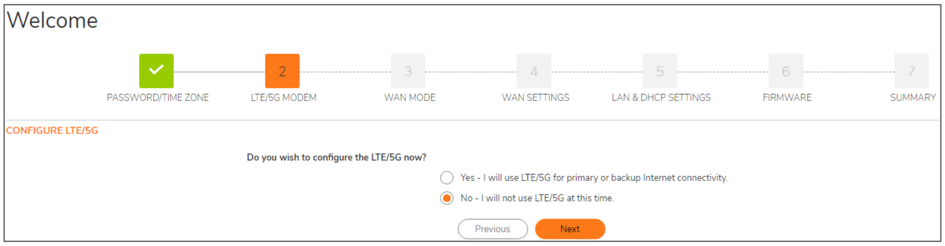
CHANGE ADMINISTRATOR PASSWORD

Old Password

New Password

Confirm Password

5. Click **NEXT**.
6. Configure the **LTE/5G** screen.



Welcome

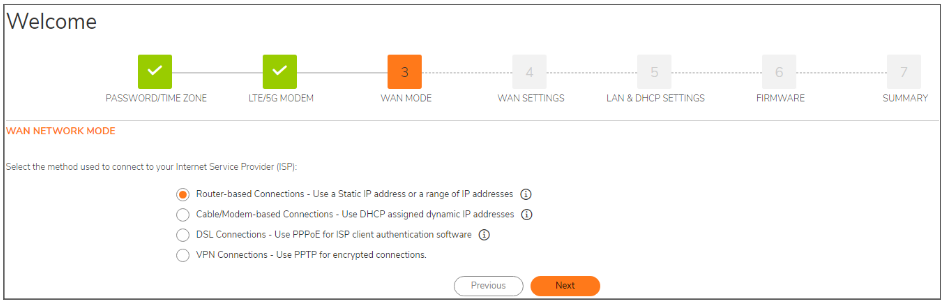
CONFIGURE LTE/5G

Do you wish to configure the LTE/5G now?

○ Yes - I will use LTE/5G for primary or backup Internet connectivity.

● No - I will not use LTE/5G at this time.

7. Click **NEXT**.
8. On the **WAN Mode** screen select the method used to connect to your Internet Service Provider.



Welcome

WAN NETWORK MODE

Select the method used to connect to your Internet Service Provider (ISP):

● Router-based Connections - Use a Static IP address or a range of IP addresses

○ Cable/Modem-based Connections - Use DHCP assigned dynamic IP addresses

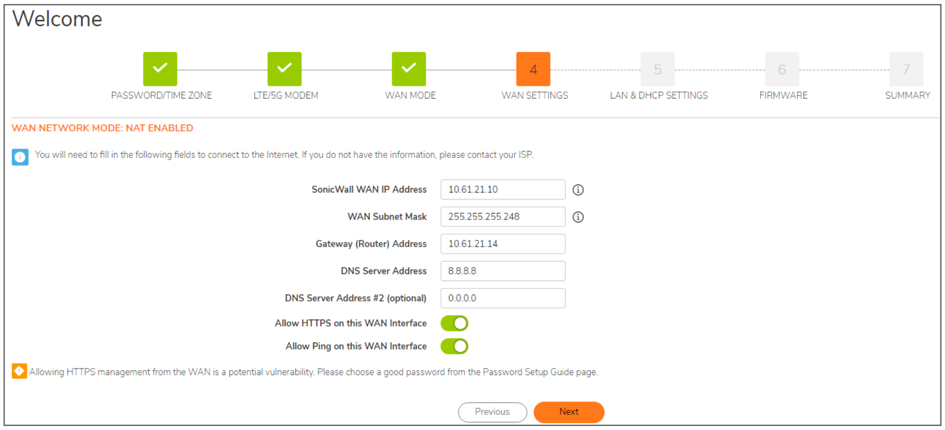
○ DSL Connections - Use PPPoE for ISP client authentication software

○ VPN Connections - Use PPTP for encrypted connections.

By default, **Router-based Connections - Use a Static IP address or a range of IP addresses** option is selected.

9. Click **NEXT**.

10. On the **WAN Settings** screen fill the fields to connect to the internet.



Welcome

WAN NETWORK MODE: NAT ENABLED

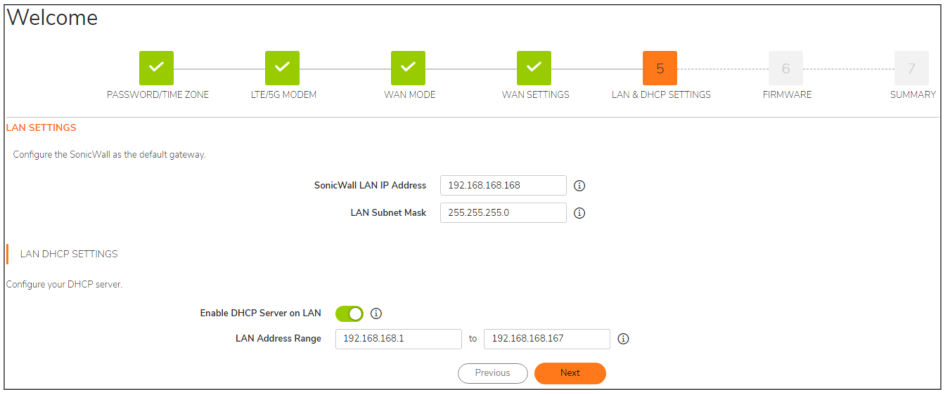
You will need to fill in the following fields to connect to the Internet. If you do not have the information, please contact your ISP.

| | |
|---|---|
| SonicWall WAN IP Address | 10.61.21.10 |
| WAN Subnet Mask | 255.255.255.248 |
| Gateway (Router) Address | 10.61.21.14 |
| DNS Server Address | 8.8.8.8 |
| DNS Server Address #2 (optional) | 0.0.0.0 |
| Allow HTTPS on this WAN Interface | ● |
| Allow Ping on this WAN Interface | ● |

Allowing HTTPS management from the WAN is a potential vulnerability. Please choose a good password from the Password Setup Guide page.

11. Click **NEXT**.

12. On the **LAN and DHCP Settings** screen configure the default gateway and DHCP server.



Welcome

LAN SETTINGS

Configure the SonicWall as the default gateway.

| | |
|---|---|
| SonicWall LAN IP Address | 192.168.168.168 |
| LAN Subnet Mask | 255.255.255.0 |

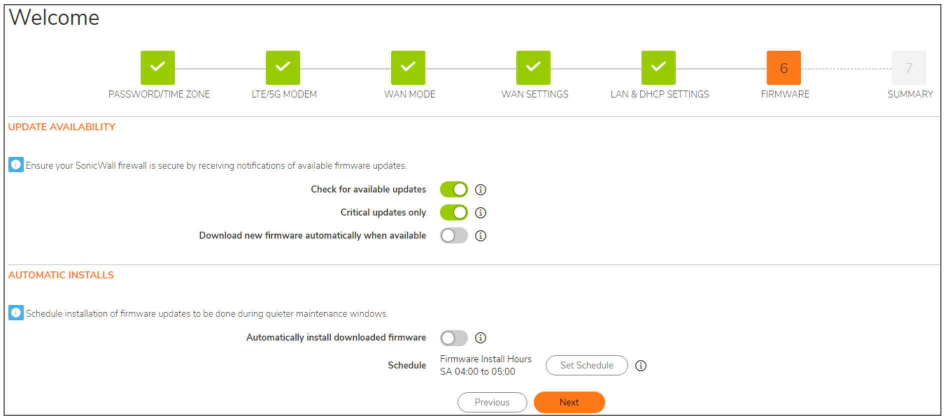
LAN DHCP SETTINGS

Configure your DHCP server.

| | | | |
|---|---|---|---|
| Enable DHCP Server on LAN | ● | | |
| LAN Address Range | 192.168.168.1 | to | 192.168.168.167 |

13. Click **NEXT**.

14. On the **Firmware** screen select the updates needed and automatic firmware installs.



Welcome

UPDATE AVAILABILITY

Ensure your SonicWall firewall is secure by receiving notifications of available firmware updates.

| | |
|---|---|
| Check for available updates | ● |
| Critical updates only | ● |
| Download new firmware automatically when available | ○ |

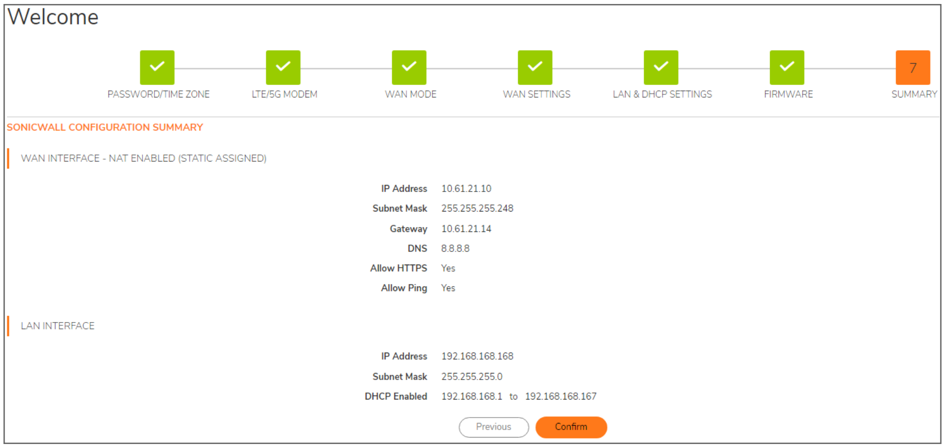
AUTOMATIC INSTALLS

Schedule installation of firmware updates to be done during quieter maintenance windows.

| | |
|---|---|
| Automatically install downloaded firmware | ○ |
| Schedule | Firmware Install Hours<br>SA 04:00 to 05:00 |

15. Click **NEXT**.

16. On the **Summary** screen, review the settings and click **Confirm**.



SONICWALL CONFIGURATION SUMMARY

WAN INTERFACE - NAT ENABLED (STATIC ASSIGNED)

| | |
|---|---|
| IP Address | 10.61.21.10 |
| Subnet Mask | 255.255.255.248 |
| Gateway | 10.61.21.14 |
| DNS | 8.8.8.8 |
| Allow HTTPS | Yes |
| Allow Ping | Yes |

LAN INTERFACE

| | |
|---|---|
| IP Address | 192.168.168.168 |
| Subnet Mask | 255.255.255.0 |
| DHCP Enabled | 192.168.168.1 to 192.168.168.167 |

The SonicOS configuration summary is applied.

# Testing and Troubleshooting Connectivity

***To test your internet connection:***

1. Reset your computer to use DHCP IP addressing and connect it to your LAN subnet or to the appliance X0 interface.
2. Point your browser to the X0 IP address configured during initial setup (default: `192.168.168.168`).
3. Log into SonicOS using the configured credentials.
4. In a command prompt window, type: `ping sonicwall.com`. You should receive a reply.
5. Open another browser tab or window and point it to https://www.sonicwall.com or another valid web site. If the site displays, you have correctly configured your appliance.

***To troubleshoot your internet connection:***

- Verify that the Wireless Area Network (WAN) settings on your management computer are set to use either DHCP or a static IP on the WAN subnet. Restart it or renew the DHCP address.
- Verify that the WAN interface being used for internet connectivity is not configured in Wire Mode or Tap Mode.
- Restart your internet router or modem to communicate with the DHCP client in SonicOS on the appliance.
- Check all cable connections and IP addresses.

***To troubleshoot your MGMT connection, consider the following:***

- Did you correctly enter the SonicWall NSA management IP address beginning with “http://” or “https://” in your web browser?
- Did you try restarting your management station while it is connected to the appliance?

- Are the Local Area Connection settings on your computer set to a static IP address on the `192.168.1.0/24` subnet?
- Is the Ethernet cable connected to your computer and to the MGMT port on your appliance, and are the connector clips properly seated in the ports?

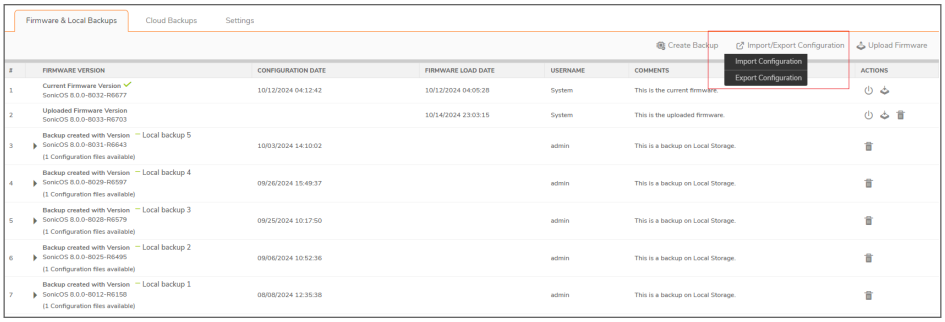
***To troubleshoot your LAN connection, consider the following:***

- Did you correctly enter the IP address for the SonicWall X0 interface into your web browser, beginning with “http://” or “https://”?
- Did you try restarting your management station while it is connected to the appliance?
- Are the Local Area Connection settings on your computer set to one of the following:
  - Obtain an IP address automatically using DHCP
  - A static IP address on the default LAN subnet (`192.168.168.0/24`)
  - A static IP address on the configured LAN subnet, if you changed it during initial setup
- Is the Ethernet cable connected to your computer and to the X0 (LAN) port on your appliance, and are the connector clips properly seated in the ports?

# Uploading the Latest Firmware

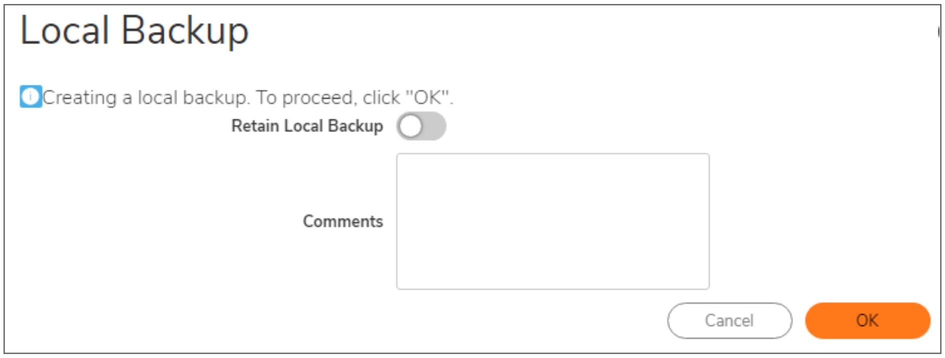
***To get and upload the latest firmware:***

1. Navigate to **Device | Settings | Firmware and Settings > Firmware & Local Backups**.
2. Select the **Import/Export Configuration** option and save the `.EXP` file to a safe location by clicking on the export configuration option.



| # | FIRMWARE VERSION | CONFIGURATION DATE | FIRMWARE LOAD DATE | USERNAME | COMMENTS | ACTIONS |
|---|---|---|---|---|---|---|
| 1 | Current Firmware Version ✓<br>SonicOS 8.0.0-8032-R6677 | 10/12/2024 04:12:42 | 10/12/2024 04:05:28 | System | This is the current firmware. | ⏻ ⇩ |
| 2 | Uploaded Firmware Version<br>SonicOS 8.0.0-8033-R6703 | | 10/14/2024 23:03:15 | System | This is the uploaded firmware. | ⏻ ⇩ 🗑 |
| 3 | ▶ Backup created with Version — Local backup 5<br>SonicOS 8.0.0-8031-R6643<br>(1 Configuration files available) | 10/03/2024 14:10:02 | | admin | This is a backup on Local Storage. | 🗑 |
| 4 | ▶ Backup created with Version — Local backup 4<br>SonicOS 8.0.0-8029-R6597<br>(1 Configuration files available) | 09/26/2024 15:49:37 | | admin | This is a backup on Local Storage. | 🗑 |
| 5 | ▶ Backup created with Version — Local backup 3<br>SonicOS 8.0.0-8028-R6579<br>(1 Configuration files available) | 09/25/2024 10:17:50 | | admin | This is a backup on Local Storage. | 🗑 |
| 6 | ▶ Backup created with Version — Local backup 2<br>SonicOS 8.0.0-8025-R6495<br>(1 Configuration files available) | 09/06/2024 10:52:36 | | admin | This is a backup on Local Storage. | 🗑 |
| 7 | ▶ Backup created with Version — Local backup 1<br>SonicOS 8.0.0-8012-R6158<br>(1 Configuration files available) | 08/08/2024 12:35:38 | | admin | This is a backup on Local Storage. | 🗑 |

3. Click **Create Backup** > **Retain Local Backup** > **OK**.



Local Backup

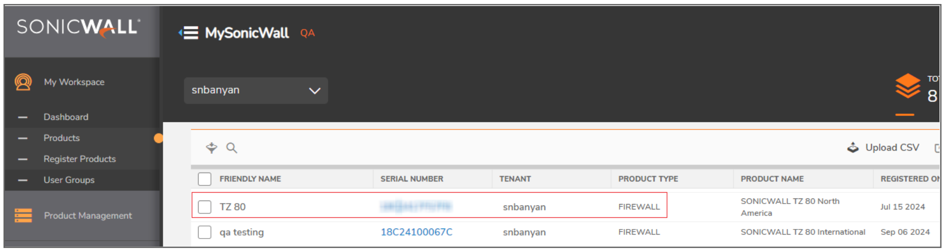
Creating a local backup. To proceed, click "OK".

Retain Local Backup ○

Comments

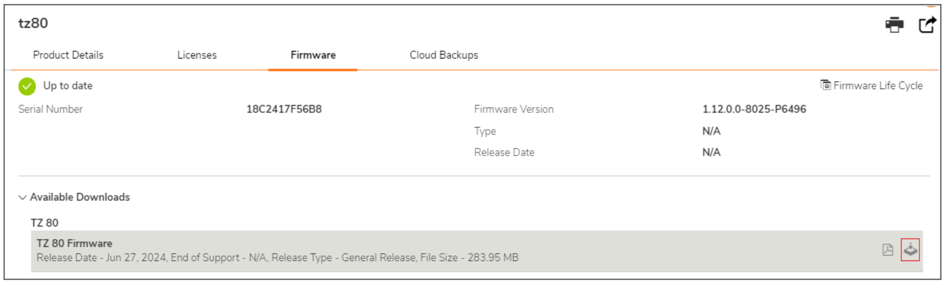
This will save a copy of the existing Settings to the SonicWall non-volatile memory.

4. In a web browser, navigate to http://www.mysonicwall.com and login with the account that your SonicWall is registered to.
5. Click  **Products** and locate the device you want to update. Click on the device serial number and select the Firmware icon to access the firmware version available.



| | FRIENDLY NAME | SERIAL NUMBER | TENANT | PRODUCT TYPE | PRODUCT NAME | REGISTERED O |
|---|---|---|---|---|---|---|
| □ | TZ 80 | [redacted] | snbanyan | FIREWALL | SONICWALL TZ 80 North America | Jul 15 2024 |
| □ | qa testing | 18C24100067C | snbanyan | FIREWALL | SONICWALL TZ 80 International | Sep 06 2024 |

6. The current firmware version shows up.
7. Go to **Firmware** tab and click on the download button and save the file to a location on your computer.



tz80

Up to date

Serial Number 18C2417F56B8

Firmware Version 1.12.0.0-8025-P6496

Type N/A

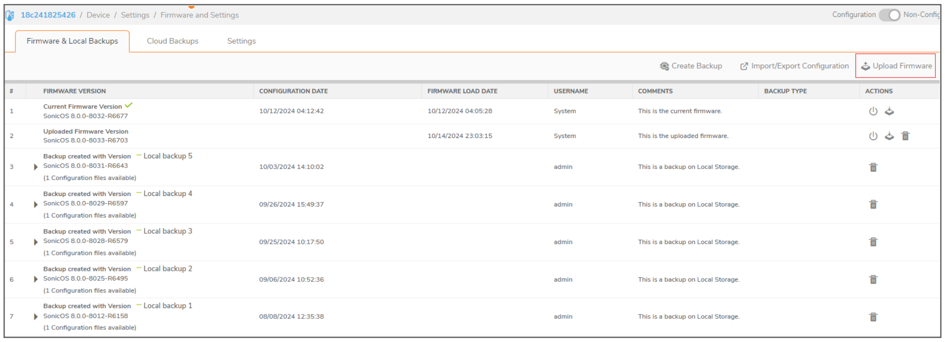
Release Date N/A

Available Downloads

TZ 80

TZ 80 Firmware
Release Date - Jun 27, 2024, End of Support - N/A, Release Type - General Release, File Size - 283.95 MB

8. On the TZ appliance, navigate to the **DEVICE > Settings > Firmware and Settings** page and click **Upload Firmware** and navigate to where the Firmware file is stored on your local device. Click **Upload**.

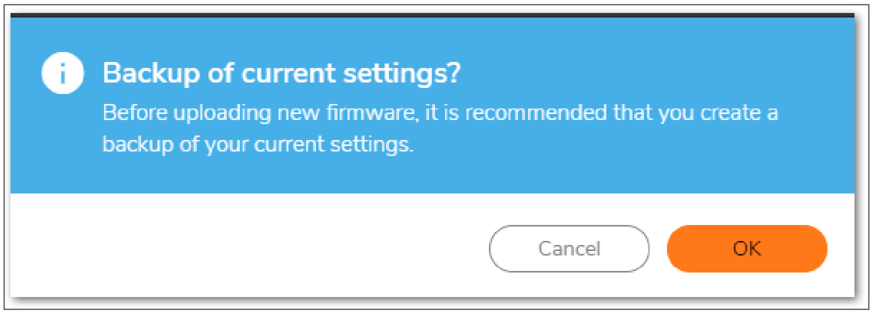


18c241825426 / Device / Settings / Firmware and Settings

Configuration Non-Config

| # | FIRMWARE VERSION | CONFIGURATION DATE | FIRMWARE LOAD DATE | USERNAME | COMMENTS | BACKUP TYPE | ACTIONS |
|---|---|---|---|---|---|---|---|
| 1 | Current Firmware Version ✓<br>SonicOS 8.0.0-8032-R6677 | 10/12/2024 04:12:42 | 10/12/2024 04:05:28 | System | This is the current firmware. | | ⏻ ⬇ |
| 2 | Uploaded Firmware Version<br>SonicOS 8.0.0-8033-R6703 | | 10/14/2024 23:03:15 | System | This is the uploaded firmware. | | ⏻ ⬇ 🗑 |
| 3 | Backup created with Version — Local backup 5<br>SonicOS 8.0.0-8031-R6643<br>(1 Configuration files available) | 10/03/2024 14:10:02 | | admin | This is a backup on Local Storage. | | 🗑 |
| 4 | Backup created with Version — Local backup 4<br>SonicOS 8.0.0-8029-R6597<br>(1 Configuration files available) | 09/26/2024 15:49:37 | | admin | This is a backup on Local Storage. | | 🗑 |
| 5 | Backup created with Version — Local backup 3<br>SonicOS 8.0.0-8028-R6579<br>(1 Configuration files available) | 09/25/2024 10:17:50 | | admin | This is a backup on Local Storage. | | 🗑 |
| 6 | Backup created with Version — Local backup 2<br>SonicOS 8.0.0-8025-R6495<br>(1 Configuration files available) | 09/06/2024 10:52:36 | | admin | This is a backup on Local Storage. | | 🗑 |
| 7 | Backup created with Version — Local backup 1<br>SonicOS 8.0.0-8012-R6158<br>(1 Configuration files available) | 08/08/2024 12:35:38 | | admin | This is a backup on Local Storage. | | 🗑 |

9. Message appears to remind you to take backup of your current settings, click **OK** if you have taken the backup already.



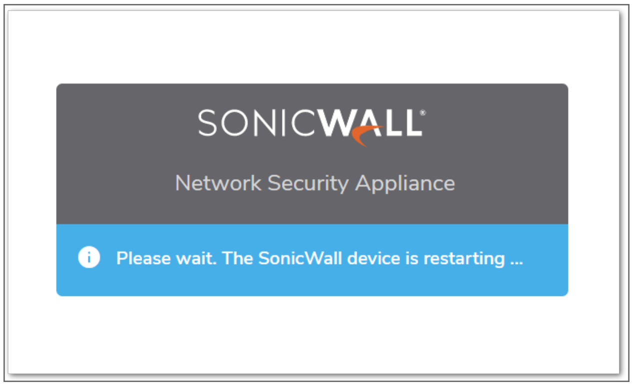
Backup of current settings?

Before uploading new firmware, it is recommended that you create a backup of your current settings.

It takes a few minutes to upload the firmware to the firewall, do not navigate away from the screen during this time.

10. Select the **Boot Power** Icon on the far-right. Once you click on the boot icon, the image will be first saved to the flash memory and then the firewall will reboot automatically.

The restart procedure takes place and the following screen would appear.



Please wait. The SonicWall device is restarting ...

# Zones and Policies

A zone is a logical method of grouping one or more interfaces (or sub-interfaces) into a logical entity that can be given a friendly, user-definable name. It allows the grouping of similar interfaces:

- The same policies can be applied to a zone.
- Traffic can be restricted between different zones.
- Configuration overhead can be minimized.

Security services are enabled in a zone.

**Topics:**

## Using Zones

Firewall security zones add an extra, flexible layer of security. With zone-based security, administrators can group similar interfaces and apply the same policies to them rather than writing separate policies for each interface.

SonicOS zones allow the application of security policies to the internal network, enabling administrators to organize network resources into different zones and control traffic between them.

Zones enable full exposure of the NAT table, allowing administrators to control traffic across interfaces by managing the source and destination addresses as traffic moves from one zone to another. This means that NAT can be applied internally or across VPN tunnels. Security appliances can also direct VPN traffic through the NAT policy and zone policy, as VPNs are logically grouped into their own VPN zone.

The security appliance has 7 predefined security zones that cannot be modified. The specific predefined zones depend on the device.

- LAN: This zone can consist of one to five interfaces, depending on your network design. Although each interface will have a different network subnet attached to it, when grouped together, they can be managed as a single entity.

- WAN: This zone can consist of either one or two interfaces.
- DMZ: This zone is normally used for publicly accessible servers. This zone can consist of one to four interfaces.
- VPN: The VPN zone does not have an assigned physical interface. It is used to apply a security policy to VPN traffic.
- SSLVPN: This virtual zone is used for providing secure remote access using the SSL VPN NetExtender feature. All traffic from SSL VPN clients is treated as being sourced from the SSLVPN zone, which seamlessly integrates UTM security features for SSL VPN traffic.
- MGMT: This zone is used for appliance management and includes only the MGMT interface.
- MULTICAST: This zone provides support for IP multicasting.
- WLAN: This Wireless LAN zone provides support for SonicWall's Access Points (SonicPoints). It has additional tabs and parameters that are used to configure the SonicPoints.

Each firewall also has a set of Zone defaults. See Default Zones.

# Default Zones

Each firewall also has a set of Zone defaults:

- LAN – The default interface is X0.

  Outbound traffic is allowed to any other zone; Inbound traffic is allowed from DMZ and VPN.
- WAN – The default interface is X1.

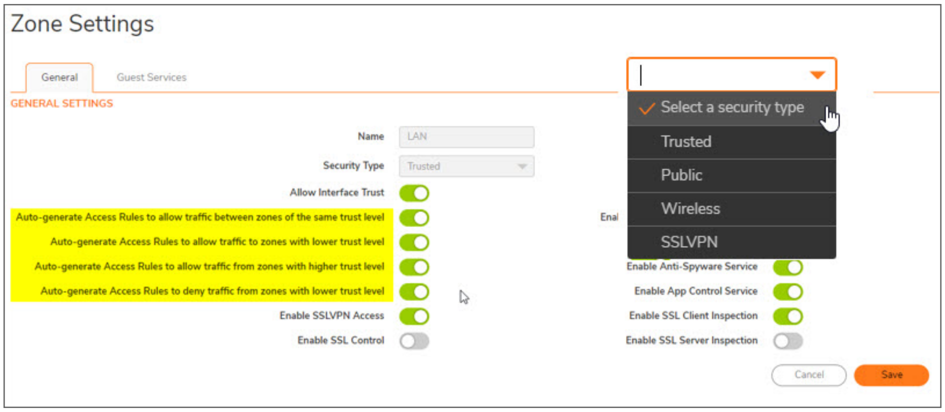
  Outbound traffic is allowed to this zone from all other zones; inbound traffic is blocked from this zone to all other zones.
- VPN – There is no default physical interface for VPN.

  Outbound traffic is allowed to any zone except the WLAN; inbound traffic is allowed from the LAN and DMZ only.
- WLAN – There can be multiple physical interfaces or multiple VLANS & VAPs.

  Outbound traffic is allowed to the WAN only; Inbound traffic is allowed from the LAN or DMZ.
- DMZ – Multiple physical interfaces can be assigned.

  Outbound traffic is allowed to the WAN & VPN for remote access networks only; Inbound traffic is allowed from any zone except the WAN (WAN access via access rules).

Default zones include auto-generated firewall rules.



Zone Settings

GENERAL SETTINGS

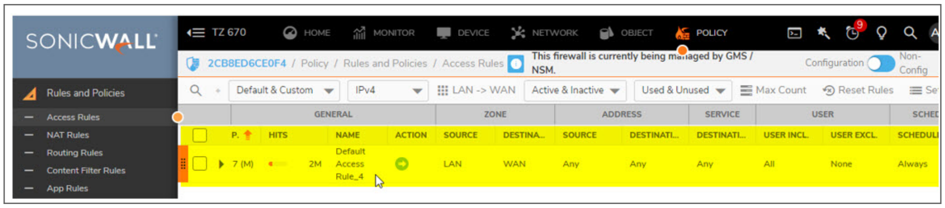
| | |
|---|---|
| Name | LAN |
| Security Type | Trusted |
| Allow Interface Trust | ● |
| Auto-generate Access Rules to allow traffic between zones of the same trust level | ● |
| Auto-generate Access Rules to allow traffic to zones with lower trust level | ● |
| Auto-generate Access Rules to allow traffic from zones with higher trust level | ● |
| Auto-generate Access Rules to deny traffic from zones with lower trust level | ● |
| Enable SSLVPN Access | ● |
| Enable SSL Control | ○ |
| Enable Anti-Spyware Service | ● |
| Enable App Control Service | ● |
| Enable SSL Client Inspection | ● |
| Enable SSL Server Inspection | ○ |

ⓘ **NOTE:** By default, SonicWall does not suppress auto-added access rules, leading to either restriction or allowance of access between zones. In environments with multiple zones, this can create a significant number of access rules. For more information refer to this KB article Auto-added access rules on the SonicWall can be disabled.

# Default Access Rules Overview

By default, the 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 behaviours are defined by the default stateful inspection packet access rule that gets enabled in the security appliance:

- Allow all sessions originating from the LAN, the WLAN to the WAN, or DMZ (except when the destination WAN IP address is the WAN interface of the appliance 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.



2CB8ED6CE0F4 / Policy / Rules and Policies / Access Rules

This firewall is currently being managed by GMS / NSM.

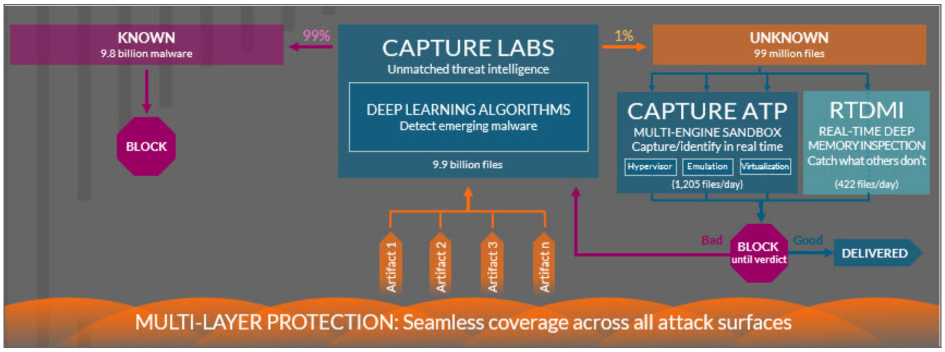
| | GENERAL | | | | ZONE | | ADDRESS | | SERVICE | USER | | SCHED |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | P. | HITS | NAME | ACTION | SOURCE | DESTINA... | SOURCE | DESTINATI... | DESTINATI... | USER INCL. | USER EXCL. | SCHEDULI |
| □ | 7 (M) | 2M | Default Access Rule_4 | → | LAN | WAN | Any | Any | Any | All | None | Always |

SANS Institute is a trusted resource for cybersecurity research. They offer a firewall checklist that can help you identify recommended ports to block if you choose to use it.

# Using Capture ATP and RTDMI

Capture Advance Threat Protection brings a layer of defense to capture and identity Zero-day threats in real time. This involves two elements:

- Our multi-engine sandbox continuously isolates and analyzes never-before-seen and potentially malicious files.
- Our patent-pending Real-Time Deep Memory Inspection™ (RTDMI) leverages artificial intelligence and machine learning to catch what others do not.



All of this occurs in real time across all attack surfaces (network, cloud, email, remote/mobile, endpoints, apps). This comprehensive coverage also facilitates the sharing of threat intelligence across the products. If the same malware targets multiple layers, detection in one layer automatically leads to identification in the others. The Capture Labs team uses real-time intelligence from the SonicWall Capture Threat Network, which comprises data from various sources:

- Intelligence-sharing consortiums of threat researchers
- 1.1 million sensors located across the globe
- Continuous real-time monitoring
- The more than 100K malware samples collected per day and 100K events analyzed each day

SonicWall has been recognized by ISCA Labs for its high detection of previously unknown threats. See ICSA Labs Certification.

***To set up Capture ATP:***

1. Navigate to **Policy | Capture ATP | Settings > Basic**.
2. Click the switch to **Enable Capture ATP**.
3. Enable to the appropriate features on the **Basic**, **Advanced**, and **Capture ATP Location** tabs.

   For more information refer to SonicOS 8 Capture ATP Administration Guide.

6

# Security Services

**IMPORTANT:** This section provides a baseline security stance but does not guarantee 100% security. Be sure to evaluate your environment to determine what security settings are required. For more information refer to SonicOS 8 Security Services Administration Guide.

Security Services are like layers; when used together, they combine to protect your environment more effectively. The following services are reviewed in this section.

- Detection Prevention
- Summary Settings
- Gateway Anti-Virus
- Summary Settings
- Intrusion Prevention
- Geo-IP
- Botnet Filter
- App Control
- Content Filtering

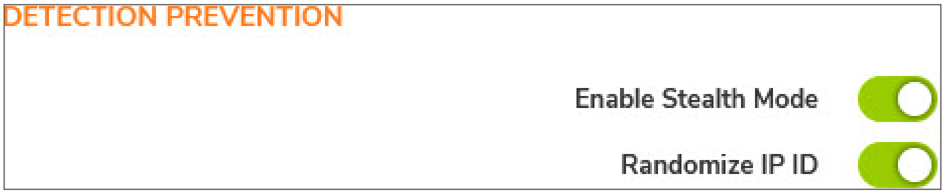
## Detection Prevention

One key action you can take is to make it hard for hackers to detect you. By default, the security appliance responds to incoming connection requests as blocked or open. To ensure your security appliance does not respond to blocked inbound connection requests, use Stealth Mode to make it essentially invisible to hackers. This option is not selected by default.

Use the Randomize IP ID feature to prevent hackers from using various detection tools to detect 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. This option is not selected by default, either. For more information refer to SonicOS 8 Security Services Administration Guide.

***To enable detection prevention:***

1. Navigate to **Network | Firewall | Advanced > Settings**.
2. In the **Detection Prevention** section select **Enable Stealth Mode** and **Randomize IP ID**.



DETECTION PREVENTION

Enable Stealth Mode ●

Randomize IP ID ●

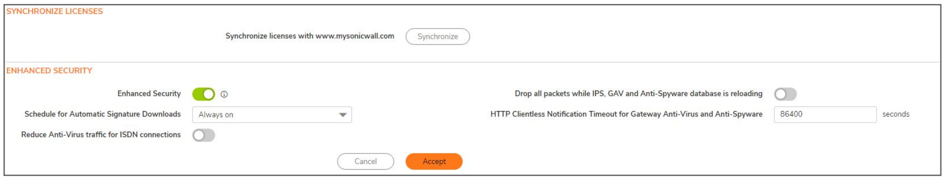
# Summary Settings

SonicWall appliances can connect to the Internet through a proxy server to download signatures and register securely.

The  **Policy | Security Services > Summary** page includes these key settings:

- Synchronize Licenses
- Security Services Settings
- Signature Downloads Through a Proxy Server
- Security Services Information

You can choose settings for maximum security or better performance, applying them to the whole network, a group, or a single appliance. For more information refer to SonicOS 8 Security Services Administration Guide.



SYNCHRONIZE LICENSES

Synchronize licenses with www.mysonicwall.com

ENHANCED SECURITY

Enhanced Security ●

Schedule for Automatic Signature Downloads: Always on

Reduce Anti-Virus traffic for ISDN connections ○

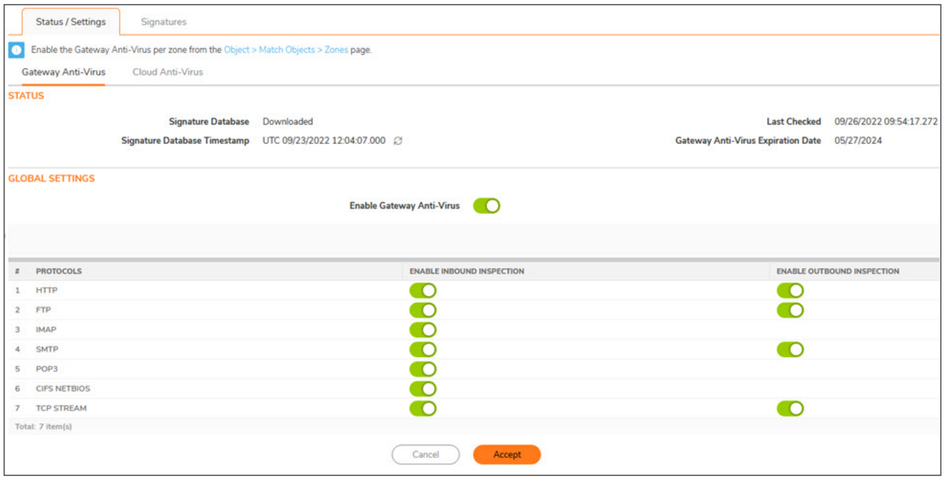
Drop all packets while IPS, GAV and Anti-Spyware database is reloading ○

HTTP Clientless Notification Timeout for Gateway Anti-Virus and Anti-Spyware: 86400 seconds

# Gateway Anti-Virus

SonicWall Gateway Anti-Virus (GAV) provides real-time virus protection by scanning all traffic through the SonicWall device. It has no file size limits and can unzip various formats for scanning. GAV checks files against an updated virus database to stop threats before reaching your computers and logs email header information for security analysis.

Gateway Anti-Virus is available under **Policy | Security Services | Gateway Anti-Virus**. For more information refer to SonicOS 8 Security Services Administration Guide.



Enable the Gateway Anti-Virus per zone from the Object > Match Objects > Zones page.

STATUS

Signature Database: Downloaded
Signature Database Timestamp: UTC 09/23/2022 12:04:07.000
Last Checked: 09/26/2022 09:54:17.272
Gateway Anti-Virus Expiration Date: 05/27/2024

GLOBAL SETTINGS

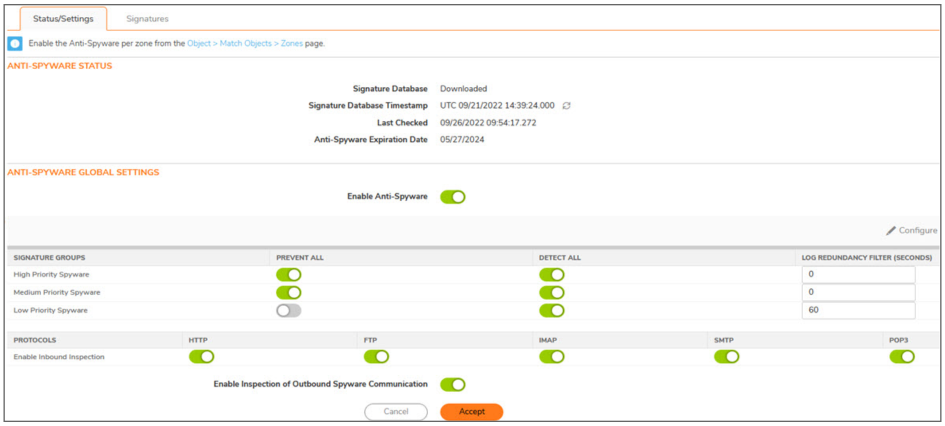
Enable Gateway Anti-Virus ●

| # | PROTOCOLS | ENABLE INBOUND INSPECTION | ENABLE OUTBOUND INSPECTION |
|---|---|---|---|
| 1 | HTTP | ● | ● |
| 2 | FTP | ● | ● |
| 3 | IMAP | ● | |
| 4 | SMTP | ● | ● |
| 5 | POP3 | ● | |
| 6 | CIFS NETBIOS | ● | |
| 7 | TCP STREAM | ● | ● |

Total: 7 item(s)

# Anti-Spyware

Under **Policy | Security Services | Anti-Spyware**, selecting the **Prevent All** option technically reduces security by allowing low-priority spyware, which could lead to false positives. Before finalizing your choices, review and test the settings in your environment before deciding how to enable those settings. For more information refer to SonicOS 8 Security Services Administration Guide.



Enable the Anti-Spyware per zone from the Object > Match Objects > Zones page.

ANTI-SPYWARE STATUS

Signature Database: Downloaded
Signature Database Timestamp: UTC 09/21/2022 14:39:24.000
Last Checked: 09/26/2022 09:54:17.272
Anti-Spyware Expiration Date: 05/27/2024

ANTI-SPYWARE GLOBAL SETTINGS

Enable Anti-Spyware ●

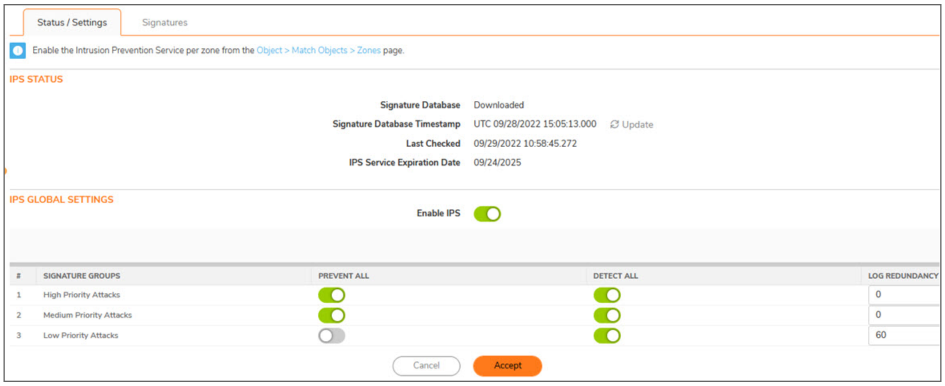
| SIGNATURE GROUPS | PREVENT ALL | DETECT ALL | LOG REDUNDANCY FILTER (SECONDS) |
|---|---|---|---|
| High Priority Spyware | ● | ● | 0 |
| Medium Priority Spyware | ● | ● | 0 |
| Low Priority Spyware | ○ | ● | 60 |

| PROTOCOLS | HTTP | FTP | IMAP | SMTP | POP3 |
|---|---|---|---|---|---|
| Enable Inbound Inspection | ● | ● | ● | ● | ● |

Enable Inspection of Outbound Spyware Communication ●

# Intrusion Prevention

Under **Policy | Security Services | Intrusion Prevention**, leaving the **Prevent All** option on low priority in IPS/IDS is technically lowers security and may potentially produce false positives. Before finalizing your choices, review and test the settings in your environment before deciding how to enable those settings. For more information refer to SonicOS 8 Security Services Administration Guide.



Enable the Intrusion Prevention Service per zone from the Object > Match Objects > Zones page.

IPS STATUS

Signature Database: Downloaded

Signature Database Timestamp: UTC 09/28/2022 15:05:13.000

Last Checked: 09/29/2022 10:58:45.272

IPS Service Expiration Date: 09/24/2025

IPS GLOBAL SETTINGS

Enable IPS: ●

| # | SIGNATURE GROUPS | PREVENT ALL | DETECT ALL | LOG REDUNDANCY |
|---|---|---|---|---|
| 1 | High Priority Attacks | ● | ● | 0 |
| 2 | Medium Priority Attacks | ● | ● | 0 |
| 3 | Low Priority Attacks | ○ | ● | 60 |

# Geo-IP

The **Geo-IP Filter** feature allows you to block connections to or from a geographic location. This is available under **Policy | Security Services**.The network security appliance uses the IP address to determine the connection's location. The feature also allows you to create custom country lists that affect the identification of an IP address. It also allows you to create a custom message when you block a website.

You can also use the **Geo-IP Filter > Diagnostics** tool to show resolved locations, monitor Geo-IP cache and custom country statistics, and look up GEO-IP servers.

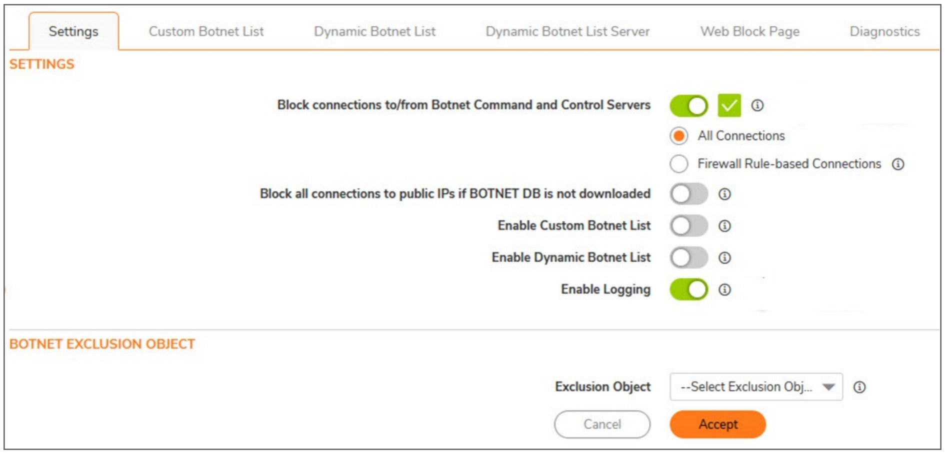
Blocking by Anonymous Proxy and unknown countries is a good default for your base configuration, but you should consider blocking specific countries. On the countries tab, you can move a country between an Allowed Countries list and a Blocked Countries list. For more information refer to SonicOS 8 Security Services Administration Guide.

# Botnet Filter

The Botnet Filter feature enables you to block connections to or from Botnet commands, control servers, and create custom Botnet lists. It also allows you to set up a custom message to send when you block a website or to enable dynamic Botnet HTTP authentication. On this page, you will find information icons that you can hover over for a screen tip. For more information refer to SonicOS 8 Security Services Administration Guide.

Two settings are particularly important when setting the options for Botnet Filter.

1. Navigate to **Policy | Security Services | Botnet Filter**
2. Under the **Settings** tab enable the option to **Block connections to/from Botnet Command and Control Servers** and **Enable Logging**.



SETTINGS

Block connections to/from Botnet Command and Control Servers ☑ ☑

● All Connections

○ Firewall Rule-based Connections

Block all connections to public IPs if BOTNET DB is not downloaded □

Enable Custom Botnet List □

Enable Dynamic Botnet List □

Enable Logging ☑

BOTNET EXCLUSION OBJECT

Exclusion Object: --Select Exclusion Obj...

# App Control

The **POLICY | Security Services| App Control** page provides a way to configure global App Control policies using categories, applications, and signatures. 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 **POLICY | Rules and Policies > App Rules** page. All application detection and prevention configurations are available on the **POLICY | Rules and Policies > App Control** page. For more information refer to SonicOS 8 Security Services Administration Guide.

# Content Filtering

SonicWall offers comprehensive web content security that blocks selected web content and enforces protection and productivity policies. Content Filtering Service (CFS) protects the devices behind the firewall and provides administrators with the means to define and manage policies for groups or individual users. **SonicWall CFS** is available under **POLICY | Security Services| Content Filtering**.

Before configuring Content Filtering make sure CFS is enabled and the database is loaded and the server is ready to go. For more information on Content Filtering refer to SonicOS 8 Content Filtering Administration Guide.

The following content filtering categories are blocked by default. Blocking these categories provides a minimum baseline of protection:

- **Violence/Hate/Racism**
- **Intimate Apparel/Swimsuit**
- **Nudism**
- **Pornography**
- **Weapons**

- **Adult/Mature Content**
- **Cult/Occult**
- **Drugs/Illegal Drugs**
- **Illegal Skills/Questionable Skills**
- **Sex Education**
- **Gambling**
- **Alcohol/Tobacco**
- **Malware**

It is recommended to also block **Not Rated**, but test it before deploying in production.

For a complete list of categories refer to Content Filtering Rating Categories.

7

# 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.

***To enable the SNMP engine:***

1. Navigate to **Device | Settings | SNMP**
2. In the **SNMP** tab, click **Configure**.
3. On the **General** tab configure the SNMP View.

SNMP must be enabled on the interface you wish to monitor from or in the VPN tunnel configuration, if monitoring a remote firewall. For more information about configuring SNMP, refer to SonicOS 8 Device Settings Administration Guide.

8

# Email Automation Setup and Tuning

The **Device | Log | Automation** page includes settings for configuring the SonicWall to send log files using Email and configuring mail server settings. For more information refer to SonicOS 8 Device Log Administration Guide

| Settings | Used to |
|---|---|
| **Email Log Automation** | Automatically send emails, including manual log email dispatching. You can set up email notifications for log digests, alerts, and user creation and activation. Additionally, you can configure the frequency and format of log emails. |
| **Email Audit Records Automation** | Send audit records to specific e-mail addresses automatically on a predefined schedule. |
| **Health Check Email Notification** | Create a predefined email notification with a set subject and body at the times specified by the selected schedule. |
| **Mail Server Settings** | Specify the name or IP address of your mail server, the email address, and the authentication method. You can also enter a POP3 server name or IP address, with username and password. |
| **FTP Log Automation** | Send logs to an FTP server. |

9

# User Authentication

Setting up user authentication is essential for securing user data in applications and websites. These resources provide step-by-step instructions for establishing a secure user authentication system.

- How to Configure LDAP User Authentication
- SonicOS 8 Users Administration Guide
- Configuration Active Directory/LDAP over TLS (Certificate)

Once the user is authenticated, reporting is possible, and session information is displayed in the firewall's status window.

## User Status

The **Device | Users | Status >Users** page displays the **Active User Sessions** on the firewall. Both IPv4 and IPv6 IP addresses are accepted and displayed in the **Active User Sessions** table, which includes:

- User Name
- Domain
- Messaging
- IP Address
- Session Time
- Time Remaining
- Inactivity Remaining
- Type/Mode
- Quota
- User groups

# User Settings

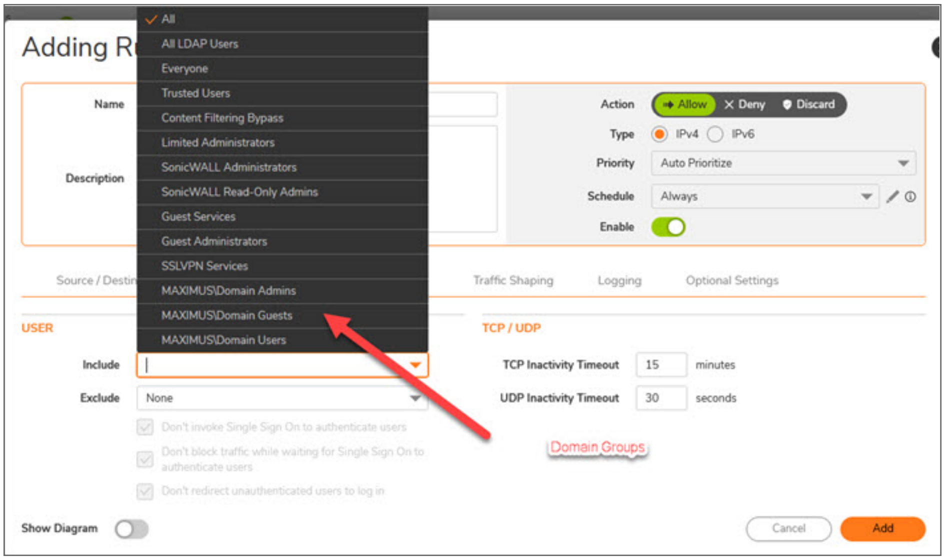
Local users can access the firewall using Radius with NPS, OKTA, or other IdP providers. LDAP can be used with Active Directory or Azure AD via Legacy LDAP over SSL. Capture Client provides the local username to the firewall.

| | |
|---|---|
| **Local Users** | To configure users in the local database using the **Device \| Users \| Local Users and Groups > Local Users (or Local Groups)** tabs. pages. |
| **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 Use RADIUS for user authentication, user much log into the firewall using HTTPS to encrypt the password sent to the firewall. For information on configuring RADIUS, refer to "Configuring Radius" section inSonicOS 8 Users Administration Guide |
| **RADIUS + Local Users** | If you want to use both RADIUS and the SonicWall local user database for authentication. |
| **LDAP** | If you use an LDAP (Lightweight Directory Access Protocol) server or AD (Microsoft Active Directory) to maintain all your user account data. For information on configuring LDAP, refer to "Configuring LDAP" section in SonicOS 8 Users Administration Guide |
| **LDAP + Local Users** | If you want to use both LDAP and the SonicWall local user database for authentication. |
| **TACACS** | If you use Terminal Access Controller Access-Control System Plus (TACAS+) protocol for authentication. For information on configuring LDAP, refer to "Configuring TACACS+" section in SonicOS 8 Users Administration Guide |
| **TACACS+ Local Users** | If you use Terminal Access Controller Access-Control System Plus (TACAS+) protocol and the SonicWall local user database for authentication. |

# LDAP Authentication

LDAP authentication can be used for the following features:

- Access Rules
- Content Filtering
- App Rules
- VPN Access
- DPI-SSL
- AppFlow Reporting/Monitoring
- User Based Reporting



Action: Allow ✕ Deny Discard
Type: ● IPv4 ○ IPv6
Priority: Auto Prioritize
Schedule: Always
Enable

Include:
Exclude: None

☑ Don't invoke Single Sign On to authenticate users
☑ Don't block traffic while waiting for Single Sign On to authenticate users
☑ Don't redirect unauthenticated users to log in

TCP Inactivity Timeout: 15 minutes
UDP Inactivity Timeout: 30 seconds

# Single Sign-On

To enhance visibility into the user behind the traffic, utilize SSO (Single Sign-On). This provides greater visibility in reporting and logs, making it easier to investigate or remediate issues on infected machines. Options include:

- SonicWall SSO Agent or Terminal Services Agent
- SonicWall Capture Client

Directory Services Connector can also be used. It confirms the existence of an AD account when mapping static users. Individual devices need a dummy account created in Active Directory. For more details, refer to SonicWall Directory Connector with SSO 4.1 Administration Guide.

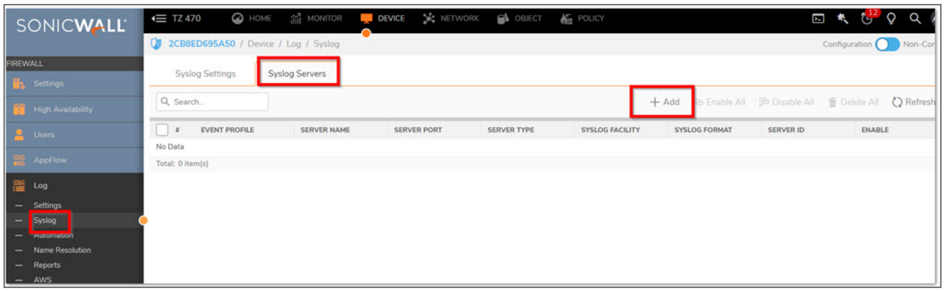
10

# Syslog Setup

The syslog server is a centralized system for logging. It allows to collect error and system logs in one location, decode and coordinate system events across multiple systems during forensic investigations. The logs are aggregated on a syslog collector and can then be fed into a SIEM/XDR platform for a SOC to monitor.

***To configure syslog:***

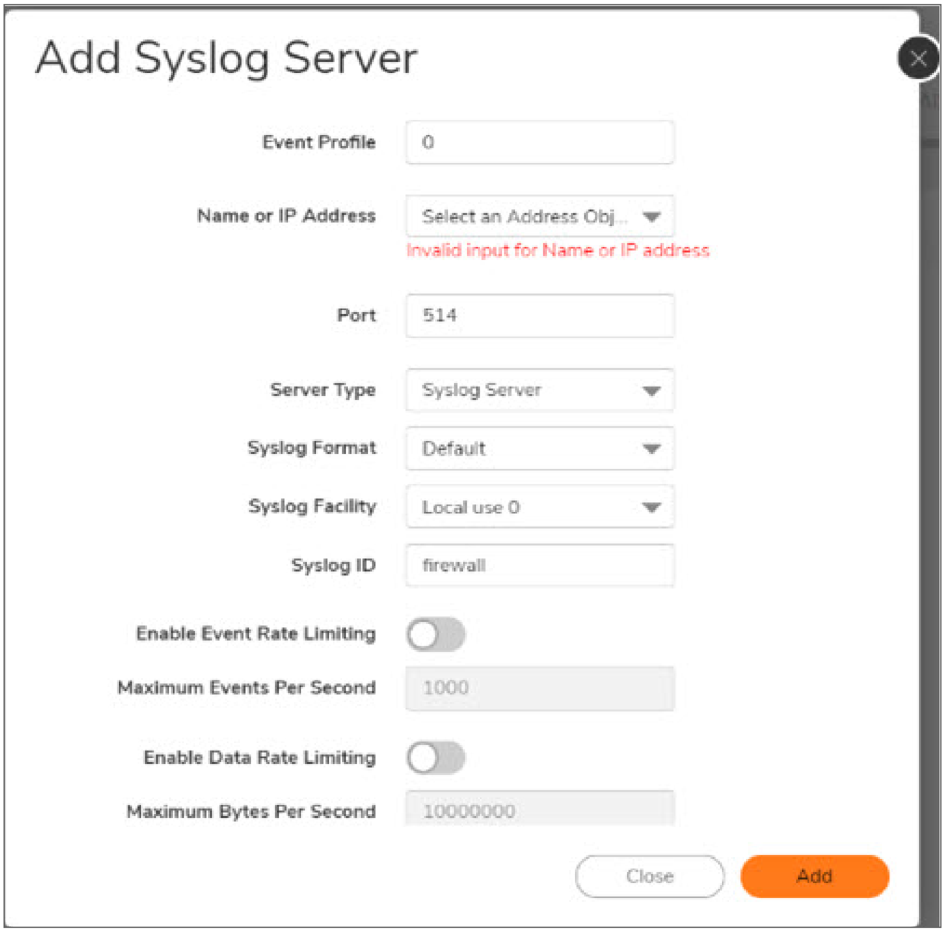
1. Navigate to **Device | Log | Syslog > Syslog Servers**.



| □ | # | EVENT PROFILE | SERVER NAME | SERVER PORT | SERVER TYPE | SYSLOG FACILITY | SYSLOG FORMAT | SERVER ID | ENABLE |
|---|---|---|---|---|---|---|---|---|---|
| No Data | | | | | | | | | |

Total: 0 item(s)

2. Click **+Add**.



Add Syslog Server

| | |
|---|---|
| Event Profile | 0 |
| Name or IP Address | Select an Address Obj... |
| | Invalid input for Name or IP address |
| Port | 514 |
| Server Type | Syslog Server |
| Syslog Format | Default |
| Syslog Facility | Local use 0 |
| Syslog ID | firewall |
| Enable Event Rate Limiting | ○ |
| Maximum Events Per Second | 1000 |
| Enable Data Rate Limiting | ○ |
| Maximum Bytes Per Second | 10000000 |

3. Select the **Name or IP Address** of the Syslog server from the drop-down list.
4. Update fields as needed and click **Add**.

11

# DPI-SSL

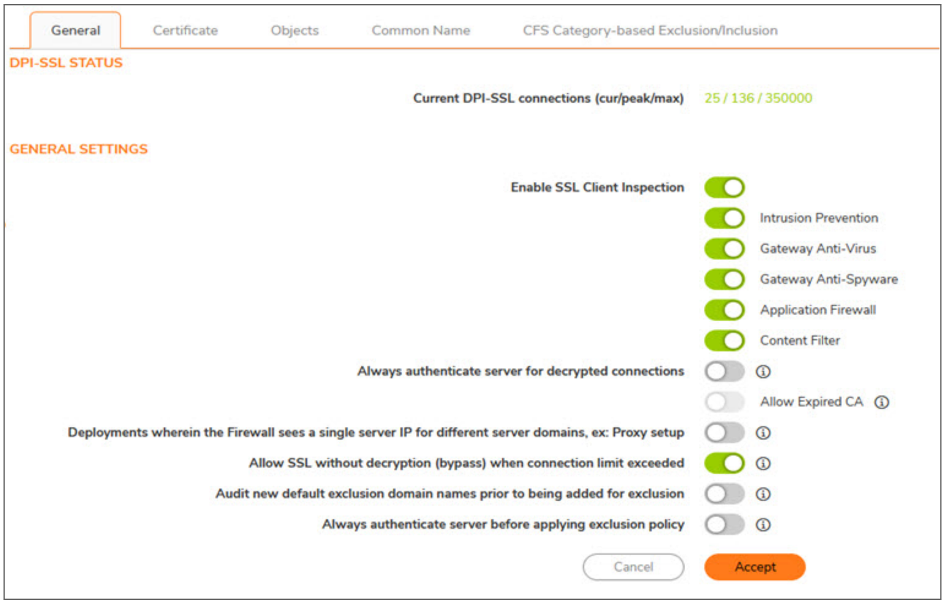
Deep Packet Inspection of Secure Socket Layer (DPI-SSL) is an extension of SonicWall's Deep Packet Inspection technology. It allows for the inspection of encrypted HTTPS traffic and other SSL-based traffic. The SSL traffic is decrypted (intercepted) transparently, scanned for threats, and then re-encrypted before being sent along to its destination if no threats or vulnerabilities are found. DPI-SSL provides additional security, application control, and data leakage prevention for analyzing encrypted HTTPS and other SSL-based traffic.

**Policy > DPI-SSL** is deployed in two main scenarios:

- **Client DPI-SSL**
- **Server DPI-SSL**

For decrypted and intercepted connections, use DPI-SSL:

- Blocks connections to sites with untrusted certificates
- Blocks connection if the domain name in client
- Does not validate against the Server Certificate for this connection



DPI-SSL STATUS

Current DPI-SSL connections (cur/peak/max) 25 / 136 / 350000

GENERAL SETTINGS

Enable SSL Client Inspection ☑

☑ Intrusion Prevention

☑ Gateway Anti-Virus

☑ Gateway Anti-Spyware

☑ Application Firewall

☑ Content Filter

Always authenticate server for decrypted connections ☐ ⓘ

☐ Allow Expired CA ⓘ

Deployments wherein the Firewall sees a single server IP for different server domains, ex: Proxy setup ☐ ⓘ

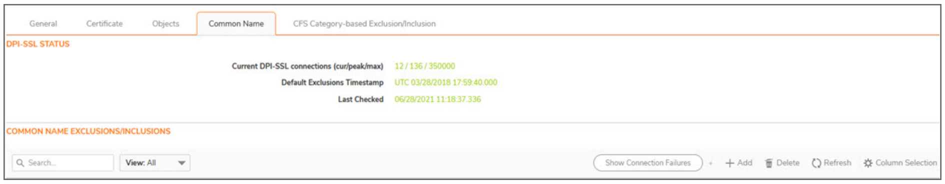
Allow SSL without decryption (bypass) when connection limit exceeded ☑ ⓘ

Audit new default exclusion domain names prior to being added for exclusion ☐ ⓘ

Always authenticate server before applying exclusion policy ☐ ⓘ

### *To fix connection failures:*

1. Navigate to **Policy | DPI-SSL | Client SSL > Common Name**.

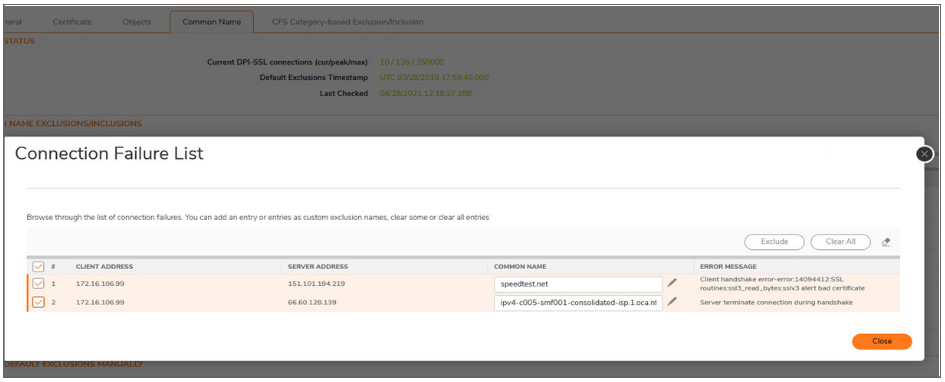


DPI-SSL STATUS

Current DPI-SSL connections (cur/peak/max) 12 / 136 / 350000
Default Exclusions Timestamp UTC 03/28/2018 17:59:40.000
Last Checked 06/28/2021 11:18:37.336

COMMON NAME EXCLUSIONS/INCLUSIONS

2. Check the boxes to see if something was mistakenly blocked and click the **Exclude** button. A custom exemption is automatically created and takes effect immediately.



STATUS

Current DPI-SSL connections (cur/peak/max) 10 / 136 / 350000
Default Exclusions Timestamp UTC 03/28/2018 17:59:40.000
Last Checked 06/28/2021 12:18:37.288

NAME EXCLUSIONS/INCLUSIONS

Connection Failure List

Browse through the list of connection failures. You can add an entry or entries as custom exclusion names, clear some or clear all entries

| ☑ | # | CLIENT ADDRESS | SERVER ADDRESS | COMMON NAME | ERROR MESSAGE |
|---|---|---|---|---|---|
| ☑ | 1 | 172.16.106.99 | 151.101.194.219 | speedtest.net | Client handshake error-error:14094412:SSL routines:ssl3_read_bytes:sslv3 alert bad certificate |
| ☑ | 2 | 172.16.106.99 | 66.60.128.139 | ipv4-c005-smf001-consolidated-isp.1.oca.nf | Server terminate connection during handshake |

12

# AppFlow Reporting and Monitoring

With the AppFlow feature, you can manage the firewall's flow reporting, statistics, and settings to send data to a local collector or external AppFlow server. The feature supports various external reporting formats and includes support for Quest™ Change Auditor for SonicWall. On the **DEVICE | AppFlow | Flow Reporting** page, you can configure the firewall to view statistics based on Flow Reporting and Internal Reporting.

Once the AppFlow reports are enabled and configured, you can view and monitor aggregated reports and evaluate your firewall's performance on **Monitor | AppFlow | AppFlow Report**.

**Topics:**

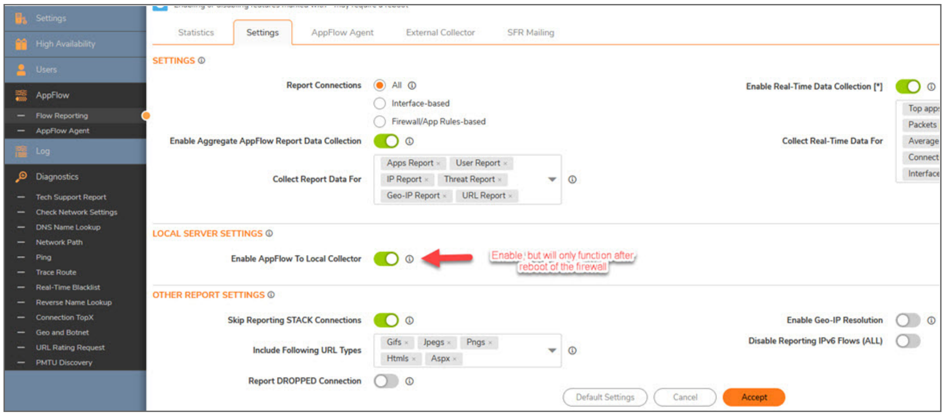
- AppFlow Reporting
- AppFlow Monitoring
- Capture Threat Assessment Report

## AppFlow Reporting

The AppFlow collector offers detailed, clickable session information for various web categories, including intrusions, virus details, and more.

***To enable AppFlow reporting:***

1. Navigate to **Device | AppFlow | Flow Reporting > Settings**.
2. In the **Local Server Settings** section, click the switch to **Enable AppFlow To Local Collector**.



SETTINGS

Report Connections ● All ○ Interface-based ○ Firewall/App Rules-based

Enable Aggregate AppFlow Report Data Collection: on

Collect Report Data For: Apps Report, User Report, IP Report, Threat Report, Geo-IP Report, URL Report

Enable Real-Time Data Collection [*]: on

Collect Real-Time Data For: Top apps, Packets, Average, Connect, Interface

LOCAL SERVER SETTINGS

Enable AppFlow To Local Collector: on

Enable, but will only function after reboot of the firewall

OTHER REPORT SETTINGS

Skip Reporting STACK Connections: on

Include Following URL Types: Gifs, Jpegs, Pngs, Htmls, Aspx

Report DROPPED Connection: off

Enable Geo-IP Resolution: off

Disable Reporting IPv6 Flows (ALL): off

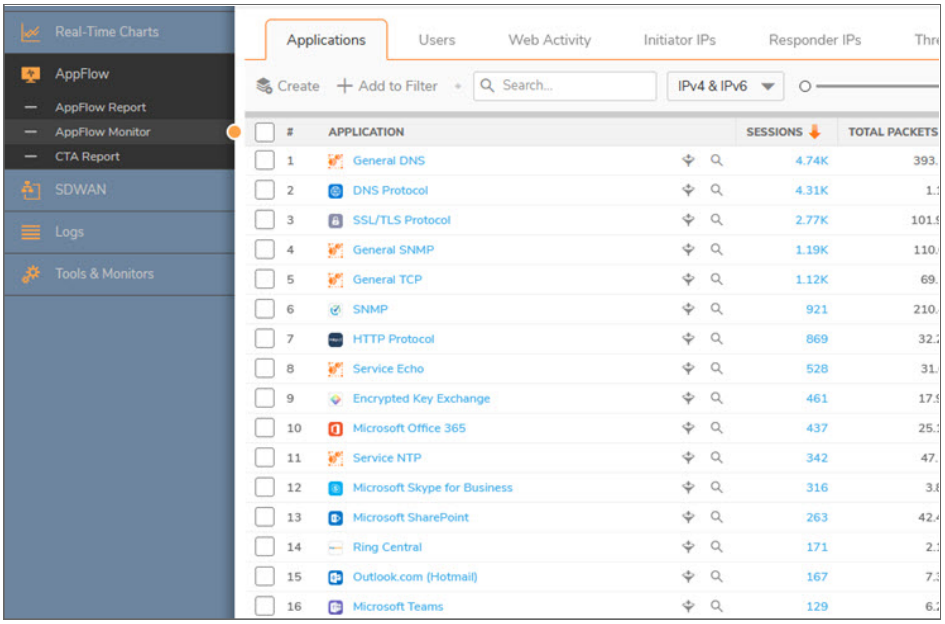
ⓘ | **IMPORTANT:** A reboot is required for the AppFlow reporting to start working properly.

For more details about configuring AppFlow reporting, refer to SonicOS 8 AppFlow Device Administration Guide.

# AppFlow Monitoring

The following are a few quick tips for monitoring the AppFlow reports. For more details on AppFlow monitoring, refer SonicOS 8 Monitor Guide.

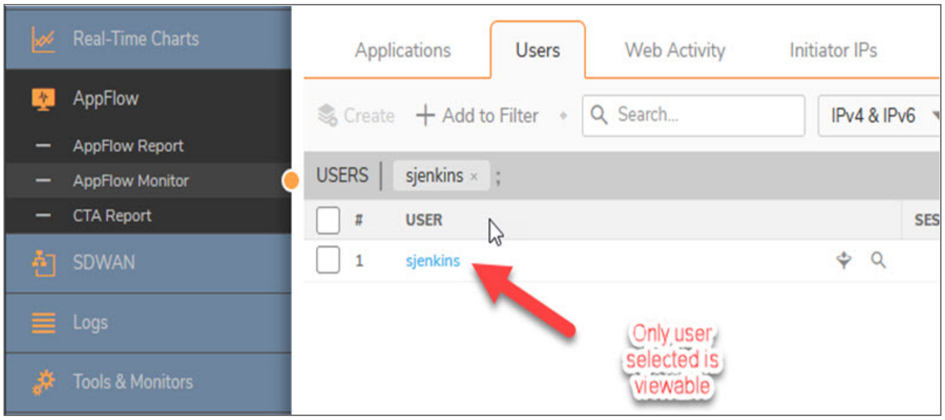
When viewing the AppFlow Monitor option (**Monitor | AppFlow | AppFlow Monitor**), ensure to use the firewall in configuration mode and logged in as admin. You can access the applications through the firewall. You can also gather information on a per-user and per-session basis.



| # | APPLICATION | SESSIONS | TOTAL PACKETS |
|---|---|---|---|
| 1 | General DNS | 4.74K | 393. |
| 2 | DNS Protocol | 4.31K | 1. |
| 3 | SSL/TLS Protocol | 2.77K | 101. |
| 4 | General SNMP | 1.19K | 110. |
| 5 | General TCP | 1.12K | 69. |
| 6 | SNMP | 921 | 210. |
| 7 | HTTP Protocol | 869 | 32. |
| 8 | Service Echo | 528 | 31. |
| 9 | Encrypted Key Exchange | 461 | 17. |
| 10 | Microsoft Office 365 | 437 | 25. |
| 11 | Service NTP | 342 | 47. |
| 12 | Microsoft Skype for Business | 316 | 3. |
| 13 | Microsoft SharePoint | 263 | 42. |
| 14 | Ring Central | 171 | 2. |
| 15 | Outlook.com (Hotmail) | 167 | 7. |
| 16 | Microsoft Teams | 129 | 6. |

***To monitor per user.:***

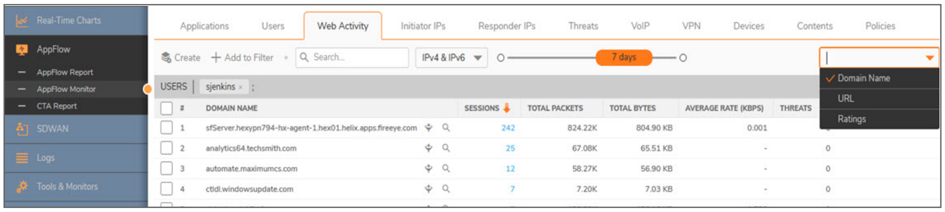
1. Navigate to **Monitor | AppFlow | AppFlow Monitor > Users**.
2. Select the **USER** checkbox.
3. Click **+Add to Filter**. Each tab shows only user-filtered data for websites and activity.



| □ | # | USER | SES |
|---|---|---|---|
| □ | 1 | sjenkins | |

Only user selected is viewable

4. Click the **Web Activity** tab and view reports listed by **Domain Name**, **UL** and **Web Rating**. Traffic data rates and threat data are also includes in this display.

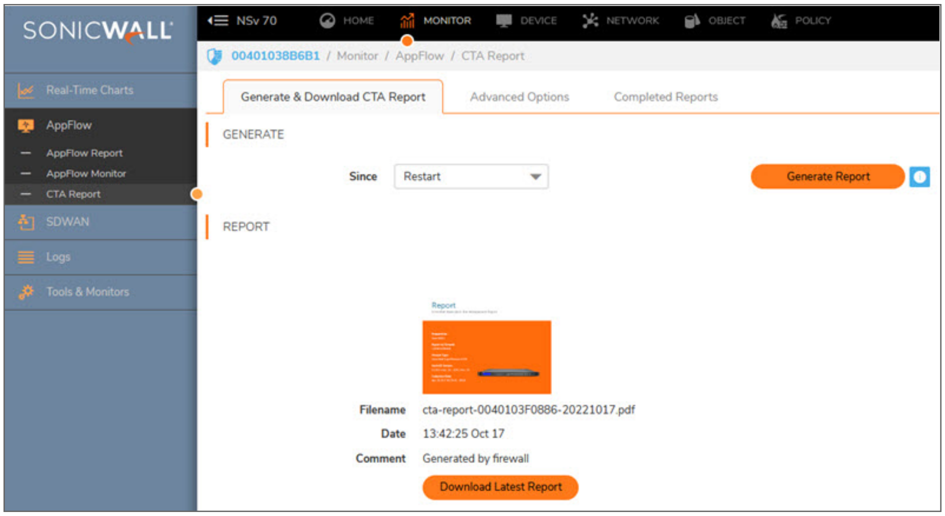


| □ | # | DOMAIN NAME | SESSIONS | TOTAL PACKETS | TOTAL BYTES | AVERAGE RATE (KBPS) | THREATS |
|---|---|---|---|---|---|---|---|
| □ | 1 | sfServer.hexypn794-hx-agent-1.hex01.helix.apps.fireeye.com | 242 | 824.22K | 804.90 KB | 0.001 | |
| □ | 2 | analytics64.techsmith.com | 25 | 67.08K | 65.51 KB | - | 0 |
| □ | 3 | automate.maximumcs.com | 12 | 58.27K | 56.90 KB | - | 0 |
| □ | 4 | ctldl.windowsupdate.com | 7 | 7.20K | 7.03 KB | - | 0 |

# Capture Threat Assessment Report

Capture Threat Assessment (CTA) is a service offered by SonicWall that generates network traffic and threat reports. This service is accessible directly from the SonicOS firewall interface. To generate the report, you can go to the Capture Threat Assessment page. The report is generated in PDF format and previous reports are saved in the cloud and displayed in a table for later access. For more information about the CTA Report, refer to the CTA User Guide.

1. Navigate to **Monitor | AppFlow | CTA Report > Generate and Download CTA Report**.



Since: Restart

Filename: cta-report-0040103F0886-20221017.pdf

Date: 13:42:25 Oct 17

Comment: Generated by firewall

2. Click on **Generate Report**, and once it is finished, click **Download Latest Report**.

13

# SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

# About This Document

SonicOS TZ80 Getting Started Guide
Updated - November 2024
Software Version - 8
232-006201-00 Rev A

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

## Open Source Code

SonicWall Inc. 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 USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035