SonicOS 7.1

Release Notes

These release notes provide information about these SonicWall SonicOS 7.1.2 releases:

Versions:

Version 7.1.1-7058

June 2024

This version of SonicOS 7.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

IMPORTANT: In this firmware version, CFS and DPI-SSL supports the TLS hybridized Kyber feature on Chrome and Edge browsers (GEN7-48526 and GEN7-47567).

Important

- This SonicOS 7.1 firmware will not be available on MySonicWall for NSsp 15700. Please contact your Service Account Manager for the firmware.
- If you are managing your firewall using Network Security Manager (NSM), make certain that you are using NSM version 2.4 or later.
- Downgrading to SonicOS 7.0.1 from SonicOS 7.1 is not supported.
- Upgrading SonicOS 7.0.1 to 7.1 for NSv requires a fresh installation of NSv for all platforms. (For more information, refer to NSv upgrade from 7.0.1 to 7.1.1.)
- Use the Firmware Auto Update Feature in SonicOS 7.1 to ensure that your firewall always has the latest updates for critical vulnerabilities. (For more information, refer to Firmware Auto Update.)

Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.

Supported Platforms

The platform-specific versions for this unified release are all the same:

Platform	Firmware Version
TZ Series	7.1.1-7058
NSa Series	7.1.1-7058
NSv Series	7.1.1-7058
NSsp Series	7.1.1-7058

- TZ270 / TZ270W
- TZ370 / TZ370W
- TZ470 / TZ470W
- TZ570 / TZ570W
- TZ570P
- TZ670

- NSa 2700
- NSa 3700
- NSa 4700
- NSa 5700
- NSa 6700

- NSv 270
- NSv 470
- NSv 870

- NSsp 10700
- NSsp 11700
- NSsp 13700
- NSsp 15700

SonicOS NSv deployments are supported on the following platforms:

- AWS (BYOL and PAYG)
- Microsoft Azure (BYOL)
- VMware ESXi
- Microsoft Hyper-V
- Linux KVM

Resolved Issues

Issue ID	Issue Description
GEN7-33934	Users are unable to send emails with attachments larger than 1MB when DPI-SSL is enabled.
GEN7-39872	Users may be intermittently disconnected when using NetExtender and downloading a file.
GEN7-46338	Bandwidth Management is not working in an App Rule when the action object is selected to use a BWM object.
GEN7-47327	The Virtual Office web page times out and displays a blank white screen.

Issue ID	Issue Description
GEN7-47567	App Rules over DPI-SSL are not working when TLS hybridized Kyber support is enabled on Chrome browsers. (This support is now enabled by default on Chrome browsers).
GEN7-47628	The ability to update microcode using Safe Mode has been added to be used under direction of customer support when needed.
GEN7-47736	SSL-VPN licenses are being consumed, preventing users from connecting.
GEN7-47756	Login fails when an user with accent characters in their name when using LDAP authentication.
GEN7-47953	*All TZ models, NSa 2700, and NSa 3700 only:* Under some conditions, the core dump storage may grow larger than 500 MB in size.
GEN7-48149	The hardware monitor controller may report occasional false alarms, including fan failures.
GEN7-48173	Two-Factor Authentication via TOTP fails for LDAP and Radius users when using NetExtender.
GEN7-48288	Logging in using Radius using a RSA pin authentication for SSLVPN users fails.
GEN7-48420	Stack-based buffer overflow vulnerability in SonicOS HTTP server (SNWLID-2024-0008)
GEN7-48526	Content Filtering Service (CFS) blocking over DPI-SSL is not working when TLS hybridized Kyber support is enabled on Chrome browsers. (This support is now enabled by default on Chrome browsers).
GEN7-48612	Heap-based buffer overflow vulnerability in SonicOS SSL-VPN (SNWLID-2024-0009)
GEN7-49115	When using DPI-SSL, the block page may sometimes fail to display.
GEN7-49189	Under some conditions, the firewall might restart itself when handling error conditions.
GEN7-49451	*NSsp 15700 only:* The default buffer size for a non-master blade when fetching the Geo-IP map database may experience an overflow if the database size exceeds the maximum limit.

Known Issues

Issue ID	Issue Description
GEN7-43016	When deploying an NSv using an `.ova` file on VMWare ESXi 8.0., the error message `Disk image missing` is displayed.
GEN7-43500	After changing the name of a local user, the entry is still displayed in the **Server DPI SSL Inclusion** and **Server DPI SSL Exclusion** lists and the user with the changed name cannot be selected.
GEN7-43554	Unable to add valid domains to the **Custom Malicious Domain Name List** and **White List** pages after adding an invalid domain because the pending configuration is still present.

Issue ID	Issue Description
GEN7-44642	*NSsp 15700 only:* HTTPS management on X1 is not accessible when the MGMT/Chassis IP and X1/Aux IP are in the same subnet.
GEN7-45252	*NSsp 15700 only:* A Standby firewall may occasionally fail to start from uploaded firmware. The message `Wrong firmware to boot` is displayed in printed in the command-line interface (CLI) after clicking **Restart image with current settings**.
GEN7-47528	When installing the NetExtender software from the SSL VPN portal page for 32-bit Windows, the message `The installer is only for x64 machine` is displayed.

Additional References

GEN7-46935, GEN7-47809, GEN7-47928, GEN7-48060, GEN7-48185, GEN7-48198, GEN7-48389

Version 7.1.1-7051

March 2024

This version of SonicOS7.1.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

Important

- If you are managing your firewall using Network Security Manager(NSM), make certain that you are using NSM version 2.4 or later.
- Downgrading to SonicOS 7.0.1 from SonicOS 7.1.1 is not supported.
- Upgrading SonicOS 7.0.1 to 7.1.1 for NSv requires a fresh installation of NSv for all platforms. (For more information, refer to NSv upgrade from 7.0.1 to 7.1.1.)
- Use the Firmware Auto Update Feature in SonicOS 7.1.1 to ensure that your firewall always has the latest updates for critical vulnerabilities. (For more information, refer to Firmware Auto Update.)

Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.

Resolved Issues

Issue ID	Issue Description
GEN7-37742	SSH login to the management console is not allowed for cloud instances.
GEN7-41340	The connected route of sub-VLAN WAN interface turns gray when its parent interface is set to **Unassigned**.
GEN7-42260	Syslog traffic is not being generated when two or more syslog servers are configured.
GEN7-43029	SonicOS SSL VPN Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability: SNWLID-2024-0005
GEN7-44112	The error **Firmware upload image failed** is displayed on some firewalls when upgrading the firmware.
GEN7-44483	When FIPS mode is enabled, there are no AES GCM encryption options in the IPSec phase 2 proposal of a VPN policy.
GEN7-44805	When NAC is enabled, using a Policy Mode security policy does not work correctly in conjunction with the threat user group.
GEN7-44806	When using NAC, TCP and UDP traffic send from a Threat User and received on a non-master blade security policy is not triggered and traffic and will be incorrectly dropped or allowed.
GEN7-44809	The firewall may intermittently fail to export the Tech Support Report (TSR).
GEN7-44899	DNS rules do not support address objects of type MAC or FQDN.
GEN7-44909	The **Threat Logs** page does not display any data until **Refresh** is clicked.
GEN7-45060	A TZ series firewall may intermittently restart when two SonicWave access points are connected using the built-in wireless using the mesh gateway method and the **Radio Mode** is changed from 2.4G to 5g mixed-80M-48 on the **Internal Wireless** page .
GEN7-45077	Clicking **Graph** on the **Access Rules** page displays the message **No Data** for **Used Rules** when **All** is selected for the **Since** filter.
GEN7-45081	When logged into a firewall managed by Network Security Manager (NSM), and the session has expired, clicking on **Config** or **Non-Config** will fail without allowing the administrator to login again.
GEN7-45110	Editing an NAC policy in an Access Rule, then changing the source address group, causes the error message ***<address object name>* is not a reasonable value** to be displayed.
GEN7-45225	When UO is configured as Final Backup in WAN Load Balancing, and X1 is not configured, the web management interface and console diagnostic pings cannot reach the internet.

Issue ID	Issue Description
GEN7-45474	The firewall drops TLS 1.2 traffic with a SSHv2 payload because some TCP packets are mistakenly recognized by the firewall as sslv2 clienthello packets. The log shows `HTTPS Access Denied: SSL2.0 (Unidentified), SSL Control: Weak SSL Version being used.`
GEN7-45497	Virtual Office is not accessible when HTTPS management is disabled in the interface configuration.
GEN7-45508	The **Real-time Monitor**, **BWM Monitor**, and **SD-WAN Monitor** pages under the **Monitor** tab are not loading and the graphs are not being displayed when using Classic View.
GEN7-45522	Unable to configure a Virtual sub-interface when the interface is configured in L2 Bridge mode.
GEN7-45578	SD-WAN routes are not disabled on the **Routing Rules** page when all of the interfaces in the SD-WAN group are not qualified.
GEN7-45837	A PDF file declared benign by Capture ATP when **Block Until Verdict** is enabled is counted as a virus by AppFlow Reports and Network Security Manager (NSM) when using HTTPS only.
GEN7-46037	Thermal alerts are intermittently displayed for some devices, but are a false alarm.
GEN7-46038	Unable to enable FIPS Mode in a High Availability configuration.
GEN7-46044	Integer-Based Buffer Overflow Vulnerability In SonicOS via IPSec: SNWLID-2024-0004
GEN7-46111	When setting an interface in WLAN zone L2 Bridge mode, the bridged-to list does not contain VLAN interfaces.
GEN7-46319	Configuring DDNS with `dyn.com` displays the error **Network error** in the status.
GEN7-47176	DNS rebinding attack prevention is now available for the DNS Proxy feature.
GEN7-47177	Duplicate records are displayed on AppFlow Report **Users** tab.
GEN7-47373	The NetExtender version is updated to the latest release (v10.2.339). If the NetExtender client **Autoupdate** option is enabled on the **Firewall SSL VPN/Client** settings page, NetExtender clients will check for the newer version and automatically update to v10.2.339.
GEN7-45735	CVE-2023-48795: Prefix Truncation Attacks in SSH Specification (Terrapin Attack): SNWLID-2024-0002

Known Issues

Issue ID	Issue Description
GEN7-28519	BGP cannot be established when MD5 authentication is enabled.
GEN7-34246	Browser NTLM Authentication functionality is not functioning as expected. Users must log in to the device in order to authenticate.
GEN7-34484	Audit logs are cleared after the firewall is restarted.

Issue ID	Issue Description
GEN7-41102	The **Password Change** page is not prompting for a new password when **Password change** is enabled on the firewall for a Imported user.
GEN7-41593	When upgrading a High Availability pair, if LACP is enabled, then High Availability should be disabled to upgrade and each unit has to be upgraded separately.
GEN7-41996	When disabling the **Automatically adjust clock for daylight saving time** setting, no change is made to the current system time.
GEN7-43016	NSv deployment displays the error **disk image missing** when using an `.ova` file on VMWare ESXi UI version 8.0. **Workaround:** 1. Unzip the `.ova` file to three files: `vmdk` file, `nvram` file and `ovf` file. 2. Upload the three files instead of the `.ova` file.
GEN7-43500	After changing the name of a local user, the entry is still displayed in the Server DPI-SSL Exclusion and Server DPI SSL Inclusion lists and the user with the changed name cannot be selected.
GEN7-43554	Unable to add valid domains to the **Custom Malicious Domain Name** list and **White List** pages after adding an domain one because the pending configuration is still present. **Workaround:** Logging out and back in should resolve the issue.
GEN7-44642	*For NSSP 15700 only:* HTTPS Management on X1 is not accessible when the MGMT/Chassis IP and X1/Aux IP are in the same subnet.
GEN7-45252	*For NSSP 15700 only:* An intermittent issue occurs when the Standby firewall fails to start from uploaded firmware. `Wrong firmware to boot` is displayed in printed in the command-line interface (CLI) after clicking the restart image with current settings. **Workaround:** Perform a forced failover of the firewall. The upgrade should now be successful.
GEN7-45303	When there are a large number of FTP-data channels (200,000), where the sessions expire in a short time interval causing the deletion of the caches, this can cause the device to have a high CPU usage and become unresponsive when handling the connection cache timer. This scenario is extremely unlikely to occur but is a current limitation of the firewall.
GEN7-46030	When an incorrect firmware file is uploaded using the **Firmware Upload** page, no error is displayed.
GEN7-47528	When installing the NetExtender software from the SSL VPN portal page for 32-bit Windows, the message `The installer is only for x64 machine` is displayed. **Workaround:** Download and install the NetExtender software directly from sonicwall.com.

Additional References

GEN7-40887, GEN7-43525, GEN7-43829, GEN7-44593, GEN7-44698, GEN7-44721, GEN7-44840, GEN7-45101, GEN7-45130, GEN7-45261, GEN7-45381, GEN7-45577, GEN7-45603, GEN7-45833, GEN7-45834, GEN7-45867, GEN7-45958, GEN7-45979, GEN7-45988, GEN7-46002, GEN7-46032, GEN7-46075, GEN7-46211, GEN7-46823, GEN7-47187, GEN7-47260, GEN7-47283

Version 7.1.1-7047

February 2024

This version of SonicOS 7.1.1 is a maintenance release for SonicWall next-generation firewalls and provides a fix for SNWLID-2024-0003.

Important

- If you are managing your firewall using Network Security Manager(NSM), make certain that you are using NSM version 2.4 or later.
- Downgrading to SonicOS 7.0.1 from SonicOS 7.1.1 is not supported.
- Upgrading SonicOS 7.0.1 to 7.1.1 for NSv requires a fresh installation of NSv for all platforms. (For more information, refer to NSv upgrade from 7.0.1 to 7.1.1.)
- Existing SonicOS 7.1.1-7040 NSv deployments can use `.sig` files to upgrade to SonicOS 7.1.1-7047.
- Use the Firmware Auto Update Feature in SonicOS 7.1.1 to ensure that your firewall always has the latest updates for critical vulnerabilities. (For more information, refer to Firmware Auto Update.)
- For additional information about this update, refer to this PSIRT Advisory.

Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.

Version 7.1.1-7040

December 2023

SonicOS 7.1.1 is a major feature release of SonicOS.

Important

- The SonicOS 7.1.1 firmware will not be available on MySonicWall for NSsp 15700. Please contact your Service Account Manager for the firmware.
- Network Security Manager (NSM) 2.3.5 does not support SonicOS 7.1.1. NSM 2.4 will support SonicOS 7.1.1.

Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.

What's New

- **DNS Filtering**

  Introduces a significant update aimed at enhancing the security and efficiency of your online experience, including:

  - ***Safeguarding Against Malicious Websites:*** Proactively blocking access to known malicious domains through DNS filtering mitigates the risk of malware infections and other cyberattacks.
  - ***Enhancing Bandwidth:*** By blocking access to unnecessary or undesirable websites, it reduces bandwidth consumption and optimizes internet speeds
  - ***Filtering Inappropriate Content:*** DNS filtering delivers an additional layer of protection by blocking access to websites hosting explicit content, violence, or objectionable material.

- **Content Filtering 5.0**

  Introducing Content Filtering Engine 5.0 provides major enhancements:

  - ***Category Extension:*** Increases number and types of supported categories, resulting in improved categorization of websites.
  - ***Reputation-based blocking:*** Reputation-based URL blocking proactively identifies and blocks suspicious entities based on Reputation.

- **Network Access Control Support**

  SonicOS provides APIs so that NAC vendors can pass security context to SonicWall firewalls. Using the security context, SonicOS builds policies for mitigation actions, fetches dynamic user roles and other information from the NAC vendor to build information models and perform the traffic filtering. SonicOS can support multiple NAC servers from different vendors simultaneously.

- **SonicWave AX Support**

  SonicOS 7.1.1 integrates SonicWave 600 Series Access Points with the firewall.

  ⓘ **NOTE:** If you have SonicWave 600 Series Access Points connected to a WLAN zone of a firewall configured with version 7.0.x and managed by WNM, the access points will be acquired by the firewall after updating the firewall to SonicOS 7.1. After upgrading the firewall, all WNM settings will no longer be available. To ensure seamless management, disable SonicPoint/SonicWave management on the WLAN zone.

- **NSv Enhancements**

  - ***NSv Base Updated from SonicCore to SonicCoreX***

    This update introduces Secure Boot, UEFI Virtual TPM, and many performance enhancements.

  - ***NSV Bootstrapping***

    SonicOS 7.1.1 introduces a bootstrapping ability on NSvs that provide an agile, consistent, and scalable process for setting up NSv firewalls for mass deployments.

    Token-based Registration

    Token-Based Registration replaces the MySonicWall username and password in the bootstrap file with a string to automate mass deployments with basic configuration and licensing information. This also helps prevent misuse of MySonicWall credentials, which can be used for accessing information on other registered products with the same account.

  ⓘ **IMPORTANT:** Upgrading to the 7.1.1 version of NSv requires that you deploy a new NSv installation and import backup settings and certificates exported from your current installation. For more information, see NSv upgrade from 7.0.1 to 7.1.1.

- **Automatic Update Firmware Support**

  This feature simplifies the process of keeping your firewall up-to-date with the latest firmware versions, patches, and security updates.

  ⓘ **NOTE:** This feature is not supported on NSsp 15700.

- **Ability to store Threat/System Monitor, Audit Log, and Packet Capture files on an external storage module**

  Use external storage to store System Logs, Threat Logs, AppFlow reporting data, and Packet Captures, ensuring that the historical data for these features remains even after a firewall restarts. You can also search the data saved on external storage.

  ⓘ **NOTE:** This feature is not supported on NSsp 15700.

- **UI Monitor and Page Enhancements**

  SonicOS 7.1.1 introduces several user interface enhancements to improve its ease of use:

  - The **Dashboard** displays the details about the last License Manager Contact for License synchronization and signature updates.
  - A new Capture Labs icon is available on the Help Slider. When you click this icon, a new browser tab or window is opened that displays the SonicWall Capture Labs website.
  - The Objects and Rules relationship viewer provides a graphical representation of the security and access rules.
  - You can now use Global Search to search for values specified for objects and profiles.

- **Policy Mode Enhancements**

  - ***Intrusion Protection Service (IPS) Tuning Capabilities***

    You can now selectively enable and disable specific Intrusion Protection Service rules.

    SonicOS 7.1.1 allows administrators to bypass a specific set of IPS signatures from being checked, reducing false alarms by selectively disabling selected IPS signatures.

    On the **Object > IPS Threat** page, the IPS signatures are enabled by default. Disable the IPS signatures you want ignored without the system taking any action.

  - ***Gateway Anti-Virus and Anti-Spyware Threat Profile Support***

    Administrators can now configure Anti-Spyware and Gateway Anti-Virus profiles as action profiles. Signatures can be configured so that they require verification for specific security policies while ignoring the other signatures. This enhancement eliminates unnecessary checks for known signatures.

  - ***Ability to enable Management tabs (HTTPS/PING/SSH) and Source (IP) on Interfaces***

    SonicOS 7.1.1 provides the ability to enable management service features such as HTTP, HTTPS, Ping, SNMP, and SSH, and to allow those services to be managed from a specific IP address object or a group on any interface.

  - ***Ability to view Anti-Spyware, Gateway Anti-Virus, and Intrusion Prevention Profile Objects***

    SonicOS7.1.2 simplifies the rule creation and allows users to view all Objects and Profiles in a single page, regardless of their location within the application. The Object Viewer feature enables users to get a summary of the Objects and Profiles in the User Interface .If a searched object needs to be used in a Rule, users can simply drag and drop it into the appropriate dropdown menu in the Rule page, making it more convenient to find and select the desired object.

  - ***Shadow feature enhancements***

    SonicOS7.1.2 extends the Shadow feature to work over a large number of policies or rules, adding the ability to edit a group of security rules, and to add rules above or below based on the location of an existing rule.

  - ***Improved filtering and searching***

    SonicOS 7.1.1 extends filtering and searching support by adding column-based filtering. The firmware version and serial number is now displayed on the side bar so that it is always visible.

- **Active/Standby High Availability Support for SonicWall Capture Security Appliance**
    - SonicOS 7.1.1 provides the Active/Standby High Availability Support for the SonicWall Capture Security Appliance.
- **Tooling Support Enhancements**

  Several enhancements have been made to some diagnostics and reporting tools on the **Tech Support Report** page.
    - The layout was changed to add an **Action** section where you can download several different reports.
    - A tooltip was added for the **Download System Logs** button.
    - The System Logs file package includes event logs in CSV format.

Resolved Issues

Issue ID	Issue Description
GEN7-15658	Packet capture is not displaying some application signatures.
GEN7-19707	Unable to disable the **Allow Geo-IP/Botnet Filter map database file upload** option.
GEN7-24864	Packet mirroring does not work for a local packet mirror.
GEN7-26633	Inbound audio for both incoming and outgoing calls is unavailable when SIP UDP frames are above certain size.
GEN7-28520	A Red or Yellow alert does not trigger the Alarm indicator on the front panel of the firewall.
GEN7-31345	SMB File transfer speed over VPN drops significantly when the files are copied to LAN device behind an NSv instance in Azure.
GEN7-31899	The configuration on the DOS policy page cannot be audited
GEN7-35181	**Synchronize Firmware** may not work as expected under some conditions.
GEN7-35248	Deleting the DHCPv6 prefix delegation for one interface will clear the prefix delegation configuration on other interfaces.
GEN7-35275	The effect of enabling **Enforce DNS Proxy For All DNS Requests** in the web management interface has been improved: If a firewall sends a DNS query itself, this kind of packets will not pass into the DNS proxy module. 2. On the **Diagnostics** page, if we add a static domain entry in static cache, and enable this option, this domain won't be resolved. but it doesn't matter if FW resolves static entry in other non-stack modules.
GEN7-36178	FTP automation fails if the server response time takes more than 2 seconds.
GEN7-37282	*TZ models, NSa2700, NSa3700, and NSv models only:* The connection cache will not correctly synchronize with the standby appliance if the Stateful Failover setting is disabled and then enabled again..

Issue ID	Issue Description
GEN7-37326	Editing the WAN GroupVPN settings and then immediately enabling or disabling WAN GroupVPN will cause some configuration settings to be lost.
GEN7-37501	After the Deny MAC-filter list containing a wireless client MAC is changed to **No MAC address** or if the deny mac-filter list has been disabled, the wireless client is still blocked.
GEN7-37511	When trying to configure the gateway when adding a policy-based route using **6to4AutoTunnel**, the error **Gateway must be default** is displayed.
GEN7-38529	With devices with a MGMT interface, the default High Availability heartbeat interface is **MGMT**. The default should be **Control HA interface**.
GEN7-38767	The SSL VPN portal cannot handle jumbo frames correctly.
GEN7-39795	The **Packet Monitor** page in not displayed when a user logs in as a system administrator.
GEN7-39850	The management interface will display the warning **Gateway must be default** when choosing an 6to4AutoTunnel interface for an IPv6 policy-based route for the gateway.
GEN7-39990	On a High Availability idle device, workload balancing operations do not get set correctly due to condition checking.
GEN7-40116	HTTPS management over Site-to-Site VPN fails when trying to use the X0 port of a NSv hosted on VMWare.
GEN7-40300	When changing the SSL-VPN client Network Address IPv4 pool, the change may not have been initiated even though it was reported as having been successful.
GEN7-40352	Adding a Content Filter Profile Objects when selecting block for **29. Search Engines and Portals** causes the error: **Command 'category "1. Violence/Hate/Racism" block' does not match.**
GEN7-40886	M-LAG/LACP does not work with Huawei Multi-chassis switches because the switch cannot manage a 132-byte LACP BPDU.
GEN7-40997	FQDN AO's used in source edited management access rules do not inherit new DNS record changes which causes stale entries to be maintained and traffic is dropped with the condition `Policy drop`. The address object table and policy table will not be properly synchronized if the hosts already exist in the address object's host list.
GEN7-41630	A disabled IPv6 VPN policy becomes enabled after being edited.
GEN7-41656	SSO enforcement shows as disabled for all zones even when there is an user-based Content Filter Service (CFS) policy.
GEN7-43151	Client loses internet access after a High Availability failover because the device receives a mismatched serial number from Capture Client, and it incorrectly considers the client as invalid.
GEN7-43386	If a VPN tunnel uses AESGCM for Phase 1 encryption, the command `show vpn tunnel` does not show the encryption and displays an incorrect PRF algorithm.

Issue ID	Issue Description
GEN7-43436	The Virtual Office portal remains accessible even when the SSL-VPN service is disabled.
GEN7-43505	Unable to add a central gateway VPN policy for DHCP over VPN when the authentication method is set to **Certificate**.
GEN7-43710	When using the web management interface to edit the WAN Group VPN, an error is displayed when the pre-shared key contains non-printable characters.
GEN7-44890	The SSL-VPN portal page cannot display the bookmark for users whose names contain an @ symbol. LDAP users that use "name@domain.com" as their display name instead of the simple "name" causes LDAP users to be unable to save bookmarks in SSL-VPN portal page.

Known Issues

Issue ID	Issue Description
GEN7-28519	Border Gateway Protocol (BGP) cannot be established when MD5 authentication is enabled.
GEN7-34246	Browser Network Time Lockout and Login Mechanism (NTLM) authentication functionality may not function as expected. **Workaround:** Users must log in to their device to authenticate.
GEN7-34484	Audit logs are cleared when the firewall is restarted.
GEN7-37742	*NSv only:* SSH login to the management console is not allowed..
GEN7-41011	Groups imported from LDAP will not be automatically filled in with the LDAP location.
GEN7-41040	A security policy is automatically added from **SSO Bypass** settings, but should not be added to firewalls configured on Policy Mode.
GEN7-41102	The **Password Change** page is not prompting for a new password when **Password change** is enabled on a firewall for an imported user.
GEN7-41340	The connected route of a sub-VLAN WAN interface turns gray when its parent interface is set to **Unassigned**.
GEN7-41593	If LACP is enabled when upgrading a High Availability pair, then High Availability should be disabled to upgrade, and each firewall must be upgraded separately.
GEN7-41996	Disabling the **Automatically adjust clock for daylight saving time** setting makes no change to the current system time.
GEN7-42202	A custom uploaded botnet signature file is not saved on the firewall and then lost when the firewall is restarted.

Issue ID	Issue Description
GEN7-43016	*VMWare ESXi UI version only:* When deploying an NSv using an `.ova` file, the error **disk image missing** is displayed. **Workaround:** 1. Unzip the `.ova` file to three files: `.vmdk` file, `.nvram` file and `.ovf` file. 2. Upload above three files to the firewall instead of the single `.ova` file.
GEN7-43049	An issue may occur intermittently when a network error is displayed in the web management interface after uploading the firmware and restarting the firewall with the factory default settings. The API sends the response and closes the HTTP connection before restarting the firewall, making it appear that the firewall is accessible.
GEN7-43500	After changing the name of a local user, the entry is still displayed in Server DPI SSL Exclusion/Inclusion lists and the user with the changed name cannot be selected.
GEN7-43554	Unable to add valid domains on **Custom Malicious Domain Name List** and **White List** pages after adding an invalid domain because the configuration change is still pending. **Workaround:** Log out of the firewall and then log in again.
GEN7-43677	The option to select the refresh rate of the Real-time Charts is not available. (The default is that the data is refreshed every 5 seconds.)
GEN7-43890	When **Enable UDP checksum enforcement** is enabled, a L2TP client cannot connect if the L2TP clients are behind NAT because in transport mode with NAT, UDP headers will have incorrect checksums due to the change of parts of the IP header during transit.
GEN7-44642	*NSsp 15700 only:* HTTPS Management using the X1 port is not accessible when the MGMT/Chassis IP and X1/Aux IP are in the same subnet.
GEN7-44690	SSL-VPN login fails to authenticate when LDAPS is configured and user tries to authenticate using CAC.
GEN7-44809	High CPU utilization may occur, causing the console to become unresponsive and the Tech Support Report (TSR) is not exported. **Workaround:** Disable **Collect Top Memory Caller** on the **Diagnostics** page. (A restart of the firewall is required for this change to be applied.)
GEN7-44866	Setting the schedule for Firmware Auto Update results in an error when using the Safari web browser to administer the firewall using the web management interface.
GEN7-44892	When using **RSA Secure ID Pin with Radius** without the PIN being set, and attempting log in using NetExtender, after entering the PIN in the prompt, the Next Prompt in which the user needs to enter **PIN + SecureID** is not being displayed and the NetExtender displays the message **Login incorrect - Incorrect username/password**. **Workaround:** An administrator logs out the user. The user should be able connect successfully afterward.
GEN7-44899	DNS rules do not support address objects of type MAC or FQDN by design. Address Object Groups currently bypass this restriction.

Issue ID	Issue Description
GEN7-44909	The **Threat Logs** page does not display any data until the user clicks **Refresh**.
GEN7-45060	*TZ series only:* The firewall may restart intermittently when two SonicWave devices are connected using the built-in wireless using the mesh gateway method and the **Radio Mode** on the **Internal Wireless** Page is changed from **2.4G** to **5G mixed-80M-48**.
GEN7-45077	Clicking **Graph** on the **Access Rules** page displays **No Data** for **Used Rules** when **All** is selected for the **Since** filter.
GEN7-45081	When logged in to a firewall that is managed by Network Security Manager (NSM) and the session has expired, clicking **Config** or **Non-Config** will fail without redirecting the user to log in again.
GEN7-45110	Editing a NAC policy in an Access Rule,then changing the source address group causes an error message to be displayed: **<*address object name*> is not a reasonable value**.
GEN7-45163	The App Rule number of times matched displays zero when the application rule policy name is followed by a space.
GEN7-45194	VPN-based SD-WAN groups are displayed in the dropdown list on the **SLA Probes** page, but should be excluded.
GEN7-45207	When an LDAP server with subdomains that are added as dynamic LDAP servers, and using LDAP search for a username in the subdomain, the web management interface may become unresponsive.
GEN7-45225	When U0 is configured as Final Backup in WAN Load Balancing and X1 is not configured, the web management interface and console diagnostic pings cannot reach the internet.
GEN7-45241	An intermittent issue may occur when downloading the system log or TSR with the CPU going to 100%. **Workaround:** Disabling "Periodic secure diagnostic reporting for support purposes" on the Device > Diagnostics > Tech Support Report page is a possible workaround.
GEN7-45252	*NSsp 15700 only:* An intermittent issue occurs when the Standby firewall fails to boot from uploaded firmware with `Wrong firmware to boot` displayed in the CLI after clicking **Reboot image with current settings**. After forcing a failover on the firewall, the upgrade will complete successfully.
GEN7-45257	Bookmarks created as an LDAP user are not visible when the firewall is upgraded from SonicOS 7.0.1 to SonicOS 7.1.1.
GEN7-45303	When there are a large number of FTP-data channels (20,000), and the sessions expire in a short time interval, the caches are deleted. This can cause the firewall to have a high CPU usage and become unresponsive when handling the connection cache timer. **NOTE:** This scenario is extremely unlikely to occur, but is a current limitation of the firewall itself.

Additional References

GEN7-21050, GEN7-30510, GEN7-30873, GEN7-32613, GEN7-36401, GEN7-37384, GEN7-37924, GEN7-38708, GEN7-39004, GEN7-39068, GEN7-39249, GEN7-39837, GEN7-40176, GEN7-40351, GEN7-40379, GEN7-40499, GEN7-40657, GEN7-40659, GEN7-40662, GEN7-40738, GEN7-40780, GEN7-40803, GEN7-40913, GEN7-41276, GEN7-41658, GEN7-41967, GEN7-42015, GEN7-42120, GEN7-42230, GEN7-42246, GEN7-42417, GEN7-42425, GEN7-42545, GEN7-42955, GEN7-42956, GEN7-42964, GEN7-43124, GEN7-43319, GEN7-43448, GEN7-43732, GEN7-43774, GEN7-43799, GEN7-44083, GEN7-44255, GEN7-44281, GEN7-44538

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

ⓘ | **NOTE:** A NOTE icon indicates supporting information.

ⓘ | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

ⓘ | **TIP:** A TIP icon indicates helpful information.

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

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

SonicOS Release Notes
Updated - October 2024
Software Version - 7.1.2
232-005888-00 Rev G