



About SonicOS 7.1

SONICWALL[®]

Contents

About SonicOS	4
What is SonicOS?	4
Where Do I Find Information About SonicOS?	5
SonicOS Web Interface to Administration Guide Reference	6
Guide Conventions	10
Firewall Management Methods	11
About the SonicOS Management Interface	13
Logging Into SonicOS	13
Logging Out of SonicOS	14
Contemporary vs Classic Web Interface	15
Global Search	16
Online Help	18
Notification Center	19
SonicOS Guides (Wizards)	21
Public Server Guide	22
VPN Guide	23
Wireless Guide	24
SDWAN Guide	25
SSH Terminal Access	25
About the Top Menu Views	27
About the API and CLI	29
Legal Information	30
What's New in SonicOS 7.1	31
Features of SonicOS	34
Features Available in Policy Mode	43
About Unified Policies in SonicOS	44
About the Shadow Feature	50
About Action Profiles	52
Features Available on TZ Series, NSa Series, and NSsp Series	54
Switch Management	54
PortShield Groups	56
Access Points Management	57
WWAN and 4G/LTE	58

Storage Device Configuration	59
Features Available on NSv Series	60
Feature Support on NSv Series	60
Changing Between Classic Mode and Policy Mode	68
Features Available on NSsp 15700	72
About Multi-Instance	72
SonicWall Support	74
About This Document	75

About SonicOS

SonicWall SonicOS runs on SonicWall firewalls and provides the web management interface, API and the Command Line Interface for firewall configuration.

This guide provides information about the SonicOS web management interface and introduces the API and CLI interfaces. This guide also discusses SonicOS features, the set of administration guides, available wizards, login/logout pages, and the legal page.

This introduction covers these topics:

Topics:

- [What is SonicOS?](#)
- [Where Do I Find Information About SonicOS?](#)
- [SonicOS Web Interface to Admin Guides Reference](#)
- [SonicOS Web Interface to Administration Guide Reference](#)
- [Guide Conventions](#)

What is SonicOS?

SonicOS 7.1 runs on SonicWall network security appliances (firewalls) and provides the web management interface for configuring the features, policies, and security services, updating the firmware, managing connected devices such as switches and access points, monitoring traffic/users/threats, investigating events, and much more. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

SonicOS are two modes of the same operating system, differing mainly in the areas of policy and object configuration. [[[Undefined variable Book_Variables.Product_Name]]] Policy Mode provides a unified policy configuration workflow combining Layer 2 to Layer 7 policy enforcement for security policies and optimizing the workflow for other policy types. This unified policy workflow gathers many security settings into one place, which were previously configured on different pages of the management interface in SonicOS 6.5. SonicOS 7.1 is more consistent with earlier releases, but is also redesigned with the new look and feel.

- SonicOS Policy Mode is supported on SonicWall NSv series and NSsp 15700 firewalls. SonicOS 7.1
- SonicOS Classic Mode is supported on SonicWall TZ series, NSa series, NSsp series (except for NSsp 15700), and NSv series firewalls. Refer to the *SonicOS 7.1 Release Notes* for the specific supported platforms.

SonicOS provides a modern graphical management interface that facilitates:

- Setting up and configuring your security appliance
- Monitoring the health and status of the security appliance, network, users, connections and the status of the incoming and outgoing traffic
- Configuring external devices, such as access points or switches

SonicOS also provides full-featured API and a command-line interface (CLI) in addition to the graphical management interface. For more information, see [About the API and CLI](#).

For information about the SonicOS management interface, see [About the SonicOS Management Interface](#).

Where Do I Find Information About SonicOS?

SonicOS administration guides are available for each main menu in the left navigation pane of the SonicOS web management interfaces. Within each guide, you will find topics covering each page in that menu group, with procedures and detailed information. Some guides are specific to SonicWall firewalls configured for either Classic or Policy Mode.

SonicOS administration guides are published on the SonicWall Technical Documentation portal at:

<https://www.sonicwall.com/support/technical-documentation/?language=English&category=Firewalls>.

On the left side of the page, you can select SonicOS, SonicOS, or the firewall series of your choice: TZ, NSa, NSv or NSsp. Scrolling down on the left, you can select the type of document and then the firmware version, followed by the virtual platform, date range, and language.

For example, the *SonicOS 7.1 Tools & Monitors* administration guide covers the following main topics:

- Using Packet Monitor
- Viewing Connections
- Monitoring Core 0 Processes
- Using Packet Replay

For a mapping of SonicOS 7.1 web management interface sections to the SonicOS 7.1 administration guides, refer to [SonicOS Web UI to Admin Guides Reference](#).

SonicOS Web Interface to Administration Guide Reference

SonicOS 7.1 is supported on SonicWall NSv Series and NSsp Series firewalls.

Management Interface Section	Guide Name	Topics Covered in this Admin Guide
HOME Dashboard	SonicOS 7.1 Dashboard	<p>Describes the key information and actionable features of the Dashboard pages, including:</p> <p>On all platforms:</p> <ul style="list-style-type: none">• System screens: Device, Summary, Network and Threat.• Policy Overview screens: Policies, Objects, Groups, Profiles and Signatures <p>On NSv Series only:</p> <ul style="list-style-type: none">• Capture ATP page showing Verdicts, File Types, Insights, Source IP Addresses, Analysis Depths, Attack Origins• Topology page showing Devices, IP Addresses, MAC Addresses
HOME Legal Information HOME API Wizards button in top banner Login/Logout screens	About SonicOS 7.1	<p>Provides an overview of the web management interface. Describes the Legal Information page and API page with Swagger access. Provides an overview of available wizards and of the SonicOS Login and Logout screens. Also describes key features, differences between SonicOS, and where to find information in the set of admin guides.</p>
MONITOR Real-Time Charts	SonicOS 7.1 Real-Time Charts	<p>Describes real-time charts on the System Monitor, Protocol Monitor, Policy Monitor, Users Monitor, and BWM Monitor (Bandwidth Management) pages.</p>

Management Interface Section	Guide Name	Topics Covered in this Admin Guide
MONITOR AppFlow	SonicOS 7.1 Monitor AppFlow	<p>Describes the AppFlow pages, including:</p> <p>On all platforms:</p> <ul style="list-style-type: none"> AppFlow Report screens: Applications, Users, IP Addressess, Virus, Intrusions, Spyware, Locations, Botnets, Web Categories CTA Report screens: Generate & Download CTA Report, Advanced Options, Completed Reports <p>On NSv Series only:</p> <ul style="list-style-type: none"> AppFlow Monitor screens: Applications, Users, Web Activity, Initiator IPs, Responder IPs, Threats, VoIP, VPN, Devices, Contents, Policies AppFlow Sessions screens: All, Threats, Web Access
MONITOR SDWAN	SonicOS 7.1 SDWAN	<p>Describes NETWORK SDWAN configuration pages and MONITOR SDWAN pages for Software Defined WAN features.</p> <p>NETWORK SDWAN pages include Groups, SLA Probes, SLA Class Object, Path Selection Profiles, and Rules.</p> <p>MONITOR SDWAN pages include SDWAN Monitor and SD-WAN Connections.</p>
MONITOR Logs	SonicOS 7.1 Monitor Logs	Describes the System Logs and Auditing Logs pages.
MONITOR Tools & Monitors	SonicOS 7.1 Tools & Monitors	Covers using Packet Monitor, viewing Connections, monitoring Core 0 Processes, and using Packet Replay.
DEVICE Settings	SonicOS 7.1 Device Settings	Configuration options and procedures for security service and support licenses, administration settings, system time settings, certificates, SNMP settings, firmware backups, upgrade, bootup options, and configuration settings export and import, and restarting the firewall.
DEVICE Multi-Instance	SonicOS 7.1 Multi-Instance for the NSsp Series	Configuration options and procedures for multi-instance settings, instances, instance firmware management, and instance licenses. (NSsp Series only.)
DEVICE High Availability	SonicOS 7.1 High Availability	Configuration options and procedures for High Availability settings. Describes HA status, settings, advanced settings and monitoring options.

Management Interface Section	Guide Name	Topics Covered in this Admin Guide
DEVICE Users	SonicOS 7.1 Users	Configuration options and procedures for authentication partitioning, adding local users and groups, guest accounts and services. Describes viewing status of local and guest users.
DEVICE AppFlow	SonicOS 7.1 Device AppFlow	Configuration options and procedures for Flow Reporting and AppFlow Agent.
DEVICE Log	SonicOS 7.1 Device Log	Configuration options and procedures for log settings, syslog, automation, name resolution, reports, and AWS.
DEVICE Diagnostics	SonicOS 7.1 Diagnostics for NSv Series SonicOS 7.1 Diagnostics for NSsp Series	Configuration options and procedures for system diagnostics, including the Tech Support Report (TSR), network settings, DNS lookup and reverse name lookup, network paths, using ping, using trace route, real-time blacklist, Geo-IP and botnet, making a URL rating request, PMTU discovery, terminal access, switch diagnostics (NSsp Series only), and policy lookup.
NETWORK System	SonicOS 7.1 System	Configuration options and procedures for system networking settings, including interfaces, failover and load balancing, neighbor discovery, ARP, MAC IP anti-spoof, web proxy, VLAN translation, IP helper, dynamic routing, DHCP server, multicast, network monitor, and AWS configuration.
NETWORK Firewall	SonicOS 7.1 Network Firewall	Configuration options and procedures for advanced firewall settings, SSL control, cipher control, and real-time-blacklist filter.
NETWORK VoIP	SonicOS 7.1 VoIP	Configuration options and procedures for voice over IP settings. Describes viewing call status and controlling calls.
NETWORK DNS	SonicOS 7.1 DNS	Configuration options and procedures for Domain Name Service settings, dynamic DNS, DNS proxy, and DNS security.
NETWORK Switching	SonicOS 7.1 Switching	Switching features are supported only on NSsp and NSa Series. Configuration options and procedures for VLAN trunking, Layer 2 discovery, link aggregation, and port mirroring.
NETWORK IPSec VPN	SonicOS 7.1 IPSec VPN	Configuration options and procedures for IPSec VPN rules and settings, advanced settings, DHCP over VPN, Layer 2 Tunneling Protocol server, and AWS VPN.

Management Interface Section	Guide Name	Topics Covered in this Admin Guide
NETWORK SSL VPN	SonicOS 7.1 SSL VPN	Configuration options and procedures for SSLVPN server, client, and portal settings. Virtual Office portal access. Viewing SSL VPN status.
OBJECT Match Objects	SonicOS 7.1 Match Objects	Configuration options and procedures for objects to be used in policy rules, including object types for zones, addresses, services, countries, applications, web categories, websites, URI lists, match patterns, custom matching, schedules, dynamic groups, and email addresses.
OBJECT Profile Objects	SonicOS 7.1 Profile Objects	Configuration options and procedures for profile objects to be used in policy rules, including profile objects for endpoint security, bandwidth, CFS block pages, logging and alerts, intrusion prevention, quality of service marking, DHCP option, and AWS.
OBJECT Action Profiles	SonicOS 7.1 Action Profiles	Configuration options and procedures for action profiles to be used in policy rules, include security action profiles and DoS action profiles.
OBJECT Signatures	SonicOS 7.1 Signatures	Viewing and refreshing anti-virus signatures and anti-spyware signatures.
POLICY Rules and Policies	SonicOS 7.1 Rules and Policies	Configuration options and procedures for security services settings, security policies, NAT policies, routing policies, decryption policies, DoS policies, endpoint policies. Viewing shadow characteristics of policies.
POLICY Capture ATP	SonicOS 7.1 Capture ATP	Configuration options and procedures for Capture ATP settings and viewing Capture ATP scanning history.
POLICY Endpoint Security	SonicOS 7.1 Endpoint Security	Configuration options and procedures for endpoint (client machines) security.

Guide Conventions

These text conventions are used in this guide:

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **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.

Convention	Description
Bold text	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Function Menu group > Menu item	Indicates a multiple step menu choice on the user interface. For example, NETWORK System > Interfaces means to select the NETWORK functions at the top of the window, then click on System in the left navigation menu to open the menu group (if needed) and select Interfaces to display the page.
Code	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<Variable>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment serialnumber=<your serial number> , replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004 .
Italics	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

Firewall Management Methods

SonicOS allows you to manage your SonicWall firewalls using these methods:

- **Local Management**

You can manage individual SonicWall firewalls by logging into the local web-based management interface in your browser. The admin account or other full-administrator account provides access to configure every feature in SonicOS. Point your browser to the LAN or WAN IP address and enter the user name and password to get started.

- **NSM Management**

SonicWall firewalls can be managed by SonicWall Network Security Manager (NSM) version 2.2 and higher. NSM is an application that centralizes management, reporting, and analytics for the SonicWall family of network security appliances and web services. The NSM cloud or on-premise solution automates the steps to set up an appliance and offers robust reporting and management tools.

- **API Management**

You can manage the firewall with API commands. SonicOS 7.1 provides complete, full-featured API support for each and every aspect of firewall management. SonicOS and the underlying management of the firewall is entirely API-driven.

You can access the API by clicking the link in the **HOME | API** page or enter the link directly into your browser, <https://sonicos-api.sonicwall.com>. The SonicOS API Swagger access page is displayed.

For more information, see the *SonicOS/X 7 API Reference Guide* on the [Technical Documentation portal](#).

- **CLI Management**

The SonicOS Command Line Interface (CLI) provides a concise and powerful way to configure SonicWall network security appliances without using the SonicOS web-based management user interface. You can use the CLI commands individually on the command line, or in scripts for automating configuration tasks. In addition, you can copy the output of a **show** command and post it back as a CLI command at the prompt. This feature gives the interface even greater speed and flexibility.

For more information, see the *SonicOS/X 7 Command Line Interface Reference Guide* on the [Technical Documentation portal](#).

- **SonicExpress Mobile App Management**

SonicWall SonicExpress is a mobile app that lets you easily register, set up, manage and monitor your SonicWall firewalls. To set up your new SonicWall next-generation firewall, simply launch the app, plug in the USB cable and follow instructions from the intuitive setup guide with step-by-step instructions. The SonicExpress Setup Guide is a very user-friendly way to initialize your new firewall. SonicExpress is

integrated with SonicWall WiFi Cloud Manager (WCM) which simplifies wireless access point deployment, management, and monitoring.

- **Capture Security Center ZeroTouch Registration and Provisioning**

Capture Security Center (CSC) supports Zero Touch registration and provisioning to manage and configure your firewall.

- Log into CSC at cloud.sonicwall.com using your MySonicWall credentials.
- Select the MySonicWall tile to register your firewall.
- Enable Zero Touch and NSM licensing on your firewall in MySonicWall.
- Select the Network Security Manager tile in CSC to manage your firewall from the cloud.

① | **NOTE:** This option requires a Cloud Management license.

About the SonicOS Management Interface

SonicOS is redesigned from the ground up for higher security, improved workflow and scalability, and a better user experience and ease of use.

This section introduces these top-level interface features:

Topics:

- [Logging Into SonicOS](#)
- [Logging Out of SonicOS](#)
- [Contemporary vs Classic Web Interface](#)
- [Global Search](#)
- [Online Help](#)
- [Notification Center](#)
- [SonicOS Guides \(Wizards\)](#)
- [SSH Terminal Access](#)
- [About the Top Menu Views](#)
- [About the API and CLI](#)
- [Legal Information](#)

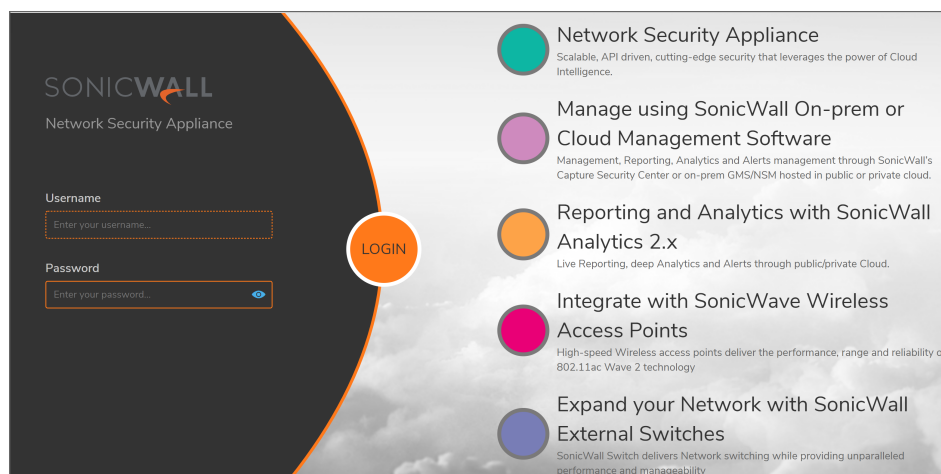
Logging Into SonicOS

To log into the SonicOS web management interface, enter the firewall IP address into your browser using HTTPS. The default X0 LAN IP address is <https://192.168.168.168>. The default credentials are:

- Username: *admin*
- Password: *password*

You can also log in using the WAN IP address if the WAN interface (usually X1 or X2) is configured to allow HTTPS management. SonicOS provides a DHCP server to give your computer an IP address in the same subnet, so there is no need to give it a static IP address before logging in.

The login page provides links to related SonicWall products at the right while you enter your SonicOS credentials at the left.

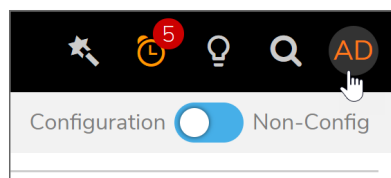
The image shows the SonicWall login page. On the left, there is a dark grey sidebar with the SonicWall logo and the text "Network Security Appliance". Below this, there are two input fields: "Username" with a placeholder "Enter your username..." and "Password" with a placeholder "Enter your password..." and an eye icon. A large orange "LOGIN" button is positioned to the right of the password field. On the right side of the page, there is a list of product links, each with a colored circle icon and a brief description. The links are: "Network Security Appliance" (teal), "Manage using SonicWall On-prem or Cloud Management Software" (purple), "Reporting and Analytics with SonicWall Analytics 2.x" (orange), "Integrate with SonicWave Wireless Access Points" (pink), and "Expand your Network with SonicWall External Switches" (blue).

After entering the **Username** and **Password**, click **LOGIN** or press **Enter** to log in.

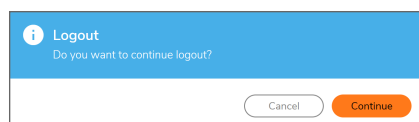
① | **NOTE:** The SonicOS web management interface is best viewed using 1920x1080 resolution.

Logging Out of SonicOS

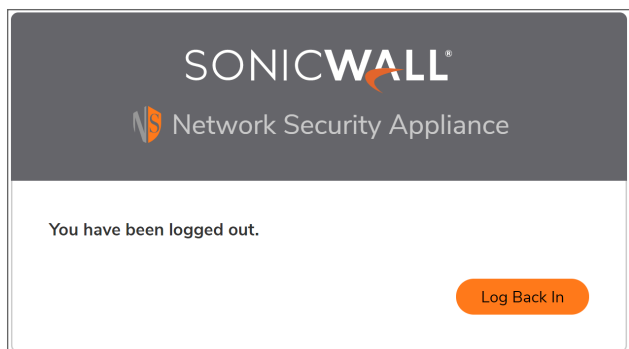
To log out of the SonicOS web management interface, click on the username initials at the top right corner of the banner and select **Logout** from the drop-down list.



In the confirmation dialog, click **Continue**.



The logout page is displayed.



To log back into the firewall, click **Log Back In**.

For security reasons, SonicOS automatically logs the administrator out after a specified period of inactivity. The default inactive time is 5 minutes. To change this duration, configure the desired number of minutes in the **Log out the Admin after inactivity of (mins)** field in the **Login / Multiple Administrators** screen on the **DEVICE | Settings > Administration** page.

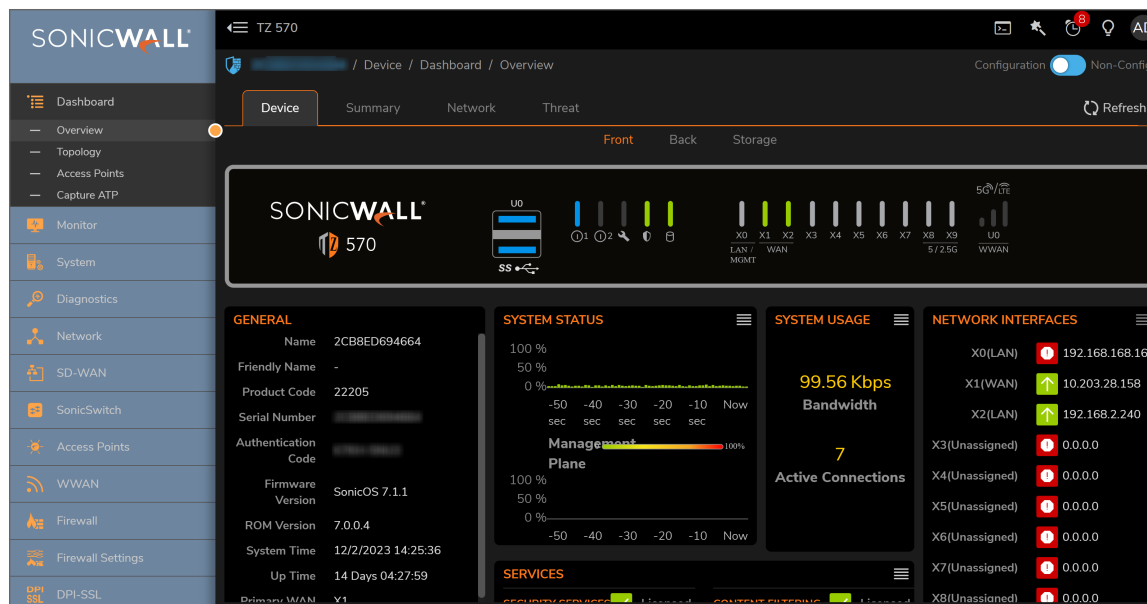
Contemporary vs Classic Web Interface

SonicOS 7.1 provides two web management interfaces, the contemporary interface with the menu group views across the top, and the classic interface with the menu groups in the left navigation pane. Both interfaces support the same feature set on SonicOS and the right-hand pages look the same.

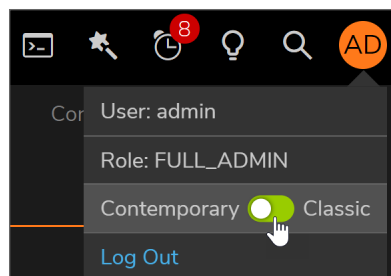
Contemporary interface:



Classic interface:



You can switch between the two interfaces by clicking on the username initials at the top right corner of the banner to show the drop-down list and using the slider button to select **Contemporary** or **Classic**.

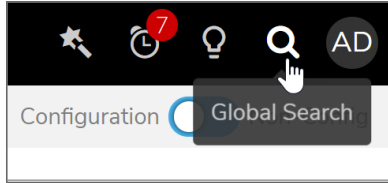


The interface changes immediately without asking you to confirm. You do not need to restart the system.

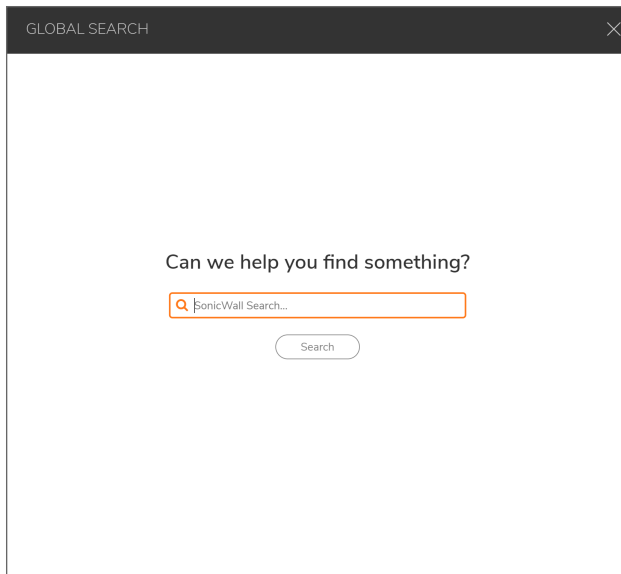
Global Search

SonicOS provides a global search feature that lets you look up elements in the web management interface, including page names, options, fields and so forth in the user interface itself, as well as configured values within features. This option to search for parameters globally helps the administrator to determine the sections, such as within Objects or Policies, in which the parameters are referenced.

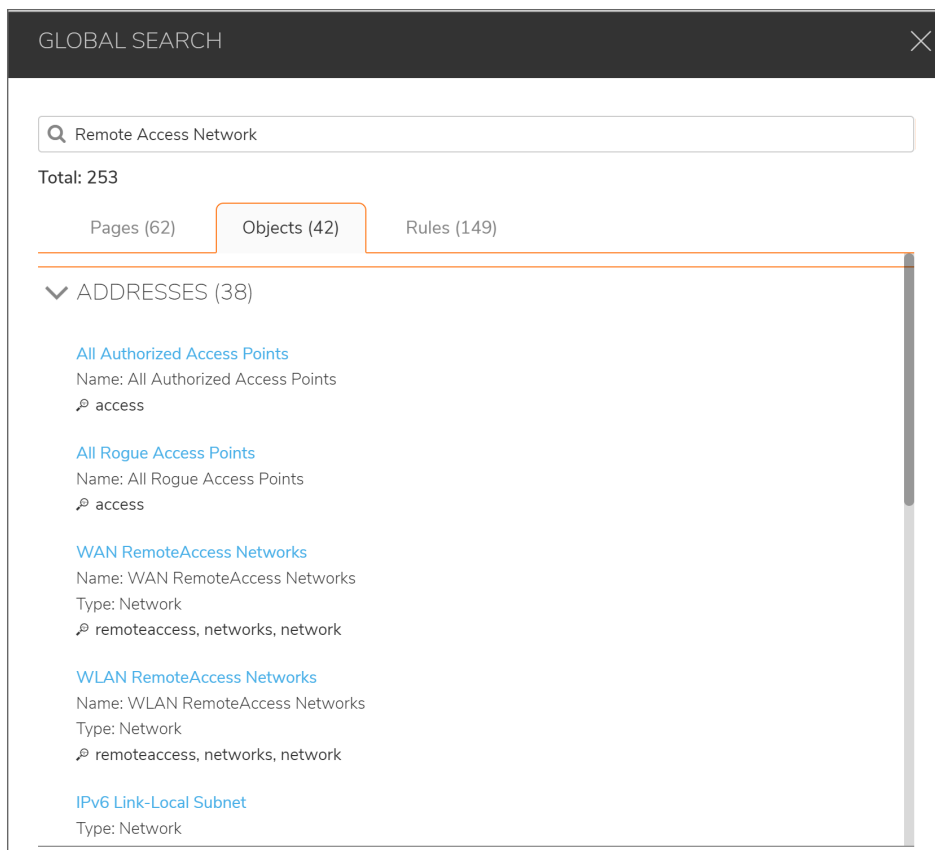
Launch a search by clicking the Global Search button at the top right, in the banner.



In the Global Search dialog, type in the string to search.



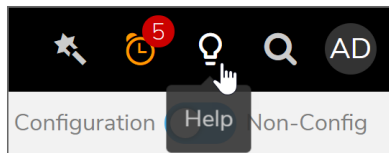
The results are displayed in the dialog, and may be divided by category. The number of results in each category is displayed in the category tab. Below, the categories are Pages, Objects, and Rules.



Click on any result to go to that location.

Online Help

Click the lightbulb icon at the top right in the banner to access SonicOS online help.



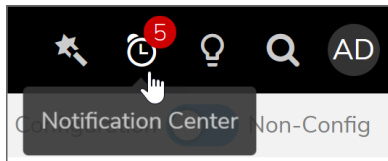
Your browser opens the SonicWall technical documentation page for your appliance platform and firmware version in another tab or window. From here, you can search for a keyword or open the relevant document.

There are many administration guides for SonicOS, each covering a menu group such as **Dashboard** or **Rules and Policies**. For more information and a mapping of the SonicOS menu groups to the associated admin guides, refer to:

- [Where Do I Find Information About SonicOS?](#)
- [SonicOS Web Interface to Administration Guide Reference](#)
- [SonicOS Web Interface to Admin Guides Reference](#)

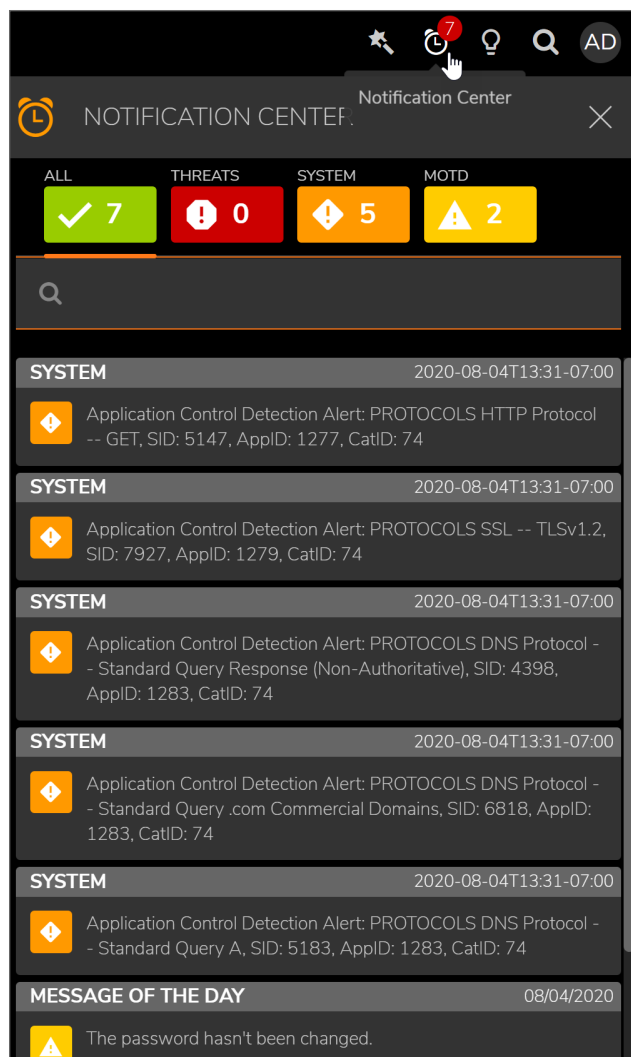
Notification Center

The SonicOS Notification Center provides actionable alerts with outstanding tasks to help administrators maintain their organization's security posture. The Notification Center is accessed by clicking the alarm clock button at the top right corner in the banner.



The number of current notifications is displayed in the red circle over the button.

The Notification Center displays a list of categorized messages with colored buttons at the top showing the number of each type.

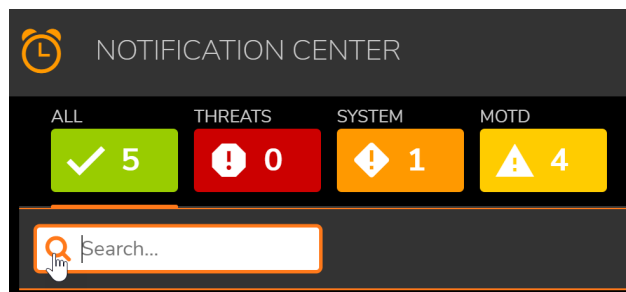


The notification categories are:

- **All** (Shows the total number of notifications)
- **Threats**
- **System**
- **MOTD** (Message of the Day)

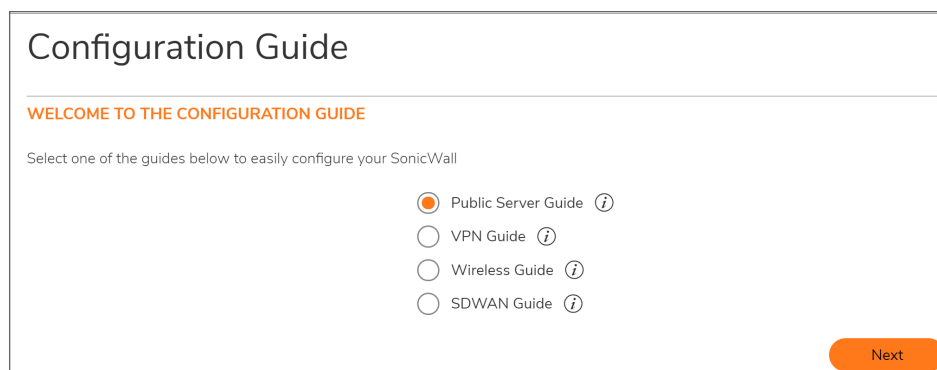
Click a category button to display notifications of that type only.

You can search the messages by clicking the Search icon and entering the value to search for into the field.



SonicOS Guides (Wizards)

SonicOS provides easy-to-use configuration guides (wizards) to assist you with initial configuration of server access, VPN policies, wireless network and security settings, and Software-Defined WAN network settings.



Each wizard displays a sequence of screens in which you select or enter the necessary settings. To continue to the next screen, click **Next**. To go back and make a change, click **Previous**. To exit the wizard, click the **X**.

The **Summary** page displays all the objects, NAT policies, access rules, security settings, or other settings that will be created. To proceed, click **Apply**.

These configuration guides are available:

- [Public Server Guide](#)
- [VPN Guide](#)
- [Wireless Guide](#)
- [SDWAN Guide](#)

Public Server Guide

The **Public Server Guide** lets you quickly configure the firewall to provide public access to an internal server.

Public Service Guide

1

2


3

4


5

ER TYPEPRIVATE NETWORKPUBLIC INFORMATIONSUMMARYCOMPLETE

PUBLIC SERVER TYPE

 If a particular service is not listed, you can choose 'Other' and on the following steps you will have the opportunity to create new services or define a service group that encompasses all of your needs.

Server Type

Web Server 

Service

☒ HTTP (TCP 80)

☒ HTTPS (TCP 443)

Click the "Next" button to proceed.

Previous

Next

You can select any of these server types:

- **Web Server**
- **FTP Server**
- **Mail Server**
- **Terminal Services Server**
- **Other**

If you select **Other**, you can select from a long list of service types or select **Create new Service**.

The wizard provides the well-known port(s) for known services and asks for other options required for configuration of the server. If necessary, SonicOS creates objects, such as a network object bound to the WAN zone for the non-default IP address of a public server.

VPN Guide

The **VPN Guide** lets you quickly create a **Site-to-Site** VPN policy to another SonicWall device or configure a **WAN GroupVPN** policy to accept incoming VPN connections from SonicWall Global VPN Client.

VPN Guide

VPN POLICY TYPE

Type of VPN Policy ☒ Site-to-Site ⓘ ☐ WAN GroupVPN ⓘ

[Previous](#) [Next](#)

The **Site-to Site** wizard provides sequential screens in which you input preshared key information, the IP address of the remote peer, local and destination network objects, and security settings for IKE Phase 1 and IPSec Phase 2.

The **WAN GroupVPN** wizard provides sequential screens in which you input preshared key information, the encryption and authentication security settings, user authentication, and optionally enable the virtual adapter for obtaining DHCP addresses in the X0 range.

Wireless Guide

The **Wireless Guide** lets you quickly configure the network settings and security features of the WLAN Radio Interface.

Wireless Guide

2

3

4

5

6

WIRELESS LAN SETTINGSWLAN RADIO SETTINGSWLAN VAP SETTINGSWLAN SECURITY SETTINGSUMMARY

WIRELESS LAN SETTINGS

IP Assignment

Static

Configure the SonicWall as the default gateway for your WLANs

WLAN IP Address

172.16.31.1

WLAN Subnet Mask

255.255.255.0

Previous

Next

For regulatory compliance, the **Wireless Guide** first asks you to select the country where the wireless TZ is being deployed. Then the wizard provides sequential screens in which you input the Wireless LAN network settings, WLAN radio settings, WLAN virtual access point settings, and WLAN security settings.

SDWAN Guide

The **SDWAN Guide** lets you quickly configure a software-defined WAN.

SD-WAN Guide

1

2

3

4

5

SERVICE/APPLICATION SELECTIONSLA CRITERIAPATH SELECTIONHEALTH CHECK PROBESSUMMARY

CHOOSE SERVICE/APPLICATION FOR DYNAMIC PATH SELECTION

ApplicationService

Select a Application O... ▼

SOURCE AND DESTINATION FOR THE CHOSEN SERVICE/APPLICATION

Traffic Source/NetworkSelect AddressObject/... ▼

Service/Application destinationSelect AddressObject/... ▼

Service Selection is recommended for known IP/FQDN destinations reachable via VPN. Example: VoIP PBX hosted at HQ or DC. Application Selection is recommended for SaaS applications reachable over internet. Example: Office365, RingCentral.

Previous

Next

The **SDWAN Guide** provides a sequence of screens in which you input the service or application, SLA criteria for latency, jitter, and packet loss, path selection using WAN or route based VPN tunnels, and health check probes.

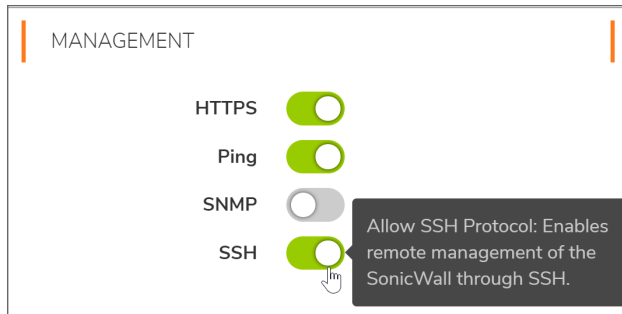
SSH Terminal Access

An SSH Terminal can be accessed by clicking the **Terminal** icon button on the top banner of the SonicOS web management interface.

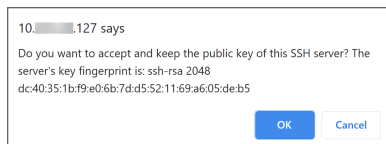
A screenshot of the top banner of the SonicOS web management interface. It features a dark background with several icons: a terminal icon (highlighted with a hand cursor), a star, a clock with a red '8' notification badge, a lightbulb, a magnifying glass, and a button labeled 'AD'. Below the icons is a dark button labeled 'Open SSH terminal session' and a toggle switch labeled 'Non-Config'.

About SonicOS 7.1 | 25
About the SonicOS Management Interface

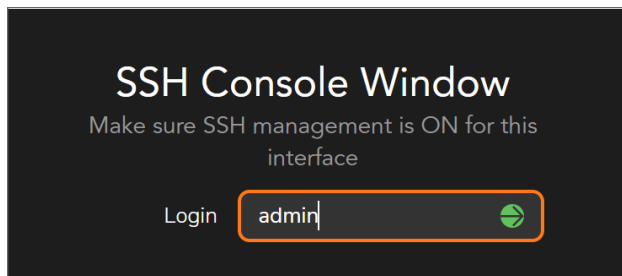
Before initiating the Terminal, make sure that the interface has SSH enabled for management. To check, go to **NETWORK | System > Interfaces** and edit the WAN (usually X1) interface. On the **General** screen, scroll down to the **MANAGEMENT** options and enable **SSH**.



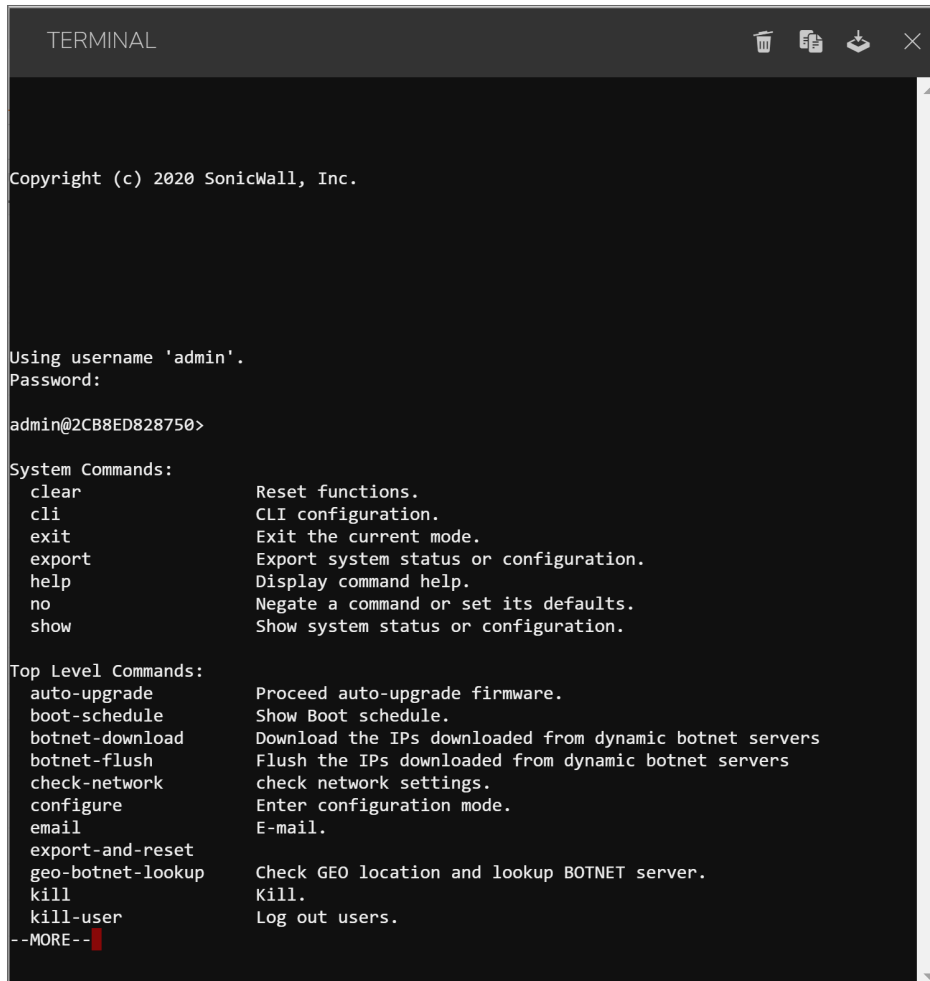
If prompted, click **OK** in the SSH Server warning dialog to accept the certificate.



Then, enter the administrator username and password at the prompts (default *admin/password*).



The SSH terminal window is available for use with all the standard commands. Type a question mark, '?', to see the list of system commands and top level commands. Press the spacebar at the **--MORE--** prompt to display more commands.

A screenshot of a terminal window titled "TERMINAL" with standard window controls (minimize, maximize, close) in the top right. The terminal content shows a copyright notice for SonicWall, Inc. (2020), followed by a login prompt for username 'admin'. After the password is entered, the prompt changes to 'admin@2CB8ED828750>'. Below this, two lists of commands are displayed: "System Commands" and "Top Level Commands". Each command is followed by a brief description of its function. The list ends with "--MORE--" and a red cursor, indicating that more commands are available.

```
TERMINAL

Copyright (c) 2020 SonicWall, Inc.

Using username 'admin'.
Password:
admin@2CB8ED828750>

System Commands:
clear          Reset functions.
cli            CLI configuration.
exit           Exit the current mode.
export         Export system status or configuration.
help           Display command help.
no             Negate a command or set its defaults.
show           Show system status or configuration.

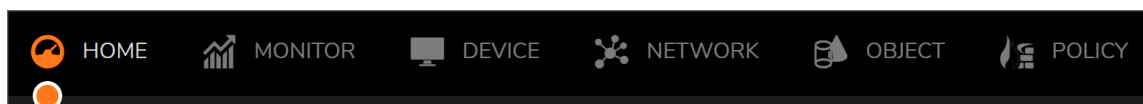
Top Level Commands:
auto-upgrade   Proceed auto-upgrade firmware.
boot-schedule  Show Boot schedule.
botnet-download Download the IPs downloaded from dynamic botnet servers
botnet-flush   Flush the IPs downloaded from dynamic botnet servers
check-network  check network settings.
configure      Enter configuration mode.
email          E-mail.
export-and-reset
geo-botnet-lookup Check GEO location and lookup BOTNET server.
kill           Kill.
kill-user      Log out users.
--MORE--
```

You can type `logout` or `exit` to end the session, or click the 'X' in the top right corner to return to web management.

For more information about the command line interface (CLI), refer to the *SonicOS/X 7 Command Line Interface Reference Guide* on the [Technical Documentation portal](#).

About the Top Menu Views

The contemporary SonicOS 7.1 web management interface layout is organized into high-level, intuitive workflows, with six top-level views in a menu across the top.



The currently selected top view is marked with an orange dot. A similar orange dot marks the currently selected page in the left navigation pane.

The six top-level views are:

- **HOME** – The HOME view provides dashboards and graphs designed to help you quickly see the health and security status of your security appliance, connected devices, and networks. In SonicOS, the Policy Overview page provides status information for your policies. On NSsp 13700 and TZ, NSa and NSv series, a graphical representation of your network topology is available in the HOME view. The API and Legal pages are also in the HOME view.
- **MONITOR** – The MONITOR view provides Real-Time Charts, AppFlow reports and/or monitoring, AppFlow sessions (on NSv), Capture Threat Assessment report, SDWAN monitoring, system logs, and tools for packet capture and monitoring connections and processes.
- **DEVICE** – The DEVICE view provides configuration pages for firewall administration and settings, internal wireless settings for TZ wireless firewalls, high availability, users, AppFlow settings, log settings, and system diagnostic tools. In SonicOS, the Policy Lookup page is available under Diagnostics. On TZ, NSa and NSsp 13700 firewalls, configuration pages for external devices such as the SonicWall Switch, Access Points, and WWAN 4G/LTE are available.
- **NETWORK** – The NETWORK view provides System configuration pages for network interfaces and system settings including for load balancing, ARP, web proxy, PortShield (on TZ and NSa series), VLAN translation, dynamic routing, DHCP server, etc, as well as pages for advanced firewall settings, VoIP, DNS, SDWAN, IPSec VPN, and SSL VPN settings.
- **OBJECT** – In SonicOS, the OBJECT view provides configuration pages for Match Objects, Profile Objects, and Action Objects, which are used when creating rules and policies on the POLICY view. In SonicOS, the OBJECT view provides configuration pages for Match Objects, Profile Objects, and Action Profiles, which are used when creating rules and policies on the POLICY view. A Signatures page allows refresh of Anti-Virus and Anti-Spyware signature databases on the firewall.
- **POLICY** – In SonicOS, the POLICY view provides menu groups for Rules and Policies, Capture ATP, and EndPoint Security. In SonicOS, the POLICY view provides those menu groups plus four additional ones: DPI-SSL, DPI-SSH, Security Services and Anti-Spam.

The configuration pages within Rules and Policies have significant differences between SonicOS (Classic mode) and SonicOS (Policy mode). The configuration pages in Classic mode include Access Rules, NAT Rules, Routing Rules, Content Filter Rules, App Rules and Endpoint Rules. In Policy mode, the Rules and Policies menu group pages are Settings, Security Policy, NAT Policy, Route Policy, Decryption Policy, DoS Policy, Endpoint Policy and Shadow. These policy configuration pages cover the same security aspects as those in Classic mode, but with a more unified approach. The Settings page provides status for all security services on a single page, while the services are configured within each policy as an integral component. The Shadow page shows which rules are being shadowed by other rules and which rules are shadowing other rules. If a rule is shadowed by another rule, the first rule might never be hit.

About the API and CLI

The SonicOS Enterprise Command Line Interface (E-CLI) provides a concise and powerful way to configure SonicWall security appliances without using the SonicOS web management interface. You can use the CLI commands individually on the command line or in scripts for automating configuration tasks. You can access the CLI by connecting to the Console port via SSH or with a serial connection. For more information, refer to the *SonicOS 7.1 Command Line Interface Reference Guide* on the SonicWall technical documentation portal.

The SonicOS RESTful API (Representational State Transfer Application Program Interface) provides an alternative method to the SonicOS CLI for configuring the firewall. You can use the API to configure each and every feature on the firewall or to script configuration sequences.

For more information, see the *SonicOS 7 API Reference Guide* on the SonicWall technical documentation portal.

To access the API, navigate to **HOME | API** and click the link in the **SONICWALL SONICOS API AGREEMENT** section.

COPYRIGHT & LIMITED LIABILITY


© 2020 SonicWall Inc. ALL RIGHTS RESERVED.
SonicWall is a registered trademark of SonicWall Inc. All other trademarks are property of their respective owners.

SONICWALL SONICOS API AGREEMENT

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING SONICOS API. BY DOWNLOADING, INSTALLING OR USING THIS API, YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. PLEASE GO TO [HTTPS://SONICOS-API.SONICWALL.COM](https://sonicos-api.sonicwall.com) TO VIEW THE APPLICABLE VERSION OF API FOR YOUR PRODUCT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL OR USE THIS API.

You can also enter the link directly into your browser, <https://sonicos-api.sonicwall.com>.

The SonicOS API Swagger access page is displayed.

 **swagger**

Explore

SonicOS API

7.0.0-P337_gen7-api OAS3

/sonicos_files/default/sonicos_openapi.yml

Swagger Specification for SonicOS APIs


THIS YML IS FOR SONICWALL INTERNAL USE ONLY

SonicOS support two-factor and bearer token login from SWAGGER only.

Please follow the following steps to login.

1. POST "tfa" with your username, password, and two-factor code to the firewall. If you are authenticating a username for the first time, please login to GUI and scan the QR code to activate two-factor authentication.
2. The Bearer Token is returned in response to the "tfa" message. Copy the Bearer Token to the "Authorize" button.
3. DELETE "auth" to logout of the current session.

[Terms of service](#)
[Contact SonicOS API Support](#)

Authorize 

Set up your authentication and log in for the complete API command list and syntax.

```
openapi: "3.0.0"

info:
  description: |
    __Swagger Specification for SonicOS APIs__

    __THIS YML IS FOR SONICWALL INTERNAL USE ONLY__

    __SonicOS support two-factor and bearer token login from SWAGGER only.__

    Please follow the following steps to login.
    > 1. POST "tfa" with your username, password, and two-factor code to the firewall. If you are authenticating
    > 2. The Bearer Token is returned in response to the "tfa" message. Copy the Bearer Token to the "Authorize"
    > 3. DELETE "auth" to logout of the current session.

  version: 7.0.0-R370_gen7-api
  title: "SonicOS API"
  termsOfService: "http://help.sonicwall.com/help/sw/eng/7621/8/0/0/content/app-license_agreement.65.2.htm"
  contact:
    name: "SonicOS API Support"
    email: "sonicOsApiSupport@SonicWall.com"
  servers:
    - url: "https://{IP}:{PORT}/api/sonicos"
      description: "SonicWALL Appliance"
      variables:
        IP:
          description: "SonicWALL IP address or hostname"
          default: "192.168.168.168"
        PORT:
          description: "SonicWALL PORT"
          default: "443"

tags:
  - name: tfa
    description: Post user name, password and two-factor code to get bearer token.

  - name: auth
    description: logout current session.

  - name: config-pending
    description: "Pending configuraiton API."

  - name: administration
    description: "administration configuration API endpoint."
```

Legal Information

SonicWall SonicOS is protected by copyright and is provided *as is*.

The SonicWall copyright statement and End User Product Agreement (EUPA) are displayed on the **HOME | Legal Information** page.

COPYRIGHT & LIMITED LIABILITY

© 2020 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a registered trademark of SonicWall Inc. All other trademarks are property of their respective owners.

END USER PRODUCT AGREEMENT

The terms and conditions applicable to your download and use of this product are located at <https://www.sonicwall.com/legal/#tab-id-3> ("Agreement"). Please read this Agreement carefully as it contains provisions such as how you may use the product and associated restrictions, warranties and warranty disclaimers, limitation on damages and remedies that may be claimed, audit rights. BY DOWNLOADING, INSTALLING OR USING THIS PRODUCT, YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL, ACCESS OR USE THE PRODUCT BECAUSE YOU DO NOT HAVE A LICENSE TO THE PRODUCT.

What's New in SonicOS 7.1

The new features in SonicOS 7.1 include:

- **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 integrates SonicWave 600 Series Access Points with the firewall.

① **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, Virtual TPM, and many performance enhancements.

- **NSV Bootstrapping**

- SonicOS7.1 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.

- ① | **IMPORTANT:** Upgrading to the 7.1 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 <https://www.sonicwall.com/support/knowledge-base/231208132612487>.

- **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.

- ① | **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.

- ① | **NOTE:** This feature is not supported on NSsp 15700.

- **UI Monitor and Page Enhancements**

SonicOS7.1 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.

- SonicOS7.1 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**

SonicOS7.1 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 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 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**

SonicOS7.1 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**

- SonicOS7.1 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.

Features of SonicOS

This section describes a number of features introduced or enhanced in SonicOS 7.1. These features are available on all (or most) platforms.

For features of SonicOS available only on specific SonicWall firewall model series, refer to any of these topics:

- [Features Available in Policy Mode](#)
- [Features Available on TZ Series, NSa Series, and NSsp Series](#)
- [Features Available on NSv Series](#)
- [Features Available on NSsp 15700](#)

Key features available in SonicOS on all platforms include:

- **Actionable Dashboard**

In SonicOS 7.1, the Dashboard is enhanced with actionable alerts. The **HOME | Dashboard > System** page provides four screens with actionable alerts: Device, Summary, Network and Threat.

The Device, Network and Threat dashboards provide a top-level summary of the overall health of the appliance and threat insights. The actionable alerts help administrators maintain their organization's security posture.

An example of an actionable alert on the Device screen is, if any service is unlicensed, you can click to be redirected to the **DEVICE | Settings > Licenses** page and take action on missing licenses.

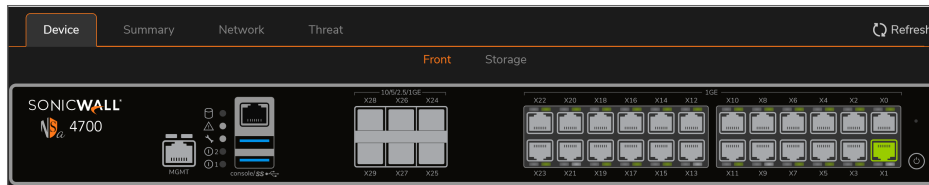
- **Device View - Front Panel**

You can check the physical status of your firewall from the **HOME | Dashboard > System** page, in the **Device** screen. This gives the same feel as when you are physically looking at the hardware and also provides a graphical representation of the NSv virtual firewall. Some example screens are shown below.

TZ:



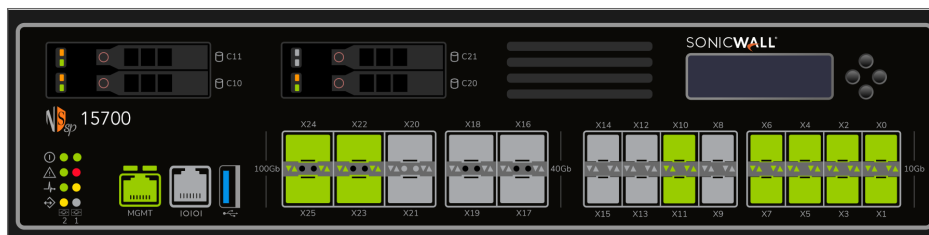
NSa Series and NSsp 13700:



NSv:



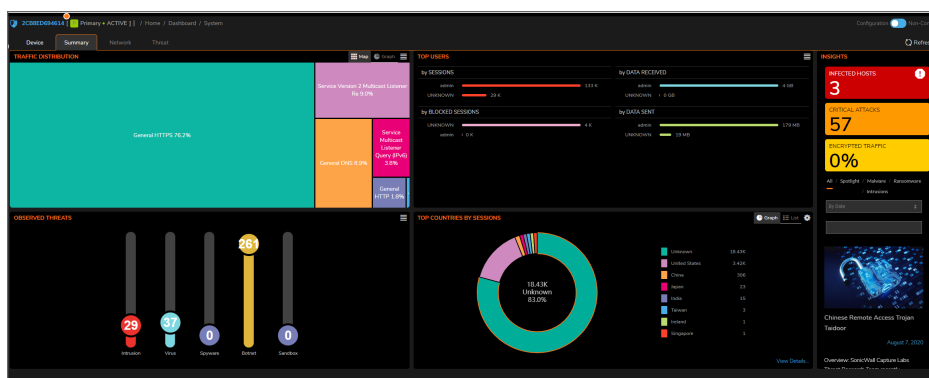
NSsp 15700:



• Top Traffic and User Summary

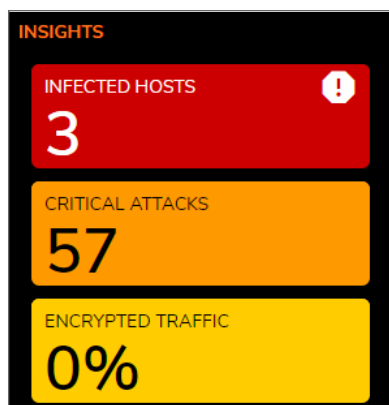
The **Dashboard > System > Summary** page displays:

- Traffic distribution usage on the firewall with real-time updates of the most used applications
- Summary of top users based on allowed or blocked sessions and by data sent and received



- **Insights Into Threats**

The **Dashboard > System > Summary** page displays a section at the right with insights into threats of several types.



Insights on infected hosts displays the total number of infected host machines in your network in real-time. Insights on critical attacks displays the total number of mission-critical attacks in your network in real-time. Insights on encrypted traffic displays the total number of encrypted traffic in your network in real-time.

- **Decryption Features**

SonicOS 7.1 supports several new decryption features:

- **Decryption Support for TLSv1.3**

The TLS 1.3 encryption standard is supported to inspect encrypted traffic across several protocols like HTTPS, SSH, and FTPS. Support for TLS 1.3 improves overall security on the firewall. This is implemented in Firewall Management, SSL VPN and Deep Packet Inspection (DPI).

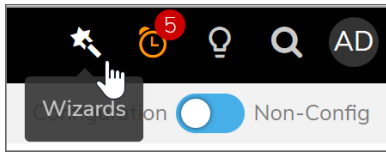
- **Selective Blocking of Ciphers**

On the **NETWORK | Firewall > Cipher Control** page, you can select from over 300 ciphers and block or unblock them. Filtering controls at the top of the page make it easy to view certain cipher types or strength ratings.

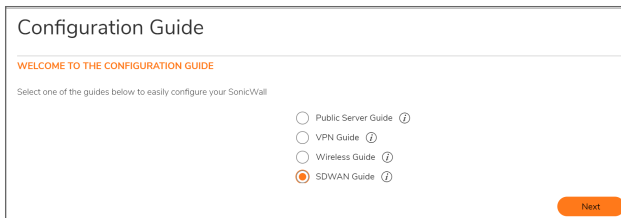
TLS Ciphers		SSH Ciphers									
Search...		Action: All	Strength: All	CBC: All	TLS:		Block	Unblock			
<input type="checkbox"/>	CIPHER NAME	STRENGTH	BLOCK...	IS CBC	TLS1.0	TLS1.1	TLS1.2	TLS1.3	DPI-SSL	HTTPS...	SSL CONT
<input type="checkbox"/>	TLS_AES_128_GCM_SHA256	Recommended						✓	✓	✓	
<input type="checkbox"/>	TLS_AES_256_GCM_SHA384	Recommended						✓	✓	✓	
<input type="checkbox"/>	TLS_CHACHA20_POLY1305_SHA256	Recommended						✓	✓	✓	
<input type="checkbox"/>	TLS_AES_128_CCM_SHA256	Recommended						✓			
<input type="checkbox"/>	TLS_AES_128_CCM_8_SHA256	Recommended						✓			
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Recommended					✓		✓	✓	
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Recommended					✓		✓	✓	
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	Recommended					✓		✓		
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Recommended					✓		✓		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Recommended					✓		✓	✓	
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Recommended					✓		✓	✓	
<input type="checkbox"/>	TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256	Recommended					✓		✓		
<input type="checkbox"/>	TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384	Recommended					✓				
<input type="checkbox"/>	TLS_ECDHE_PSK_WITH_AES_128_CCM_8_SHA256	Recommended					✓				
<input type="checkbox"/>	TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256	Recommended					✓				

- **SDWAN Wizard**

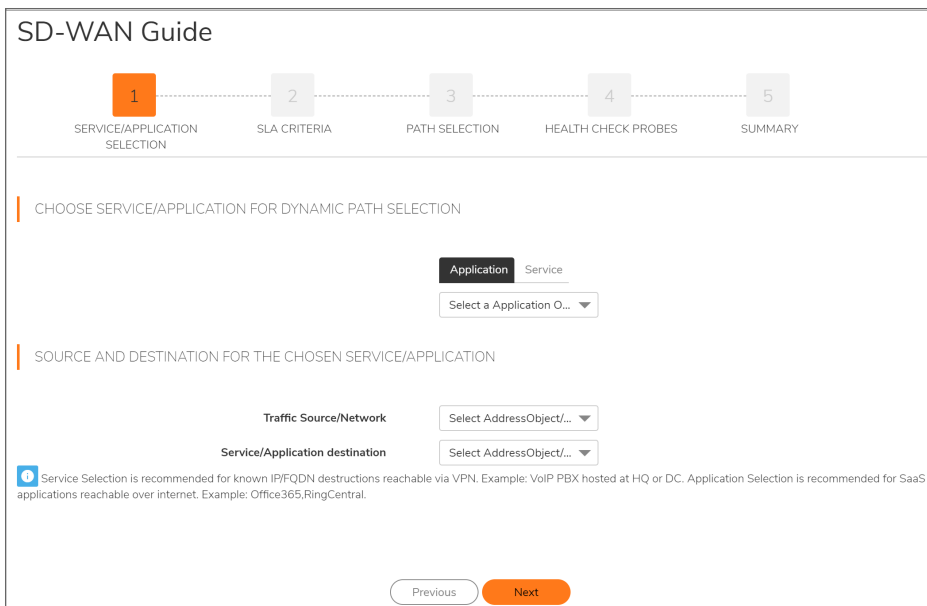
The SDWAN Wizard guides you through configuring SDWAN Policies on the firewall. The wizard intuitively walks through setting up SDWAN rules to connect to HQ or Cloud SaaS applications without complex configurations. The wizard is accessed by clicking the wizard button in the top, right corner of the web management interface.



Select **SDWAN Guide** from the available wizards.



The SD-WAN Guide has five screens to assist you with creating the policy.



- **Capture ATP**

The newly designed Capture ATP dashboard provides insights into Zero-Day threats that are coming into the organization's network with location-based attack origin information.



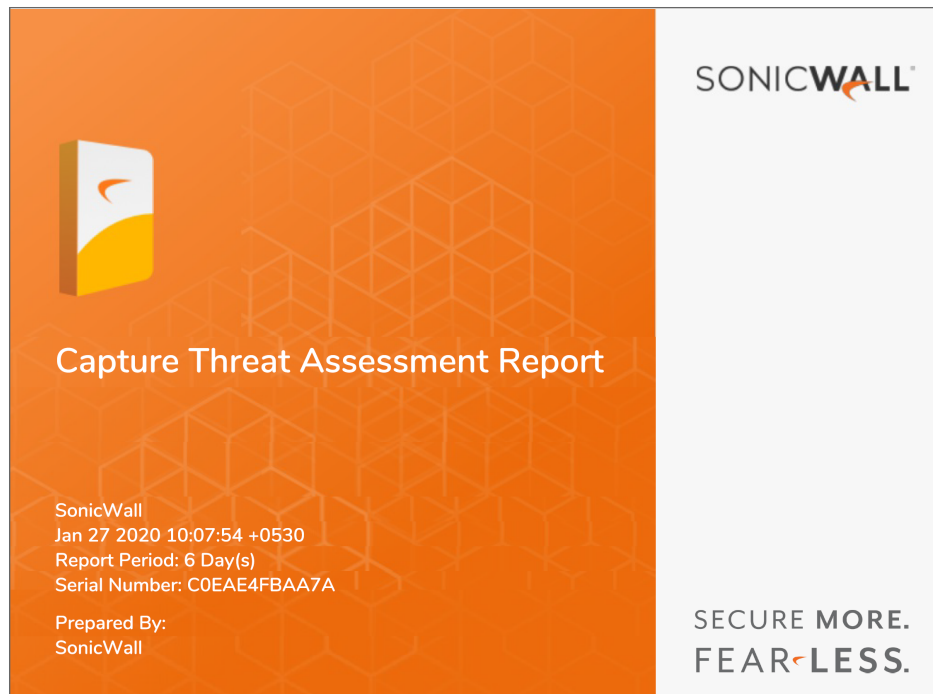
- **Capture Threat Assessment 2.0**

SonicOS 7.1 supports Capture Threat Assessment (CTA) v2.0. Capture Threat Assessment is a SonicWall service that provides network traffic and threat report generation in PDF format. The service is provided directly from the SonicOS web management interface. You can navigate to the **MONITOR | AppFlow > CTA Report** page to configure settings and generate the report. Previous reports are saved in the cloud and displayed as a table on the page.

① | **NOTE:** App Visualization licensing is recommended for complete report data.

CTA v2.0 provides a number of enhancements for the current Capture Threat Assessment cloud service and reporting on all SonicWall firewalls, as described below.

- New report template – latest look and feel



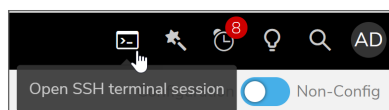
- Meaningful application statistics – adds more meaningful application, threat, web and network data
- Industry and global level statistics comparison – Industry averages let you compare your statistics alongside industry and global data
- Risky applications analysis – rates the amount of risk compared to industry standards
- Malware web activity – Web Activity page provides information about exposure to malware from web activity
- Glimpse of threats – Glimpse of Threats page details the application exploits, spyware, other malware and botnet activity observed on your network
- Report customization and advanced options – provide a way to customize the report features, control the report title and company information, and add a custom logo so you can design the report according to your requirements
- Executive Summary with Key Findings – summarizes the overall pages into a single page for quick reference by busy executives
- Recommendations – provides a summary of steps you can take to fix the issues found during the reporting period

- **System Logs Download**

System logs, including console logs, can be downloaded from the **DEVICE | Diagnostics > Tech Support Report** page. The ability to download console logs without connecting to the console port simplifies debugging and reduces the time needed for troubleshooting.

- **SSH Terminal Access**

An SSH Terminal can be accessed by clicking the Terminal icon button on the top banner of the SonicOS web management interface.



Before initiating the Terminal, make sure that the interface has SSH enabled for management. To check, go to **NETWORK | System > Interfaces** and edit the WAN interface. The first time, click **OK** in the SSH Server warning dialog to accept the certificate.

Then, enter the administrator username and password at the prompts (default *admin/password*).

- **SonicExpress Mobile App Compatibility**

SonicWall SonicExpress is a mobile app that lets you easily register, set up, manage and monitor your SonicWall firewalls. To set up your new SonicWall next-generation firewall, simply launch the app, use your USB phone cable to connect the firewall USB port to your smartphone, and follow the step-by-step instructions in the intuitive SonicExpress setup guide. Additionally, stay updated with the latest SonicWall security news from the app.

The SonicExpress Setup Guide is a very user-friendly way to initialize your new firewall.

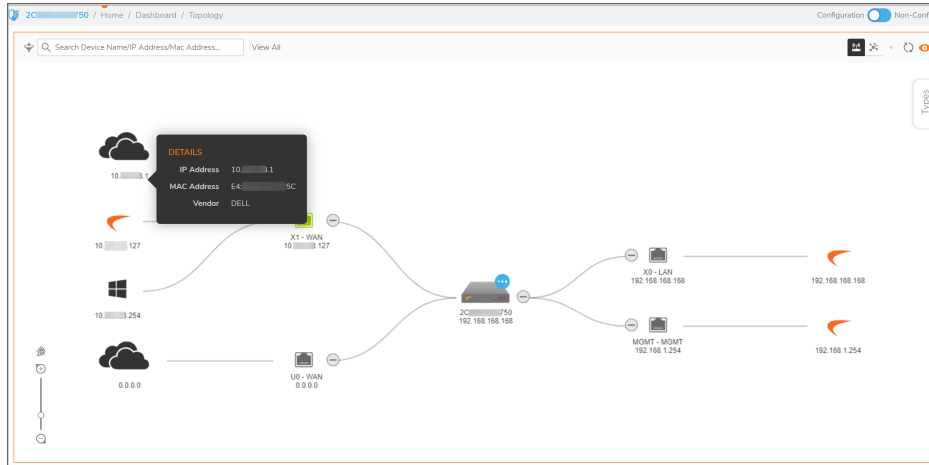


The key features available in both SonicOS on **most** platforms are:

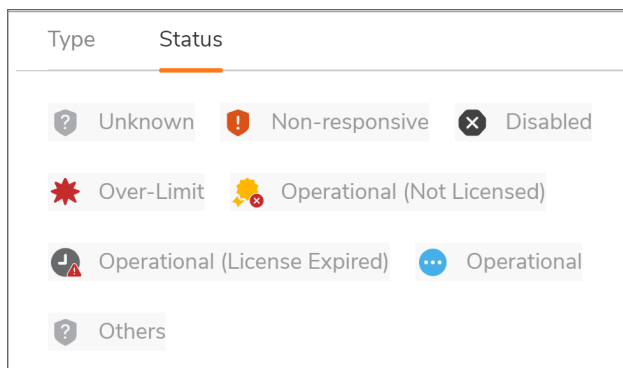
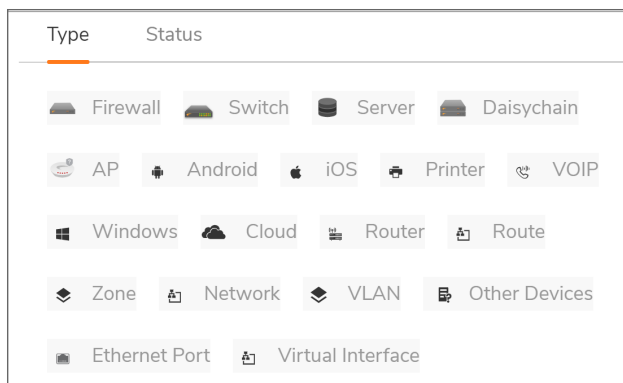
- **Network Topology View**

The **HOME | Dashboard > Topology** page shows an image of your firewall with hosts, access points, and other devices deployed in your network. This feature is supported on TZ, NSa and NSv series firewalls.

The Topology view provides physical and logical connectivity of all SonicWall devices, including firewalls, wireless access points and SonicWall Switches and their connected network devices in one place for easy visualization and policy enforcement. Device insights include device type, IP address, MAC address and traffic statistics to identify trouble spots or choke points.



- You can use the buttons at the top right to refresh, display or hide labels, and change the view style.
- Move your mouse over each device to see details about it in a popup screen.
- Click the **Types** tab on the right to see the device type and status legend.



- **Authentication Partitions**

Authentication partitions control which authentication servers are used for which users. Partitions are supported on NSa, NSv, and NSsp series firewalls. You can configure partitions on the **DEVICE | Users > Partitions** page.

There is always one authentication partition, the automatically created Default partition. You cannot delete this partition. You can, however, edit it and select servers, agents, and clients for it as well as subpartitions. If you disable authentication partitioning, all LDAP servers, SSO agents, TSAs, and RADIUS accounting clients are reassigned to the Default partition; when you re-enable authentication partitioning, you must reassign them. RADIUS servers are not affected and remain with their assigned partitions.

Features Available in Policy Mode

Some features are only provided for firewalls configured for SonicOS in Policy Mode and are not available for firewalls configured for Classic Mode. These SonicOS features are mostly in the areas of policy and object configuration, and are based on a complete redesign and unified architecture of the underlying policy engine.

Topics:

- [About Unified Policies in SonicOS](#)
- [About the Shadow Feature](#)
- [About Action Profiles](#)

About Unified Policies in SonicOS

SonicOS 7.1 introduces a new, redesigned unified policy configuration workflow combining Layer 2 to Layer 7 policy enforcement for security policies and optimizing the workflow for other policy types. This unified policy workflow gathers many security settings into one place, which were previously configured on different pages of the SonicOS management interface. The benefits of this new approach also include improved reporting, auditing and logging, better diagnostics, monitoring and debugging, and faster loading and searching of rules and objects in the management interface.

All rules are manually created by administrators, there are no automatic or system-added rules.

Priority characteristics of rules:

- Rules are applied in the order of priority, as shown by the rule order in the policy table.
- Rules are created at a certain priority.
- No automatic priority of rules.

A policy is defined by a group of rules that are applied to do a certain job. SonicOS provides six policy types based on their characteristics, of which four are introduced in SonicOS 7.1 and the others are improved and enhanced over previous implementations.

The following new policy types consolidate and reorganize policy configuration for improved logic and efficiency:

- **Security Policy**

Security Policy configuration unifies elements that were configured independently in previous versions of SonicOS. A Security Policy consists of one or more rules that apply security services to traffic. Each security rule merges the following security settings:

- Access Rules
- App Rules
- App Control
- Content Filter
- Botnet Filter
- Geo-IP Filter
- Intrusion Detection and Prevention
- Anti-Virus
- Anti-Spyware

Adding Rule

Name

My Rule

Tags

add upto 3 tags, use comma as separator...

Description

provide a short description of your access rule...

Action

Allow

Deny

Discard

Type

IPv4

IPv6

Schedule

Always

Enable

Security Rule Action

--- Select Security Rule Action ---

Source / Destination

App/URL/Custom Match

SOURCE

Zone/Interface

Any

Address

Any

Port/Services

Any

DESTINATION

Zone/Interface

Any

Address

Any

Port/Services

Any

USERS

Include

All

GEO COUNTRY

(From / To) Country

Any

Show Diagram

Create Another

Validate

Cancel

Add

Adding Rule

Name

My Rule

Tags

add upto 3 tags, use comma as separator...

Description

provide a short description of your access rule...

Action

Allow

Deny

Discard

Type

IPv4

IPv6

Schedule

Always

Enable

Security Rule Action

--- Select Security Rule Action ---

Source / Destination

App/URL/Custom Match

Match Operation

OR

AND

Application

Any

AND All Matched App Signatures

Web Category

Any

URL

Any

Custom Match

Any

Show Diagram

Create Another

Validate

Cancel

Add

- **Decryption Policy**

In SonicOS, DPI-SSL and DPI-SSH settings are converted into decryption rules that define which SSL/TLS traffic should be decrypted. DPI-SSL and DPI-SSH settings are only configurable within decryption rules. You have granular control over what needs to be decrypted and how.

Adding Decryption Rule

Name

My Rule

Tags

add upto 3 tags, use comma as separator...

Description

provide a short description of your decryption rule...

Action

Decrypt

Bypass

Type

☒ IPv4
 ☐ IPv6

Schedule

Always

Enable

☒

Source / Destination

URL

Source Address

Any

Destination Address

Any

Service

Any

User

All

(From / To) Country

Any

Show Diagram

☐

Cancel

Save

Adding Decryption Rule

Name

My Rule

Tags

add upto 3 tags, use comma as separator...

Description

provide a short description of your decryption rule...

Action

Decrypt

Bypass

Type

☒ IPv4
 ☐ IPv6

Schedule

Always

Enable

☒

Source / Destination

URL

Match Operation

☒ OR
 ☐ AND

Web Category

Any

Website

Any

Show Diagram

☐

Cancel

Save

- **DoS Policy**

DoS rules define which traffic can cause Denial of Service and how to protect the system from such attacks. DoS rule configuration provides a unified workflow that includes connection limiting settings and all the settings to protect against Flood attacks (UDP/TCP-syn/ICMP floods), Smurf attacks, LAND (Local Area Network Denial) attacks and other denial of service attacks. These settings are no longer configured from various pages of the management interface as in versions prior to 7.0.

Adding DoS Policy

Name

My Rule

Tags

add upto 3 tags, use comma as separator...

Description

provide a short description of your DoS rule...

Action

Protect

Bypass

Type

IPv4

IPv6

Schedule

Always

Enable

Source/Destination

Source

Any

Destination

Any

Service

Any

Action Profile

--Select profile--

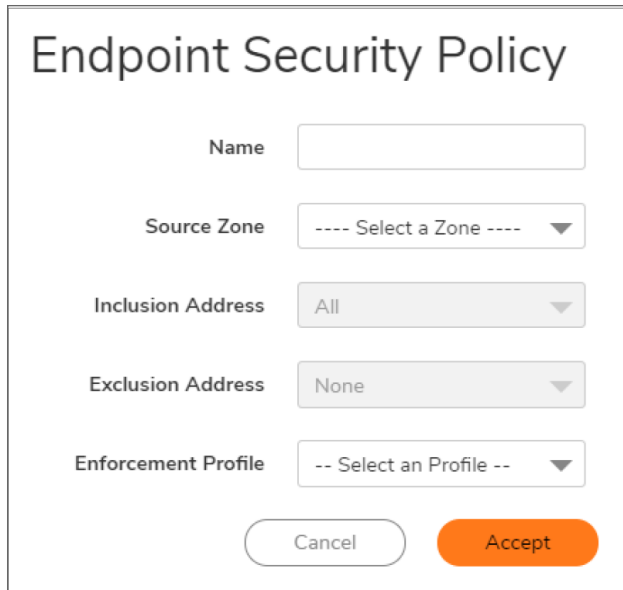
Show Diagram

Cancel

Add

- **Endpoint Policy**

Endpoint rules provide client security settings that apply to traffic on the specified zone. These rules combine settings for the zone, inclusion and exclusion addresses, and an enforcement profile that controls grace period and bypass settings for guest users. At least one client security service must be licensed before endpoint rules can be configured.



The image shows a configuration form titled "Endpoint Security Policy". It contains five fields, each with a label and a dropdown menu:

- Name**: A text input field.
- Source Zone**: A dropdown menu with the text "---- Select a Zone ----" and a downward arrow.
- Inclusion Address**: A dropdown menu with the text "All" and a downward arrow.
- Exclusion Address**: A dropdown menu with the text "None" and a downward arrow.
- Enforcement Profile**: A dropdown menu with the text "-- Select an Profile --" and a downward arrow.

At the bottom of the form are two buttons: "Cancel" (a light gray button) and "Accept" (an orange button).

The following two policy types are carried forward from earlier versions of SonicOS with minor enhancements:

- **NAT Policy**

NAT rules define which traffic needs to be translated and how.

- **Route Policy**

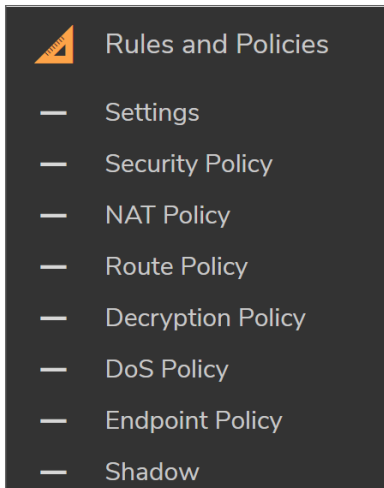
Routing rules define how traffic should be routed.

Traffic is defined by *match criteria*. Each policy type has its own set of match criteria. Each rule defines the specific criteria to match, and defines an associated action. Actions are defined in an Action Profile. Some policy types do not need an action profile, such as Decryption Policy.

In summary, a policy is a set of rules and each rule is defined by match criteria and has an action and/or action profile.

The SonicOS unified policy redesign provides additional enhancements, including:

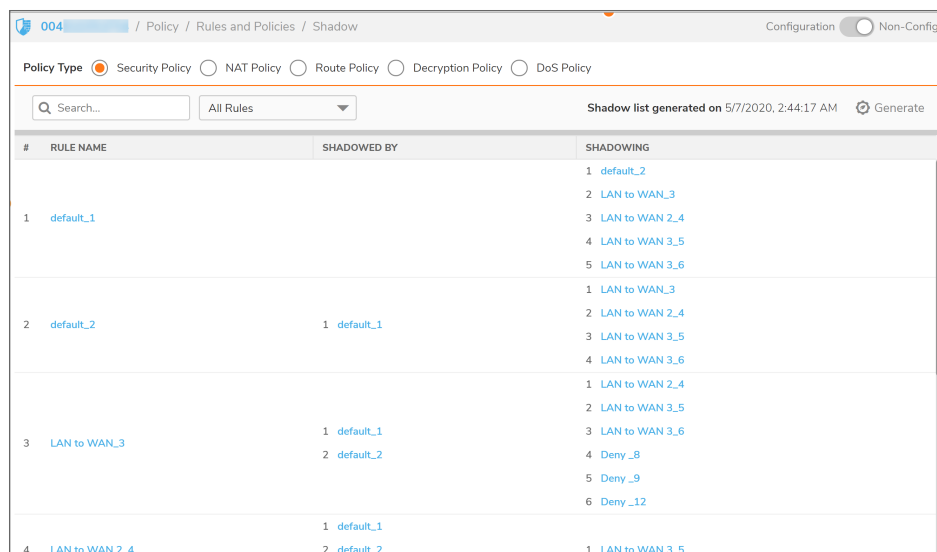
- Enhanced rules and policy processing engine for Security, NAT, Route, Decryption, DoS, and Endpoint policies:



- SonicOS policy rules can scale up to 8KB (8192 bytes) in size to accommodate the additional configuration data.
- Rule configuration is intuitive with a simplified view, even with all the merged settings.
- Relevant objects and action profiles for individual components are selected within the workflow.
- Policy cloning is available.
- In-cell editing capability can be used from within the policies table.
- Shadow policy views allow analysis for Security, NAT, Route, Decryption, and DoS policy sets.
- Simplified and advanced policy views for policy management:
 - Policy grid column customizations for simple and advanced use cases
 - Rule grouping
- Rule statistics:
 - Used vs unused rules
 - Active vs inactive rules
 - Hit counts and bandwidth consumption

About the Shadow Feature

The **POLICY | Rules and Policies > Shadow** page shows which rules are being shadowed by other rules and which rules are shadowing other rules. Select the **Policy Type** at the top to view shadowing for each type of policy.



The screenshot shows the SonicOS web interface for the 'Shadow' page. At the top, there's a breadcrumb '004 / Policy / Rules and Policies / Shadow' and a 'Configuration' toggle set to 'Non-Config'. Below this, a 'Policy Type' section has radio buttons for 'Security Policy' (selected), 'NAT Policy', 'Route Policy', 'Decryption Policy', and 'DoS Policy'. A search bar and a dropdown menu set to 'All Rules' are present. A timestamp indicates the 'Shadow list generated on 5/7/2020, 2:44:17 AM' with a 'Generate' button. The main table has three columns: '#', 'RULE NAME', 'SHADOWED BY', and 'SHADOWING'. It lists four rules: 'default_1', 'default_2', 'LAN to WAN_3', and 'LAN to WAN_4', showing their shadowing relationships and the specific rules that shadow them.

#	RULE NAME	SHADOWED BY	SHADOWING
1	default_1		1 default_2 2 LAN to WAN_3 3 LAN to WAN_2_4 4 LAN to WAN_3_5 5 LAN to WAN_3_6
2	default_2	1 default_1	1 LAN to WAN_3 2 LAN to WAN_2_4 3 LAN to WAN_3_5 4 LAN to WAN_3_6
3	LAN to WAN_3	1 default_1 2 default_2	1 LAN to WAN_2_4 2 LAN to WAN_3_5 3 LAN to WAN_3_6 4 Deny_8 5 Deny_9 6 Deny_12
4	LAN to WAN_2_4	1 default_1 2 default_2	1 LAN to WAN_3_5

Each rule in the **RULE NAME** column might have a rule in the **SHADOWED BY** column and the **SHADOWING** column. The rule in the SHADOWING column might not be hit because the rule in the RULE NAME column will match the traffic first. The rules under SHADOWED BY will be hit before the rules in the RULE NAME column, possibly preventing the RULE NAME column rule from being hit.

Rules can be partially shadowed. In this case they will be hit if they match traffic characteristics that the other rule is not matching on.

For example, say A+B is being matched in rule #2 which is shadowed by rule #1, where rule #1 matches A. If traffic matches A, rule #1 will hit. If traffic matches B, rule #2 will hit.

Another example involves two subnets. Rule #1 blocks traffic matching the 10.0.0/24 subnet. Rule #2 allows traffic matching the 10.0/16 subnet.

Rule #1 shadows Rule #2. This is a partial shadow.

You can click on any rule to view details:

Security Policy Details

RULE DETAILS

Name	LAN to WAN_3
ID	3
UUID	"00000000-0000-0001-0700-004010351f54"
IP Version	IPv4
Comment	Adding default rule

ACTION

Name	Default Profile
Access Control	Allow

BANDWIDTH MANAGEMENT

Bandwidth Aggregation	-
Egress Status	Disabled
Ingress Status	Disabled

QOS PROPERTIES

DSCP Marking Action	Preserve
802.1p Marking Action	Preserve

ANTI-VIRUS PROFILE

Gateway Anti-Virus	-
--------------------	---

IPS/THREAT PROFILE

IPS/Threat	-
------------	---

ANTI-SPYWARE PROFILE

Anti-Spyware	-
--------------	---

BOTNET FILTER PROFILE

Botnet Filter	Disabled
---------------	----------

CONTENT FILTER PROFILE

Content Filter	-
----------------	---

LOGGING

Logging	-
Flow Reporting	-
Packet Monitoring	-

MISCELLANEOUS

TCP Inactivity Timeout	15 minutes
UDP Inactivity Timeout	30 minutes
Source IP Address Limit	Disabled
Destination IP Address Limit	Disabled
Allow Fragmented Packets	Enabled

ZONE/INTERFACE

Source	Any
Destination	Any

ADDRESS

Source	Any
Destination	Any

SERVICE

Source Port	Any
Service	Any

USER

User	"All"
------	-------

APP/URL/CUSTOM MATCH

Match Operation	OR
Application	Any
App AND Operation	Disabled
Web Category	Any
Website	Any
Custom Match	Any

GEO

(From/To) Country	Any
-------------------	-----

SCHEDULE

Schedule	Always
----------	--------

TICKET

Tag 1	
Tag 2	

About Action Profiles

Action profiles are used in Security Rules and DoS Rules and are configured globally under **OBJECTS | Actions Profiles**. Click the **+Add** button to configure all types of action profiles for use in the policy rule.

Security Rule Action Profiles:

The **Add Security Action Profile** page provides the following screens to configure action profiles for Security Rules:

- **Bandwidth/QoS**
- **Anti-Virus**
- **Threat Prevention**
- **Anti-Spyware**
- **Botnet Filter**
- **Content Filter**
- **Block Page and Logging**
- **Miscellaneous**

When the **Add Security Action Profile** window opens, the first screen is **Bandwidth/QoS**. You can select other tabs/screens to configure other types of Action Profiles.

Add Security Action Profile

Bandwidth/QoS

Anti-Virus

Intrusion Prevention

Anti-Spyware

Botnet Filter

Content Filter

Block Page and Logging

Miscellaneous

Action Profile Name

BANDWIDTH MANAGEMENT PROFILE

Bandwidth Aggregation Method

Per Policy

Enable Egress Bandwidth Management

Bandwidth Object

--Select a Bandwidth ...

Enable Ingress Bandwidth Management

Bandwidth Object

--Select a Bandwidth ...

Enable Tracking Bandwidth Usage

QOS MARKING PROFILE

DSCP Marking Action

None

802.1p Marking Action

Preserve

Cancel

Save

The **Miscellaneous** screen provides options for:

- Connection Settings
- Advanced Settings
- SIP / H.323
- For Traffic from an Unauthenticated User

Action Profile Name

CONNECTION SETTINGS

TCP Connection Inactivity Timeout (minutes)

15

UDP Connection Inactivity Timeout (seconds)

30

ADVANCED SETTINGS

Allow Fragmented Packets

☒

Bypass Inspection Of Server To Client Packets

☐

SIP / H.323

Enable SIP Transformation

☐

Enable H.323 Transformation

☐

FOR TRAFFIC FROM AN UNAUTHENTICATED USER

Don't redirect unauthenticated users to log in

☐

DoS Rule Action Profiles:

The **Add DoS Action Profile** page provides the following screens to configure action profiles for DoS Rules:

- Flood Protection
- DDoS Protection
- Attack Protection
- Connection Limiting

Add DoS Action Profile

Flood Protection | DDoS Protection | Attack Protection | Connection Limiting

DoS Rule Action Name:

LAYER 3 SYN FLOOD PROTECTION - SYN PROXY

Enable SYN Flood Protection: ☐

SYN Flood Protection Mode:

SYN Attack Threshold:

Suggested value calculated from gathered statistics: 300

Attack threshold (incomplete connection attempts / second):

SYN-Proxy options:

All LAN/DMZ servers support the TCP SACK option: ☐

Limit MSS sent to WAN clients (when connections are proxied): ☐

Maximum TCP MSS sent to WAN clients:

Always log SYN packets received: ☐

LAYER 2 SYN/RST/FIN FLOOD PROTECTION - MAC BLACKLISTING

Threshold for SYN/RST/FIN flood blacklisting (Packets / Sec):

Enable SYN/RST/FIN flood blacklisting on all interfaces: ☐

Never blacklist WAN machines: ☐

Always allow SonicWall management traffic: ☐

ENABLE UDP FLOOD PROTECTION

Enable UDP Flood Protection: ☐

UDP Flood Attack Threshold (UDP Packets / Sec):

UDP Flood Attack Blocking Time (Sec):

ENABLE ICMP FLOOD PROTECTION

Enable ICMP Flood Protection: ☐

ICMP Flood Attack Threshold (ICMP Packets / Sec):

ICMP Flood Attack Blocking Time (Sec):

Features Available on TZ Series, NSa Series, and NSsp Series

This section describes features supported only on SonicWall TZ series, NSa series, and NSsp series (except NSsp 15700) firewalls. Many of these features are only supported on physical appliances.

These features are described in these topics:

- [Switch Management](#)
- [PortShield Groups](#)
- [Access Points Management](#)
- [WWAN and 4G/LTE](#)
- [Storage Device Configuration](#)

Switch Management

SonicWall Switches can be connected to and managed by TZ and NSa series and NSsp 13700 firewalls.

SonicWall Switches offer multi-gigabit wired performance that lets you rapidly scale your branch networks through remote installation. Available in seven models — ranging from eight to 48 ports, with gigabit and 10 gigabit Ethernet ports — SonicWall Switches deliver network switching that accommodates the growing number of mobile and IoT devices in branch locations and provides the network performance needed to support cloud-delivered applications. SonicWall Switches also fit seamlessly into your existing SonicWall ecosystem, helping you to unify your network security posture. They're SD-Branch-ready and managed via firewalls — either locally

or through SonicWall's cloud-based Capture Security Center — for unified, single-pane-of-glass management of your entire SonicWall infrastructure.

SonicWall Switches provide additional ports and are designed to connect SonicWall firewalls with external devices such as wireless access points, IP surveillance cameras, VoIP phones and other PoE-capable devices as well as other Ethernet-based networking equipment or computers. The Switch provides simple, yet powerful PoE manageability with features such as IEEE 802.3af or IEEE 802.3at/af ports, PoE port management, voice VLAN, QoS, static routing, 802.1x authentication, and access point management.

Seven Switch models are available, providing a range of capabilities to choose from.



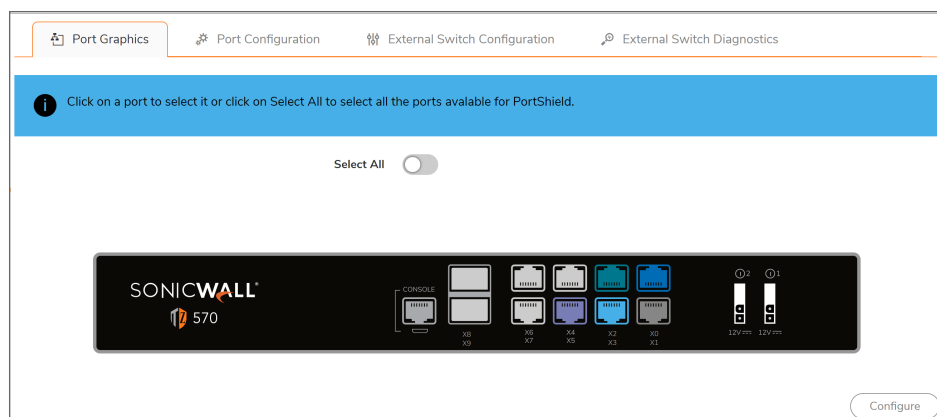
SonicWall Switches can be deployed in standalone mode or daisy chain mode.

In SonicOS, there are three ways to view a connected Switch:

- Physical view
- List view
- VLAN view

SonicOS displays Switch information, including bandwidth usage per port and PoE Statistics with power usage.

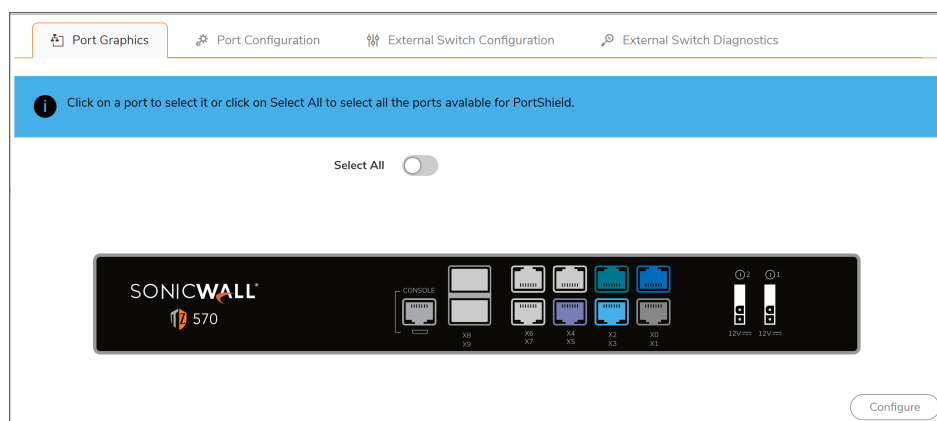
SonicWall Switch ports can be added to **PortShield Groups** configurations.



PortShield Groups

A PortShield interface is a virtual interface with a set of ports, including ports on SonicWall Switches or other supported external switches assigned to it. PortShield architecture enables you to configure some or all of the LAN ports into separate security contexts, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each context has its own wire-speed PortShield that enjoys the protection of a dedicated, deep packet inspection security appliance.

You can configure PortShield interfaces on the **NETWORK | System > PortShield Groups** pages.



<div> Port Graphics Port Configuration External Switch Configuration External Switch Diagnostics </div> <div>Clear Statistics</div>							
#	NAME	PORTSHIELD INTERF...	TYPE	LINK SETTINGS	LINK STATUS	ENABLED	COMMENT
1	X0	LAN	Copper	Auto Negotiate	No link	✓	Default LAN
2	X1	WAN	Copper	Auto Negotiate	1 Gbps Full Duplex		Default WAN
3	X2	Independent	Copper	Auto Negotiate	1 Gbps Full Duplex	✓	Firewall Uplink - SonicWall Switch
4	X3	Independent	Copper	Auto Negotiate	No link	✓	N/A
5	X4	Unassigned	Copper	Auto Negotiate	No link	✓	N/A
6	X5	Independent	Copper	Auto Negotiate	1 Gbps Full Duplex	✓	Firewall Uplink - SonicWall Switch
7	X6	Unassigned	Copper	Auto Negotiate	No link	✓	N/A
8	X7	Unassigned	Copper	Auto Negotiate	No link	✓	N/A
9	X8	Unassigned	Copper	N/A	No link	✓	N/A
10	X9	Unassigned	Copper	N/A	No link	✓	N/A
Total: 10 item(s)							

Access Points Management

SonicWall SonicPoint and SonicWave wireless access points are specially engineered to work with SonicWall security appliances to provide wireless access throughout your enterprise. SonicWall access points integrate with SonicWall TZ, NSa and NSp 13700 firewalls to create a secure wireless solution that delivers comprehensive protection for wired and wireless networks. They provide high-speed wireless access with enhanced signal quality and reliability that takes advantage of the latest capabilities to achieve gigabit wireless performance. With support for IEEE 802.11a/b/g/n/ac standards, the SonicPoint/SonicWave series enables your organization for bandwidth-intensive mobile applications in high density environments without signal degradation.

You can connect SonicPoint/SonicWave access points to your firewall or to a connected Switch, and manage them from the **DEVICE | Access Points** pages in SonicOS 7.1.

<div>EXTERNAL CONTROLLERS</div> <div> Access Point Provisioning Profiles Access Point Objects </div> <div> Search... Synchronize Access Points Register Reboot Delete Refresh </div>							
#	NAME	ENABLE	INTERFACE	NETWORK SETTINGS	STATUS	5 GHZ RADIO	
1	SonicPoint ACe a76304 Model: ACe	✓	X3 (WLAN)	IP: 194.153.3.239 MAC: c0:a0:e4:a7:63:04 MGMT: Layer 2	Non-responsive	MSSID: AP_group Mode: 5GHz n/a/ac Mesh: Not Supported	
2	SonicWave 4320 4d289c Model: 4320	✓	X3 (WLAN)	IP: 194.153.3.240 MAC: 18:b1:69:4d:28:9c MGMT: Layer 2	Non-responsive	MSSID: AP_group Mode: 5GHz n/a/ac Mesh: Disabled	

SonicOS 7.1 provides several new features for wireless access points:

- **Enhanced Access Point Snapshot**
SonicOS displays real-time statistics on access point status in the network and wireless client associations.
- **Access Point Traffic Rate**
SonicOS displays real-time bandwidth usage by access points.
- **WiFi Client Report**
SonicOS provides a real-time WiFi client report based on OS type and frequency, along with a top client chart.
- **Real-Time WiFi Client Monitor**
SonicOS displays the client host machine, OS type, frequency, access point details, and data transfer information.

WWAN and 4G/LTE

SonicWall TZ, NSa and NSsp 13700 appliances support a number of external 4G/LTE devices. You can connect a 4G/LTE device to a USB port on the firewall to provide Wireless WAN (WWAN) connectivity to the internet over cellular networks.

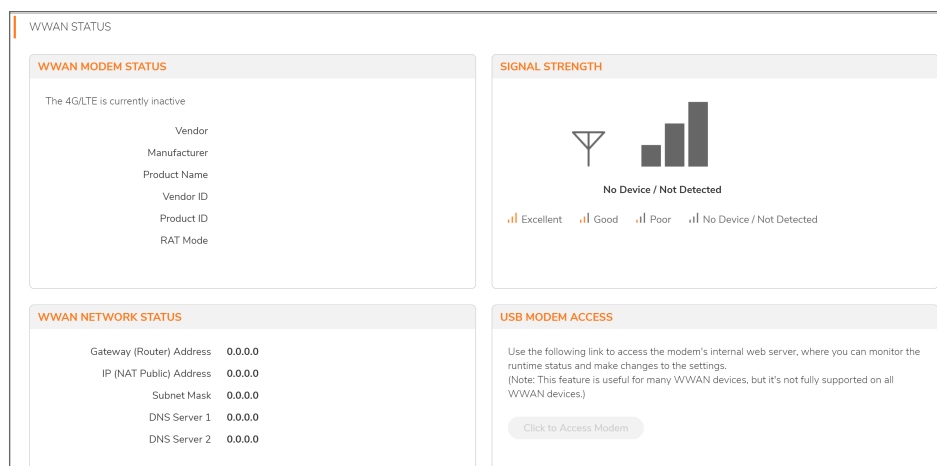
The 4G/LTE connection can be used for:

- WAN failover to a connection that is not dependent on wire or cable.
- Temporary networks where a preconfigured connection might not be available, such as at trade-shows and kiosks.
- Mobile networks, where the SonicWall appliance is based in a vehicle.
- Primary WAN connection where wire-based connections are not available and 4G/LTE cellular is.

To use the 4G/LTE interface, you must have a 4G/LTE PC card or USB device and a contract with a wireless service provider. A 4G/LTE service provider should be selected based primarily on the availability of supported hardware. SonicOS supports the devices listed online at:

<https://www.sonicwall.com/support/knowledge-base/what-wireless-cards-and-usb-broadband-modems-are-supported-on-firewalls-and-access-points>

By default, the firewall tries to detect the type of device that is connected. If it can successfully identify what kind it is, the left side navigation changes to provide configuration pages in the **DEVICE | WWAN** menu group. Without a connected 4G/LTE device, the **WWAN** page displays the current status.

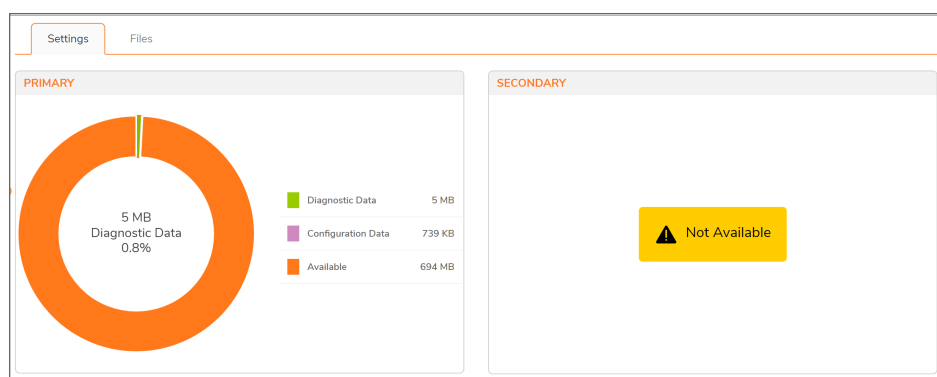


Storage Device Configuration

SonicOS 7.1 provides the **DEVICE | Settings > Storage** page showing the status of M.2 storage modules on the firewall, including the secondary storage module, if installed. Storage modules are supported on TZ, NSa and NSsp 13700 firewalls. The storage module resides in a small compartment on the bottom of the firewall.

Module usage statistics are displayed and the file names of the stored files can be viewed on the **Settings** and **Files** screens.

Settings screen:



Files screen:

Settings		Files					
Diagnostic Data		Configuration Backup		Logs			
				Create Backup Refresh			
#	FIRMWARE VERSION	CONFIGURATION BACKUP DATE	FIRMWARE LOAD DATE	USERNAME	COMMENTS	BACKUP TYPE	ACTIONS
1	Backup created with version SonicOS 7.0.0-P859 (1 Configuration Files available) Local backup 2			admin	This is a backup on Local Storage.		
2	Backup created with version SonicOS 7.0.0-P689 (1 Configuration Files available) Local backup 1			admin	This is a backup on Local Storage.		
Total: 2 item(s)							

Features Available on NSv Series

The NSv series are the only platforms that can run either SonicOS or SonicOS 7.1.

Because the NSv is a virtual appliance, it does not support features that manage a physically connected device, such as a SonicWave wireless access point or a SonicWall Switch.

Topics:

- [Feature Support on NSv Series](#)
- [Changing Between Classic Mode and Policy Mode](#)

Feature Support on NSv Series

SonicOS 7.1 on SonicWall NSv Series supports the majority of features supported on SonicWall physical firewalls, with only a few exceptions. These exceptions are generally those features that control an external device, such as a switch, wireless hardware, or cellular WWAN devices.

The table below lists the key SonicOS and SonicOS features and whether they are supported or not supported on the NSv Series.

SONICOS 7.1 FEATURE SUPPORT ON THE NSV SERIES

Main Category	Feature Category	Feature	Description	Supported
Unified Policy Features	Unified Security Policy	Source/Destination IP, Port, Service, and User	SPI Rule based on user Information	Yes
		Application Control	Application Signature and Component control within a Security Rule	Yes

Main Category	Feature Category	Feature	Description	Supported
		CFS/Web Filtering	Content Filtering Rules within a Security Rule	Yes
		Botnet	Botnet control within a Security Rule	Yes
		Geo-IP / Country	Country-based control within a Security Rule	Yes
		EndPoint Security Policy	Endpoint Security with Capture Client based on Rules	Yes
		Rule Diagram	Pictorial view of a Security Policy, NAT Policy or Route Policy to assist in finding real-time statistics	Yes
	Decryption Policy		Rules to inspect SSL/TLS traffic	Yes
	DoS Policy		Rules to inspect Denial of Service (DoS) and Distributed DoS (DDOS) attacks, such as flooding or Smurf	Yes
	Profile Objects	Endpoint Security		Yes
		Bandwidth Management		Yes
		QoS Marking		Yes
		Content Filter		Yes
		Intrusion Prevention		Yes
		DHCP Option		Yes
		AWS VPN		Yes
	Action Profiles	Security Profile		Yes
		DoS Profile		Yes
	Signature Objects	Anti-Virus Signature Object	Anti-Virus Signatures with more details on each signature	Yes

Main Category	Feature Category	Feature	Description	Supported
		Anti-Spyware Signature Object	Anti-Spyware Signatures with more details on each signature	Yes
	Rule management	Cloning	Cloning of an existing security rule to create a new rule	Yes
		Shadow rule analysis	Displays duplicate and shadowing rules within every policy	Yes
		In-cell editing	Ability to perform selective cell editing on the security rule without opening the rule, reducing the number of clicks for the administrator	Yes
		Group editing		Yes
		Export of Rules	Rules can be exported in CSV format	Yes
		Live Counters	Capture live statistics for a security policy	Yes
	Managing views	Used/Unused Rules	Display the security rules which are being actively used or not being used	Yes
		Active/Inactive Rules	Display the security rules which are enabled or disabled	Yes
		Section Policy Grouping	Grouping of policies by sections to help manage thousands of security rules	Yes
		Customizable Grid/Layout	Customizable and movable columns within Security Policy, NAT Policy, Route Policy, Decryption Policy, and DoS Policy pages	Yes

Main Category	Feature Category	Feature	Description	Supported
		Custom Grouping	Grouping of policies by custom options like zone, tag, or other	Yes
Decryption Features	Decryption Support for TLSv1.3		TLS 1.3 enhanced security implemented in firewall management, SSL VPN and DPI	Yes
	Blocking Cipher Controls		Block or unblock cipher control selectively	Yes
	Decryption Rule Monitoring		Enhanced monitoring of Decryption Rules including Bandwidth, Connection Rate, Connection Usage	Yes
Multi-Instance Features	Multi-Instance Support		Multiple virtual firewalls running on a single firewall	No
	Instance View		View usage and other related statistics for each instance	No
	Per-Instance Separate Firmware		Ability to run separate firmware on each instance and the root instance	No
	Instance Licensing from Root		License the instances from the root instance and display the key for each instance	No
SDWAN Features	SDWAN Scalability		Scalable tunnel interfaces for distributed enterprises	Yes
	SDWAN Usability Wizard		Wizard to automatically configure an SDWAN Policy on the firewall	Yes
API Features	RESTful API Support		Complete API support for configuring every section of the management interface	Yes

Main Category	Feature Category	Feature	Description	Supported
HOME Page Features	Dashboard Features	Actionable Dashboard	Dashboard with actionable alerts	Yes
		Device View Enhancements	Displays the real-time status of the front panel interfaces and LEDs	Yes
		Top Traffic Summary	Traffic distribution usage on the firewall with real-time updates and the most-used applications	Yes
		Top User Summary	Summary of top users based on allowed or blocked sessions, by data sent and received	Yes
		Insights into Threats	Real-time threat summary for the network, including virus, zero-day malware, spyware, vulnerabilities, risky applications	Yes
		Policy Overview	Graphical view of used/unused and allowed/denied statistics for Security, NAT, Route, Decryption, and DoS Policies	Yes
		Objects Overview	Graphical view of custom and default Address, Zone, Service, Schedules, Custom Match, Application, Country, URI, Website, and Web Category objects	Yes

Main Category	Feature Category	Feature	Description	Supported
		Profiles and Signatures Overview	Graphical view of custom and default profiles and signatures for IPS, Security, DoS, Block Page, Gateway Anti-Virus, Anti-Spyware and others	Yes
		Zero-Day Attack Origin Analysis	Displays location-based attack origin by countries	Yes
	Network Topology		Topology View displaying hosts, access points connected in the network based on device name, MAC address and IP address	Yes
	Notification Center		Summary of threats, event logs, system alerts with actionable alerts and outstanding tasks for the administrator	Yes
	Packet Monitoring Enhancement		Packet Monitor ability to find the related Security Rule, NAT Rule, Route Rule, Decryption Rule, and Signatures for Application, IPS, Anti-Virus, and Anti-Spyware	Yes
Debugging and Diagnostic Features	System Logs Download		Console logs can be downloaded from the web management interface without requiring connection to the Console port	Yes

Main Category	Feature Category	Feature	Description	Supported
		SSH Terminal	SSH Terminal access within web management interface for troubleshooting	Yes
		System Diagnostics	Enhanced system diagnostics for troubleshooting	Yes
		Policy Lookup	Policy Lookup displays the rule that will be used for a particular type of traffic based on the match attributes	Yes
Capture Threat Assessment (CTA 2.0)	Template Customization	Executive Template	Executive Template for company executives with a summarized report containing Key Findings and Recommendations	Yes
	Report Customization	Customizable Logo, Name, and Company	Customization of logo, administrator name and company name	Yes
	Reporting Enhancements	Key Findings		Yes
		Risky File Analysis		Yes
		Risky Application Summary		Yes
		Malware Analysis		Yes
		Glimpse of Threats		Yes
		Web Filtering Statistics		Yes
		Recommendations		Yes
	Comparison Statistics	Industry Average	Comparison with peer industry statistics	Yes
		All Organizations Average	Comparison with global statistics	Yes

Main Category	Feature Category	Feature	Description	Supported
Wireless Features	Enhanced Access Point Snapshot		Displays real-time statistics about access point network status and client associations	No
	Access Point Traffic Rate		Real-Time bandwidth usage by access points	No
	WiFi Client Report		Real-Time WiFi client report based on OS type, frequency, top client chart	No
	Real-Time WiFi Client Monitor		Determines the host machine, OS type, frequency, access point information, data transfer	No
Switch Features	SonicWall Switch Support		SonicWall Switch in standalone and daisy chain deployments	No
	Switch Network Overview		SonicWall Switch views: physical view, list view, and VLAN view	No
	Bandwidth Usage per Switch Port		Display SonicWall Switch bandwidth usage per port	No
	PoE Usage		Display SonicWall Switch PoE statistics including power usage	No
Monitoring Features	Risky Application Statistics			Yes
	AppFlow Monitoring Enhancements			Yes
Management	NSM Management			No
	API Driven Management			Yes

Main Category	Feature Category	Feature	Description	Supported
	ZeroTouch Registration and Provisioning			Yes
	CSC Simple Reporting			No
General Features	Global Search		Search globally for parameters within the SonicOS configuration to determine the Objects or Policies in which the parameters are referenced	Yes
	Storage Device Configuration		Configuration of storage modules including extended modules, and display module usage statistics	No

Changing Between Classic Mode and Policy Mode

SonicWall NSv series firewalls support can be configured for both Classic mode and Policy mode. Selection of or changing between Classic and Policy modes is supported on NSv series starting in SonicOS 7.0 with the following use cases:

- Fresh deployments of SonicOS
- Upgrading an existing deployment from SonicOS 7.0 to SonicOS 7.1
- Upgrading an existing deployment from SonicOS 6.5.4.v to SonicOS 7.1
- Changing an existing deployment from SonicOS 7.0 to SonicOS 7.1 (from Classic mode to Policy mode)
- Changing an existing deployment from SonicOS 7.1 to SonicOS 7.1 (from Policy mode to Classic mode)

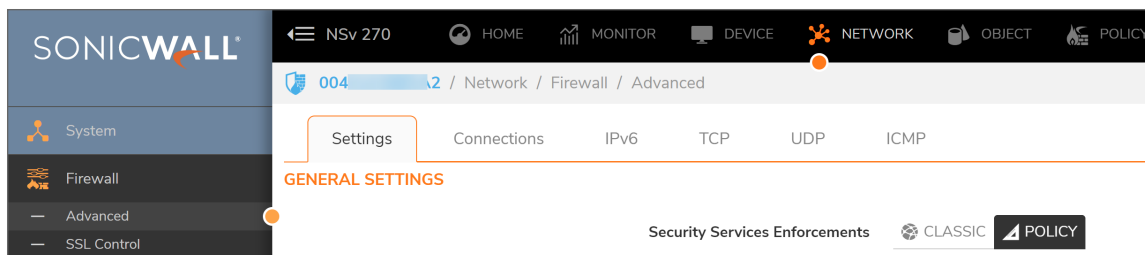
If you have existing NSv deployments running SonicOS 6.5.4.v and plan to continue using NSv on SonicOS 7.1, the ability to change modes provides flexibility to upgrade seamlessly into Classic mode while evaluating or preparing for the move to Policy mode.

Closed-network NSv deployments also support Classic and Policy modes. In a closed network, the lack of internet access prevents the NSv from communicating with the SonicWall License Manager, so the Manual Keyset option is used to apply the security services and other licensing on the firewall. You can select the mode

when obtaining the license keyset in MySonicWall. If you switch between modes, you will need to obtain and apply a new license keyset for your NSv.

The **CLASSIC** and **POLICY** mode switching option is only visible in SonicOS after it is enabled in MySonicWall. Log into your MySonicWall account and enable Firewall Mode Switching for the respective firewall serial number.

The **Settings** screen on the **NETWORK | Firewall > Advanced** page displays the **CLASSIC** and **POLICY** options for **Security Services Enforcements**.



The current mode is indicated by the black button. These buttons are used to initiate the mode change.

For more information, refer to:

- [Choosing the Mode in Fresh Deployments or Upgrades](#)
- [Changing From Classic to Policy Mode](#)
- [Changing From Policy to Classic Mode](#)

Choosing the Mode in Fresh Deployments or Upgrades

During NSv registration after fresh deployments or upgrades of existing NSv firewalls to SonicOS 7.0.1, you are prompted to choose Classic or Policy mode.

The specific use cases where this applies are:

- Fresh deployments of SonicOS or SonicOS 7.0.1
- Upgrading an existing deployment from SonicOS 7.0.0 to SonicOS 7.0.1
- Upgrading an existing deployment from SonicOS 6.5.4.v to SonicOS 7.0.1
- Resetting the registration of (deregistering) an existing NSv deployment running SonicOS 7.0.1

Choosing Classic Mode will cause the NSv to boot up running SonicOS 7.0.1 with the SonicOS features.

Choosing Policy Mode will cause the NSv to boot up running SonicOS 7.0.1 with the SonicOS features.

When upgrading an NSv from SonicOS 6.5.4.v to SonicOS 7.1 (Classic mode) using the SWI file, the supported features are on par with a SonicWall TZ or NSa running SonicOS 7.1, except that the following are not supported on NSv:

- Switch Network (SonicWall Switch management support)
- Access Points / Wireless

- WWAN (4G / LTE)
- PortShield

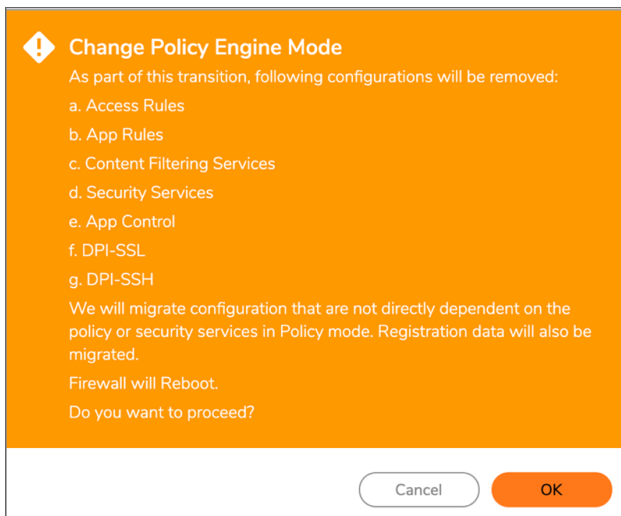
① **NOTE:** After upgrading your NSv from SonicOS 6.5.4.v to SonicOS 7.1, you will need to register it using the new (7.0) serial number.

Changing From Classic to Policy Mode

This section describes how to change from Classic mode (SonicOS) to Policy mode (SonicOS) on an existing NSv deployment. After this change, some of the current configuration settings might not be available in Policy mode. The list of configuration settings that will not be available in policy mode is shown in the popup screen when you click the **POLICY** button.

To change from Classic mode to Policy mode:

1. Navigate to the **NETWORK | Firewall > Advanced** page.
2. On the **Settings** screen next to **Security Services Enforcements**, click the **POLICY** button.
3. Read the popup notifications.



4. Click **OK** to proceed with the mode change or click **Cancel** to cancel the mode change.

The NSv reboots and comes up in Policy mode. You must manually reconfigure any settings that were removed during the mode change. These can include configuration settings involving:

- Access Rules
- App Rules
- Content Filtering Service (CFS)
- Security Services
- App Control

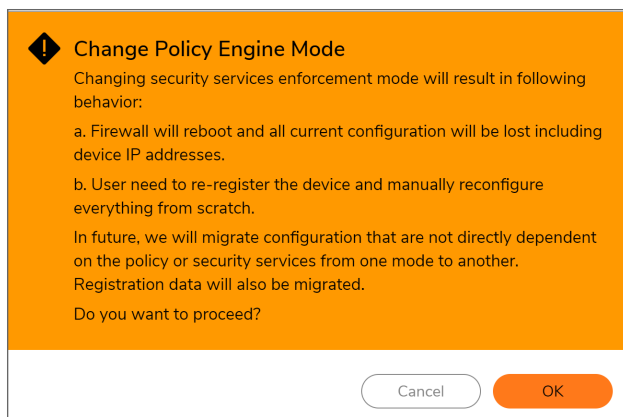
- DPI-SSL
- DPI-SSH

Changing From Policy to Classic Mode

This section describes how to change from Policy mode (SonicOS) to Classic mode (SonicOS) on an existing NSv deployment. After this change, all of the current configuration settings will be lost and the NSv will reboot with factory default settings. A warning to this effect is shown in the popup screen when you click the **CLASSIC** button.

To change from Policy mode to Classic mode:

1. Navigate to the **NETWORK | Firewall > Advanced** page.
2. On the **Settings** screen next to **Security Services Enforcements**, click the **CLASSIC** button.
3. Read the popup notifications.



4. Click **OK** to proceed with the mode change or click **Cancel** to cancel the mode change. The NSv reboots and comes up in Classic mode.
5. Log into the NSv using the default credentials, *admin / password*.
6. Configure the network settings to allow your NSv to connect to your local network and to the internet for access to MySonicWall and the SonicWall licensing server. For more information, refer to the *NSv Series 7.0 Getting Started Guide* for your platform (Azure, AWS, VMware, Hyper-V or KVM). The NSv Getting Started guides are available on the SonicWall technical documentation portal at [NSv 7.0 Getting Started Guides](#).
7. Register the NSv to enable full functionality. The **Register Device** button is available on the **HOME | Dashboard > System** pages.

At this point you can manually reconfigure the NSv or import a configuration settings file previously exported from one of the following:

- An NSv running SonicOS 7.0 (in Classic mode)
- An NSv running SonicOS 6.5.4.v

Features Available on NSsp 15700

Designed for large distributed enterprises, data centers, government agencies and service providers, the multi-blade SonicWall NSsp 15700 pairs advanced technologies like Real-Time Deep Memory Inspection (RTDMI™) with high-speed performance. This powerful security appliance supports advanced features including multi-instance deployments, advanced switching, authentication partitioning, and unified policy creation.

While most of these advanced features are available on other platforms running SonicOS 7.1, the Multi-Instance feature is unique to the NSsp 15700.

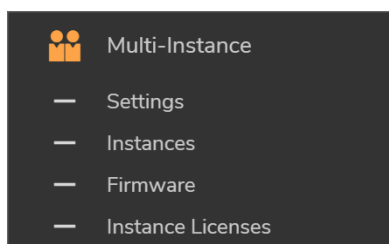
The following topic introduces the Multi-Instance feature:

- [About Multi-Instance](#)

About Multi-Instance

SonicOS 7.1 on NSsp 15700 supports the **Multi-Instance** feature. This feature allows the security appliance to launch multiple instances of SonicOS, each serving as an independent firewall. The Root Instance configures and launches each instance. Once the individual instances are up and running, their X0...X7 interfaces allow access for detailed firewall configuration.

Multi-Instance is configured from the **DEVICE | Multi-Instance** menu group.



Configuration starts from the **Multi-Instance > Settings** page:

SETUP MULTI-INSTANCE

Enable ☒

Reserve CPUs for Instance

Reserved CPU for Root Instance ?

Reserve physical interfaces for multi-tenancy

SONICWALL[®]

NSsp 15700

MGMT 10G/10T 40Gb

X24 X22 X20 X18 X16 X14 X12 X10 X8 X6 X4 X2 X0

X25 X23 X21 X19 X17 X15 X13 X11 X9 X7 X5 X3 X1

100Gb 40Gb 100Gb

4 RESERVED
20 AVAILABLE
3 IN USE

Cancel Accept

Each instance's X0, X1, X2... X7 interfaces are mapped to a VLAN on the NSsp front panel port (X0 to X25) by the Root Instance. Each instance can be configured with up to 8 ports. Each instance port can be mapped to a front panel port and tagged with a VLAN ID.

When you register your NSsp 15700 appliance, a number of instance licenses are automatically created. These licenses are displayed in the **Multi-Instance > Instance Licenses** page.

You can configure two instances as a High Availability pair: on a single NSsp 15700 and across two NSsp 15700 appliances that are already established as an HA pair.

- On a Single NSsp – Multiple instances within an NSsp can support Stateful HA. This multi-instance HA model exactly mimics the NSv HA model in terms of the behavior and capabilities. Two instances can be paired to form a Stateful HA pair. One of them assumes the role as a Primary active instance and the other as the Secondary standby instance. The active and standby roles can change during an instance's lifetime.
- On an NSsp HA pair – Multiple instances residing on different units of an established NSsp HA pair can support Stateful HA. This requires a physical connection between at least one dedicated physical port on each of the NSsp HA units, to be used for the Multi-instance HA Control interface and HA Data interface.

For more information about enabling and configuring Multi-Instance, refer to the *SonicOS 7.1 Multi-Instance Administration Guide* and the *SonicOS 7.1 Getting Started for the NSsp 15700* guide on the SonicWall technical documentation portal.

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

About SonicOS
Updated - March 2024
Software Version - 7.1
232-005857-00 Rev B

Copyright © 2024 SonicWall Inc. All rights reserved.

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