

SonicOS 7.0.1

Common Criteria

Administration Guide

for NDPP

SONICWALL[®]

Contents

Introduction	7
Supported Platforms	7
Operational Environment	8
Product Functionality Not Included in the Scope of the Evaluation	8
Initial Setup	10
Secure Device Delivery	10
Delivery of Hardware Devices	10
Delivery of Virtual Firewalls	10
Product Registration	11
Connect and Power On	11
Initial Setup and Registration Using Local Management	11
Enabling NDCPP Compliance	13
Enabling NDPP Mode	13
Enabling FIPS Mode	18
Internal Settings	19
Startup and Self-Test	20
Deployment Modes	21
IPS Sniffer Mode	21
Configure IPS Sniffer mode in SonicOS	21
Wire Mode	23
Configuring Wire Mode in SonicOS	23
Bypass Mode	25
Secure Mode	26
Tap Mode	27
Management Mode	27
Zones and Interfaces	29
Zones in SonicWall	29
Predefined Zones in SonicOS	29
Adding and Configuring a Zone	30
Deleting a Zone	32
Configuring Interfaces	32

Product Administration	36
Managing through HTTP/HTTPS	36
Managing through the Local Console	37
Selecting a Security Certificate	38
Enforcing TLS Version	39
Local User Creation	40
Editing Local User	41
User Session Settings	41
Configure Inactivity Time	41
Configure Administrator Lockout	42
Password Compliance	43
Pre-Login Policy Banner	45
System Restart	45
Logging Out	46
Setting System Time	46
Managing Certificates	48
Certificates Table	48
Certificate Details	49
Importing Certificates	50
Importing a Local Certificate	50
Importing a Certificate Authority Certificate	51
Certificate Validation	51
Revocation Checking Using OCSP	52
Deleting a Certificate	53
Generating a Certificate Signing Request	53
Deleting a Certificate Signing Request	57
Checking Certificate Expiration	57
Configuring Client Certificate Verification	58
Object Classes	60
Addresses	60
Services	61
Match Objects	62
Schedules	63
Packet Dissection Objects	64
About Negative Matching	65
IPSec VPN	66
Configure VPN	66
General Tab on VPN Policy	67
Network Tab on VPN Policy	67

Proposals Tab on VPN Policy	68
Advanced Tab on VPN Policy	69
Configuring IKE Using a Preshared Secret Key	69
Configuring IKE Using Third Party Certificates	77
NAT Traversal	85
Configuring Routing Rules	86
Firewall	88
Access Rules	88
About Stateful Packet Inspection Default Access	89
Configuring Access Rules for a Zone	90
Adding Access Rules	90
Editing Access Rules	94
Deleting a Custom Access Rule	94
Default Deny Rule	95
Reconnection	95
TCP Connection	95
Source Routed Packets	96
Intrusion Protection	98
Deep Packet Inspection	98
IPS Status	98
IPS Global Settings	99
Detection vs Prevention	100
Resetting the IPS Settings and Policies	101
Configuring IPS Protection on Zones	101
Signatures	102
App Rules	103
SYN Flood Protection	105
ICMP Flood Protection	106
Port Scan Detection	107
Header-Based Signature	108
Firmware	110
Firmware Management	110
Firmware Upgrade	110
Log Settings	112
System Logs	112
Viewing System Logs	112
System Log Functions	112
Display Options	113

Auditing Logs	114
Viewing Auditing Logs	114
Audit Log Functions	115
Log Rotation and Deletion Policy	116
Log Settings and Levels	116
Audit Server Configuration	118
Configuring the Syslog Settings	118
Audit Server Configuration	120
Configuring the Syslog Settings	120
Syslog Servers	121
Adding a Syslog Server	122
Editing the Syslog Server	123
Enabling Syslog Servers	123
Disabling Syslog Servers	124
Deleting Syslog Servers	124
Audit Logs	125
Audit Data Generation	125
Start-Up of the Audit Functions	125
Shutdown of the Audit Functions	126
Administrative login and logout	126
Changes to TSF data related to configuration changes	126
Generating/import of, changing, or deleting of cryptographic keys	127
Resetting Passwords	128
Session Establishment with peer	128
Failure to Establish a TLS/HTTPS Session	129
Unsuccessful Login Attempts Limit is Met or Exceeded	129
All Use of Identification and Authentication Mechanism	130
Unsuccessful Attempt to Validate a Certificate	130
Any addition, replacement or removal of trust anchors in the TOE's trust store	132
Any attempt to initiate a manual update	132
All Management activities of TSF data	133
Ability to configure the session inactivity time before session termination or locking	134
Ability to configure the lifetime for IPsec SAs	135
All Management Activities of TSF Data (including creation, modification and deletion of firewall rules)	137
Discontinuous changes to time – either Administrator actuated or changed via an automated process	138
Initiation of update; result of the update attempt (success or failure)	138
The termination of a remote session by the session locking mechanism	139
The termination of an interactive session	139
The termination of a local session by the session locking mechanism	139
Initiation of the trusted channel	139
Termination of the trusted channel	140
Failure of the trusted channel functions	142
Initiation of the trusted path	142

Termination of the Trusted Path	142
Failure of the Trusted Path Functions	143
Application of Rules Configured with the Log Operation	143
Failure of Self-Test	143
All Administrative Actions	143
Start-up and shut-down of the IPS functions	144
All dissimilar IPS events/ reactions	145
Totals of similar events and reactions occurring within a specified time period	145
Modification of an IPS policy element	145
Inspected traffic matches an anomaly-based IPS policy	146
Inspected traffic matches a list of known-good or known-bad addresses applied to an IPS policy	146
Inspected traffic matches a signature-based IPS rule with logging enabled	146
Modification of which IPS policies are active on a TOE interface	147
Enabling a TOE interface with IPS policies applied	147
Disabling a TOE interface with IPS policies applied	147
Modification of which mode(s) is/are active on a TOE interface	147
Inspected traffic matches a signature-based IPS rule with logging enabled	148
Cryptographic Key Destruction	149
References	151
SonicWall Support	152
About This Document	153

Introduction

This document details the operational and preparative procedures for the Common Criteria evaluation. It highlights the specific SonicOS v7.0.1 configuration and administration functions and interfaces necessary to configure and maintain the devices in the evaluated configuration as defined in the Security Target (SonicWall SonicOS v7.0.1 with VPN and IPS on TZ, NSa, NSsp, and NSv Appliances Security Target).

This document does not mandate configuration settings for features of the TOE (Target of Evaluation) outside the evaluation scope. This document assumes that the administrator is a trusted individual.

Supported Platforms

The following tables describe the appliance hardware included in the evaluated configuration. The first describes the physical boundary components for the SonicOS 7.0.1 hardware models. The second describes the physical boundary components for the SonicOS 7.0.1 virtual appliances.

Appliance Series	Appliance Model	Operational Environment	Microarchitecture
TZ	TZ 670	Marvell CN9130	Quad Core Armv8 Cortex-A72
	TZ 570	Marvell CN9130	Quad Core Armv8 Cortex-A72
	TZ 570W	Marvell CN9130	Quad Core Armv8 Cortex-A72
	TZ 570P	Marvell CN9130	Quad Core Armv8 Cortex-A72
	TZ 470	Marvell 88F7040	Quad core Armv8 Cortex-A72
	TZ 470W	Marvell 88F7040	Quad core Armv8 Cortex-A72
	TZ 370	Marvell 88F7040	Quad core Armv8 Cortex-A72
	TZ 370W	Marvell 88F7040	Quad core Armv8 Cortex-A72
	TZ 270	Marvell 88F7040	Quad core Armv8 Cortex-A72
	TZ 270W	Marvell 88F7040	Quad core Armv8 Cortex-A72

Appliance Series	Appliance Model	Operational Environment	Microarchitecture
NSa	NSa 2700	Marvell CN9130	Quad Core Armv8 Cortex-A72
	NSa 3700	Marvell CN9130	Quad Core Armv8 Cortex-A72
	NSa 4700	Intel Xeon D-2123IT	Skylake
	NSa 5700	Intel Xeon D-2123IT	Skylake
	NSa 6700	Intel Xeon D-2123IT	Skylake
NSsp	NSsp 10700	Intel Xeon D-2166NT	Skylake
	NSsp 11700	Intel Xeon D-2166NT	Skylake
	NSsp 13700	Intel Xeon D-2187NT	Skylake

Appliance Series	Appliance Model	Operational Environment
NSv	NSv 270	ESXi 7.0 and 8.0 on Dell PowerEdge R640 (Running on Intel Xeon Silver 4208 (Cascade Lake))
	NSv 470	
	NSv 870	

Operational Environment

The following environmental components are required to operate the TOE (Target of Evaluation) in the evaluated configuration:

- **TOE:** Sonicwall SonicOS 7.0.1 running on a claimed physical appliance or a virtual appliance, typically deployed as a gateway between two networks, such as LAN and the internet.
- **Management workstation:** Any IT environment management workstation.
- **Remote Logging:** Audit Server supporting syslog protocol with an IPsec peer supporting IKEv2 and ESP.
- **Management Console:** Any computer that provides a supported browser to access administrative web GUI via HTTPS and direct serial connection providing administrative CLI access.
- **VPN Gateway:** VPN connections via IPsec.
- **WAN/Internet:** External IP interface.
- **LAN/Internal:** Internal IP interface.

Product Functionality Not Included in the Scope of the Evaluation

The following product functionality is not included in the Common Criteria evaluation:

- Although SonicWall SonicOS Enhanced supports several authentication mechanisms, the following mechanisms are excluded from the evaluated configuration:
 - Remote Authentication Dial-In User Service (RADIUS)
 - Lightweight Directory Access Protocol (LDAP)
 - Active Directory (AD)
 - eDirectory authentication
- Command Line Interface (CLI) (Secure Shell (SSH))
- Hardware Failover
- Real-time Blacklist (Simple Mail Transfer Protocol (SMTP))
- Global Security Client (including Group VPN)
- Global Management System
- SonicPoint
- Voice over IP (VoIP)
- Network Time Protocol (NTP)
- Antivirus
- Application Firewall

Initial Setup

The following describes how to set up the firewall or virtual appliance.

Secure Device Delivery

Delivery of Hardware Devices

The hardware devices are delivered via commercial couriers. The devices will contain packing slips with the serial numbers of all shipped devices. The receiver must verify that the hardware serial numbers match the serial numbers listed on the packing slip. The receiver must also verify that the external and internal packaging is not cut or damaged to access the device/s.

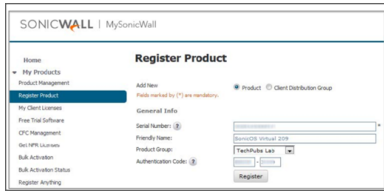
For any concerns about the integrity of the delivery, contact the supplier immediately.

Delivery of Virtual Firewalls

To access the virtual firewall OVA, you need to have a MySonicWall account. To setup a MySonicWall account, refer to [MySonicWall](#) and click on **Sign Up**. Follow the wizard to set up your account.

Refer to the purchase confirmation email for information about downloading the Ova files. To obtain the OVA from MySonicwall:

1. In a browser, log into your **MySonicWall** account.
2. Navigate to **My Products > Register Product**.
3. Fill in the **Serial Number**, **Friendly Name**, **Product Group**, and **Authentication Code** fields, and then click **Register**.



4. The Registration Code is displayed. Make a note of it. You are now given access to the OVA file for your NSv model.
5. Download the OVA file and save it to your management computer.

Product Registration

Before you register the appliance, you must have a mySonicWall account. Go to [MySonicWall](#) and click on **Sign Up**. Follow the wizard to set up your account.

Once the device is registered online, the local device extracts the registration information from MySonicWall once it has internet access through the WAN interface.

Connect and Power On

This section describes steps to power on the appliance and connect the LAN and WAN interface.

- Connect the provided power cord to the appliance and an electrical outlet (100-240 volts).
- The appliance powers on. The startup sequence takes about eight minutes.
- Connect the appliance LAN interface (X0 by default) to your local, internal network.
- Connect the appliance WAN interface (X1) to the Internet.

Initial Setup and Registration Using Local Management

Set up and manage your device by connecting it to a management computer via an Ethernet cable.

To minimize scrolling, set your screen resolution to at least 1920 x 1080 pixels.

To setup and register your device:

1. Configure your computer with a static IP address in the 192.168.1.x subnet, such as 192.168.1.100, and set the network mask to 255.255.255.0.
2. Using the provided Ethernet cable, connect the MGMT interface to your computer.

3. Navigate to <https://192.168.1.254> in your web browser and log in with the default credentials:

- Username: admin
- Password: password



4. Launch the Setup Guide wizard or manually configure the device to configure your WAN interface, change the admin password, and select other settings.

Enabling NDCPP Compliance

The following reviews the requirements for NDCPP compliance.

Enabling NDPP Mode

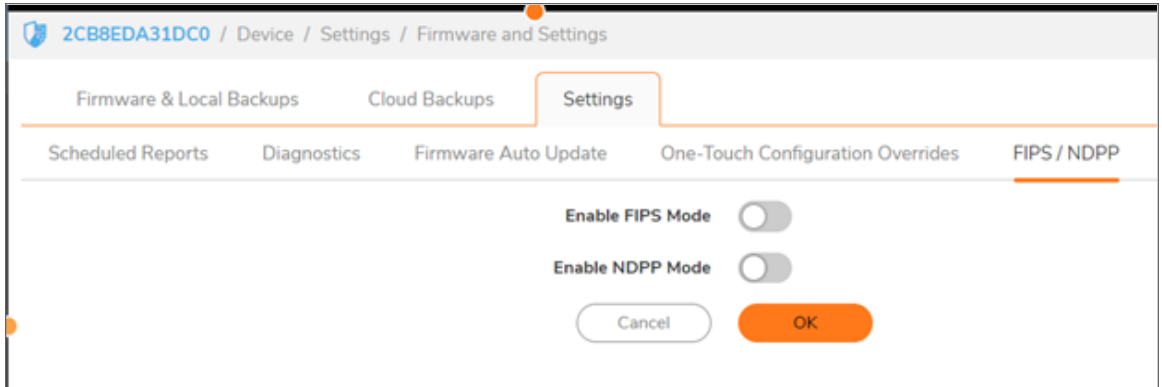
A SonicWall network security appliance can be enabled to be compliant with the Network Device Protection Profile (NDPP), but certain firewall configurations are either not allowed or are required.

The security objectives for a device that claims compliance with a Protection Profile are defined as follows: Compliant TOEs (Targets Of Evaluation) will provide security functionality that addresses threats to the TOE and implement policies that are imposed by law or regulation. The security functionality provided includes protected communications to and between elements of the TOE; administrative access to the TOE and its configuration capabilities; system monitoring for detection of security-relevant events; control of resource availability; and the ability to verify the source of updates to the TOE.

You enable NDPP by selecting the **Enable NDPP Mode** option on the **Device | Firmware and Setting** page. Once you do this, a popup message displays with the NDPP mode setting compliance checklist. The checklist displays every setting in your current SonicOS configuration that violates NDPP compliance so that you can change these settings. You need to navigate around the SonicOS management interface to make the changes. The checklist for an appliance with factory default settings is shown in the following procedure.

To enable NDPP and see a list of which of your current configurations are not allowed or are not present:

1. Navigate to the **Device | Firmware & Setting** page.
2. Click the **Settings** button. The **Settings** window displays.
3. Click **FIPS/NDPP**.



4. Click on **Enable NDPP Mode**. The NDPP MODE SETTING COMPLIANCE CHECKLIST appears with a list of required and not-allowed configurations. Note that the checklists are slightly different for each mode.

Classic Mode Checklist

NDPP MODE SETTING COMPLIANCE CHECKLIST

- The SonicWall can not be operated in NDPP mode without the above settings.
Please manually change or disable settings to be compliant with NDPP mode requirement at first.
- Admin or Users password can not be less than 15 characters.
- Minimum length of Admin or User password can not be less than 15.
- Enforced password complexity must contain letters, numbers and symbols.
- Enforced password complexity requirement must contain at least 1 upper case letter, 1 lower case letter, 1 numeric character, and 1 special character.
- New password must contain 8 characters different from the old password must be applied in NDPP mode.
- Admin password life time is required.
- Require users to relogin after password change.
- Must set session quota for each management IP.
- Must enable 'Drop and log network packets whose source or destination address is reserved by RFC' in Advanced Firewall Settings.
- Must set session quota for each IPv6 management IP.
- HTTPS Certificate is self signed.
- SSLVPN Certificate is self signed.
- Required to enable NDPP enforcement for Syslog Server.
- IKEv2 Dynamic Client Proposal in VPN advanced settings requires DH Group 14, 19, 20 or 21 in NDPP Mode.
- Must configure at least one Syslog Server.
- Must enable 'Start With Policy Banner Before Login Window' in User Settings.
- Must enable 'Enforce TLS 1.1 and Above' in Administration page.
- SonicOS API digest MD5 can not be enabled in NDPP mode
- SonicOS API CHAP authentication can not be enabled in NDPP mode
- SonicOS API RSA1024 can not be accepted in NDPP mode for public key authentication
- Must enable 'Enable TCP handshake enforcement' in TCP Settings.
- Must enable 'Enforce strict TCP compliance with RFC 793 and RFC 1122' in TCP Settings.

Policy Mode Checklist

NDPP MODE SETTING COMPLIANCE CHECKLIST

- i** The SonicWall can not be operated in NDPP mode without the above settings.
Please manually change or disable settings to be compliant with NDPP mode requirement at first.
- Admin or Users password can not be less than 15 characters.
 - Minimum length of Admin or User password can not be less than 15.
 - Enforced password complexity must contain letters, numbers and symbols.
 - Enforced password complexity requirement must contain at least 1 upper case letter, 1 lower case letter, 1 numeric character, and 1 special character.
 - New password must contain 8 characters different from the old password must be applied in NDPP mode.
 - Admin password life time is required.
 - Require users to relogin after password change.
 - Must create session quota DOS policy for management IPs. Please set connection limitation of management policies in diag page.
 - Must enable 'Drop and log network packets whose source or destination address is reserved by RFC' in Advanced Firewall Settings.
 - HTTPS Certificate is self signed.
 - SSLVPN Certificate is self signed.
 - Required to enable NDPP enforcement for Syslog Server.
 - IKEv2 Dynamic Client Proposal in VPN advanced settings requires DH Group 14, 19, 20 or 21 in NDPP Mode.
 - Must configure at least one Syslog Server.
 - Must enable 'Start With Policy Banner Before Login Window' in User Settings.
 - Must enable 'Enforce TLS 1.1 and Above' in Administration page.
 - SonicOS API digest MD5 can not be enabled in NDPP mode
 - SonicOS API CHAP authentication can not be enabled in NDPP mode
 - SonicOS API RSA1024 can not be accepted in NDPP mode for public key authentication
 - Must enable 'Enable TCP handshake enforcement' in TCP Settings.
 - Must enable 'Enforce strict TCP compliance with RFC 793 and RFC 1122' in TCP Settings.

- If the SonicWall appliance does not comply with the checklist, manually change or disable settings to be compliant with the NDPP mode requirement.
- If the SonicWall appliance complies with the checklist, click **OK**.

Leave the checklist dialog open while you make the configuration changes. If you click OK before all required changes are complete, the Enable NDPP Mode option is cleared automatically upon closing the checklist dialog. Select the option again to see what configuration changes are still needed for NDPP compliance.

Once NDPP compliance is enabled, the following settings will be applied by default without any additional configuration changes.

- Appliance provides AES encryption/decryption in CBC mode with 128-bit, 192-bit, and 256-bit keys and in GCM mode with 128-bit and 256-bit keys.
- Appliance supports signature generation and verification for RSA (4096 bits) and ECDSA (P-256, P-384, P-521), in accordance with FIPS PUB 186-4.
 - RSA and ECDSA are used in IKE authentication.
 - RSA is called to verify signatures on firmware uploads for the NSsp 15700 or the NSv Series. For the NSsp 15700 or the NSv Series the NDPP mode does not need to be enabled. It is enabled by default.
 - ECDSA is used to verify the signature on firmware updates for the TZ Series, NSa Series firewalls as well as the NSsp 10700, NSsp 11700, and NSsp 13700.
- It provides cryptographic hashing services for key generation using SHA-256 as specified in NIST SP 800-90 DRBG.
 - SHA-1 and SHA-256 are used in support of TLS.
 - SHA-256, SHA-384, and SHA-512 are used in support of IPsec.
 - SHA-256 is used with ECDSA for the verification of firmware.
 - ① **NOTE:** NSsp 15700 or the NSv Series uses SHA256+RSA2048. These options are enabled by default.
 - Appliance implements HMAC message authentication. HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 are supported with cryptographic key sizes of 160, 256, 384, and 512 bits and message digest sizes of 160, 256, 384, and 512 bits.
 - The appliance implements a DRBG in accordance with ISO/IEC 18031:2011, using Hash_DRBG.
- Once NDPP compliance is enabled, the following packets are discarded and logged by default, without any additional configuration changes or access rules:
 - Packets which are invalid fragments
 - Fragmented packets which cannot be re-assembled completely
 - Packets where the source address of the network packet is defined as being on a broadcast network
 - Packets where the source address of the network packet is defined as being on a multicast network
 - Network packets where the source address of the network packet is defined as being a loopback address
 - Network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address reserved for future use (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4
 - Network packets where the source or destination address of the network packet is defined as an unspecified address or an address reserved for future definition and use (i.e. unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6
 - Network packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified and no other rules

- Packets where the source address of the network packet is equal to the address of the network interface where the network packet was received
- Packets where the source or destination address of the network packet is a link-local address
- Packets where the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received

① **IMPORTANT:** For Common Criteria evaluated configuration, FIPS Mode option cannot be enabled together with NDPP Mode. Enabling FIPS Mode together with the NDPP Mode will enable certain algorithms that are not permitted in Common Criteria.

Enabling FIPS Mode

When operating in FIPS (Federal Information Processing Standard) Mode, the SonicWall security appliances support FIPS 140-2 Compliant security. Among the FIPS-compliant features of the son include PRNG-based on SHA-1 and support of only FIPS-approved algorithms (DES, 3DES, and AES with SHA-1).

To enable FIPs and see a list of which of your current configurations are not allowed or are not present:

Classic mode from factory defaults:

FIPS Mode Setting Verification

| FIPS MODE SETTING COMPLIANCE CHECKLIST

● The SonicWall can not be operated in FIPS mode without the above settings.
Please manually change or disable settings to be compliant with FIPS mode requirement at first.

- Only support IKE DH Group 14, 19, 20, 21 in FIPS mode
- Only support AES CBC for IKE Phase 1/2 Encryption in FIPS mode
- Only SHA-256 Authentication or higher is allowed in FIPS mode
- IKEv2 Dynamic Client Proposal in VPN advanced settings requires DH Group 14, 19, 20, 21
- Advanced Routing Service is not allowed in FIPS mode
- SonicOS API digest MD5 can not be enabled in FIPS mode
- SonicOS API CHAP authentication can not be enabled in FIPS mode
- SonicOS API RSA1024 can not be accepted in FIPS mode for public key authentication
- Must enable 'Enforce TLS 1.1 and Above' in Administration page.

Policy Mode from factory defaults:

FIPS Mode Setting Verification

FIPS MODE SETTING COMPLIANCE CHECKLIST

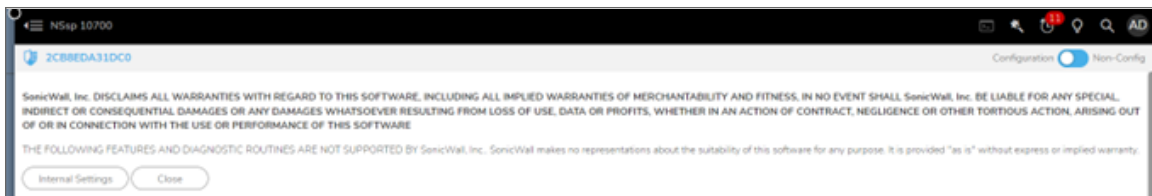
- i** The SonicWall can not be operated in FIPS mode without the above settings.
Please manually change or disable settings to be compliant with FIPS mode requirement at first.
- Only support IKE DH Group 14, 19, 20, 21 in FIPS mode
 - Only support AES CBC for IKE Phase 1/2 Encryption in FIPS mode
 - Only SHA-256 Authentication or higher is allowed in FIPS mode
 - IKEv2 Dynamic Client Proposal in VPN advanced settings requires DH Group 14, 19, 20, 21
 - Advanced Routing Service is not allowed in FIPS mode
 - SonicOS API digest MD5 can not be enabled in FIPS mode
 - SonicOS API CHAP authentication can not be enabled in FIPS mode
 - SonicOS API RSA1024 can not be accepted in FIPS mode for public key authentication

i **NOTE:** The Enable FIPS Mode option cannot be enabled at the same time as the **Enable NDPP Mode** option, which is also on the **Firmware and Settings > Settings** dialog.

Internal Settings

This section describes how to access the Internal settings of the SonicWall firewall.

1. The **Diag** page can be reached by typing in the LAN IP/Mgmt IP of the SonicWall in the browser, with IP/sonicui/7/m/diag at the end.
EXAMPLE: 192.168.168.168/sonicui/7/m/diag
2. Click on Internal settings to access the internal settings page or diag page.



Startup and Self-Test

During system start-up, SonicOS performs several self-tests, these self-tests include:

- CPU test of the following (MMU, Memory, I/O ports, Interrupts, Timers)
- RAM memory corruption test
- Firmware integrity test
- AES-CBC Encrypt and Decrypt Known Answer Tests
- AES-GCM
- 3DES (supported in non-FIPS mode)
- SHA-1, -256, -384, -512 Known Answer Tests
- HMAC-SHA-1, -256, -512 Known Answer Tests
- DSA Signature Verification Pairwise Consistency Test
- RSA Sign and Verify Known Answer Tests
- DH Pairwise Consistency Test (including FFC, ECC and KAT tests)
- DRBG Known Answer Test
- ECDSA Known Answer Test
- ECDSA Signature and Verification Known Answer Tests (including SSH, IKEv2, IKEv1, TLS, SNMP, and KAT tests)

If any of these tests fail, the product enters a hard error state, and the local console provides an error message reflecting information about the specific failure to the security administrator. Rebooting the product generally clears the errors; however, if errors persist, contact [SonicWall Technical Support](#).

Deployment Modes

The product supports multiple modes of operation. The following sections describe each.

IPS Sniffer Mode

Supported on SonicWall security appliances, IPS Sniffer Mode is a variation of Layer 2 Bridged Mode that is used for intrusion detection. IPS Sniffer Mode configuration allows an interface on the appliance to be connected to a mirrored port on a switch to examine network traffic. Typically, this configuration is used with a switch inside the main gateway to monitor traffic on the intranet.

Configure IPS Sniffer mode in SonicOS

Choose an interface to act as the Primary Bridge Interface. In this example, the X4 interface (WAN) is used.

You may also optionally navigate to the **VLAN Filtering** tab to control VLAN traffic through the L2 bridge. By default, all VLANs are allowed.

To configure the Primary Bridge Interface:

1. Login to your SonicWall management page and click the **Network** option at the top of the page.
2. Navigate to the **System > Interfaces** page.
3. Click the **Configure** button of the X4 interface.

4. Set the following:

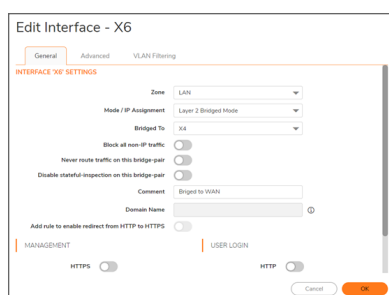
- **Zone:** WAN
 - **IP Assignment:** Static
 - **IP Address:** 10.1.4.117 (in this example the 10.1.4.0/24 subnet was configured)
 - Configure **Subnet Mask**, **Default Gateway**, **DNS Server 1**, **DNS Server 2**, and **DNS Server 3**.
5. Enable or disable Management & User login of new zone based on your requirement.
 6. Click **OK**.

① | **NOTE:** The Primary Bridge Interface must have a static IP address.

Choose an interface to act as the Secondary Bridge Interface. In this example, the X6 (automatically assigned to the LAN) interface was used.

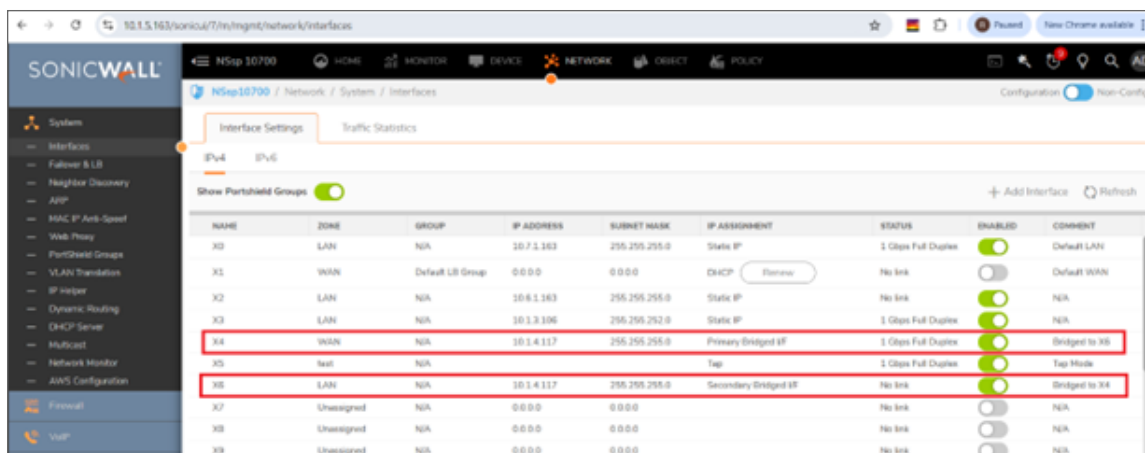
To configure the Secondary Bridge Interface:

1. Login to your SonicWall management page, and click the **Network** option at the top of the page.
2. Navigate to the **System > Interfaces** page.
3. Click the **Configure** button of the X0 interface.



4. Set the following:
 - **Zone:** LAN
 - **Mode/IP Assignment:** Layer 2 Bridge Mode (IP Route Option)
 - **Bridged to:**X4
5. Enable Management & User login if you want to manage it.
6. Click **OK**.
7. You may optionally enable the **Block all non-IPv4 traffic** setting to prevent the L2 bridge from passing non-IPv4 traffic (VLAN Filtering on SonicWall NSA series appliances).
8. Select **Block listed VLANs** (blacklist) from the drop-down list and move the VLANs you wish to block from the left pane to the right pane. All VLANs added to the right pane will be blocked, and all VLANs remaining in the left pane will be allowed.
9. Select **Allow listed VLANs** (whitelist) from the drop-down list and move the VLANs you wish to explicitly allow from the left pane to the right pane. All VLANs added to the right pane will be allowed, and all VLANs remaining in the left pane will be blocked.

The **Network | System > Interfaces** page displays the updated configuration: You may now apply security services to the appropriate zones, as desired. In this example, they should be applied to the LAN, WAN, or both zones.



Wire Mode

Wire Mode is a simplified form of Layer 2 Bridged Mode, and is configured as a pair of interfaces. In Wire Mode, the destination zone is the Paired Interface Zone. Access rules are applied to the Wire Mode pair based on the direction of traffic between the source Zone and its Paired Interface Zone. For example, if the source Zone is WAN and the Paired Interface LAN Zone is LAN, then WAN to LAN and LAN to WAN rules are applied, depending on the direction of the traffic.

In Wire Mode, you can enable Link State Propagation, which propagates the link status of an interface to its paired interface. If an interface goes down, its paired interface is forced down to mirror the link status of the first interface. Both interfaces in a Wire Mode pair always have the same link status.

In Wire Mode, you can Disable Stateful Inspection. When Disable Stateful Inspection is selected, Stateful Packet Inspection is turned off. When Disable Stateful Inspection is not selected, new connections can be established without enforcing a 3-way TCP handshake. Disable Stateful Inspection must be selected if asymmetrical routes are deployed.

Configuring Wire Mode in SonicOS

Wire Mode is a deployment option where the SonicWall appliance can be deployed as a Bump in the Wire. It provides a least-intrusive way to deploy the appliance in a network.

Wire Mode is very well suited for deploying behind a pre-existing Stateful Packet Inspection (SPI) Firewall. Wire Mode is a simplified form of Layer 2 Bridge Mode. A Wire Mode interface does not take any IP address and it is typically configured as a bridge between a pair of interfaces. None of the packets received on a Wire Mode interface are destined to the firewall, but are only bridged to the other interface.

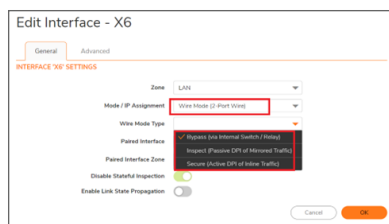
Wire Mode operates in one of 4 different modes:

- **Bypass Mode** allows for the quick and relatively non-interruptive introduction of firewall hardware into a network. Upon selecting a point of insertion into a network (for example, between a core switch and a perimeter firewall, in front of a VM server farm, or at a transition point between data classification domains), the firewall is inserted into the physical data path, requiring a very short maintenance window. One or more pairs of switch ports on the firewall are used to forward all packets across segments at full line rates, with all the packets remaining on the firewall's 112 Gbps switch fabric rather than getting passed up to the multi-core inspection and enforcement path. While Bypass Mode does not offer any inspection or firewalling, this mode allows the administrator to physically introduce the firewall into the network with a minimum of downtime and risk, and to obtain a level of comfort with the newly inserted component of the networking and security infrastructure. The administrator can then transition from Bypass Mode to Inspect or Secure Mode instantaneously through a simple user-interface driven reconfiguration.
- **Inspect Mode** extends Bypass Mode without functionally altering the low-risk, zero latency packet path. Packets continue to pass through the firewall's switch fabric, but they are also mirrored to the multi-core RF-DPI engine for the purposes of passive inspection, classification, and flow reporting. This reveals the firewall's Application Intelligence and threat detection capabilities without any actual intermediate processing.
- **Secure Mode** is the progression of Inspect Mode, actively interposing the firewall's multi-core processors into the packet processing path. This unleashes the inspection and policy engines' full-set of capabilities, including Application Intelligence and Control, Intrusion Prevention Services, Gateway and Cloud-based Anti-Virus, Anti-Spyware, and Content Filtering. Secure Mode affords the same level of visibility and enforcement as conventional NAT or L2 Bridged Mode deployments, but without any L3/L4 transformations, and with no alterations of ARP or routing behavior. Secure Mode thus provides an incrementally attainable NGFW deployment requiring no logical and only minimal physical changes to existing network designs.

① **NOTE:** When operating in Wire Mode, the firewall's dedicated Management interface is used for local management. To enable remote management and dynamic security services and application intelligence updates, a WAN interface (separate from the Wire Mode interfaces) must be configured for Internet connectivity. This is easily done given that SonicOS supports interfaces in mixed-modes of almost any combination.

To configure an interface for Wire Mode:

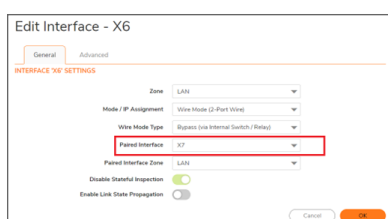
1. On the **Network | System > Interfaces** page, click the **Configure** button for the interface you want to configure for Wire Mode.



2. In the **Zone** drop-down menu, select any zone type except **WLAN**.

3. To configure the interface for Wire Mode, in the **Mode / IP Assignment** drop-down menu, select **Wire Mode (2-Port Wire)**.
4. In the **Wire Mode Type** drop-down menu, select the appropriate mode:
 - **Bypass (via Internal Switch/Relay)**
 - **Inspect (Passive DPI of Mirrored Traffic)**
 - **Secure (Active DPI of Inline Traffic)**
5. In the **Paired Interface** drop-down menu, select the interface that connects to the upstream firewall. The paired interfaces must be of the same type (two 1 GB interfaces or two 10 GB interfaces).

① **NOTE:** Only unassigned interfaces are available in the **Paired Interface** drop-down menu. To make an interface unassigned, click on the **Configure** button for it, and in the **Zone** drop-down menu, select **Unassigned**.



6. Click **OK**.

Bypass Mode

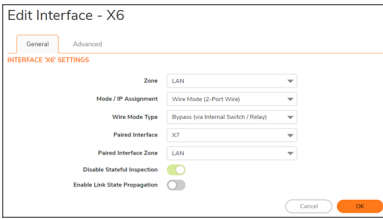
Bypass Mode can be configured between a pair of interfaces. All traffic received is bridged to the paired interface. While Bypass Mode does not offer any inspection or firewalling, this mode allows the administrator to physically introduce the firewall into the network with a minimum of downtime and risk, and to obtain a level of comfort with the newly inserted component of the networking and security infrastructure.

To configure for Bypass Mode:

1. Log in to the SonicWall management interface.
2. Navigate to the **Network | System > Interfaces** page.
3. Click on **Configure** on any one interface.
4. In the **Zone** field, choose **LAN**.
5. Set **Mode / IP Assignment** to **Wire Mode (2-Port Wire)**.
6. Set **Wire Mode Type** to **Bypass Mode (via Internal Switch / Relay)**.
7. Choose an unassigned interface under **Paired Interface**.

① **NOTE:** The paired Interfaces must be of the same type. For example two 1 GB interfaces or two 10 GB interfaces.

In the screenshot below, X6 Interface has been configured in Bypass Mode and paired with X7 Interface.



Secure Mode

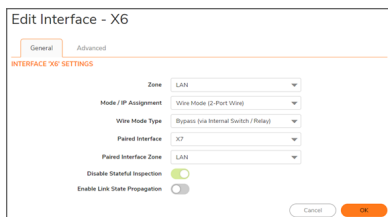
Secure Mode is the progression of Inspect Mode, actively applying SonicWall Application Intelligence and Control, Intrusion Prevention Service, Gateway and Cloud-based Anti-Virus, Anti-Spyware and Content Filtering. Secure Mode affords the same level of visibility and enforcement as conventional NAT or L2 Bridge mode deployments, but without any L3/L4 transformations, and with no alterations of ARP or routing behavior. Secure Mode requires no logical, and only minimal physical, changes to existing network designs.

Secure Mode can be configured between a pair of interfaces. All traffic received is fully processed by the firewall. There is full application visualization and control in Secure Mode.

To configure for Secure Mode:

1. Log in to the SonicWall management interface.
 2. Navigate to the **Network | System > Interfaces** page.
 3. Click on **Configure** on any one interface.
 4. In the **Zone** field, choose **LAN**.
 5. Set **Mode / IP Assignment** to **Wire Mode (2-Port Wire)**.
 6. Set **Wire Mode Type** to **Secure (Active DPI of Inline Traffic)**.
 7. Choose an unassigned interface under **Paired Interface**.
- ① **NOTE:** The paired Interfaces must be of the same type. For example two 1 GB interfaces or two 10 GB interfaces.

In the screenshot below, X6 Interface has been configured in SecureMode and paired with X7 Interface.



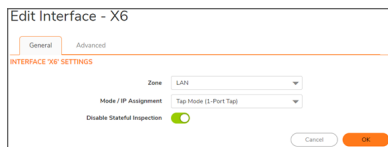
Tap Mode

Tap Mode can be configured for a single interface. All traffic received is never sent out of the firewall, but the firewall performs full SPI and DPI processing. There is full application visualization, but no application control in Tap Mode. Typically, a mirror port is set up on the switch to mirror the network traffic to the firewall. Tap Mode provides the same visibility as Inspect Mode but differs from the latter in that it ingests a mirrored packet stream via a single switch port on the SonicWall eliminating the need for physically intermediated insertion. Tap Mode is designed for use in environments employing network taps, smart taps, port mirrors, or SPAN ports to deliver packets to external devices for inspection or collection. Like all other forms of Wire Mode, Tap Mode can operate on multiple concurrent port instances, supporting discrete streams from multiple taps.

To configure TAP Mode:

1. Log in to the SonicWall management interface.
2. Navigate to the **Network | System > Interfaces** page.
3. Click on **Configure** on any one interface.
4. In the **Zone** field, choose **LAN**.
5. Set **Mode / IP Assignment** to **Tap Mode (1-Port Tap)**.

In the screenshot below, X6 Interface has been configured for Tap Mode.



Management Mode

Each appliance includes a distinct and dedicated MGMT port. When using this port, you are in management mode.

Configure Management Mode in SonicOS

To configure Management Mode in SonicOS:

1. Log in to the SonicWall management interface.
2. Navigate to the **Network | System > Interfaces** page.
3. Click on **Configure** on the **MGMT** interface.
4. In the **Zone** field, choose **MGMT**.
5. Set **Mode / IP Assignment** to **Static IP Mode**.
6. Assign the **IP Address**, **Subnet Mask**, and **Default Gateway (Optional)**.

The screenshot below shows the MGMT interface configured.

General | Advanced

INTERFACE MGMT SETTINGS

Zone	MGMT
Mode / IP Assignment	Static IP Mode
IP Address	10.1.5.183
Subnet Mask	255.255.255.0
Default Gateway (Optional)	10.1.5.1
Comment	Default MGMT
Domain Name	

For NSv devices, an interface has to be configured in the management zone for it to be distinctly identified as the management interface.

Zones and Interfaces

Topics:

- Zones in SonicWall
- Predrined Zones in SonicOS
- Adding and Configuring a Zone
- Deleting a Zone
- Configuring Interfaces

Zones in SonicWall

Zones in SonicWall is logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. Security zones provide an additional, more flexible, layer of security for the firewall. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface.

Zones allows users to apply security policies to the inside of the network. This allows the administrator to do this by organizing network resources to different zones, and allowing or restricting traffic between those zones. This way, access to critical internal resources such as payroll servers or engineering code servers can be strictly controlled.

Zones also allow full exposure of the NAT table to allow the administrator control over the traffic across the interfaces by controlling the source and destination addresses as traffic crosses from one zone to another. This means that NAT can be applied internally, or across VPN tunnels, which is a feature that users have long requested. SonicWall security appliances can also drive VPN traffic through the NAT policy and zone policy, since VPNs are now logically grouped into their own VPN zone.

Predefined Zones in SonicOS

The predefined zones on the SonicWall security appliance depend on the device and are not modifiable. These are defined as follows:

- WAN: This zone can consist of either one or two interfaces. If you're using the security appliance's WAN Failover capability, you need to add the second Internet interface to the WAN zone.
- LAN: This zone can consist of one to five interfaces, depending on your network design. Even though each interface will have a different network subnet attached to it, when grouped together they can be managed as a single entity.
- DMZ: This zone is normally used for publicly accessible servers. This zone can consist of one to four interfaces, depending on your network design.
- VPN: This virtual zone is used for simplifying secure, remote connectivity. It is the only zone that does not have an assigned physical interface.
- MULTICAST: This zone provides support for IP multicasting, which is a method for sending IN packets from a single source simultaneously to multiple hosts.
- WLAN: This zone provides support to SonicWall access points (SonicPoint or SonicWave). When assigned to the Opt port, it enforces SonicPoint Enforcement, automatically dropping all packets received from non-SonicPoint devices. The WLAN zone supports SonicPoint Discovery Protocol (SDP) to automatically poll for and identify attached SonicPoint access points. It also supports SonicWall Simple Provisioning Protocol to configure a SonicPoint using profiles.
- SSLVPN: This virtual zone is used for simplifying secure, remote connectivity with SSL encryption. This zone is assigned to the SSLVPN traffic only.

Apart from predefined zones, custom, user-friendly zones can also be configured in SonicOS, with different security types.

① **NOTE:** In the SonicWall NSA series, **MGMT** is a predefined zone for management, so in SonicWall TZ series, we cannot create a custom zone named **MGMT**.

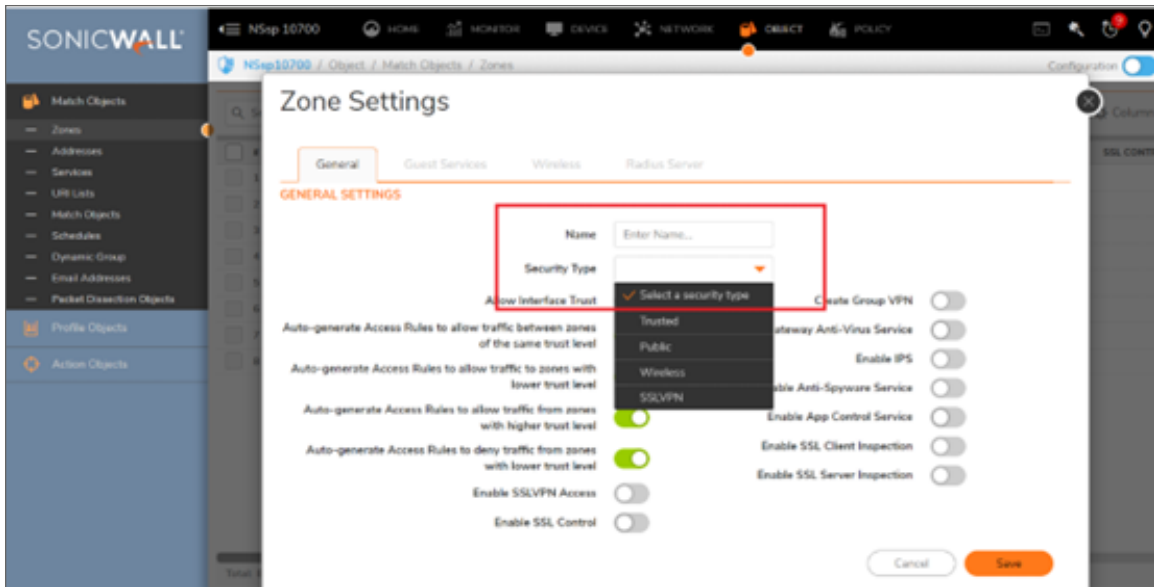
Adding and Configuring a Zone

To add a new zone:

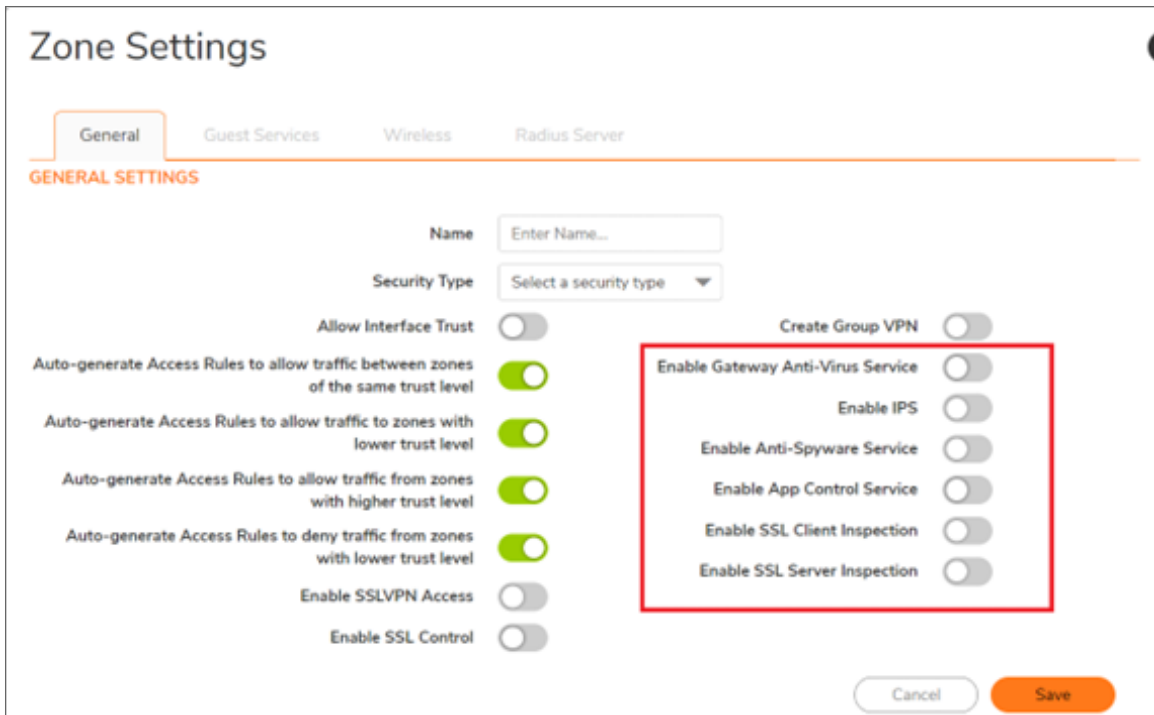
1. Click the **Objects** option in the top menu.
2. Navigate to **Match Objects > Zones** and click **Add Zone**.



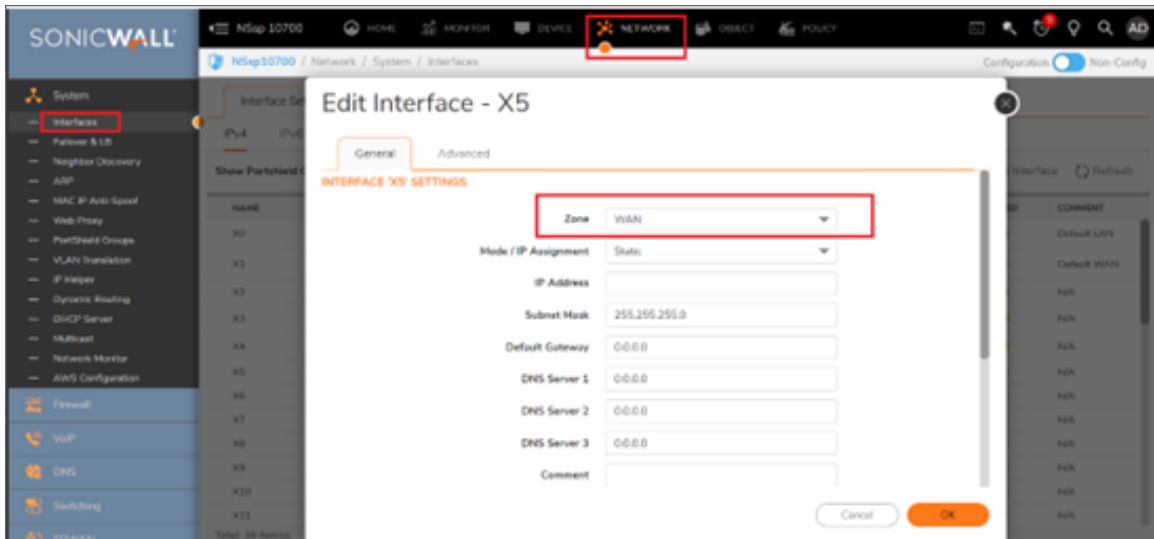
3. Select the appropriate security type for the zone.



4. Apply the required security services on the custom zones.

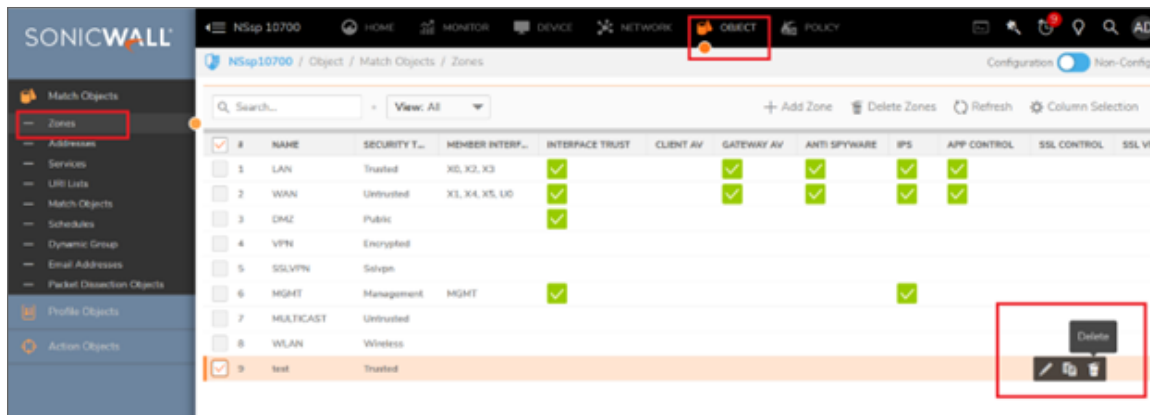


5. Bind the newly created custom zone to a physical interfaces to allow for configuration of Access Rules to govern inbound and outbound traffic. If there is no interface, traffic cannot access the zone or exit the zone.
6. Navigate to **Network | Interface > Edit** and find the interface to which you would like to bind this zone.



Deleting a Zone

You can delete a custom zone by clicking the delete icon under **Objects | Match Objects > Zones**.



① | **NOTE:** Pre-defined zones can't be deleted.

Configuring Interfaces

The number of physical interfaces vary on each of them, depending upon the model of firewall. Each interface is configurable with various IP assignments depending upon the zone type:

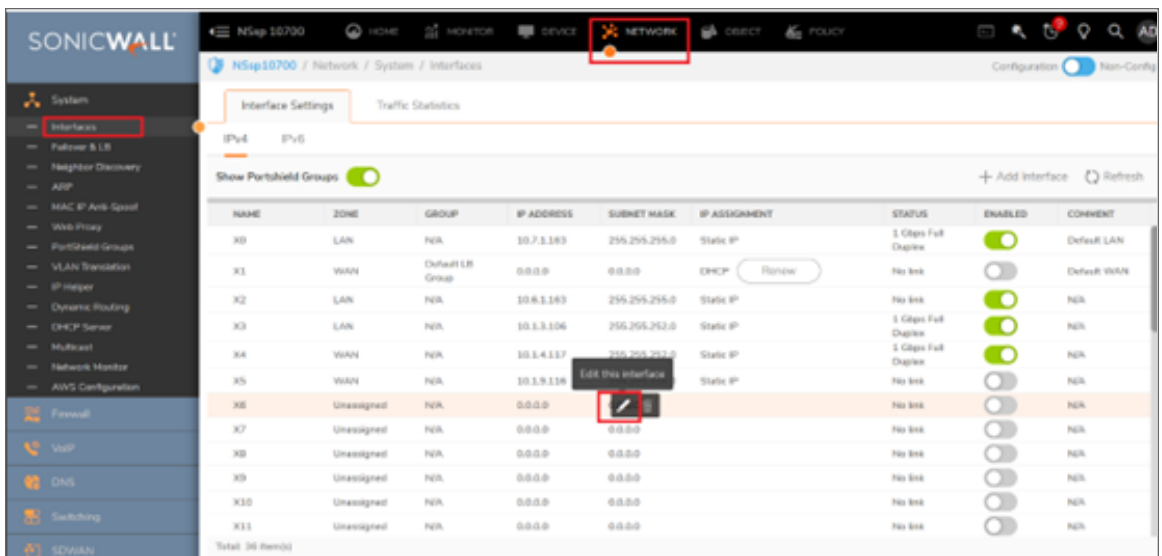
- LAN: Static IP Mode (default), Transparent IP Mode (Splice L3 Subnet), Layer 2 Bridged Mode (IP Route Option), Wire Mode (2-Port Wire), Tap Mode (1-Port Tap), IP Unnumbered, PortShield Switch Mode,

NativeBridge Mode

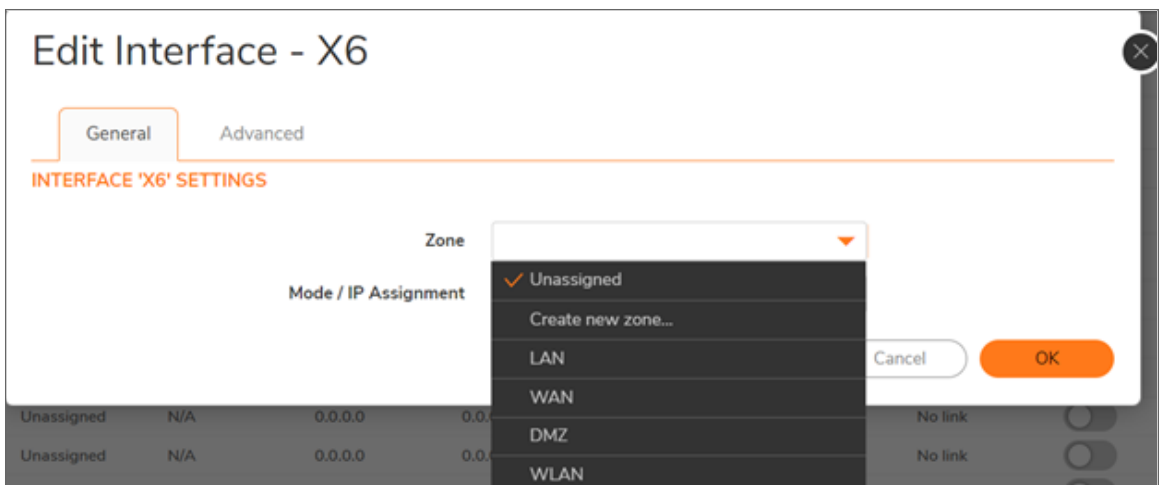
- WAN: Static (default), DHCP, PPPoE, PPTP, L2TP, Wire Mode, (2-Port Wire), Tap Mode (1-Port Tap)
- DMZ: Static IP Mode (default), Transparent IP Mode (Splice L3 Subnet), Layer 2 Bridged Mode (IP Route Option), Wire Mode (2-Port Wire), Tap Mode (1-Port Tap), IP Unnumbered, PortShield Switch Mode, NativeBridge Mode
- WLAN: Static IP Mode (default), PortShield Switch Mode, Layer 2 Bridged Mode, NativeBridge Mode

To configure a physical interface with a static IP Mode:

1. Navigate to **Network | System > Interfaces**.
2. In the **Interface Settings** table, place the cursor on the interface you want to edit, and when the icons appear, select **Edit this interface**.

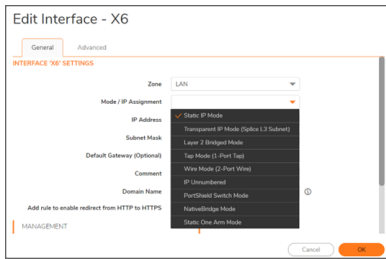


3. In the Zone field, select a zone to assign to the interface: **LAN**, **WAN**, **DMZ**, **WLAN**, or any custom zone you've created.

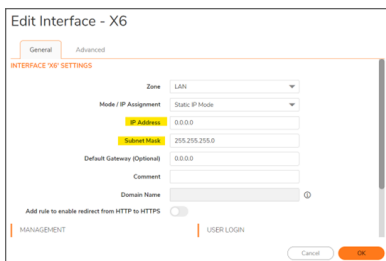


NOTE: You can create new zone as well.

- From the **Mode / IP Assignment** field, select **Static (default for WAN)** or **Static IP Mode (default for LAN)**.



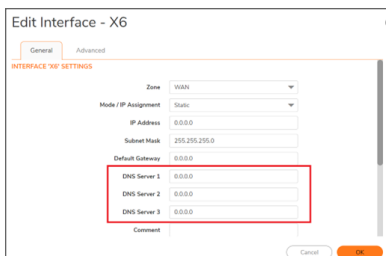
- Enter the IP address and subnet mask for the interface their respective fields.



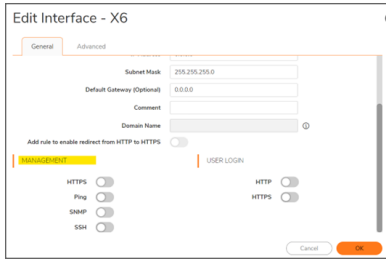
- If configuring a WAN zone interface or the MGMT interface, enter the IP address of the gateway device in the **Default Gateway** field. If configuring a LAN zone interface or a DMZ zone interface, optionally enter the IP address of the gateway device in the **Default Gateway (Optional)** field.

NOTE: You cannot enter an IP address that is in the same subnet as another zone.

- For a WAN zone interface, enter the IP addresses of up to three DNS servers into the **DNS Server** fields.



- Enter any optional comment text in the **Comment** field.
- If you want to enable remote management of the security appliance from this interface, enable the supported Management protocols: **HTTPS**, **Ping**, **SNMP**, or **SSH**.



10. If you want to allow selected users with limited management rights to log in to the security appliance, enable **HTTP** and **HTTPS** in the **User Login** section.

Product Administration

Configure the following parameters to help with product administration. Only authorized administrators can update and modify product functions.

Managing through HTTP/HTTPS

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

To manage through HTTP or HTTPS:

1. Navigate to **Device | Settings > Administration**.
2. Click **Management**.
3. To enable HTTP management globally, select **Allow management via HTTP** in the **WEB MANAGEMENT SETTINGS** section. This option is not selected by default.
 - The default port for HTTP is port 80, but you can configure access through another port. Enter the number of the desired port in the HTTP Port field.
 - ① **IMPORTANT:** If you configure another port for HTTP management, you must include the port number when you use the IP address to log into the SonicWall Security Appliance. For example, if you configure the port to be 76, then you must type LAN IP Address:76 into the Web browser, for example, `http://192.18.16.1:76`.
 - The default port for HTTPS management is 443. To add another layer of security for logging into the SonicWall Security Appliance, change the default port, and enter the preferred port number into the HTTPS Port field.
 - ① **IMPORTANT:** If you configure another port for HTTPS management Port, you must include the port number when you use the IP address to log into the SonicWall Security Appliance. For example, if you use 700 for the port, then you must log in using the port number as well as the IP address; for example, `https://192.18.16.1:700`.

The appliance operates as a TLS server for the web GUI trusted path.

- The server only allows TLS protocol version 1.2 and rejects all other protocol version, including SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1 and any other unknown TLS version string supplied.
- The TLS server is restricted to the following cipher suites:
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- To configure supported cipher suites no other configuration is required other than enabling NDCPP mode refer Enabling NDCPP Compliance.
- To enforce TLS, NDCPP requires only TLS 1.2. By default, the appliance rejects SSL 2.0 and SSL 3.0.
- The appliance does not support DHE cipher suite. For ECDSA key agreement schemes, the key agreement parameters are by default restricted by default to secp256r1, secp384r1, and secp521r1 curves; no other configuration is required once NDPP mode is enabled.
- By default, the TLS server supports session resumption based on session tickets and session IDs. No additional configuration is required once NDPP mode id enabled.

Managing through the Local Console

SonicWall console data can be useful to obtain vital information helpful for troubleshooting purposes.

To access the local console of hardware appliances:

1. Attach the included null modem cable to the appliance port marked **CONSOLE**. Attach the other end of the null modem cable to a serial port on the configuring computer.
2. Launch the terminal application and select the **COM** port.
3. Use the following settings to communicate with the serial port connected to the appliance:
 - 115,200 baud
 - 8 data bits
 - No parity

- 1 stop bit
 - No flow control
4. Press **Enter** to display the **DEVICE NAME>** prompt.
 5. At the **User:** prompt enter the administrator's username.
 - ① | **NOTE:** Only the administrator will be able to log in from the CLI. The default administrator's username is **admin**. The default username can be changed.
 6. At the **Password:** prompt, enter the administrator's password.
 - ① | **NOTE:** If an invalid or mismatched username or password is entered, the CLI prompt returns to **User:**, and an error message is logged: **CLI administrator login denied due to bad credentials**.

To access the local console of virtual appliances:

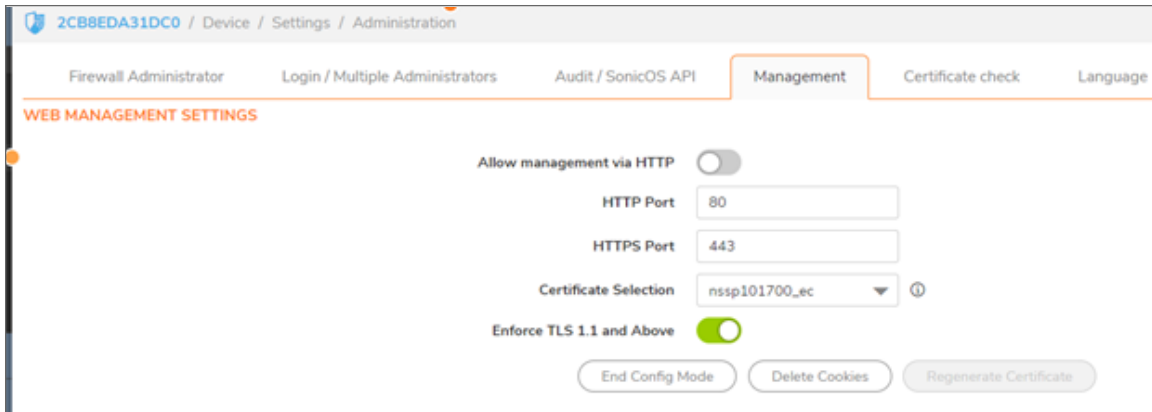
1. Once the virtual appliance is installed on the ESXi, we can use the ESXi IP to take the console access.
2. Take the access to the ESXi server from browser.
3. Navigate to virtual machines and click on the appliance name. The appliance console displays.
4. Press **Enter** to display the **DEVICE NAME>** prompt.
5. At the **User:** prompt enter the administrator's username. Only the administrator can log in from the CLI. The default administrator's username is **admin**. The default username can be changed.
6. At the **Password:** prompt, enter the administrator's password.
If an invalid or mismatched username or password is entered, the CLI prompt returns to **User:**, and an error message is logged: **CLI administrator login denied due to bad credentials**.

Selecting a Security Certificate

Security certificates provide data encryption and a secure website.

To specify the type of security certificate:

1. Navigate to **Device | Settings > Administration**.
2. Click **Management**.
3. From **Certificate Selection** drop-down list, select the type of certificate for your website:



- Using **Self-signed Certificate** allows you to continue using a certificate without downloading a new one each time you log into the SonicWall Security Appliance. This option is selected by default.
 - Use **Import Certificate** to select an imported certificate from the **Device | Settings > Certificates** page to use for authentication to the management interface. A confirmation message displays.
4. Click **OK**. The **Device | Settings > Certificates** page displays.
 5. In the **Certificate Common Name** field, enter the IP address or common name for the firewall. If you choose **Use Selfsigned Certificate**, SonicOS populates the field with the firewall's IP address.
 6. Click **Accept**.

To regenerate a Self-Signed Certificate::

1. Navigate to **Device | System > Administration > Management**.
2. In the **WEB MANAGEMENT SETTINGS** section, click **Regenerate Certificate**.
3. Click **OK** in the confirmation message that displays.

Enforcing TLS Version

SonicOS supports versions 1.0, 1.1, and 1.2 of the Transport Layer Security (TLS) protocol. You should ensure that the more secure version 1.1 and above are used.

To enforce use of TLS versions 1.1 and above:

1. Navigate to **Device | Settings > Administration**.
2. Click **Management**.
3. In the **WEB MANagements SETTINGS** section, enable **Enforce TLS 1.1 and Above**.



4. Click **Accept**.

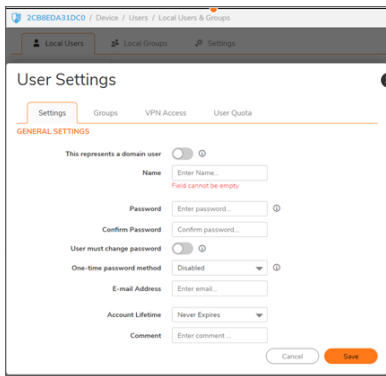
- ① **NOTE:** When NDPP mode is enabled, the server only allows TLS protocol version 1.2 and rejects all other protocol versions, including SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, and any other unknown TLS version strings supplied.

Local User Creation

Local users can be added to the internal database on the security appliance from the **Device | Users | Local Users & Groups** page.

To add local users to the database:

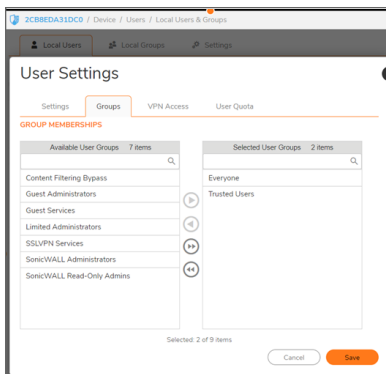
1. Navigate to **Device | Users > Local Users & Groups** page.
2. Click **Add User**. The **Add User** dialog box displays.



The screenshot shows the 'User Settings' dialog box with the 'GENERAL SETTINGS' tab selected. The 'This represents a domain user' checkbox is checked. The 'Name' field contains 'Enter Name...' with a red error message 'Field cannot be empty'. The 'Password' field contains 'Enter password...' and the 'Confirm Password' field contains 'Confirm password...'. The 'User must change password' checkbox is checked. The 'One-time password method' is set to 'Disabled'. The 'E-mail Address' field contains 'Enter email...'. The 'Account Lifetime' is set to 'Never Expires'. The 'Comment' field contains 'Enter comment...'. There are 'Cancel' and 'Save' buttons at the bottom.

3. Type the username into the Name field.
4. In the Password field, type a password for the user. Passwords are case sensitive and should consist of a combination of letters, numbers and other characters.
5. Confirm the password by retyping it in the Confirm Password field.

① **NOTE:** Passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: !, @, #, \$, %, ^, &, *, (, and).
6. To give privileges, click on **Groups** and select the groups per the requirements.



The screenshot shows the 'User Settings' dialog box with the 'GROUPS' tab selected. The 'GROUP MEMBERSHIPS' section is visible. On the left, under 'Available User Groups', there are 7 items: Content Filtering Bypass, Guest Administrators, Guest Services, Limited Administrators, SSLVPN Services, SonicWALL Administrators, and SonicWALL Read-Only Admins. On the right, under 'Selected User Groups', there are 2 items: Everyone and Trusted Users. There are 'Cancel' and 'Save' buttons at the bottom.

NOTE: Only administrators may login to the administrative interface, ensuring that access to TSF data is disallowed for non-administrative users.

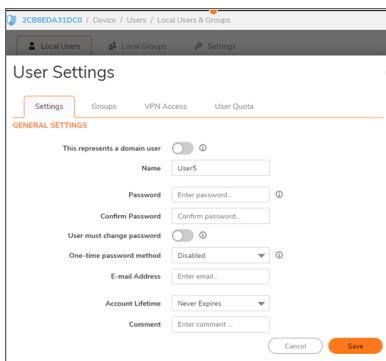
7. Click **Save**.

Editing Local User

Local users can be edited from the **Device | Users > Local Users & Groups** page.

To edit a local user:

1. Navigate to **Device | Users > Local Users & Groups** page.
2. In the **Local Users** table, click the user's **Edit** icon under **Configure**. The **Edit User** dialog displays.



3. Configure the options exactly as when adding a new user.
4. Click on **Save**.

User Session Settings

This section gives details about the steps required to configure inactivity time, the number of successive unsuccessful authentication attempts, and the lockout period.

Configure Inactivity Time

Inactive local and remote sessions to the appliance are automatically terminated after a Security Administrator-configurable time interval.

To configure inactivity time for webUI:

1. Navigate to **Device | Settings > Administration**.
2. Click **Login/Multiple Administrators**.

3. To specify the inactive time that can elapse before you are automatically logged out of the Management Interface, enter the time, in minutes, in the **Log out the Admin after inactivity of (mins)** field. By default, the SonicWall Security Appliance logs out the administrator after 5 minutes of inactivity. The inactivity timeout can range from 1 to 9999 minutes.



A screenshot of a configuration form. At the top right, there is a checkbox labeled 'Audit admin'. Below it, on the left, is the text 'Log out the Admin after inactivity of (mins)'. To the right of this text is a text input field containing the number '7'.

To configure inactivity time for CLI:

1. Login into the local console and type `config` to start the configuration session.
2. Type the command `cli idle-timeout *` (where * is the timeout value provided in minutes.)
3. To save the configuration, type `commit`.

Configure Administrator Lockout

The SonicWall security appliance can be set up to lockout an administrator or a user if the login credentials are incorrect.

To configure login constraints:

1. Navigate to **Device | Settings > Administration**.
2. Click **Login/Multiple Administrators**.
3. Enable **Admin/user lockout**.

Both administrators and users are locked out of accessing the firewall after the specified number of incorrect login attempts. This option is disabled by default.

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

When this option is enabled, the fields in the following steps become active.

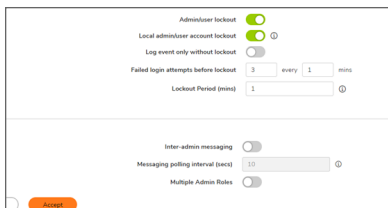
4. Enable **local admin/user account lockout** (uncheck for login IP address lockout). This option locks out user accounts and IP addresses when they have surpassed a specified number of incorrect login attempts. It is only available when admin/user lockout is enabled.
5. Select **Log event only without lockout** for SonicOS to log failed user login attempts that have reached the established threshold but does not lock out the user or IP address. This option is only available when the admin or /user lockout is enabled.

After a user or IP address is locked out, the message **User login denied - User is locked out** displays on the login screen, and the login is rejected.

NOTE: You can review and edit all locked-out user accounts on the Active Users page (Device | User | Status) when local admin/user account lockout is enabled.

6. Enter the number of failed attempts within a specified time frame before the user is locked out in the **Failed login attempts per minute before lockout** field. The default number is 5, the minimum is 1, and the maximum is 99.

7. Enter the maximum time in which failed attempts can be made. The default is 5 minutes, the minimum is 1 minute, and the maximum is 240 minutes (4 hours).
8. Enter the length of time that must elapse before the user is allowed to attempt to log into the firewall again in the **Lockout Period (mins)** field. The default is 5 minutes, the minimum is 0 (permanent lockout), and the maximum is 60 minutes. The user will be allowed to log in successfully only after the configured length of time has elapsed.
9. From the command line interface (CLI), enter the number of incorrect login attempts that triggers a lockout in the **Max login attempts through CLI** field. The default is 5, the minimum is 3, and the maximum is 15.
10. Click **Accept**.



The appliance ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available, either permanently or temporarily, by providing a local logon which is not subject to blocking.

Password Compliance

To configure password compliance:

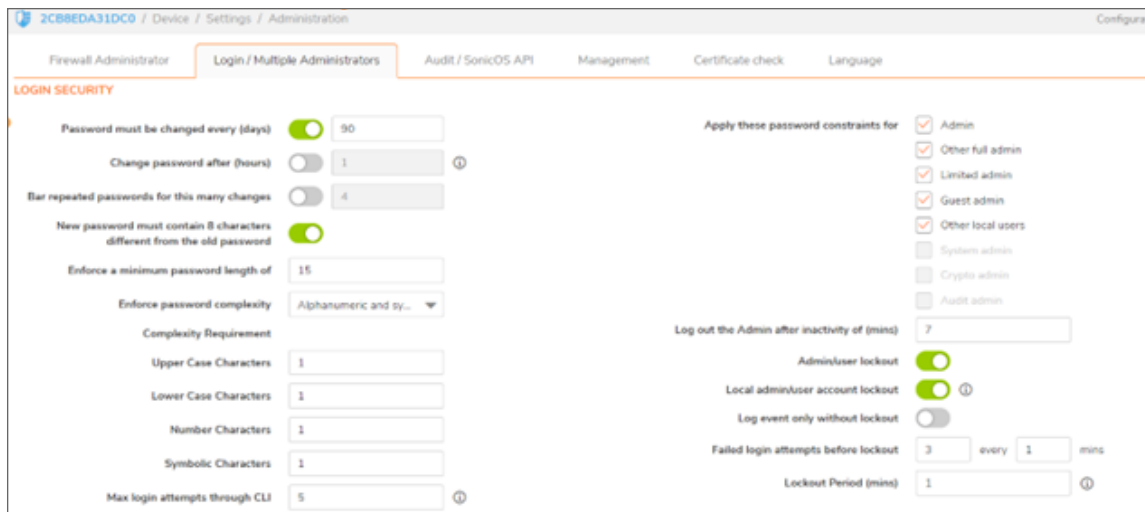
Navigate to **Device | Settings > Administration**.

1. Click **Login / Multiple Administrators**.
2. Configure the following settings in the **LOGIN SECURITY** section.
3. To require users to change their passwords after a designated number of days has elapsed:
 - Select **Password must be changed every (days)**. The field becomes active. This option is not selected by default.
 - Enter the elapsed time in the field. The default number of days is 90, the minimum is 1 day, and the maximum is 9999.

When a user attempts to login with an expired password, a popup window prompts the user to enter a new password. The **User Login Status** window now includes a **Change Password** button so users can change their passwords at any time.

4. To specify the minimum length of time, in hours, allowed between password changes:
 - Select **Change password after (hours)**. The field becomes active.
 - Enter the number of hours. The minimum – and default – time is 1 hour; the maximum is 9999 hours.
5. To require users to use unique passwords for the specified number of password changes:

- Select Bar repeated passwords for this many changes. The field becomes active.
 - Enter the number of changes. The default number is 4, the minimum number is 1, and the maximum number is 32.
6. To require users to change at least 8 alphanumeric/symbolic characters of their old password when creating a new one, select **New password must contain 8 characters different from the old password**.
 7. Specify the shortest allowed password, enter the minimum number of characters in the **Enforce a minimum password length of** field. The default number is 8, the minimum is 1, and the maximum is 99.
ⓘ | NOTE: When in NDPP mode, the minimum supported length is 15 characters.
 8. Choose how complex a user's password must be to be accepted from the Enforce password complexity drop-down menu:
 - None (default)
 - Alphanumeric characters— Requires both alphabetic and numeric characters
 - Alphanumeric and symbolic characters— Requires alphabetic, numeric, and symbolic characters – for symbolic characters, only !, @, #, \$, %, ^, &, *, (, and) are allowed; all others are denied.When a password complexity option other than None is selected, the options under Complexity Requirement become active.
 9. Enter the minimum number of alphanumeric and symbolic characters required in a user's password. The default number for each is 0, but the total number of characters for all options cannot exceed 99.
 - Upper case characters
 - Lower case characters
 - Numbers
 - Symbols**ⓘ | NOTE:** The Symbols field becomes active only if alphanumeric and symbolic characters is selected.
 10. Select which classes of users the password constraints are applied **under Apply the above password constraints for**. By default, all options are selected:
 - Admin – Refers to the default administrator with the username admin.
 - Other full admin
 - Limited admin
 - Guest admin
 - Other local users



For the management interface, passwords are obscured with dots to prevent an unauthorized individual from inadvertently viewing the password. For the console, the passwords are obscured with blank spaces. The TOE hashes the user-entered password and compare it to the stored hash for the associated username.

Pre-Login Policy Banner

This section describes steps required to configure pre-login policy statement that is presented to all users as a banner in the window before web login or console login.

To create a pre-login policy banner:

1. Navigate to **Device | Users > Settings**.
2. Click **Customization**.
3. Scroll to the **Pre-Login Policy Banner** section.
4. In the **Pre-Login Policy Banner** section, select **Start with policy banner before login** page. This option is not selected by default.
5. In the **Policy banner content** field, enter your policy text. You can include HTML formatting. The page displayed includes an **I Accept** button and **Cancel** button for user confirmation.
6. Click **Accept**.

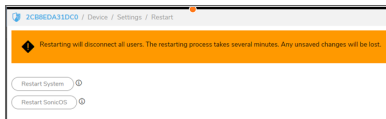
System Restart

The SonicWall Security Appliance can be restarted from the Web Management interface and local console interface.

- ❗ **IMPORTANT:** The restarting process takes a few minutes. During the restart time, all users are disconnected. If you made any changes to the settings, apply them before you restart.

To restart the firewall from the Web Management interface:

1. Navigate to **Device | Settings > Restart**.
2. Click the **Restart SonicOS** button.



- **Restart System** does a full restart with booting the system from scratch.
- **Restart SonicOS** restarts the operating system without rebooting the system.

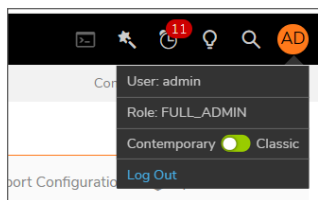
To restart the firewall from the local console interface:

1. Login into the local console.
2. Type `restart`.
3. Type `yes` once the warning message is displayed and press enter.

```
admin@2CB8EDA31DC0> restart
Are you sure you wish to restart firewall? (yes/cancel)
[console] yes
```

Logging Out

Logout occurs when the user actively ends the session by closing their session window or by using the **Logout** option provided on the session window. The session window is the preferred method for user logout; however, the same result can be achieved by allowing the session to expire. The latter removes the dependency on the session window but manages resources less efficiently.

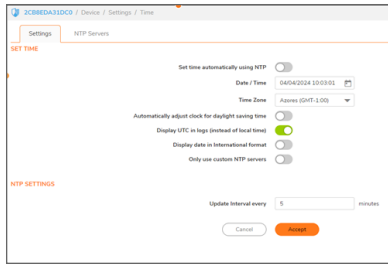


To log out of the CLI, enter `logout`.

```
admin@2CB8EDA31DC0> logout
```

Setting System Time

The system time can be set in the section **Device | Settings > Time**.



To set the system time:

1. Navigate to **Device | Settings > Time**.
2. Select the time zone you are in from **Time Zone**.
3. Disable **Set time automatically using NTP**. The Time and Date options become available.
4. Select the time in the 24-hour format using the **Time (hh:mm:ss)** drop-down menus
5. Select the date from the **Date** drop-down menus.

Date / Time	04/04/2024 10:03:01
Time Zone	Azores (GMT-1.00)

Managing Certificates

To implement the use of certificates for VPN policies, you must locate a source for a valid CA certificate from a third-party CA service. When you have a valid CA certificate, you can import it into the firewall to validate your Local Certificates. You import the valid CA certificate into the firewall using the **Device | Settings > Certificates** page. After you import the valid CA certificate, you can use it to validate your local certificates. SonicOS provides a large number of certificates with the SonicWall network security appliance. These are built-in certificates and cannot be deleted or configured.

The device automatically uses all valid certificates without needing any additional configuration. It does not permit the use of invalid, expired, or unverified certificates.

Certificates Table

The screenshot shows the SonicOS interface for managing certificates. The page title is "2CBBEDA31DC0 / Device / Settings / Certificates". There is a search bar, a dropdown menu for "All Certificates", and a checkbox for "Include expired built-in certificates". Action buttons include "New Signing Request", "SCEP", "Import", and "Delete". The main content is a table with columns for "CERTIFICATE", "TYPE", "VALIDATED", and "EXPIRES".

CERTIFICATE	TYPE	VALIDATED	EXPIRES
ComSign CA	CA certificate		Mar 19 15:02:18 2029 GMT
Shavite Primary Root CA - G3	CA certificate		Dec 1 23:59:59 2037 GMT
TC TrustCenter Class 2 CA II	CA certificate		Dec 31 22:59:59 2025 GMT
ACCVRAIZ1	CA certificate		Dec 31 09:37:37 2030 GMT
GlobalSign	CA certificate		Mar 18 10:00:00 2029 GMT
ACEDICOM Root	CA certificate		Apr 13 16:24:22 2028 GMT
COMODO Certification Authority	CA certificate		Dec 31 23:59:59 2029 GMT
Atos TrustedRoot 2011	CA certificate		Dec 31 23:59:59 2030 GMT
T-TeleSec GlobalRoot Class 3	CA certificate		Oct 1 23:59:59 2033 GMT
SwissSign Platinum CA - G2	CA certificate		Oct 25 08:36:00 2036 GMT
Chambers of Commerce Root	CA certificate		Sep 30 16:13:44 2037 GMT
S-TRUST Authentication and Encryption Root CA 2005-PN	CA certificate		Jun 21 23:59:59 2030 GMT
VeriSign Class 3 Public Primary Certification Authority - G5	CA certificate		Jul 16 23:59:59 2036 GMT
AffirmTrust Networking	CA certificate		Dec 31 14:08:24 2030 GMT
TC TrustCenter Universal CA I	CA certificate		Dec 31 22:59:59 2025 GMT
TWCA Global Root CA	CA certificate		Dec 31 15:59:59 2030 GMT
Secure Global CA	CA certificate		Dec 31 19:52:06 2029 GMT
TeliaSonera Root CA v1	CA certificate		Oct 18 12:00:50 2032 GMT
AffirmTrust Commercial	CA certificate		Dec 31 14:06:06 2030 GMT
Entrust.net Certification Authority (2048)	CA certificate		Jul 24 14:15:12 2029 GMT
The Go Daddy Group, Inc.	CA certificate		Jun 29 17:06:20 2034 GMT

The **Certificates** page provides all the settings for managing CA and Local Certificates. The table page displays this information about certificates:

Column	Information Displayed
CERTIFICATE	Name of the certificate.
TYPE	Type of certificate: <ul style="list-style-type: none"> • CA certificate • Local certificate • Pending request
VALIDATED	Validation information: <ul style="list-style-type: none"> • Blank • Yes—When a local certificate with a valide CA is loaded onto the TOE, the VALIDATED column displays Yes. • Invalid • Expire in n days • Expired
EXPIRES	Date and time the certificate expires.

Certificate Details

Click the certificate's row in the table to display information about the certificate. This might include the following, depending on the type of certificate:

HTTPS MANAGEMENT CERTIFICATE

Signature Algorithm	sha256WithRSAEncryption
Certificate Issuer	C = US, O = acumen, OU = CC, CN = CA
Subject Distinguished Name	C = US, O = acumen, OU = CC, CN = CA
Public Key Algorithm	RSA 2048 bits
Certificate Serial Number	19582D25951BCB28
Valid from	Oct 18 07:19:00 2023 GMT
Expires On	Oct 18 07:19:00 2033 GMT
CRL Status	No CRL loaded
CRL is required	off
CA Hash	/w4WQN7zqLYqD0iu23VYKQ==

- Signature Algorithm
- Certificate Issuer
- Subject Distinguished Name
- Public Key Algorithm
- Certificate Serial Number
- Valid from
- Expires On
- CRL Status (for Pending requests and local certificates)
- CA Hash

- Alternate Subject Name
- Alternate Subject Name Type
- Status—Shows **Verified** when a local certificate with a valid CA is successfully loaded onto the TOE.

The details shown depend on the type of certificate. **Certificate Issuer**, **Certificate Serial Number**, **Valid from**, and **Expires On** are not shown for **Pending** requests as this information is generated by the Certificate provider.

Importing Certificates

After your CA service has issued a Certificate for your Pending request, or has otherwise provided a Local Certificate, you can import it for use in VPN or Web Management authentication. CA Certificates might also be imported to verify local Certificates and peer Certificates used in IKE negotiation.

Importing a Local Certificate

To import a local certificate :

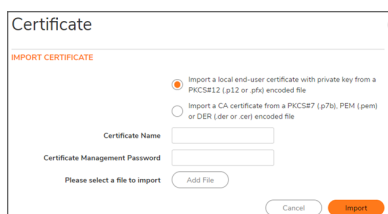
1. Navigate to **Device | Settings > Certificates**.
2. Click **Import**. The **IMPORT CERTIFICATE** dialog displays.

3. Enter a certificate name in the **Certificate Name** field.
4. Enter the password used by your Certificate Authority to encrypt the PKCS#12 file in the **Certificate Management Password** field.
5. Click **Add File** to locate the certificate file.
6. Select the certificate and click **Open**.
7. Click **Import** to import the certificate into the firewall. When it is imported, you can view the certificate entry in the **Certificates** table.
8. Click the certificate displayed on the **Certificates** page to see the status and other details.

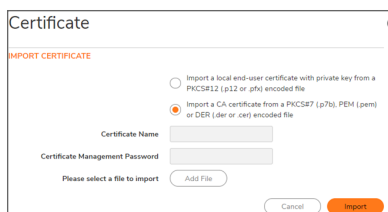
Importing a Certificate Authority Certificate

To import a certificate from a certificate authority:

1. Navigate to **Device | Settings > Certificates**.
2. Click **Import**. The **IMPORT CERTIFICATE** dialog is displayed.



3. Choose **Import a CA certificate from a PKCS#7 (*.p7b) or DER (.der or .cer) encoded file**. The **Import Certificate** dialog settings change.



4. Click **Add File** and locate the certificate file.
5. Click **Open**.
6. Click **Import** to import the certificate into the firewall. When it is imported, you can view the certificate entry in the **Certificates** table.
7. Click the certificate displayed on the **Certificates** page to see the status and other details.

Certificate Validation

The validity of certificates is checked on certificate import and prior to usage of the public key within the certificate.

Certificate validation includes checks of:

- The certificate validity dates
- The validation path, ensuring that the certificate path terminates with a trusted CA certificate
- basicConstraints, ensuring the presence of the basicConstraints extension
- Revocation status, using OCSP & CRLs
- extendedKeyUsage properties, when the certificate is used for OCSP or CRLs

The TOE validates the extendedKeyUsage field according to the following rules:

- Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
- Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
- Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
- OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

The certificate path is also validated when a certificate is imported. This validation includes a check of the certificate chain, and the keys of each of the certificates in the chain. The validity period of the certificate is also checked at this time.

For the web server certificate (local), the validity of the certificate is determined by connecting to a remote CRL server. If the validity of the web server certificate cannot be verified, the system accepts the certificate and an audit log is generated to indicate that the web server certificate is expired.

Revocation Checking Using OCSP

When a certificate is used for IPsec tunnel, an OCSP server is contacted to verify that the certificate is still valid. If the validity of a certificate that is used for IPsec tunnel cannot be verified, the system rejects the certificate and drops the connection for IPsec tunnels.

The device communicates with an OCSP responder. The OCSP server must also be configured with an OCSP response signing certificate issued by the CA server. The OCSP responder can be a CA server or another server that communicates with the CA server to determine the certificate status. The device issues a status request to an OCSP responder and suspends the acceptance of the certificate until the responder provides a response.

The OCSP responder receives the request from the client and checks that the message is properly formed and if the responder is able to respond to the service request. Then it checks if the request contains the correct information needed for the service desired. If all conditions are satisfied, the responder returns a definitive response to the OCSP client. The OCSP responder is required to provide a basic response of GOOD, REVOKED, or UNKNOWN.

The GOOD state is the desired response as it indicates the certificate has not been revoked. The REVOKED state indicates that the certificate has been revoked. The UNKNOWN state indicates the responder does not have information about the certificate in question.

The certificate revocation checking is performed on the local and Intermediate certificates.

If the validity of a certificate cannot be verified, the system rejects the certificate and drops the connection.

A Security Administrator can follow these steps if a connection cannot be established during the validity check of a certificate:

1. Check OCSP Responder URL: Verify that the OCSP responder URL specified in the certificate is correct and accessible.

2. **Test OCSP Responder Connectivity:** Try accessing the OCSP responder URL directly to confirm that the responder is reachable from your network.
3. **Check System Time and Date:** Ensure that the system time and date are correct, as incorrect time settings can affect certificate validity checks.
4. **Check OCSP Responder Status:** Ensure that the OCSP responder service is up and running.
5. **Review Logs:** Examine system and application logs for any errors or warnings related to the certificate validation process. These logs can provide clues about what might be going wrong.

Deleting a Certificate

You can delete an imported certificate if it has expired or if you decide not to use third-party certificates for VPN authentication. You can always delete certificates you created.

To delete a certificate:

1. Navigate to **Device | Settings > Certificates**.
2. Hover over the certificate and click the **Delete** icon.

To delete multiple certificates:

1. Navigate to **Device | Settings > Certificates**.
2. Select the certificates that you want to delete by selecting the checkboxes next to the certificates.
① | **TIP:** To select all the certificates, select the checkbox next to the Certificate column in the header row.
3. Click the **Delete** icon at the top of the table.
① | **NOTE:** Built-in certificates cannot be deleted.

Generating a Certificate Signing Request

You should create a Certificate Policy to be used in conjunction with local certificates. A Certificate Policy determines the authentication requirements and the authority limits required for the validation of a certificate. The security administrator can manage generating and importing keys. Private keys and public keys certificates are stored encrypted in flash memory in PEM (.pem) or DER (der or .cer) encoded format.

To generate a certificate signing request:

1. Navigate to **Device | Settings > Certificates**.
2. Click **New Signing Request**. The **Certificate** dialog displays.

3. Enter an alias name for the certificate in the **Certificate Alias** field.
4. Create a **Distinguished Name (DN)** using the drop-down menus shown in table below; then enter information for the certificate in the associated fields.
 - ① **NOTE:** For each DN, you can select your country from the associated drop-down menu. For all other components, enter the information in the associated field.

Drop-down menu	Select appropriate information
Country	Country (default) State Locality or County Company or Organization
State	Country State (default) Locality, City, or County Company or Organization Department
Locality, City, or County	Locality, City, or County (default) Company or Organization Department Group Team
Company or Organization	Company or Organization (default) Department Group Team Common Name Serial Number E-Mail Address

Drop-down menu	Select appropriate information
Department	Department (default) Group Team Common Name Serial Number E-Mail Address
Group	Group (default) Team Common Name Serial Number E-Mail Address
Team	Team (default) Common Name Serial Number E-Mail Address
Common Name	Common Name (default) Serial Number E-Mail Address

As you enter information for the components, the Distinguished Name (DN) is created in the **Subject Distinguished Name** field.

The screenshot shows a form titled "GENERATE CERTIFICATE SIGNING REQUEST". It contains several dropdown menus and text input fields. The "Department" dropdown is selected, and the "Subject Distinguished Name" field displays the value "C: ST: Maryland: Maryland".

- Optionally, you can also attach a **SUBJECT ALTERNATIVE NAME** to the certificate after selecting the type from the drop-down menu:
 - Domain Name
 - Email Address
 - IPv4 Address
- Select a signature algorithm from the **Signature Algorithm** drop-down menu:
 - SHA1 (default)
 - MD5
 - SHA256

- SHA384
- SHA512

7. Select a subject key type from the **Subject Key Type** drop-down menu:

RSA (default)	A public key cryptographic algorithm used for encrypting data.
ECDSA	Encrypts data using the Elliptic Curve Digital Signature Algorithm, which has a high strength-per-key-bit security.

8. Select a subject key size or curve from the **Subject Key Size/Curve** drop-down menu.

① **NOTE:** Not all key sizes or curves are supported by a Certificate Authority, therefore, you should check with your CA for supported key sizes.

If you selected a key type of:

RSA, select a key size	ECDSA, select a curve
1024 bits (default)	prime256vi: X9.62.SECP curve over a 256 bit prime field (default)
1536 bits	secp384r1: NIST/SECP curve over a 384 bit prime field
2048 bits	secp521r1: NIST/SECP curve over a 521 bit prime field
4096 bits	

9. Click **Generate** to create a certificate signing request file.

When the Certificate Signing Request is generated, a message describing the result is displayed and a new entry appears in the Certificates table with the type Pending request.

<input type="checkbox"/>	CERTIFICATE	TYPE	VALIDATED	EXPIRES
<input type="checkbox"/>	test	Pending request		

10. Click the **Export** icon. The **Export Certificate Request** dialog displays.

Export Certificate Request

test

Subject Distinguished Name C=US,ST=Maryland,L=Maryland,O=acumensec,OU=ccou=testing,CN=10.1.5.163

Subject Key Identifier 0x4D2093AA32DF21F38D286ACE0C11827CF7785A2C5

Public Key Algorithm RSA 2048 bits

11. Click the **Export** icon to download the file to your computer. An **Opening <certificate>** dialog displays.

12. Click **OK** to save the file to a directory on your computer.

You have generated the Certificate Request that you can send to your Certificate Authority for validation.

13. Click the **Upload** icon to upload the signed certificate for a signing request. The **Upload Certificate** dialog is displayed.



14. Click **Choose File** to select a file.
15. Select the file and click **Open**.
16. Click **UPLOAD**.

Deleting a Certificate Signing Request

You can always delete certificates signing requests you created. The security administrator can manage deleting keys.

To delete a certificate signing request:

1. Navigate to **Device | Settings > Certificates**.
2. Hover over the certificate signing request and click the **Delete** icon.

Checking Certificate Expiration

To activate periodic checks of certificate's expiration:

1. Navigate to **Device | Settings > Administration > Certificate Check**.
2. In the **CHECK CERTIFICATE EXPIRATION SETTINGS** section, select **Enable periodic certificate expiration check**. This option is selected by default. When enabled, the **Certificate expiration alert interval** field becomes available.



3. To set the interval between certificate checks, enter the interval, in hours, in the **Certificate expiration alert interval: 1 - 168 (in hours)** field. The minimum time is 1 hour, the maximum is 168 hours, and the default is 168.
4. Click **Accept**.

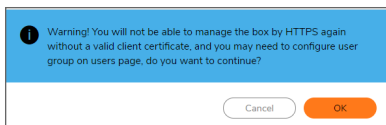
Configuring Client Certificate Verification

To configure Client Certificate Check:

1. Navigate to **Device | Settings > Administration**.
2. Click **Certificate Check**.



3. To enable client certificate checking and Common Access Card (CAC) support on the SonicWall Security Appliance, select **Enable Client Certificate Check**. If you enable this option, other options become available. A warning confirmation message displays:



4. Click **OK**.
5. To activate the client certification cache, select **Enable Client Certificate Cache**.
① | **NOTE:** The cache expires 24 hours after being enabled.
6. To specify from which certificate field the username is obtained, choose an option from **User Name Field**:
 - Subject: Common Name (default)
 - Sub Alt: Email
 - Sub Alt: Microsoft Universal Principal Name
7. To select a Certification Authority (CA) certificate issuer, choose one from the **Client Certificate Issuer** drop-down menu. The default is **thawte Primary Root CA - G3**.
① | **NOTE:** If the appropriate CA is not listed, you need to import that CA into the SonicWall Security Appliance.
8. To select how to obtain the CAC user group membership and, thus, determine the correct user privilege, choose from the **CAC user group memberships retrieve method** drop-down menu:
 - **Local Configured** (default) – If selected, you should create local user groups with proper memberships.
 - **From LDAP** – If selected, you need to configure the LDAP server
9. To enable the Online Certificate Status Protocol (OCSP). check to verify the client certificate is still valid and has not been revoked by selecting **Enable OCSP Checking**. When this option is enabled, the **OCSP Responder URL** field displays and the **Enable periodic OCSP Check** option displays.

Enable OSCP Checking

OCSP Responder URL

Enable periodic OSCP Check

OCSP check interval: 1-72 (hours)

10. Enter the URL of the OSCP server that verifies the status of the client certificate in the **OCSP Responder URL** field.

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

11. To enable a periodic OCSP, check for the client certificate to verify that the certificate is still valid and has not been revoked:
 - Select **Enable periodic OCSP Check**. The OCSP check interval field becomes available.
 - Enter the interval between OCSP checks, in hours, in the **OCSP check interval 1~72 (hours)** field. The minimum interval is 1 hour, the maximum is 72 hours, and the default is 24 hours.
12. Click **Accept**.

Object Classes

This section provides information about different object classes used in SonicOS. Match objects represent the set of conditions which must be matched for actions to take place.

Addresses

Address Objects are one of four object classes (address, user, service, and schedule) in SonicOS Enhanced. These address objects allow for entities to be defined one time, and to be re-used in multiple referential instances throughout the SonicOS interface.

To create an address object:

1. Navigate to **Object | Match Objects | Addresses**.
2. Click on **ADD**. The **Add object** dialog displays.

3. Enter the **Name of Object**.
4. Assign a zone from drop down list in **Zone Assignment** field.
5. Select the **Type** from drop down list:
 - **Host:** Host Address Objects define a single host by its IP address. The Netmask for a Host Address Object is automatically set to 32-bit (255.255.255.255) to identify it as a single host.
 - **Range:** Range Address Objects define a range of contiguous IP addresses. No Netmask is associated with Range Address Objects, but internal logic generally treats each member of the specified range as a 32-bit masked Host object.
 - **Network:** Network Address Objects are like Range objects in that they comprise multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are

defined by a valid Netmask. Network Address Objects must be defined by the network's address and a corresponding Netmask.

- **FQDN:** FQDN address objects allow for the identification of a host by its Fully Qualified Domain Names (FQDN), such as www.SonicWall.com. FQDNs are resolved to their IP address (or IP addresses) using the DNS server configured on the security appliance. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.
- **MAC Address:** MAC Address Objects allow the identification of a host by its hardware address or MAC (Media Access Control) address. MAC addresses are uniquely assigned to every piece of wired or wireless networking device by their hardware manufacturers, and are intended to be immutable. MAC addresses are 48-bit values that are expressed in 6 byte hex-notation, for example *<My Access Point>* with a MAC address of C0:EA:E4:00:C2:E8. MAC addresses resolve to an IP address by referring to the ARP cache on the security appliance. MAC address objects are used by various components of Wireless configurations throughout SonicOS.

6. Enter the value for the selected type and click on **Save**.

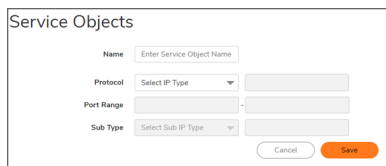
Services

Services control network traffic by creating rules for allowing access to the network or blocking an item from it. The device has Default Services and custom services:

- **Default services:** Default services are the defined services which will have the standard ports which cannot be deleted. The service has following parameters:
 - Name:** Service Name
 - Protocol Type:** Type of IP protocol
 - Port Range:** Range of the port
- **Custom services:** All custom services created are listed in the **Custom Services** table. You can create a group of services by creating a **Custom Service Group** for easy policy enforcement.

To create a Service Object::

1. Navigate to **Object | Match Object | Services > Service Object**.
2. Click **Add**.



The screenshot shows a form titled "Service Objects" with the following fields:

- Name:** A text input field with the placeholder "Enter Service Object Name".
- Protocol:** A dropdown menu labeled "Select IP Type" with an adjacent empty text input field.
- Port Range:** Two adjacent empty text input fields.
- Sub Type:** A dropdown menu labeled "Select Sub IP Type" with an adjacent empty text input field.

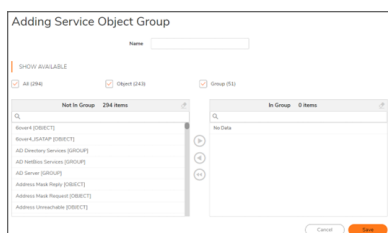
At the bottom of the form are two buttons: "Cancel" and "Save".

3. Enter the **Name of the Service Object**.
4. Select the **Protocol from IP Type** drop down. You can also use a **Custom Type**.
5. Enter the **Port Range** or **IP protocol Sub Type**, depending on your IP protocol selection:

- For TCP and UDP protocols, specify the **Port Range**. You do not need to specify a **Sub Type**.
 - For ICMP, IGMP, OSPF and PIMSM protocols, select from the **Sub Type** drop-down menu .
 - For the remaining protocols, you do not need to specify a **Port Range** or **Sub Type**.
6. Select the **Sub Type** from the drop-down list.
 7. Click on **Save**.

To create a Service Group::

1. Navigate to **Object | Match Object | Services > Service Group**.
2. Click on **Add**.



3. Enter the group name in the **Name** field.
4. Select the objects or groups and click on **Save**.

Match Objects

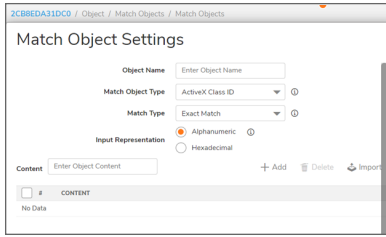
Match objects represent the set of conditions that must be matched for actions to take place. This includes the object type, the match type (exact, partial, regex, prefix, or suffix), the input representation (text or hexadecimal), and the actual content to match. Match objects were referred to as application objects in previous releases.

Hexadecimal input representation is used to match binary content such as executable files, while alphanumeric (text) input representation is used to match things like file or email content. You can also use hexadecimal input representation for binary content found in a graphic image. Text input representation could be used to match the same graphic if it contains a certain string in one of its property's fields. Regular expressions (regex) are used to match a pattern rather than a specific string or value and use alphanumeric input representation.

The File Content match object type provides a way to match a pattern or keyword within a file. This type of match object can only be used with FTP Data Transfer, HTTP Server, or SMTP Client policies.

To configure a match object:

1. Navigate to **Object | Match Objects | Match Objects**.
2. Click on **ADD**. The Add object dialog displays.



3. In the **Object Name** field, type a descriptive name for the object.
4. Select a **Match Object Type** from the drop-down menu. Your selection affects available options in this screen.
5. Select a **Match Type** from the drop-down menu. The available selections depend on the match object type.
6. For the **Input Representation** field, click **Alphanumeric to match a text pattern**, or click **Hexadecimal** if you want to match binary content.
7. In the Content text box, type the pattern to match.
8. Click **Add** icon. The content appears in the **List** field. Repeat to add another element to match.

If the **Match Type** is **Regex Match**, you can select one of the predefined regular expressions and then click on the type to add it to the list. You can also type a custom regular expression into the **Content** field, and then click the **Add** icon to add it to the list.

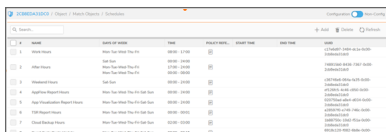
Schedules

In SonicOS, schedules in access rules determine when a specific rule is applied. If traffic is received during the scheduled time, the access rule becomes active and allows the traffic to pass. However, if the traffic is received outside the scheduled time, the access rule is not active, and the traffic will be blocked or handled by default rules.

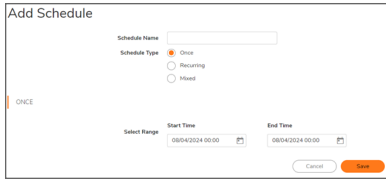
Schedule Groups are groups of schedules to which you can apply firewall rules. For example, you might want to block access to auction sites during business hours but allow employees to access the sites after hours. SonicOS also includes default schedules, such as **Work Hours**, **After Hours**, and **Weekend Hours**. These schedules can be modified, but they cannot be deleted.

To create a Schedule Group:

1. Navigate to **Object | Match Objects > Schedules**.



2. Click on **ADD**. The **Add object** dialog displays.



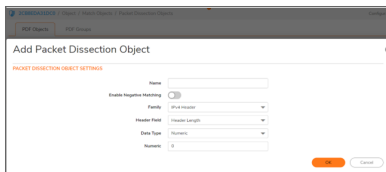
3. In the **Schedule Type** section, select how often the schedule occurs: **Once**, **Recurring**, or **Mixed**.
 - For a schedule that occurs only once, select the year, month, date, hour, and minutes for the **Start** and **End** fields.
 - For recurring schedules, select the check boxes for each day the schedule applies. Enter the start time for the recurring schedule in the **Start Time** field and also the **End Time** field. Make sure to use the 24-hour format for both of them.
 - For the mixed schedule type, you can use the recurring and once options in the same configuration.
4. After configuring the desired schedule click on **Add**.
5. To delete an existing schedule, click on **Delete this schedule** icon.
6. To edit an existing schedule, click on the **Edit this schedule** icon .

Packet Dissection Objects

The Packet Dissection Objects lets you specify specific packet characteristics to filter on.

To create Packet Dissection object:

1. Navigate to **Object | Match Objects | Packet Dissection Object**.
2. In the **PDF Objects** section click on **+**.



3. To specify the characteristics to filter on select from the following:
 - Name – Name of the rule.
 - Enable Negative Matching – Allows you to only examine the traffic type specified in the rule.
 - Family – Type of analysis to be performed.
 - Header field – The header to be examined.
 - Data Type – Type of data to be examined.
 - Numeric – Examination value

The following fields can be examined:

- IPv4: Version; Header Length; Packet Length; ID; IP Flags; Fragment Offset; Time to Live (TTL); Protocol; Header Checksum; Source Address; Destination Address; and IP Options.
- IPv6: Version; traffic class; flow label; payload length; next header; hop limit; source address; destination address; routing header; home address options.
- ICMP: Type; Code; Header Checksum; and Rest of Header (varies based on the ICMP type and code).
- ICMPv6: Type; Code; and Header Checksum.
- TCP: Source port; destination port; sequence number; acknowledgment number; offset; reserved; TCP flags; window; checksum; urgent pointer; and TCP options.
- UDP: Source port; destination port; length; and UDP checksum.

About Negative Matching

Negative matching provides an alternate way to specify which content to block. You can enable negative matching in a match object when you want to block everything except a particular type of content. When you use the object in a policy, the policy executes actions based on the absence of the content specified in the match object. Multiple list entries in a negative matching object are matched using the logical AND, meaning that the policy action is executed only when all specified negative matching entries are matched.

Although all App Rules policies are DENY policies, you can simulate an ALLOW policy by using negative matching. For instance, you can allow email .txt attachments and block attachments of all other file types. Or you can allow a few types and block all others.

Not all match object types can utilize negative matching. For those that can, you see the **Enable Negative Matching Checkbox on the Match Object Settings** dialog.

IPSec VPN

This section reviews the general process for site-to-site configurations. Specific scenarios might be different and some are described in subsequent sections. Note that configuring IPsec VPNs for IPv4 and IPv6 are very similar; however, certain VPN features are currently not supported in IPv6.

IPSec policies are used to encrypt data between the appliance and the audit server. In general, an IPSec policy can be used to encrypt data (PROTECT). If traffic not belonging to the protected interface or subnet is found on this interface, the traffic bypasses encryption and is routed to the destination in plaintext (BYPASS). If plaintext traffic is received on a protected interface or subnet, the traffic is discarded and deleted (DISCARD).

IPSec VPN traffic is secured in two stages:

- **Authentication:** The first phase establishes the authenticity of the sender and receiver of the traffic using an exchange of the public key portion of a public-private key pair. This phase must be successful before the VPN tunnel can be established.
- **Encryption:** The traffic in the VPN tunnel is encrypted using AES.

The information exchange for authentication and encryption/decryption uses the Internet Key Exchange (IKE) protocol for exchanging authentication keys and establishing the VPN tunnel.

The appliance only operates in Tunnel mode in the evaluated configuration. This is a default setting and cannot be changed when using IKEv2.

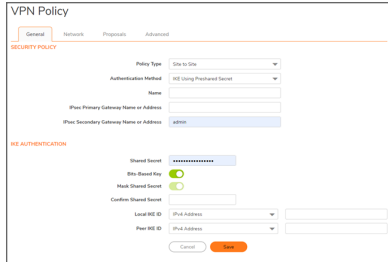
Configure VPN

To configure a VPN:

1. Navigate to the **NETWORK | IPSec VPN > Rules and Settings** page.
2. Make the appropriate version selection, either **IPv4** or **IPv6**.
3. Click **+Add**.
4. Complete the **General**, **Network**, **Proposals**, and **Advanced** tabs on the **VPN Policy** dialog. The following sections provide additional information for each of those tabs.

General Tab on VPN Policy

On the **General** tab, begin defining the site-to-site VPN policy. There are some slight differences between IPv4 and IPv6 networks, which are noted.



To configure settings on the General tab:

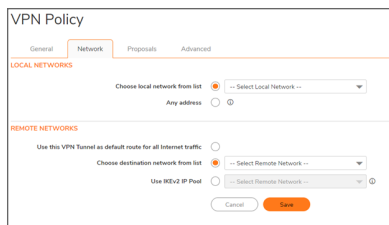
1. If configuring an IPv4 VPN, select **Policy Type** from the drop-down menu.
NOTE: The **Policy Type** field is not available for IPv6.
2. Select the authentication method from the **Authentication Method** drop-down menu. The remaining fields in the **General** tab change depending on which option you select. The following options are available:

IPv4	IPv6
Manual Key	Manual Key
IKE using Preshared Secret (default)	IKE using Preshared Secret (default)
IKE using 3rd Party Certificates	IKE using 3rd Party Certificates
SonicWall Auto Provisioning Client	
SonicWall Auto Provisioning Server	

3. Type a **Name** for the policy.
 - For **IPsec Primary Gateway Name or Address**, type in the gateway name or address.
 - For **IPsec Secondary Gateway Name or Address**, type in the gateway name or address.
4. Under IKE Authentication, provide the required authentication information.
NOTE: When configuring IKE authentication, IPv6 addresses can be used for the local and peer IKE IDs.

Network Tab on VPN Policy

On the Network tab, define the networks that comprise the site to site VPN policy.



On the **Network** tab of the VPN policy, select the local and remote networks from the **Local Network and Remote Network** options.

For IPv6:

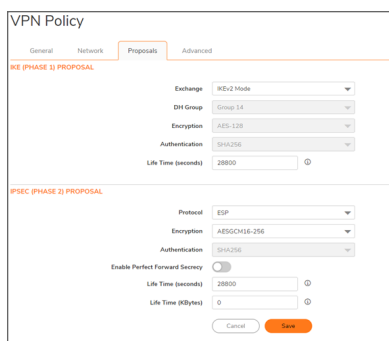
- The drop-down menus are the only option provided and only the address objects that can be used by IPv6 are listed.
- DHCP is not supported, so those options are not available.
- The **Any address** option for **Local Networks** and the **Tunnel All** option for **Remote Networks** are removed.
- An all-zero IPv6 network address object could be selected for the same functionality and behavior.

For IPv4:

- Under **Local Networks**, you can **Choose local network** from list or choose **Any address**. If **Any address** is selected, auto-added rules are created between Trusted Zones and the VPN zone.
- For IPv4 under Remote Networks, you can choose one of the following:
 - Use this VPN tunnel as default route for all Internet traffic.
 - Choose a destination network from the list. If none are listed, you can create a new address object or address group.
 - Use **IKEv2 IP Pool**. Select this to support **IKEv2 Config Payload**.

Proposals Tab on VPN Policy

On the **Proposals** tab, define the security parameters for your VPN policy. The page is the same for IPv4 and IPv6, but the options are different depending on what you selected. IPv4 offers both IKEv1 and IKEv2 options in the **Exchange** field, whereas IPv6 only has IKEv2.



Advanced Tab on VPN Policy

The **Advanced** tabs for IPv4 and IPv6 are similar, but some options are available only for one version or the other, as shown in **Advanced Settings: Option Availability**. Options also change depending on the authentication method selected.

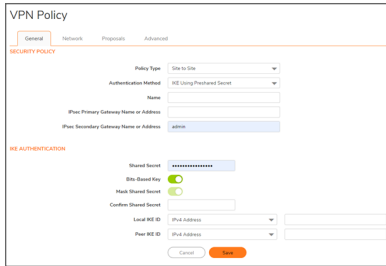
Option	IP Versions	
	IPv4	IPv6
Enable Keep Alive	Supported	Supported
Suppress automatic Access Rules creation for VPN Policy	Supported	-
Disable IPsec Anti-Replay	Supported	Supported
Enable Windows Networking (NetBIOS) Broadcast	Supported	-
Enable Multicast	Supported	-
Display Suite B Compliant Algorithms Only	Supported	Supported
Apply NAT Policies	Supported	-
Using Primary IP Address	-	Supported
Specify the local gateway IP address	-	Supported
Preempt Secondary Gateway	Supported	Supported
Primary Gateway Detection Interval (seconds)	Supported	Supported
Do not send trigger packet during IKE SA negotiation	Supported	Supported
Accept Hash & URL Certificate Type	Supported	Supported
Send Hash & URL Certificate Type	Supported	Supported

Because an interface might have multiple IPv6 addresses, the local address of the tunnel might vary periodically. If a user needs a consistent IP address, select the **Using Primary IP Address** or **Specify the local gateway IP address** option or configure the VPN policy to be bound to an interface instead of a Zone. Manually specify the local gateway IP address. The address must be one of the IPv6 addresses for that interface.

Configuring IKE Using a Preshared Secret Key

To configure a VPN Policy using Internet Key Exchange (IKE) with a Preshared secret key:

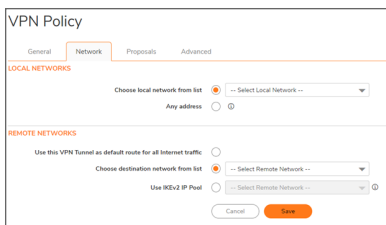
1. Navigate to **NETWORK | IPsec VPN > Rules and Settings**.
2. Click **ADD** to create a new policy or click the **Edit** icon if you are updating an existing policy.



3. From **Policy Type** on the **General** screen, select **Site to Site**.
4. From **Authentication Method**, select **IKE using Preshared Secret**.
5. Enter a name for the policy in the **Name** field.
6. Enter the host name or IP address of the remote connection in the **IPsec Primary Gateway Name or Address** field.
If the Remote VPN device supports more than one endpoint, enter a second host name or IP address of the remote connection in the IPsec Secondary Gateway Name or Address field (optional).
7. In the **IKE Authentication** section, in the **Shared Secret** and **Confirm Shared Secret** fields, enter a Shared Secret password. This is used to set up the SA (Security Association). The Shared Secret password must be at least four characters long and should include both numbers and letters.
ⓘ | NOTE: Ensure that the pre-shared secret is configured identically on both sides of the tunnel.
8. To see the shared secret key in both fields, clear the checkbox for **Mask Shared Secret**. By default, **Mask Shared Secret** is selected, which causes the shared secret key to be displayed as black circles.
9. Optionally, specify a **Local IKE ID** and **Peer IKE ID for this Policy**. You can select from the following IDs from the drop-down menu:
 - IPv4 Address
 - Domain Name
 - E-mail Address
 - Firewall Identifier
 - Key Identifier

By default, the **IP Address** (ID_IPv4_ADDR) is used for Main Mode negotiations, and the firewall identifier (ID_USER_FQDN) is used for Aggressive Mode.

10. Enter the address, name, or ID in the **Local IKE ID** and **Peer IKE ID** fields.
11. Click **Network**.



12. Under **Local Networks**, select one of the following:

Chose local network from lists	Select a network from the drop-down list if a specific network can access the VPN tunnel.
Any address	Use this option if traffic can originate from any local network or if a peer has Use this VPN tunnel as default route for all Internet traffic selected. Auto-added rules are created between Trusted Zones and the VPN Zone. ⓘ NOTE: DHCP over VPN is not supported with IKEv2.

13. Under **Remote Networks**, select one of the following:

Use this VPN Tunnel as default route for all Internet traffic	Select this option if traffic from any local user cannot leave the firewall unless it is encrypted. ⓘ NOTE: You can only configure one SA to use this setting.
Destination network obtains IP addresses using DHCP through this VPN Tunnel	Select this option if the remote network requests IP addresses from a DHCP Server in the local network. ⓘ NOTE: This option is only available if Main Mode or Aggressive Mode is selected on the Proposals tab.
Choose Destination network from list	Select a remote network from the drop-down list.
Use IKEv2 IP Pool	Select this option to support IKEv2 Config Payload. ⓘ NOTE: This option is only available if IKEv2 Mode is selected on the Proposals tab.

14. Click **Proposals**.

15. Under **IKE (Phase 1) Proposal**, choose one of the following options from the **Exchange** drop-down menu:

Main Mode	Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
------------------	---

Aggressive Mode	Generally used when WAN addressing is dynamically assigned. Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
IKEv2 Mode	Causes all negotiation to happen through IKEv2 protocols, rather than using IKEv1 phase 1.

16. Under **IKE (Phase 1) Proposal**, set the values for the remaining options. The default values for **DH Group, Encryption, Authentication, and Life Time** are acceptable for most VPN configurations.
- ① | **NOTE:** If IKEv2 Mode is selected for the Exchange field, the DH Group, Encryption, and Authentication fields are dimmed and no selection can be made for those options.
- ① | **NOTE:** Be sure the Phase 1 values on the opposite side of the tunnel are configured to match. For the DH Group, when in Main Mode or Aggressive Mode, you can select from several Diffie-Hellman exchanges:

Diffie-Hellman Groups Included in Suite B Cryptography	Other Diffie-Hellman Options
256-bit Random ECP Group	Group 1
384-bit Random ECP Group	Group 2
521-bit Random ECP Group	Group 5
192-bit Random ECP Group	Group 14
224-bit Random ECP Group	

For **DH Group**, when in **IKEv2 mode**, you can select from supports Group 14, 256-bit Random ECP Group (Group 19), 384-bit Random ECP Group (Group 20), and 521-bit Random ECP Group (Group 21).

For the **Encryption** field, if **IKEv2 mode** was selected, choose **AES-CBC-128, AES-CBC-192, and AES-CBC-256** from the drop-down menu.

For the **Encryption** field, if **Main Mode** or **Aggressive Mode** was selected, choose **3DES, DES, AES-128 (default), AES-192, or AES-256** from the drop-down menu.

For the **Authentication** field, if **Main Mode** or **Aggressive Mode** was selected, choose **SHA-1 (default), MD5, SHA256, SHA384, or SHA512** for enhanced authentication security.

For the **Authentication** field if **IKEv2 mode** was selected, choose **SHA-256, SHA-384, and SHA-512** from the drop-down menu.

For all **Exchange** modes, enter a value for **Life Time (seconds)**. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

17. Set the options in the **IPsec (Phase 2) Proposal** section. The default values for **Protocol, Encryption, Authentication, Enable Perfect Forward Secrecy, and Life Time (seconds)** are acceptable for most VPN SA configurations.:
- ① | **NOTE:** Be sure the Phase 2 values on the opposite side of the tunnel are configured to match. If you selected **ESP** in the **Protocol** field, in the **Encryption** field you can select from six encryption algorithms that are included in Suite B cryptography:

Suite B Cryptography Options	Other Options
AESGCM16-128	DES
AESGCM16-192	3DES
AESGCM16-256	AES-128
AESGMAC-128	AES-192
AESGMAC-192	AES-256
AESGMAC-256	None

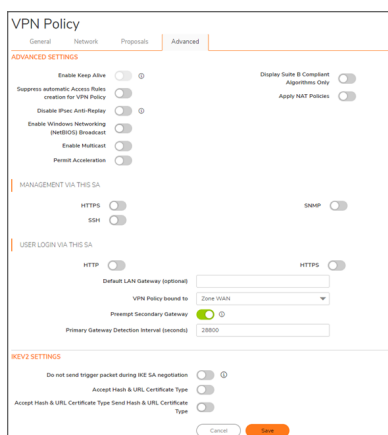
If NDCPP compliance is enabled, then in the **Encryption** field you can select from AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, or AES-GCM-256.

If you selected **AH** in the **Protocol** field, the **Encryption** field is dimmed, and you cannot select any options.

For the **Authentication** field, if **IKEv2 mode** was selected, choose **SHA-256**, **SHAT-384**, and **SHA-512** from the drop-down menu.

For all **Exchange** modes, enter a value for **Life Time (seconds)**. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

18. Click **Advanced**.



19. Select any of the optional settings you want to apply to your VPN policy. The options change depending on the options you selected in the **Proposals** screen.

Options	Main Mode or Aggressive Mode	KEv2 Mode
Advanced Settings		
Enable Keep Alive	Select to use heartbeat messages between peers on this VPN tunnel if one end of the tunnel fails, using a keep-alive heartbeat allows automatic renegotiation of the tunnel after both sides are available again without having to wait for the proposed Life Time to expire. NOTE: The Keep Alive option is disabled when the VPN policy is configured as a central gateway for DHCP over VPN or with a primary gateway name or address 0.0.0.0.	Cannot be selected for IKEv2 mode.
Suppress automatic Access Rules creation for VPN Policy	When not selected (default), accompanying Access Rules are created automatically.	When not selected (default), accompanying Access Rules are created automatically.
Disable IPsec Anti-Replay	Anti-replay is a form of partial sequence integrity, and it detects arrival of duplicate IP datagrams (within a constrained window).	Anti-replay is a form of partial sequence integrity, and it detects arrival of duplicate IP datagrams (within a constrained window).
Require authentication of VPN clients by XAUTH	Requires that all inbound traffic on this VPN policy is from a user authenticated by XAUTH/RADIUS. Unauthenticated traffic is not allowed on the VPN tunnel.	Not available in IKEv2 Mode.
Enable Windows Networking (NetBIOS) Broadcast	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.
Enable Multicast	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.
WXA Group	Select None (default) or Group One.	Select None (default) or Group One.
Display Suite B Compliant Algorithms Only	Select if you want to show only the Suite B compliant algorithms.	Select if you want to show only the Suite B compliant algorithms.

Options	Main Mode or Aggressive Mode	KEv2 Mode
Advanced Settings		
Apply NAT Policies	<p>Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a Translated Local Network or a Translated Remote Network or one of each from the two drop-down menus.</p> <p>NOTE: Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. Apply NAT Policies is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.</p>	<p>Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a Translated Local Network or a Translated Remote Network or one of each from the two drop-down menus.</p> <p>NOTE: Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. Apply NAT Policies is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.</p>
Management via this SA	Select any of HTTPS, SSH, or SNMP for this option to manage the local SonicWall firewall through the VPN tunnel.	Select any of HTTPS, SSH, or SNMP for this option to manage the local SonicWall firewall through the VPN tunnel.
User login via this SA	Select HTTP, HTTPS, or both to allow users to login using the SA. HTTP user login is not allowed with remote authentication.	Select HTTP, HTTPS, or both to allow users to login using the SA. HTTP user login is not allowed with remote authentication.
Default LAN Gateway (optional)	If you want to route traffic that is destined for an unknown subnet through a LAN before entering this tunnel, select this option. For example, if you selected Use this VPN Tunnel as a default route for all Internet traffic (on the Network screen, under Remote Networks) enter the router address.	If you want to route traffic that is destined for an unknown subnet through a LAN before entering this tunnel, select this option. For example, if you selected Use this VPN Tunnel as a default route for all Internet traffic (on the Network screen, under Remote Networks) enter the router address.

Options	Main Mode or Aggressive Mode	KEv2 Mode
Advanced Settings		
VPN Policy bound to	Select an interface or zone from the drop-down menu. Zone WAN is the preferred setting if you are using WAN load balancing and you want the VPN to use either WAN interface. Important: Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.	Select an interface or zone from the drop-down menu. Zone WAN is the preferred setting if you are using WAN load balancing and you want the VPN to use either WAN interface. Important: Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.
Preempt Secondary Gateway	To preempt a second gateway after a specified time, select this checkbox and configure the desired time in the Primary Gateway Detection Interval (seconds) option. The default time is 28800 seconds, or 8 hours.	To preempt a second gateway after a specified time, select this checkbox and configure the desired time in the Primary Gateway Detection Interval (seconds) option. The default time is 28800 seconds, or 8 hours.

Options	Main Mode or Aggressive Mode	KEv2 Mode
IKEV2 Settings		
Do not send trigger packet during IKE SA negotiation	Not available in Main or Aggressive modes.	Is not selected (default). Should only be selected when required for interoperability if the peer cannot handle trigger packets. The recommended practice is to include trigger packets to help the IKEv2 Responder select the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it might be appropriate to disable the inclusion of trigger packets to some IKE peers.
Accept Hash & URL Certificate Type	Not available in Main or Aggressive modes.	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, sends a message to the peer device saying that HTTP certification look-up is supported.

Options	Main Mode or Aggressive Mode	KEv2 Mode
IKEV2 Settings		
Send Hash & URL Certificate Type	Not available in Main or Aggressive modes.	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, responds to the message from the peer device and confirms HTTP certification look-up is supported.

- Click **OK**.
- Click **Accept** on the **NETWORK | IPSec VPN > Rules and Settings** page to update the VPN Policies.

Configuring IKE Using Third Party Certificates

NOTE: You must have a valid certificate from a third-party certificate authority installed on your SonicWall firewall before you can configure your VPN policy using a third-party IKE certificate.

With SonicWall firewalls, you can opt to use third-party certificates for authentication instead of the SonicWall Authentication Service. Using certificates from a third-party provider or using local certificates is a more manual process; therefore, experience with implementing Public Key Infrastructure (PKI) is necessary to understand the key components of digital certificates.

Reference identifiers are supported for SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), SAN: user FQDN, and Distinguished Name (DN). SAN takes precedence over CN.

The format of any Subject Distinguished Name is determined by the issuing Certification Authority. Common fields are Country (C=), Organization (O=), Organizational Unit (OU=), Common Name (CN=), Locality (L=), and vary with the issuing Certification Authority.

To create a VPN SA using IKE and third-party certificates::

- Navigate to **NETWORK | IPSec VPN > Rules and Settings**.
- Click **+Add** to create a new policy or click the **Edit** icon if you are updating an existing policy.

- In the **Authentication Method** field, select **IKE using 3rd Party Certificates**. The VPN policy window displays the third-party certificate options in the **IKE Authentication** section.

4. Type a name for the Security Association in the **Name** field.
5. Type the IP address or Fully Qualified Domain Name (FQDN) of the primary remote SonicWall in the **IPsec Primary Gateway Name or Address** field.
6. If you have a secondary remote SonicWall, enter the IP address or Fully Qualified Domain Name (FQDN) in the **IPsec Secondary Gateway Name or Address** field.
7. Under **IKE Authentication**, select a third-party certificate from the **Local Certificate** list. You must have imported local certificates before selecting this option.
8. For **Local IKE ID Type**, the default is **Default ID from Certificate**. Or, choose one of the following:
 - Distinguished Name (DN)
 - Email ID (UserFQDN)
 - Domain Name (FQDN)
 - IP Address (IPV4)

These alternate selections are the same as those for Peer IKE ID Type, described in the next step.

① | **NOTE:** SAN takes precedence over CN. The appliance does not guarantee unique identifiers.

① | **NOTE:** In NDPP mode, only certificates with a valid CA are available for selection.
9. From the **Peer IKE ID Type** drop-down menu, select one of the following **Peer ID** types:

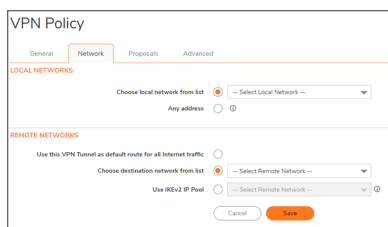
Peer IKE ID Type	
Option	Definition
Default ID from Certificate	Authentication is taken from the default ID on the certificate.
Distinguished Name (DN)	Authentication is based on the certificate's Subject Distinguished Name field, which is contained in all certificates by default. The entire Distinguished Name field must be entered for site-to-site VPNs. Wild card characters are not supported. The format of any Subject Distinguished Name is determined by the issuing Certificate Authority. Common fields are Country (C=), Organization (O=), Organizational Unit (OU=), Common Name (CN=), Locality (L=), and vary with the issuing Certificate Authority. The actual Subject Distinguished Name field in an X.509 Certificate is a binary object which must be converted to a string for matching purposes. The fields are separated by the forward slash character, for example: /C=US/O=SonicWall, Inc./OU=TechPubs/CN=Joe Pub.
Email ID (UserFQDN)	Authentication based on the Email ID (UserFQDN) types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate contains a Subject Alternative Name, that value must be used. For site-to-site VPNs, wild card characters cannot be used. The full value of the Email ID must be entered. This is because site-to-site VPNs are expected to connect to a single peer, whereas Group VPNs expect to connect to multiple peers.

Peer IKE ID Type

Option	Definition
Domain Name (FQDN)	Authentication based on the Domain Name (FQDN) types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate contains a Subject Alternative Name, that value must be used. For site-to-site VPNs, wild card characters cannot be used. The full value of the Domain Name must be entered because site to site VPNs are expected to connect to a single peer, whereas Group VPNs expect to connect to multiple peers.
IP Address (IPv4)	Based on the IPv4 IP address.

To find the certificate details (Subject Alternative Name, Distinguished Name, and so on), navigate to the **DEVICE | Settings > Certificates** page.

10. Type an ID string in the **Peer IKE ID** field.
11. Click **Network**.



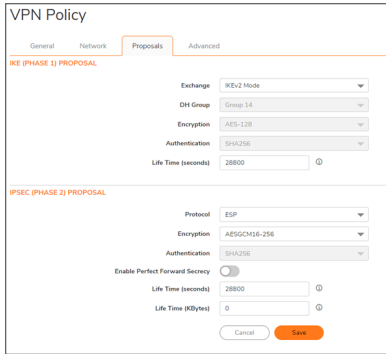
12. Under **Local Networks**, select one of the following:

Chose local network from lists	Select a network from the drop-down list if a specific network can access the VPN tunnel.
Any address	Use this option if traffic can originate from any local network or if a peer has Use this VPN tunnel as default route for all Internet traffic selected. Auto-added rules are created between Trusted Zones and the VPN Zone. ⓘ NOTE: DHCP over VPN is not supported with IKEv2.

13. Under Remote Networks, select one of the following:

Use this VPN Tunnel as default route for all Internet traffic	Select this option if traffic from any local user cannot leave the firewall unless it is encrypted. ⓘ NOTE: You can only configure one SA to use this setting.
Choose Destination network from list	Select a remote network from the drop-down list.
Use IKEv2 IP Pool	Select this option to support IKEv2 Config Payload and select the address object or IP Pool Network from the drop-down list.

14. Click **Proposals**.



15. Under **IKE (Phase 1) Proposal**, choose one of the following options from the **Exchange** drop-down menu:

Main Mode	Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
Aggressive Mode	Generally used when WAN addressing is dynamically assigned. Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
IKEv2 Mode	Causes all negotiation to happen through IKEv2 protocols, rather than using IKEv1 phase 1.

16. Under **IKE (Phase 1) Proposal**, set the values for the remaining options. The default values for **DH Group**, **Encryption**, **Authentication**, and **Life Time** are acceptable for most VPN configurations.

① | **NOTE:** If IKEv2 Mode is selected for the **Exchange** field, the **DH Group**, **Encryption**, and **Authentication** fields are dimmed and no selection can be made for those options.

① | **NOTE:** Be sure the Phase 1 values on the opposite side of the tunnel are configured to match.

For the DH Group, when in Main Mode or Aggressive Mode, you can select from several Diffie-Hellman exchanges:

Diffie-Hellman Groups Included in Suite B Cryptography	Other Diffie-Hellman Options
256-bit Random ECP Group	Group 1
384-bit Random ECP Group	Group 2
521-bit Random ECP Group	Group 5
192-bit Random ECP Group	Group 14
224-bit Random ECP Group	

For DH Group, when in **IKEv2 mode**, you can select from supports Group 14, 256-bit Random ECP Group (Group 19), 384-bit Random ECP Group (Group 20), and 521-bit Random ECP Group (Group 21). For the Encryption field, if **IKEv2 mode** was selected, choose AES-CBC-128, AES-CBC-192, and AES-CBC-256 from the drop-down menu.

For the Encryption field, if **Main Mode** or **Aggressive Mode** was selected, choose **3DES**, **DES-128 (default)**, **AES-192**, or **AES-256** from the drop-down menu.

For the Authentication field, if **Main Mode** or **Aggressive Mode** was selected, choose **SHA-1 (default)**, **MD5**, **SHA-256**, **SHA-384**, or **SHA-512** for enhanced authentication security.

For the Authentication field if **IKEv2** mode was selected, choose **SHA-256**, **SHA-384**, and **SHA-512** from the drop-down menu.

17. For all **Exchange** modes, enter a value for **Life Time (seconds)**. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.
18. Set the options in the **IPsec (Phase 2) Proposal** section. The default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, and **Life Time (seconds)** are acceptable for most VPN SA configurations. Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

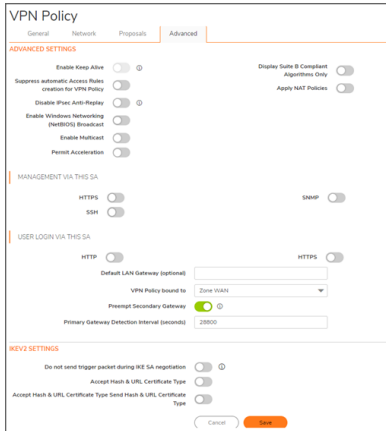
If you selected **ESP** in the **Protocol** field, you can select from six encryption algorithms in the **Encryption** field that are included in Suite B cryptography:

Suite B Cryptography Options	Other Options
AESGCM16-128	DES
AESGCM16-192	3DES
AESGCM16-256	AES-128
AESGMAC-128	AES-193
AESGMAC-192	AES-256
AESGMAC-256	None

If NDCPP compliance is enabled, then in the **Encryption** field you can select from AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, or AES-GCM-256. If you selected AH in the **Protocol** field, the **Encryption** field is dimmed, and you cannot select any options.

For the **Authentication** field if **IKEv2 mode** was selected, choose SHA-256, SHA-384, and SHA-512 from the drop-down menu.

19. For all Exchange modes, enter a value for **Life Time (seconds)**. The default setting of 28800 forces the tunnel to renegotiate and exchange keys every 8 hours.
20. Click **Advanced**.



21. Select any of the optional settings you want to apply to your VPN policy. The options change depending on the options you selected in the **Proposals** screen.

Options	Main Mode or Aggressive Mode	KEv2 Mode
Advanced Settings		
Enable Keep Alive	Select to use heartbeat messages between peers on this VPN tunnel if one end of the tunnel fails, using a keep-alive heartbeat allows automatic renegotiation of the tunnel after both sides are available again without having to wait for the proposed Life Time to expire.	Cannot be selected for IKEv2 mode.
	<p>i NOTE: The Keep Alive option is disabled when the VPN policy is configured as a central gateway for DHCP over VPN or with a primary gateway name or address 0.0.0.0.</p>	
Suppress automatic Access Rules creation for VPN Policy	When not selected (default), accompanying Access Rules are created automatically.	When not selected (default), accompanying Access Rules are created automatically.
Disable IPsec Anti-Replay	Anti-replay is a form of partial sequence integrity, and it detects arrival of duplicate IP datagrams (within a constrained window).	Anti-replay is a form of partial sequence integrity, and it detects arrival of duplicate IP datagrams (within a constrained window).
Require authentication of VPN clients by XAUTH	Requires that all inbound traffic on this VPN policy is from a user authenticated by XAUTH/RADIUS. Unauthenticated traffic is not allowed on the VPN tunnel.	Not available in IKEv2 Mode.

Options	Main Mode or Aggressive Mode	KEv2 Mode
Advanced Settings		
Enable Windows Networking (NetBIOS) Broadcast	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.
Enable Multicast	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.
WXA Group	Select None (default) or Group One .	Select None (default) or Group One .
Display Suite B Compliant Algorithms Only	Select if you want to show only the Suite B compliant algorithms.	Select if you want to show only the Suite B compliant algorithms.
Apply NAT Policies	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a Translated Local Network or a Translated Remote Network or one of each from the two drop-down menus.	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a Translated Local Network or a Translated Remote Network or one of each from the two drop-down menus.
	<p>NOTE: Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. Apply NAT Policies is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.</p>	<p>NOTE: Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. Apply NAT Policies is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.</p>
Management via this SA	Select any of HTTPS, SSH, or SNMP for this option to manage the local SonicWall firewall through the VPN tunnel.	Select any of HTTPS, SSH, or SNMP for this option to manage the local SonicWall firewall through the VPN tunnel.
User login via this SA	Select HTTP, HTTPS, or both to allow users to login using the SA. HTTP user login is not allowed with remote authentication.	Select HTTP, HTTPS, or both to allow users to login using the SA. HTTP user login is not allowed with remote authentication.

Options	Main Mode or Aggressive Mode	KEv2 Mode
Advanced Settings		
Default LAN Gateway (optional)	If you want to route traffic that is destined for an unknown subnet through a LAN before entering this tunnel, select this option. For example, if you selected Use this VPN Tunnel as a default route for all Internet traffic (on the Network screen, under Remote Networks) enter the router address.	If you want to route traffic that is destined for an unknown subnet through a LAN before entering this tunnel, select this option. For example, if you selected Use this VPN Tunnel as a default route for all Internet traffic (on the Network screen, under Remote Networks) enter the router address.
VPN Policy bound to	Select an interface or zone from the drop-down menu. Zone WAN is the preferred setting if you are using WAN load balancing and you want the VPN to use either WAN interface. Important: Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.	Select an interface or zone from the drop-down menu. Zone WAN is the preferred setting if you are using WAN load balancing and you want the VPN to use either WAN interface. Important: Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.
Preempt Secondary Gateway	To preempt a second gateway after a specified time, select this checkbox and configure the desired time in the Primary Gateway Detection Interval (seconds) option. The default time is 28800 seconds, or 8 hours.	To preempt a second gateway after a specified time, select this checkbox and configure the desired time in the Primary Gateway Detection Interval (seconds) option. The default time is 28800 seconds, or 8 hours.

Options	Main Mode or Aggressive Mode	KEv2 Mode
IKEV2 Settings		
Do not send trigger packet during IKE SA negotiation	Not available in Main or Aggressive modes.	Is not selected (default). Should only be selected when required for interoperability if the peer cannot handle trigger packets. The recommended practice is to include trigger packets to help the IKEv2 Responder select the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it might be appropriate to disable the inclusion of trigger packets to some IKE peers.

Options	Main Mode or Aggressive Mode	KEv2 Mode
IKEV2 Settings		
Accept Hash & URL Certificate Type	Not available in Main or Aggressive modes.	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, sends a message to the peer device saying that HTTP certification look-up is supported.
Send Hash & URL Certificate Type	Not available in Main or Aggressive modes.	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, responds to the message from the peer device and confirms HTTP certification look-up is supported.

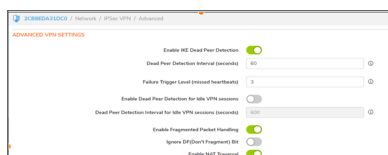
22. • Click **OK**.
23. • Click **Accept** on the **NETWORK | IPsec VPN > Rules and Settings** page to update the VPN Policies.

NAT Traversal

NAT Traversal, if enabled, automatically detects if network address translation (NAT) is being performed between the two VPN tunnel endpoints. Since this in-between NAT can interfere with IPsec/ESP traffic also, some routers that may exist between the VPN peers might be programmed to block IPsec pass-through, or have been programmed to block IP 50 (ESP).

To find NAT Traversal setting:

1. Login to SonicWall appliance.
2. Click **Network** in the top navigation menu.
3. Click **IPsec VPN > Advanced**.
4. Toggle the **Enable NAT Traversal** switch.

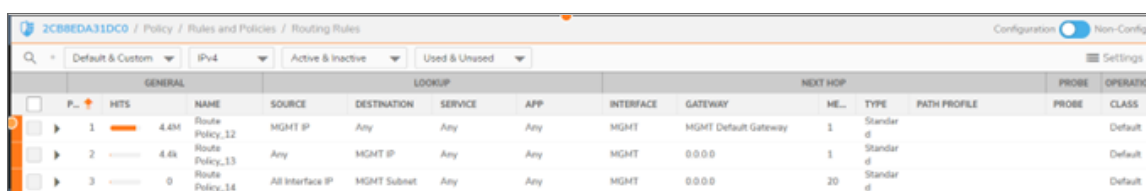


Configuring Routing Rules

If you have routers on your interfaces, you can configure the SonicWall appliance to route network traffic to specific predefined destinations. Static routes must be defined if the network connected to an interface is segmented into subnets, either for size or practical considerations.

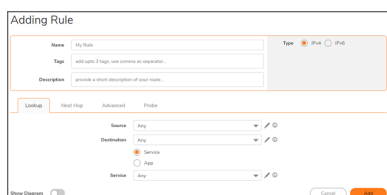
To add a static route:

1. Navigate to the **POLICY | Rules and Policies > Routing Rules** page.



GENERAL		LOOKUP				NEXT HOP			PROBE	OPERATION			
P...	HTS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	HE...	TYPE	PATH PROFILE	PROBE	CLASS
1	4.4k	Route Policy_12	MGMT IP	Any	Any	Any	MGMT	MGMT Default Gateway	1	Standard			Default
2	4.4k	Route Policy_13	Any	MGMT IP	Any	Any	MGMT	0.0.0.0	1	Standard			Default
3	0	Route Policy_14	All Interface IP	MGMT Subnet	Any	Any	MGMT	0.0.0.0	20	Standard			Default

2. Click **+Add** (in the bottom left corner). The Adding Rule dialog displays.



Adding Rule

Name: My Rule Type: IPv4

Type: add up to 3 tags, use comma as separator

Description: provide a short description of your rule.

Lookup | Next Hop | Advanced | Probe

Source: Any

Destination: Any

Service: Any

Show Diagram

Cancel Add

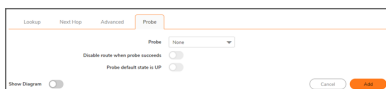
3. In the **Lookup** view, enter a friendly name for this route policy in **Name**.
4. Type any rule **Tags** that might aid in a search criteria. You can use up to three separated by commas.
5. Type a descriptive comment into the **Description** field.
6. Indicate the **Type** as **IPv4** or **IPv6**.
7. Select the source address object from **Source**.
8. Select the destination address object from **Destination**.
9. Specify the type of service object that is routed from **Service**.
10. Click **Add** or click to the **Next Hop** view to continue the configuration.



11. Choose the type of route:
 - Standard Route (default)
 - Multi-Path Route
 - SD-WAN Route
12. Select the interface through which these packets are routed from **Interface**.
13. Select the address object that acts as a gateway for packets matching these settings from **Gateway**.
14. Specify the RIP metric in the **Metric** field.
15. Click **Add** or click **Advanced** to continue the configuration.



16. Optionally, select **Disable route** when the interface is disconnected.
17. Select **Allow VPN path to take precedence** to allow a matching VPN network to take precedence over the static route when the VPN tunnel is up. This option is not selected by default.
18. Enter the ToS hexadecimal value in the **TOS (Hex)** field.
19. Enter the ToS Mask hexadecimal value in the **TOS Mask (Hex)** field.
20. Enter a value for the **Admin Distance**, or select **Auto** for an automatically created **Admin Distance**.
21. Click **Add** or click the **Probe** tab to continue the configuration.



22. Select a probe type from **Probe**. The default is **None**. If a probe type is selected additional options become available.
23. Select **Disable route when probe succeeds**. This option is not selected by default.
24. Select **Probe default state is UP**.
25. When you are finished, click **Add**. The route settings are configured for the selected SonicWall appliance (s).

Firewall

This section provides an overview of the SonicWall network security appliance default access rules and custom access rules. Access rules are network management tools that allow you to define inbound and outbound access policies, configure user authentication, and enable remote management of your firewall. This section provides configuration examples to customize your access rules to meet your business requirements.

P	HITS	NAME	ACTION	SOURCE	DESTINATION	SOURCE	DESTINATION	SERVICE	USER INCL.	USER EXCL.	SCHEDULE
1 (M)	0	X3-X4_allowall_1	✓	LAN	WAN	X3 Subnet	X4 Subnet	Any	All	None	Always
2 (M)	0	x4-x3_allowall_2	✓	WAN	LAN	X4 Subnet	X3 Subnet	Any	All	None	Always
3 (M)	0	Default Access Rule_619	✓	VPN	LAN	Any	All Interface IP	SonicpointN Layer3 Management	All	None	Always
4 (M)	0	Default Access Rule_3	✓	VPN	LAN	Any	All Interface IP	Source Quench	All	None	Always
5 (M)	0	Default Access Rule_4	✓	VPN	LAN	Any	All Interface IP	Squid	All	None	Always
6 (M)	0	Default Access Rule_5	✓	VPN	LAN	Any	All Interface IP	Src Address Failed Ingress Egress	All	None	Always
7 (A)	100	Default Access Rule_6	✓	LAN	LAN	X0 IP	Any	IKE	All	None	Always
8 (A)	144	Default Access Rule_7	✓	LAN	LAN	Any	X0 IP	IKE	All	None	Always
9 (M)	0	Default Access Rule_8	✓	LAN	LAN	Any	All X3 Management IP	Ping	All	None	Always
10 (M)	0	Default Access Rule_9	✓	WAN	WAN	Any	Any	Any	All	None	Always
11 (M)	0	Default Access Rule_10	✓	VPN	LAN	Any	All Interface IP	Streaming media	All	None	Always

Access Rules

Access rules are network management tools that allow you to define ingress and egress access policy, configure user authentication, and enable remote management of the SonicWall security appliance. Rules may be applied to various types of traffic including:

- Internet Control Message Protocol version 4 (ICMPv4) (Type, Code): RFC 792
- Internet Control Message Protocol version 6 (ICMPv6) (Type, Code): RFC 4443
- Internet Protocol (IPv4) (Source Address, Destination Address, Transport Layer Protocol): RFC 791,
- Internet Protocol version 6 (IPv6) (Source Address, Destination Address, Transport Layer Protocol): RFC 2460

- Transmission Control Protocol (TCP) (Source Port, Destination Port): RFC 793
- User Datagram Protocol (UDP) (Source Port, Destination Port): RFC 768.

The **Policy | Rules and Policies > Access Rules** page provides a sortable access rule management interface (see above). The subsequent sections provide high-level overviews on configuring access rules by zones and configuring bandwidth management using access rules.

The rules are categorized into separate tables for each source zone to destination zone and for IPv4/IPv6. Thus, all the priority types only apply within the rule table to which the rule belongs.

About Stateful Packet Inspection Default Access

By default, the SonicWall network security appliance's stateful packet inspection allows all communication from the LAN to the Internet and blocks all traffic to the LAN from the Internet. The following behaviors are defined by the Default stateful inspection packet access rule enabled on the SonicWall network security appliance:

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

Additional network access rules can be defined to extend or override the default access rules. address or, access rules can be created that allow access from the LAN zone to the WAN Primary IP address, or block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

Custom access rules evaluate network traffic source IP addresses, destination IP addresses, IP protocol types, and compare the information to access rules created on the SonicWall security appliance. Network access rules take precedence and can override the SonicWall security appliance's stateful packet inspection. For example, an access rule that blocks IRC traffic takes precedence over the SonicWall security appliance default setting of allowing this type of traffic.

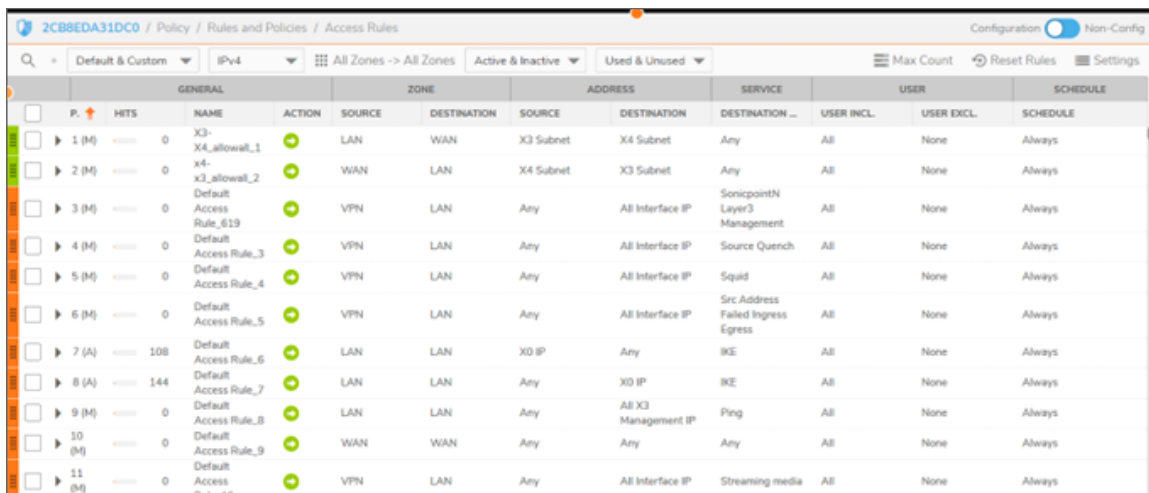
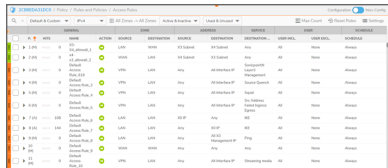
SonicOS monitors the initiation sequence, typically a TCP three-way handshake, and records the packet's state: open, established, or closed. Each packet transferred across the network is examined, and its headers and flags are compared against the state table. If the packet is part of an existing, approved connection, it is allowed to pass. If not, the stateful inspection firewall consults its rule set to determine the appropriate action.

Configuring Access Rules for a Zone

To configure rules, the service or service group that the rule applies to must first be defined. If it is not, you can define the service or service group and then create one or more rules for it.

The following sections describe how to add, modify, reset to defaults, or delete firewall rules for firewall appliances running SonicOS.

To display the Access Rules for a specific zone, select a zone from the Matrix or from Zone (Source/Destination).



GENERAL	ZONE	ADDRESS	SERVICE	USER	SCHEDULE						
P.	HITS	NAME	ACTION	SOURCE	DESTINATION	SOURCE	DESTINATION	DESTINATION ...	USER INCL.	USER EXCL.	SCHEDULE
1 (M)	0	X3-X4_allowat_1	Allow	LAN	WAN	X3 Subnet	X4 Subnet	Any	All	None	Always
2 (M)	0	x4-x3_allowat_2	Allow	WAN	LAN	X4 Subnet	X3 Subnet	Any	All	None	Always
3 (M)	0	Default Access Rule_619	Allow	VPN	LAN	Any	All Interface IP	SonicpointN Layer3 Management	All	None	Always
4 (M)	0	Default Access Rule_3	Allow	VPN	LAN	Any	All Interface IP	Source Quench	All	None	Always
5 (M)	0	Default Access Rule_4	Allow	VPN	LAN	Any	All Interface IP	Squid	All	None	Always
6 (M)	0	Default Access Rule_5	Allow	VPN	LAN	Any	All Interface IP	Src Address Failed Ingress Egress	All	None	Always
7 (A)	108	Default Access Rule_6	Allow	LAN	LAN	X0 IP	Any	IKE	All	None	Always
8 (A)	144	Default Access Rule_7	Allow	LAN	LAN	Any	X0 IP	IKE	All	None	Always
9 (M)	0	Default Access Rule_8	Allow	LAN	LAN	Any	All X3 Management IP	Ping	All	None	Always
10 (M)	0	Default Access Rule_9	Allow	WAN	WAN	Any	Any	Any	All	None	Always
11 (M)	0	Default Access Rule_10	Allow	VPN	LAN	Any	All Interface IP	Streaming media	All	None	Always

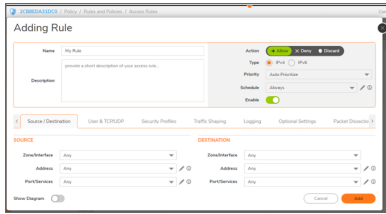
The access rules are sorted from the most specific at the top, to less specific at the bottom of the table. At the bottom of the table is the **Any** rule. The default access rule is all IP services except those listed in the **Access Rules** page. Access rules can be created to override the behavior of the **Any** rule; for example, the **Any** rule allows users on the LAN to access all Internet services, including NNTP News.

① **NOTE:** If the **Delete** or **Edit** icons are dimmed (unavailable), the access rule cannot be changed or deleted from the list.

Adding Access Rules

To add Access Rules:

1. Navigate to **Policy | Rules and Policies > Access Rules**.
2. Click on **Add**. The **Add Rule** dialog displays.



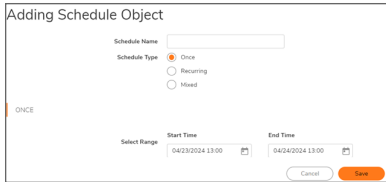
3. In the **Name** field, add or edit the **My Rule Name**.
4. You can provide a short description of your access rule in the **Description**.
5. Select an **Action**, that is, how the rule processes (permits or blocks) the specified IP traffic:
 - **Allow** (default): As long as the **Enable** option is selected, your access rule is active and permits the traffic.
 - **Deny**: The firewall denies all connections matching this rule and blocks the page specified and the action profile is served for web traffic. The firewall also resets the connections on both sides.
 - **Discard**: Firewall silently drops any packets matching this rule.
6. Select IP address **Type** IPv4 or IPv6.
7. Set your access rule's **Priority**. You can choose to **Auto Prioritize**, **Insert at the End**, or a **Manual** priority for your access rule.

NOTE: Higher numbers indicate lower priority. The lowest priority rule is the final/default rule applied to matching traffic (traffic matching the defined attributes) when no higher priority rules apply. Lower priority rules should be more general than rules with higher priorities. If a higher priority rule does not match all the attributes, then the next rule is evaluated to see if it applies, all the way down the list of rules. Rules with more specific matching attributes need to be set at a higher priority or else a more general rule could match before that specific rule is evaluated.

When you add a new Access Rule, the rule module decides where to place it in the Access Rule table. The rule module uses an Auto Prioritize algorithm that places the most specific rules at the top. The only way to change the priority is to manually edit the rule and then provide the index of where to place it. Finding the rule in a large table to edit it can be difficult.

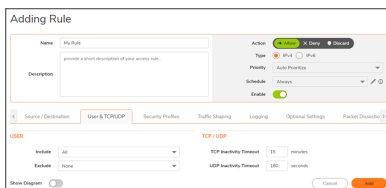
The User Priority for Access Rules provides two choices for the priority types of the new rule:

- **Auto Prioritize**, which uses the Auto Prioritize algorithm that places the most specific rules on the top of the Access Rules table. This is the default choice.
 - **Insert at the end**, which indicates to the rule module to place the rule at the end of the Access Rules table, and as a result, makes the new rule easy to locate regardless of the size of the table.
8. Specify when the rule is applied by selecting a schedule from the **Schedule** drop-down menu. If the rule is always applied, select **Always**. If the schedule you want is not listed in the drop-down menu, click the pencil icon to the right of the menu and create a **New Schedule Object**. The **Adding Schedule Object** dialog appears.

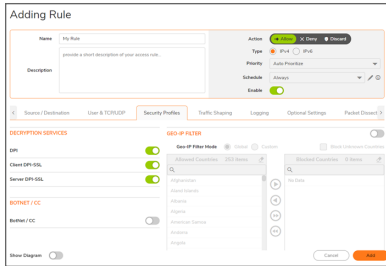


In SonicOS, schedules in access rules determine when a specific rule is applied. If traffic is received during the scheduled time, the access rule becomes active and allows the traffic to pass. However, if the traffic is received outside the scheduled time, the access rule is not active, and the traffic will be blocked or handled by default rules.

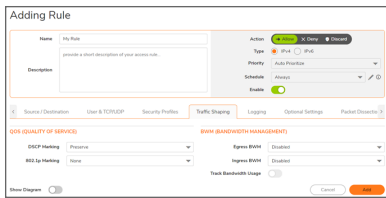
9. Select the source and destination **Zone/Interface** from the drop-down menus.
10. Select from the Predefined zones WAN, LAN, DMZ, VPN, MULTICAST, WLAN, and SSLVPN. In addition to predefined zones, custom user-friendly zones can also be configured in SonicOS, with different security types.
11. Select an interface from the range X0–X33.
 - ① | **NOTE:** The number of physical interfaces varies depending on the firewall model.
12. Specify the **source** and **destination address** through the drop down, which lists the custom and default address objects created.
 - ① | **NOTE:** The appliance supports both single IP addresses and ranges of IP addresses.
13. Specify the **source** and **destination services/ports** for the ingress and egress traffic, by default we can keep the source service as any and keep the destination port configured.
14. Specify if this rule applies to all users or to an individual user or group in the **Users include** and **Exclude** option.



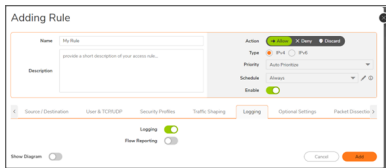
15. Specify how long (in minutes) TCP connections might remain idle before the connection is terminated in the **TCP Connectivity Inactivity Timeout** field.
16. Specify how long (in seconds) UDP connections might remain idle before the connection is terminated in the **UDP Connectivity Inactivity Timeout** field.
17. Configure the security profiles on the access rules which includes enabling/disabling the Client DPI-SSL and Server DPI-SSL services, Botnet/cc and Geo-IP based on firewall rule connections.



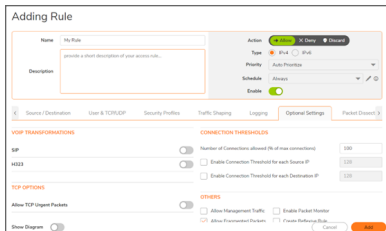
18. Configure Egress and Ingress bandwidth on the firewall access rules for the specific source, destination, and services.



19. To track bandwidth usage for this service, select **Enable Track Bandwidth Usage**.
20. To enable logging for this rule select **Logging**.



21. Specify the percentage of the maximum connections this rule is to allow in the **Number of connections allowed (% of maximum connections)** field.

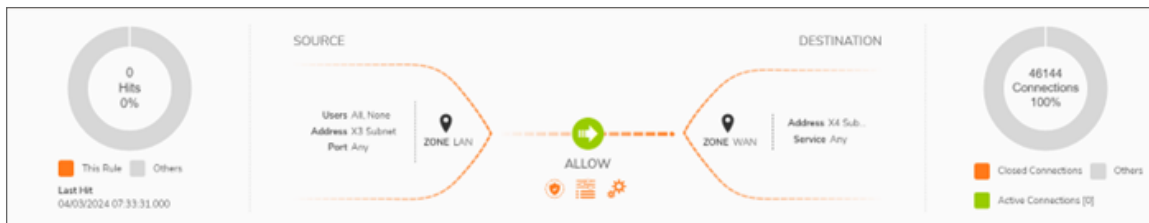


22. Set a limit for the maximum number of connections allowed per source IP Address by selecting Enable connection limit for each Source IP Address and entering the value in the Threshold field. This is only available for Allow rules.
23. Set a limit for the maximum number of connections allowed per destination IP Address by selecting the Enable connection limit for each Destination IP Address field and entering the value in the Threshold field. (Only available for Allow rules).
24. Before adding the rule consider the following:
 - You can enable fragmented packets on the access rule as well as allow management traffic over the access rule.

- The Packet Dissection Filter allows you to set up rules based on deep packet inspection (DPI). It can analyze not only basic attributes like IP and port but also elements like specific application protocols or encrypted traffic. By integrating Packet Dissection Objects with access rules, this feature provides the ability to inspect traffic before allowing or denying it based on security policies.
- When a PDF object configured with negative matching is applied to a rule, the behavior depends on the Access rule action. If the Access rule action is "allow," packets that match the PDF object are rejected, while all other traffic is allowed. Conversely, if the Access rule action is "deny," all traffic, including packets that match the PDF object, is denied.

25. Click **Add** when finished.

The access rules can also show the diagram flow of the rule created:

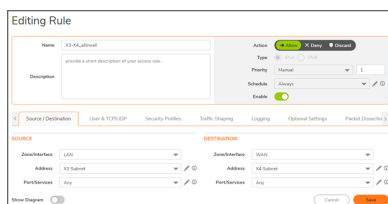


The appliance supports all the IPv4 and IPv6 protocols mentioned in [Protocol Numbers by Iana](#).

Editing Access Rules

To edit an access rule:

1. Navigate to **Policy | Rules and Policies | Access Rules**.
2. Click the **Edit** icon of the access rule. The Edit Rule dialog has the same settings as the Add Rule dialog.



3. Make changes and click on **Save**.

Deleting a Custom Access Rule

To delete a Custom Access Rule:

- To delete an individual custom access rule, click its **Delete** icon.
- To delete selected custom access rules, click their checkboxes, and then click the **Delete** button. This

button is dimmed until a custom access rule checkbox is selected.

- To delete all custom access rules, click the **Delete All** button.

Default Deny Rule

In the evaluated configuration, a deny rule applied to any interface, any zone, and for any traffic with the lowest priority must be created. This ensures that any traffic that does not match a configured rule will be denied.

Reconnection

If an IPsec tunnel loses connectivity, no additional administrative actions are required. The tunnel will attempt to restart automatically. Plaintext data will never be sent.

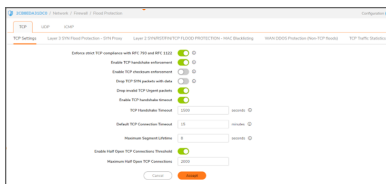
TCP Connection

The appliance tracks and maintains information relating to the number of half-open TCP connections as follows:

- There is an administratively defined limit for half-open TCP connections based on:
 - TCP Handshake Timeout (seconds)
 - Maximum Half Open TCP Connections
- There is a TCP Handshake Timeout (seconds)
 - Each half-open TCP connection is removed if the handshake is not complete by the time this timeout is reached.
- There is a maximum number of allowable Half Open TCP Connections.

To change TCP settings:

1. Navigate to **Network | Firewall | Flood Protection**.



2. Adjust settings as needed.
 - Enforce strict TCP compliance with RFC 793 and RFC 1122 – This setting ensures strict compliance with several TCP timeout rules. This setting maximizes TCP security, but it might cause problems with the Window Scaling feature for Windows Vista users. This option is not selected by default.

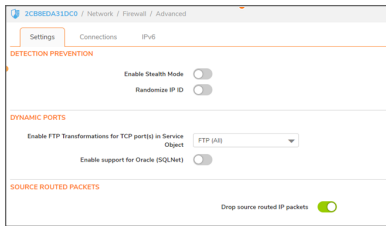
- Enable TCP handshake enforcement – This option requires a successful three-way TCP handshake for all TCP connections. It is available only if the Enforce strict TCP compliance with RFC 793 and RFC 1122, is selected.
- Enable TCP checksum enforcement – If an invalid TCP checksum is calculated, the packet is dropped. This option is not selected by default.
- Drop TCP SYN packets with data - This option allows the system to drop TCP SYN packets with data. This option is not selected by default.
- Drop invalid TCP Urgent packets - This option allows the system to drop invalid TCP urgent packets. This option is selected by default.
- Enable TCP handshake timeout – This selection enforces the timeout period (in seconds) for a three-way TCP handshake to complete its connection. If the three-way TCP handshake does not complete in the timeout period, it is dropped. This option is selected by default.
- TCP Handshake Timeout – This is the maximum time a TCP handshake has to complete the connection. The default is 30 seconds. This option is only available if Enable TCP Handshake Timeout is selected.
- Default TCP Connection Timeout – This is the time assigned to Access Rules for TCP traffic. If a TCP session is active for a period in excess of this setting, the TCP connection is cleared by the firewall. The default value is 15 minutes, the minimum value is 1 minute, and the maximum value is 999 minutes.
 - ① **NOTE:** Setting an excessively long connection time-out slows the reclamation of stale resources, and in extreme cases, could lead to exhaustion of the connection cache.
- Maximum Segment Lifetime – This setting determines the number of seconds that any TCP packet is valid before it expires. This setting is also used to determine the amount of time (calculated as twice the Maximum Segment Lifetime, or 2MSL) that an actively closed TCP connection remains in the TIME_WAIT state to ensure that the proper FIN / ACK exchange has occurred to cleanly close the TCP connection. The default value is 8 seconds, the minimum value is 1 second, and the maximum value is 60 seconds.
- Enable Half Open TCP Connections Threshold – This option denies new TCP connections if the threshold of TCP half-open connections has been reached. By default, the half-open TCP connection is not monitored, so this option is not selected by default.
- Maximum Half Open TCP Connections – This option specifies the maximum number of half-open TCP connections. The default maximum is half the number of maximum connection caches. It is only available if the Enable Half Open TCP Connections Threshold is selected.

3. Click on **Accept**.

Source Routed Packets

1. Navigate to **Network | Firewall > Advanced**.
2. Clear the check box for **Drop Source Routed IP Packets** (enabled by default) if you are testing traffic

between two specific hosts and you are using source routing.



Intrusion Protection

SonicWall Intrusion Prevention Service (SonicWall IPS) delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS. SonicWall IPS is designed to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and backdoor exploits. The extensible signature language used in SonicWall's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. SonicWall IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks through SonicWall's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWall IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

The appliance analyzes traffic based on IP address, port, and interface. By default, traffic is first analyzed against the anomaly-based rules and then against the signature-based rules.

Intrusion Prevention Service (IPS) is configured on the **Policy | Security Services > Intrusion Prevention** page.

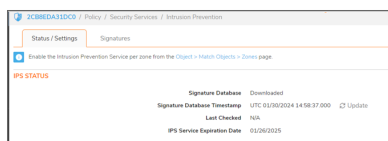
Deep Packet Inspection

Deep Packet Inspection looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds the anomalies in the traffic and reacts to it, preventing the traffic from passing through. Deep Packet Inspection is a technology that allows a SonicWall Security Appliance to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the SonicWall Security Appliance, as well as prevent them (i.e. dropping the packet or resetting the TCP connection). SonicWall's Deep Packet Inspection technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred.

IPS Status

The **IPS Status** panel displays status information for the signature database and your IPS license.

1. Navigate to **Policy | Security Services | Intrusion Prevention > Status/Setting**.



The IPS Status panel displays the following information:

- Signature Database indicates whether the signature database is being downloaded, has been downloaded, or needs to be downloaded. The signature database is updated automatically about once an hour. You can also manually update your IPS database at any time by clicking the Update button located in the IPS Status section.
- Signature Database Timestamp displays the last update to the IPS signature database, not the last update to your SonicWALL security appliance.
- Last Checked indicates the last time the SonicWALL security appliance checked the signature database for updates. The SonicWALL security appliance automatically attempts to synchronize the database on startup, and once every hour.
- IPS Service Expiration Date indicates the date when the IPS service expires. If your IPS subscription expires, the SonicWALL IPS inspection is stopped and the IPS configuration settings are removed from the SonicWALL security appliance. After renewing your IPS license, these settings are automatically restored to the previously configured state.
- Enable the Intrusion Prevention Service per zone from the Network > Zones page.

IPS Global Settings

The IPS Global Settings panel provides the key settings for enabling IPS on your firewall.

To enable IPS:

1. Navigate to **Policy | Security Services | Intrusion Prevention**.
2. Go to the **IPS Global Settings** panel.



3. Select **Enable IPS**.
4. Select the action that you want (**Prevent All**, **Detect All**, or both) for each of the Signature Groups:
 - High Priority Attacks—These attacks are the most dangerous to your network. They can take down your entire network or disable servers, such as various Backdoor, DDoS, and DOS attacks.
 - Medium Priority Attack—These attacks can cause disruption to your network, such as increased network traffic that slows down performance. For example, various DNS, FTP, and Telnet attacks.
 - Low Priority Attacks—These attacks are characterized more as informational events, such as various Scan, RPC, and SMTP attacks.

- Log Redundancy Filter—The Log Redundancy Filter (seconds) field allows you to define the time in seconds that the same attack is logged as a single entry in the SonicWall log. Various attacks are often rapidly repeated, which can quickly fill up a log if each attack is logged. The default 60 seconds entry for Low Priority Attacks in the Log Redundancy Filter (seconds) field is recommended because the relatively high volume of these types of signature triggers. You can view and manage the SonicWall log events by clicking on the Log button in the Management Interface. The **Log > View** page displays the log contents.

5. Click on **Accept**.

Detection vs Prevention

SonicWall IPS provides two methods for managing global attack threats: detection (Detect All) and prevention (Prevent All). You must specify a Prevent All action in the Signature Groups table for intrusion prevention to occur on the SonicWall security appliance.

If **Prevent All** is enabled for a signature group in the IPS Settings table, the SonicWall security appliance automatically drops and resets the connection, to prevent the traffic from reaching its destination.

If **Detect All** is enabled for a signature group in the Signature Groups table, the SonicWall security appliance logs and alerts any traffic that matches any signature in the group, but does not take any action against the traffic. The connection proceeds to its intended destination.

#	CATEGORY	NAME	ID	GID	PREVENT	DETECT
1	BACKDOOR	Compromised Host Backdoor Traffic 1	14	608510	✓	✓
2	BACKDOOR	Q Backdoor IOC (ICMP)	49	708318	✓	✓
3	BACKDOOR	Back Orifice Remote Login 1	1116	708306	✓	✓
4	BACKDOOR	HP SiteScope Administration Interface Backdoor Account Login 1	1843	707868	✓	✓
5	BACKDOOR	FireEye RUBEUS nonce 2 IOC TCP	2007	707902	✓	✓
6	BACKDOOR	FireEye RUBEUS nonce 2 IOC UDP	2009	707903	✓	✓
7	BACKDOOR	zerodium Backdoor IOC	2040	743246	✓	✓
8	BACKDOOR	HLIGHT Trojan IOC	2089	708160	✓	✓
9	BACKDOOR	SessionManager Cookie Header IOC	2987	716245	✓	✓
10	BACKDOOR	Wervely Backdoor IOC 1	3069	743441	✓	✓

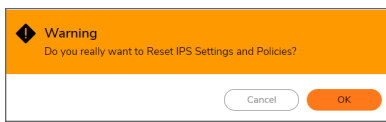
Resetting the IPS Settings and Policies

To reset IPS setting and policies:

1. Navigate to **Policy | Security Services | Intrusion Prevention**.
2. Go to the **IPS Global Settings** and click on **Reset**.



The following warning message will be displayed:



3. Click on **OK**.

Configuring IPS Protection on Zones

You apply SonicWall IPS to zones on the **Object | Zones** page to enforce SonicWall IPS not only between each network zone and the WAN, but also between internal zones.

To enable SonicWall on a zone:

1. Go to **Object | Match Object | Zones** or go to the **IPS Status** section on **Policy | Security Service | Intrusion Prevention | Status/Setting** and click the **Enable the Intrusion Prevention Service per zone** from the **Object > Match Objects > Zones** page.
2. Click the **Edit** icon for the zone you want to apply SonicWall IPS. The **Edit Zone** window is displayed.
3. Click the **Enable IPS** checkbox. A checkmark appears. To disable SonicWALL IPS, clear the box.

Zone Settings

General
Guest Services
Wireless
Radius Server

GENERAL SETTINGS

Name

Security Type

Allow Interface Trust

Auto-generate Access Rules to allow traffic between zones of the same trust level

Auto-generate Access Rules to allow traffic to zones with lower trust level

Auto-generate Access Rules to allow traffic from zones with higher trust level

Auto-generate Access Rules to deny traffic from zones with lower trust level

Enable SSLVPN Access

Enable SSL Control

Create Group VPN

Enable Gateway Anti-Virus Service

Enable IPS

Enable Anti-Spyware Service

Enable App Control Service

Enable SSL Client Inspection

Enable SSL Server Inspection

4. Click **Save**.

Signatures

All the entries listed in the IPS Policies table are from the SonicWall IPS signature database downloaded to your SonicWall security appliance. Categories and signatures are dynamically updated by the SonicWall Intrusion Prevention Service. Categories and signatures dynamically change over time in response to new threats.

Administrators can configure the IPS data analysis by selecting signatures from a pre-loaded list or by creating custom signatures. Custom Signatures are created using a combination of Application and Access rules. If a signature calls for matching L3/L4 header content, the Packet Dissection Filter can be used in conjunction with the rules. If the signature calls for application layer header/data matching, the application rules can be created with custom policy and match objects to match the desired offset in the application layer header or payload. The IPS data analysis configuration options provide the ability to deploy selections globally to either all WAN or all LAN interfaces.

To view Signatures:

1. Navigate to **Policy | Security Services | Intrusion Prevention**.
2. Under **Signatures** tab you can view and manage IPS signatures by category groups or on a signature-by-signature basis. Categories are signatures grouped together based on the type of attack, and they are listed in the **Category** menu.

#	CATEGORY	NAME	ID	GID	PREVENT	DETECT	PRIORITY
1	BACKDOOR	Compromised Host Backdoor Traffic 1	14	688510	✓	✓	3/5
2	BACKDOOR	Q Backdoor IOC (ICMP)	49	708318	✓	✓	3/5
3	BACKDOOR	Back Office Remote Login 1	1116	708306	✓	✓	3/5
4	BACKDOOR	HP SiteScope Administration Interface Backdoor Account Login 1	1843	707868	✓	✓	3/5
5	BACKDOOR	FireEye RUBEUS nonce 2 IOC TCP	2007	707902	✓	✓	3/5
6	BACKDOOR	FireEye RUBEUS nonce 2 IOC UDP	2009	707903	✓	✓	3/5
7	BACKDOOR	zerodium Backdoor IOC	2040	743246	✓	✓	3/5
8	BACKDOOR	HIGHLIGHT Trojan IOC	2089	708160	✓	✓	3/5
9	BACKDOOR	SessionManager Cookie Header IOC	2987	716245	✓	✓	2/5
10	BACKDOOR	Weeveety Backdoor IOC 1	3069	743441	✓	✓	3/5
11	BACKDOOR	Weeveety Backdoor IOC 2	3101	743444	✓	✓	3/5
12	BACKDOOR	Weeveety Backdoor IOC 3	3120	743445	✓	✓	3/5

3. Select all categories or an individual category from the **Category** menu. Or enter the Signature ID (SID) or signature name in the search box.
4. To change any settings for individual signature or category, click on the **Edit** icon that appears when you hover the mouse over respective signature or category.
5. To view additional signature information, click on the signature directly.

App Rules

App Rules provide a solution for setting policy rules for application signatures. As a set of application-specific policies, App Rules provide you with granular control over network traffic on the level of users, email addresses, schedules, and IP-subnets. The primary functionality of this application-layer access control feature is to regulate Web browsing, file transfer, email, and email attachments.

To configure App Rules:

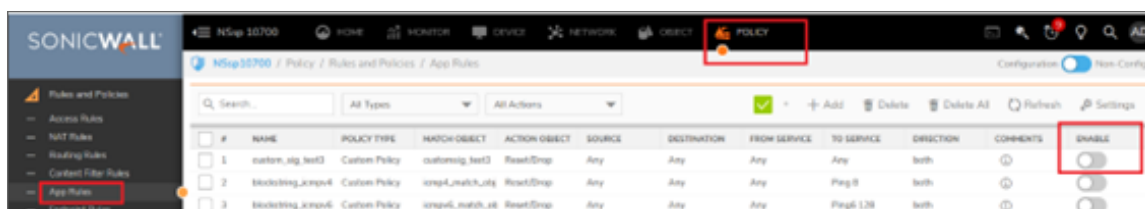
1. Navigate to **Policy | Rules and Policies | App Rules**.
2. Click on **Add**. Add App Rule dialog displays.

3. Enter a descriptive name in the **Policy Name** field.

4. Select a **Policy Type** from the drop-down menu. Your selection here affects the options available in the dialog.
5. Select the **Address Source** and **Address Destination** from the drop-down menu.
6. Select the **Service Source** and **Service Destination** from the drop-down menu.
7. For **Exclusion Address**, optionally select an **Address Group** or **Address Object** from the drop-down menu. This address is not affected by the policy.
8. For **Exclusion Service**, optionally select a **Service Group** or **Service Object** from the drop-down menu. This address is not affected by the policy.
9. For **Match Object Included**, select a match object from the drop-down menu containing the defined match objects applicable to the policy type.
10. For **Match Object Excluded**, select the match object from the drop-down. The excluded match object provides the ability to differentiate subdomains in the policy.
 - ① **NOTE:** The Excluded Match Object does not take effect when the match object type is set to Custom Object. Custom Objects cannot be selected as the Exclusion Match Object.
11. For **Action Object**, select an action from the drop-down menu containing actions applicable to the policy type, and can include predefined actions plus any customized actions. The default for all policy types, except CFS, is **Reset/Drop**; the default for CFS is **No Action**.
12. For **Users/Groups**, select from the drop-down menus for both **Included** and **Excluded**. The selected users or group under **Excluded** are not affected by the policy.
13. For **Schedule**, select from the drop-down menu, which contains a variety of schedules for the policy to be in effect. Specifying a schedule other than the default, **Always On**, turns on the rule only during the scheduled time.
14. If you want the policy to create a flow reporting when a match is found, select the **Enable Flow Reporting** checkbox.
15. If you want the policy to create a log entry when a match is found, select the **Enable Logging** checkbox.
16. To record more details in the log, select the **Log individual object content** checkbox.
17. If the policy type is **IPS Content**, select the **Log using IPS message format** checkbox to display the category in the log entry as **Intrusion Prevention** rather than **Application Control**, and to use a prefix such as **IPS Detection Alert** in the log message rather than **Application Control Alert**. This is useful if you want to use log filters to search for IPS alerts.
18. If the policy type is **App Control Content**, select the **Log using App Control message format** checkbox to display the category in the log entry as **Application Control**, and to use a prefix such as **Application Control Detection Alert** in the log message. This is useful if you want to use log filters to search for **Application Control** alerts.
19. If the policy type is **CFS**, select the **Log using CFS message format** checkbox to display the category in the log entry as **Network Access**, and to use a log message such as website access denied in the log message rather than no prefix. This is useful if you want to use log filters to search for content filtering alerts.

20. For **Log Redundancy Filter**, you can select **Global Settings** to use the global value, or you can enter a number of seconds to delay between each log entry for this policy. The local setting overrides the global setting only for this policy; other policies are not affected.
21. For **Direction**, click either **Basic** or **Advanced** and select a direction from the drop-down menu. **Basic** allows you to select incoming, outgoing, or both. **Advanced** allows you to select between zones, such as LAN to WAN. **IPS Content**, **App Control Content**, or **CFS** policy types do not provide this configuration option.
22. If the policy type is **IPS Content**, **App Control Content**, or **CFS**, select a zone from the **Zone** drop-down menu. The policy is applied to this zone.
23. Click **OK**.

Once the APP rule is configured, it is automatically enabled. You can manually enable or disable the APP rule. Navigate to **Policy | Rules and Policies > App Rules** and click on the **Enable** option.

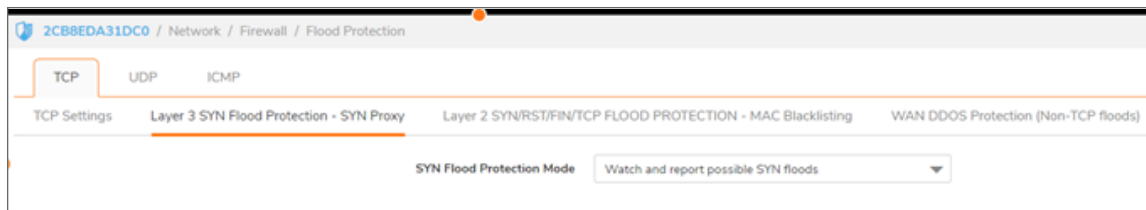


SYN Flood Protection

A SYN Flood Protection mode is the level of protection that you can select to protect your network against half-opened TCP sessions and high frequency SYN packet transmissions.

To enable SYN flood Protection:

1. Navigate to **Network | Firewall**.
2. Go to **TCP > Layer 3 SYN Flood Protection- SYN Proxy** tab.



3. In the **SYN Flood Protection Mode** drop-down menu, select a protection mode.
 - **Watch and Report Possible SYN Floods** – The device monitors SYN traffic on all interfaces and logs suspected SYN flood activity that exceeds a packet-count threshold. This option does not actually turn on the SYN Proxy on the device, so the device forwards the TCP three-way handshake without modification.

This is the least invasive level of SYN Flood protection. Select this option if your network is not in a high-risk environment.

- **Proxy WAN Client Connections When Attack is Suspected** – The device enables the SYN Proxy feature on WAN interfaces when the number of incomplete connection attempts per second exceeds a specified threshold. This method ensures that the device continues to process valid traffic during the attack, and that performance does not degrade. Proxy mode remains enabled until all WAN SYN flood attacks stop occurring, or until the device blacklists all of them using the SYN Blacklisting feature.

This is the intermediate level of SYN Flood protection. Select this option if your network sometimes experiences SYN Flood attacks from internal or external sources.

- **Always Proxy WAN Client Connections** – This option sets the device to always use SYN Proxy. This method blocks all spoofed SYN packets from passing through the device. This is an extreme security measure, which directs the device to respond to port scans on all TCP ports. The SYN Proxy feature forces the device to respond to all TCP SYN connection attempts, which can degrade performance and generate false positive results. Select this option only if your network is in a high-risk environment.
- **SYN ATTACK THRESHOLD** – Select the SYN Attack Threshold configuration options to provide limits for SYN Flood activity before the device drops packets. The device gathers statistics on WAN TCP connections, keeping track of the maximum and average maximum and incomplete WAN connections per second. Out of these statistics, the device suggests a value for the SYN flood threshold.
- **Suggested value calculated from gathered statistics** - This is a read-only field provided by the system. After you select the level of protection, the appliance gathers statistics on current WAN TCP connections, keeping track of the maximum, average maximum, and incomplete WAN connections per second. These calculations provide support for a suggested value for the SYN Attack threshold.
- **Attack Threshold** - Enables you to set the threshold for the number of incomplete connection attempts per second before the device drops packets at any value between 5 and 200,000. The default is the suggested value calculated from gathered statistics by the appliance.

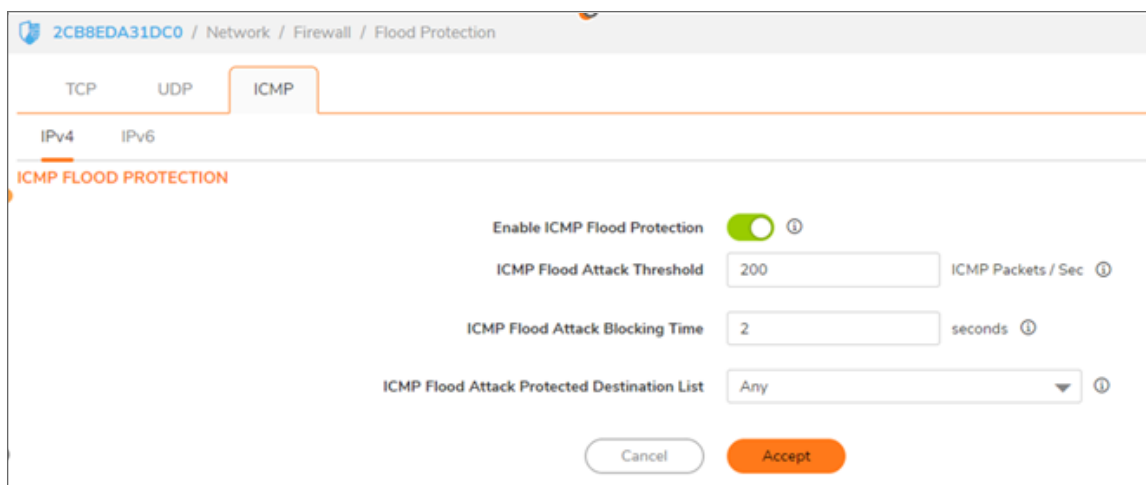
ICMP Flood Protection

ICMP Flood attacks are a type of denial-of-service (DoS) attack. It is initiated by sending a large number of ICMP packets to a remote host. As a result, the victimized system's resources are consumed with handling the attacking packets, which eventually causes the system to be unreachable by other clients.

SonicWall ICMP Flood Protection defends against these attacks by using a watch and block method. The appliance monitors ICMP traffic to a specified destination or to any destination. If the rate of ICMP packets per second exceeds the allowed threshold for a specified duration of time, the appliance drops subsequent ICMP packets to protect against a flood attack.

To enable ICMP flood protection:

1. Navigate to **Network | Firewall | Flood Protection**.
2. Under ICMP Flood Protection, enable the check box for **Enable ICMP Flood Protection**.
3. The following settings configure **ICMP Flood Protection**.
 - **ICMP Flood Attack Threshold (ICMP Packets / Sec)**: The rate of ICMP packets per second sent to a host, range or subnet that triggers ICMP Flood protection. The Threshold must be set carefully as too small a threshold may affect unintended traffic and too large a threshold may not effectively protect from an attack. The default value is 200.
 - **ICMP Flood Attack Blocking Time (Sec)**: After the appliance detects the rate of ICMP packets exceeding the attack threshold for this duration of time, ICMP Flood protection is activated, and the appliance will begin dropping subsequent ICMP packets.
 - **ICMP Flood Attack Protected Destination List**: The destination address object or address group that are protected from ICMP Flood attack.



The screenshot shows the configuration page for ICMP Flood Protection. The breadcrumb navigation is "2CB8EDA31DC0 / Network / Firewall / Flood Protection". There are tabs for "TCP", "UDP", and "ICMP", with "ICMP" selected. Below the tabs are "IPv4" and "IPv6" options, with "IPv4" selected. The main heading is "ICMP FLOOD PROTECTION". The configuration includes: "Enable ICMP Flood Protection" (toggle on), "ICMP Flood Attack Threshold" (input field with "200" and "ICMP Packets / Sec" label), "ICMP Flood Attack Blocking Time" (input field with "2" and "seconds" label), and "ICMP Flood Attack Protected Destination List" (dropdown menu with "Any" selected). At the bottom are "Cancel" and "Accept" buttons.

4. Click on **Accept**.

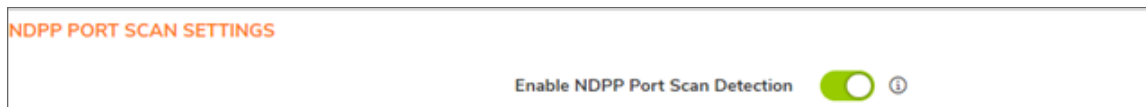
Port Scan Detection

Port scanning is a popular method that hackers use to determine which of your computer's ports are open to communication. Ports are dynamically blocked in the Distributed Security Client and are protected from hacking attempts. The Port Scan Detection feature detects if someone is scanning your ports and notifies you.

To enable Port Scan Detection:

1. Open the **Internal Diag** page/**Internal Settings**.
2. Click on **Internal settings** to access the **Internal Settings** page or **Diag** page.

3. In **NDPP Port Scan Settings**, select **Enable NDPP Port Scan Detection**.



Header-Based Signature

Header-based signature attack detection in SonicWall involves identifying and mitigating attacks by analyzing specific fields or patterns in the headers of network packets.

SonicWall maintains a database of predefined attack signatures. These signatures include patterns or anomalies commonly associated with various types of attacks.

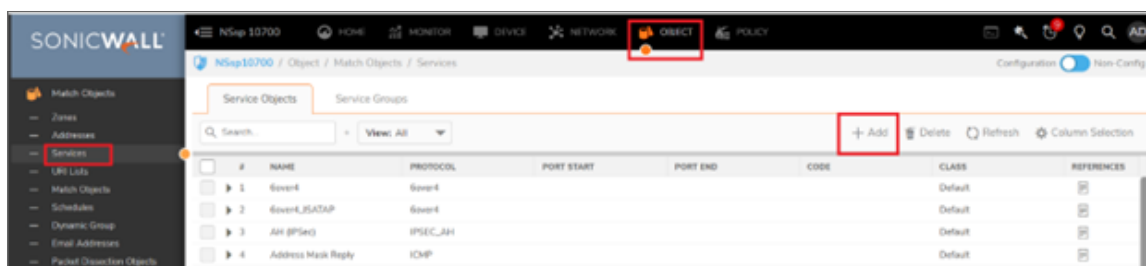
When a packet is received, SonicWall inspects the packet headers, such as the source IP, destination IP, source port, destination port, and other relevant fields. The device compares the packet header information against the signature database. It looks for matches or deviations that correspond to known attack patterns or vulnerabilities.

The following attacks are detected, blocked, and logged by the appliance by default, without any additional configuration:

- IP Attacks
 - IP Fragments Overlap (Teardrop attack, Bonk attack, or Boink attack)
 - iIP source address equal to the IP destination (Land attack)
- ICMP Attacks
 - Fragmented ICMP Traffic (e.g. Nuke attack)
 - Large ICMP Traffic (Ping of Death attack)
- TCP Attacks
 - TCP NULL flags
 - TCP SYN+FIN flags
 - TCP FIN only flags
 - TCP SYN+RST flags
- UDP Attacks
 - UDP Bomb Attack
 - UDP Chargen DoS Attack: This attack is not detected by default.

To detect and block header-based signatures:

1. Navigate to **OBJECT | Match Objects > Service** and click on **+Add**.



2. Create a service object for UDP port 19 to represent a Chargen packet.

Service Objects

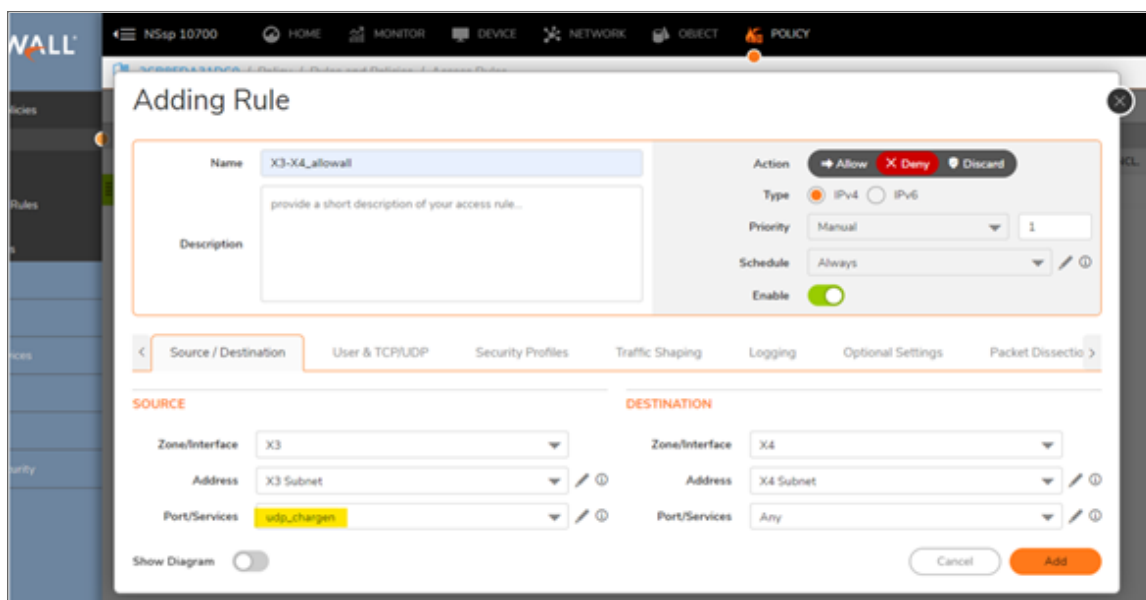
Name

Protocol

Port Range -

Sub Type

3. Navigate to **POLICY | Rules and Policies | Access Rules** and click on **+Add**
4. Create an access rule, select the created service object in the access rule, and set the action to 'Drop'.



When UDP traffic on port 19 is received, the appliance detects and drops it according to the configured rule, and a log is generated.

Firmware

The following sections review firmware management and firmware upgrades.

Firmware Management

To verify current firmware version, navigate to **Device | Settings | Firmware and Settings**.

#	FIRMWARE VERSION	CONFIGURATION BACKUP DATE	FIRMWARE LOAD DATE	USERNAME	COMMENTS	BACKUP TYPE	ACTIONS
1	Current Firmware Version ✓ SonicOS 7.0.1-5145-R5179	04/05/2024 07:35:12	10/25/2023 13:57:11	System	This is the current firmware.		⏴ ⏵
2	Backup created with version — Local backup 2 SonicOS 7.0.1-5065-R2800 (1 Configuration Files available)			admin	This is a backup on Local Storage.		🗑️
3	Backup created with version — Local backup 1 SonicOS 7.0.1-5025-R1891 (1 Configuration Files available)			admin	This is a backup on Local Storage.		🗑️

The **Firmware & Local Backup** section displays the following information:

- **Current Firmware Version** - Firmware currently loaded on the firewall.
- **Configuration backup Date** - The date and time when the configuration of the appliance was last backed up.
- **Firmware Load Date** - The date and time the firmware was installed on the appliance.
- **Username** - The user who installed or updated the firmware.
- **Comments** – Comments related to firmware and backup file.
- **Backup Type** - Type of backup.
- **Firmware Actions**- Clicking the Download icon saves the firmware to a new location on your computer or network. Only uploaded firmware can be saved to a different location.

Firmware Upgrade

When you do a firmware upgrade using SonicOS, you can restart with your current settings.

To upload new firmware:

1. Download the SonicOS firmware image file from **MySonicWall** and save it to a location on your local computer.
2. Point your browser to the appliance IP address and log in as an administrator.
3. In the **DEVICE** view, on the **Settings > Firmware and Settings** page, on the **Firmware & Local Backups** screen, click **Upload Firmware**.
4. In the **Backup of current settings popup** dialog, click **OK** to continue the firmware upload.
5. In the **Upload Firmware** dialog, browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**.

The digital signature on the firmware is automatically verified using the SonicWall public key. This key is appended to each firmware image made available to customers and is used to verify the new firmware. When a new firmware image is loaded on the physical appliances, the cryptographic module verifies the ECDSA signed SHA-256 hash of the image. When a new image is loaded on a virtual appliance, the cryptographic module verifies the RSA signed SHA-256 hash of the image.

- If the signature verification succeeds, the firmware is automatically installed.
 - If the signature verification fails, the firmware is not loaded and an error appears.
 - ① | **NOTE:** Uploading the same firmware is disallowed.
 - After the firmware finishes uploading, it is displayed in the table on the **Firmware & Local Backups** screen.
 - **Firmware & Local Backup** tab now shows the **Current Firmware Version** and recently **Uploaded Firmware Version** which is inactive image.
6. Click the **Boot** icon in the **Uploaded Firmware Version** row and select **Boot firmware with Current Configuration**.
 - ① | **NOTE:** Once the new version is installed as the boot image, the previously installed image gets replaced.
 7. In the **Warning** dialog box, click **OK**. The appliance restarts and displays the login page.
 - ① | **NOTE:** No functionality ceases during the update process. The device remains fully operational until the administrator reboots the product.
 8. Enter your username and password. Your new SonicOS image version information is displayed on the **Settings > Status** page.

Log Settings

SonicWall security appliances have system and audit logs that can be used to track security threats and configuration changes.

System Logs

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

Viewing System Logs

To view system events, navigate to **MONITOR | Logs > System Logs** page.

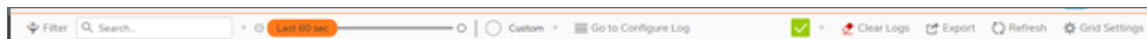
		GENERAL				INTERFACE	
#	TIME	ID	CATEGORY	PRIORITY	MESSAGE	SOURCE	DESTINATION
1	06:25:48 Sep 13	98	Network	Debug	Connection Opened	192.168.254.254, 15113, MGMT	10.1.5.163, 443, MGMT
2	06:25:47 Sep 13	537	Network	Debug	Connection Closed	192.168.254.254, 15107, MGMT	10.1.5.163, 443, MGMT
3	06:25:47 Sep 13	98	Network	Debug	Connection Opened	192.168.254.254, 15113, MGMT	10.1.5.163, 443, MGMT
4	06:25:46 Sep 13	98	Network	Debug	Connection Opened	192.168.254.254, 15106, MGMT	10.1.5.163, 443, MGMT
5	06:25:46 Sep 13	98	Network	Debug	Connection Opened	192.168.254.254, 15105, MGMT	10.1.5.163, 443, MGMT
6	06:25:46 Sep 13	98	Network	Debug	Connection Opened	192.168.254.254, 15110, MGMT	10.1.5.163, 443, MGMT
7	06:25:46 Sep 13	537	Network	Debug	Connection Closed	192.168.254.254, 15105, MGMT	10.1.5.163, 443, MGMT
8	06:25:44 Sep 13	98	Network	Debug	Connection Opened	192.168.254.254, 15107, MGMT	10.1.5.163, 443, MGMT
9	06:25:44 Sep 13	537	Network	Debug	Connection Closed	192.168.254.254, 15103, MGMT	10.1.5.163, 443, MGMT
10	06:25:43 Sep 13	700	Network	Debug	TCP packet received with invalid SEQ number, TCP packet dropped	192.168.254.254, 15105, MGMT	10.1.5.163, 443, MGMT

System Log Functions



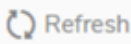


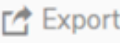
The System Log table provides numerous settings to allow you to navigate, view, and export results. Table columns can be customized, so that you can view full data on any event, or only the data you need. Table entries can be sorted to display in either ascending or descending order. To sort the entries in the Event Log, click the column heading. The entries are sorted by ascending or descending order. The arrow to the right of the column

name indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

The top row of the Event Log contains various functions. Functions pertaining only to Event Logs are described in the below table.



System Event Log Functions:

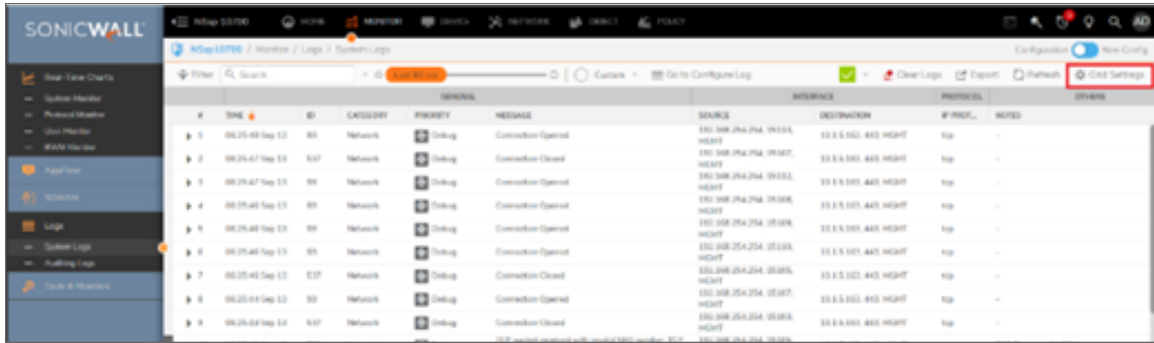
Option	Function	Action
 Filter	Filter	Set the filter for any specific log in the Event Log. You can set the filters based on GENERAL, SOURCE, and DESTINATION categories. For more information, refer to Filtering the View .
<input type="text" value="Search..."/>	Search	The Event Log displays the log entries that match the search string.
 60 Secs	Time Interval	Set the slider to filter the Event Log based on the time interval for the Event Log. You can set the slider anywhere between 60 Sec to 365 days.
 Refresh	Refresh	Click to refresh the system log data.
 Configure	Configure Log	Click this link and you are navigated to DEVICE Log > Settings to configure the items which needs to be tracked in the Event Log.
 Clear	Clear Logs	Click to clear the logs from the table.
 Export	Export	Click to export the logs in CSV, TXT files, and email

Display Options

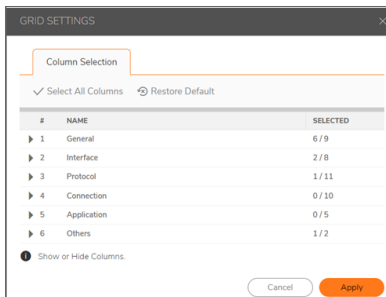
Customize the Events log to display as many or few columns that meet your needs.

To select which columns to display:

1. Navigate to **MONITOR | Logs > System Logs**.
2. Click **Grid Settings** icon . The **Grid Settings** dialog displays.



3. Select the items you want to appear as columns in the System Log.



4. When done, click **Apply** to preserve any changes or click **Restore Default** to revert back to the default settings.

Auditing Logs

This section describes in detail the recording feature that collects and records information on any changes in the security appliance configuration. To access this feature, navigate to **MONITOR | Logs > Auditing Logs** in the SonicOS management interface.

A configuration auditing records table is created to record all attempted configuration changes, both successful and failed. With configuration auditing, SonicOS archives the history of its configuration changes, so that the administrator or others can later revisit and analyze the records. This feature is enabled by default for the platforms where it is available.

Viewing Auditing Logs

The **MONITOR | Logs > Auditing Logs** page displays all the configuration auditing records. It allows a user to view, search, and sort the records.

#	AUDIT ID	TRANSACTION ID	TIME	GROUP INDEX	GROUP NAME	DESCRIPTION	OLD VALUE	NEW VALUE	TRANSACTION S...	USER
1	8876	8437	11:09:01 Sep 12 2024			'Low Priority Attacks (Detect AIE)	enabled	disabled	Succeeded	admin
2	8877	8437	11:09:01 Sep 12 2024			'Low Priority Attacks (Prevent AIE)	enabled	disabled	Succeeded	admin
3	8876	8437	11:09:01 Sep 12 2024			'Medium Priority Attacks (Detect AIE)	enabled	disabled	Succeeded	admin
4	8875	8437	11:09:01 Sep 12 2024			'Medium Priority Attacks (Prevent AIE)	enabled	disabled	Succeeded	admin
5	8874	8437	11:09:01 Sep 12 2024			'High Priority Attacks (Detect AIE)	enabled	disabled	Succeeded	admin
6	8873	8437	11:09:01 Sep 12 2024			'High Priority Attacks (Prevent AIE)	enabled	disabled	Succeeded	admin
7	8872	8436	11:09:01 Sep 12 2024			'Enable IPS'	enabled	disabled	Succeeded	admin
8	8871	8435	11:07:41 Sep 12 2024			'Low Priority Attacks (Detect AIE)	disabled	enabled	Succeeded	admin
9	8870	8435	11:07:41 Sep 12 2024			'Low Priority Attacks (Prevent AIE)	disabled	enabled	Succeeded	admin
10	8868	8435	11:07:41 Sep 12 2024			'Medium Priority Attacks (Detect AIE)	disabled	enabled	Succeeded	admin

- The first column is expandable to display the summary of the log entry.
- There are also buttons for **Select all Columns** and **Restore Default** for ease of operation. Click **Grid Settings** icon to perform the desired action.
- The user can search for a specific string pattern and highlight the matched results, if any are found.
- Failed configuration changes are marked in red.
- All columns are sortable.

Audit Log Functions

The **Audit Log** table provides numerous settings to allow you to navigate, view, and export results. The top row of the Log contains various functions.



- **Email Audit Records:** When a valid mail server and email address are configured, the user can click the email button on the tool bar of the Auditing Records page to manually email auditing records at any time.
- **Supplemental:** This option can be used to configure Displaying the Auditing Logs on the console and Audit Supplemental Parameter Changes
- **Export:** There are two export options for auditing records. You can export the records as a text file or as a CSV file.
- **Refresh:** The **Refresh** button provides a way to refresh the page and display the latest auditing records.
- **Grid Setting:** Customize the log to display as many or few columns that meet your needs.

Log Rotation and Deletion Policy

The appliance log limit is set to 75% by default. When the log capacity reaches 100%, the oldest 25% of log entries are automatically deleted to free up space for new entries.

- The maximum log capacity is 10,000 entries.
- After a factory default boot-up, log entries will begin from 1 and increase sequentially.
- When the number of logs reaches 7,500 (which is 75% of the capacity), the system will not yet delete logs. However, when the log count continues to 10,000, the system will trigger the deletion process.
- Upon reaching the 10,000 log entry limit, the appliance will delete the oldest 2,500 log entries.
- The next log added will start at entry #7,501, maintaining a total of 7,500 logs.
- As new logs continue to be generated, once the log count reaches 10,000 again, the system will delete the oldest 2,500 entries once more, starting the process over.

This approach ensures efficient log management by maintaining the most recent logs and removing older ones as the capacity limit is reached.

① | **NOTE:** For NSsp 15700, log output limit can be changed.

To change the log output limit:

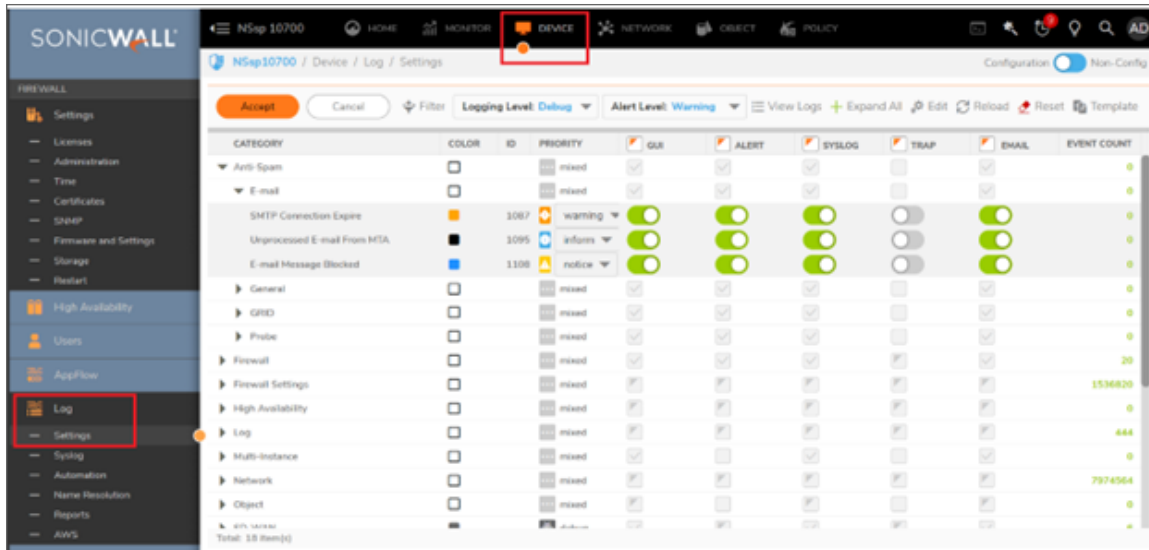
1. Go to internal setting page using link IP/sonicui/7/m/diag.
2. Enter numbers of logs in **Log Output Limit (entries)**.

Log Settings and Levels

The logging on appliances can be quite intensive. In some instances too much information may be recorded and this may overwhelm the appliance. It is important to gauge which information is required and how often this information is refreshed. The Log Monitor may not need to display certain events or their refresh interval may not need to be so frequent.

The log settings offer different options to reduce the logging intensity and to reduce the logging frequency.

To change the log settings go to **Device / Log / Settings**:



Column	Description
Category Column	<p>The Category column of the Log Monitor table has three levels:</p> <ul style="list-style-type: none"> • Category, first and highest level of the tree structure • Group, the second level • Event, the third level <p>Clicking the small black triangle expands or collapses the category or group contents.</p>
Color Column	The Color column shows the color with which the event, group, or category is highlighted in the Log Monitor table.
ID Column	The ID column shows the ID number of the event. The ID for a particular message is listed in the SonicOS Combined Log Events Reference Guide.
Positive Column	<p>The Priority column shows the severity or priority of a category, group, or event. For events, a menu is provided that lists the selectable priorities. For categories and groups, the priorities are listed in the dialog when you click the Configure button at the end of the row. The available priorities are: Alert, Critical, Error, Warning, Notice, Inform, Debug.</p> <p>NOTE: Changing the Event Priority may have serious consequences as the Event Priority for all categories will be changed. Modifying the Event Priority will affect the Syslog output for the tag “pri=” as well as how the event will be treated when performing filtering by priority level. Setting the Event Priority to a level that is lower than the Logging Level will cause those events to be filtered out. Also, as GMS ignores received Syslogs that have a level of Debug, heartbeat messages and reporting messages must have a minimum Event Priority of Inform.</p>

Column	Description
GUI Column	The GUI column shows checkboxes that indicate whether this event is displayed in the Log Monitor. For events, you can show or hide the event by selecting or deselecting the checkbox in the column. For categories and groups, you must use the configure dialog.
Alert Column	The Alert column shows checkboxes that indicate whether an Alert message will be sent for this event, group, or category.
Syslog Column	The Syslog column shows checkboxes that indicate whether the event, group, or category will be sent to a Syslog server.
Trap Column	The Trap column shows checkboxes that indicate whether the event or event category for which traps should be sent.
Email Column	The Email column shows checkboxes that indicate whether the log will be emailed to the configured address. For events, these checkboxes are configurable in the column. For categories and groups, Email is configured in the Edit Log Group or Edit Log Category dialogs that appear when you click the Configure button at the end of the row.
Event Count Column	The Event Count column shows the count of events by: <ul style="list-style-type: none"> • Event level — the value shows the number of times that this event has occurred. • Group level — the value shows the total events that occurred within the group. • Category level — the value shows the total events that occurred within the category.

Audit Server Configuration

The SonicWall security appliance can send a detailed log to an external Syslog server. The detailed log captures all log activity and includes every connection source and destination IP address, IP service, and number of bytes transferred. If the connection to the audit server is lost, the logs are stored in a 32-kilobyte rolling log buffer. When the buffer becomes full, the oldest logs are overwritten and access to these records is restricted to authorized administrators with the appropriate privilege.

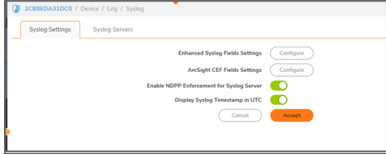
The appliance is configured to send audit records to an audit server over an IPsec protected link. The link is established between the appliance and the audit server, and the records are sent over this connection.

Configuring the Syslog Settings

The appliance can be configured to send audit records to an audit server over an IPsec protected link. The link is established between appliance and the audit server, and the records are sent over this connection. The logs are sent continuously and are removed from the buffer as they are sent. If the connection to the audit server is lost,

the logs are stored in a 32-kilobyte rolling log buffer. When the buffer becomes full, the oldest logs are overwritten.

The **Device | Log > Syslog** page enables you to configure the various settings you want when you send the log to a Syslog server. You can choose the Syslog facility and the Syslog format.



Audit Server Configuration

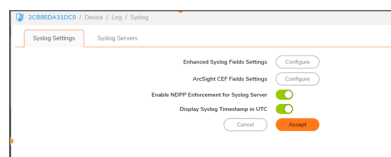
The SonicWall security appliance can send a detailed log to an external Syslog server. The detailed log captures all log activity and includes every connection source and destination IP address, IP service, and number of bytes transferred. If the connection to the audit server is lost, the logs are stored in a 32-kilobyte rolling log buffer. When the buffer becomes full, the oldest logs are overwritten and access to these records is restricted to authorized administrators with the appropriate privilege.

The appliance is configured to send audit records to an audit server over an IPsec protected link. The link is established between the appliance and the audit server, and the records are sent over this connection.

Configuring the Syslog Settings

The appliance can be configured to send audit records to an audit server over an IPsec protected link. The link is established between appliance and the audit server, and the records are sent over this connection. The logs are sent continuously and are removed from the buffer as they are sent. If the connection to the audit server is lost, the logs are stored in a 32-kilobyte rolling log buffer. When the buffer becomes full, the oldest logs are overwritten.

The **Device > Log > Syslog** page enables you to configure the various settings you want when you send the log to a Syslog server. You can choose the Syslog facility and the Syslog format.



To configure Syslog settings on your firewall:

1. Navigate to **Device > Log > Syslog** page.
2. (Optional) If you selected **Enhanced Syslog**, click the **Enhanced Syslog Fields Settings Configure** icon. The **Enhanced Syslog Field Settings** pop-up dialog displays.
(Optional) Select the Enhanced Syslog options to log. By default, all options are selected; the Host (sn) and Event ID (m) options are dimmed as they cannot be changed.

- To select all options, click **Enable All**.
 - To deselect all options, click **Disable All**.
 - Select only some options, either: **Click Disable All** and select only those options to log. Or deselect only those options to not log.
3. Click **Save**.
 4. Optionally, if you selected **ArcSight**, click the **ARCSight CEF Fields Settings Configure** icon. **ArcSight CEF Fields Settings** pop-up dialog displays.
 5. Optionally, select the ArcSight options to log. By default, all options are selected; the Host and Event ID options are dimmed as they cannot be changed.
 - To select all options, click **Enable All**.
 - To deselect all options, click **Disable All**.
 - To select only some options, either **Click Disable All** and select only those options to log. Or deselect only those options to not log.
 6. Click **Save**.
 7. Optionally, select the **Enable NDPP Enforcement for Syslog Server**.
 8. Optionally, select **Display Syslog Timestamp in UTC**.
 9. Click **Accept**.

Syslog Servers

Global settings affect all servers. For example, a change in a global format changes the format of all the servers to the selected value.

#	EVENT PROFILE	SERVER NAME	SERVER PORT	SERVER TYPE	SYSLOG FACILITY	SYSLOG FORMAT	SERVER ID	ENABLE
1	0	10.177.190.100 (SYSLOG_SERVER)	514	syslog-server	local-use0	default	firewall	<input checked="" type="checkbox"/>
2	0	10.1.1.107 (Secondary_Syslog)	514	syslog-server	local-use0	default	firewall	<input type="checkbox"/>

Event Profile	Profile configured for the Syslog Server
Server Name	IP address and name of the Syslog server
Server Port	Port of Syslog server
Server Type	Type of server
Syslog Facility	Type of facility for the Syslog server

Syslog Format	Format expected by the Syslog server: <ul style="list-style-type: none"> • Default (default) • WebTrends • Enhanced Syslog • ArcSight
Server ID	ID configured for the Syslog server; default is firewall.
Enable	Indicates whether the Syslog Server is enabled and allows you to enable or disable the sending of Syslog messages to a specific Syslog Server.
Configure	Contains the Edit and Delete icons for a Syslog server

Adding a Syslog Server

To add a Syslog server to the firewall:

1. Go to **Device > Log > Syslog** page.
2. Click **Syslog Servers** tab.
3. Click **Add**. The **Add Syslog Server** dialog appears.

4. Specify the **Event Profile** for this server in the **Event Profile** field. The minimum value is 0 (1 group), the maximum is 23 (24 groups), and the default is 0. Each group can have a maximum of 7 Syslog servers.
5. Select the Syslog server name or IP address from the **Name or IP Address** drop-down menu. Messages from the firewall are then sent to the servers.
6. If your Syslog server does not use default port 514, type the port number in the **Port Number** field.
7. Select the Syslog format from the **Syslog Format** drop-down menu. The default is **Default**.
8. Select the **Syslog Facility** from the **Syslog Facility** drop-down menu. The default is **Local Use 0**.
9. Optionally, to limit events logged and prevent the internal or external logging mechanism from being overwhelmed by log events, select **Enable Event Rate Limiting**.

① **NOTE:** Event rate limiting is applied regardless of **Log Priority** of individual events. Specify the maximum number of events in the **Maximum Events Per Second** field; the minimum number is 0, the maximum is 1000, and the default is 1000 per second.

10. Optionally, to limit events logged and prevent the internal or external logging mechanism from being overwhelmed by log events, select **Enable Data Rate Limiting**.

① **NOTE:** Data rate limiting is applied regardless of **Log Priority** of individual events. Specify the maximum number of bytes in the **Maximum Bytes Per Second** field; the minimum number is 0, the maximum is 1000000000, and the default is 10000000 bytes per second. This control limits data logged to prevent the internal or external logging mechanism from being overwhelmed by log events.

11. To bind to a VPN tunnel and create a network monitor policy in NDPP mode:
 - Optionally, choose an interface from the **Local Interface** drop-down menu.
 - Optionally, choose an Interface from the **Outbound Interface** drop-down menu.
12. Click **Add**.

Editing the Syslog Server

To edit a Syslog server:

1. Mouse over on the Syslog server that you want to edit and click the **Edit** icon. The **Edit Syslog Server** dialog displays.

The screenshot shows the 'Edit Syslog Server' dialog box with the following configuration:

- Event Profile: 0
- Name or IP Address: SYSLOG_SERVER
- Port: 514
- Server Type: Syslog Server
- Syslog Format: Default
- Syslog Facility: Local use 0
- Syslog ID: firewall
- Enable Event Rate Limiting:
- Maximum Events Per Second: 1000
- Enable Data Rate Limiting:
- Maximum Bytes Per Second: 10000000
- Local Interface: X2
- Outbound Interface: SYSLOG

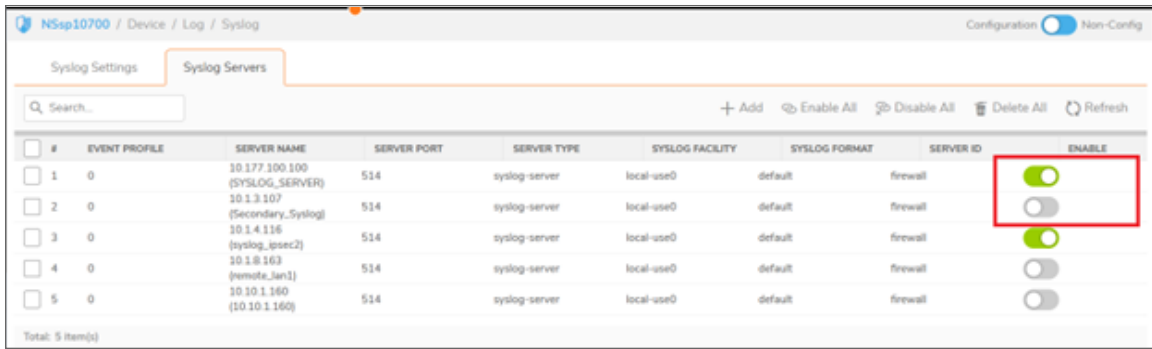
Buttons: Cancel, Save

2. Make the changes to the appropriate fields. Refer to the steps for "Adding a Syslog Server" for details.

Enabling Syslog Servers

To enable a single Syslog server:

1. Navigate to **Device | Log > Syslog**.
2. Select the toggle button in the **Enable** column.

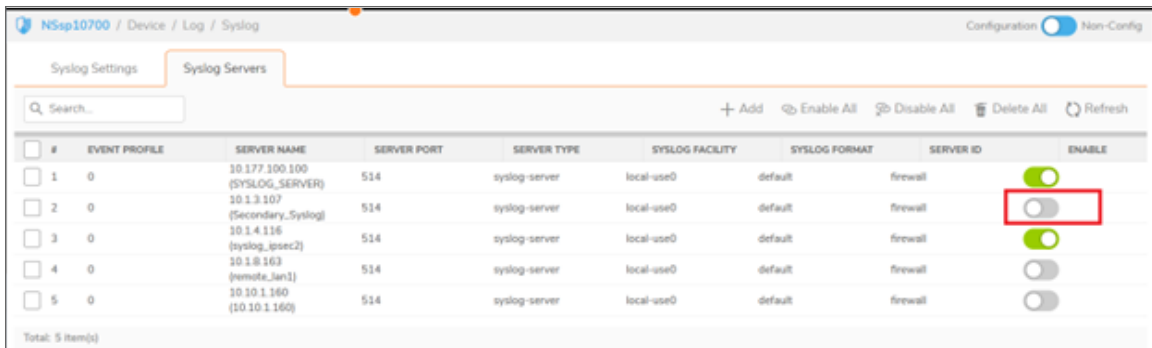


3. To enable all Syslog servers, select the Syslog servers and click **Enable All**.

Disabling Syslog Servers

To disable a single Syslog server:

1. Navigate to **Device | Log > Syslog**.
2. Deselect the toggle button in the **Enable** column.



3. To disable all Syslog servers, select the Syslog servers and click **Disable All**.

① **NOTE:** When NDPP mode is enabled, you cannot disable all syslog servers. At least one syslog server is needed to meet NDPP requirements.

Deleting Syslog Servers

To delete a single Syslog server, mouse over the Syslog server you want to delete and select the **Delete** icon.

To delete all Syslog servers, select the Syslog servers and click **Delete All**.

Audit Logs

The date stamp of the local audit log is displayed on the web management, but it does not include the year. Audit logs exported to external syslog servers and locally exported to CSV, TXT, or email has the full date/time stamp including the year.

It is recommended that the administrators use the formats with the full date/time stamp when operated in the CC evaluated configuration.

To Export the logs:

1. Go to **Monitor > Logs > System Logs** page.
2. Click on **Export** option.
3. Logs can be exported in CSV, TXT, or via email.

To set up a syslog server for audit logs, refer to the section 'Adding a Syslog Server'.

Audit Data Generation

Start-Up of the Audit Functions

Time	ID	Category	Group	Event	Msg Type	Priority	Message
UTC 08/09/2024 09:58:29	521	System	Status	Initializing	Simple	Information	Network Security Appliance initializing

Shutdown of the Audit Functions

Time	ID	Category	Group	Event	Msg Type	Priority	Message
UTC	1682	System	Restart	System Reboot	Simple Message String	Debug	System Reboot
08/09/2024							
12:39:25							

Administrative login and logout

WebUI login

```
2024-08-08T09:31:18.287563+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-08
09:31:20 UTC" fw=none_1 pri=6 c=16 m=29 msg="Administrator login allowed" sess="Web" dur=0
n=14 usr="admin" src=192.168.254.254::X1 dst=10.1.5.163:443:MGMT proto=tcp/https
note="User: admin" fw_action="NA"
```

WebUI logout

```
2024-08-08T09:34:10.918490+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-08
09:34:13 UTC" fw=none_1 pri=6 c=16 m=261 msg="Administrator logged out" sess="Web" dur=0
n=4 usr="admin" src=192.168.254.254::X1 dst=10.1.5.163:443:MGMT proto=tcp/https note="User:
admin, web logout" fw_action="NA"
```

Console login

```
2023-11-03T06:43:49.956818+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-03
06:43:49 UTC" fw=none_1 pri=6 c=16 m=199 msg="CLI administrator login allowed" n=2
usr="test" fw_action="NA"
```

Console logout

```
2023-11-03T06:45:00.863654+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-03
06:45:00 UTC" fw=none_1 pri=6 c=16 m=520 msg="CLI administrator logged out" n=2 fw_
action="NA"
```

Changes to TSF data related to configuration changes

Time Change

```
22024-04-04T06:48:15.821338+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-04
11:11:11 UTC" fw=none_1 pri=5 c=0 m=881 msg="System clock manually updated" n=18 note="UTC
04/04/2024 06:48:02.368 changed to UTC 04/04/2024 11:11:11.080 from 192.168.254.122" fw_
action="NA"
```

```
2024-04-04T06:48:15.833805+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-04
11:11:11 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Set Hour' , System
Time, changed from [6], changed to [11]" oldValue="6" newValue="11" usr="admin"
src=192.168.254.122:32589 dst=10.1.5.163:443:MGMT auditId=7624 tranxId=7964 grpName="Time
Settings" grpIndex="System Time" auditTime="UTC 06:48:02 Apr 04 2024" sess="API"
userMode="Full"
```

```
023-10-31T10:57:57.283949+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-10-23
10:11:11 UTC" fw=none_1
```

```
pri=5 c=0 m=881 msg="System clock manually updated" n=18 note="10/31/2023 10:57:57.192
changed to 10/23/2023 11:11:11.080 from 192.168.254.169" fw_action="NA"
```

Addition of trust anchors

```
2024-08-08T09:40:29.841233+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-08
09:40:32 UTC" fw=none_1 pri=6 c=0 m=1336 msg="Certification acumensec is imported" n=2
usr="admin" fw_action="NA"
```

```
2024-08-08T09:40:29.841233+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-08
09:40:32 UTC" fw=none_1 pri=6 c=0 m=1438 msg="CA Certificate acumensec Added." n=2 fw_
action="NA"
```

Removal of trust anchors

```
2023-11-30T12:57:26.265404+00:00 10.1.3.106 id=firewall sn=2CB8EDA31DC0 time="2023-11-30
12:57:33 UTC" fw=none_1 pri=6 c=0 m=1336 msg="Certification ICA_OCSP1 is deleted" n=4
usr="admin" fw_action="NA"
```

Generating/import of, changing, or deleting of cryptographic keys

Generating CSR

```
2023-11-23T09:29:27.485242+00:00 10.1.3.106 id=firewall sn=2CB8EDA31DC0 time="2023-11-23
09:29:34 UTC" fw=none_1 pri=6 c=16 m=1382 msg="Configuration succeeded: Generate PKCS10
Request" oldValue="" newValue="" usr="admin" src=192.168.254.169:32801
dst=10.1.5.163:443:MGMT auditId=2087 tranxId=6060 auditTime="UTC 09:29:34 Nov 23 2023"
sess="API" userMode="Full"
```

```
2023-11-23T09:29:27.631614+00:00 10.1.3.106 id=firewall sn=2CB8EDA31DC0 time="2023-11-23
09:29:34 UTC" fw=none_1 pri=6 c=0 m=1109 msg="CSR Generation: PKCS10 Request generation
complete." n=2 fw_action="NA"
```

Importing signed CSR

```
2024-08-08T09:59:51.678086+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-08
09:59:54 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: Import Req Cert"
oldValue="" newValue="" usr="admin" src=192.168.254.254:23393 dst=10.1.5.163:443:MGMT
auditId=8047 tranxId=8264 auditTime="UTC 09:59:54 Aug 08 2024" sess="API" userMode="Full"
```

Deleting CSR

```
2024-08-12T14:35:31.813198+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-12
14:35:17 UTC" fw=none_1 pri=6 c=0 m=1336 msg="Certification test1 is deleted" n=2
usr="admin" fw_action="NA"
```

```
2024-08-12T14:35:31.813198+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-12
14:35:17 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: Delete
Certificates, test1, changed from [test1]" oldValue="test1" newValue="" usr="admin"
src=192.168.254.254:36236 dst=10.1.5.163:443:MGMT auditId=8187 tranxId=8307
grpIndex="test1" auditTime="14:35:17 Aug 12 2024" sess="API" userMode="Full"
```

Resetting Passwords

```
2024-04-02T10:39:11.825181+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-02
10:40:48 UTC" fw=none_1 pri=6 c=0 m=1338 msg="User good password is changed" n=2 fw_
action="NA"
```

```
2024-04-02T10:39:11.825181+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-02
10:40:48 UTC" fw=none_1 pri=6 c=0 m=1337 msg="Administrative admin changes user good
password." n=2 fw_action="NA"
```

```
2024-04-02T10:39:11.825181+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-02
10:40:48 UTC" fw=none_1 pri=6 c=16 m=1334 msg="User good is edited" n=30 usr="admin" fw_
action="NA"
```

```
2024-04-02T10:39:11.825181+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-02
10:40:48 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Local User
Password' , good, changed from [*****], changed to [*****]" oldValue="*****"
newValue="*****" usr="admin" src=192.168.228.45:57233 dst=10.1.5.163:443:MGMT auditId=7549
tranxId=7920 grpName="User Object" grpIndex="good" uuid="00000000-0000-0008-0500-
2cb8eda31dc0" auditTime="UTC 10:40:48 Apr 02 2024" sess="API" userMode="Full"
```

Session Establishment with peer

```
2023-12-11T11:14:34.842672+00:00 10.1.3.106 id=firewall sn=2CB8EDA31DC0 time="2023-12-11
11:13:58 UTC" fw=none_1 pri=6 c=16 m=978 msg="IKEv2 negotiation complete" n=30
src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy: ipsec2; Local Net:
10.1.4.117-10.1.4.117; Remote Net: 10.1.8.0-10.1.8.255; inSPI:0xcd50c8ea; outSPI:
0xc10323d5" fw_action="NA"
```

```
2023-12-11T11:14:34.862988+00:00 10.1.3.106 id=firewall sn=2CB8EDA31DC0 time="2023-12-11
11:13:58 UTC" fw=none_1 pri=6 c=65536 m=427 msg="IPsec Tunnel status changed" n=48
note="Tunnel Up. policy 5(ipsec2), Dst 10.1.8.0 - 10.1.8.255, Src 10.1.4.117 - 10.1.4.117,
GW 10.1.4.116, inSpi 0xcd50c8ea, Reason: IKEv2 IPsec Negotiation Done." fw_action="NA"
```


Failure to Establish a TLS/HTTPS Session

Unsupported Ciphersuite

```
2023-11-10T10:01:56.085508+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-10
10:01:47 UTC" fw=none_1 pri=6 c=0 m=1686 msg="SSL Error : no shared cipher" note="Error1
L=20 F=378 R=193 tls_post_process_client_hello" n=60 src=10.1.5.162:37730:X1
dst=10.1.5.163:443:MGMT proto=tcp/https fw_action="NA"
```

Modify a byte in Client Finished handshake Message

```
2023-11-20T07:11:28.367440+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-20
07:11:31 UTC" fw=none_1 pri=6 c=0 m=1686 msg="SSL Error : decryption failed or bad record
mac" note="Error1 L=20 F=143 R=281 ssl3_get_record" n=8 src=10.1.5.162:56692:X1
dst=10.1.5.163:443:MGMT proto=tcp/https fw_action="NA"
```

Unsupported Protocol Version

```
2023-11-20T07:48:15.996776+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-20
07:48:18 UTC" fw=none_1 pri=6 c=0 m=1226 msg="HTTPS Handshake: unknown protocol" n=20
src=10.1.5.162:46340:X1 dst=10.1.5.163:443:MGMT proto=tcp/https fw_action="NA"
```

```
2023-11-20T07:48:15.996776+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-20
07:48:18 UTC" fw=none_1 pri=6 c=0 m=1686 msg="SSL Error : unknown protocol" note="Error1
L=20 F=521 R=252 tls_early_post_process_client_hello" n=20 src=10.1.5.162:46340:X1
dst=10.1.5.163:443:MGMT proto=tcp/https fw_action="NA"
```

Unsupported EC Curve

```
2023-11-20T13:28:34.129810+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-20
13:28:37 UTC" fw=none_1 pri=6 c=0 m=1226 msg="HTTPS Handshake: no shared cipher" n=34
src=10.1.5.162:43388:X1 dst=10.1.5.163:443:MGMT proto=tcp/https fw_action="NA"
```

```
2023-11-20T13:28:34.129810+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-20
13:28:37 UTC" fw=none_1 pri=6 c=0 m=1686 msg="SSL Error : no shared cipher" note="Error1
L=20 F=378 R=193 tls_post_process_client_hello" n=34 src=10.1.5.162:43388:X1
dst=10.1.5.163:443:MGMT proto=tcp/https fw_action="NA"
```

Unsuccessful Login Attempts Limit is Met or Exceeded

```
2023-11-02T11:41:20.276270+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-02
11:41:20 UTC" fw=none_1 pri=3 c=32 m=1572 msg="User login failed because the user is
currently locked out." sess="Web" dur=0 n=2 usr="admin" src=192.168.254.169::X1
dst=10.1.5.163:443:MGMT proto=tcp/https note="User: admin" fw_action="NA"
```

All Use of Identification and Authentication Mechanism

Successful authentication of Web UI

```
2023-11-01T09:53:21.384471+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-01 09:53:21 UTC" fw=none_1 pri=6 c=16 m=31 msg="User login from an internal zone allowed" sess="Web" dur=0 n=2 usr="test" src=192.168.254.169::X1 dst=10.1.5.163:443:MGMT proto=tcp/https note="User: test" fw_action="NA"
```

Unsuccessful authentication of Web UI

```
2023-11-01T09:50:20.091954+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-01 09:50:20 UTC" fw=none_1 pri=6 c=16 m=32 msg="User login denied due to bad credentials" sess="Web" dur=0 n=2 usr="test" src=192.168.254.169::X1 dst=10.1.5.163:443:MGMT proto=tcp/https note="User: test" fw_action="NA"
```

Successful authentication of Console

```
2023-11-01T09:57:48.328675+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-01 09:57:48 UTC" fw=none_1 pri=6 c=16 m=199 msg="CLI administrator login allowed" n=2 usr="test" fw_action="NA"
```

Unsuccessful authentication of Console

```
2023-11-01T09:56:37.763963+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-01 09:56:37 UTC" fw=none_1 pri=4 c=16 m=200 msg="CLI administrator login denied due to bad credentials" n=2 usr="test" fw_action="NA"
```

Unsuccessful Attempt to Validate a Certificate

Certificate verification failure due to invalid/incomplete certificate chain

```
2024-08-02T11:43:18.258139+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-02 11:43:15 UTC" fw=none_1 pri=4 c=16 m=953 msg="IKEv2 Payload processing error" n=8 src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy: Nssp_tunnel; Type: AUTH Payload; Error: IKEV2 AUTH SIGNATURE VERIFY FAILED" fw_action="NA"
```

Expired server certificate

```
2024-08-02T13:12:35.013935+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-02 13:12:32 UTC" fw=none_1 pri=4 c=16 m=953 msg="IKEv2 Payload processing error" n=234 src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy: Nssp_tunnel; Type: AUTH Payload; Error: IKEV2 AUTH PEER CERT EXPIRED OR NOT VALID YET" fw_action="NA"
```

```
2024-08-02T14:07:10.529705+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-02 14:07:07 UTC" fw=none_1 pri=6 c=0 m=1523 msg="Invalid certificate is imported: Local Certificate Expired" sess="Web" n=6 usr="admin" src=192.168.254.254 fw_action="NA"
```

Revoked server certificate

2024-08-07T14:13:51.298820+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-07 14:13:52 UTC" fw=none_1 pri=6 c=16 m=850 msg="OCSP received response." n=12 note="Status: Revoked - InitCookie: 0xc248e1fe1344d4b5" fw_action="NA"

2024-08-07T14:13:52.112014+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-07 14:13:53 UTC" fw=none_1 pri=4 c=16 m=953 msg="IKEv2 Payload processing error" n=28 src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy: Nssp_tunnel; Type: AUTH Payload; Error: IKEV2 AUTH PEER CERT IS REVOKED" fw_action="NA"

Revoked Intermediate CA Certificate

2024-08-05T10:09:30.449416+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-05 10:09:31 UTC" fw=none_1 pri=6 c=16 m=850 msg="OCSP received response." n=82 note="Status: Revoked - InitCookie: 0xcbf97ddccb2f620e" fw_action="NA"

2024-08-05T10:09:33.466527+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-05 10:09:34 UTC" fw=none_1 pri=4 c=16 m=953 msg="IKEv2 Payload processing error" n=41338 src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy: Nssp_tunnel; Type: AUTH Payload; Error: IKEV2 AUTH PEER CERT OCSP FAILED" fw_action="NA"

Invalid OCSP signer certificate

2024-08-05T08:39:12.665840+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-05 08:39:13 UTC" fw=none_1 pri=6 c=16 m=850 msg="OCSP received response." n=58 note="Status: Responder Certificate has no OCSPSigning - InitCookie: 0x150a4f9dba1531" fw_action="NA"

2024-08-05T08:39:16.659555+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-05 08:39:17 UTC" fw=none_1 pri=4 c=16 m=953 msg="IKEv2 Payload processing error" n=40428 src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy: Nssp_tunnel; Type: AUTH Payload; Error: IKEV2 AUTH PEER CERT OCSP FAILED" fw_action="NA"

Error due to modified certificate bytes

2024-08-02T14:31:50.201664+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-02 14:31:47 UTC" fw=none_1 pri=4 c=16 m=953 msg="IKEv2 Payload processing error" n=1658 src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy: Nssp_tunnel; Type: CERT Payload; Error: 47" fw_action="NA"

Failure due to Modified byte in signature

2024-08-02T14:45:04.430493+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-02 14:45:01 UTC" fw=none_1 pri=4 c=16 m=953 msg="IKEv2 Payload processing error" n=1786 src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy: Nssp_tunnel; Type: AUTH Payload; Error: IKEV2 AUTH SIGNATURE VERIFY FAILED" fw_action="NA"

Failure due to modified byte in the public key

2024-08-02T14:58:41.879845+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-02 14:58:39 UTC" fw=none_1 pri=4 c=16 m=953 msg="IKEv2 Payload processing error" n=1918 src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy: Nssp_tunnel; Type: CERT Payload; Error: 47" fw_action="NA"

Error due to modified public key

```
2023-12-01T10:19:19.820504+00:00 10.1.3.106 id=firewall sn=2CB8EDA31DC0 time="2023-12-01
10:19:26 UTC" fw=none_1 pri=6 c=16 m=1383 msg="Configuration failed: Import CA Cert,
changed to [Mod_ICA_EC.pem]" oldValue="" newValue="Mod_ICA_EC.pem" usr="admin"
src=192.168.254.169:1187 dst=10.1.5.163:443:MGMT auditId=2352 tranxId=6255 auditTime="UTC
10:19:26 Dec 01 2023" sess="API" userMode="Full"
```

Basic constraint is not present in the CA certificate

```
2024-07-11T07:20:58.268027+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-07-11
07:22:55 UTC" fw=none_1 pri=6 c=0 m=1523 msg="Invalid certificate is imported: No
basicConstraints is included." sess="Web" n=2 usr="admin" src=192.168.254.254 fw_
action="NA"
```

Basic constraint is set to False in the CA certificate

```
2024-07-11T09:33:12.358461+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-07-11
09:35:08 UTC" fw=none_1 pri=6 c=0 m=1523 msg="Invalid certificate is imported: CA flag is
not set." sess="Web" n=2 usr="admin" src=192.168.254.254 fw_action="NA"
```

Any addition, replacement or removal of trust anchors in the TOE's trust store

Addition of trust anchors

```
2024-08-08T09:40:29.841233+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-08
09:40:32 UTC" fw=none_1 pri=6 c=0 m=1336 msg="Certification acumensec is imported" n=2
usr="admin" fw_action="NA"
```

```
2024-08-08T09:40:29.841233+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-08
09:40:32 UTC" fw=none_1 pri=6 c=0 m=1438 msg="CA Certificate acumensec Added." n=2 fw_
action="NA"
```

Removal of trust anchors

```
2023-11-30T12:57:26.265404+00:00 10.1.3.106 id=firewall sn=2CB8EDA31DC0 time="2023-11-30
12:57:33 UTC" fw=none_1 pri=6 c=0 m=1336 msg="Certification ICA_OCSP1 is deleted" n=4
usr="admin" fw_action="NA"
```

Any attempt to initiate a manual update

Successful Attempt

```
2024-08-09T11:43:01.380731+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-09
11:43:03 UTC" fw=none_1 pri=7 c=0 m=1269 msg="Firmware Update Succeeded SonicOS 7.0.1-5161-
R6165" n=2 fw_action="NA"
```

Time	ID	Category	Group	Event	Msg Type	Priority	Message
UTC 08/09/2024 09:59:19	1496	System	Status	Firewall was rebooted by firmware	Simple Message String	Debug	System Reboot

Unsuccessful Attempt

```
2024-03-13T09:55:14.973895+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-13
09:56:30 UTC" fw=none_1 pri=7 c=0 m=1268 msg="Firmware Update Failed" n=8 usr="admin" fw_
action="NA"
```

All Management activities of TSF data

Ability to administer the TOE locally

```
2023-11-01T09:57:48.328675+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-01
09:57:48 UTC" fw=none_1 pri=6 c=16 m=199 msg="CLI administrator login allowed" n=2
usr="test" fw_action="NA"
```

Ability to administer the TOE remotely

```
2024-08-08T09:31:18.287563+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-08
09:31:20 UTC" fw=none_1 pri=6 c=16 m=29 msg="Administrator login allowed" sess="Web" dur=0
n=14 usr="admin" src=192.168.254.254::X1 dst=10.1.5.163:443:MGMT proto=tcp/https
note="User: admin" fw_action="NA"
```

Ability to configure the access banner

```
2023-11-03T10:51:12.283083+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-03
10:51:12 UTC" fw=none_1 pri=6 c=16 m=1382 msg="Configuration succeeded: 'Acceptable use
policy text before user login' , changed from [#012
<center><b><i>Welcome</i></b></center></b></i>#012 <font size=2>#012#012 <table width=\"100%\"
border=\"1\"#012 <tr><td>#012 <font size=2>#012 <br><br><br>#012 <" oldValue="\<font
face=arial size=3>#012 <center><b><i>Welcome</i></b></center></b></i>#012 <font size=2>#012#012
<table width=\"100%\" border=\"1\"#012 <tr><td>#012 <font size=2>#012 <br><br><br>#012
<center>Enter your usage policy terms here.#012 <br><br><br>#012 </td></tr>#012
</table>#012#012 C..." newValue="\<font face=arial size=3>#012 <center><b><i>Welcome to
SonicWall NSsp10700 </center></b></i>#012<center><b><i>You are accessing a restricted
system. This system is monitored. </center></b></i>#012 <font size=2>#012#012 <table
width=\"100%\" border=\"1\"#012 <tr><td>..." usr="admin" src=192.168.254.169:56897
dst=10.1.5.163:443:MGMT auditId=1963 tranxId=5967 auditTime="10:51:12 Nov 03 2023"
sess="API" userMode="Full"
```

Ability to configure the session inactivity time before session termination or locking

Remote Session

```
2024-07-31T08:49:00.828062+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-07-31 08:48:58 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Log out the Administrator after inactivity of (minutes)', changed from [5], changed to [2]" oldValue="5" newValue="2" usr="admin" src=192.168.254.254:29577 dst=10.1.5.163:443:MGMT auditId=7810 tranxId=8121 auditTime="UTC 08:48:58 Jul 31 2024" sess="API" userMode="Full"
```

Local Session

```
2024-07-31T09:41:24.152663+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-07-31 09:41:21 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Idle Timeout', changed from [300], changed to [120]" oldValue="300" newValue="120" usr="admin" dst=:Console auditId=7816 tranxId=8127 auditTime="UTC 09:41:21 Jul 31 2024" sess="CLI" userMode="Full"
```

Ability to update the TOE, and to verify the updates using digital signature

```
2024-08-09T11:43:01.380731+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-09 11:43:03 UTC" fw=none_1 pri=7 c=0 m=1269 msg="Firmware Update Succeeded SonicOS 7.0.1-5161-R6165" n=2 fw_action="NA"
```

Time	ID	Category	Group	Event	Msg Type	Priority	Message
UTC 08/09/2024 09:59:19	1496	System	Status	Firewall was rebooted by firmware	Simple Message String	Debug	Firewall was rebooted by Uploaded Firmware SonicOS 7.0.1-5161-R6165 08/09/2024 09:48:06.000 by admin from 192.168.254.254 WEBUI

Ability to configure the authentication failure parameters for FIA_AFL.1

```
2023-11-02T11:38:00.223028+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-02 11:38:00 UTC" fw=none_1 pri=6 c=16 m=1382 msg="Configuration succeeded: 'Max. login attempts in assigned period', changed from [5], changed to [3]" oldValue="5" newValue="3" usr="admin" src=192.168.254.169:14145 dst=10.1.5.163:443:MGMT auditId=1920 tranxId=5935 auditTime="11:38:00 Nov 02 2023" sess="API" userMode="Full"
```

```
2023-11-02T11:38:00.223028+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-02 11:38:00 UTC" fw=none_1 pri=6 c=16 m=1382 msg="Configuration succeeded: 'Lockout Period (minutes)', changed from [10], changed to [2]" oldValue="10" newValue="2" usr="admin" src=192.168.254.169:14145 dst=10.1.5.163:443:MGMT auditId=1921 tranxId=5936 auditTime="11:38:00 Nov 02 2023" sess="API" userMode="Full"
```

Ability to manage the cryptographic keys

```
2023-11-02T13:49:30.823743+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-02
13:49:30 UTC" fw=none_1 pri=6 c=16 m=1382 msg="Configuration succeeded: Generate PKCS10
Request" oldValue="" newValue="" usr="admin" src=192.168.254.169:19391
dst=10.1.5.163:443:MGMT auditId=1949 tranxId=5953 auditTime="13:49:30 Nov 02 2023"
sess="API" userMode="Full"
```

```
2023-11-02T13:49:30.904435+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-02
13:49:30 UTC" fw=none_1 pri=6 c=0 m=1109 msg="CSR Generation: PKCS10 Request generation
complete." n=2 fw_action="NA"
```

Ability to configure the cryptographic functionality

```
2023-11-23T09:29:27.485242+00:00 10.1.3.106 id=firewall sn=2CB8EDA31DC0 time="2023-11-23
09:29:34 UTC" fw=none_1 pri=6 c=16 m=1382 msg="Configuration succeeded: Generate PKCS10
Request" oldValue="" newValue="" usr="admin" src=192.168.254.169:32801
dst=10.1.5.163:443:MGMT auditId=2087 tranxId=6060 auditTime="UTC 09:29:34 Nov 23 2023"
sess="API" userMode="Full"
```

```
2023-11-23T09:29:27.631614+00:00 10.1.3.106 id=firewall sn=2CB8EDA31DC0 time="2023-11-23
09:29:34 UTC" fw=none_1 pri=6 c=0 m=1109 msg="CSR Generation: PKCS10 Request generation
complete." n=2 fw_action="NA"
```

Ability to configure the lifetime for IPsec SAs

Phase1 SAs

```
2024-08-08T10:38:19.389321+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-08
10:38:22 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Primary Gateway
Detection interval' , Tunnel_Yo, changed from [28800], changed to [2880]" oldValue="28800"
newValue="2880" usr="admin" src=192.168.254.254:39210 dst=10.1.5.163:443:MGMT auditId=8048
tranxId=8265 grpName="VPN SA" grpIndex="Tunnel_Yo" auditTime="UTC 10:38:22 Aug 08 2024"
sess="API" userMode="Full"
```

Phase2 SAs

```
2024-04-02T11:40:30.766164+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-02
11:42:07 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'IPsec (Phase 2)
Life Time' , ipsec2, changed from [28800], changed to [2880]" oldValue="28800"
newValue="2880" usr="admin" src=192.168.228.45:59492 dst=10.1.5.163:443:MGMT auditId=7563
tranxId=7925 grpName="VPN SA" grpIndex="ipsec2" auditTime="UTC 11:42:07 Apr 02 2024"
sess="API" userMode="Full"
```

Ability to start and stop services

```
2024-03-27T10:42:41.553930+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27
10:44:09 UTC" fw=none_1 pri=6 c=65536 m=427 msg="IPsec Tunnel status changed" n=121276
note="Tunnel Up. policy 5(ipsec2), Dst 10.1.8.0 - 10.1.8.255, Src 10.1.3.0 - 10.1.3.255, GW
10.1.4.116, inSpi 0xb8d04248, Reason: IKEv2 IPsec Negotiation Done." fw_action="NA"
```

```
2024-03-27T07:38:00.035332+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27
07:39:27 UTC" fw=none_1 pri=6 c=65536 m=427 msg="IPsec Tunnel status changed" n=121172
```

note="Tunnel Down. policy 5(ipsec2), Dst 10.1.8.0 - 10.1.8.255, Src 10.1.3.0 - 10.1.3.255, GW 10.1.4.116, inSpi 0x61805aa6, Reason: Remove IPSec SaNode." fw_action="NA"

① **NOTE:** When the IPsec tunnel status is changed to enable tunnel comes up and when it is disabled tunnel status changes to down.

Ability to configure the list of TOE-provided services available before an entity is identified and authenticated

```
2023-11-03T10:51:12.283083+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-03
10:51:12 UTC" fw=none_1 pri=6 c=16 m=1382 msg="Configuration succeeded: 'Acceptable use
policy text before user login' , changed from [
```

Ability to set the time which is used for time-stamps

```
2024-04-04T06:48:15.821338+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-04
11:11:11 UTC" fw=none_1 pri=5 c=0 m=881 msg="System clock manually updated" n=18 note="UTC
04/04/2024 06:48:02.368 changed to UTC 04/04/2024 11:11:11.080 from 192.168.254.122" fw_
action="NA"
```

```
2024-04-04T06:48:15.833805+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-04
11:11:11 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Set Hour' , System
Time, changed from [6], changed to [11]" oldValue="6" newValue="11" usr="admin"
src=192.168.254.122:32589 dst=10.1.5.163:443:MGMT auditId=7624 tranxId=7964 grpName=" Time
Settings" grpIndex="System Time" auditTime="UTC 06:48:02 Apr 04 2024" sess="API"
userMode="Full"
```

```
2024-04-04T06:48:15.833805+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-04
11:11:11 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Set Minute' ,
System Time, changed from [48], changed to [11]" oldValue="48" newValue="11" usr="admin"
src=192.168.254.122:32589 dst=10.1.5.163:443:MGMT auditId=7625 tranxId=7964 grpName="Time
Settings" grpIndex="System Time" auditTime="UTC 06:48:02 Apr 04 2024" sess="API"
userMode="Full"
```

```
2024-04-04T06:48:15.833805+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-04
11:11:11 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Set Second' ,
System Time, changed from [2], changed to [11]" oldValue="2" newValue="11" usr="admin"
src=192.168.254.122:32589 dst=10.1.5.163:443:MGMT auditId=7626 tranxId=7964 grpName="Time
Settings" grpIndex="System Time" auditTime="UTC 06:48:02 Apr 04 2024" sess="API"
userMode="Full"
```


Ability to configure the reference identifier for the peer

```
2024-04-25T10:06:01.384281+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-25
10:06:30 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Peer IKE ID' ,
Syslog_Secondary1, changed to [10.1.3.107]" oldValue="" newValue="10.1.3.107" usr="admin"
src=192.168.254.122:15559 dst=10.1.5.163:443:MGMT auditId=7661 tranxId=7976 grpName="VPN
SA" grpIndex="Syslog_Secondary1" auditTime="UTC 10:06:30 Apr 25 2024" sess="API"
userMode="Full"
```

Ability to import X.509v3 certificates to the TOE's trust store

```
2023-11-28T13:53:52.501219+00:00 10.1.3.106 id=firewall sn=2CB8EDA31DC0 time="2023-11-28
13:53:59 UTC" fw=none_1 pri=6 c=16 m=1382 msg="Configuration succeeded: Import CA Cert,
changed to [CA_OCSP1.pem]" oldValue="" newValue="CA_OCSP1.pem" usr="admin"
src=192.168.228.38:53136 dst=10.1.5.163:443:MGMT auditId=2273 tranxId=6191 auditTime="UTC
13:53:59 Nov 28 2023" sess="API" userMode="Full"
```

All Management Activities of TSF Data (including creation, modification and deletion of firewall rules)

Creation of Firewall Rules

```
2024-01-04T10:41:44.650152+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-01-04
10:41:38 UTC" fw=none_1 pri=6 c=16 m=440 msg="Security Policy added" sess="Web" n=12
usr="admin" src=192.168.254.68 note="Allow 'ICMP_T8' from 'LAN X3 Subnet' to 'VPN remote_
lan1'" uuid="00000000-0000-0010-0700-2cb8eda31dc0" rule="1 (LAN->VPN)" fw_action="NA"
```

Modification of Firewall rules

```
a2024-01-04T11:01:26.785923+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-01-04
11:01:20 UTC" fw=none_1 pri=6 c=16 m=441 msg="Security Policy modified" sess="Web" n=4
usr="admin" src=192.168.254.68 note="Allow 'ICMP_T3' from 'LAN X3 Subnet' to 'VPN remote_
lan1'" uuid="00000000-0000-0011-0700-2cb8eda31dc0" rule="2 (LAN->VPN)" fw_action="NA"aaa
```

Deletion of Firewall rules

```
2024-04-02T11:04:49.397893+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-02
11:06:25 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: Deleted 'Policy
Action' , test, changed from [test]" oldValue="test" newValue="" usr="admin"
src=192.168.228.45:58590 dst=10.1.5.163:443:MGMT auditId=7562 tranxId=7924
grpName="Firewall Access Rules" grpIndex="test" uuid="00000000-0000-004f-0700-2cb8eda31dc0"
auditTime="UTC 11:06:25 Apr 02 2024" sess="API" userMode="Full"
```

Discontinuous changes to time – either Administrator actuated or changed via an automated process

```
2024-04-04T06:48:15.821338+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-04 11:11:11 UTC" fw=none_1 pri=5 c=0 m=881 msg="System clock manually updated" n=18 note="UTC 04/04/2024 06:48:02.368 changed to UTC 04/04/2024 11:11:11.080 from 192.168.254.122" fw_action="NA"
```

```
2024-04-04T06:48:15.833805+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-04 11:11:11 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Set Hour' , System Time, changed from [6], changed to [11]" oldValue="6" newValue="11" usr="admin" src=192.168.254.122:32589 dst=10.1.5.163:443:MGMT auditId=7624 tranxId=7964 grpName="Time Settings" grpIndex="System Time" auditTime="UTC 06:48:02 Apr 04 2024" sess="API" userMode="Full"
```

Initiation of update; result of the update attempt (success or failure)

Successful Attempt

```
2024-08-09T11:43:01.380731+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-09 11:43:03 UTC" fw=none_1 pri=7 c=0 m=1269 msg="Firmware Update Succeeded SonicOS 7.0.1-5161-R6165" n=2 fw_action="NA"
```

Time	ID	Category	Group	Event	Msg Type	Priority	Message
UTC 08/09/2024 09:59:19	1496	System	Status	Firewall was rebooted by firmware	Simple Message String	Debug	Firewall was rebooted by Uploaded Firmware SonicOS 7.0.1-5161-R6165 08/09/2024 09:48:06.000 by admin from 192.168.254.254 WEBUI

Unsuccessful Attempt

```
2024-03-13T09:47:40.364739+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-13 09:48:55 UTC" fw=none_1 pri=7 c=0 m=1268 msg="Firmware Update Failed" n=4 usr="admin" fw_action="NA"
```

The termination of a remote session by the session locking mechanism

```
2023-11-03T08:53:20.629950+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-03 08:53:20 UTC" fw=none_1 pri=6 c=16 m=262 msg="Administrator logged out - inactivity timer expired" sess="Web" dur=120 n=6 usr="admin" src=192.168.254.169::X1 dst=10.1.5.163:443:MGMT proto=tcp/https note="User: admin" fw_action="NA"
```

The termination of an interactive session

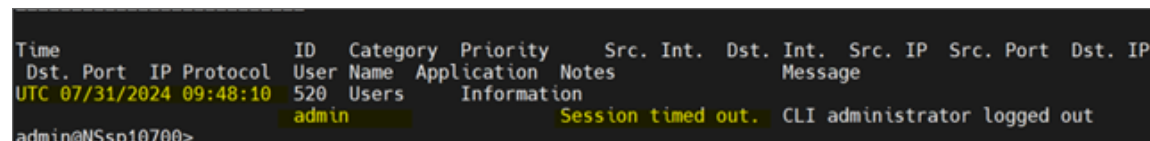
Local Console Logout

```
2023-11-03T06:45:00.863654+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-03 06:45:00 UTC" fw=none_1 pri=6 c=16 m=520 msg="CLI administrator logged out" n=2 fw_action="NA"
```

Remote Logout – Web

```
2024-08-08T09:34:10.918490+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-08-08 09:34:13 UTC" fw=none_1 pri=6 c=16 m=261 msg="Administrator logged out" sess="Web" dur=0 n=4 usr="admin" src=192.168.254.169::X1 dst=10.1.5.163:443:MGMT proto=tcp/https note="User: admin, web logout" fw_action="NA"
```

The termination of a local session by the session locking mechanism



Time	ID	Category	Priority	Src. Int.	Dst. Int.	Src. IP	Src. Port	Dst. IP
07/31/2024 09:48:10	520	Users	Information					
admin								
Session timed out. CLI administrator logged out								

admin@NSsp10700>

Initiation of the trusted channel

```
2024-03-27T10:42:41.513534+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27 10:44:09 UTC" fw=none_1 pri=7 c=16 m=171 msg="SENDING>>>> ISAKMP OAK IKE_AUTH (InitCookie:0xfa5b59ebf938ff4a RespCookie:0x8f31e1641762df63, MsgID: 0x1) *(ID_I, CERT_REQ, AUTH, SA, TS_I, TS_R, NOTIFY: Initial Contact)" n=559586 src=10.1.4.117:500 dst=10.1.4.116:500 proto=udp/500 fw_action="NA"
```

```
2024-03-27T10:42:41.513534+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27 10:44:09 UTC" fw=none_1 pri=6 c=16 m=940 msg="IKEv2 Initiator: Send IKE_AUTH Request" n=46
```

```

src=10.1.4.117:500 dst=10.1.4.116:500 proto=udp/500 note="VPN Policy: ipsec2; " fw_
action="NA"

2024-03-27T10:42:41.533616+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27
10:44:09 UTC" fw=none_1 pri=7 c=16 m=171 msg="RECEIVED<<< ISAKMP OAK IKE_AUTH
(InitCookie:0xfa5b59ebf938ff4a RespCookie:0x8f31e1641762df63, MsgID: 0x11000000001) *(ID_R,
AUTH, SA, TS_I, TS_R)" n=559588 src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 fw_
action="NA"

2024-03-27T10:42:41.533818+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27
10:44:09 UTC" fw=none_1 pri=6 c=16 m=974 msg="IKEv2 Initiator: Received IKE_AUTH response"
n=46 src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy: ipsec2; " fw_
action="NA"2024-03-27T10:42:41.533818+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0
time="2024-03-27 10:44:09 UTC" fw=none_1 pri=6 c=16 m=942 msg="IKEv2 Authentication
successful" n=138 src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy:
ipsec2; " fw_action="NA"

2024-03-27T10:42:41.533818+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27
10:44:09 UTC" fw=none_1 pri=6 c=16 m=944 msg="IKEv2 Accept IPsec SA Proposal" n=121094
src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy: ipsec2; ESP; AES_CBC-
128; HMAC_SHA512_256; ; Sequence Number 32-bit" fw_action="NA"

2024-03-27T10:42:41.533818+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27
10:44:09 UTC" fw=none_1 pri=6 c=16 m=978 msg="IKEv2 negotiation complete" n=121094
src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy: ipsec2; Local Net:
10.1.3.0-10.1.3.255; Remote Net: 10.1.8.0-10.1.8.255; inSPI:0xb8d04248; outSPI: 0xc5a87a74"
fw_action="NA"

2024-03-27T10:42:41.553930+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27
10:44:09 UTC" fw=none_1 pri=6 c=65536 m=427 msg="IPsec Tunnel status changed" n=121276
note="Tunnel Up. policy 5(ipsec2), Dst 10.1.8.0 - 10.1.8.255, Src 10.1.3.0 - 10.1.3.255, GW
10.1.4.116, inSpi 0xb8d04248, Reason: IKEv2 IPsec Negotiation Done." fw_action="NA"

```

Termination of the trusted channel

```

2024-03-27T07:37:19.991439+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27
07:38:47 UTC" fw=none_1 pri=7 c=16 m=171 msg="SENDING>>>> ISAKMP OAK IKEV2_INFORMATIONAL
(InitCookie:0x00b2498fc0577870 RespCookie:0x9d29e04ca1790957, MsgID: 0x2) *()" n=559038
src=10.1.4.117:500 dst=10.1.4.116:500 proto=udp/500 fw_action="NA"

2024-03-27T07:37:19.991439+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27
07:38:47 UTC" fw=none_1 pri=6 c=16 m=972 msg="IKEv2 Initiator: Remote party Timeout -
Retransmitting IKEv2 Request." n=59944 src=10.1.4.117:500 dst=10.1.4.116:500 proto=udp/500
note="VPN Policy: ipsec2; " fw_action="NA"

2024-03-27T07:37:19.991439+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27
07:38:47 UTC" fw=none_1 pri=7 c=262144 m=98 msg="Connection Opened" app=13 n=22098
src=10.1.4.117:500:X4 dst=10.1.4.116:500:X4 dstMac=00:50:56:8b:d6:67 proto=udp/500 sent=124
dpi=0 rule="Default Access Rule" fw_action="NA"

```

2024-03-27T07:37:29.986335+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27 07:38:57 UTC" fw=none_1 pri=6 c=0 m=1683 msg="Ikev2 Packet sent/received" n=559040 src=10.1.4.117:500 dst=10.1.4.116:500 note="IKEv2 Packet Sent" fw_action="NA"

2024-03-27T07:37:29.986335+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27 07:38:57 UTC" fw=none_1 pri=7 c=16 m=171 msg="SENDING>>>> ISAKMP OAK IKEV2_INFORMATIONAL (InitCookie:0x00b2498fc0577870 RespCookie:0x9d29e04ca1790957, MsgID: 0x2) *()" n=559040 src=10.1.4.117:500 dst=10.1.4.116:500 proto=udp/500 fw_action="NA"

2024-03-27T07:37:29.986335+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27 07:38:57 UTC" fw=none_1 pri=6 c=16 m=972 msg="IKEv2 Initiator: Remote party Timeout - Retransmitting IKEv2 Request." n=59946 src=10.1.4.117:500 dst=10.1.4.116:500 proto=udp/500 note="VPN Policy: ipsec2; " fw_action="NA"

2024-03-27T07:37:39.981967+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27 07:39:07 UTC" fw=none_1 pri=6 c=0 m=1683 msg="Ikev2 Packet sent/received" n=559042 src=10.1.4.117:500 dst=10.1.4.116:500 note="IKEv2 Packet Sent" fw_action="NA"

2024-03-27T07:37:39.981967+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27 07:39:07 UTC" fw=none_1 pri=7 c=16 m=171 msg="SENDING>>>> ISAKMP OAK IKEV2_INFORMATIONAL (InitCookie:0x00b2498fc0577870 RespCookie:0x9d29e04ca1790957, MsgID: 0x2) *()" n=559042 src=10.1.4.117:500 dst=10.1.4.116:500 proto=udp/500 fw_action="NA"

2024-03-27T07:37:39.981967+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27 07:39:07 UTC" fw=none_1 pri=6 c=16 m=972 msg="IKEv2 Initiator: Remote party Timeout - Retransmitting IKEv2 Request." n=59948 src=10.1.4.117:500 dst=10.1.4.116:500 proto=udp/500 note="VPN Policy: ipsec2; " fw_action="NA"

2024-03-27T07:37:49.998179+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27 07:39:17 UTC" fw=none_1 pri=6 c=0 m=1683 msg="Ikev2 Packet sent/received" n=559044 src=10.1.4.117:500 dst=10.1.4.116:500 note="IKEv2 Packet Sent" fw_action="NA"

2024-03-27T07:37:49.998179+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27 07:39:17 UTC" fw=none_1 pri=7 c=16 m=171 msg="SENDING>>>> ISAKMP OAK IKEV2_INFORMATIONAL (InitCookie:0x00b2498fc0577870 RespCookie:0x9d29e04ca1790957, MsgID: 0x2) *()" n=559044 src=10.1.4.117:500 dst=10.1.4.116:500 proto=udp/500 fw_action="NA"

2024-03-27T07:37:49.998179+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27 07:39:17 UTC" fw=none_1 pri=6 c=16 m=972 msg="IKEv2 Initiator: Remote party Timeout - Retransmitting IKEv2 Request." n=59950 src=10.1.4.117:500 dst=10.1.4.116:500 proto=udp/500 note="VPN Policy: ipsec2; " fw_action="NA"

2024-03-27T07:37:49.998179+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27 07:39:17 UTC" fw=none_1 pri=6 c=16 m=972 msg="IKEv2 Initiator: Remote party Timeout - Retransmitting IKEv2 Request." n=59950 src=10.1.4.117:500 dst=10.1.4.116:500 proto=udp/500 note="VPN Policy: ipsec2; " fw_action="NA"

2024-03-27T07:38:00.035332+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27 07:39:27 UTC" fw=none_1 pri=4 c=16 m=971 msg="IKEv2 Peer is not responding. Negotiation aborted." n=14966 src=10.1.4.117:500 dst=10.1.4.116:500 proto=udp/500 note="VPN Policy:

```
ipsec2; Failed 5 retries; IKEv2 InitSPI: 0x00b2498fc0577870; IKEv2 RespSPI:
0x9d29e04ca1790957" fw_action="NA"
```

```
2024-03-27T07:38:00.035332+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-27
07:39:27 UTC" fw=none_1 pri=6 c=65536 m=427 msg="IPsec Tunnel status changed" n=121172
note="Tunnel Down. policy 5(ipsec2), Dst 10.1.8.0 - 10.1.8.255, Src 10.1.3.0 - 10.1.3.255,
GW 10.1.4.116, inSpi 0x61805aa6, Reason: Remove IPSec SaNode." fw_action="NA"
```

Failure of the trusted channel functions

```
2023-12-13T13:19:38.566628+00:00 10.1.3.106 id=firewall sn=2CB8EDA31DC0 time="2023-12-13
13:19:05 UTC" fw=none_1 pri=4 c=16 m=968 msg="IKEv2 IPsec proposal does not match" n=4
src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy: ipsec2; Encryption
algorithm mismatch. Local: AES_CBC-128; Peer: 3DES" fw_action="NA"
```

```
2023-12-13T13:19:38.566628+00:00 10.1.3.106 id=firewall sn=2CB8EDA31DC0 time="2023-12-13
13:19:05 UTC" fw=none_1 pri=4 c=16 m=953 msg="IKEv2 Payload processing error" n=26
src=10.1.4.116:500 dst=10.1.4.117:500 proto=udp/500 note="VPN Policy: ipsec2; Type: SA
Payload; Error: 23" fw_action="NA"
```

Initiation of the trusted path

```
2023-11-03T14:55:17.523560+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-03
14:55:17 UTC" fw=none_1 pri=6 c=16 m=31 msg="User login from an internal zone allowed"
sess="Web" dur=0 n=2 usr="test" src=10.1.5.162::X1 dst=10.1.5.163:443:MGMT proto=tcp/https
note="User: test" fw_action="NA"
```

```
2023-11-03T14:55:17.523560+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-03
14:55:17 UTC" fw=none_1 pri=6 c=16 m=996 msg="Read-only mode GUI administration session
started" sess="Web" dur=0 n=2 usr="test" src=10.1.5.162::X1 dst=10.1.5.163:443:MGMT
proto=tcp/https note="User: test" fw_action="NA"
```

Termination of the Trusted Path

```
2024-04-02T11:20:49.432164+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-02
11:22:25 UTC" fw=none_1 pri=6 c=16 m=261 msg="Administrator logged out" sess="Web" dur=0
n=70 usr="admin" src=192.168.228.45::X1 dst=10.1.5.163:443:MGMT proto=tcp/https note="User:
admin, web logout" fw_action="NA"
```

```
2024-04-02T11:20:49.432164+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-02
11:22:25 UTC" fw=none_1 pri=6 c=16 m=995 msg="Configuration mode administration session
ended" n=102 usr="admin" src=192.168.228.45::MGMT dst=10.1.5.163:443:MGMT proto=tcp/https
note="admin at SonicOS API from 192.168.228.45" fw_action="NA"
```

```
2024-04-02T11:20:49.432164+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-04-02
11:22:25 UTC" fw=none_1 pri=6 c=16 m=998 msg="GUI administration session ended" sess="Web"
```

```
dur=0 n=98 usr="admin" src=192.168.228.45::X1 dst=10.1.5.163:443:MGMT proto=tcp/https
note="User: admin" fw_action="NA"
```

Failure of the Trusted Path Functions

```
2023-11-01T10:06:24.281390+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2023-11-01
10:06:24 UTC" fw=none_1 pri=1 c=32 m=30 msg="Administrator login denied due to bad
credentials" sess="Web" dur=0 n=18 usr="admin" src=192.168.254.169::X1
dst=10.1.5.163:443:MGMT proto=tcp/https note="User: admin" fw_action="NA"
```

Application of Rules Configured with the Log Operation

```
2024-03-19T14:26:48.437672+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-03-19
14:28:12 UTC" fw=none_1 pri=6 c=0 m=1235 msg="Packet allowed: code2 matched policy for non-
MGMT traffic" note="policyCheck" n=19042 src=10.1.3.107:50808:X3 dst=10.1.4.116:5655:X4
srcMac=00:50:56:8b:73:b0 dstMac=2c:b8:ed:a3:1d:c3 proto=udp/5655 uuid="00000000-0000-004c-
0700-2cb8eda31dc0" rule="1 (LAN->WAN)" fw_action="forward"
```

Time	ID	Category	Group	Event	Msg Type	Priority	Message
UTC 09/03/2024 11:57:50	1299	Security Services	Crypto Test	Self Test Passed	Simple	Alert	Ndpp SelfTest write/read encrypt/decrypt successfully

Failure of Self-Test

When a self-test fails, the appliance enters into an error state and the local console provides an error message reflecting information about the specific failure to the security administrators."

When the device enters into an error state audit service will not work.

All Administrative Actions

Definition of packet filtering rules

```
2024-09-04T10:29:36.088089+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-04
10:29:34 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Policy Action' ,
test, changed to [Allow Policy]" oldValue="" newValue="Allow Policy" usr="admin"
src=192.168.228.43:34713 dst=10.1.5.163:443:MGMT auditId=8799 tranxId=8410
```

```
grpName="Firewall Access Rules" grpIndex="test" uuid="00000000-0000-0057-0700-2cb8eda31dc0"
auditTime="UTC 10:29:34 Sep 04 2024" sess="API" userMode="Full"
```

```
2024-09-04T10:29:36.088089+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-04
10:29:34 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'From Zone' , test,
changed to [LAN]" oldValue="" newValue="LAN" usr="admin" src=192.168.228.43:34713
dst=10.1.5.163:443:MGMT auditId=8800 tranxId=8410 grpName="Firewall Access Rules"
grpIndex="test" uuid="00000000-0000-0057-0700-2cb8eda31dc0" auditTime="UTC 10:29:34 Sep 04
2024" sess="API" userMode="Full"
```

```
2024-09-04T10:29:36.088089+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-04
10:29:34 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'To Zone' , test,
changed to [WAN]" oldValue="" newValue="WAN" usr="admin" src=192.168.228.43:34713
dst=10.1.5.163:443:MGMT auditId=8801 tranxId=8410 grpName="Firewall Access Rules"
grpIndex="test" uuid="00000000-0000-0057-0700-2cb8eda31dc0" auditTime="UTC 10:29:34 Sep 04
2024" sess="API" userMode="Full"
```

Association of packet filtering rules to network interfaces

```
2024-09-04T10:29:36.088089+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-04
10:29:34 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'From Interface' ,
test, changed to [X3]" oldValue="" newValue="X3" usr="admin" src=192.168.228.43:34713
dst=10.1.5.163:443:MGMT auditId=8802 tranxId=8410 grpName="Firewall Access Rules"
grpIndex="test" uuid="00000000-0000-0057-0700-2cb8eda31dc0" auditTime="UTC 10:29:34 Sep 04
2024" sess="API" userMode="Full"
```

```
2024-09-04T10:29:36.088089+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-04
10:29:34 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'To Interface' ,
test, changed to [X4]" oldValue="" newValue="X4" usr="admin" src=192.168.228.43:34713
dst=10.1.5.163:443:MGMT auditId=8803 tranxId=8410 grpName="Firewall Access Rules"
grpIndex="test" uuid="00000000-0000-0057-0700-2cb8eda31dc0" auditTime="UTC 10:29:34 Sep 04
2024" sess="API" userMode="Full"
```

Ordering of packet filtering rules by priority

```
2024-09-04T10:29:36.088089+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-04
10:29:34 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Priority for
policy' , test, changed to [Insert at the top]" oldValue="" newValue="Insert at the top"
usr="admin" src=192.168.228.43:34713 dst=10.1.5.163:443:MGMT auditId=8808 tranxId=8410
grpName="Firewall Access Rules" grpIndex="test" uuid="00000000-0000-0057-0700-2cb8eda31dc0"
auditTime="UTC 10:29:34 Sep 04 2024" sess="API" userMode="Full"
```

Start-up and shut-down of the IPS functions

Start-up of the IPS functions

```
2024-09-18T07:11:28.268575+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-18
07:11:40 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Enable IPS' ,
changed from [disabled], changed to [enabled]" oldValue="disabled" newValue="enabled"
```



```
usr="admin" src=192.168.228.44:13790 dst=10.1.5.163:443:MGMT auditId=9490 tranxId=8549
auditTime="UTC 07:11:40 Sep 18 2024" sess="API" userMode="Full"
```

Shut-down of the IPS functions

```
2024-09-18T07:11:42.288561+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-18
07:11:54 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Enable IPS' ,
changed from [enabled], changed to [disabled]" oldValue="enabled" newValue="disabled"
usr="admin" src=192.168.228.44:13807 dst=10.1.5.163:443:MGMT auditId=9491 tranxId=8550
auditTime="UTC 07:11:54 Sep 18 2024" sess="API" userMode="Full"
```

All dissimilar IPS events/ reactions

Packets allowed

```
2024-01-12T10:43:13.430946+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-01-12
10:43:13 UTC" fw=none_1 pri=7 c=512 m=598 msg="ICMP packet from LAN allowed" n=454
src=10.1.3.107::X3 dst=10.1.4.111::X4 srcMac=00:50:56:8b:73:b0 dstMac=2c:b8:ed:a3:1d:c3
proto=icmp type=8 icmpCode=0 rule="1 (LAN->WAN)" fw_action="forward"
```

Packets denied

```
2024-01-12T10:58:22.775966+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-01-12
10:58:23 UTC" fw=none_1 pri=7 c=256 m=38 msg="ICMP packet dropped due to Policy" n=278
src=10.1.3.107::X3 dst=10.1.4.109::X4 srcMac=00:50:56:8b:73:b0 dstMac=2c:b8:ed:a3:1d:c3
proto=icmp type=8 icmpCode=0 uuid="00000000-0000-0027-0700-2cb8eda31dc0" rule="1 (LAN-
>WAN)" note="policyCheck" fw_action="drop"
```

Totals of similar events and reactions occurring within a specified time period

```
2024-02-07T11:06:36.605456+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-02-07
11:07:10 UTC" fw=none_1 pri=7 c=32 m=860 msg="Possible SYN Flood on IF X4" n=18
src=10.1.4.116:2417:X4 dst=10.1.4.117:1001 srcMac=00:50:56:8b:d6:67
dstMac=2c:b8:ed:a3:1d:c4 proto=tcp/1001 fw_action="NA"
```

Modification of an IPS policy element

```
2024-02-01T07:22:55.275988+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-02-01
07:23:20 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Application
Firewall policy object' , custom_sig, changed to [customsig]" oldValue=""
newValue="customsig" usr="admin" src=192.168.254.68:8982 dst=10.1.5.163:443:MGMT
auditId=4523 tranxId=7197 grpName="App Rules" grpIndex="custom_sig" auditTime="UTC 07:23:20
Feb 01 2024" sess="API" userMode="Full"
```

```
2024-02-01T07:22:55.275988+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-02-01
07:23:20 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Application
Firewall policy object exclude' , custom_sig, changed to [None]" oldValue=""
newValue="None" usr="admin" src=192.168.254.68:8982 dst=10.1.5.163:443:MGMT auditId=4524
tranxId=7197 grpName="App Rules" grpIndex="custom_sig" auditTime="UTC 07:23:20 Feb 01 2024"
sess="API" userMode="Full"
```

Inspected traffic matches an anomaly-based IPS policy

Allow:

```
2024-09-27T11:11:51.989715+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-27
11:12:17 UTC" fw=none_1 pri=7 c=0 m=1497 msg="Packet Dissection Check -- Pdf Name: ipv4,
Action: ALLOW" n=548 src=10.1.3.107::X3 dst=10.1.4.116::X4 srcMac=00:50:56:8b:73:b0
dstMac=2c:b8:ed:a3:1d:c3 proto=icmp rule="1 (LAN->WAN)" fw_action="NA"
```

Deny:

```
2024-01-12T08:18:31.342598+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-01-12
08:18:31 UTC" fw=none_1 pri=7 c=256 m=38 msg="ICMP packet dropped due to Policy" n=244
src=10.1.3.107::X3 dst=10.1.4.116::X4 srcMac=00:50:56:8b:73:b0 dstMac=2c:b8:ed:a3:1d:c3
proto=icmp type=8 icmpCode=0 note="err1: policy not found for packet on Zones(LAN -> WAN)"
fw_action="drop"
```

Inspected traffic matches a list of known-good or known-bad addresses applied to an IPS policy

```
2024-01-29T08:38:24.589789+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-01-29
08:38:49 UTC" fw=none_1 pri=7 c=0 m=1497 msg="Packet Dissection Check -- Pdf Name: IPv4ver,
Action: DROP" n=2 src=10.1.3.107::X3 dst=10.1.4.116::X4 srcMac=00:50:56:8b:73:b0
dstMac=2c:b8:ed:a3:1d:c3 proto=icmp rule="1 (LAN->WAN)" fw_action="NA"
```

Inspected traffic matches a signature-based IPS rule with logging enabled

```
2024-01-29T08:38:24.589789+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-01-29
08:38:49 UTC" fw=none_1 pri=7 c=0 m=1497 msg="Packet Dissection Check -- Pdf Name: IPv4ver,
Action: DROP" n=2 src=10.1.3.107::X3 dst=10.1.4.116::X4 srcMac=00:50:56:8b:73:b0
dstMac=2c:b8:ed:a3:1d:c3 proto=icmp rule="1 (LAN->WAN)" fw_action="NA"
```

Modification of which IPS policies are active on a TOE interface

```
2024-09-27T09:58:03.430752+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-27
09:58:28 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Zone IPS Enable' ,
LAN, changed from [enabled], changed to [disabled]" oldValue="enabled" newValue="disabled"
usr="admin" src=192.168.254.254:21523 dst=10.1.5.163:443:MGMT auditId=10553 tranxId=8675
grpName="Zone Object" grpIndex="LAN" uuid="8bdcd73-a017-cd2e-0a00-2cb8eda31dc0"
auditTime="UTC 09:58:28 Sep 27 2024" sess="API" userMode="Full"
```

Enabling a TOE interface with IPS policies applied

```
2024-09-27T10:01:07.606869+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-27
10:01:32 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: Port Enabled 'Port
Enabled' , X3, changed from [disabled], changed to [enabled]" oldValue="disabled"
newValue="enabled" usr="admin" src=192.168.254.254:21757 dst=10.1.5.163:443:MGMT
auditId=10556 tranxId=8678 grpIndex="X3" auditTime="UTC 10:01:32 Sep 27 2024" sess="API"
userMode="Full"
```

Disabling a TOE interface with IPS policies applied

```
2024-09-27T10:00:50.853663+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-27
10:01:15 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: Port Enabled 'Port
Enabled' , X3, changed from [enabled], changed to [disabled]" oldValue="enabled"
newValue="disabled" usr="admin" src=192.168.254.254:21712 dst=10.1.5.163:443:MGMT
auditId=10555 tranxId=8677 grpIndex="X3" auditTime="UTC 10:01:15 Sep 27 2024" sess="API"
userMode="Full"
```

Modification of which mode(s) is/are active on a TOE interface

```
2024-09-27T10:07:52.600214+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-27
10:08:17 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Interface Wire
Mode Type' , X5, changed from [Bypass], changed to [Network Tap]" oldValue="Bypass"
newValue="Network Tap" usr="admin" src=192.168.254.254:22324 dst=10.1.5.163:443:MGMT
auditId=10560 tranxId=8680 grpName="Network Interfaces" grpIndex="X5" auditTime="UTC
10:08:17 Sep 27 2024" sess="API" userMode="Full"
```

```
2024-09-27T10:07:52.600214+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-27
10:08:17 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Wire Mode
```

```
Interface' , X5, changed from [X7], changed to [Any]" oldValue="X7" newValue="Any"  
usr="admin" src=192.168.254.254:22324 dst=10.1.5.163:443:MGMT auditId=10561 tranxId=8680  
grpName="Network Interfaces" grpIndex="X5" auditTime="UTC 10:08:17 Sep 27 2024" sess="API"  
userMode="Full"
```

```
2024-09-27T10:07:52.600214+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-09-27  
10:08:17 UTC" fw=none_1 pri=7 c=16 m=1382 msg="Configuration succeeded: 'Wire Mode Disable  
Stateful' , X5, changed from [enabled], changed to [disabled]" oldValue="enabled"  
newValue="disabled" usr="admin" src=192.168.254.254:22324 dst=10.1.5.163:443:MGMT  
auditId=10562 tranxId=8680 grpName="Network Interfaces" grpIndex="X5" auditTime="UTC  
10:08:17 Sep 27 2024" sess="API" userMode="Full"
```

Inspected traffic matches a signature-based IPS rule with logging enabled

```
2024-01-29T08:38:24.589789+00:00 10.7.1.163 id=firewall sn=2CB8EDA31DC0 time="2024-01-29  
08:38:49 UTC" fw=none_1 pri=7 c=0 m=1497 msg="Packet Dissection Check -- Pdf Name: IPv4ver,  
Action: DROP" n=2 src=10.1.3.107::X3 dst=10.1.4.116::X4 srcMac=00:50:56:8b:73:b0  
dstMac=2c:b8:ed:a3:1d:c3 proto=icmp rule="1 (LAN->WAN)" fw_action="NA"
```

Cryptographic Key Destruction

The table below describes the key zeroization provided by the appliance. The deletion of keys is a straight forward process and should not result in any delays. Setting the appliance to factory default zeroizes all keys, including those stored in the flash memory.

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
RSA private key used for TLS	RSA (2048 bits, 3072 bits, 4096 bits)	Stored in flash memory. Held in the RAM buffer in plaintext.	The key is overwritten with a block erase when deleted. The plaintext key is overwritten with a pseudo-random pattern upon termination of the session or reboot of the appliance.
RSA public key used for TLS	RSA (2048 bits, 3072 bits, 4096 bits)	Stored in flash memory. Held in the RAM buffer in plaintext.	The key is overwritten with a block erase when deleted. The plaintext key is overwritten with a pseudo-random pattern upon termination of the session or reboot of the appliance.
AES key used for TLS	AES-128 AES-192 AES-256	Keys are not stored. Held in the RAM buffer in plaintext.	The key is overwritten with a pseudo-random pattern upon termination of the session or reboot of the appliance.
Key Agreement Keys used for IPsec	DH (2048 bits) ECDH (P-256, P-384, P-521)	Keys are not stored. Held in the RAM buffer in plaintext.	The key is overwritten with a pseudo-random pattern upon termination of the session or reboot of the appliance.

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
Authentication Keys used for IPsec	RSA (2048 bits)	Stored in flash memory.	The key is overwritten with a block erase when deleted.
	ECDSA (P-256, P-384, P-521)	Held in the RAM buffer in plaintext.	The plaintext key is overwritten with a pseudo-random pattern upon termination of the session or reboot of the appliance.
AES Keys used for IPsec	AES-128 AES-256	Keys are not stored. Held in the RAM buffer in plaintext.	The plaintext key is overwritten with a pseudo-random pattern upon termination of the session or reboot of the appliance.
SonicWall Public Key used to verify firmware updates	ECDSA (P-256)	Stored in Flash Memory .	The key may be overwritten by a software update.

References

- Security Target: Sonicwall SonicOS/X 7.0.1 with VPN and IPS on TZ, NSa, NSsp, and NSv Appliances Security Target, version 1.1, May 2024
- FIPS 140-3 Security Policy: SonicOS
- Quick Start Guides:
Sonicwall TZ270/TZ270W, TZ370/TZ370W, and TZ470/TZ470W Quick Start Guide
 - Sonicwall TZ670 / TZ570 / TZ570W / TZ570P Quick Start Guide
 - Sonicwall NSa 2700 Quick Start Guide
 - Sonicwall NSa 3700 Quick Start Guide
 - Sonicwall NSa 5700 Quick Start Guide
 - Sonicwall NSa 6700 Quick Start Guide
 - Sonicwall NSsp 10700 Quick Start Guide
 - Sonicwall NSsp 11700 Quick Start Guide
 - Sonicwall NSsp 13700 Quick Start Guide
- SonicOSX 7 System Administration Guide
- SonicOSX 7 Rules and Policies Administration Guide
- SonicOSX 7 Match Objects Administration Guide
- SonicOS and SonicOSX 7 IPSec VPN Administration Guide
- Audit Log Guides
 - SonicOS and SonicOSX 7 Device Log Administration Guide
 - SonicOS and SonicOSX 7 Monitor Logs Administration Guide
 - SonicWall SonicOS/X 7.0.1 Log Events Reference Guide
- Virtual Appliance Guide
 - SonicOS and SonicOSX 7 NSv Getting Started Guide for ESXi
 - SonicOS and SonicOSX 7 Upgrade Guide for the NSv Series

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
- Learn about [SonicWall Professional Services](#)
- Review [SonicWall Support services and warranty information](#)
- Register at [SonicWall University](#) for training and certification

About This Document

SonicOS Common Criteria Administration Guide for the NDPP Series

Updated - December 2024

Software Version - 7.0.1

232-006131-00 Rev A

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