SonicOS 7.1

System

Administration Guide

SONICWALL®

Contents

1

About SonicOS

This guide is a part of the SonicOS collection of administrative guides that describes how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators the management interface, API (Application Program Interface), and the Command Line Interface (CLI) for firewall configuration by setting objects to secure and protect the network services, to manage traffic, and to provide the desired level of network service. This guide focuses on

Topics:

Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and threats to your network. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices like access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers two different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration and diagnostics.

- *Policy Mode* provides a unified policy configuration work flow. It combines Layer 3 to Layer 7 policy enforcement for security policies and optimizes the work flow for other policy types. This unified policy work flow gathers many security settings into one place, which were previously configured on different pages of the management interface.
- *Classic Mode* is more consistent with earlier releases of SonicOS; you need to develop individual policies and actions for specific security services. The Classic Mode has a redesigned interface.

This table identifies which modes can be used on the different SonicWall firewalls:

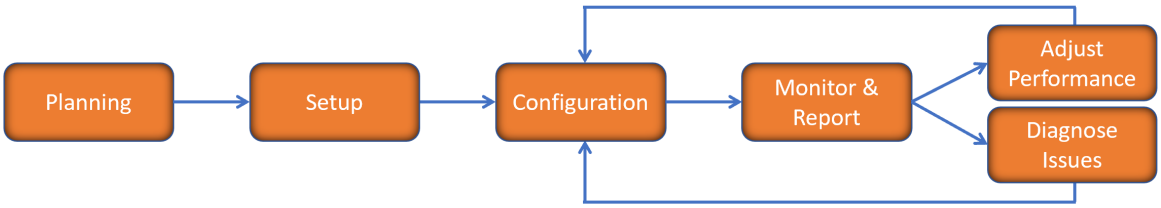
Firewall Type	Classic Mode	Policy Mode	Comments
TZ Series	yes	no	The entry level TZ Series, also known as desktop firewalls, deliver revamped features such as 5G readiness, better connectivity options, improved threat, SSL and decryption performance that address HTPPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support.
NSa Series	yes	no	NSa firewalls provide your mid sized network with enhanced security . They are designed specifically for businesses with 250 and up. it can provide cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, SD-WAN, real-time visualization, and WLAN management.
NSsp 10700, NSsp 11700, NSsp 13700	yes	no	The NSsp platforms high-end firewalls that deliver the advanced threat protection and fast speeds that large enterprises, data centers, and service providers need.
NSsp 15700	no	yes	The NSsp 15700 is designed for large distributed enterprises, data centers, government agencies and services providers. It provides advanced threat protection like Real-Time Deep Memory Inspection, multi-instance firewall configuration, and unified policy creation and modification, with scalability and availability.
NSv Series	yes	yes	The NSv series firewalls offers all the security advantages of a physical firewall with the operational and economic benefits of virtualization. The NSv firewalls can operate in either Policy Mode or Classic Mode. You can switch between modes, but some configuration information from extra interfaces is removed.

In addition to the management interface, SonicOS also has a full-featured API and a command-line interface (CLI) to manage the firewalls. For more information, refer to:

- SonicOS 7.1 API Reference Guide
- *SonicOS Command Line Interface Reference Guide*

SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.

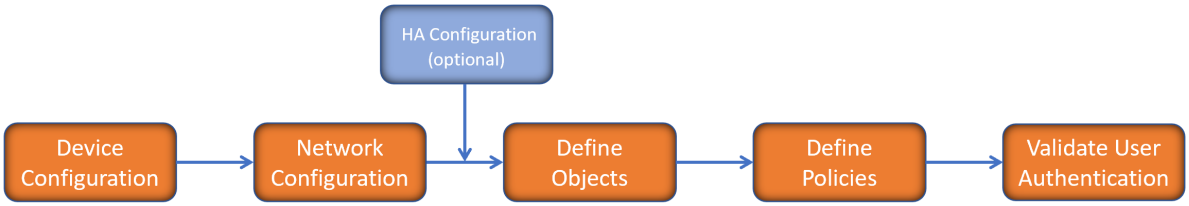


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing product information and solutions. After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The Getting Started Guides for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used use only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the specific Administration Guide for a SonicOS feature for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

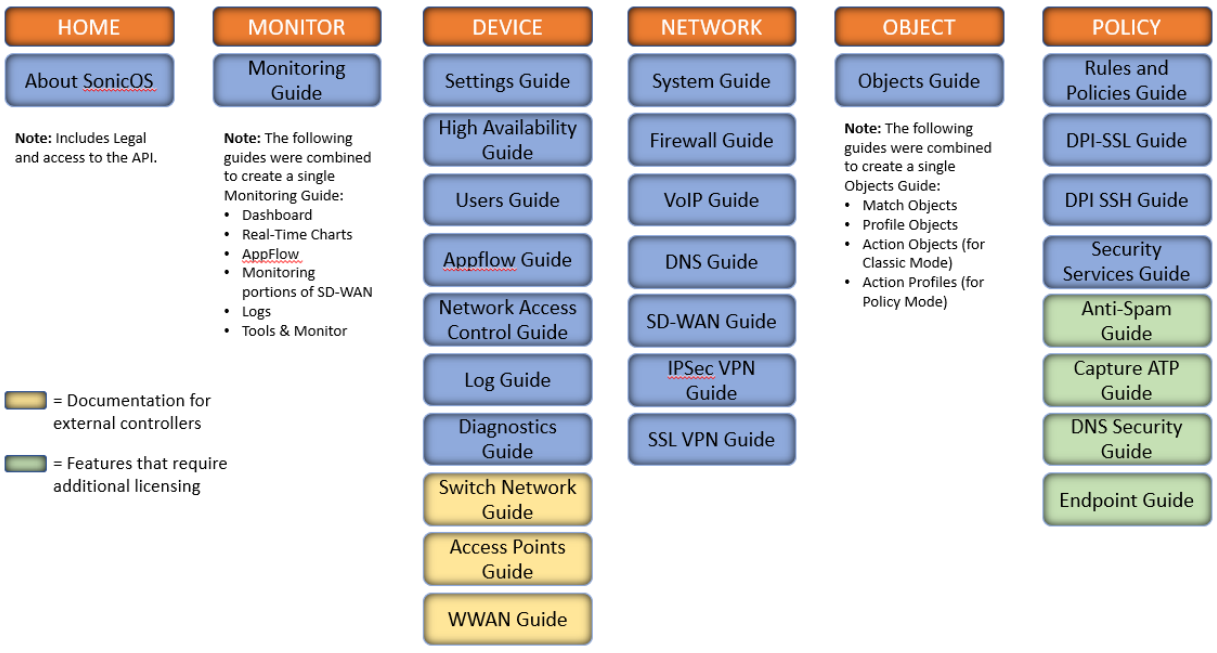


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the SonicOS 7.1 Monitor Guide and the SonicOS 7.1 Objects Guide which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicWall management interface.



The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the https://www.sonicwall.com/support/technical-documentation/.

Guide Conventions

These text conventions are used in this guide:

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

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

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

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

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

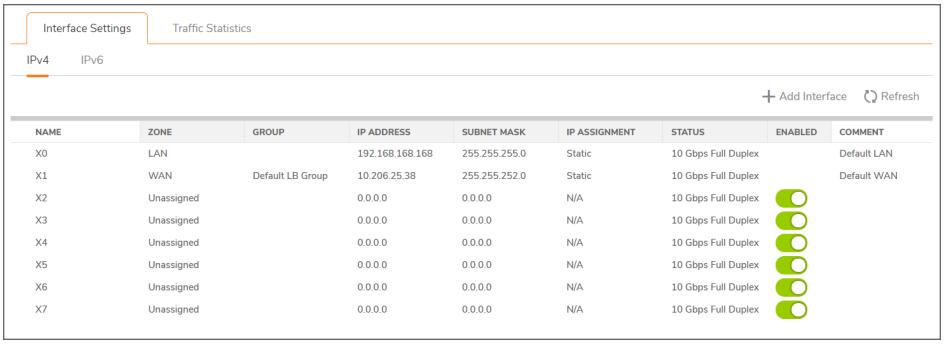
Convention	Description
Bold text	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Function | Menu group > Menu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

2

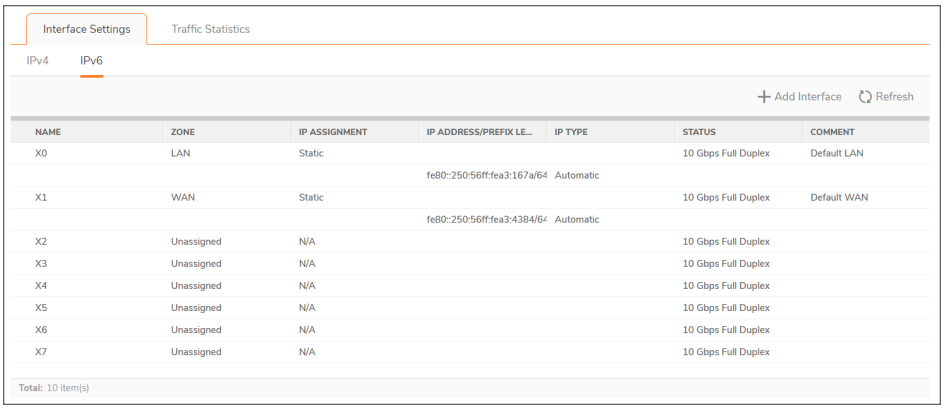
Interfaces

The **NETWORK | System > Interfaces | Interface Settings** pages include interface objects that are directly linked to physical interfaces for both IPv4 and IPv6. The SonicOS scheme of interface addressing works in conjunction with your network zones and address objects.

IPV4 INTERFACE SETTINGS



IPV6 INTERFACE SETTINGS



Topics:

About Interfaces

Topics:

Physical and Virtual Interfaces

Interfaces in SonicOS can be:

- **Physical interfaces** – Physical interfaces are bound to a single port.
- **Virtual interfaces** – Virtual interfaces are assigned as subinterfaces to a physical interface and allow the physical interface to carry traffic assigned to multiple interfaces.

Topics:

Physical Interfaces

The front panel of a SonicWall firewall has a number of physical interfaces. The number and type of interfaces depend on the model and version (for more information about the interfaces on your appliance, see the *Quick Start Guide* for your appliance):

Physical interfaces must be assigned to a zone to allow for configuration of Access Rules to govern inbound and outbound traffic. Security zones are bound to each physical interface where it acts as a conduit for inbound and outbound traffic. If there is no interface, traffic cannot access the zone or exit the zone.

For more information on zones, see *About Zones*.

Virtual Interfaces (VLAN)

Supported on SonicWall firewalls, virtual Interfaces are subinterfaces assigned to a physical interface. Virtual interfaces allow you to have more than one interface on one physical connection.

Virtual interfaces provide many of the same features as physical interfaces, including zone assignment, DHCP Server, and NAT and Access Rule controls.

Virtual Local Area Networks (VLANs) can be described as a “tag-based LAN multiplexing technology” because through the use of IP header tagging, VLANs can simulate multiple LAN’s within a single physical LAN. Just as two physically distinct, disconnected LAN’s are wholly separate from one another, so too are two different VLANs; however, the two VLANs can exist on the very same wire. VLANs require VLAN aware networking devices to offer this kind of virtualization — switches, routers and firewalls that have the ability to recognize, process, remove and insert VLAN tags (IDs) in accordance with the network’s design and security policies.

VLANs are useful for a number of different reasons, most of which are predicated on the VLANs ability to provide logical rather than physical broadcast domain, or LAN boundaries. This works both to segment larger physical LAN’s into smaller virtual LAN’s, as well as to bring physically disparate LAN’s together into a logically contiguous virtual LAN. The benefits of this include:

- **Increased performance** – Creating smaller, logically partitioned broadcast domains decreases overall network utilization, sending broadcasts only where they need to be sent, thus leaving more available bandwidth for application traffic.
- **Decreased costs** – Historically, broadcast segmentation was performed with routers, requiring additional hardware and configuration. With VLANs, the functional role of the router is reversed – rather than being used for the purposes of inhibiting communications, it is used to facilitate communications between separate VLANs as needed.
- **Virtual workgroups** – Workgroups are logical units that commonly share information, such as a Marketing department or an Engineering department. For reasons of efficiency, broadcast domain boundaries should be created such that they align with these functional workgroups, but that is not always possible: Engineering and Marketing users might be commingled, sharing the same floor (and the same workgroup switch) in a building, or just the opposite – the Engineering team might be spread across an entire campus. Attempting to solve this with complex feats of wiring can be expensive and impossible to maintain with constant adds and moves. VLANs allow for switches to be quickly reconfigured so that logical network alignment can remain consistent with workgroup requirements.
- **Security** – Hosts on one VLAN cannot communicate with hosts on another VLAN unless some networking device facilitates communication between them.

Subinterfaces

VLAN support on SonicOS is achieved by means of subinterfaces, which are logical interfaces nested beneath a physical interface. Every unique (tag) requires its own subinterface. For reasons of security and control, SonicOS does not participate in any VLAN trunking protocols, but instead requires that each VLAN that is to be supported be configured and assigned appropriate security characteristics.

NOTE: VLAN IDs range from 0 – 4094, with these restrictions: VLAN 0 is reserved for QoS and VLAN 1 is reserved by some switches for native VLAN designation.

NOTE: Dynamic VLAN Trunking protocols, such as VTP (VLAN Trunking Protocol) or GVRP (Generic VLAN Registration Protocol), should not be used on trunk links from other devices connected to the firewall.

Trunk links from VLAN capable switches are supported by declaring the relevant VLAN ID's as a subinterface on the firewall, and configuring them in much the same way that a physical interface would be configured. In other words, only those VLANs that are defined as subinterfaces are handled by the firewall, the rest are discarded as uninteresting. This method also allows the parent physical interface on the firewall to which a trunk link is connected to operate as a conventional interface, providing support for any native (untagged) VLAN traffic that might also exist on the same link. Alternatively, the parent interface could remain in an 'unassigned' state.

VLAN subinterfaces have most of the capabilities and characteristics of a physical interface, including zone assignability, security services, GroupVPN, DHCP server, IP Helper, routing, and full NAT policy and Access Rule controls. Multicast support is excluded from VLAN subinterfaces at this time.

SonicOS Secure Objects

The SonicOS scheme of interface addressing works in conjunction with address objects, service objects, and network zones. This structure is based on secure objects, which are utilized by rules and policies within SonicOS.

Secured objects include interface objects that are directly linked to physical interfaces and managed in the **NETWORK | System > Interfaces** page. Address and Service Objects are defined in **Match Objects > Addresses** and **Match Objects > Services** respectively.

Zones are the hierarchical apex of SonicOS's secure objects architecture. SonicOS includes predefined zones as well as allow you to define your own zones. Predefined zones include LAN, WAN, DMZ, VPN, SSLVPN, Multicast, and Custom. For more information about zones, see *Configuring Network Zones*.

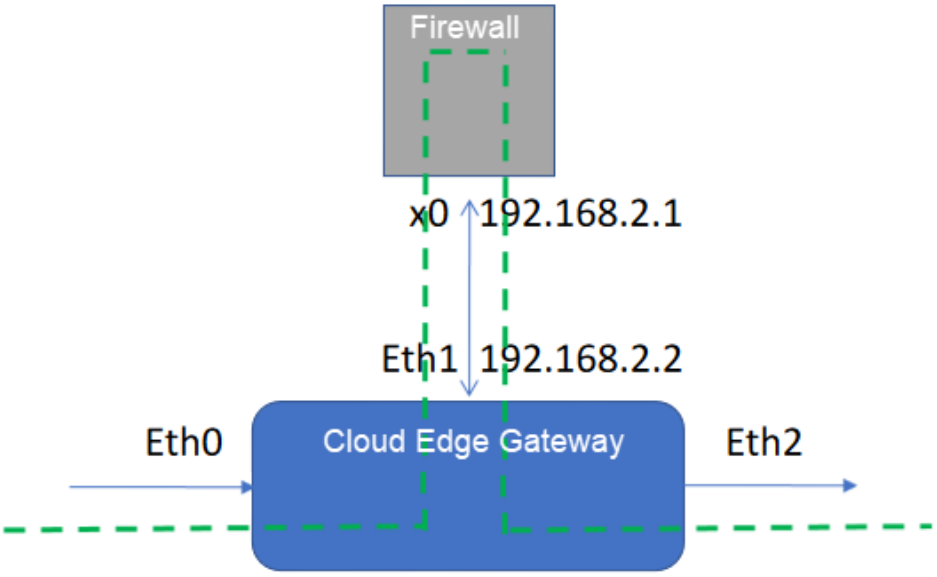
Zones can include multiple interfaces; the WAN zone, however, is restricted to a maximum of the total number of interfaces minus one. Within the WAN zone, either one or more WAN interfaces can be actively passing traffic depending on the WAN Failover and Load Balancing configuration on **NETWORK | System > Failover & Load Balancing**. For more information on WAN Failover and Load Balancing on SonicWall firewalls, see Failover & LB.

At the zone configuration level, the **Allow Interface Trust** setting for zones automates the processes involved in creating a permissive intra-zone Access Rule. It creates a comprehensive Address Object for the entire zone and a inclusively permissive Access Rule from zone address to zone addresses.

One Arm Mode and Single Interface Support

One Arm Mode is when only one firewall interface is used, and all traffic comes into and out from the same interface. It is possible to apply security rules and Deep Packet Inspection (DPI) scans on data traffic from the One Arm interface. Data received from this interface is scanned by SonicOS security services and then sent out on this interface.

One example usage scenario is shown as follows for SonicWall Cloud Edge. Cloud Edge works well when using a single interface on the firewall where traffic comes into and goes out from the same interface.



For One Arm Mode, you need to configure the interface:

- Interface must have a valid IP address (IPv4 or IPv6) configured. This can be a static IP address or a DHCP address.
- Must have **One Arm Peer** (next hop IP address) configured.
- Only LAN or WAN zone interfaces allow One Arm Mode in SonicOS 7.1.

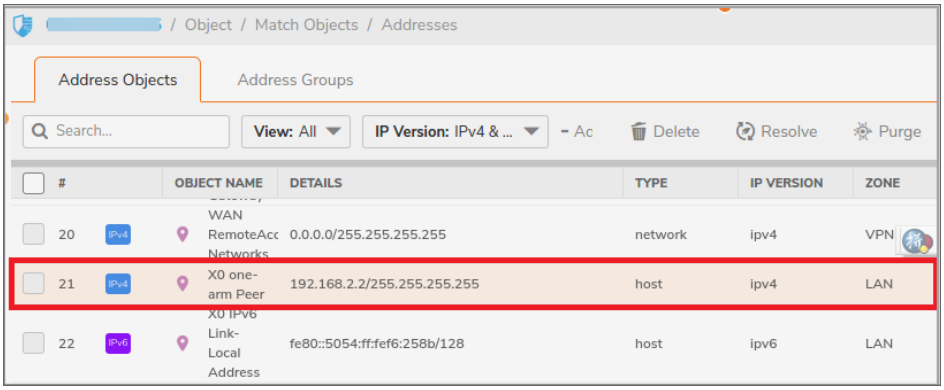
When you complete the One Arm Mode interface configuration, SonicOS automatically updates the system configuration to support One Arm Mode.

If the One Arm Mode interface is in the LAN zone, options on the **NETWORK | Firewall > Advanced** page are enabled or disabled. These are under **ACCESS RULE OPTIONS**:

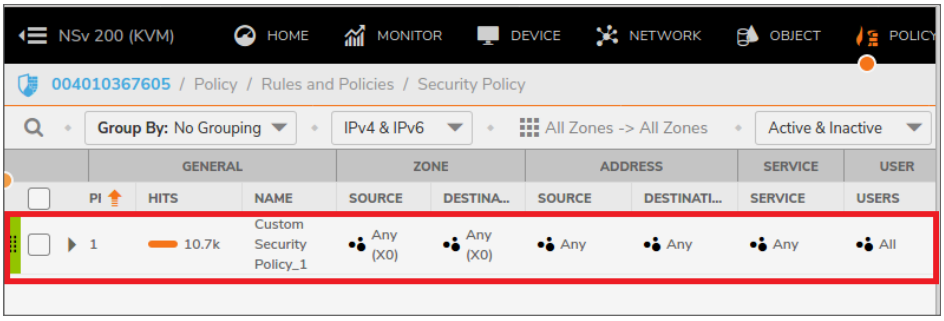
- Enable **Apply firewall rules for intra-LAN traffic to/from the same interface** - enable LAN-to-LAN security scanning
- Disable **Enable ICMP Redirect on LAN zone** - disable ICMP redirect if One Arm Mode interface is in

LAN zone

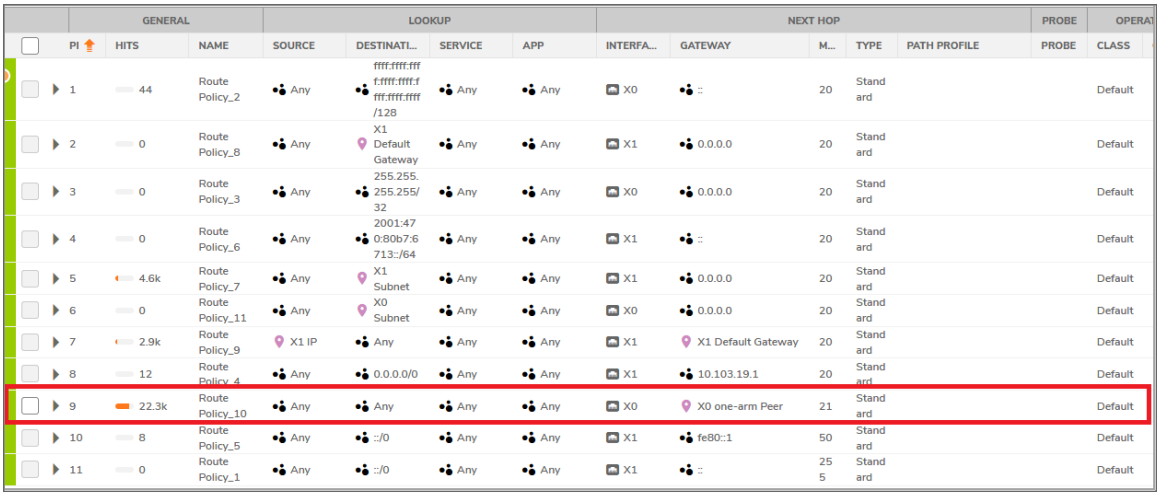
An address object for the One Arm Peer is automatically created.



A security policy to allow traffic from One Arm Mode interface to One Arm Mode interface is automatically created so traffic is always allowed.



A routing policy is automatically added with the One Arm Peer as the gateway to allow other traffic to apply One Arm routing, if needed.



	GENERAL			LOOKUP				NEXT HOP				PROBE	OPERAT
	PI	HITS	NAME	SOURCE	DESTINATI...	SERVICE	APP	INTERFA...	GATEWAY	M...	TYPE	PATH PROFILE	PROBE	CLASS
	1	44	Route Policy_2	Any	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128	Any	Any	X0	::	20	Standard			Default
	2	0	Route Policy_8	Any	X1 Default Gateway	Any	Any	X1	0.0.0.0	20	Standard			Default
	3	0	Route Policy_3	Any	255.255.255.255/32	Any	Any	X0	0.0.0.0	20	Standard			Default
	4	0	Route Policy_6	Any	2001:470:80b7:6713::/64	Any	Any	X1	::	20	Standard			Default
	5	4.6k	Route Policy_7	Any	X1 Subnet	Any	Any	X1	0.0.0.0	20	Standard			Default
	6	0	Route Policy_11	Any	X0 Subnet	Any	Any	X0	0.0.0.0	20	Standard			Default
	7	2.9k	Route Policy_9	X1 IP	Any	Any	Any	X1	X1 Default Gateway	20	Standard			Default
	8	12	Route Policy_4	Any	0.0.0.0/0	Any	Any	X1	10.103.19.1	20	Standard			Default
	9	22.3k	Route Policy_10	Any	Any	Any	Any	X0	X0 one-arm Peer	21	Standard			Default
	10	8	Route Policy_5	Any	::/0	Any	Any	X1	fe80::1	50	Standard			Default
	11	0	Route Policy_1	Any	::/0	Any	Any	X1	::	255	Standard			Default

For using a single interface on the firewall, the minimum number of NIC is changed to 1. To use only X0, you need to shut down X1 to make all traffic go out from X0. When you shut down X1, the priority of the One Arm routing policy becomes higher than the default route priority and traffic uses the X0 One Arm routing policy.

	GENERAL			LOOKUP				NEXT HOP		
	PI	HITS	NAME	SOURCE	DESTINATI...	SERVICE	APP	INTERFA...	GATEWAY	M...
	1	44	Route Policy_2	Any	f:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128	Any	Any	X0	::	20
	2	0	Route Policy_3	Any	255.255.255.255/32	Any	Any	X0	0.0.0.0	20
	3	0	Route Policy_11	Any	X0 Subnet	Any	Any	X0	0.0.0.0	20
	4	22.9k	Route Policy_10	Any	Any	Any	Any	X0	X0 one-arm Peer	21
	5	14	Route Policy_4	Any	0.0.0.0/0	Any	Any	X1	0.0.0.0	255
	6	0	Route Policy_1	Any	::/0	Any	Any	X1	::	255

For configuration of a One Arm Mode interface, see Configuring One Arm Mode.

Transparent Mode

Transparent Mode in SonicOS uses interfaces is the top level of the management hierarchy. Transparent Mode supports unique addressing and interface routing.

IPS Sniffer Mode

Topics:

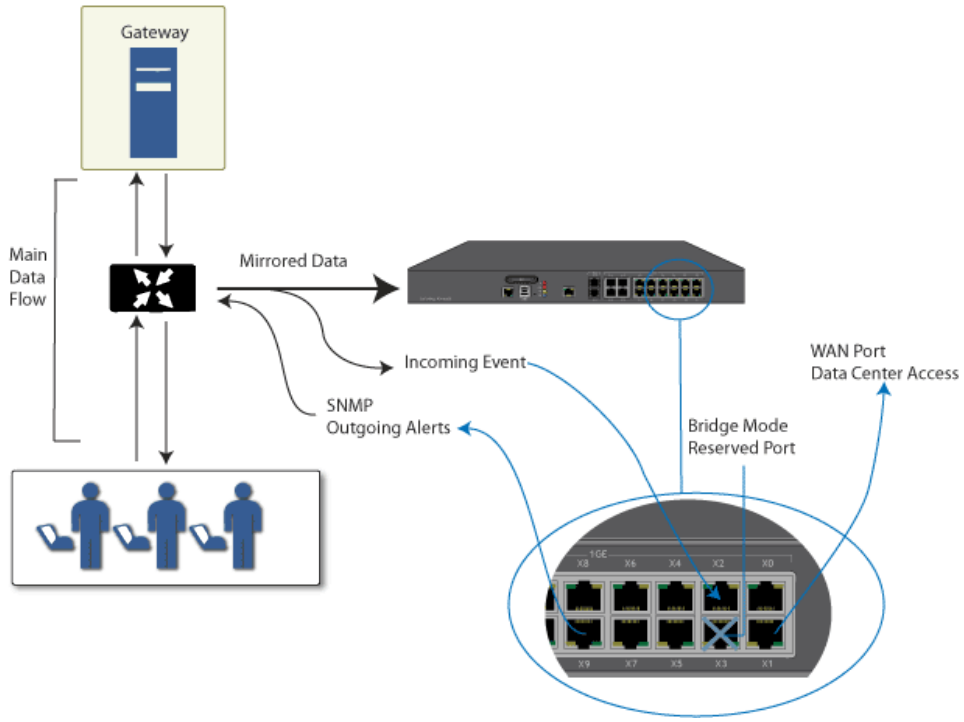
- Sample IPS Sniffer Mode Topology

Supported on SonicWall firewalls, 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.

In IPS Sniffer Mode: Network diagram, traffic flows into a switch in the local network and is mirrored through a switch mirror port into a IPS Sniffer Mode interface on the appliance. The appliance inspects the packets according to the settings configured on the Bridge-Pair. Alerts can trigger SNMP traps that are sent to the specified SNMP manager through another interface on the appliance. The network traffic is discarded after the appliance inspects it.

The WAN interface of the appliance is used to connect to the firewall Data Center for signature updates or other data.

IPS SNIFFER MODE: NETWORK DIAGRAM



In IPS Sniffer Mode, a Layer 2 Bridge is configured between two interfaces in the same zone on the appliance, such as LAN-LAN or DMZ-DMZ. You can also create a custom zone to use for the Layer 2 Bridge.

Only the WAN zone is **not** appropriate for IPS Sniffer Mode. The reason for this is that SonicOS detects all signatures on traffic within the same zone such as LAN-LAN traffic, but some directional specific (client-side versus server-side) signatures do not apply to some LAN-WAN cases.

Either interface of the Layer 2 Bridge can be connected to the mirrored port on the switch. As network traffic traverses the switch, the traffic is also sent to the mirrored port and from there into the appliance for deep packet inspection. Malicious events trigger alerts and log entries, and if SNMP is enabled, SNMP traps are sent to the configured IP address of the SNMP manager system. The traffic does not actually continue to the other interface

of the Layer 2 Bridge. IPS Sniffer Mode does not place the appliance inline with the network traffic, it only provides a way to inspect the traffic.

The **Edit Interfaces** dialog available from the **NETWORK | System > Interfaces** page provides an option, **Only sniff traffic on this bridge-pair**, for use when configuring IPS Sniffer Mode. When selected, this option causes the appliance to inspect all packets that arrive on the L2 Bridge from the mirrored switch port. The Never route traffic on this bridge-pair option should also be selected for IPS Sniffer Mode to ensure that the traffic from the mirrored switch port is not sent back out onto the network.

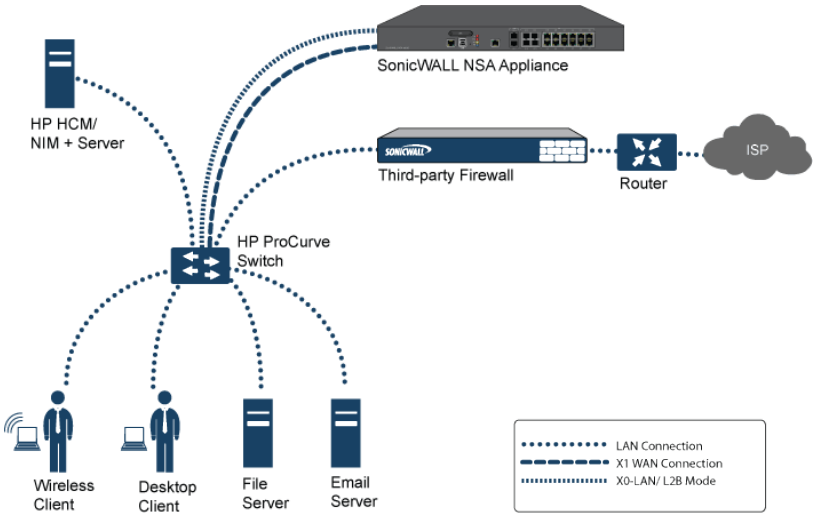
For detailed instructions on configuring interfaces in IPS Sniffer Mode, see *Configuring IPS Sniffer Mode*.

Sample IPS Sniffer Mode Topology

This example topology uses SonicWall IPS Sniffer Mode in a Hewlett Packard ProCurve switching environment. This scenario relies on the ability of HP's ProCurve Manager Plus (PCM+) and HP Network Immunity Manager (NIM) server software packages to throttle or close ports from which threats are emanating.

This method is useful in networks where there is an existing appliance that remains in place, but you wish to use the appliance's security services as a sensor.

IPS SNIFFER MODE: SAMPLE TOPOLOGY



In this deployment the WAN interface and zone are configured for the internal network's addressing scheme and attached to the internal network. The X2 port is Layer 2 bridged to the LAN port, but it is not attached to anything. The X0 LAN port is configured to a second, specially programmed port on the HP ProCurve switch. This special port is set for mirror mode: it forwards all the internal user and server ports to the "sniff" port on the firewall. This allows the firewall to analyze the entire internal network's traffic, and if any traffic triggers the security signatures it immediately traps out to the PCM+/NIM server through the X1 WAN interface, which then can take action on the specific port from which the threat is emanating.

Firewall Sandwich

You can deploy and configure a SonicWall Firewall Sandwich to improve availability, scalability, and manageability across the IT infrastructure. Deployment of the Firewall Sandwich provides the following features:

- **Scalability** - add more capacity as you go, reusing existing equipment
- **Redundancy and resiliency** – primary and secondary components
- **Inline upgrades** – upgrade firewalls and switches without shutting down the system
- **Single point of management** - manage policies for multiple firewall clusters and blades
- **Full security services** - including DPI-SSL capability

Firewall Sandwich deployment and configuration can be implemented using these equipment and services:

- Dell Force10 Series switches, such as the S5000, S4810, S4048, or S6000 running FTOS v9.8+.
- SonicWall services, such as Gateway Anti-Virus, Intrusion Prevention, ASPR, DPI-SSL, and CFS in conjunction with Single Sign-On All in Wire Mode.

HTTP/HTTPS Redirection

Topics:

When the firewall configuration requires user authentication, HTTP/HTTPS traffic from an unauthenticated source is redirected to the SonicOS login screen for the user to enter their credentials. A problem occurs when HTTP and HTTPS traffic arrive from sources from which users do not log in, and one or more such sources repeatedly try to open new connections, which keeps triggering this redirection. These could be non-user devices that are validly trying to get access or could be malicious code attempting a Denial of Service (DoS) attack. The effect that it has on the firewall is to cause high CPU load in the CP, both in the data plane task initiating the redirections and in the web server thread tasks that are serving up the target redirect pages.

To minimize this effect, ensure the **Add rule to enable redirect from HTTP to HTTPS** option is selected when adding or editing an interface. Enabling this option causes SonicOS to add an access rule that allows HTTP to the interface; a side effect of this rule is that it also allows SonicOS to be able to redirect HTTPS to HTTP in certain cases without security issues. One such case is the first step of redirecting traffic that needs to be authenticated, at which point there is no sensitive data that needs to be hidden. Then HTTP processing can occur on the data plane (DP) rather than on the CP.

NOTE: This option is not available when adding or editing VPN tunnel interfaces or when Wire Mode (2-Port Wire), Tap Mode (1-Port Tap) is selected for Mode/IP Assignment.

HTTP/HTTPS Redirection with DP Offload

This feature improves handling of HTTP/HTTPS redirection requests that occur when user authentication is required for users to get access through the firewall. HTTP/HTTPS requests received from sources that are not authenticated users are redirected to the firewall's login page, which is served up by its built-in web server. This redirection happens if Single Sign-On (SSO) cannot identify the user or if SSO is not in use.

This feature improves efficiencies in both the web server and the HTTP/HTTPS redirection processes, and offloads most of the redirection processes to the Data Plane (DP) where the processing can be spread across multiple cores.

NOTE: Elements of this feature can be controlled by internal User Authentication Settings options. This includes an option to globally enable/disable redirection processing in the DP, a flush option to clear the redirect files cache, and an option to specify the internal NAT port number used for the web server. Contact SonicWall Technical Support for information about internal settings.

Enabling DNS Proxy on an Interface

When DNS Proxy is enabled globally, you can enable it on individual interfaces. This allows you to enable the feature for different network segments independently. For how to enable DNS Proxy on an interface, see *Enabling DNS Proxy*.

LTE Modem Support

When an LTE USB modem is connected to a SonicWall firewall, SonicOS detects the model and displays a U0 interface in the **NETWORK | System > Interfaces** page. This interface belongs to the WAN zone by default and can be used for Failover and Load Balancing as well as for configuring the LTE connection, profiles and advanced settings.

LAN Bypass

The main functionality of the LAN Bypass feature, when enabled:

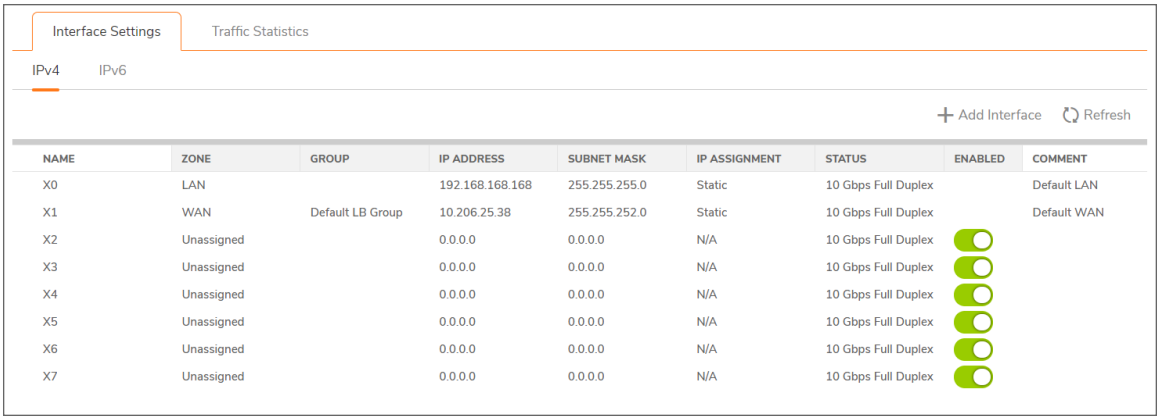
- Pass traffic in between the LBP-capable interfaces while rebooting.
- Even when the firewall is powered off, pass traffic in between those LBP-capable Interfaces.

Interface Settings IPv4

Topics:

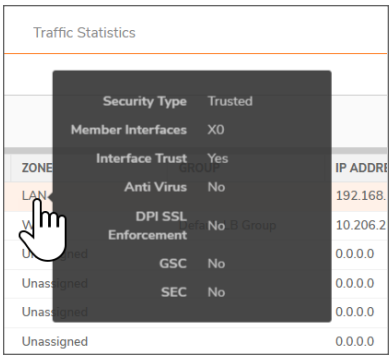
- Adding Virtual Interfaces
- Configuring Routed Mode
- Enabling Bandwidth Management on an Interface
- Configuring Interfaces in Transparent IP Mode (Splice L3 Subnet)
- Configuring Wireless Interfaces
- Configuring WAN Interfaces
- Configuring Tunnel Interfaces
- Configuring VPN Tunnel Interfaces
- Configuring Link Aggregation and Port Redundancy
- Configuring One Arm Mode
- Configuring an IPS Sniffer Mode Appliance
- Configuring Security Services (Unified Threat Management)
- Configuring Wire and Tap Mode
- Layer 2 Bridged Mode

The **Interface Settings** table lists this information for each interface:



NAME	ZONE	GROUP	IP ADDRESS	SUBNET MASK	IP ASSIGNMENT	STATUS	ENABLED	COMMENT
X0	LAN		192.168.168.168	255.255.255.0	Static	10 Gbps Full Duplex		Default LAN
X1	WAN	Default LB Group	10.206.25.38	255.255.252.0	Static	10 Gbps Full Duplex		Default WAN
X2	Unassigned		0.0.0.0	0.0.0.0	N/A	10 Gbps Full Duplex		
X3	Unassigned		0.0.0.0	0.0.0.0	N/A	10 Gbps Full Duplex		
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	10 Gbps Full Duplex		
X5	Unassigned		0.0.0.0	0.0.0.0	N/A	10 Gbps Full Duplex		
X6	Unassigned		0.0.0.0	0.0.0.0	N/A	10 Gbps Full Duplex		
X7	Unassigned		0.0.0.0	0.0.0.0	N/A	10 Gbps Full Duplex		

- **Name** - The name of the interface.
- **Zone** - LAN, WAN, and WLAN are listed by default as are DMZ and MGMT when applicable. As zones are configured, the names are listed in this column. Non-configured zones are designated Unassigned. Mousing over the zone displays zone properties:



Security Type	Displays security type selected for the zone when it was configured.
Member Interfaces	Lists interfaces assigned to this zone.
Interface Trust	Indicates whether **Allow Interface Trust** is enabled for this zone.
Anti-Virus	Indicates whether **Enable Client AV Enforcement Service** and/or **Enable Gateway Anti-Virus Service** is enabled for this zone.
DPI SSL Enforcement	Indicates whether **DPI SSL Enforcement** is enabled for this zone.
GSC	Indicates whether **Enforce Global Security Clients** (GSC) protection is enabled for this zone. For more information, see *Enabling SonicWall Security Services on Zones*.
SEC	Indicates whether **SonicWall Enforced Client (SEC)** protection is enabled for this zone.

- **Group** - If the interface is assigned to a Load Balancing group, it is displayed in this column.
- **IP Address** - IP address assigned to the interface.
- **Subnet Mask** - The network mask assigned to the subnet.
- **IP Assignment** - The available methods of IP assignment depend on the zone to which the interface is assigned:

  ⓘ | **NOTE:** Wire mode is available only on NSa 2600 and higher firewalls.

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, 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, NativeBridge Mode**

WLAN	**Static IP Mode** (default), **Layer 2 Bridged Mode, NativeBridge Mode**

- **Status** - The link status and speed.
- **Enabled** - Indicates ports that can be enabled/disabled through **NETWORK | System > Interfaces**. Ports that are enabled are indicated by an **Enabled** icon, those that are disabled by a **Disabled** icon. Clicking the icon displays a message verifying you want the port enabled/disabled. Click **OK**. The port is enabled/disabled, and the icon changes.
- **Comment** - Any user-defined comments.
- **Configure** - Click the **Edit** icon to display the dialog, which allows you to configure the settings for the specified interface. For information about configuring interfaces, see Configuring Interfaces.

Adding Virtual Interfaces

Topics:

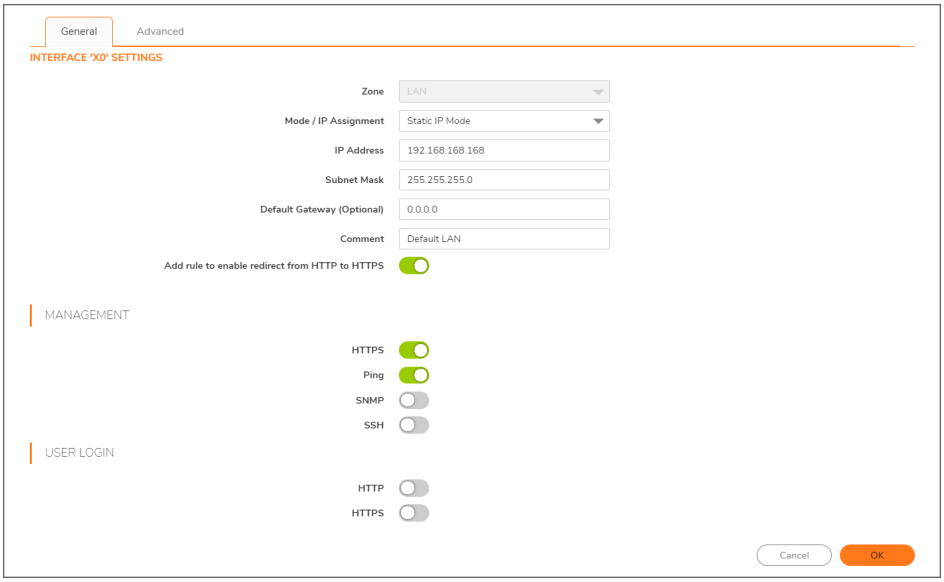
- Configuring General Settings for Virtual Interface
- Configuring Advanced Settings for a Virtual Interface
- Configuring Virtual Interfaces (VLAN Subinterfaces)

For general information on interfaces, see Physical and Virtual Interfaces.

Static means that you assign a fixed IP address to the interface.

To configure a static interface:

1. Navigate to **NETWORK | System > Interfaces**.
2. In the **Interface Settings** table, click **+ Add Interface** and select the type of interface you want to configure. The options change depending on which interface you choose. A version of the **Add Interface** dialog displays.



Configuring General Settings for Virtual Interface

To configure general settings for a virtual interface:

1. Navigate to **NETWORK | System > Interfaces | General**.
2. Select a zone to assign to the interface from Zone:
   - **LAN**
   - **WAN**
   - **DMZ**
   - **WLAN**
   - Custom zone that you have created
   - **Create new zone**. The **Add Zone** dialog is displayed. See *About Zones* for instructions on adding a zone.

ⓘ | **NOTE:** The options displayed change, depending on the Zone you select.

3. From **IP Assignment** select:
    - **Static** (default for WAN)
    - **Static IP Mode** (default for LAN)
4. Enter the IP address and subnet mask for the interface into the **IP Address** and **Subnet Mask** fields.

    NOTE: You cannot enter an IP address that is in the same subnet as another zone.
5. If configuring a:
    - WAN zone interface or the MGMT interface, enter the IP address of the gateway device into the **Default Gateway** field.

        NOTE: A default gateway IP is required on the WAN interface if any destination is required to be reached through the WAN interface that is not part of the WAN subnet IP address space, regardless whether a default route is received dynamically from a routing protocol of a peer device on the WAN subnet. A default gateway IP is optional on a LAN interface.
    - LAN zone interface or a DMZ zone interface, optionally enter the IP address of the gateway device into the **Default Gateway (Optional)** field.

    The gateway device provides access between this interface and the external network, whether it is the Internet or a private network.
6. If configuring a:
    - LAN zone interface, go to Configuring General Settings for Virtual Interface
    - WAN zone interface, enter the IP addresses of up to three DNS servers into the **DNS Server** fields. These can be public or private DNS servers. For more information, see *Configuring a WAN Interface*.
7. Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface Settings** table.
8. If you want to enable remote management of the firewall from this interface, choose the supported **Management** protocol(s): **HTTPS**, **Ping**, **SNMP**, and/or **SSH**. If **HTTPS** is chosen, **Add rule to enable redirect from HTTP to HTTPS** becomes available and selected; selecting **HTTP**, disables **Add rule to enable redirect from HTTP to HTTPS**, and it becomes dimmed.

    NOTE: Elements of this feature can be controlled by internal User Authentication Settings options. For more information, see HTTP/HTTPS Redirection with DP Offload.

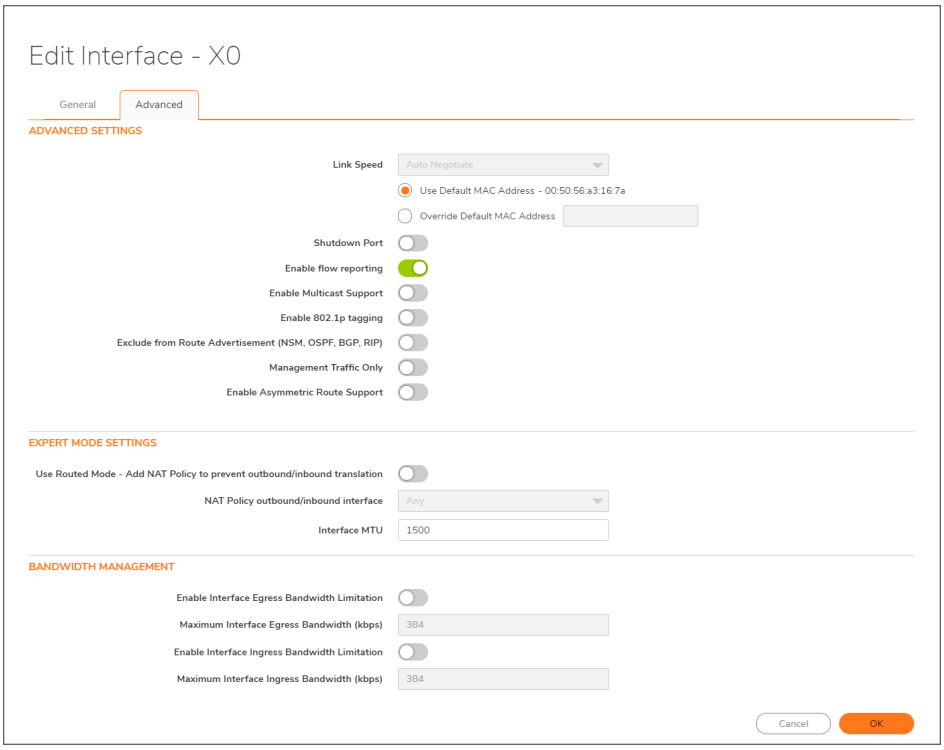
    NOTE: To allow access to the WAN interface for management from another zone on the same firewall, access rules must be created.
9. If you want to allow selected users with limited management rights to log in to the firewall, choose **HTTP** and/or **HTTPS in User Login**. If **HTTPS** is chosen, **Add rule to enable redirect from HTTP to HTTPS** becomes available and selected; selecting **HTTP**, disables **Add rule to enable redirect from HTTP to HTTPS,** and it becomes dimmed.
10. Configure **Advanced Settings**; go to *Configuring Advanced Settings for a Static Interface*.
11. Click **OK**.

    NOTE: The administrator password is required to regenerate encryption keys after changing the firewall's address.

Configuring Advanced Settings for a Virtual Interface

To configure advanced settings for a static interface:

1. In the **Add/Edit Interface** dialog, click **Advanced**.



> **NOTE:** The options available in **Advanced** for a virtual interface vary depending on the selected zone and platform.

2. For **Link Speed**, **Auto Negotiate** is selected by default, which causes the connected devices to negotiate the speed and duplex mode of the Ethernet connection automatically. To force Ethernet speed and duplex, select one of the following options from **Link Speed**:

For 1 Gbps Interfaces	For 10 Gbps Interfaces
1 Gbps - Full Duplex	10 Gbps - Full Duplex
100 Mbps - Full Duplex	
100 Mbps - Half Duplex	
10 Mbps - Full Duplex	
10 Mbps - Half Duplex	

> **CAUTION: If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the firewall as well.**

3. **Use Default MAC Address** is selected by default. You override **Use Default MAC Address** for the Interface by choosing **Override Default MAC Address** and entering the MAC address in the field.

4. Select **Shutdown Port** to temporarily take this interface offline for maintenance or other reasons. If connected, the link goes down. This option is not selected by default.
   Clear the option to activate the interface and allow the link to come back up.

   ⓘ **IMPORTANT:** You cannot shut down the management interface or the interface you are currently using.
   If you select this option, a confirmation message displays: Click **OK** to shut down the port.

   ⓘ **TIP:** You can shut down the interface by clicking the **Enabled** icon in the **Enabled** column for the interface. A confirmation message displays:
   - If you click **OK**, the **Enabled** icon turns to a **Disabled** icon. To enable the interface, click the **Disabled** icon. A confirmation message displays:
   - If you click **OK**, the **Disabled** icon turns to an **Enabled** icon.

5. For the AppFlow feature, select **Enable flow reporting** to allow flow reporting on flows created for this interface. This option is selected by default.
6. Optionally, select **Enable Multicast Support** to allow multicast reception on this interface. This option is not selected by default.
7. Optionally, select **Enable Default 802.1p CoS** to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. This option is not selected by default.

   ⓘ **NOTE:** This option is available only for VLAN interfaces.

   Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. To make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on **Policies | Rules and Policies > Access Rules**.
8. Optionally, to exclude the interface from Route Advertisement, select **Exclude from Route Advertisement (NSM, OSPF, BGP, RIP)** This option is not selected by default.
9. Optionally, select **Management Traffic Only** to restrict traffic to only SonicWall management traffic and routing protocols. This option is not selected by default.
10. Optionally, if you have enabled DNS Proxy, the **Enable DNS Proxy** option for displays for LAN, DMZ, or WLAN interfaces. To enable DNS Proxy on the interface, select the option. This option is not selected by default.
11. Optionally, enable Asymmetric Route Support on the interface by selecting **Enable Asymmetric Route Support**. If enabled, the traffic initialized from this interface supports asymmetric routes, that is, the initial packet or response packet can pass through from other interfaces. This option is not selected by default.
12. If configuring a TZ series firewall for a:
    - LAN/DMZ/WLAN interface, go to *Configuring Routed Mode*.
    - WAN interface, go to Step 15.
13. Optionally, select **Link Aggregation** or **Port Redundancy** from **Redundant /Aggregate Ports**. For more information see *Configuring Link Aggregation and Port Redundancy*.

14. To specify the largest packet size (MTU – maximum transmission unit) that a WAN interface can forward without fragmenting the packet, enter the size of the packets that the port receives and transmits in the **Interface MTU** field:

Standard packets (default)	1500
Jumbo frame packets	9000

ⓘ **NOTE:** Jumbo frame support must be enabled before a port can process jumbo frames, as explained in *Policies Administration*. Because of the jumbo frame packet buffer size requirements, jumbo frames increase memory requirements by a factor of 4.

15. Optionally, to fragment non-VPN outbound packets larger than the interface's MTU, select Fragment non-VPN outbound packets larger than this Interface's MTU. This option is selected by default. When selected, the following option becomes available.

ⓘ **IMPORTANT:** Specify fragmentation of outbound VPN traffic in **Advanced Settings**.

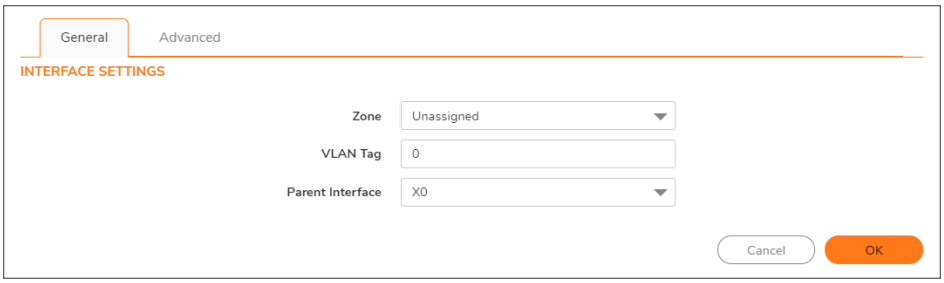
16. Optionally, to override the Do-not-fragment packet bit, select **Ignore Don't Fragment (DF) bit**. This option is not selected by default.
17. To block notification that the WAN interface can receive fragmented packets, select **Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU**. This option is not selected by default.
18. If configuring bandwidth management for this interface, go to **Enabling Bandwidth Management on an Interface**.
19. Click **OK**.

Configuring Virtual Interfaces (VLAN Subinterfaces)

When you add a VLAN subinterface, you need to assign it to a zone, assign it a VLAN Tag, and assign it to a physical interface. Based on your zone assignment, you configure the VLAN subinterface the same way you configure a physical interface for the same zone.

To add a virtual interface:

1. Navigate to **NETWORK | System > Interfaces**.
2. In **Interface Settings**, select **Virtual Interface** from **+ Add Interface**. The **Add Virtual Interface** dialog displays.



3. Select a **Zone** to assign to the interface. You can select LAN, WAN, DMZ, WLAN, or a create a new zone. The zone assignment does not have to be the same as the parent (physical) interface. In fact, the parent interface can even remain **Unassigned**.

   Your configuration choices for the network settings of the subinterface depend on the zone you select.

   - **LAN**, **DMZ**, or a **create a new zone** of Trusted type: **Static** or **Transparent**
   - **WLAN** or a custom Wireless zone: static IP only (no IP Assignment list).

4. Assign a VLAN tag (ID) to the subinterface in the **VLAN Tag** field. Valid VLAN IDs are **0** (default) to 4094, although some switches reserve VLAN 1 for native VLAN designation, and VLAN 0 is reserved for QoS. You need to create a VLAN subinterface with a corresponding VLAN ID for each VLAN you wish to secure with your appliance.

   ⓘ **IMPORTANT:** If X-Series switches are provisioned, VLAN IDs from 0 - 35 are internal VLAN IDs and cannot be used for VLAN subinterfaces.

5. Select the parent (physical) interface to which this subinterface belongs from **Parent Interface**. There is no per-interface limit to the number of subinterfaces you can assign – you can assign subinterfaces up to the system limit.

6. Configure the subinterface network settings based on the zone you selected. See the interface configuration instructions:

   - Configuring a Static Interface
   - Configuring Advanced Settings for a Static Interface
   - Configuring Interfaces in Transparent IP Mode (Splice L3 Subnet)
   - Configuring Wireless Interfaces
   - Configuring a WAN Interface

7. Select the management and user-login methods for the subinterface.
8. Click **OK**.

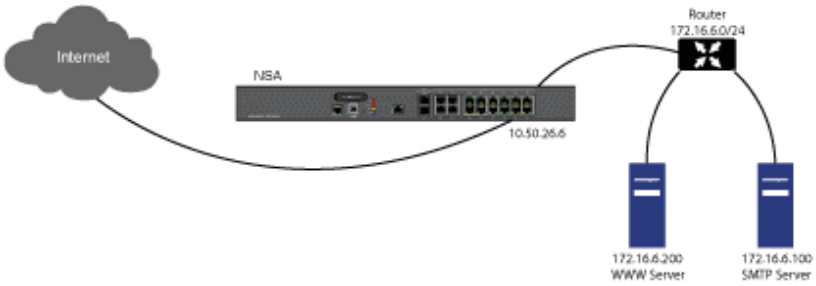
Configuring Routed Mode

Routed Mode provides an alternative for NAT for routing traffic between separate public IP address ranges. Consider the topology in *Routed Mode Configuration*, where the firewall is routing traffic across two public IP address ranges:

- 10.50.26.0/24

- 172.16.6.0/24

ROUTED MODE CONFIGURATION



By enabling Routed Mode on the interface for the 172.16.6.0 network, NAT translations are automatically disabled for the interface, and all inbound and outbound traffic is routed to the WAN interface configured for the 10.50.26.0 network.

NOTE: Routed Mode is available when using Static IP Mode for interfaces in the LAN, DMZ, and WLAN zones. For DMZ, it is also available when using Layer 2 Bridged Mode. Routed mode is not available for WAN mode.

To configure Routed Mode:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Configure** icon for the appropriate interface. The **Edit Interface** dialog displays.
3. Click **Advanced**.
4. Scroll to the **Expert Mode Settings** section.

5. To enable Routed Mode for the interface, select **Use Routed Mode - Add NAT Policy to prevent outbound\inbound translation**. This option is not selected by default. When you select it, the next **Expert Mode** setting become available.
6. From **NAT Policy outbound/inbound interface**, select the WAN interface that is to be used to route traffic for the interface. The default is **Any**.

7. To specify the largest packet size (MTU – maximum transmission unit) that the interface can forward without fragmenting the packet, enter the size of the packets that the port receives and transmits in the **Interface MTU** field:

Standard packets (default)	1500
Jumbo frame packets	9000

> **NOTE:** Jumbo frame support must be enabled before a port can process jumbo frames. Because of jumbo frame packet buffer size requirements, jumbo frames increase memory requirements by a factor of 4.

If Bandwidth Management has been enabled on the appliance, the Bandwidth Management section displays. To configure BWM for this interface, go to *Enabling Bandwidth Management on an Interface*.

8. Click **OK**.

> **IMPORTANT:** The appliance creates “no-NAT” policies for both the configured interface and the selected WAN interface. These policies override any more general M21 NAT policies that might be configured for the interfaces.

Enabling Bandwidth Management on an Interface

Bandwidth Management (BWM) allows you to guarantee minimum bandwidth and prioritize traffic. BWM is enabled in **Firewall Settings > Bandwidth Management**. By controlling the amount of bandwidth to an application or user, you can prevent a small number of applications or users from consuming all available bandwidth. Balancing the bandwidth allocated to different network traffic and then assigning priorities to traffic improves network performance.

Various types of bandwidth management can be enabled:

- **Advanced**—Enables you to configure maximum egress and ingress bandwidth limitations per interface, by configuring bandwidth objects, access rules, and application policies.
- **Global**—Allows you to enable BWM settings globally and apply them to any interfaces.
- **Global Enh**—Similar to Global, but uses a first-come, first-served queue and does not limit the number of packets processed.
- **None** (default)—Disables BWM.

For more information about configuring bandwidth management and the effect of the various BWM types, see the SonicOS administration documentation, available at https://www.sonicwall.com/support/technical-documentation.

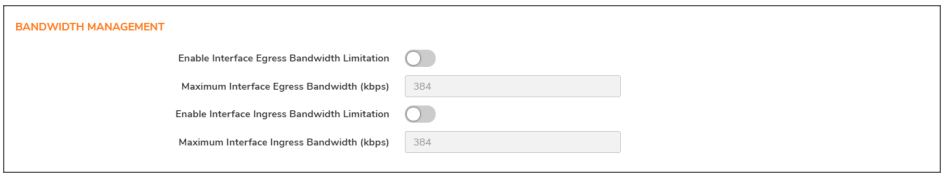
SonicOS can apply bandwidth management to both egress (outbound) and ingress (inbound) traffic on any interfaces. Outbound bandwidth management is done using Class-based Queuing. Inbound Bandwidth Management is done by implementing an ACK delay algorithm that uses TCP’s intrinsic behavior to control the traffic.

Class-based Queuing (CBQ) provides guaranteed and maximum bandwidth Quality of Service (QoS) for the firewall. Every packet destined to the interface is queued in the corresponding priority queue. The scheduler then dequeues the packets and transmits them on the link depending on the guaranteed bandwidth for the flow and the available link bandwidth.

The options described in this section are only available if Bandwidth Management is enabled in **Firewall Settings > Bandwidth Management**.

To enable or disable ingress and egress BWM:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Edit** icon of an interface. The **Edit Interface** dialog displays.
3. If this is an unassigned interface, configure the interface according to the sections contained in Configuring Interfaces.
4. On the **Advanced** screen, scroll to **Bandwidth Management**.



NOTE: Advanced Settings might differ, depending on the firewall model and the type of zone selected.

5. Enable **Bandwidth Management** for this interface.
   a. To limit outgoing traffic to a maximum bandwidth on the interface, select **Enable Interface Egress Bandwidth Limitation**. This option is not selected by default.
      Specify the maximum bandwidth, in kbps, in the **Maximum Interface Egress Bandwidth (kbps)** field. The minimum is 20 Kbps, the maximum is 1000000, and the default is 384.000000.
   b. To limit incoming traffic to a maximum bandwidth on the interface, select **Enable Interface Ingress Bandwidth Limitation**. This option is not selected by default.
      Specify the maximum bandwidth, in kbps, in the **Maximum Interface Ingress Bandwidth (kbps)** field. The minimum is 20 Kbps, the maximum is 1000000, and the default is 384.000000.

   When either of these options are:

   - Selected, the maximum available egress BWM is defined, but as advanced BWM is policy-based, the limitation is not enforced unless there is a corresponding Access Rule or App Rule.
   - Not selected, no bandwidth limitation is set at the interface level, but traffic can still be shaped using other options.
6. Optionally, select **Enable Default 802.1p tagging** to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. This option is not selected by default.
   Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. To make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled with access rules established on **POLICY | Rules and Policies > Access Rules**.
7. Click **OK**.

Configuring Interfaces in Transparent IP Mode (Splice L3 Subnet)

Topics:

Transparent IP Mode enables the appliance to bridge the WAN subnet onto an internal interface.

To configure an interface for transparent mode:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click on the **Configure** icon for the **Unassigned** interface you want to configure. The **Edit Interface** dialog is displayed.
3. Either select:
    - **LAN** or **DMZ** for **Zone**.
    - The options available change according to the type of zone you select.
    - Create a new zone for the configurable interface by selecting **Create a new zone**. The **Add Zone** dialog displays. See *About Zones* for instructions on adding a zone.
4. Select Transparent IP Mode (Splice L3 Subnet) from Mode / IP Assignment. The options change.
5. From Transparent Range, select an address object that contains the range of IP addresses you want to have access through this interface. The address range must be within an internal zone, such as LAN, DMZ, or another trusted zone matching the zone used for the internal transparent interface.
6. If you do not have an address object configured that meets your needs, select **Create New Address Object**. The **Add Address Object** dialog displays.
7. Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table. This option is not selected by default.
8. To enable remote management of the firewall from this interface, choose the supported management protocol(s): **HTTPS**, **Ping**, **SNMP**, and/or **SSH**. This option is not selected by default.
9. To allow access to the WAN interface for management from another zone on the same firewall, access rules must be created.
10. To allow selected users with limited management rights to log directly into the firewall through this interface, choose **HTTP** and/or **HTTPS** in **User Login**.
11. If you selected **HTTPS** for either **Management** and/or **User Login** protocol, **Add rule to enable redirect from HTTP to HTTPS** becomes available and selected. To prevent redirection of HTTP to HTTPS, deselect the option.
12. Selecting **HTTP** for **User Login** protocol disables redirection.
13. Elements of this feature can be controlled by internal **User Authentication Settings** options. For more

information, see *HTTP/HTTPS Redirection with DP Offload*.

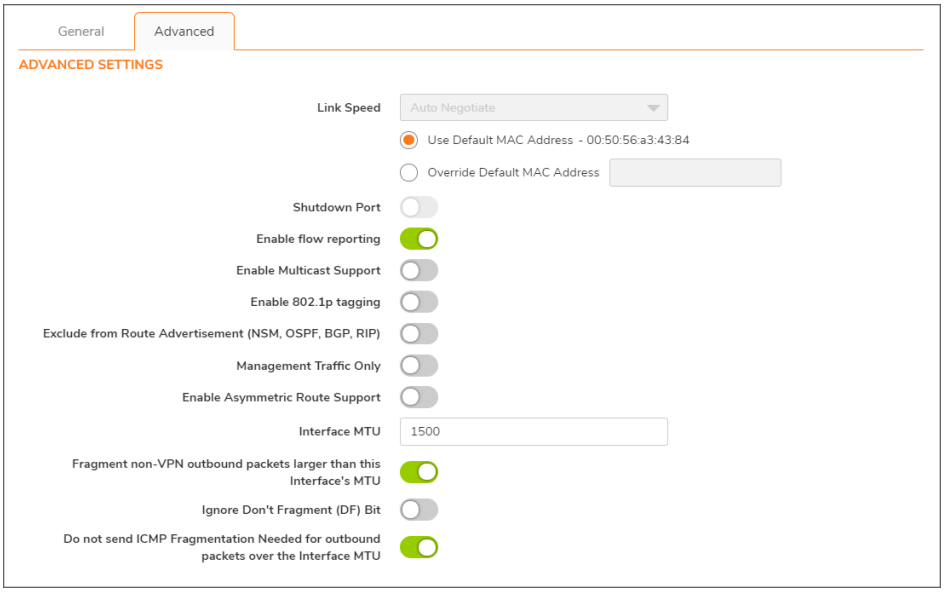
14. Click **OK**.

NOTE: The administrator password is required to regenerate encryption keys after changing the appliance's address.

Configuring Advanced Settings for a Transparent IP Mode Interface

To configure advanced settings for a transparent IP mode interface:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click **Edit** on the interface you would like to modify.
3. In the **Edit Interface** dialog, click **Advanced**.



4. For **Link Speed**, **Auto Negotiate** is selected by default, which causes the connected devices to negotiate the speed and duplex mode of the Ethernet connection automatically. To force Ethernet speed and duplex, select one of the following options from **Link Speed**:

For 1 Gbps interfaces	For 10 Gbps interfaces
1 Gbps - Full Duplex	10 Gbps - Full Duplex
100 Mbps - Full Duplex	
100 Mbps - Half Duplex	
10 Mbps - Full Duplex	
10 Mbps - Half Duplex	

CAUTION: If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the firewall as well.

5. **Use Default MAC Address** is selected by default. Override **Use Default MAC Address** for the Interface by choosing **Override Default MAC Address** and entering the MAC address in the field.
6. Select **Shutdown Port** to temporarily take this interface offline for maintenance or other reasons. If connected, the link goes down. This option is not selected by default.

   Clear the option to activate the interface and allow the link to come back up. This option is not selected by default.

   NOTE: You cannot shut down the management interface or the interface you are currently using. If you select this option, a confirmation message displays: Click **OK** to shut down the port.

   TIP: You can shut down the interface by clicking **Enabled** in the **Enabled** column for the interface. A confirmation message displays.
   - If you click **OK**, the **Enabled** icon turns to a **Disabled** icon. To enable the interface, click the **Disabled** icon. A confirmation message displays.
   - If you click **OK**, the **Disabled** icon turns to an **Enabled** icon.
7. For the AppFlow feature, select **Enable flow reporting** to allow flow reporting on flows created for this interface. This option is selected by default.
8. Optionally, select **Enable Multicast Support** to allow multicast reception on this interface. This option is not selected by default.
9. Optionally, select **Enable Default 802.1p CoS** to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. This option is not selected by default.

   NOTE: This option is available only for VLAN interfaces.

   Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. To make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on **POLICY | Rules and Policies > Access Rules**.
10. Optionally, to exclude the interface from Route Advertisement, select **Exclude from Route Advertisement (NSM, OSPF, BGP, RIP)**. This option is not selected by default.
11. Optionally, if you have enabled DNS Proxy, the **Enable DNS Proxy** option displays. To enable DNS Proxy on the interface, select the option. This option is not selected by default.
12. Optionally, enable **Asymmetric Route Support** on the interface by selecting **Enable Asymmetric Route Support**. If enabled, the traffic initialized from this interface supports asymmetric routes, that is, the initial packet or response packet can pass through from other interfaces. This option is not selected by default. For more information about asymmetric routing, see *Asymmetric Routing In Cluster Configurations*.
13. To specify the largest packet size (MTU – maximum transmission unit) that the interface can forward without fragmenting the packet, enter the size of the packets that the port receives and transmits in the **Interface MTU** field:

Standard packets (default)	1500
Jumbo frame packets	9000

14. If bandwidth management has been enabled, to configure BWM for this interface, go to Enabling Bandwidth Management on an Interface.
15. Click **OK**.

Configuring Wireless Interfaces

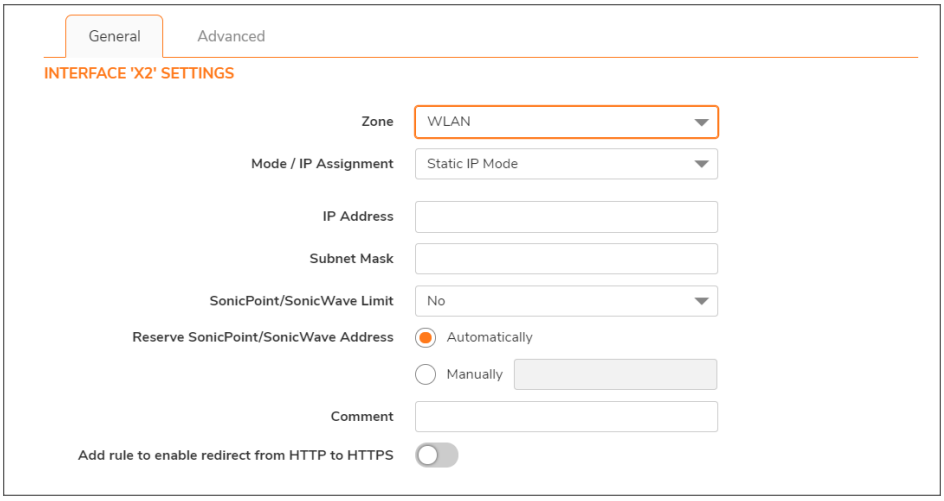
Topics:

- Configuring Advanced Settings for a Wireless Interface

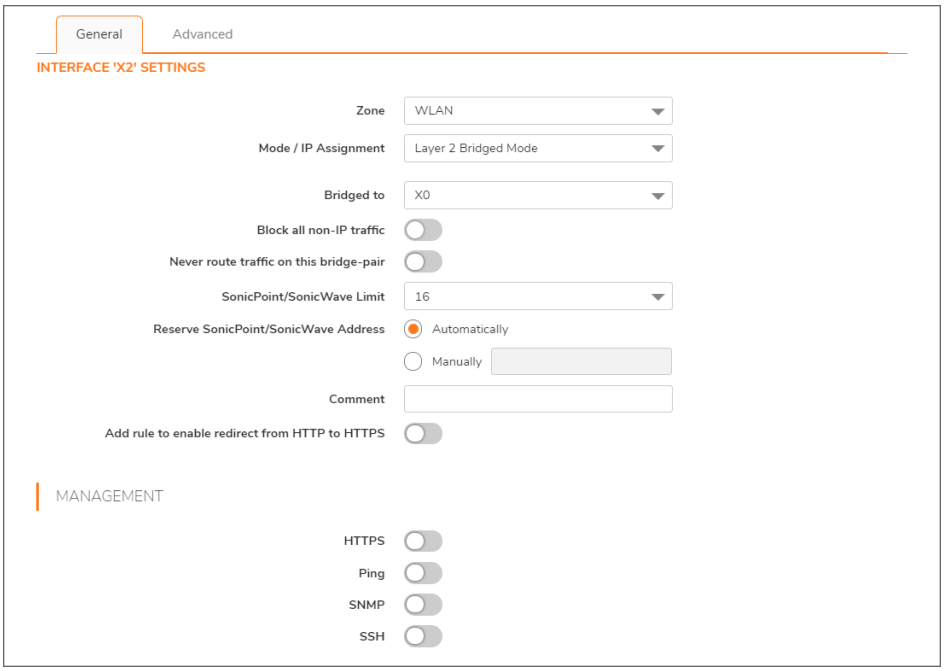
A wireless interface is an interface that has been assigned to a Wireless zone and is used to support SonicWall SonicWave secure access points.

SonicPoints can only be provisioned and managed on the interfaces of security-type wireless (WLAN by default).

To configure wireless interfaces:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Edit** icon in the **Configure** column for the interface you want to configure. The **Edit Interface** dialog displays.
3. 

4. From **Zone**, select **WLAN** or a previously defined custom Wireless zone.
5. For **Mode/IP Assignment**, select either:
   - **Static IP Mode (default)**; go to Step 12.
   - **Layer 2 Bridged Mode**:
6. Click **OK**. The options change.

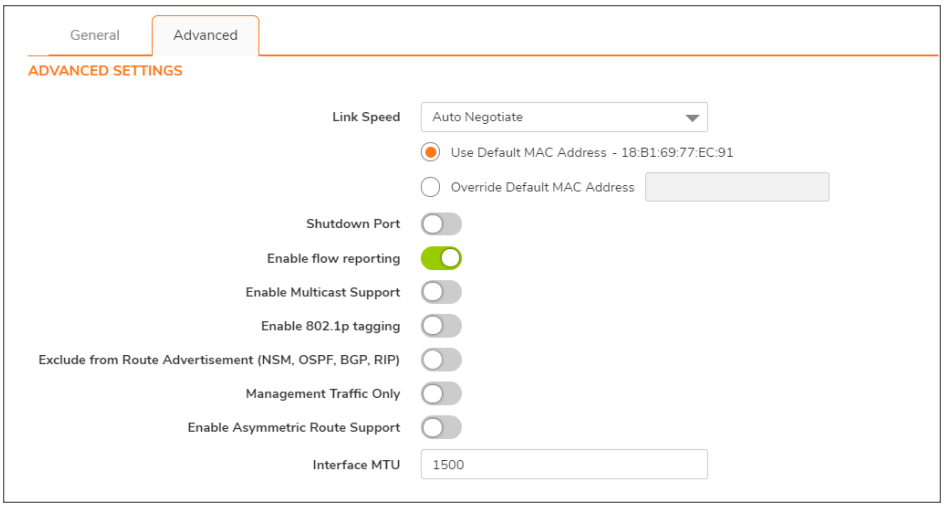
7. 

8. Select an interface to bridge to from **Bridged to**. Only those interfaces to which this interface can be bridged are displayed.
9. To block all non-IP traffic, select **Block all non-IP traffic**.
10. To never route traffic on the bridged pair, select **Never route traffic on this bridge-pair**.
11. Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.
12. If you want to enable remote management of the firewall from this interface, select the supported **Management** protocol(s): **HTTPS**, **Ping**, **SNMP**, and/or **SSH**.
13. If you want to allow selected users with limited management rights to log in to the appliance, select **HTTP** and/or **HTTPS** in **User Login**.
14. If you selected HTTPS for either **Management** or **User Login** protocol, the **Add rule to enable redirect from HTTP to HTTPS** becomes available and selected. Selecting **HTTP** for **User Login** deselects the option even if **HTTPS** is also selected.
15. Click **OK**.

Configuring Advanced Settings for a Wireless Interface

To configure advanced settings for a wireless interface:

1. In the **Edit Interface** dialog, click **Advanced**. The options you see depend on the platform of the appliance.



2. For the AppFlow feature, select **Enable flow reporting** to allow flow reporting on flows created for this interface. This option is selected by default.
3. Optionally, select **Enable Multicast Support** to allow multicast reception on this interface. This option is not selected by default.
4. Optionally, select **Enable Default 802.1p CoS** to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. This option is not selected by default.

   ⓘ | **NOTE:** This option is available only for VLAN interfaces.

   Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. To make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on **Policies | Rules and Policies > Access Rules**.
5. Optionally, to exclude the interface from Route Advertisement, select **Exclude from Route Advertisement (NSM, OSPF, BGP, RIP)**. This option is not selected by default.
6. Optionally, select **Management Traffic Only** to restrict traffic to only SonicWall management traffic and routing protocols. This option is not selected by default.
7. Optionally, if you have enabled DNS Proxy, the **Enable DNS Proxy** option displays. To enable DNS Proxy on the interface, select the option. This option is not selected by default.
8. Optionally, enable Asymmetric Route Support on the interface by selecting **Enable Asymmetric Route Support**. If enabled, the traffic initialized from this interface supports asymmetric routes, that is, the initial packet or response packet can pass through from other interfaces. This option is not selected by default. For more information about asymmetric routing, see *Asymmetric Routing In Cluster Configurations*.
9. Select **Enable Gratuitous ARP Forwarding Towards WAN** to forward gratuitous ARP packets received on this interface toward the WAN, using the hardware MAC address of the WAN interface as the source MAC address.
10. Select **Enable Automatic Gratuitous ARP Generation Towards WAN** to automatically send gratuitous ARP packets toward the WAN whenever a new entry is added to the ARP table for a new machine on this

interface. The hardware MAC address of the WAN interface is used as the source MAC address of the ARP packet.

11. To specify the largest packet size (MTU – maximum transmission unit) that the interface can forward without fragmenting the packet, enter the size of the packets that the port receives and transmits in the Interface MTU field:

Standard packets (default)	1500
Jumbo frame packets	9000

12. If configuring routed mode for this interface, go to Configuring Routed Mode.
13. If bandwidth management has been enabled, to configure BWM for this interface, go to Enabling Bandwidth Management on an Interface.
14. Click **OK**.

Configuring WAN Interfaces

Topics:

- Configuring Advanced Settings for a WAN Interface
- Configuring Protocol Settings for a WAN Interface

NOTE: A default gateway IP is required on the WAN interface if any destination is required to be reached through the WAN interface that is not part of the WAN subnet IP address space, regardless whether we receive a default route dynamically from a routing protocol of a peer device on the WAN subnet.

Configuring a WAN interface enables Internet connectivity. You can configure up to *N minus 2* WAN interfaces on the appliance, where *N* is the number of interfaces defined on the unit (both physical and VLAN). Only X0 and MGMT interfaces cannot be configured as WAN interfaces.

To configure your WAN interface:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click on the **Edit** icon in the **Configure** column for the Interface you want to configure. The **Edit Interface** dialog displays.
3. If you are configuring an unassigned Interface, select **WAN** from the Zone menu. If you selected the **Default WAN** interface, **WAN** is already selected in the **Zone** menu.
4. Select one of the following WAN Network Addressing Modes from **IP Assignment**.

   NOTE: Depending on the option you choose from the IP Assignment drop-down menu, the options available change. Complete the corresponding fields that are displayed after selecting the option.

   - **Static** - configures the appliance for a network that uses static IP addresses.
   - **DHCP** - configures the appliance to request IP settings from a DHCP server on the Internet. NAT with DHCP Client is a typical network addressing mode for cable and DSL customers.

- **PPPoE** - uses Point to Point Protocol over Ethernet (PPPoE) to connect to the Internet. If a username and password is required by your ISP, enter them into the **User Name** and **User Password** fields. This protocol is typically found when using a DSL modem.
- **PPTP** - uses PPTP (Point to Point Tunneling Protocol) to connect to a remote server. It supports older Microsoft Windows implementations requiring tunneling connectivity.
- **L2TP** - uses IPsec to connect a L2TP (Layer 2 Tunneling Protocol) server and encrypts all data transmitted from the client to the server. However, it does not encrypt network traffic to other destinations.
- **Tap Mode (1-Port Tap)** - allows insertion of the appliance into a network for use with network taps, port mirrors, or SPAN ports. For detailed information, see *Configuring Wire and Tap Mode*.
- **Wire Mode (2-Port Wire)** - allows insertion of the appliance into a network, in Bypass, Inspect, or Secure mode. For detailed information, see *Configuring Wire and Tap Mode*.
- **Static One Arm Mode** - only one firewall interface with a static IP address is used, and all traffic comes into and out from the same interface. See Configuring One Arm Mode.
- **DHCP One Arm Mode** - only one firewall interface with a DHCP IP address is used, and all traffic comes into and out from the same interface. See Configuring One Arm Mode.

5. If using **DHCP**, optionally enter a descriptive name in the **Host Name** field and any desired comments in the **Comment** field.
6. If using **PPPoE**, **PPTP**, or **L2TP**, additional fields display:
   - If **Schedule** is displayed, select the desired schedule from the drop-down menu during which this interface should be connected.
   - In **User Name** and **User Password**, type in the account name and password provided by your ISP.
   - If the **Server IP Address** field is displayed, enter the server IP address provided by your ISP.
   - If the **(Client) Host Name** field is displayed, enter the host name of the appliance. This is the firewall name from **System > Administration | Firewall Administrator**.
   - If the **Shared Secret** field is displayed, enter the value provided by your ISP.
7. If you want to enable remote management of the appliance from this interface, select the supported management protocol(s): **HTTPS**, **Ping**, **SNMP**, and/or **SSH**.

   To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. For information about creating access rules, see *SonicOS Policies Administration Guide*.
8. If using PPPoE, PPTP, or L2TP, additional fields display:
   - For PPPoE, choose one of the following:
     - **Obtain IP Address Automatically** to get the IP address from the PPPoE server.
     - **Specify IP Address** and enter the desired IP address into the field to use a static IP address for this interface.
     - **Unnumbered interface** and either:

- Select an unnumbered interface.
- Create a new unnumbered interface by selecting **Create new Unnumbered Interface**.

ⓘ | **NOTE:** The interface must be unassigned.

- For PPTP or L2TP, configure these options:
  - From **IP Assignment**, select either:
    - **DHCP**; the IP Address, Subnet Mask, and Gateway Address fields are automatically provisioned by the server.
    - **Static**, enter the appropriate values for these fields.
  - Select **Inactivity Disconnect** and enter the number of minutes of inactivity after which the connection is terminated. Clear this option to disable inactivity timeouts.

9. If using DHCP, optionally choose:
   - **Request renew of previous IP on startup** to request the same IP address for the WAN interface that was previously provided by the DHCP server.
   - **Renew DHCP lease on any link up occurrence** to send a lease renewal request to the DHCP server every time this WAN interface reconnects after being disconnected.

   The fields displayed below these options are provisioned by the DHCP server. After provisioning, these buttons are available; choose:
   - **Renew** to restart the DHCP lease duration for the currently assigned IP address.
   - **Release** to cancel the DHCP lease for the current IP address. The connection is dropped. You need to obtain a new IP address from the DHCP server to reestablish connectivity.
   - **Refresh** to obtain a new IP address from the DHCP server.
10. To allow selected users with limited management rights to log directly into the appliance from this interface, select **HTTP** and/or **HTTPS** in **User Login**.
11. Check **Add rule to enable redirect from HTTP to HTTPS**, if you want an HTTP connection automatically redirected to a secure HTTPS connection to the appliance. For more information about this option, see *HTTP/HTTPS Redirection*.
12. Continue the configuration on the **Advanced** and **Protocol** tabs (if displayed) as described in *Configuring Advanced Settings for a WAN Interface*.
13. To continue with Advanced settings; go to *Configuring Advanced Settings for a WAN Interface*.
14. If you selected **PPPoE**, **PPTP**, or **L2TP** for **IP Assignment**, go to *Configuring Protocol Settings for a WAN Interface*.
15. Click **OK**.

Configuring Advanced Settings for a WAN Interface

To configure advanced settings for a WAN interface:

1. In the **Edit Interface** dialog, click **Advanced**.
2. For **Link Speed**, **Auto Negotiate** is selected by default, which causes the connected devices to automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

For 1 Gbps interfaces	For 10 Gbps interfaces
1 Gbps - Full Duplex	10 Gbps - Full Duplex
100 Mbps - Full Duplex	
100 Mbps - Half Duplex	
10 Mbps - Full Duplex	
10 Mbps - Half Duplex	

   IMPORTANT: If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the firewall as well.

3. You can choose to override the **Use Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC address in the field.
4. Select **Shutdown Port** to temporarily take this interface off line for maintenance or other reasons. If connected, the link goes down. Clear the checkbox to activate the interface and allow the link to come back up.
5. For the AppFlow feature, select **Enable flow reporting** to allow flow reporting on flows created for this interface.
6. Select **Enable Multicast Support** to allow multicast reception on this interface.
7. Select **Enable 802.1p tagging** to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on **OBJECT | Profile Objects > QoS Marking**. For information on QoS and bandwidth management, see *SonicOS System Administration Guide*.
8. Optionally select **Link Aggregation** or **Port Redundancy** from the Redundant /Aggregate Ports drop-down menu. For more information see *Configuring Link Aggregation and Port Redundancy*.
9. **Interface MTU** - Specifies the largest packet size that the interface can forward without fragmenting the packet. Identify the size of the packets that the port receives and transmits:

Standard packets (default)	1500
Jumbo frame packets	9000

   - **Fragment non-VPN outbound packets larger than this Interface's MTU** - Specifies all non-VPN outbound packets larger than this Interface's MTU be fragmented. Specifying the fragmenting

of VPN outbound packets is set in **Network| IPSec VPN | Policies/Settings**; for more information about VPN traffic, see *SonicOS Network Administration Guide*.

- **Ignore Don't Fragment (DF) Bit** - Overrides DF bits in packets.
- **Suppress ICMP Fragmentation Needed message generation** - blocks notification that this interface can receive fragmented packets.

10. If using DHCP, the following options are displayed:
    - Select **Initiate renewals with a Discover when using DHCP** if the server might change.
    - Select **Use an interval of _ seconds between DHCP Discovers** during lease acquisition and adjust the number of seconds for the interval if the DHCP server might not respond immediately.
11. Optionally enable Bandwidth Management for this interface. For more information about Bandwidth Management, see Enabling Bandwidth Management on an Interface.

Configuring Protocol Settings for a WAN Interface

If you specified a **PPPoE**, **PPTP**, or **L2TP** for **IP assignment** when configuring the WAN interface, the **Edit Interface** dialog displays the **Protocol** view.

The Internet Service Provider (ISP) provisions the fields (for example, **SonicWall IP Address**, **Subnet Mask**, and **Gateway Address**) in the **Settings Acquired via** section of the **Protocol** view. These fields show actual values after you connect the appliance to the ISP.

Additionally, specifying PPPoE causes SonicOS to set the **Interface MTU** option in the **Advanced** view to **1492** and provides additional settings in the **Protocol** view.

To configure additional settings for PPPoE:

1. In the **Edit Interface** dialog, click **Protocol**.
2. Enable the following options in the **PPPoE Client Settings** section:
    - **Inactivity Disconnect (minutes)**: Enter the number of minutes (the default is 10) after which SonicOS terminates the connection when it detects that packets are not being sent. This option is not selected by default.
    - **Strictly use LCP echo packets for server keep-alive**: Select this to have SonicOS terminate the connection if it detects that the PPoE server has not sent a ppp LCP echo request packet within a minute. Select this option only if your PPPoE server supports the send LCP echo function. This option is not selected by default.
    - **Reconnect the PPPOE client if the server does not send traffic for __ minutes**: Enter the number of minutes (the default is **5**) after which SonicOS terminates the PPPoE server's connection, and then reconnects, if the server does not send any packets (including the LCP echo request). This option is selected by default.
    - If your PPPoE connectivity is not stable, you can amend the **Ncp Retrans Time**. SonicWall suggests changing this figure to 2000, but you could have better results making it 1999.

Configuring Tunnel Interfaces

You can configure several types of tunnel interfaces in SonicOS:

- Numbered and unnumbered tunnel interfaces, WLAN tunnel interfaces, and IPv6 6to4 tunnel interfaces are configured on **NETWORK | System > Interfaces**.
- Drop tunnel interfaces and VPN tunnel interfaces are configured from **NETWORK | System > Dynamic Routing**; for more information, see *Configuring Route Advertisements and Route Policies*.
- Unnumbered tunnel interfaces are configured as part of a VPN policy from **NETWORK | IPSec VPN > Rules and Settings**; for information about VPN policies, see the *SonicOS IPSec VPN Administration Guide*.

Numbered and unnumbered tunnel interfaces are used with VPNs. A numbered tunnel interface is assigned its own IP address, but an unnumbered tunnel interface borrows an IP address from an existing physical or virtual (VLAN) interface.

Both numbered and unnumbered tunnel interface types support static routing and dynamic routing with RIP and OSPF, while numbered tunnel interfaces can also be used with BGP.

Also, both numbered VPN and unnumbered tunnel interfaces can support advanced routing, and unnumbered tunnel interfaces have no restrictions.

See these sections for configuring the various types of tunnel interfaces:

- Numbered Tunnel Interfaces; see *Configuring VPN Tunnel Interfaces*
- Unnumbered Tunnel Interfaces; see *SonicOS Network Administration Guide*
- WLAN Tunnel Interfaces; see *Creating a WLAN Tunnel Interface*
- Drop Tunnel Interfaces; see *Drop Tunnel Interface*
- IPv6 6to4 Tunnel Interfaces; see *Configuring the 6to4 Auto Tunnel*

Configuring VPN Tunnel Interfaces

You can create a numbered tunnel interface by selecting **VPN Tunnel Interface** from the **Add Interface** drop-down menu. VPN tunnel interfaces are added to the Interface Settings table and then can be used with dynamic routing, including RIP, OSPF, and BGP, or a static route policy can use the VPN tunnel interface as the interface in a configuration for a static route-based VPN.

A VPN Tunnel Interface (TI) can be configured like a standard interface, including options to enable appliance management or user login using HTTP, HTTPS, Ping, or SSH in addition to multicast, flow reporting, asymmetric routing, fragmented packet handling, and Don't Fragment (DF) Bit settings.

ⓘ **NOTE:** A similar VPN policy and numbered tunnel interface must be configured on the remote gateway. The IP addresses assigned to the numbered tunnel interfaces (on the local gateway and the remote gateways) must be on the same subnet.

VPN tunnel interface deployment lists how a VPN Tunnel Interface can be deployed.

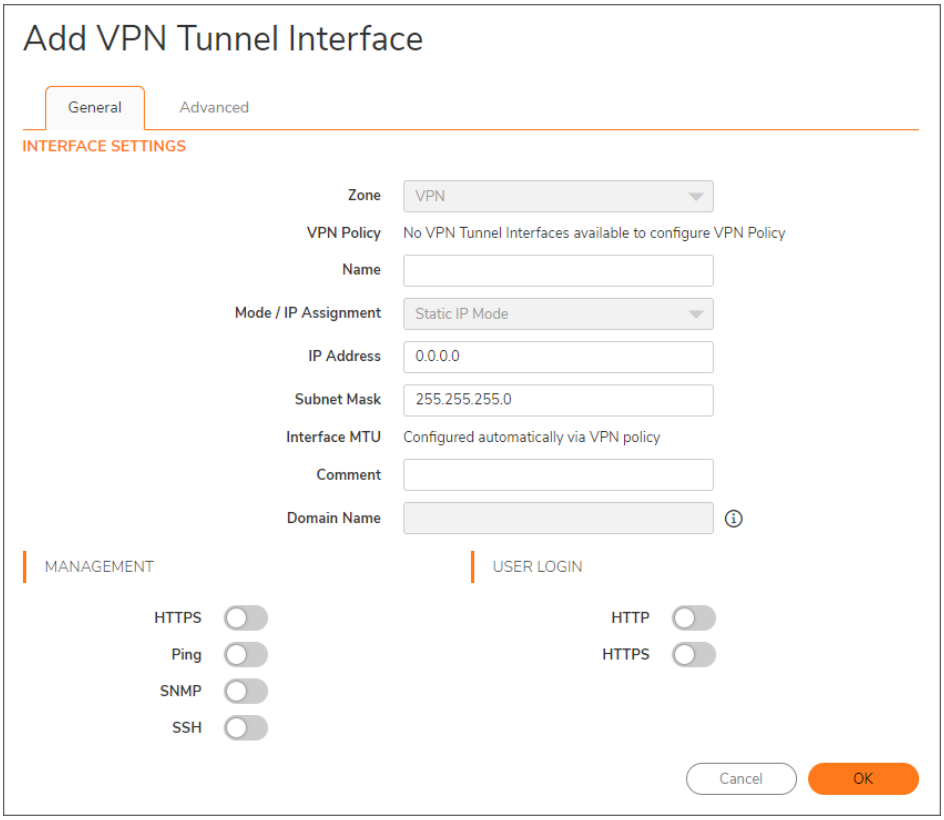
VPN TUNNEL INTERFACE DEPLOYMENT

TI can be configured as an interface in	TI cannot be configured as
Static Route	Static ARP entries interface
NAT	HA interface
ACL (Virtual Access Point Access Control List)	WLB (WAN Load Balancing) interface
	Static NDP (Neighbor Discovery Protocol) entries interface
OSPF	OSPFv3/RIPnG: currently not supported for IPv6 advanced routing
RIP	MAC_IP Anti-spoof interface
BGP	DHCP server interface

For all platforms, the maximum supported number of VPN Tunnel Interfaces (numbered tunnel interfaces) is 64. The maximum number of unnumbered tunnel interfaces differs by platform and directly corresponds to the maximum number of VPN policies supported on each platform.

To configure a VPN Tunnel Interface:

1. Navigate to **NETWORK | System > Interfaces**.
2. From **Add Interface** under the **Interface Settings** table, select **VPN Tunnel Interface**. The **Add VPN Tunnel Interface** dialog displays.

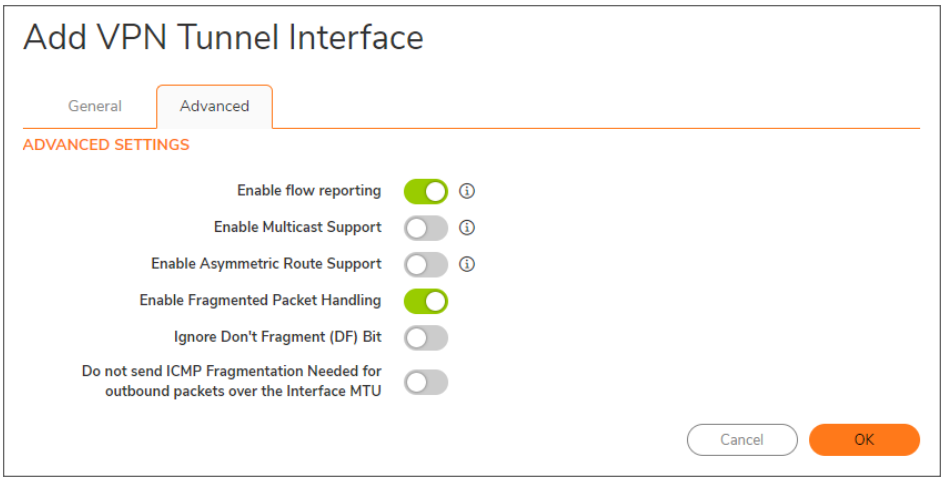


The zone is defined as VPN and cannot be changed.

3. From **VPN Policy**, select a VPN policy.
4. In the **Name** field, enter a friendly name for this interface. The name can contain alphanumeric characters, periods (dots), or underscores; it cannot contain spaces or hyphens.
5. Enter an IP address in the **IP Address** field. The default is `0.0.0.0`, but you need to enter an explicit IP address or an error message displays.
6. In the **Subnet Mask** field, enter the subnet mask. The default is `255.255.255.0`.
7. Optionally, add a comment in the **Comment** field.
8. The **Domain Name** field is used to bound an accurate domain name with all web services provided by this interface. The value can be one of the following:
   - An FQDN address (`*.company.com / www.company.com`)
   - An IPv4 or IPv6 address string (`a.a.a.a / b:b:b:b:b:b:b:b`)

     When configured, all web access, along with SSL VPN service, should be accessed by only the **Domain Name**. No other attempts are allowed.

     ⓘ | **NOTE:** Access through an exact IP address is implicitly trusted, whether this field is set or not. To enable this feature, make sure the **Enforce HTTP Host Header Check** option located on the Administrator page, is enabled as well.
9. Optionally, specify the **Management** protocol(s) allowed on this interface: **HTTPS**, **Ping**, **SNMP**, and/or **SSH**.
10. Optionally, specify the **User Login** protocol(s) allowed on this interface: **HTTP** and/or **HTTPS**.
11. Click **Advanced**.



12. To enable flow reporting on flows created for the tunnel interface, select **Enable flow reporting**.
13. Optionally, enable multicast reception on the interface by selecting **Enable Multicast Support**. This option is not selected by default.

14. Optionally, enable Asymmetric Route Support on the tunnel interface by selecting **Enable Asymmetric Route Support**. This option is not selected by default. For more information about asymmetric routing, see *Asymmetric Routing*.
15. To use Routed Mode and add a NAT policy to prevent outbound/inbound translation, select **User Routed Mode – Add NAT Policy to prevent outbound/inbound translation**. When selected, the following option becomes available. This option is not selected by default.
16. If **Routed Mode** is selected, to specify an interface for the NAT policy, select an interface from NAT Policy outbound/inbound interface. The available interfaces depend on your appliance. The default is **ANY**.
17. To enable fragmented packet handling on this interface, select **Enable Fragmented Packet Handling**. If this option is not selected, fragmented packets are dropped and the VPN log report shows the log message Fragmented IPsec packet dropped.

    If this option is selected, the **Ignore Don't Fragment (DF) Bit** option is available.
18. Select **Ignore Don't Fragment (DF) Bit** to ignore the DF bit in the packet header. Some applications can explicitly set the **Don't Fragment** option in a packet, which tells all appliances to not fragment the packet. This option, when enabled, causes the appliance to ignore the DF bit and fragment the packet regardless.
19. Select **Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU** to block the notification that this interface can receive fragmented packets.
20. Click **OK**. The numbered VPN tunnel interface is added to the **Interface Settings** table.

Configuring Link Aggregation and Port Redundancy

Both Link Aggregation and Port Redundancy are configured on the **Advanced** view of the **Edit Interface** dialog in the SonicOS Management Interface.

- **Link Aggregation** - Groups multiple Ethernet interfaces together forming a single logical link to support greater throughput than a single physical interface could support. This provides the ability to send multi-gigabit traffic between two Ethernet domains.
- **Port Redundancy** - Configures a single redundant port for any physical interface that can be connected to a second switch to prevent a loss of connectivity in the event that either the primary interface or primary switch fail.

Topics:

Link Aggregation

Link Aggregation is based on interface link speed, for example: a 10 Gbps port cannot be link aggregated with another interface that does not support 10 Gbps. Any ports that are link aggregated together should support the

same link speeds.

Link Aggregation allows you to interconnect devices with two or more links between them in such a way that the multiple links are combined into one larger virtual pipe that can carry a higher combined bandwidth. Because multiple links are present between the two devices, when one link fails, the traffic is transferred through the other links without disruption. With multiple links being present, traffic can also be load balanced in such a way to achieve even distribution.

Link Aggregation is also used to increase the available bandwidth between the firewall and a switch by aggregating up to four interfaces into a single aggregate link, referred to as a Link Aggregation Group (LAG). All ports in an aggregate link must be connected to the same switch. The appliance uses a round-robin algorithm for load balancing traffic across the interfaces in a Link Aggregation Group. Link Aggregation also provides a measure of redundancy, in that if one interface in the LAG goes down, the other interfaces remain connected.

There are two types of LAG: Static and Dynamic. With Static Link Aggregation all configuration settings are set up on both participating LAG components. Static LAG is already supported on NSA and SuperMassive platforms in SonicOS 6.2.7 and previous firmware releases.

Dynamic Link Aggregation is supported using LACP defined by the IEEE 802.3ad standard. LACP allows the exchange of information related to link aggregation between the members of the link aggregation group in protocol packets called Link Aggregation Control Protocol Data Units. With LACP, errors in configuration, wiring, and link failures can be detected quickly.

Link Aggregation is referred to using different terminology by different vendors, including Port Channel, Ether Channel, Trunk, and Port Grouping.

The two major benefits of LAG are increased throughput and link redundancy that can be achieved efficiently using LACP. LACP is the signaling protocol used between members in a LAG. It ensures links are only aggregated into a bundle when they are correctly configured and cabled. LACP can be configured in one of two modes:

- **Active mode** - the device immediately sends LACP PDUs when the port comes up.
- **Passive mode** - the port is placed in a passive negotiating state, in which the port only responds to LACP PDUs it receives but does not initiate LACP negotiation.

If both sides are configured as Active, LAG can be formed assuming successful negotiation of the other parameters. If one side is configured as Active and the other one as Passive, LAG can be formed as the Passive port responds to the LACP PDUs received from the Active side. If both sides are Passive, LACP fails to negotiate the bundle. Passive mode is rarely used in deployments.

During the configuration, all member ports of the same LAG must be set up on the same VLAN as the Aggregator port. Data packets received on the LAG members are associated with the parent Aggregator port using the VLAN. After the state of the Aggregator/member ports of a LAG reaches a stable Collection/Distribution state, the ports are ready to transmit and receive data traffic.

All information related to LAG such as the Aggregator ports configured, member ports that are part of the LAG, status of each of the ports that form the LAG, and the Partner MAC address received by way of LACP are displayed on the **NETWORK | Switching > Link Aggregation** page.

There, you will see six load balancing options are available for configuration. The load balancing option needs to be chosen during creation of a LAG when the Aggregator port is chosen. You cannot modify the load balancing option after the LAG is created.

- SRC_MAC, ETH_TYPE, VLAN, INTF
- DST_MAC, ETH_TYPE, VLAN, INTF
- SRC_MAC, DST_MAC, ETH_TYPE,VLAN, INTF
- SRC_IP, SRC_PORT
- DST_IP, DST_PORT
- SRC_IP, SRC_PORT, DST_IP, DST_PORT

Topics:

Link Aggregation Failover

SonicWall provides multiple methods for protecting against loss of connectivity in the case of a link failure, including High Availability (HA), Load Balancing Groups (LB Groups), and now Link Aggregation. If all three of these features are configured on an appliance, the following order of precedence is followed in the case of a link failure:

1. High Availability
2. Link Aggregation
3. Load Balancing Groups

HA takes precedence over Link Aggregation. Because each link in the LAG carries an equal share of the load, the loss of a link on the Active firewall forces a failover to the Idle firewall (if all of its links remain connected). Physical monitoring needs to be configured only on the primary aggregate port.

When Link Aggregation is used with a LB Group, Link Aggregation takes precedence. LB takes over only when all the ports in the aggregate link are down.

Link Aggregation Limitations

- Currently only static addressing is supported for Link Aggregation. Static port channel, which is referred to as PAG (port aggregation), is one way of configuring Ethernet port channels. No LACP or PAGP packets are sent out to form an EtherChannel with the partnering device (switch or server and so on).
- A static Link Aggregation Group (LAG) configured with Ethernet port channels must be manually configured/bundled for NSa 3600 or higher firewalls.
- The dynamic Link Aggregation Control Protocol (LACP) is not supported on TZs but is available for use with the NSa 2700 and higher. Dynamic, through a protocol to bundle Ethernet ports such as IEEE LACP or Cisco's PAGP, is another way of configuring Ethernet port channels. In this method, LACP or PAGP packets are sent out on the port.
- LACP only works with interfaces connected to the internal SonicWall switch.

Link Aggregation Configuration

To configure Link Aggregation:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Configure** icon for the interface that is to be designated the master of the Link Aggregation Group. The **Edit Interface** dialog displays.
3. Click **Advanced**.
4. From **Redundant/Aggregate Ports**, select **Link Aggregation**. More options appear.
5. The **Aggregate Port** option displays with each of the currently unassigned interfaces on the appliance. None of the ports are selected. Select up to three other interfaces to assign to the LAG.

   ⓘ **NOTE:** After an interface is assigned to a Link Aggregation Group, its configuration is governed by the Link Aggregation master interface and it cannot be configured independently. In the **Interface Settings** table, the interface's zone is displayed as **Aggregate Port** and the **Configuration** icon is removed.
6. Set the **Link Speed** for the interface to **Auto-Negotiate**.
7. Click **OK**. If Web Management has not been configured for the interface, a message displays.
   a. Click **OK**.
   b. Enable **Web Management** on another interface.

ⓘ **IMPORTANT:** Link Aggregation requires a matching configuration on the switch. The switch's method of load balancing varies depending on the vendor. Consult the documentation for the switch for information on configuring Link Aggregation. Remember that it might be referred to as Port Channel, Ether Channel, Trunk, or Port Grouping.

Port Redundancy

Port Redundancy provides a simple method for configuring a redundant port for a physical Ethernet port. This is a valuable feature, particularly in high-end deployments, to protect against switch failures being a single point of failure.

When the primary interface is active, it processes all traffic to and from the interface. If the primary interface goes down, the secondary interface takes over all outgoing and incoming traffic. The secondary interface assumes the MAC address of the primary interface and sends the appropriate gratuitous ARP on a failover event. When the primary interface comes up again, it resumes responsibility for all traffic handling duties from the secondary interface.

In a typical Port Redundancy configuration, the primary and secondary interfaces are connected to different switches. This provides for a failover path in case the primary switch goes down. Both switches must be on the same Ethernet domain. Port Redundancy can also be configured with both interfaces connected to the same switch.

Port Redundancy Failover

SonicWall provides multiple methods for protecting against loss of connectivity in the case of a link failure, including High Availability (HA), Load Balancing Groups (LB Groups), and now Port Redundancy. If all three of these features are configured on an appliance, the following order of precedence is followed in the case of a link failure:

1. Port Redundancy
2. HA
3. LB Group

When Port Redundancy is used with HA, Port Redundancy takes precedence. Typically an interface failover causes an HA failover to occur, but if a redundant port is available for that interface, then an interface failover occurs, but not an HA failover. If both the primary and secondary redundant ports go down, then an HA failover occurs (assuming the secondary firewall has the corresponding port active).

When Port Redundancy is used with a LB Group, Port Redundancy again takes precedence. Any single port (primary or secondary) failures are handled by Port Redundancy just like with HA. When both the ports are down then LB kicks in and tries to find an alternate interface.

Port Redundancy Configuration

To configure Port Redundancy:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Configure** icon for the interface that is to be designated the master of the Link Aggregation Group. The **Edit Interface** dialog displays.
3. Click **Advanced**.
4. Set the **Link Speed** for the interface to **Auto-Negotiate**.
5. From **Redundant/Aggregate Ports**, select **Port Redundancy**. Another option displays.
6. The **Redundant Port** option displays all of the currently unassigned interfaces available. Select one of the interfaces; the default is **None**.

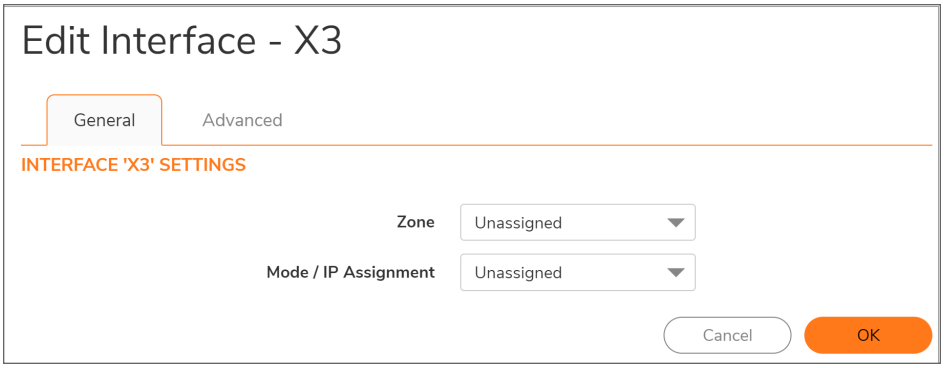
   ⓘ **NOTE:** After an interface is selected as a Redundant Port, its configuration is governed by the primary interface and it cannot be configured independently. In the **Interface Settings** table, the interface's zone is displayed as **Redundant Port**, and the **Configuration** icon is removed.
7. Click **OK**. If Web Management has not been configured for the interface, a message displays.
   a. Click **OK**.
   b. Enable **Web Management** on another interface.

Configuring One Arm Mode

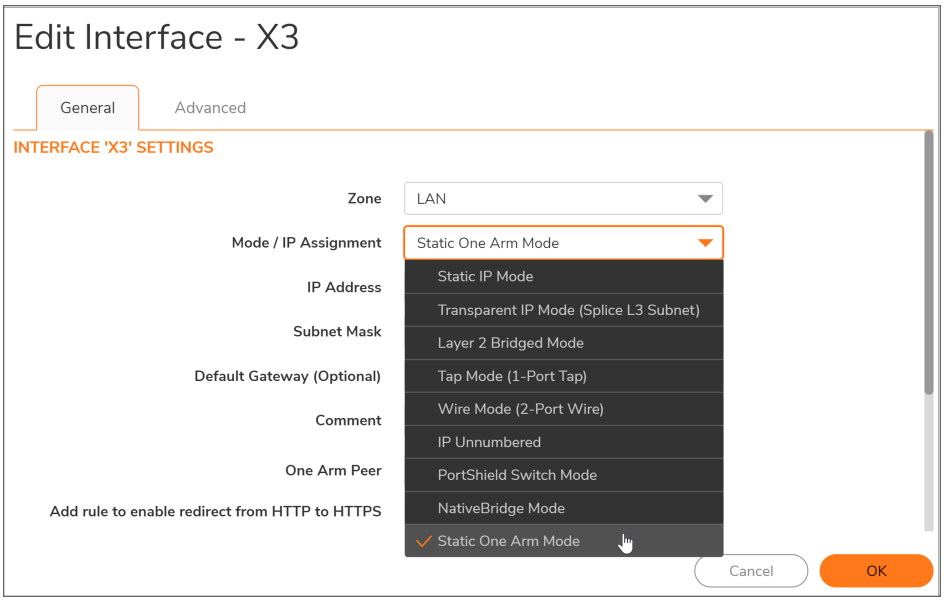
For more information about One Arm Mode, refer to One Arm Mode and Single Interface Support.

To configure an interface for One Arm Mode:

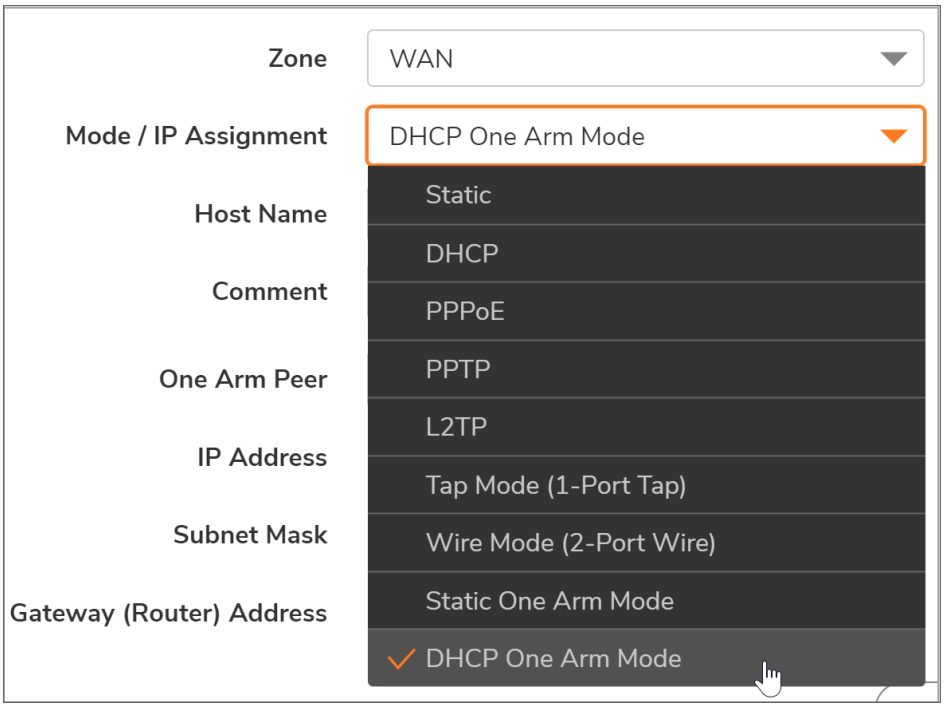
1. Navigate to **NETWORK | System > Interfaces**.
2. Click on the Edit icon for the desired interface. The **Edit Interface** dialog displays.



3. For **Zone**, select **LAN** or **WAN**. One Arm Mode is only supported for these zones. The dialog displays more fields.

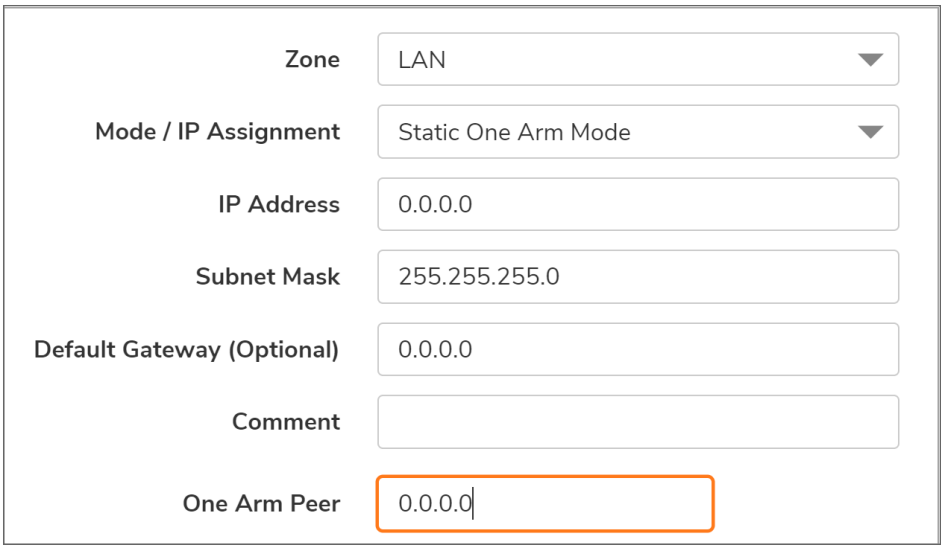


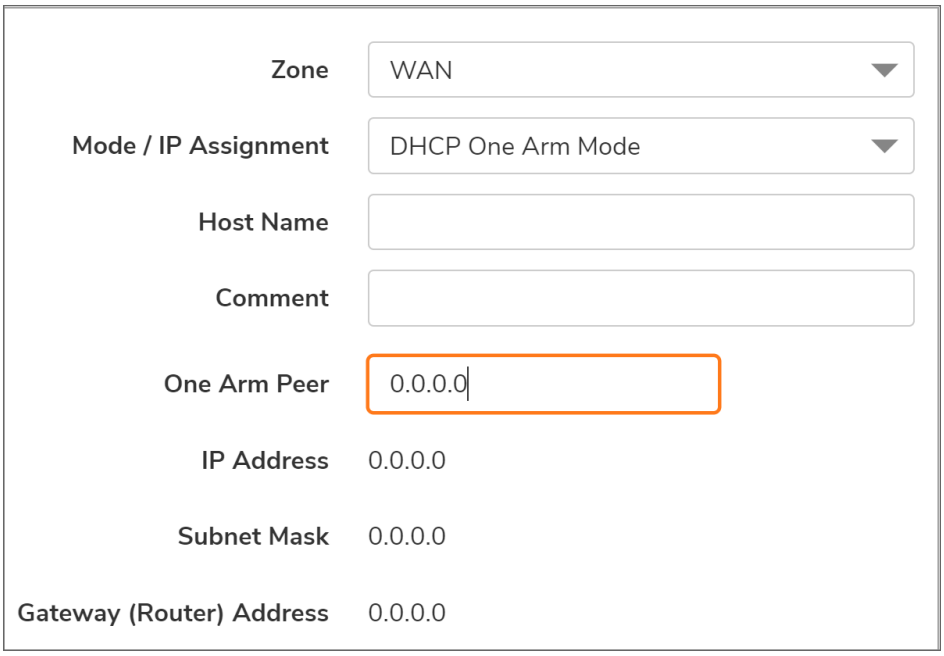
4. For **Mode/IP Assignment**, select an available One Arm Mode option:
   - **Static One Arm Mode**
   - **DHCP One Arm Mode**



DHCP One Arm Mode is not always offered, but it might be available with either the LAN or WAN zone.

5. For **One Arm Peer**, enter the IP address of the next-hop destination for traffic going out of the interface.





The interface **IP Address** and the **One Arm Peer** address can be in the same subnet, but this is not required. A Route Policy is automatically created. See One Arm Mode and Single Interface Support for more information about automatic system configuration changes.

6. Fill in the other fields in the **Edit Interface** dialog.

   Depending on the zone and whether **Static One Arm Mode** or **DHCP One Arm Mode** is selected, other fields might differ. In general, the other fields displayed with **Static One Arm Mode** selected match those displayed with a **Mode/IP Assignment** of **Static**. And the other fields shown with **DHCP One Arm Mode** selected match those shown with a **Mode/IP Assignment** of **DHCP**.

7. When done, click **OK**.

Configuring an IPS Sniffer Mode Appliance

To configure the appliance for IPS Sniffer Mode, use two interfaces in the same zone for the L2 Bridge-Pair. You can use any interfaces except the WAN interface. For this example, X2 and X3 are used for the Bridge-Pair and are configured in the LAN zone. The WAN interface (X1) is used by the firewall for access to the firewall Data Center as needed. The mirrored port on the switch connects to one of the interfaces in the Bridge-Pair.

Topics:

Configuration Task List for IPS Sniffer Mode

- Configure the Primary Bridge Interface
    - Select LAN as the Zone for the Primary Bridge Interface
    - Assign a static IP address
- Configure the Secondary Bridge Interface
    - Select LAN as the Zone for the Secondary Bridge Interface
    - Enable the L2 Bridge to the Primary Bridge interface
- Enable SNMP and configure the IP address of the SNMP manager system where traps can be sent
- Configure Security Services for LAN traffic
- Configure logging alert settings to “Alert” or below
- Connect the mirrored port on the switch to either one of the interfaces in the Bridge-Pair
- Connect and configure the WAN to allow access to dynamic signature data over the Internet

Configuring the Primary Bridge Interface

To configure the primary bridge interface:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Configure** icon in the right column of interface X2. The **Edit Interface** dialog displays.
3. Select **LAN** from the **Zone** drop-down menu. More options display.
   ⓘ | **NOTE:** You do not need to configure settings on the **Advanced** or **VLAN Filtering** tabs.
4. For **Mode / IP Assignment**, select **Static IP Mode**.
5. Configure the interface with a static **IP Address** (for example, `10.1.2.3`). The IP address you choose should not collide with any of the networks that are seen by the switch.
   ⓘ | **NOTE:** The Primary Bridge Interface must have a static **Mode / IP Assignment**.
6. In the **Subnet Mask** field, enter the subnet mask. The default is `255.255.255.0`.
7. A gateway is optional for DMZ and LAN zone interfaces. If desired, type the IP address of the gateway device into the **Default Gateway** field. The gateway device provides access between this interface and the external network, whether it is the Internet or a private network.

ⓘ | **NOTE:** A default gateway IP is required on a WAN interface if any destination is required to be reached through the WAN interface that is not part of the WAN subnet IP address space, regardless whether we receive a default route dynamically from a routing protocol of a peer device on the WAN subnet.

8. Type in a descriptive **Comment**.
9. The **Domain Name** field is used to bound an accurate domain name with all web services provided by this interface. The value can be one of the following:
   - An FQDN address (`*.company.com / www.company.com`)
   - An IPv4 or IPv6 address string (`a.a.a.a / b:b:b:b:b:b:b:b`)

     When configured, all web access, along with SSL VPN service, should be accessed by only the **Domain Name**. No other attempts are allowed.

     ⓘ | **NOTE:** Access through an exact IP address is implicitly trusted, whether this field is set or not.

     To enable this feature, make sure the **Enforce HTTP Host Header Check** option located on the Administrator page, is enabled as well.
10. Choose **Management** option(s) for the interface: **HTTPS**, **Ping**, **SNMP**, **SSH**.
11. Choose **User Login** options: **HTTP**, **HTTPS**.
12. To enable redirect to HTTPS from HTTP, select **Add rule to enable redirect from HTTP to HTTPS**. For more information about this option, see *HTTP/HTTPS Redirection*.
13. Click **OK**.

Configuring the Secondary Bridge Interface

Our example continues with X3 as the secondary bridge interface.

To configure the secondary bridge interface:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Configure** icon in the right column of interface X2. The **Edit Interface** dialog displays.
3. Select **LAN** from the **Zone** drop-down menu. More options display.

   ⓘ | **NOTE:** You do not need to configure settings on the **Advanced** or **VLAN Filtering** tabs.
4. From **IP Assignment**, select **Layer 2 Bridged Mode**.
5. From **Bridged to**, select the **X2** interface.
6. Do not enable the **Block all non-IP traffic** setting if you want to monitor non-IP traffic.
7. Select **Never route traffic on this bridge-pair** to ensure that the traffic from the mirrored switch port is not sent back out onto the network.
8. Select **Disable stateful-inspection on this bridge-pair** to exempt these interfaces from stateful high availability inspection. If Deep Packet Inspection services are enabled for these interfaces, the DPI services continue to be applied.
9. Choose **Management** option(s) for the interface: **HTTPS**, **Ping**, **SNMP**, **SSH**.

10. Choose **User Login** options: **HTTP**, **HTTPS**.
11. To enable redirect to HTTPS from HTTP, select **Add rule to enable redirect from HTTP to HTTPS**. For more information about this option, see *HTTP/HTTPS Redirection*.
12. Click **OK**.

Configuring SNMP

When SNMP is enabled, SNMP traps are automatically triggered for many events that are generated by SonicWall Security Services such as Intrusion Prevention and Gateway Anti-Virus (GAV).

More than 50 IPS and GAV events currently trigger SNMP traps. The *SonicOS Log Administration Guide* contains a list of events that are logged by SonicOS, and includes the SNMP trap number where applicable. This guide is available online at https://www.sonicwall.com/support/technical-documentation by selecting any SonicWall platform that runs SonicOS.

To determine the traps that are possible when using IPS Sniffer Mode with Intrusion Prevention enabled, search for **Intrusion** in the table found in the Index of Log Event Messages section in the *SonicOS Log Administration Guide*. The SNMP trap number, if available for that event, is printed in the **SNMP Trap Type** column of the table.

To determine the possible traps with Gateway Anti-Virus enabled, search the table for **Security Services**, and view the SNMP trap number in the **SNMP Trap Type** column.

To enable and configure SNMP:

1. Navigate to **DEVICE | Settings > SNMP**.
2. Select **Enable SNMP**.
3. Click **Accept**. **Configure** becomes active.
4. Click **Configure**. The **SNMP Settings** dialog displays.
5. In the **System Name** field, type the name of the SNMP manager system that receives the traps sent from the firewall.
6. Enter the name or email address of the contact person for the SNMP Contact in the **System Contact** field.
7. Enter a description of the system location, such as `3rd floor lab`, in the **System Location** field.
8. Enter the system's asset number in the **Asset Number** field.
9. In the **Get Community Name** field, type the community name that has permissions to retrieve SNMP information from the firewall, for example, `public`.
10. In the **Trap Community Name** field, type the community name that is used to send SNMP traps from the firewall to the SNMP manager, for example, `public`.
11. In the **Host 1/2/3/4** fields, type in the IP address(es) of the SNMP manager system(s) that receives the traps.
12. Enter the host name or IP address of a GMS Console in the **HostGMS** field.
13. Click **OK**.

Configuring IPS Sniffer Mode

To configure IPS Sniffer Mode:

11. Navigate to **NETWORK | System > Interfaces**.
12. Click on the **Edit** icon for the **X2** interface. The **Edit Interface** dialog displays.
13. Set the **Mode / IP Assignment** to **Layer 2 Bridged Mode**. The options change.
14. Set the **Bridged To:** interface to **X0**.
15. Do not enable the **Block all non-IP traffic** setting if you want to monitor non-IP traffic.
16. Select **Never route traffic on this bridge-pair** to ensure that the traffic from the mirrored switch port is not sent back out onto the network. (The **Never route traffic on this bridge-pair** setting is known as Captive-Bridge Mode.)
17. Select **Only sniff traffic on this bridge-pair** to enable sniffing or monitoring of packets that arrive on the L2 Bridge from the mirrored switch port.
18. Select **Disable stateful-inspection on this bridge-pair** to exempt these interfaces from stateful high availability inspection. If Deep Packet Inspection services are enabled for these interfaces, the DPI services continue to be applied.
19. The **Domain Name** field is used to bound an accurate domain name with all web services provided by this interface. The value can be one of the following:
    - An FQDN address (`*.company.com / www.company.com`)
    - An IPv4 or IPv6 address string (`a.a.a.a / b:b:b:b:b:b:b:b`)

      When configured, all web access, along with SSL VPN service, should be accessed by only the **Domain Name**. No other attempts are allowed.

      ⓘ | **NOTE:** Access through an exact IP address is implicitly trusted, whether this field is set or not.

      To enable this feature, make sure the **Enforce HTTP Host Header Check** option located on the Administrator page, is enabled as well.
20. Click **OK** to save and activate the change. The dialog closes, and the **NETWORK | System > Interfaces** page redisplays.
21. Click the **Edit** icon for the **X1 WAN** interface. The **Edit Interface** dialog displays.
22. Assign the X1 WAN interface a unique IP address for the internal LAN segment of your network — this might sound wrong, but this is actually the interface from which you manage the appliance, and it is also the interface from which the firewall sends its SNMP traps as well as the interface from which it gets security services signature updates.
23. Click **OK**.
24. For traffic to pass successfully, you must also modify the firewall rules to allow traffic from the
    - LAN to WAN
    - WAN to the LAN
25. Connect the:

- Span/mirror switch port to X0 on the firewall, not to X2 (in fact, X2 is not plugged in at all)
- X1 to the internal network

IMPORTANT: Use care when programming ports spanned/mirrored to X0.

NOTE: Informational videos with interface configuration examples are available online. For example, see *How to configure the SonicWall WAN / X1 Interface with PPPoE Connection*. This and other videos are available at: https://support.SonicWall.com/videos-product-select.

Configuring Security Services (Unified Threat Management)

The settings that you enable in this section control what type of malicious traffic you can detect in IPS Sniffer Mode. Typically, you want to enable at least Intrusion Prevention, but you might also want to enable other Security Services, such as Gateway Anti-Virus or Anti-Spyware.

To enable Security Services, your SonicWall firewall must be licensed for them and the signatures must be downloaded from the SonicWall Data Center. For complete instructions on enabling and configuring Intrusion Prevention, Gateway Anti-Virus, and Anti-Spyware, see the *SonicOS Security Services Administration Guide*.

Topics:

- Configuring Logging
- Connecting a Mirrored Switch Port to an IPS Sniffer Mode Interface
- Connecting and Configuring a WAN Interface to the Data Center

Configuring Logging

You can configure logging on the **DEVICE | Log > Settings** page to record entries for attacks that are detected by the firewall. For information on how to enable logging, see the *SonicOS Logs Administration Guide*.

Connecting a Mirrored Switch Port to an IPS Sniffer Mode Interface

Use a standard CAT-5 Ethernet cable to connect a mirrored switch port to either interface in the Bridge-Pair. Network traffic is sent automatically from the switch to the appliance where it can be inspected.

Consult the switch documentation for instructions on setting up the mirrored port.

Connecting and Configuring a WAN Interface to the Data Center

Connect the WAN port on the firewall, typically port X1, to your gateway or to a device with access to the gateway. The appliance communicates with the SonicWall Data Center automatically. For detailed instructions on configuring the WAN interface, see *Configuring a WAN Interface*.

Configuring Wire and Tap Mode

Topics:

- Configuring an Interface for Wire Mode
- Configuring Wire Mode for a WAN/LAN Zone Pair
- Configuring Wire Mode with Link Aggregation

SonicOS supports Wire Mode and Tap Mode, which provide methods of non-disruptive, incremental insertion into networks. Wire and Tap Mode Settings describe the wire and tap modes.

WIRE AND TAP MODE SETTINGS

Wire Mode Settings	Description
Bypass Mode	Bypass Mode allows for the quick and relatively non-interruptive introduction of appliance hardware into a network. Upon selecting a point of insertion into a network (for example, between a core switch and a perimeter appliance, in front of a VM server farm, at a transition point between data classification domains), the appliance is inserted into the physical data path, requiring a very short maintenance window. One or more pairs of switch ports on the appliance are used to forward all packets across segments at full line rates, with all the packets remaining on the appliance's 240Gbps switch fabric rather than getting passed up to the multi-core inspection and enforcement path. While Bypass Mode does not offer any inspection or firewalling, this mode allows you to physically introduce the appliance into the network with a minimum of downtime and risk, and to obtain a level of comfort with the newly inserted component of the networking and security infrastructure. You can then transition from Bypass Mode to Inspect or Secure Mode instantaneously through a simple user-interface driven reconfiguration.
Inspect Mode	Inspect Mode extends Bypass Mode without functionally altering the low-risk, zero-latency packet path. Packets continue to pass through the appliance'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 appliance's Application Intelligence and threat detection capabilities without any actual intermediate processing.

Wire Mode Settings	Description
Secure Mode	Secure Mode is the progression of Inspect Mode, actively interposing the appliance'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, Gateway Anti-Virus and Cloud Gateway Anti-Virus, Anti-Spyware, and Content Filtering. Secure Mode affords the same level of visibility and enforcement as conventional NAT or L2 Bridged Mode deployments, but without any L3/L4 transformations, and with no alterations of ARP or routing behavior. Secure Mode thus provides an incrementally attainable NGFW deployment requiring no logical and only minimal physical changes to existing network designs. Secure mode should be used when creating wire-mode pairs for VLAN translation.
Tap Mode	Tap Mode provides the same visibility as Inspect Mode, but differs from the latter in that it ingests a mirrored packet stream through a single switch port on the appliance, eliminating the need for physically intermediated insertion. Tap Mode is designed for use in environments employing network taps, smart taps, port mirrors, or SPAN ports to deliver packets to external devices for inspection or collection. Like all other forms of Wire Mode, Tap Mode can operate on multiple concurrent port instances, supporting discrete streams from multiple taps.

Wire modes: Functional differences summarizes the key functional differences between modes of interface configuration:

WIRE MODES: FUNCTIONAL DIFFERENCES

Interface Configuration	Bypass Mode	Inspect Mode	Secure Mode	Tap Mode	L2 Bridge, Transparent, NAT, Route Modes
Active/Active Clustering	No	No	No	No	Yes
Application Control	No	No	Yes	No	Yes
Application Visibility	No	Yes	Yes	Yes	Yes
ARP/Routing/NAT[a]	No	No	No	No	Yes
Comprehensive Anti-Spam Service[a]	No	No	No	No	Yes
Content Filtering	No	No	Yes	No	Yes
DHCP Server[a]	No	No	No	No	Yes[b]
DPI Detection	No	Yes	Yes	Yes	Yes
DPI Prevention	No	No	Yes	No	Yes
DPI-SSL[a]	No	No	Yes	No	Yes
High-Availability	Yes	Yes	Yes	Yes	Yes

Interface Configuration	Bypass Mode	Inspect Mode	Secure Mode	Tap Mode	L2 Bridge, Transparent, NAT, Route Modes
Link-State Propagation[c]	Yes	Yes	Yes	No	No
Stateful Packet Inspection	No	Yes	Yes	Yes	Yes
TCP Handshake Enforcement[d]	No	No	No	No	Yes
Virtual Groups[a]	No	No	No	No	Yes
VLAN Translation[e]	No	No	Yes	No	No

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.

[a] These functions or services are unavailable on interfaces configured in Wire Mode, but remain available on a system-wide level for any interfaces configured in other compatible modes of operation

[b] Not available in L2 Bridged Mode.

[c] **Link State Propagation** is a feature whereby interfaces in a Wire Mode pair mirror the link-state triggered by transitions of their partners. This is essential to proper operations in redundant path networks. Link State Propagation is not supported in Wire Mode over VLAN interfaces.

[d] Disabled by design in Wire Mode to allow for failover events occurring elsewhere on the network to be supported when multiple Wire Mode paths, or when multiple firewall units are in use along redundant or asymmetric paths.

[e] VLAN Translation is not supported in Wire Mode over VLAN interfaces.

Configuring an Interface for Wire Mode

To configure an interface for Wire Mode:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Configure** icon for the interface you want to configure for Wire Mode. The **Edit Interface** dialog displays.
3. From **Zone**, select any zone type except WLAN.

4. From **Mode / IP Assignment**, to configure the Interface for:
    - Tap mode, select **Tap Mode (1-Port Tap)**.
    - Wire Mode, select **Wire Mode (2-Port Wire)**.
5. From **Wire Mode Type**, select the appropriate mode:
    - **Bypass (via Internal Switch/Relay)**
    - **Inspect (Passive DPI of Mirrored Traffic)**
    - **Secure (Active DPI of Inline Traffic)**
6. From **Paired Interface**, 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).

    ⓘ **NOTE:** Only unassigned interfaces are available from **Paired Interface**. To make an interface unassigned, click its **Configure**, and from **Zone**, select **Unassigned**.
7. Wire Mode can be configured on any zone (except wireless zones). Wire Mode is a simplified form of Layer 2 Bridge Mode, and is configured as a pair of interfaces. In Wire Mode, the destination zone is the **Paired Interface Zone**. Access rules are applied to the Wire Mode pair based on the direction of traffic between the source **Zone** and its **Paired Interface Zone**. For example, if the source **Zone** is WAN and the **Paired Interface Zone** is **LAN**, then WAN to LAN and LAN to WAN rules are applied, depending on the direction of the traffic.
8. In Wire Mode, you can **Disable Stateful Inspection**. When **Disable Stateful Inspection** is selected, Stateful Packet Inspection (SPI) 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.
9. 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.
10. When **Inspect Mode** is selected, the **Restrict analysis at resource limit** option is displayed. It is disabled by default. When this option is enabled, the appliance scans the maximum number of packets it can process. The remaining packets are allowed to pass without inspection. When this option is disabled, traffic is throttled in the flow of traffic exceeds the firewalls inspection ability.

    ⓘ **NOTE:** Disabling the **Restrict analysis at resource limit** option reduces throughput if the rate of traffic exceeds the appliance's ability to scan all traffic.
11. Click **OK**.

Configuring Wire Mode for a WAN/LAN Zone Pair

The following configuration is an example of how Wire Mode can be configured. This example is for a WAN zone paired with a LAN zone. Wire Mode can also be configured for DMZ and custom zones.

To configure Wire Mode for a WAN/LAN Zone Pair:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click one of these:
   - **Add Interface**.
   - **Configure** icon for the interface you want to configure.

   The **Add/Edit Interface** dialog displays.
3. From **IP Assignment**, select **Wire Mode (2-Port Wire)**.
4. From **Zone**, select **WAN**.
5. From **Paired Interface Zone**, select **LAN**.
6. Select **Disable Stateful Inspection**.
7. Select **Enable Link State Propagation**.
8. When **Inspect Mode** is selected, the **Restrict analysis at resource limit** option is displayed. It is disabled by default. When this option is enabled, the appliance scans the maximum number of packets it can process. The remaining packets are allowed to pass without inspection. When this option is disabled, traffic is throttled in the flow of traffic exceeds the firewalls inspection ability.

   ⓘ | **NOTE:** Disabling the **Restrict analysis at resource limit** option reduces throughput if the rate of traffic exceeds the appliance's ability to scan all traffic.
9. Click **OK**. The Interface Settings table is updated.

Configuring Wire Mode with Link Aggregation

ⓘ | **NOTE:** Wire Mode over VLAN interfaces does not support Link Aggregation.

Link Aggregation (LAG) is used to bundle multiple links into a single interface to increase bandwidth. To inspect traffic over a LAG interface, a SonicWall firewall can be connected inline, allowing packets sent on one link to be bridged across to the destination transparently. Existing Wire Mode features such as link state propagation are supported. Up to 8 members per LAG are supported.

Wire Mode and Link Aggregation are configured from **NETWORK | System > Interfaces**. When **Link Aggregation** is selected on the **Edit Interface > Advanced** dialog, it also lists unassigned interfaces. You can select member interfaces for each side of the Wire Mode connection. The number of members on each side must be equal. It is recommended that the type and bandwidth size of the member interfaces also match.

To configure Wire Mode with LAG:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Configure** icon for the interface you want to configure. The **Edit Interface** dialog displays.
3. From **Zone**, select the zone you want. The options change.
4. From **Mode / IP Assignment**, select **Wire Mode (2-Port Wire)**. The options change again.
5. From **Wire Mode Type**, select **Secure (Active DPI of Inline Traffic)**.

6. From **Paired Interface**, select the interface to be paired.
7. From **Paired Interface Zone**, select the zone of the interface to be paired.
8. Select the **Disable Stateful Inspection** option. This option is selected by default.
9. Optionally, select **Enable Link State Propagation** if you want it. This option is not selected by default.
10. Click **Advanced**.

To continue on Advanced:

1. From **Redundant/Aggregate Ports**, select **Link Aggregation**. The options change.
2. From **Aggregate Port**, select the port for aggregation.
3. From **Paired Interface Aggregate Port**, select the paired port for aggregation.
4. From **Interface MTU**, indicate the largest packet size that the interface can forward without fragmenting the packet. The term MTU (Maximum Transmission Unit) refers to the size (in bytes) of the largest packet that a given layer of a communications protocol can pass onwards. MTU parameters usually appear in association with a communications interface (NIC, serial port, and so on). The default MTU size is 1500, however for some networking technologies reducing the MTU size and allowing fragmentation can help eliminate some connectivity problems occurring at the protocol level.
5. Click **OK**. The configuration is displayed in the **Interface Settings** table on **NETWORK | System > Interfaces**.

Layer 2 Bridged Mode

Topics:

SonicOS includes L2 (Layer 2) Bridged Mode, a method of unobtrusively integrating a firewall into any Ethernet network. L2 Bridged Mode is ostensibly similar to SonicOS's Transparent Mode in that it enables a firewall to share a common subnet across two interfaces, and to perform stateful and deep-packet inspection on all traversing IP traffic, but it is functionally more versatile.

In particular, L2 Bridged Mode employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent appliance integration. Using L2 Bridged Mode, a SonicWall firewall can be non-disruptively added to any Ethernet network to provide in-line

deep-packet inspection for all traversing IPv4 TCP and UDP traffic. In this scenario, the appliance is not used for security enforcement, but instead for bidirectional scanning, blocking viruses and spyware, and stopping intrusion attempts.

Unlike other transparent solutions, L2 Bridged Mode can pass all traffic types, including IEEE 802.1Q VLANs, Spanning Tree Protocol, multicast, broadcast, and IPv6, ensuring that all network communications continues uninterrupted.

Another aspect of the versatility of L2 Bridged Mode is that you can use it to configure IPS Sniffer Mode. Supported on SonicWall firewalls, IPS Sniffer Mode uses a single interface of a Bridge-Pair to monitor network traffic from a mirrored port on a switch. IPS Sniffer Mode provides intrusion detection, but cannot block malicious traffic because the appliance is not connected inline with the traffic flow. See IPS Sniffer Mode for more information.

L2 Bridged Mode provides an ideal solution for networks that already have existing appliances, and do not have immediate plans to replace their existing appliances, but wish to add the security of SonicWall deep-packet inspection and security services, such as Intrusion Prevention, Gateway Anti-Virus, and Anti-Spyware. If you do not have SonicWall security service subscriptions, you can sign up for free trials atMySonicWall.

You can also use L2 Bridged Mode in a High Availability deployment. This scenario is explained in the *Layer 2 Bridged Mode with High Availability*.

ⓘ | **NOTE:** Link Aggregation is not supported in Layer 2 Bridged Mode.

Key Features of SonicOS Layer 2 Bridged Mode

SonicOS Layer 2 Bridged Mode: Key features and benefits outlines the benefits of each key feature of layer 2 bridged mode.

SONICOS LAYER 2 BRIDGED MODE: KEY FEATURES AND BENEFITS

Feature	Benefit
L2 Bridging with Deep Packet Inspection	This method of transparent operation means that a SonicWall firewall can be added to any network without the need for readdressing or reconfiguration, enabling the addition of deep-packet inspection security services with no disruption to existing network designs. Developed with connectivity in mind as much as security, L2 Bridged Mode can pass all Ethernet frame types, ensuring seamless integration.
Secure Learning Bridge Architecture	True L2 behavior means that all allowed traffic flows natively through the L2 Bridge. Whereas other methods of transparent operation rely on ARP and route manipulation to achieve transparency, which frequently proves problematic, L2 Bridged Mode dynamically learns the topology of the network to determine optimal traffic paths.
Universal Ethernet Frame-Type Support	All Ethernet traffic can be passed across an L2 Bridge, meaning that all network communications continue uninterrupted. While many other methods of transparent operation only support IPv4 traffic, L2 Bridged Mode inspects all IPv4 traffic and passes (or blocks, if desired) all other traffic, including LLC, all Ethertypes, and even proprietary frame formats.

Feature	Benefit
Mixed-Mode Operation	L2 Bridged Mode can concurrently provide L2 Bridging and conventional appliance services, such as routing, NAT, VPN, and wireless operations. This means it can be used as an L2 Bridge for one segment of the network, while providing a complete set of security services to the remainder of the network. This also allows for the introduction of the SonicWall firewall as a pure L2 bridge, with a smooth migration path to full security services operation.
Wireless Layer 2 Bridging	Use a single IP subnet across multiple zone types, including LAN, WLAN, DMZ, or custom zones. This feature allows wireless and wired clients to seamlessly share the same network resources, including DHCP addresses. The Layer 2 protocol can run between paired interfaces, allowing multiple traffic types to traverse the bridge, including broadcast and non-IP packets.

Key Concepts to Configuring L2 Bridged Mode and Transparent Mode

The following terms are used when referring to the operation and configuration of L2 Bridged Mode:

L2 Bridged Mode – A method of configuring a SonicWall firewall, which enables it to be inserted inline into an existing network with absolute transparency, beyond even that provided by Transparent Mode. Layer 2 Bridged Mode also refers to the IP Assignment configuration that is selected for Secondary Bridge Interfaces that are placed into a Bridge-Pair.

Transparent Mode – A method of configuring a SonicWall firewall that allows it to be inserted into an existing network without the need for IP reconfiguration by spanning a single IP subnet across two or more interfaces through the use of automatically applied ARP and routing logic.

IP Assignment – When configuring a Trusted (LAN) or Public (DMZ) interface, the IP Assignment for the interface can either be:

Static – The IP address for the interface is manually entered.

Transparent Mode – The IP address(es) for the interface is assigned using an Address Object (Host, Range, or Group) that falls within the WAN Primary IP subnet, effectively spanning the subnet from the WAN interface to the assigned interface.

Layer 2 Bridged Mode – An interface placed in this mode becomes the Secondary Bridge Interface to the Primary Bridge Interface to which it is paired. The resulting Bridge-Pair then behaves like a two-port learning bridge with full L2 transparency, and all IP traffic that passes through is subjected to full stateful failover and deep packet inspection.

Bridge-Pair – The logical interface set composed of a Primary Bridge Interface and a Secondary Bridge Interface. The terms primary and secondary do not imply any inherent level of operational dominance or subordination; both interfaces continue to be treated according to their zone type, and to pass IP traffic according to their configured Access Rules. Non-IPv4 traffic across the Bridge-Pair is controlled by the Block all non-IPv4 traffic setting on the Secondary Bridge Interface. A system might support as many Bridge Pairs as it has interface pairs available. In other words, the maximum number of Bridge-Pairs is equal to ½ the number of physical interfaces on the platform. Membership in a Bridge-Pair does not preclude an interface from conventional

behavior; for example, if X1 is configured as a Primary Bridge Interface paired to X3 as a Secondary Bridge Interface, X1 can simultaneously operate in its traditional role as the Primary WAN, performing NAT for Internet-bound traffic through the Auto-added X1 Default NAT Policy.

Primary Bridge Interface – A designation that is assigned to an interface after a Secondary Bridge Interface has been paired to it. A Primary Bridge Interface can belong to an Untrusted (WAN), Trusted (LAN), or Public (DMZ) zone.

Secondary Bridge Interface – A designation that is assigned to an interface whose IP Assignment has been configured for Layer 2 Bridged Mode. A Secondary Bridge Interface can belong to a Trusted (LAN), or Public (DMZ) zone.

Bridge Management Address – The address of the Primary Bridge Interface is shared by both interfaces of the Bridge-Pair. If the Primary Bridge Interface also happens to be the Primary WAN interface, it is this address that is used for outbound communications by the appliance, such as NTP, and License Manager updates. Hosts that are connected to either segment of the Bridge-Pair might also use the Bridge Management Address as their gateway, as is common in Mixed-Mode deployments.

Bridge-Partner – The term used to refer to the other member of a Bridge-Pair.

Non-IPv4 Traffic – SonicOS supports the following IP protocol types: ICMP (1), IGMP (2), TCP (6), UDP (17), GRE (47), ESP (50), AH (51), EIGRP (88), OSPF (89), PIM-SM (103), L2TP (115). More esoteric IP types, such as Combat Radio Transport Protocol (126), are not natively handled by the appliance, nor are non-IPv4 traffic types such as IPX or (currently) IPv6. L2 Bridged Mode can be configured to either pass or drop Non-IPv4 traffic.

Captive-Bridged Mode – This optional mode of L2 Bridge operation prevents traffic that has entered an L2 bridge from being forwarded to a non-Bridge-Pair interface. By default, L2 Bridge logic forwards traffic that has entered the L2 Bridge to its destination along the most optimal path as determined by ARP and routing tables. In some cases, the most optimal path might involve routing or NATing to a non-Bridge-Pair interface. Activating Captive-Bridged Mode ensures that traffic that enters an L2 Bridge exits the L2 Bridge rather than taking its most logically optimal path. In general, this mode of operation is only required in complex networks with redundant paths, where strict path adherence is required.

Pure L2 Bridge Topology – Refers to deployments where the firewall is used strictly in L2 Bridged Mode for the purposes of providing in-line security to a network. This means that all traffic entering one side of the Bridge-Pair is bound for the other side, and is not routed/NATed through a different interface. This is common in cases where there is an existing perimeter appliance, or where in-line security is desired along some path (for example, inter-departmentally, or on a trunked link between two switches) of an existing network. Pure L2 Bridge Topology is not a functional limitation, but rather a topological description of a common deployment in heterogeneous environments.

Mixed-Mode Topology – Refers to deployments where the Bridge-Pair are not the only point of ingress/egress through the appliance. This means that traffic entering one side of the Bridge-Pair might be destined to be routed/NATed through a different interface. This is common when the appliance is simultaneously used to provide security to one or more Bridge-Pair while also providing:

- Perimeter security, such as WAN connectivity, to hosts on the Bridge-Pair or on other interfaces.
- Firewall and Security services to additional segments, such as Trusted (LAN) or Public (DMZ) interface, where communications occur between hosts on those segments and hosts on the Bridge-Pair.
- Wireless services with SonicPoints, where communications occur between wireless clients and hosts on the Bridge-Pair.

Comparing L2 Bridged Mode to Transparent Mode

While Transparent Mode allows an appliance running SonicOS to be introduced into an existing network without the need for re-addressing, it presents a certain level of disruption, particularly with regard to ARP, VLAN support, multiple subnets, and non-IPv4 traffic types. Consider a scenario where a Transparent Mode SonicWall firewall has just been added to the network with a goal of minimally disruptive integration, particularly:

- Negligible or no unscheduled downtime
- No need to re-address any portion of the network
- No need to reconfigure or otherwise modify the gateway router (as is common when the router is owned by the ISP)

Topics:

Comparison of L2 Bridged Mode to Transparent Mode

COMPARISON OF L2 BRIDGED MODE TO TRANSPARENT MODE

Attribute	Layer 2 Bridged Mode	Transparent Mode
Layer of Operation	Layer 2 (MAC)	Layer 3 (IP)
ARP behavior	ARP (Address Resolution Protocol) information is unaltered. MAC addresses natively traverse the L2 bridge. Packets that are destined for SonicWall firewall's MAC addresses are processed, others are passed, and the source and destinations are learned and cached.	ARP is proxied by the interfaces operating in Transparent Mode.

Attribute	Layer 2 Bridged Mode	Transparent Mode
Path determination	Hosts on either side of a Bridge-Pair are dynamically learned. There is no need to declare interface affinities.	The Primary WAN interface is always the master ingress/egress point for Transparent mode traffic, and for subnet space determination. Hosts transparently sharing this subnet space must be explicitly declared through the use of Address Object assignments.
Maximum interfaces	Two interfaces, a Primary Bridge Interface and a Secondary Bridge Interface.	Two or more interfaces. The master interface is always the Primary WAN. There can be as many transparent subordinate interfaces as there are interfaces available.
Maximum pairings	The maximum number of Bridge-Pairs allowed is limited only by available physical interfaces. This can be described as “many One-to-One pairings.”	Transparent Mode only allows the Primary WAN subnet to be spanned to other interfaces, although it allows for multiple interfaces to simultaneously operate as transparent partners to the Primary WAN. This can be described as “a single One-to-One” or “a single One-to-Many pairing.”
Zone restrictions	The Primary Bridge Interface can be Untrusted, Trusted, or Public. The Secondary Bridge Interface can be Trusted or Public.	Interfaces in a Transparent Mode pair must consist of one Untrusted interface (the Primary WAN, as the master of the pair’s subnet) and one or more Trusted/Public interface (such as, LAN or DMZ).
Subnets supported	Any number of subnets is supported. Access Rules can be written to control traffic to/from any of the subnets as needed.	In its default configuration, Transparent Mode only supports a single subnet (that which is assigned to, and spanned from the Primary WAN). It is possible to manually add support for additional subnets through the use of ARP entries and routes.
Non-IPv4 Traffic	All non-IPv4 traffic, by default, is bridged from one Bridge-Pair interface to the Bridge-Partner interface, unless disabled on the Secondary Bridge Interface configuration page. This includes IPv6 traffic, STP (Spanning Tree Protocol), and unrecognized IP types.	Non IPv4 traffic is not handled by Transparent Mode, and is dropped and logged.
VLAN traffic	VLAN traffic is passed through the L2 Bridge, and is fully inspected by the Stateful and Deep Packet Inspection engines.	VLAN subinterfaces can be created and can be given Transparent Mode Address Object assignments, but the VLANs are terminated by the firewall rather than passed.

Attribute	Layer 2 Bridged Mode	Transparent Mode
VLAN subinterfaces	VLAN subinterfaces can be configured on Bridge-Pair interfaces, but they are passed through the bridge to the Bridge-Partner unless the destination IP address in the VLAN frame matches the IP address of the VLAN subinterface on the appliance, in which case it is processed (for example, as management traffic).	VLAN subinterfaces can be assigned to physical interfaces operating in Transparent Mode, but their mode of operation is independent of their parent. These VLAN subinterfaces can also be given Transparent Mode Address Object assignments, but in any event VLAN subinterfaces are terminated rather than passed.
Dynamic addressing	Although a Primary Bridge Interface might be assigned to the WAN zone, only static addressing is allowable for Primary Bridge Interfaces.	Although Transparent Mode employs the Primary WAN as a master interface, only static addressing is allowable for Transparent Mode.
VPN support	VPN operation is supported with one additional route configured. See *VPN Integration with Layer 2 Bridged Mode* for details.	VPN operation is supported with no special configuration requirements.
DHCP support	DHCP can be passed through a Bridge-Pair.	Interfaces operating in Transparent Mode can provide DHCP services, or they can pass DHCP using IP Helper.
Routing and NAT	Traffic is intelligently routed in/out of the L2 Bridge-Pair from/to other paths. By default, traffic is NATed from one Bridge-Pair interface to the Bridge-Partner, but it can be NATed to other paths, as needed. Custom routes and NAT policies can be added as needed.	Traffic is intelligently routed from/to other paths. By default, traffic is not NATed from/to the WAN to/from Transparent Mode interface, but it can be NATed to other paths, as needed. Custom routes and NAT policies can be added as needed.
Stateful Packet Inspection	Full stateful packet inspection is applied to all IPv4 traffic traversing the L2 Bridge for all subnets, including VLAN traffic on firewalls.	Full stateful packet inspection is applied to traffic from/to the subnets defined by Transparent Mode Address Object assignment.
Security services	All security services (GAV, IPS, Anti-Spyware, CFS) are fully supported. All regular IP traffic, as well as all 802.1Q encapsulated VLAN traffic.	All security services (GAV, IPS, Anti-Spyware, CFS) are fully supported from/to the subnets defined by Transparent Mode Address Object assignment.
Broadcast traffic	Broadcast traffic is passed from the receiving Bridge-Pair interface to the Bridge-Partner interface.	Broadcast traffic is dropped and logged, with the possible exception of NetBIOS, which can be handled by IP Helper.

Attribute	Layer 2 Bridged Mode	Transparent Mode
Multicast traffic	Multicast traffic is inspected and passed across L2 Bridge-Pairs providing Multicast has been activated on **NETWORK | System > Multicast**. It is not dependent upon IGMP messaging, nor is it necessary to enable multicast support on the individual interfaces.	Multicast traffic, with IGMP dependency, is inspected and passed by Transparent Mode providing Multicast has been activated on **NETWORK | System > Multicast**, and multicast support has been enabled on the relevant interfaces.

Benefits of Transparent Mode over L2 Bridged Mode

Two interfaces are the maximum allowed in an L2 Bridge Pair. If more than two interfaces are required to operate on the same subnet, Transparent Mode should be considered.

ARP in Transparent Mode

ARP (Address Resolution Protocol: the mechanism by which unique hardware addresses on network interface cards are associated to IP addresses) is proxied in Transparent Mode. If the Workstation on Server on the left had previously resolved the Router (`192.168.0.1`) to its MAC address `00:99:10:10:10:10`, this cached ARP entry would have to be cleared before these hosts could communicate through the appliance. This is because the appliance proxies (or answers on behalf of) the gateway's IP (`192.168.0.1`) for hosts connected to interfaces operating in Transparent Mode. So when the Workstation at the left attempts to resolve `192.168.0.1`, the ARP request it sends is responded to by the appliance with its own X0 MAC address (`00:06:B1:10:10:10`).

The appliance also proxy ARPs the IP addresses specified in the Transparent Range (`192.168.0.100` to `192.168.0.250`) assigned to an interface in Transparent Mode for ARP requests received on the X1 (Primary WAN) interface. If the router had previously resolved the server (`192.168.0.100`) to its MAC address `00:AA:BB:CC:DD:EE`, this cached ARP entry would have to be cleared before the router could communicate with the host through the appliance. This typically requires a flushing of the router's ARP cache either from its management interface or through a reboot. When the router's ARP cache is cleared, the router can then send a new ARP request for `192.168.0.100`, to which the appliance responds with its X1 MAC `00:06:B1:10:10:11`.

VLAN Support in Transparent Mode

While the network depicted in the previous diagram is simple, it is not uncommon for larger networks to use VLANs for segmentation of traffic. If this was such a network, where the link between the switch and the router was a VLAN trunk, a Transparent Mode SonicWall firewall would have been able to terminate the VLANs to subinterfaces on either side of the link, but it would have required unique addressing; that is, non-Transparent Mode operation requiring re-addressing on at least one side. This is because only the Primary WAN interface can be used as the source for Transparent Mode address space.

Multiple Subnets in Transparent Mode

It is also common for larger networks to employ multiple subnets, be they on a single wire, on separate VLANs, multiple wires, or some combination. Transparent Mode is capable of supporting multiple subnets through the

use of Static ARP and Route entries.

Non-IPv4 Traffic in Transparent Mode

Transparent Mode drops (and generally logs) all non-IPv4 traffic, precluding it from passing other traffic types, such as IPX, or unhandled IP types.

ARP in L2 Bridged Mode

L2 Bridged Mode employs a learning bridge design where it dynamically determines which hosts are on which interface of an L2 Bridge (referred to as a Bridge-Pair). ARP is passed through natively, meaning that a host communicating across an L2 Bridge sees the actual host MAC addresses of their peers. For example, the Workstation communicating with the Router (`192.168.0.1`) sees the router as `00:99:10:10:10:10`, and the Router sees the Workstation (`192.168.0.100`) as `00:AA:BB:CC:DD:EE`.

This behavior allows for a SonicWall firewall operating in L2 Bridged Mode to be introduced into an existing network with no disruption to most network communications other than that caused by the momentary discontinuity of the physical insertion.

Stream-based TCP protocols communications (for example, an FTP session between a client and a server) needs to be re-established upon the insertion of an L2 Bridged Mode appliance. This is by design so as to maintain the security afforded by stateful packet inspection. As the stateful packet inspection engine cannot have knowledge of the TCP connections that preexisted it, it drops these established packets with a log event such as a TCP packet received on a nonexistent/closed connection; TCP packet dropped.

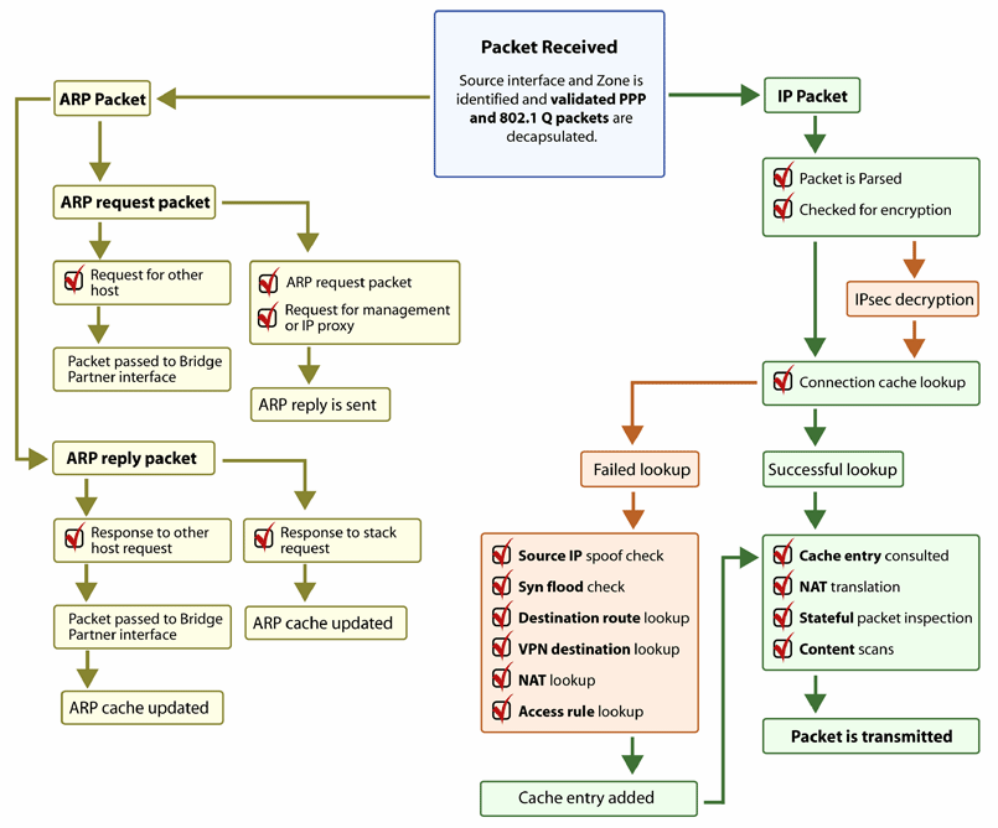
VLAN Support in L2 Bridged Mode

On SonicWall firewalls, L2 Bridged Mode provides fine control over 802.1Q VLAN traffic traversing an L2 Bridge. The default handling of VLANs is to allow and preserve all 802.1Q VLAN tags as they pass through an L2 Bridge, while still applying all firewall rules, and stateful and deep-packet inspection to the encapsulated traffic. It is further possible to specify white/black lists for allowed/disallowed VLAN IDs through the L2 Bridge.

This allows an appliance operating in L2 Bridged Mode to be inserted, for example, inline into a VLAN trunk carrying any number of VLANs, and to provide full security services to all IPv4 traffic traversing the VLAN without the need for explicit configuration of any of the VLAN IDs or subnets. Access Rules can also, optionally, be applied to all VLAN traffic passing through the L2 Bridged Mode because of the method of handling VLAN traffic.

L2 Bridge IP Packet Path

L2 BRIDGE IP PACKET FLOW

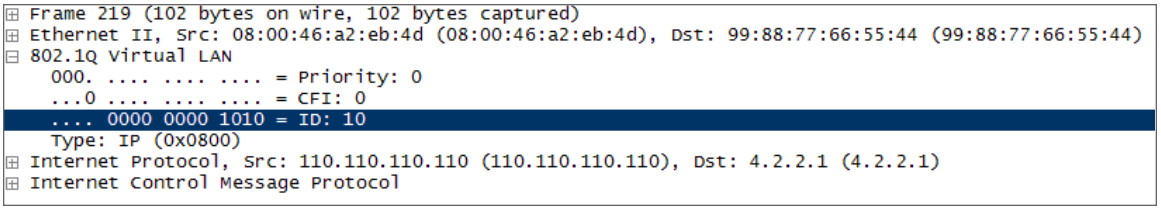


The following sequence of events describes the flow in L2 Bridge IP Packet Flow:

1. 802.1Q encapsulated frame enters an L2 Bridge interface (this first step, Step 2, and Step 12 apply only to 802.1Q VLAN traffic).
2. The 802.1Q VLAN ID is checked against the VLAN ID white/black list. If the VLAN ID is:
    - Disallowed, the packet is dropped and logged.
    - Allowed, the packet is decapsulated, the VLAN ID is stored, and the inner packet (including the IP header) is passed through the full packet handler.
3. As any number of subnets is supported by L2 Bridging, no source IP spoof checking is performed on the source IP of the packet. It is possible to configure L2 Bridges to only support a certain subnet or subnets using Access Rules.
4. SYN Flood checking is performed.
5. A destination route lookup is performed to the destination zone, so that the appropriate Access rule can be applied. Any zone is a valid destination, including the same zone as the source zone (for example, LAN to

LAN), the Untrusted zone (WAN), the Encrypted (VPN), Wireless (WLAN), Multicast, or custom zones of any type.

6. A NAT lookup is performed and applied, as needed:
    - In general, the destination for packets entering an L2 Bridge is the Bridge-Partner interface (that is, the other side of the bridge). In these cases, no translation is performed.
    - In cases where the L2 Bridge Management Address is the gateway, as is sometimes the case in Mixed-Mode topologies, then NAT is applied as needed (for more details, see *L2 Bridge Path Determination*).
7. Access Rules are applied to the packet. For example, on SonicWall firewalls, the following packet decode shows an ICMP packet bearing VLAN ID 10, source IP address `110.110.110.110` destined for IP address `4.2.2.1`.



   It is possible to construct an Access Rule to control any IP packet, independent of its VLAN membership, by any of its IP elements, such as source IP, destination IP, or service type. If the packet is disallowed, it is dropped and logged. If the packet is allowed, it continues.

8. A connection cache entry is made for the packet, and required NAT translations (if any) are performed.
9. Stateful packet inspection and transformations are performed for TCP, VoIP, FTP, MSN, Oracle, RTSP and other media streams, PPTP and L2TP. If the packet is disallowed, it is dropped and logged. If the packet is allowed, it continues.
10. Deep packet inspection, including Gateway Anti-Virus, Intrusion Prevention, Anti-Spyware, CFS and email-filtering is performed. If the packet is disallowed, it is dropped and logged. If the packet is allowed, it continues. Client notification is performed as configured.
11. If the packet is destined for the Encrypted zone (VPN), the Untrusted zone (WAN), or some other connected interface (the last two of which might be the case in Mixed-Mode Topologies) the packet is sent through the appropriate path.
12. If the packet is not destined for the VPN/WAN/Connected interface, the stored VLAN tag is restored, and the packet (again bearing the original VLAN tag) is sent out the *Bridge-Partner* interface.

Multiple Subnets in L2 Bridged Mode

L2 Bridged Mode is capable of handling any number of subnets across the bridge, as described in L2 Bridge IP Packet Path. The default behavior is to allow all subnets, but Access Rules can be applied to control traffic as needed.

Non-IPv4 Traffic in L2 Bridged Mode

Unsupported traffic is, by default, passed from one L2 Bridge interface to the Bridge-Partner interface. This allows the appliance to pass other traffic types, including LLC packets such as Spanning Tree, other EtherTypes, such as MPLS label switched packets (EtherType 0x8847), Appletalk (EtherType 0x809b), and the ever-popular Banyan Vines (EtherType 0xbad). These non-IPv4 packets are only passed across the Bridge, they are not inspected or controlled by the packet handler. If these traffic types are not needed or desired, the bridging behavior can be changed by enabling the **Block all non-IPv4 traffic** option on the **Secondary Bridge Interface** configuration dialog.

L2 Bridge Path Determination

Packets received by the appliance on Bridge-Pair interfaces must be forwarded along to the appropriate and optimal path toward their destination, whether that path is the Bridge-Partner, some other physical or subinterface, or a VPN tunnel. Similarly, packets arriving from other paths (physical, virtual or VPN) bound for a host on a Bridge-Pair must be sent out over the correct Bridge-Pair interface.

The following summary describes, in order, the logic applied to path determinations for these cases:

1. If present, the most specific non-default route to the destination is chosen. This would cover, for example:
    a. A packet arriving on X3 (non-L2 Bridge LAN) destined for host `15.1.1.100` subnet, where a route to the `15.1.1.0/24` subnet exists through `192.168.0.254` through the X0 (Secondary Bridge Interface, LAN) interface. The packet would be forwarded through X0 to the destination MAC address of `192.168.0.254`, with the destination IP address `15.1.1.100`.
    b. A packet arriving on X4 (Primary Bridge Interface, LAN) destined for host `10.0.1.100`, where a route to the `10.0.1.0/24` exists through `192.168.10.50` through the X5 (DMZ) interface. The packet would be forwarded through X5 to the destination MAC address of `192.168.10.50`, with the destination IP address `10.0.1.100`.
2. If no specific route to the destination exists, an ARP cache lookup is performed for the destination IP address. A match indicates the appropriate destination interface. This would cover, for example:
    a. A packet arriving on X3 (non-L2 Bridge LAN) destined for host `192.168.0.100` (residing on L2 Primary Bridge Interface X2). The packet would be forwarded through X2 to the known destination MAC and IP address of `192.168.0.100`, as derived from the ARP cache.
    b. A packet arriving on X4 (Primary Bridge Interface, LAN) destined for host `10.0.1.10` (residing on X5 – DMZ). The packet would be forwarded through X5 to the known destination MAC and IP address of `10.0.1.10`, as derived from the ARP cache.

3. If no ARP entry is found:
    a. If the packet arrives on a Bridge-Pair interface, it is sent to the Bridge-Partner interface.
    b. If the packet arrives from some other path, the appliance sends an ARP request out both interfaces of the Bridge-Pair to determine on which segment the destination IP resides.

    In this last case, as the destination is unknown until after an ARP response is received, the destination zone also remains unknown until that time. This precludes the appliance from being able to apply the appropriate Access Rule until after path determination is completed. Upon completion, the correct Access Rule is applied to subsequent related traffic.

With regard to address translation (NAT) of traffic arriving on an L2 Bridge-Pair interface, if it is determined to be bound for:

1. The Bridge-Partner interface, no IP translation (NAT) is performed.
2. A different path, appropriate NAT policies applies; if the path is:
    a. Another connected (local) interface, there is likely no translation. That is, it is effectively routed as a result of hitting the last-resort **Any > Original NAT Policy**.
    b. Determined to be through the WAN, then the default *Auto-added [interface] outbound NAT Policy for X1 WAN* applies, and the packet's source is translated for delivery to the Internet. This is common in the case of Mixed-Mode topologies as described in *Internal Security*.

L2 Bridge Interface Zone Selection

Bridge-Pair interface zone assignment should be done according to your network's traffic flow requirements. Unlike Transparent Mode, which imposes a system of "more trusted to less trusted" by requiring that the source interface be the Primary WAN, and the transparent interface be Trusted or Public, L2 Bridged Mode allows for greater control of operational levels of trust. Specifically, L2 Bridged Mode allows for the Primary and Secondary Bridge Interfaces to be assigned to the same or different zones (for example, LAN+LAN, LAN+DMZ, WAN+CustomLAN) This affects not only the default Access Rules that are applied to the traffic, but also the manner in which Deep Packet Inspection security services are applied to the traffic traversing the bridge. Important areas to consider when choosing and configuring interfaces to use in a Bridge-Pair are Security Services, Access Rules, and WAN connectivity:

Security Services Directionality

As it is one of the primary employments of L2 Bridged Mode, understanding the application of security services is important to the proper zone selection for Bridge-Pair interfaces. Security services applicability is based on the following criteria:

1. **The direction of the service**:
    - GAV is primarily an Inbound service, inspecting inbound HTTP, FTP, IMAP, SMTP, POP3, and TCP Streams. It also has an additional Outbound element for SMTP.
    - Anti-Spyware is primarily Inbound, inspecting inbound HTTP, FTP, IMAP, SMTP, POP3 for the delivery (that is, retrieval) of Spyware components as generally recognized by their class IDs. It also has an additional Outbound component, where Outbound is used relative to the directionality

(namely, Outgoing) ascribed to it by the IPS signatures that trigger the recognition of these Spyware components. The Outgoing classifier (described in IPS: Direction of Traffic) is used because these components are generally retrieved by the client (for example, LAN host) through HTTP from a Web-server on the Internet (WAN host). Referring to IPS: Direction of Traffic, that would be an Outgoing connection, and requires a signature with an Outgoing directional classification.

- IPS has three directions: Incoming, Outgoing, and Bidirectional. Incoming and Outgoing are described in IPS: Direction of Traffic, and Bidirectional refers to all points of intersection on the table.
- For additional accuracy, other elements are also considered, such as the state of the connection (for example, SYN or Established), and the source of the packet relative to the flow (for example, initiator or responder).

2. **The direction of the traffic**. The direction of the traffic as it pertains to IPS is primarily determined by the Source and Destination zone of the traffic flow. When a packet is received by the appliance, its source zone is generally immediately known, and its destination zone is quickly determined by doing a route (or VPN) lookup.

   Based on the source and destination, the packet's directionality is categorized as either Incoming or Outgoing, (not to be confused with Inbound and Outbound) where the criteria shown in IPS: Direction of Traffic is used to make the determination.

   IPS: DIRECTION OF TRAFFIC

Dest/Src	Untrusted	Public	Wireless	Encrypted	Trusted	Multicast
Untrusted	Incoming	Incoming	Incoming	Incoming	Incoming	Incoming
Public	Outgoing	Outgoing	Outgoing	Incoming	Incoming	Incoming
Wireless	Outgoing	Outgoing	Trust	Trust	Trust	Incoming
Encrypted	Outgoing	Outgoing	Trust	Trust	Trust	Outgoing
Trusted	Outgoing	Outgoing	Trust	Trust	Trust	Outgoing
Table data is subject to change.						

   In addition to this categorization, packets traveling to/from zones with levels of additional trust, which are inherently afforded heightened levels of security (LAN|Wireless|Encrypted <--> LAN|Wireless|Encrypted) are given the special Trust classification. Traffic with the Trust classification has all signatures applied (Incoming, Outgoing, and Bidirectional).

3. **The direction of the signature**. This pertains primarily to IPS, where each signature is assigned a direction by SonicWall's signature development team. This is done as an optimization to minimize false positives. Signature directions are:

   - **Incoming** – Applies to Incoming and Trust. The majority of signatures are Incoming, and they include all forms of application exploits and all enumeration and footprinting attempts. Approximately 85 percent of signatures are Incoming.

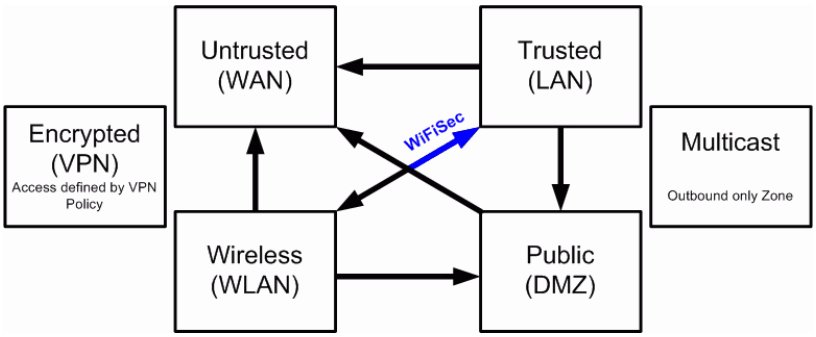
- **Outgoing** – Applies to Outgoing and Trust. Examples of Outgoing signatures would include IM and P2P login attempts, and responses to successfully launched exploits (for example, Attack Responses). Approximately 10 percent of signatures are Outgoing.
- **Bidirectional** – Applies to all. Examples of Bidirectional signatures would include IM file transfers, various NetBIOS attacks (for example, Sasser communications) and a variety of DoS attacks (for example, UDP/TCP traffic destined to port 0). Approximately five percent of signatures are Bidirectional.

4. **Zone application**. For a signature to be triggered, the desired security service *must be active on at least one of the zones it traverses*. For example, a host on the Internet (X1, WAN) accessing a Microsoft Terminal Server (on X3, Secondary Bridge Interface, LAN) triggers the Incoming signature “IPS Detection Alert: MISC MS Terminal server request, SID: 436, Priority: Low” if IPS is active on the WAN, the LAN, or both.

Access Rule Defaults

Default, zone-to-zone Access Rules. The default Access Rules should be considered, although they can be modified as needed. The defaults are shown in Access Rule Defaults:

ACCESS RULE DEFAULTS



WAN Connectivity

Internet (WAN) connectivity is required for stack communications, such as licensing, security services signature downloads, NTP (time synchronization), and CFS (Content Filtering Services). At present, these communications can only occur through the Primary WAN interface. If you require these types of communication, the Primary WAN should have a path to the Internet. Whether or not the Primary WAN is employed as part of a Bridge-Pair does not affect its ability to provide these stack communications.

ⓘ **NOTE:** If Internet connectivity is not available, licensing can be performed manually and signature updates can also be performed manually (https://www.MySonicWall.com/).

Sample Topologies

The following are sample topologies depicting common deployments:

- **Inline Layer 2 Bridged Mode** represents the addition of a SonicWall firewall to provide security services in a network where an existing appliance is in place.
- **Perimeter Security** represents the addition of a SonicWall firewall in pure L2 Bridged Mode to an existing network, where the appliance is placed near the perimeter of the network.
- **Internal Security** represents the full integration of a SonicWall firewall in mixed-mode, where it provides simultaneous L2 bridging, WLAN services, and NATed WAN access.
- **Layer 2 Bridged Mode with High Availability** represents the mixed-mode scenario where the appliance HA pair provide high availability along with L2 bridging.
- **Layer 2 Bridged Mode with SSL VPN** represents the scenario where a SonicWall SMA SSL VPN or SonicWall SSL VPN Series appliance is deployed in conjunction with L2 Bridged Mode.

Topics:

Wireless Layer 2 Bridge

In wireless mode, after bridging the wireless (WLAN) interface to a LAN or DMZ zone, the WLAN zone becomes the secondary bridged interface, allowing wireless clients to share the same subnet and DHCP pool as their wired counterparts.

To configure a WLAN to LAN Layer 2 interface bridge:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Configure** icon for the wireless interface you wish to bridge. The **Edit Interface** dialog displays.

   ⓘ **TIP:** If you have a virtual access point configured, then you already have a VLAN interface under an interface, such as X4, in the WLAN zone, and your virtual access point is configured to use that VLAN ID.
3. From **Layer 2 Bridged Mode**, select **Mode / IP Assignment**.

   ⓘ **NOTE:** Although a general rule is automatically created to allow traffic between the WLAN zone and your chosen bridged interface, WLAN zone type security properties still apply. Any specific rules must be manually added.
4. Select the Interface to which the WLAN should be bridged from **Bridged To**. In this instance, the X0 (default LAN zone) is chosen.
5. Configure the remaining options normally. For more information on configuring WLAN interfaces, see Configuring Wireless Interfaces.

Inline Layer 2 Bridged Mode

This method is useful in networks where there is an existing appliance that remains in place, but you wish to utilize the appliance's security services without making major changes to the network. By placing the appliance in Layer 2 Bridged Mode, the X0 and X1 interfaces become part of the same broadcast domain/network (that of the X1 WAN interface).

This example refers to an appliance installed in a Hewlett Packard ProCurve switching environment. SonicWall is a member of HP's ProCurve Alliance – more details can be found at the following location: https://www.hpe.com/us/en/networking.html.

HP's ProCurve Manager Plus (PCM+) and HP Network Immunity Manager (NIM) server software packages can be used to manage the switches as well as some aspects of the appliance.

To configure inline Layer 2 bridged mode:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Configure** icon for the **X0 LAN** interface.
3. On the **Edit Interface** dialog, set the **Mode / IP Assignment** to **Layer 2 Bridged Mode (IP Route Option)**. The options change.
4. Set the **Bridged To:** interface to **X1**.
5. To block all non-IP traffic on the bridged pair, select **Block all non-IP traffic**. This option is not selected by default.
6. To prevent traffic from being routed on the bridged pair, select **Never route traffic on this bridge-pair**. This option is not selected by default.
7. To prevent stateful inspection on the bridged pair, select **Disable stateful-inspection on this bridge-pair**. This option is not selected by default.
8. Ensure the interface is configured for **HTTPS** and **SNMP** so it can be managed from the DMZ by **PCM+/NIM**.
9. Configure the remaining options normally.
10. Click **OK** to save and activate the change.

You also need to make sure to modify the Access Rules to allow traffic from the LAN to WAN, and from the WAN to the LAN, otherwise traffic cannot pass successfully. You might also need to modify routing information on your firewall if your PCM+/NIM server is placed on the DMZ.

Perimeter Security

Perimeter Security is a network scenario where the appliance is added to the perimeter to provide security services (the network might or might not have an existing appliance between the appliance and the router). In this scenario, everything below the appliance (the Primary Bridge Interface segment) is generally considered as having a lower level of trust than everything to the left of the appliance (the Secondary Bridge Interface segment). For that reason, it would be appropriate to use X1 (Primary WAN) as the Primary Bridge Interface.

Traffic from hosts connected to the Secondary Bridge Interface (LAN) would be permitted outbound through the firewall to their gateways (VLAN interfaces on the L3 switch and then through the router), while traffic from the Primary Bridge Interface (WAN) would, by default, not be permitted inbound.

If there are public servers, for example, a mail and Web server, on the Secondary Bridge Interface (LAN) segment, an Access Rule allowing WAN > LAN traffic for the appropriate IP addresses and services could be added to allow inbound traffic to those servers.

Internal Security

A network scenario where the appliance acts as the perimeter security device and secure wireless platform. Simultaneously, it provides L2 Bridge security between the workstation and server segments of the network *without having to readdress any of the workstation or servers*.

This typical inter-departmental Mixed Mode topology deployment demonstrates how the appliance can simultaneously Bridge and route/NAT. Traffic to/from the *Primary Bridge Interface* (Server) segment from/to the *Secondary Bridge Interface* (Workstation) segment pass through the L2 Bridge.

As both interfaces of the Bridge-Pair are assigned to a Trusted (LAN) zone, the following apply:

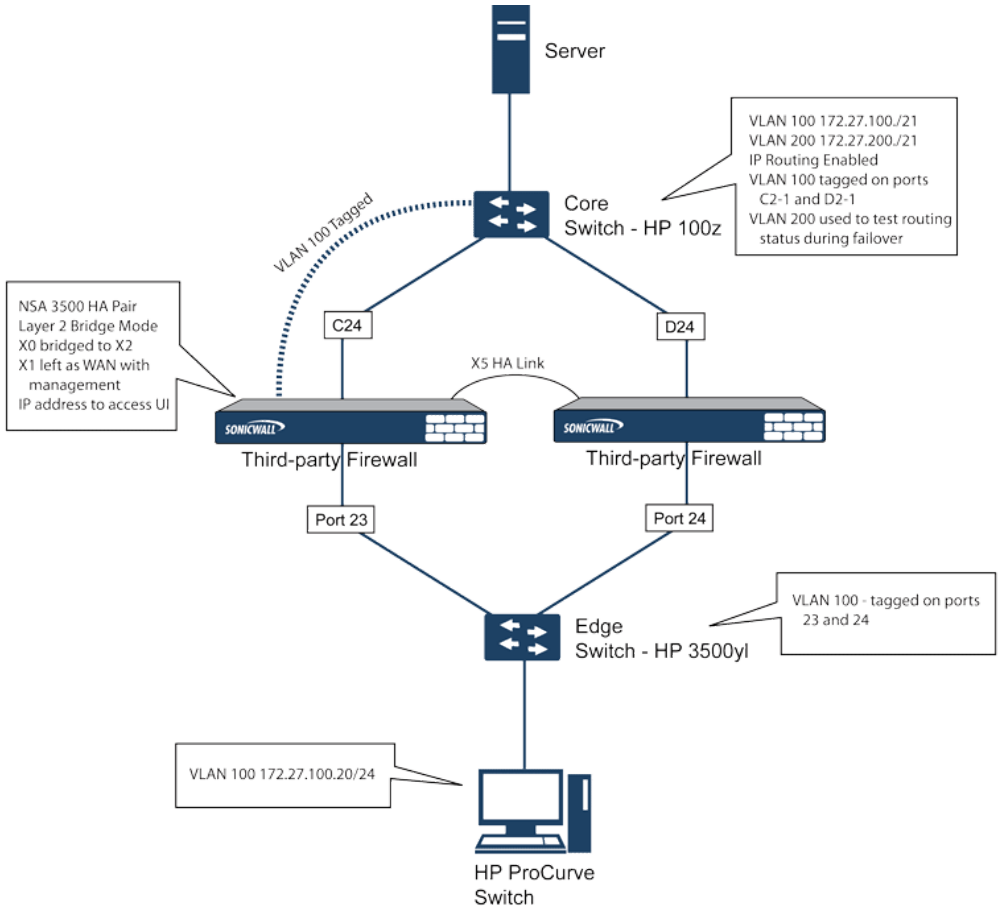
- All traffic is allowed by default, but Access Rules could be constructed as needed.
- Consider, for the point of contrast, what would occur if the X2 (Primary Bridge Interface) was instead assigned to a Public (DMZ) zone: All the Workstations would be able to reach the Servers, but the Servers would not be able to initiate communications to the Workstations. While this would probably support the traffic flow requirements (that is, Workstations initiating sessions to Servers), it would have two undesirable effects.
- The DHCP server would be in the DMZ. DHCP requests from the Workstations would pass through the L2 Bridge to the DHCP server (`192.168.0.100`), but the DHCP offers from the server would be dropped by the default DMZ > LAN Deny Access Rule. An Access Rule would have to be added, or the default modified, to allow this traffic from the DMZ to the LAN.
- Security services directionality would be classified as Outgoing for traffic from the Workstations to the Server because the traffic would have a Trusted source zone and a Public destination zone. This might be suboptimal because it would provide less scrutiny than the Incoming or (ideally) Trust classifications.
- Security services directionality would be classified as Trust, and all signatures (*Incoming*, *Outgoing*, and *Bidirectional*) are applied, providing the highest level of security to/from both segments.

For detailed instructions on configuring interfaces in Layer 2 Bridged Mode, see *Configuring Layer 2 Bridged Mode*.

Layer 2 Bridged Mode with High Availability

This method is appropriate in networks where both High Availability (HA) and Layer 2 Bridged Mode are desired. This example is for appliances, and assumes the use of switches with VLANs configured. See Internal Security Example: Both High Availability and Layer 2 Bridged Mode are Desired.

INTERNAL SECURITY EXAMPLE: BOTH HIGH AVAILABILITY AND LAYER 2 BRIDGED MODE ARE DESIRED



The appliance HA pair consists of two appliances, connected together on port X5, the designated HA port. Port X1 on each appliance is configured for normal WAN connectivity and is used for access to the management interface of that device. Layer 2 Bridged Mode is implemented with port X0 bridged to port X2.

When setting up this scenario, there are several things to take note of on both the appliances and the switches.

On the appliances:

- Do not enable the Virtual MAC option when configuring High Availability. In a Layer 2 Bridged Mode configuration, this function is not useful.
- Enabling Preempt Mode is not recommended in an inline environment such as this. If Preempt Mode is required, follow the recommendations in the documentation for your switches, as the trigger and failover time values play a key role here.
- Consider reserving an interface for the management network (this example uses X1). If it is necessary to assign IP addresses to the bridge interfaces for probe purposes or other reasons, SonicWall recommends using the management VLAN network assigned to the switches for security and administrative purposes.

ⓘ | **NOTE:** The IP addresses assigned for HA purposes do not directly interact with the actual traffic flow.

On the switches:

- Using multiple tag ports: As shown in Internal Security Example: Both High Availability and Layer 2 Bridged Mode are Desired, two tag (802.1q) ports were created for VLAN 100 on both the Edge switch (ports 23 and 24) and Core switch (C24 - D24). The appliances are connected inline between these two switches. In a high-performance environment, it is usually recommended to have Link Aggregation/ Port Trunking, Dynamic LACP, or even a completely separate link designated for such a deployment (using OSPF), and the fault tolerance of each of the switches must be considered. Consult your switch documentation for more information.
- On HP ProCurve switches, when two ports are tagged in the same VLAN, the port group is automatically placed into a failover configuration. In this case, as soon as one port fails, the other one becomes active.

Layer 2 Bridged Mode with SSL VPN

This sample topology covers the proper installation of a appliance into your existing SonicWall EX-Series SSL VPN or SonicWall SSL VPN networking environment. By placing the appliance into Layer 2 Bridged Mode, with an internal, private connection to the SSL VPN appliance, you can scan for viruses, spyware, and intrusions in both directions. In this scenario the appliance is not used for security enforcement, but instead for bidirectional scanning, blocking viruses and spyware, and stopping intrusion attempts. When programmed correctly, the appliance does not interrupt network traffic, unless the behavior or content of the traffic is determined to be undesirable. Both one- and two-port deployments of the appliance are covered in this section.

WAN to LAN Access Rules

Because the appliance is used in this deployment scenario only as an enforcement point for Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention, its existing security policy must be modified to allow traffic to pass in both directions between the WAN and LAN.

Configuring Network Interfaces and Activating L2B Mode

In this scenario, the WAN interface is used for:

- Access to the management interface for the administrator
- Subscription service updates on MySonicWall
- The default route for the device and subsequently the “next hop” for the internal traffic of the SSL VPN appliance (this is why the WAN interface must be on the same IP segment as the internal interface of the SSL VPN appliance)

The LAN interface on the appliance is used to monitor the unencrypted client traffic coming from the external interface of the SSL VPN appliance. This is the reason for running in Layer 2 Bridged Mode (instead of reconfiguring the external interface of the SSL VPN appliance to see the LAN interface as the default route).

To activate L2B mode on an interface:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Configure** icon for the WAN interface. The **Edit Interface** dialog displays.

3. Assign the interface an address that can access the Internet so that the appliance can obtain signature updates and communicate with NTP. The gateway and internal/external DNS address settings must match those of your SSL VPN appliance:
    - **IP address**: This must match the address for the internal interface on the SSL VPN appliance.
    - **Subnet Mask**, **Default Gateway**, and **DNS Server(s)**: Make these addresses match your SSL VPN appliance settings.
4. For the **Management** setting, choose **HTTPS** and **Ping**.
5. Click **OK** to save and activate the changes.

To configure the LAN interface settings:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Configure** icon for the **LAN** interface.
3. For the **Mode / IP Assignment** setting, select **Layer 2 Bridged Mode**.
4. For the **Bridged to** setting, select **X1**.
5. If you also need to pass VLAN tagged traffic, supported on the appliance, click **VLAN Filtering**.
6. Add all of the VLANs that need to be passed.
7. Click **OK** to save and activate the change.

You might be automatically disconnected from the appliance's management interface. You can now disconnect your management laptop or desktop from the appliance's X0 interface, and power the appliance off before physically connecting it to your network.

Installing the Appliance between the Network and an SSL VPN Appliance

Regardless of your deployment method (single- or dual-homed), the appliance should be placed between the X0/LAN interface of the SSL VPN appliance and the connection to your internal network. This allows the device to connect out to SonicWall's licensing and signature update servers, and to scan the decrypted traffic from external clients requesting access to internal network resources.

If your SSL VPN appliance is in two-port mode behind a third-party firewall, it is dual-homed.

To connect a dual-homed SSL VPN appliance:

1. Cable the X0/LAN port on the appliance to the X0/LAN port on the SSL VPN appliance.
2. Cable the X1/WAN port on the appliance to the port where the SSL VPN was previously connected.
3. Power on the appliance.

If your SSL VPN appliance is in one-port mode in the DMZ of a third-party firewall, it is single-homed.

To connect a single-homed SSL VPN appliance:

1. Cable the X0/LAN port on the appliance to the X0/LAN port of the SSL VPN appliance.
2. Cable the X1/WAN port on the appliance to the port where the SSL VPN was previously connected.

3. Power on the appliance.

Configuring or Verifying Settings

From a management station inside your network, you should now be able to access the management interface on the appliance using its WAN IP address.

To configure or verify settings:

1. Ensure that all security services for the appliance are enabled. See *Licensing Services* and *Activating Security Services on Each Zone*.
2. SonicWall Content Filtering Service must be disabled before the device is deployed in conjunction with a SonicWall SMA SSL VPN appliance.
    a. Navigate to **OBJECT | Match Objects > Zones** page.
    b. Click **Configure** next to the **LAN (X0)** zone.
    c. Clear **Enforce Content Filtering Service**.
    d. Click **OK**.
3. If you have not yet changed the administrative password on the appliance, you can do so on **DEVICE | Settings > Administration**.
4. To test access to your network from an external client, connect to the SSL VPN appliance and log in.
5. When connected, attempt to access to your internal network resources. If there are any problems, review your configuration and see *Configuring the Common Settings for L2 Bridged Mode Deployments*.

Configuring Layer 2 Bridged Mode

Topics:

Configuration Task List for Layer 2 Bridged Mode

- Choose a topology that suits your network
- Configuring the Common Settings for L2 Bridged Mode Deployments
    - License security services
    - Disable DHCP server
    - Configure and enable SNMP and HTTP/HTTPS management
    - Enable syslog

    - Activate security services on affected zones
    - Create Access Rules
    - Configure log settings
    - Configure wireless zone settings
- Configuring the Primary Bridge Interface
    - Select the zone for the Primary Bridge Interface
    - Activate management
    - Activate security services
- Configuring the Secondary Bridge Interface
    - Select the zone for the Secondary Bridge Interface
    - Activate management
    - Activate security services
- Apply security services to the appropriate zones

Configuring the Common Settings for L2 Bridged Mode Deployments

The following settings need to be configured on your appliance before using it in most of the Layer 2 Bridged Mode topologies:

- Licensing Services
- Disabling DHCP Server
- Configuring SNMP Settings
- Enabling SNMP and HTTPS on the Interfaces
- Enabling Syslog
- Activating Security Services on Each Zone
- Creating Access Rules
- Configuring Log Settings
- Configuring Wireless Zone Settings

Licensing Services

When your appliance is successfully registered:

1. Navigate to **DEVICE | Settings > Licenses**.
2. Click **Synchronize** from the top right of the top banner.

This contacts the appliance licensing server and ensures the appliance is properly licensed.

To check licensing status, go to **DEVICE | Settings > Licenses** and in the second column, view the license status of all security services.

Disabling a DHCP Server

When using an appliance in Layer 2 Bridged Mode in a network configuration where another device is acting as the DHCP server, you must first disable the appliance's internal DHCP engine, which is configured and running by default.

To disable the DHCP server:

1. Navigate to **NETWORK | System > DHCP Server**.
2. Disable **Enable DHCPv4/6 Server**.
3. Click **Accept**.

Configuring SNMP Settings

To configure SNMP settings:

1. Navigate to **DEVICE | Settings > SNMP**.
2. Select **Enable SNMP**.
3. Click **Accept**. **Configure** becomes active and the SNMP information is populated.
4. Click **Configure**. The **Configure SNMP** dialog displays. For how to configure SNMP, see *Setting Up SNMP Access*.

Enabling SNMP and HTTPS on the Interfaces

To enable SNMP and HTTPS on the interfaces:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Edit** icon for the interface through which you manage the appliance. The **Edit Interface** dialog displays.
3. For the **Management** option, enable **HTTPS** and **SNMP**.
4. Click **OK**.

Enabling Syslog

Enable Syslog on the **DEVICE | Log > Syslog** page. For information on how to enable Syslog, see the *SonicOS Log Administration Guide*.

Activating Security Services on Each Zone

In **NETWORK | System > Interfaces**, for each zone you are using, make sure that the security services are activated.

Then, for each service on **POLICY | Security Services**, activate and configure the settings that are most appropriate for your environment. For information about activating and configuring security services, see the *SonicOS Security Services Administration Guide*.

Creating Access Rules

If you plan to manage the appliance from a different zone, or if you are using a third-party server for management, SNMP, or syslog services, create Access Rules for traffic between the zones. On **POLICY | Rules and Policies > Access Rules**, click the icon for the intersection of the zone of the server and the zone that has users and servers (your environment could have more than one of these intersections). Create a new rule to allow the server to communicate with all devices in that zone. For information about Access Rules, see the *SonicOS Policies Administration Guide*.

Configuring Log Settings

On **DEVICE | Log > Name Resolution**, set the **Name Resolution Method** to **DNS** then **NetBios**. For information about configuring log settings, see the **SonicOS Log Administration Guide**.

Configuring Wireless Zone Settings

When you are using an HP PCM+/NIM system, if it is managing a HP ProCurve switch on an interface assigned to a WLAN/Wireless zone, you need to deactivate two features; otherwise, you cannot manage the switch.

To configure wireless zone settings:

1. Navigate to **NETWORK | System > Interfaces**.
2. Select your Wireless zone.
3. On Wireless, clear the **Only allow traffic generated by a SonicPoint and WiFiSec Enforcement** option.
4. Click **OK**.

Configuring Layer 2 Bridged Mode Procedure

Refer to the L2 Bridge Interface Zone Selection for choosing a topology that best suits your network. This example uses a topology that most closely resembles the Simple L2 Bridge Topology.

Choose an interface to act as the Primary Bridge Interface. Refer to the L2 Bridge Interface Zone Selection for information in making this selection. This example uses X1 (automatically assigned to the Primary WAN).

Topics:

Configuring the Primary Bridge Interface

To configure the primary bridge interface:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Configure** icon in the right column of the X1 (WAN) interface.

3. Configure the interface with a Static IP address (for example, `192.168.0.12`).

   NOTE: The Primary Bridge Interface must have a Static IP assignment.

4. For WAN interfaces only:
   a. Configure the default gateway. This is required for the appliance itself to reach the Internet.
   b. Configure the DNS server.
5. Choose one or more **Management** options for the interface: **HTTPS**, **Ping** (selected by default), **SNMP**, **SSH**.

   NOTE: Selecting **HTTPS** activates and selects **Add rule to enable redirect from HTTP to HTTPS automatically**. For more information about HTTP/HTTPS redirection, see HTTP/HTTPS Redirection.
6. Choose **User Login** options: **HTTP**, **HTTPS**.
7. To enable redirect to HTTPS from HTTP, select **Add rule to enable redirect from HTTP to HTTPS**. For more information about this option, see HTTP/HTTPS Redirection.
8. Click **OK**.

Choose an interface to act as the Secondary Bridge Interface. Refer to the L2 Bridge Interface Zone Selection for information in making this selection.

Configuring the Secondary Bridge Interface

This example uses X0 (automatically assigned to the LAN):

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Configure** icon in the right column of the X0 (LAN) interface.
3. From **IP Assignment**, select **Layer 2 Bridged Mode**.
4. From **Bridged to**, select the **X1** interface.
5. Choose one or more **Management** options for the interface: **HTTPS**, **Ping** (selected by default), **SNMP**, **SSH**.

   NOTE: Selecting HTTPS activates and selects Add rule to enable redirect from HTTP to HTTPS automatically. For more information about HTTP/HTTPS redirection, see HTTP/HTTPS Redirection.
6. Choose **User Login** options: **HTTP**, **HTTPS**.
7. To enable redirect to HTTPS from HTTP, select **Add rule to enable redirect from HTTP to HTTPS**. For more information about this option, see HTTP/HTTPS Redirection.
8. You can optionally enable **Block all non-IPv4 traffic** to prevent the L2 bridge from passing non-IPv4 traffic.
9. To control VLAN traffic through the L2 bridge, click **VLAN Filtering**. By default, all VLANs are allowed:
   - Select **Block listed VLANs (blacklist)** from the drop-down menu and add the VLANs you wish to block from the left pane to the right pane. All VLANs added to the right pane is blocked, and all VLANs remaining in the left pane are allowed.
   - Select **Allow listed VLANs (whitelist)** from the drop-down menu and add the VLANs you wish to explicitly allow from the left pane to the right pane. All VLANs added to the right pane are allowed,

and all VLANs remaining in the left pane are blocked.

10. Click **OK**. The **Interface Settings** table displays the updated configuration:

You can now apply security services to the appropriate zones, as desired. In this example, they should be applied to the LAN, WAN, or both zones.

Configuring an L2 Bypass for Hardware Failures

An L2 bypass enables you to perform a physical bypass of the appliance when an interface is bridged to another interface with LAN bypass capability. This allows network traffic to continue flowing when an unrecoverable firewall failure occurs.

When the L2 bypass relay is closed, the network cables attached to the bypassed interfaces (X0 and X1) are physically connected as if they were a single continuous network cable. The **Engage physical bypass on malfunction** option provides you the choice of avoiding disruption of network traffic by bypassing the firewall in the event of a malfunction.

L2 bypass is only applicable to interfaces in **Layer 2 Bridged Mode**. The **Engage physical bypass on malfunction** option only appears when the **Layer 2 Bridged Mode** option is selected from **Mode / IP Assignment**. This option does not appear unless a physical bypass relay exists between the two interfaces of the bridge-pair.

When the **Engage physical bypass on malfunction** option is enabled, the other **Layer 2 Bridged Mode** options are automatically set

- **Block all non-IPv4 traffic** – disabled. When enabled, this option blocks all non-IPv4 Ethernet frames. So, this option is disabled.
- **Never route traffic on this bridge-pair** – enabled. When enabled, this option prevents packets from being routed to a network other than the peer network of the bridged pair. So, this option is enabled.
- **Only sniff traffic on this bridge-pair** – disabled. When enabled, traffic received on the bridge-pair interface is never forwarded. So, this option is disabled.
- **Disable stateful-inspection on this bridge-pair** – unchanged. This option is not affected.

To configure an L2 bypass:

1. Navigate to **NETWORK | System > Interfaces**.
2. Click the **Edit** icon in the **Configure** column for the interface you want to configure. The **Edit Interface** dialog displays.
3. Select **Engage physical bypass on malfunction**.

   ⓘ **NOTE:** The **Engage physical bypass on malfunction** option is available only when the X0 and X1 interfaces are bridged together on an NSa-6600 or higher.
4. Click **OK**.

VLAN Integration with Layer 2 Bridged Mode

VLANs are supported on SonicWall firewalls. When a packet with a VLAN tag arrives on a physical interface, the VLAN ID is evaluated to determine if it is supported. The VLAN tag is stripped, and packet processing continues

as it would for any other traffic. A simplified view of the inbound and outbound packet path includes these potentially reiterative steps:

- IP validation and reassembly
- Decapsulation (802.1q, PPP)
- Decryption
- Connection cache lookup and management
- Route policy lookup
- NAT Policy lookup
- Access Rule (policy) lookup
- Bandwidth management
- NAT translation
- Advanced Packet Handling (as applicable)
    - TCP validation
    - Management traffic handling
    - Content Filtering
    - Transformations and flow analysis (on SonicWall firewalls): H.323, SIP, RTSP, ILS/LDAP, FTP, Oracle, NetBIOS, Real Audio, TFTP
    - IPS and GAV

At this point, if the packet has been validated as acceptable traffic, it is forwarded to its destination. The packet egress path includes:

- Encryption
- Encapsulation
- IP fragmentation

On egress, if the route policy lookup determines that the gateway interface is a VLAN subinterface, the packet is tagged (encapsulated) with the appropriate VLAN ID header. The creation of VLAN subinterfaces automatically updates the firewall's routing policy table:

The auto-creation of NAT policies, Access Rules with regard to VLAN subinterfaces behave exactly the same as with physical interfaces. Customization of the rules and policies that govern the traffic between VLANs can be performed with customary SonicOS ease and efficiency.

When creating a zone (either as part of general administration, or as a step in creating a subinterface), a checkbox is presented on the zone creation page to control the auto-creation of a GroupVPN for that zone. By default, only newly created Wireless type zones have **Create GroupVPN for this zone** enabled, although the option can be enabled for other zone types by selecting the checkbox during creation.

Management of security services between VLAN subinterfaces is accomplished at the zone level. All security services are configurable and applicable to zones comprising physical interfaces, VLAN subinterfaces, or combinations of physical and VLAN subinterfaces.

Gateway Anti-Virus and Intrusion Prevention between the different workgroups can easily be employed with the use of VLAN segmentation, obviating the need for dedicated physical interfaces for each protected segment.

VLAN support enables organizations to offer meaningful internal security (as opposed to simple packet filtering) between various workgroups, and between workgroups and server farms without having to use dedicated physical interfaces on the firewall.

Here the ability to assign VLAN subinterfaces to the WAN zone, and to use the WAN client mode (only Static addressing is supported on VLAN subinterfaces assigned to the WAN zone) is illustrated, along with the ability to support WAN Load Balancing and failover. Also demonstrated is the distribution of SonicPoints throughout the network by means of connecting them to access mode VLAN ports on workgroup switches. These switches are then backhauled to the core switch, which then connects all the VLANs to the appliance through a trunk link.

VPN Integration with Layer 2 Bridged Mode

When configuring a VPN on an interface that is also configured for Layer 2 Bridged Mode, you must configure an additional route to ensure that incoming VPN traffic properly traverses the appliance.

To configure VPN integration with Layer 2 bridged mode:

1. Navigate to **POLICY | Rules and Policies > Routing Rules**.
2. Click the **+Add** icon. The **Adding Rule** dialog displays.
3. Configure the route as follows:
    - Source: **ANY**
    - Destination: *custom-VPN-address-object* (This is the address object for the local VPN tunnel IP address range.)
    - Service: **ANY**
    - Gateway: `0.0.0.0`
    - Interface: **X0**
4. Click **OK**.

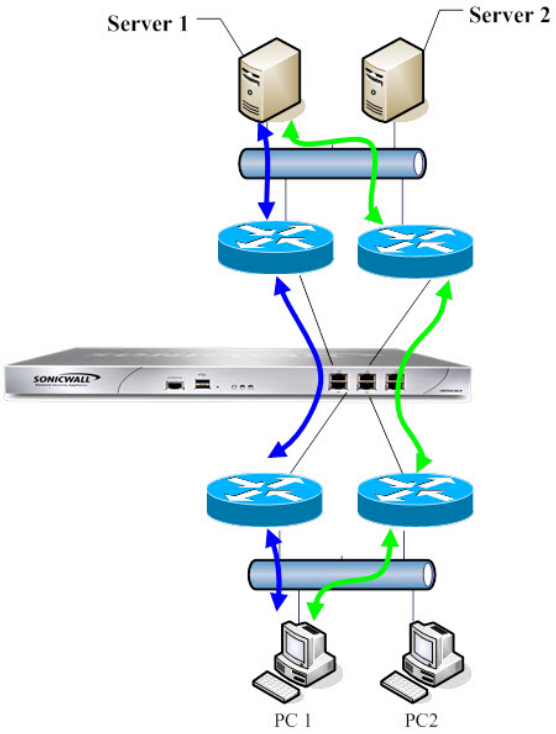
Asymmetric Routing

SonicOS supports asymmetric routing. Asymmetric routing is when the flow of packets in one direction passes through a different interface than that used for the return path. This can occur when traffic flows across different layer 2 bridged pair interfaces on the firewall or when it flows across different appliances in a high availability cluster.

Any appliance that performs deep packet inspection or stateful firewall activity must “see” all packets associated with a packet flow. This is in contrast to traditional IP routing in which each packet in a flow might technically be forwarded along a different path as long as it arrives at its intended destination — the intervening routers do not have to see every packet. Today’s routers do attempt to forward packets with a consistent next-hop for each packet flow, but this applies only to packets forwarded in one direction. Routers make no attempt to direct return traffic to the originating router. This IP routing behavior presents problems for a appliance cluster that does not support asymmetric routing because the set of Cluster Nodes all provide a path to the same networks. Routers

forwarding packets to networks through the cluster might choose any of the Cluster Nodes as the next-hop. The result is asymmetric routing, in which the flow of packets in one direction go through a node different than that used for the return path. This difference in flow causes traffic to be dropped by one or both Cluster Nodes as neither is “seeing” all of the traffic from the flow. See Asymmetric Routing.

ASYMMETRIC ROUTING



Asymmetric Routing Traffic

In Asymmetric Routing, PC1 communicates with Server1, two-way traffic passes through different routers, that is, some packets of same connection go through blue path, some go through green path. On such deployments, the routers might run some redundancy route or load balancing protocols, for example, the Cisco HSRP protocol.

SonicOS uses stateful inspection. All connections passing through the appliance are bound to interfaces. With support for asymmetric routing, however, SonicOS tracks ingress and egress traffic, even when the flows go across different interfaces, and provides stateful, deep packet inspection.

ⓘ | **NOTE:** Asymmetric routing is not the same as one-way connections without reply, that is, TCP State Bypass.

Configuring Interfaces for IPv6

For a complete description of configuring IPv6 interfaces, see *IPv6 Interface Configuration*.

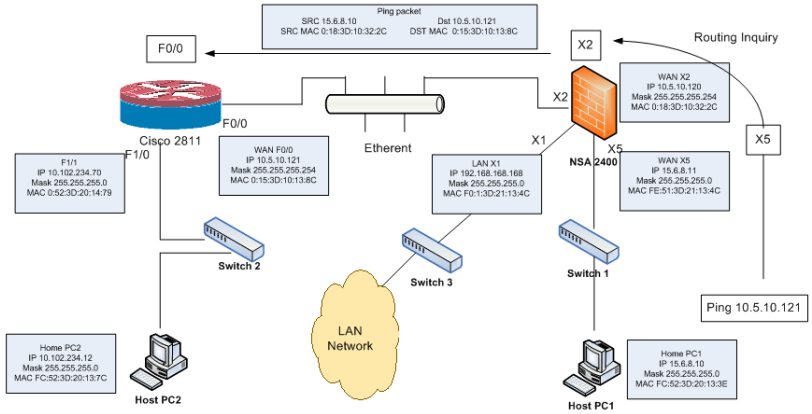
31-Bit Network Settings

SonicOS includes support for RFC 3021 that defines the use of a 31-bit subnet mask. This mask allows only two host addresses in the subnet, with no network or gateway addresses and no broadcast address. Such a configuration can be used within a larger network to connect two hosts with a point-to-point link. The savings in address space as a result of this change is recognizable as each point-to-point link in a large network would consume only two addresses instead of four.

In this context, the point-to-point link is not equivalent to PPP (point to point protocol). A point-to-point link using a 31-bit mask can use or not use the PPP protocol. 31-bit prefixed IPv4 addresses on a point-to-point link can also be used in the Ethernet network.

Topics:

31-Bit Network Environment Example



In this network environment, Host PC1 and Host PC2 can visit each other, while hosts in the LAN network can visit Host PC2.

To configure settings for this environment:

1. For Host PC1, add two route entries:
    - `Route add 10.5.10.0 mask 255.255.255.0 15.6.8.10`
    - `Route add 10.102.234.0 mask 255.255.255.0 15.6.8.10`

2. For Host PC2, add two route entries:
    - `Route add 10.5.10.0 mask 255.255.255.0 10.102.234.70`
    - `Route add 15.6.8.0 mask 255.255.255.0 10.102.234.70`
3. On the Cisco router (F0/0):
    - `interface fastEthernet 0/0`
    - `ip address 10.5.10.120 255.255.255.254`
4. On the Cisco 2811, add one route entry:

```
!
ip route 15.6.8.0 255.255.255.0 10.5.10.120
!
```

5. On the firewall, add one route entry to enable the WAN zone data flow from X2 to X5, and X5 to X2:

```
Any 10.102.234.0 Any X2 Default Gateway X2
```

Configuring a 31-Bit Network in SonicOS

To configure an interface for a 31-bit subnet in SonicOS:

1. Navigate to **NETWORK | System > Interfaces**.
2. Edit the desired interface.
3. Set the **Subnet Mask** to `255.255.255.254`.
4. Enter one host IP address into the **IP Address** field.
5. Enter the other host IP address into the **Default Gateway** field.
6. Set the other fields according to your network, as needed.
7. Click **OK**.

PPPoE Unnumbered Interface Support

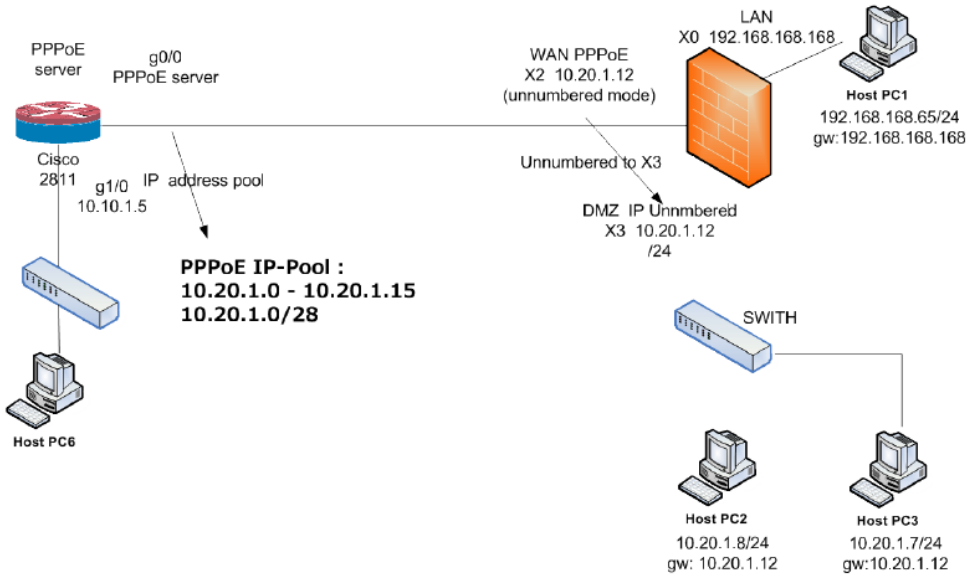
A PPPoE unnumbered interface allows you to manage a range of IP addresses with a single PPPoE connection. The Internet Service Provider (ISP) provides multiple static IP addresses that can be allocated within the subnet. The first address is designated as the network address, and the last one as the broadcast address.

The default MTU of PPPoE is **1492**.

Topics:

- Sample Network Topography
- Caveats
- Configuring a PPPoE Unnumbered Interface
- Configuring HA with PPPoE Unnumbered

Sample Network Topography



In this topology, X2 is the PPPoE unnumbered interface, and X3 is an unnumbered interface.

SonicOS adds two policies to the **NETWORK | System > Dynamic Routing** table.

SonicOS also adds two NAT policies.

Caveats

To change X3 to another mode when X2 unnumbered to X3 is configured, first terminate the relationship with X2 by changing X2 to another mode. Otherwise, if you change the IP address or mask of interface X3, it causes X3 to reconnect to the PPPoE server.

If X3 is set as unnumbered interface, other interfaces cannot connect to X3 using an L2 Bridge.

Configuring a PPPoE Unnumbered Interface

To configure a PPPoE unnumbered interface:

1. Navigate to **NETWORK | System > Interfaces**.
2. Configure the PPPoE client settings on a WAN interface by clicking its **Edit** icon. The **Edit Interface** dialog displays.
3. Select **Unnumbered interface**. The drop-down menu activates.
4. Select **Create new unnumbered Interface**. The **Add Unnumbered Interface** dialog displays.
5. For **Zone**, select **LAN**, **DMZ**, or create a new zone.

ⓘ | **NOTE: Mode / IP Assignment** is set to **IP Unnumbered** and dimmed.

6. For **IP Address**, enter the address provided by your ISP. Usually it is the second IP address assigned by the provider.
7. Enter the subnet mask assigned by the ISP in the **Subnet Mask** field.
8. Finish configuring this interface.
9. Click **OK**.
10. Finish configuring the first interface.
11. Click **OK**.

Configuring HA with PPPoE Unnumbered

For information on how to configure High Availability (HA) with PPPoE Unnumbered, see *Configuring Active/Standby High Availability Settings*.

3

Failover & LB

WAN Failover enables you to configure one of the user-defined interfaces as a secondary WAN port. The secondary WAN port can be used in a simple “active/passive” setup to allow traffic to be only routed through the secondary WAN port if the primary WAN port is unavailable. This allows the SonicWall to maintain a persistent connection for WAN port traffic by “failing over” to the secondary WAN port.

For a SonicWall appliance with a WWAN interface, you can configure failover using the WWAN interface. Failover between the Ethernet WAN (the WAN port, OPT port, or both) and the WWAN is supported through the **WAN Connection Model** setting.

This feature also allows you to do simple load balancing (LB) for the WAN traffic on the SonicWall. You can select a method of dividing the outbound WAN traffic between the two WAN ports and balance network traffic. Load-balancing is currently only supported on Ethernet WAN interfaces.

SonicOS can monitor WAN traffic using Physical Monitoring that detects when the link is unplugged or disconnected, or Physical and Logical Monitoring that monitors traffic at a higher level, such as upstream connectivity interruptions.

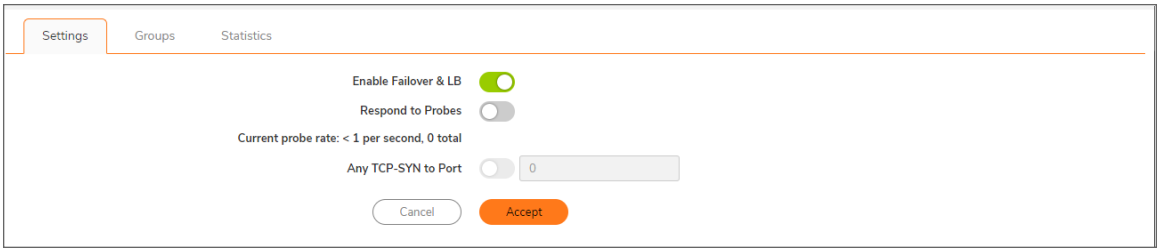
ⓘ **IMPORTANT:** Before you begin, be sure you have configured a user-defined interface to mirror the WAN port settings.

Topics:

Settings

To configure the WAN Failover for a SonicWall appliance:

1. Navigate to the **NETWORK | System > Failover & LB** page.

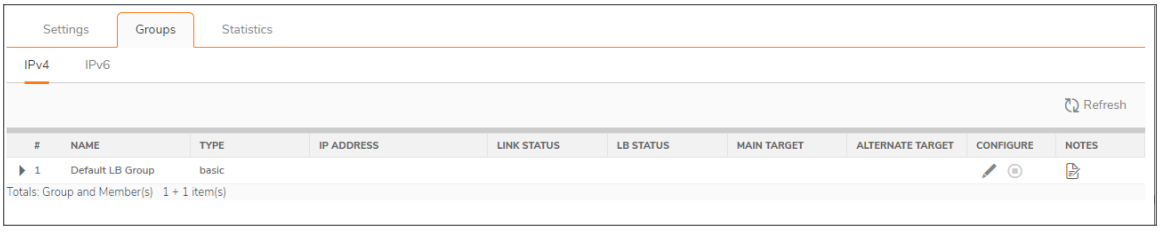


2. On the **Settings** tab, select **Enable Failover & LB**. This option must be enabled for you to access the **Groups** and **Statistics** tabs. If disabled, no options for failover and load balancing are available for configuration. This option is selected by default.
3. Select **Respond to Probes**. When enabled, the appliance can reply to probe request packets that arrive on any of the appliance's interfaces. This option is not selected by default. Enabling this option makes the **Any TCP-SYN to Port** option available.
4. Select **Any TCP-SYN to Port**.
    - This option is only available when the **Respond to Probes** option is enabled. When selected, the appliance only responds to TCP probe request packets having the same packet destination address TCP port number as the configured value. The default TCP port number is **0**.
    - This option is not selected by default.
5. Click **Accept**.

Groups

To configure Group settings:

1. Navigate to the **NETWORK | System > Failover & LB** page.
2. Click the **Groups** tab and then click **Configure** for the Group you wish to configure.



The **Edit LB Group** dialog displays.

3. From the **General** tab, choose the type (or method) of LB; options change depending on the type selected:
   - **Basic Failover**—The four WAN interfaces use rank to determine the order of preemption when **Preempt and failback to preferred interfaces when possible** has been enabled. Only a higher-ranked interface can preempt an active WAN interface. This is selected by default.
   - **Round-Robin**—This option now allows you to reorder the WAN interfaces for Round Robin selection. The default order is:
     - Primary WAN Percentage
     - Alternate WAN #1 Percentage
     - Alternate WAN #2 Percentage
     - Alternate WAN #3 Percentage

     The Round Robin then returns to the primary WAN to continue the order.
   - **Spill-Over**—The bandwidth threshold applies to the primary WAN. When the threshold is exceeded, new traffic flows are allocated to the alternates in a Round Robin manner. If the primary WAN bandwidth goes below the configured threshold, Round Robin stops, and outbound new flows are again sent out only through the Primary WAN.

     ⓘ **NOTE:** Existing flows remain associated with the alternates (as they are already cached) until they time out normally.
   - **Ratio**—A percentages can be set for each WAN in the LB group. To avoid problems associated with configuration errors, ensure that the percentage corresponds correctly to the WAN interface it indicates.
4. Depending on what you selected from **Outbound Load Balancing Method**, one of these options display:

TYPE DROP-DOWN OPTIONS

Type Selection	Option
Basic Failover	**Preempt and failback to preferred interfaces when possible** Select to enable rank to determine the order of preemption. Selected by default.
Round Robin	**Use Source and Destination IP Address binding** The option is especially useful when using HTTP/HTTPS redirection or in a similar situation. For example, connection A and connection B need to be on the same WAN interface, the source and destination IP addresses in Connection A are the same as those for connection B, but a different service is being used. In this case, source and destination IP address binding is required to keep both the connections on the same WAN interface so that the transactions do not fail. This option is not selected by default.
Spill-Over	**When bandwidth exceeds this value on X1, new flows will go to the alternate group members in Round Robin manner** Specify the bandwidth for the Primary in the field. If this value is exceeded, new flows are then sent to alternate group members according to the order listed in the Selected column. This option is not selected by default. The default value is 0.

5. Add, delete, and order member interfaces in the **Group Members: Select here:/Selected Primary/Alt. Poll**: lists. The use of the selected members in the **Selected** list depends on the **Type** selected:

   - **Basic Failover: Interface Ordering:**
   - **Round Robin: Interface Pool:**
   - **Spill-Over: Primary/Alt. Pool:**
   - **Ratio: Interface Distribution:**

6. Add members by selecting a displayed interface from the **Group Members**: column, and then clicking **Add>>**.

   If you selected **Ratio**, instead of ordering the entries, you can specify the percentage of bandwidth for each interface. See *Configuring Bandwidth as a Percentage*.

   ⓘ **IMPORTANT:** To avoid problems associated with configuration errors, ensure that the percentage corresponds correctly to the WAN interface it indicates.

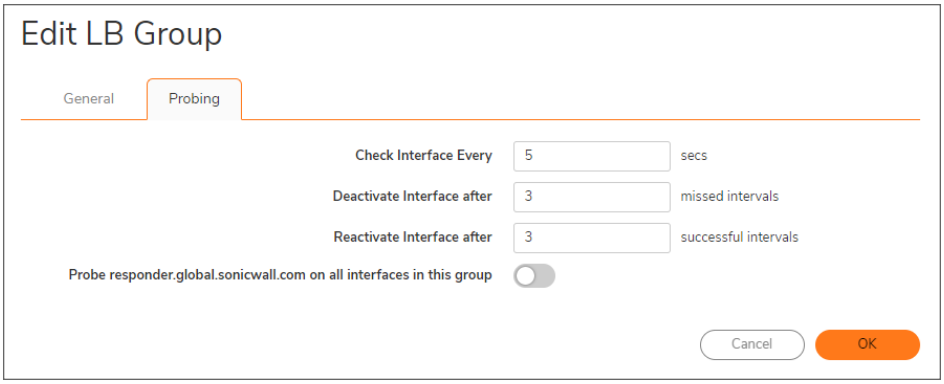
   a. Enter a percentage of bandwidth to be assigned to an interface in the percent (%) field. The total bandwidth for all interfaces should add up to 100 percent. The total percentage of bandwidth allocated is displayed.

   Delete members from the **Selected**: column by:

   1. Selecting the displayed interface.
   2. Clicking **<<Remove**.

   ⓘ **NOTE:** The interface at the top of the list is the Primary.
   The Interface Rank does not specify the operation performed on the individual member. The operation that is performed is specified by the Group Type.

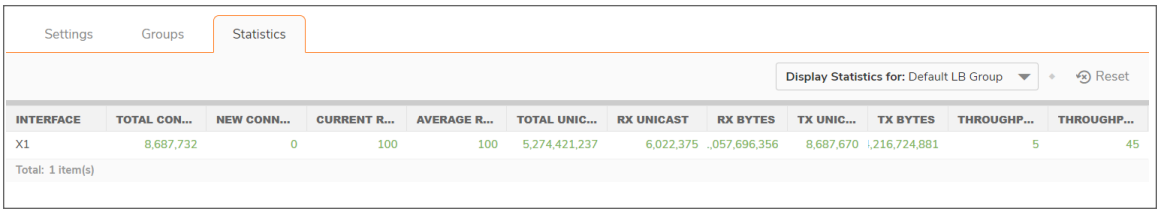
7. Click **OK**.
8. Complete the **Probing** tab.



Statistics

To see Load Balancing Statistics:

1. Navigate to the **NETWORK | System > Failover & LB** page.
2. Click **Configure** for the Statistics you wish to view in the **Statistics** table on the **NETWORK | System > Failover & LB** page. The **Statistics** dialog displays.



3. From the Display Statistics for drop-down menu, select the LB group for which you want to view statistics. The Load Balancing **Statistics** table displays the following LB group statistics for the firewall:
    - Interface –
    - Total Connections –
    - New Connection –
    - Current Ratio –
    - Average Ratio –
    - Total Unicast Bytes –
    - Rx Unicast –
    - Rx Bytes –
    - Tx Unicast –
    - Tx Bytes –
    - Throughput (KB/s) –
    - Throughput (Kbits/s) –
4. Click **Reset** on the top right of the **Statistics** table to clear its information.

4

Neighbor Discovery

The Neighbor Discovery Protocol (NDP) is a messaging protocol that was created as part of IPv6 to perform a number of the tasks that ICMP and ARP are able to accomplish with IPv4. Just like ARP, Neighbor Discovery builds a cache of dynamic entries, and you can configure static Neighbor Discovery entries. The IPv4/IPv6 neighbor table shows the IPv6 neighbor messages and functions that are analogous to the traditional IPv4 neighbor messages.

IPV4.IPV6 NEIGHBOR MESSAGES AND FUNCTIONS

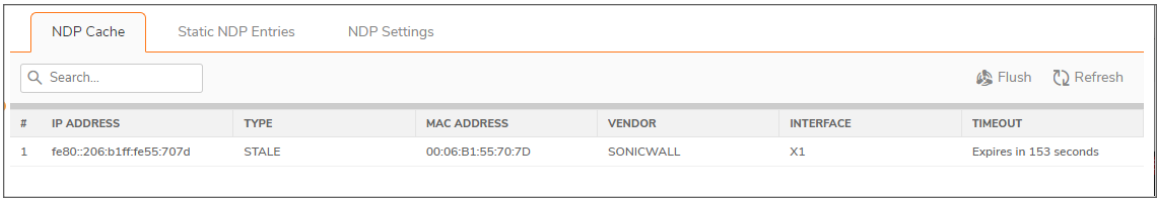
IPv4 Neighbor Message	IPv6 Neighbor Message
ARP request message	Neighbor solicitation message
ARP reply message	Neighbor advertisement message
ARP cache	Neighbor cache
Gratuitous ARP	Duplicate address detection
Router solicitation message (optional)	Router solicitation (required)
Router advertisement message (optional)	Router advertisement (required)
Redirect message	Redirect Message

The Static NDP feature allows for static mappings to be created between a layer 3 IPv6 address and a Layer 2 MAC address.

Topics:

NDP Cache

The **NDP Cache** table displays all current IPv6 neighbors.



IP Address	IPv6 IP address of the neighbor device.
Type	Type of neighbor: • **REACHABLE** - The neighbor is known to have been reachable within 30 seconds. • **STALE** - The neighbor is no longer known to be reachable, and traffic has been sent to the neighbor within 1200 seconds. • **STATIC** - The neighbor was manually configured as a static neighbor.
MAC Address	IPv6 MAC Address of the neighbor device.
Vendor	Name of the neighbor device's manufacturer.
Interface	Interface associated with this neighbor device.
Timeout	The length of inactivity time until the user times out.
Flush	Contains the **Delete** icon for the entry.

Flushing the NDP Cache

It is sometimes necessary to flush the NDP cache when an IP address has changed for a device on the network. As the IP address is linked to a physical address, the IP address can change, but still be associated with the physical address in the NDP Cache. Flushing the NDP Cache allows new information to be gathered and stored.

ⓘ **TIP:** To configure a specific length of time for an entry to time-out, enter a value in minutes in the NDP Cache entry time-out (minutes) field; see NDP Settings.

To flush an entry in the NDP Cache table:

1. Mouse-over the NDP Cache entry and click the **Flush** icon on the right side.

To flush one or more entries in the NDP Cache table:

1. Select the checkbox(es) of one or more entries to be flushed.
2. Mouse-over an NDP Cache entry and click **Flush**.

To flush all the entries in the NDP Cache table:

1. Select the top left checkbox in the **NDP Cache** table header. All NDP Cache entries are selected.
2. Mouse-over an entry and click **Flush** or **Flush All**.

Static NDP Entries

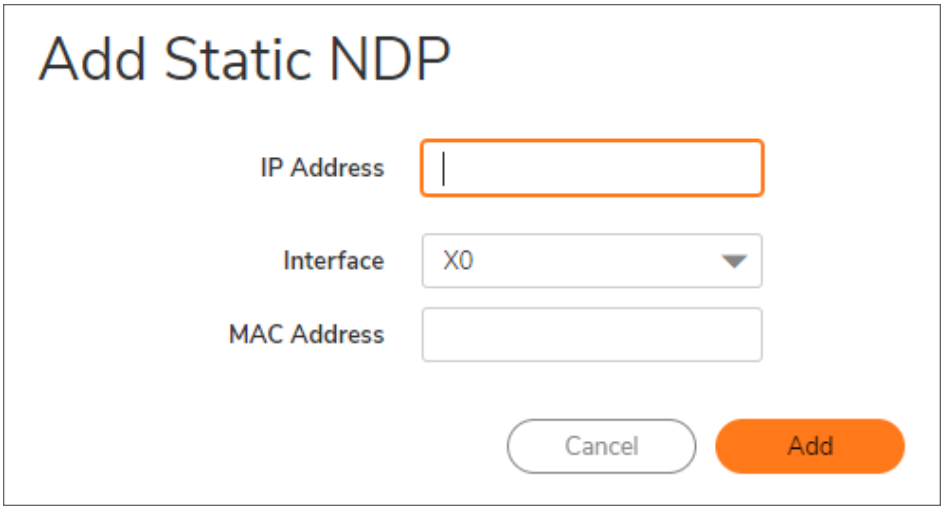
IP Address	IPv6 IP address for the remote device.
MAC Address	MAC address for the remote device.
Vendor	Name of the remote device's manufacturer.
Interface	Interface associated with the remote device.
Configure	Mouse-over contains the **Edit** and **Delete** icons for the entry.

Adding Static NDP Entries

To add a Static NDP entry:

1. Navigate to the **NETWORK | System > Neighbor Discovery** page.

2. Under the **Static NDP Entries** table, click **+Add**. The **Add Static NDP** dialog displays.



3. In the **IP Address** field, enter the IPv6 address for the remote device.
4. From **Interface**, select the interface on the SonicWall appliance that is used for the entry.
5. In the **MAC Address** field, enter the MAC address of the remote device.
6. Click **Add**. The Static NDP Entry is added.

Editing Static NDP Entries

To edit a Static NDP entry:

1. In the **Static NDP Entries** table, click the **Edit this entry** icon in the mouse-over column. The **Edit Static NDP** dialog displays.

2. Make the changes.
3. Click **Update**. The entry is updated.

Deleting Static NDP Entries

It is sometimes necessary to delete Static NDP Entries.

To delete an entry in the Static NDP Entries table:

1. Mouse-over the entry and click **Delete** or the **Delete this entry** icon.

To delete one or more entries in the Static NDP Entries table:

1. Select the checkbox(es) of one or more entries to be deleted.
2. Click **Delete**.

To flush all the entries in the Static NDP Entries table:

1. Select the top left checkbox in the **Static NDP Entries** table header.
2. Click **Delete**.

NDP Settings

In the **NDP Settings** tab, specify the maximum time to reach a neighbor.

ⓘ **NOTE:** For IPv6, this value also can be set for each interface on the **NETWORK | System > Interfaces | Edit Interface > Advanced** dialog. If **Router Advertisement** is enabled on an interface, the value set for the interface is used for that interface only. For more information, see *Configuring Interfaces*.

To specify the maximum time:

1. Navigate to the **NETWORK | System > Neighbor Discovery | NDP Settings** view.

2. Enter a number in the **Neighbor Discover BaseReachableTime (seconds)** field. The minimum is **0** seconds, the maximum is **3600** seconds, and the default is **30** seconds.

ⓘ **TIP:** When this option's value is set to **0**, the global value of NDP settings is used.

3. Click **Change**.

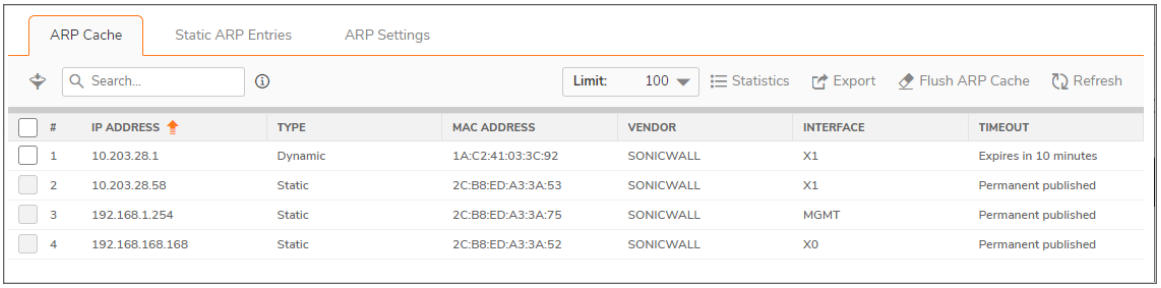
5

ARP

ARP (Address Resolution Protocol) maps layer 3 (IP addresses) to layer 2 (physical or MAC addresses) to enable communications between hosts residing on the same subnet. ARP is a broadcast protocol that can create excessive amounts of network traffic on your network. To minimize the broadcast traffic, an ARP cache is maintained to store and reuse previously learned ARP information.

Topics:

ARP Cache



IP Address	The IP Address of the appliance.
Type	Indicates whether the ARP is **Static** or **Dynamic**.
MAC Address	The MAC address associated with the IP Address.
Vendor	Name of the firewall's manufacturer.
Interface	The LAN interface associated with this ARP entry.
Timeout	Indicates the time remaining in cache for this entry. If the entry was published when configured, **Timeout** displays **Permanently published**.
Flush	Displays the **Delete** icon for flushing the entry from **ARP Cache**. ⓘ | **NOTE:** Only **Dynamic** entries have the **Delete** icon.

Topics:

- Flushing the ARP Cache

Flushing the ARP Cache

It is sometimes necessary to flush the ARP cache when the IP address has changed for a device on the network. As the IP address is linked to a physical address, the IP address can change, but still be associated with the physical address in the ARP Cache. Flushing the ARP Cache allows new information to be gathered and stored in the ARP Cache.

TIP: To configure a specific length of time for an entry to time out, enter a value in minutes in the **ARP Cache entry time out (minutes)** field; see ARP Settings.

To flush a dynamic entry in the ARP Cache table:

1. Click the **Flush ARP Cache** icon by using mouse-over on the right side of the entry.

To flush one or more dynamic entries in the ARP Cache table:

1. Select the checkbox(es) of one or more entries to be flushed. Flush becomes active.
2. Click the **Flush ARP Cache** icon.

To flush all the dynamic entries in the ARP Cache table:

1. Click the top checkbox located in the top left heading row. All dynamic entries are selected.
2. Click the **Flush ARP Cache** icon.

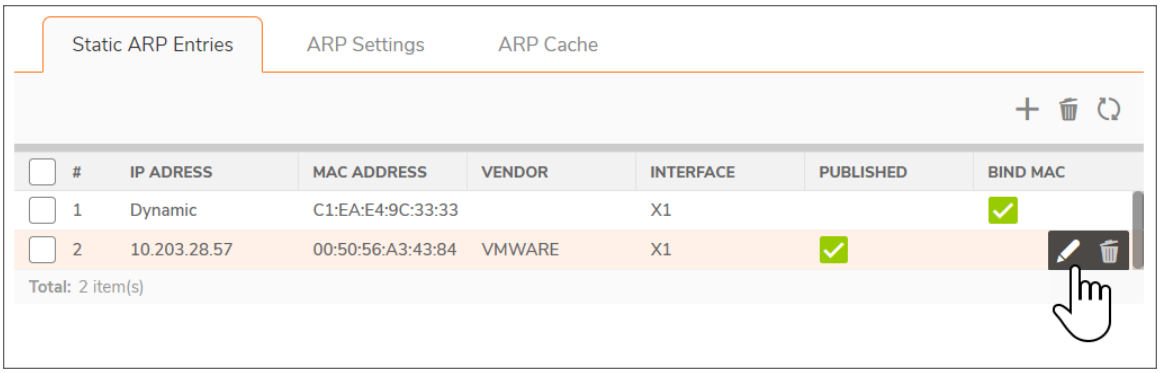
Static ARP Entries

The Static ARP Entries feature allows for static mappings to be created between layer 2 MAC addresses and layer 3 IP addresses.

Topics:

- Viewing Static ARP Entries
- Adding Static ARP Entries
- Editing Static ARP Entries
- Deleting Static ARP Entries
- Secondary Subnets with Static ARP

Viewing Static ARP Entries

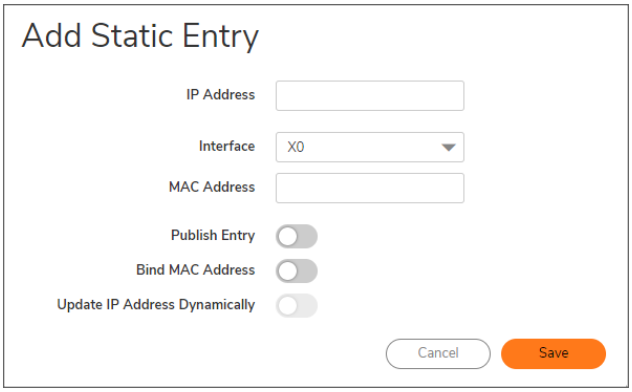


IP Address	IP address of the firewall serving as the gateway.
MAC Address	MAC address of the firewall serving as the gateway.
Vendor	Name of the firewall's manufacturer.
Interface	LAN interface associated with this entry.
Published	Indicates with a green checkmark whether the firewall responds to ARP queries for the specified IP address with the specified MAC address.
Bind MAC	Indicates with a green checkmark whether the MAC address is bound to the designated IP address and interface.

Adding Static ARP Entries

To add a Static ARP Entry:

1. Navigate to **NETWORK | System > ARP**.
2. From the **Static ARP Entries** tab, click **+Add**. The **Add Static Entry** dialog displays.



3. In the **IP Address** field, enter the IP address of the SonicWall appliance.

4. From **Interface**, select the LAN interface on the appliance to be associated with this static ARP entry.
5. In the **MAC Address** field, enter the MAC address of the appliance.
6. To cause the appliance to respond to ARP queries for the specified IP address with the specified MAC address, select the **Publish Entry** option. This option is not selected by default.

   This option can be used, for example, to have the firewall reply for a secondary IP address on a particular interface by adding the MAC address of the appliance. Selecting this option dims the **MAC Address** field and the **Bind MAC Address** option.
7. If you selected **Publish Entry**, go to **Click Save.**.
8. To bind the MAC address specified to the designated IP address and interface, select **Bind MAC Address**. This option is not selected by default.

   This option ensures that a particular workstation (as recognized by the network card's unique MAC address) can only the used on a specified interface on the appliance. After the MAC address is bound to an interface, the appliance:

   - Does not respond to that MAC address on any other interface.
   - Removes any dynamically cached references to that MAC address that might have been present.
   - Prohibits additional (non-unique) static mappings of that MAC address.

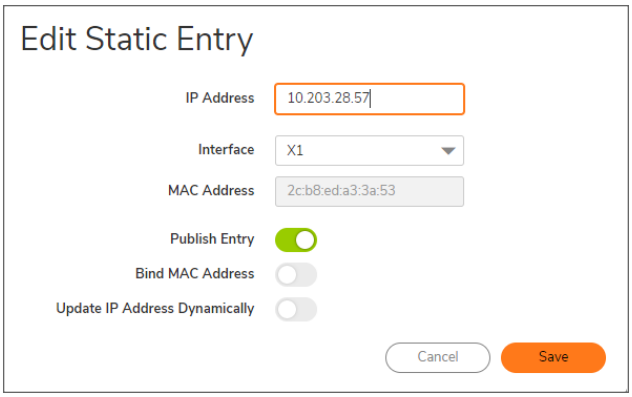
     When **Bind MAC Address** is selected, **Update IP Address Dynamically** becomes available.
9. To allow a MAC address to be bound to an interface when DHCP is being used to dynamically allocate IP addressing, select **Update IP Address Dynamically**, which is a subfeature of the **Bind MAC Address** option.

   Enabling this option dims the **IP Address** field and sets it to `0.0.0.0`, makes the **MAC Address** field available, and then populates the **ARP Cache** with the IP addresses allocated by either the appliance's internal DHCP server or when IP Helper is in use, by the external DHCP server.
10. Click **Save**.

Editing Static ARP Entries

To edit a Static ARP entry:

1. Navigate to **NETWORK | System > ARP**.
2. In the **Static ARP Entries** view, mouse-over the entry's **Edit** icon located to the right of the entry. The **Edit Static Entry** dialog displays.



3. Make any necessary changes.
4. Click **Save**. The entry is updated.

Deleting Static ARP Entries

To delete Static ARP entries from the Static ARP Entries table:

1. Navigate to **NETWORK | System > ARP | Static ARP Entries** view.
2. Select the checkbox next to the entry you would like to delete.
3. Mouse-over and click the **Trash** icon located to the right of the entry.
4. Click **Confirm** when the confirmation dialog box appears.

To delete all Static ARP entries from the Static ARP Entries table:

1. Navigate to **NETWORK | System > ARP | Static ARP Entries** view.
2. Select the top left checkbox in the table title row. All **Static ARP Entries** are selected.
3. Click the **Trash** icon on the right side of the table.
4. Click **Confirm** when the confirmation dialog box appears.

Secondary Subnets with Static ARP

The Static ARP feature allows for secondary subnets to be added on other interfaces without the addition of automatic NAT rules.

Topics:

Adding a Secondary Subnet

To add a secondary subnet using the Static ARP method:

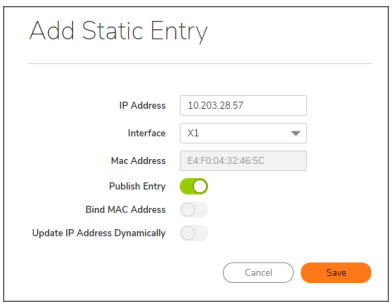
1. Add a *published* static ARP entry for the gateway address that is used for the secondary subnet, assigning it the MAC address of the appliance interface to which it is connected.
2. Add a static route for that subnet, so that the appliance regards it as valid traffic, and knows to which interface to route that subnet's traffic.
3. Add access rules to allow traffic destined for that subnet to traverse the correct network interface.
4. *Optional*: Add a static route on upstream device(s) so that they know which gateway IP to use to reach the secondary subnet.

Secondary Subnet Example

Consider the following network example (see Adding a Secondary Subnet).

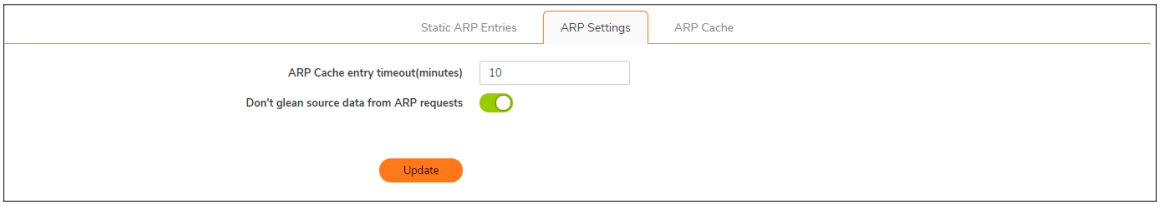
To support the added configuration:

1. Create a published static ARP entry for `10.203.28.57`, the address that serves as the gateway for the secondary subnet. Associate it with the appropriate LAN interface.
2. Navigate to the **NETWORK | System > ARP | Static ARP Entries** view.
3. Click the **Add Static ARP** (**+**) icon.
4. Add this entry:



5. Click **Save**. The entry appears in the **Static ARP Entries** table.
6. Navigate to **NETWORK | System > Dynamic Routing**.
7. Add a static route for the `10.203.28.57` network, with the `255.255.255.0` subnet mask on the X3 Interface. For information about adding static routes, see *Configuring Route Advertisements and Route Policies*.
8. To allow traffic to reach the `10.203.28.57` subnet and to allow the subnet to reach the hosts on the LAN, navigate to the **POLICY | Rules and Policies > Access Rules** page.
9. Add appropriate access rules to allow traffic to pass.

ARP Settings



ARP Cache entry timeout (minutes)	Specify a length of time for the entries to time out and to be flushed from the cache. The minimum time is two minutes, the maximum is 600 minutes (10 hours), and the default is **10** minutes.
Don’t glean source data from ARP requests	Select to prevent source data from being obtained from ARP requests. This option is not selected by default.

6

MAC IP Anti-Spoof

MAC and IP address-based attacks are increasingly common in today's network security environment. These types of attacks often target a Local Area Network (LAN) and can originate from either outside or inside a network. In fact, anywhere internal LANs are somewhat exposed, such as in office conference rooms, schools, or libraries, could provide an opening to these types of attacks. These attacks also go by various names: man-in-the-middle attacks, ARP poisoning, SPITS. The MAC-IP Anti-Spoof feature lowers the risk of these attacks by providing you with different ways to control access to a network, and by eliminating spoofing attacks at OSI Layer 2/3.

The effectiveness of the MAC-IP Anti-Spoof feature focuses on two areas. The first is admission control that allows you the ability to select which devices gain access to the network. The second area is the elimination of spoofing attacks, such as denial-of-service attacks, at Layer 2. To achieve these goals, two caches of information must be built: the MAC-IP Anti-Spoof Cache, and the ARP Cache.

The MAC-IP Anti-Spoof cache validates incoming packets and determines whether they are to be allowed inside the network. An incoming packet's source MAC and IP addresses are looked up in this cache. If they are found, the packet is allowed through. The MAC-IP Anti-Spoof cache is built through one or more of the following sub-systems:

- DHCP Server-based leases (SonicWall's - DHCP Server)
- DHCP relay-based leases (SonicWall's - IP Helper)
- Static ARP entries
- User created static entries

The ARP Cache is built through the following subsystems:

- ARP packets; both ARP requests and responses
- Static ARP entries from user-created entries
- MAC-IP Anti-Spoof Cache

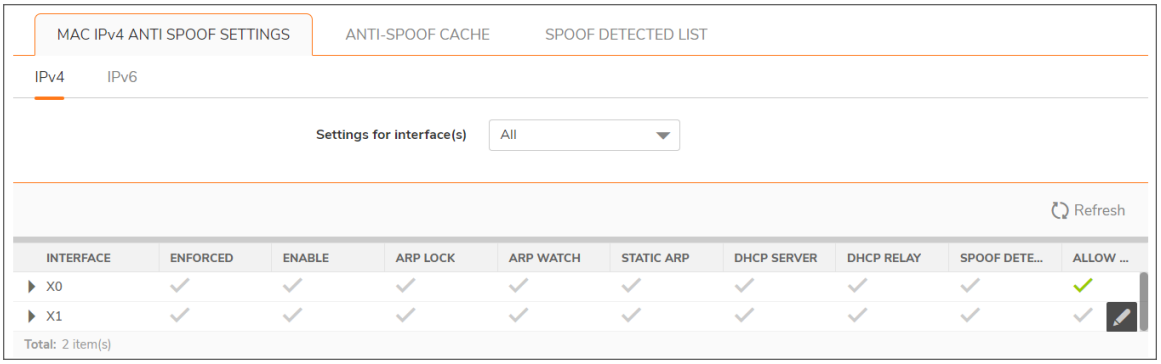
The MAC-IP Anti-Spoof subsystem achieves egress control by locking the ARP cache, so egress packets (packets exiting the network) are not spoofed by a bad device or by unwanted ARP packets. This prevents a firewall from routing a packet to the unintended device, based on mapping. This also prevents man-in-the-middle attacks by refreshing a client's own MAC address inside its ARP cache.

Topics:

MAC IPv4 and IPv6 Anti-Spoof Settings

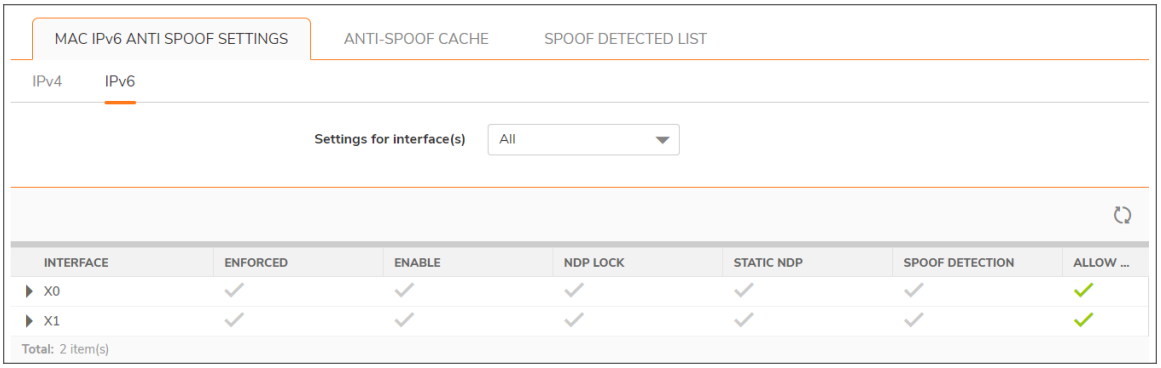
To edit MAC IPv4 Anti-Spoof Settings:

1. Navigate to the **NETWORK | System > MAC-IP Anti-Spoof** page.
2. Click the **IPv4** view.



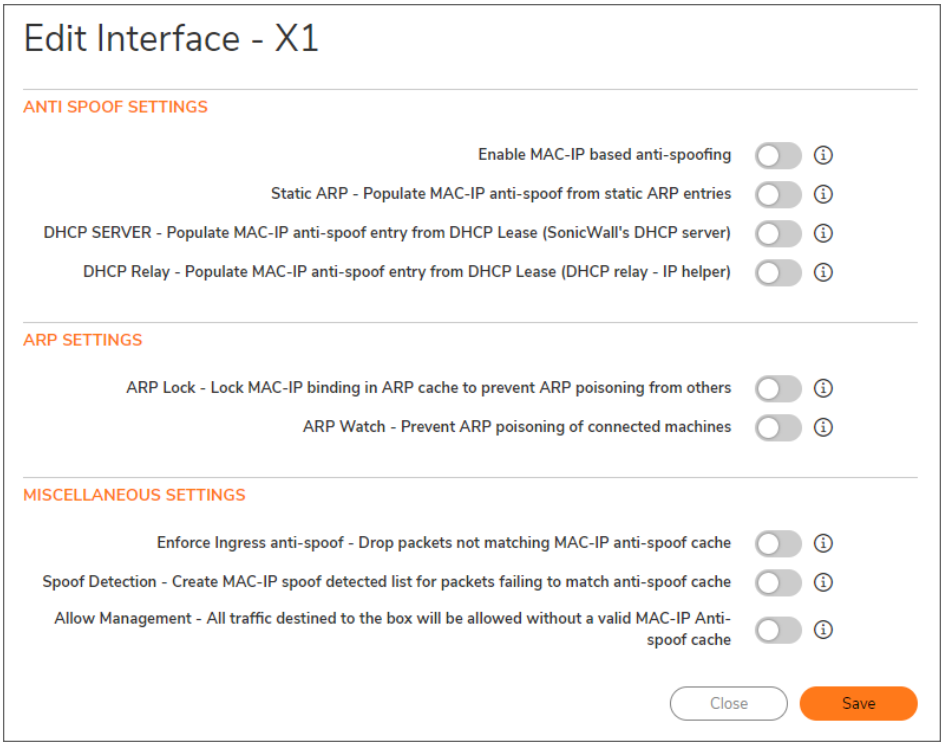
To edit MAC IPv6 Anti-Spoof Settings:

1. Navigate to the **NETWORK | System > MAC-IP Anti-Spoof** page.
2. Click the **IPv6** view.



Configuring MAC IP Anti-Spoof Settings

To configure settings for a particular interface, click the **Edit** icon in the **Configure** column for the desired interface. The **Edit Interface** dialog is displayed for the selected interface.



The following options are available:

- **Anti-Spoof Settings**
  - **Enable MAC-IP based anti-spoofing**: To enable the MAC-IP Anti-Spoof subsystem on traffic through this interface
  - **Static ARP**: Allows the Anti-Spoof cache to be built from static ARP entries
  - **DHCP Server**: Allows the Anti-Spoof cache to be built from active DHCP leases from the SonicWall DHCP server
  - **DHCP Relay**: Allows the Anti-Spoof cache to be built from active DHCP leases, from the DHCP relay, based on IP Helper
- **ARP Settings**
  - **ARP Lock**: Locks ARP entries for devices listed in the MAC-IP Anti-Spoof cache. This applies egress control for an interface through the MAC-IP Anti-Spoof configuration, and adds MAC-IP cache entries as permanent entries in the ARP cache. This controls ARP poisoning attacks, as the ARP cache is not altered by illegitimate ARP packets.

- **ARP Watch**: Prevents ARP poisoning of connected machines to protect all clients' PCs from man-in-the-middle attacks.

- **Miscellaneous Settings**
  - **Enforce Ingress anti-spoof**: Enables ingress control on the interface, blocking traffic from devices not listed in the MAC-IP Anti-Spoof Cache.
  - **Spoof Detection**: Logs all devices that fail to pass Anti-spoof cache and lists them in the **Spoof Detected List**.
  - **Allow Management**: Allows through all packets destined for the appliance's IP address, even if coming from devices currently not listed in the **Anti-Spoof Cache**.

After your setting selections for this interface are complete, click **Save**. After the settings have been adjusted, the interface's listing is updated on the MAC-IP Anti-Spoof page. The green circle with white check mark icons denote which settings have been enabled.

ⓘ | **NOTE:** The following interfaces are excluded from the MAC-IP Anti-Spoof list:

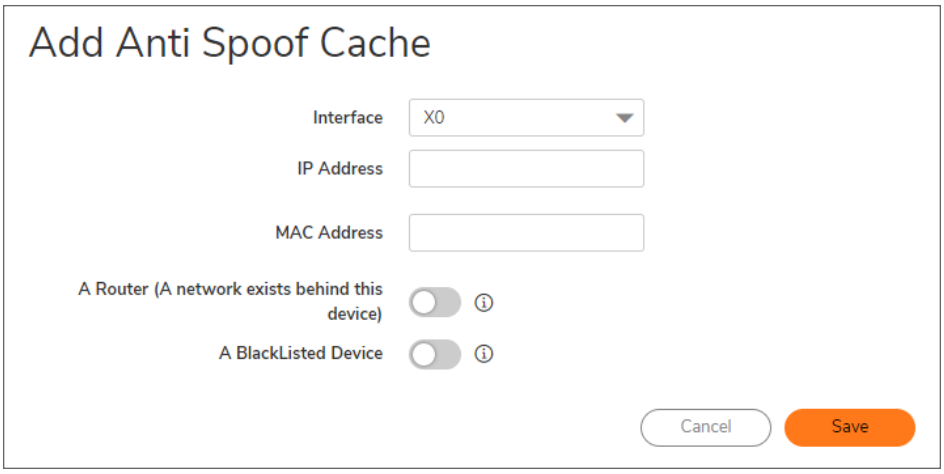
- Non-Ethernet interfaces
- Port-shield member interfaces
- Layer 2 bridge pair interfaces
- High availability interfaces
- High availability data interfaces

Anti-Spoof Cache

The MAC-IP Anti-Spoof Cache lists all the devices presently listed as "authorized" to access the network, and all devices marked as "blacklisted" (denied access) from the network.

To add a device to the list:

1. Navigate to the **NETWORK | System > MAC-IP Anti-Spoof** page.
2. Click **+Add**. The **Add Anti-Spoof Cache** dialog displays.



3. Select an interface from **Interface**.
4. Enter the IP address for the device in the **IP Address** field.
5. Enter the MAC address for the device in the **MAC Address** field.
6. Select the A Router option to allow traffic coming from behind this device.
7. Select the **A blacklisted device** option to block packets from this device, regardless of its IP address.
8. Click **Save**.

If you need to edit an Anti-Spoof cache entry, click the entry's **Edit** icon under the **Configure** column.

Single, or multiple, anti-spoof cache entries can be deleted. To do this, select the checkbox next to each entry, then click **Delete MAC-IP Anti-Spoof Cache**).

To clear cache statistics:

1. Select the desired devices, then click **Reset**.

Some packet types are bypassed even though the MAC-IP Anti-Spoof feature is enabled:

- Non-IP packets.
- DHCP packets with source IP as 0.
- Packets from a VPN tunnel.
- Packets with invalid Unicast IPs as their source IPs.
- Packets from interfaces where the Management status is not enabled under anti-spoof settings.

The Anti-Spoof Cache Search section provides the ability to search the entries in the cache.

To search the MAC-IP Anti-Spoof Cache:

1. Navigate to the **NETWORK | System > MAC-IP Anti-Spoof** page.
2. Enter a search string in the field.
3. Click **Search**. Matching entries in the MAC-IP Anti-Spoof cache are displayed.

To clear the Anti-Spoof Cache table and redisplay all entries, click **Refresh**.

Spoof Detected List

ⓘ | **NOTE:** Spoof Detected List display is available only at the Unit level.

The **Spoof Detected List** displays devices that failed to pass the ingress anti-spoof cache check. Entries on this list can be added as a static anti-spoof entry.

To view the Spoof Detected List:

1. Click **Request Spoof Detected List from Firewall**.

Entries can be flushed from the list by clicking **Flush**. The name of each device can also be resolved using NetBIOS, by clicking **Resolve**.

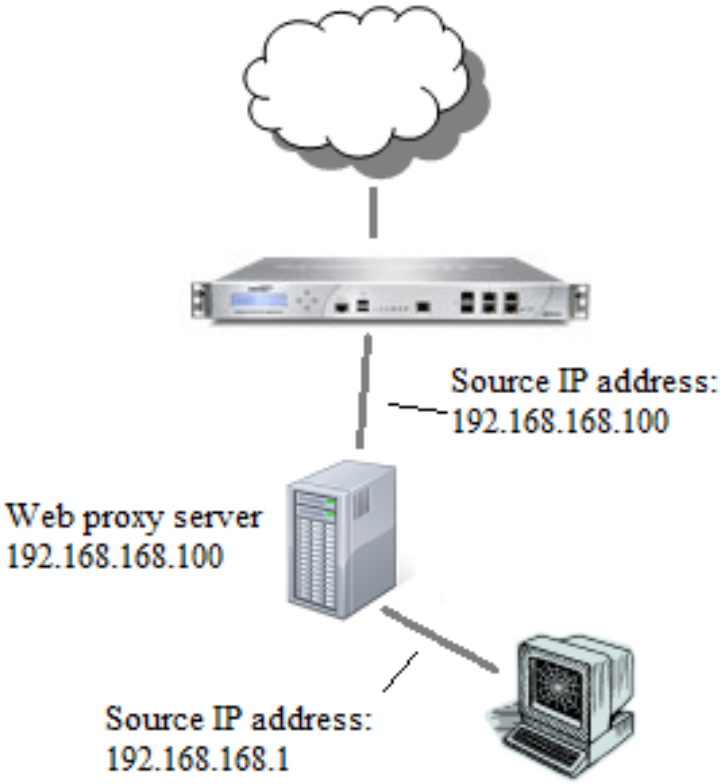
To add an entry to the static anti-spoof list:

1. Navigate to the **NETWORK | System > MAC-IP Anti-Spoof** page.
2. Click the **Edit** icon under the **Add** column for the desired device. An alert message window opens, asking if you wish to add this static entry.
3. Click **OK** to proceed.

7

Web Proxy

When accessing the web through a proxy server located on the internal network (between you and the SonicWall appliance), the HTTP/HTTPS connections recognized by the appliance originate from the proxy server, not from you.



Topics:

User Proxy Servers

A web proxy server intercepts HTTP requests and determines if it has stored copies of the requested web pages. If it does not, the proxy completes the request to the server on the Internet, returning the requested information to you and also saves it locally for future requests. Setting up a web proxy server on a network can be cumbersome, because each computer on the network must be configured to direct web requests to the server.

If you have a proxy server on your network, instead of configuring each computer's web browser to point to the proxy server, you can move the server to the WAN or DMZ zone and enable Web Proxy Forwarding using the settings on the **NETWORK | System > Web Proxy** page. The appliance automatically forwards all web proxy requests to the proxy server without requiring all the computers on the network to be configured.

Proxy Forwarding

A Web proxy server intercepts HTTP requests and determines if it has stored copies of the requested Web pages. If it does not, the proxy completes the request to the server on the Internet, returning the requested information to the user and also saving it locally for future requests.

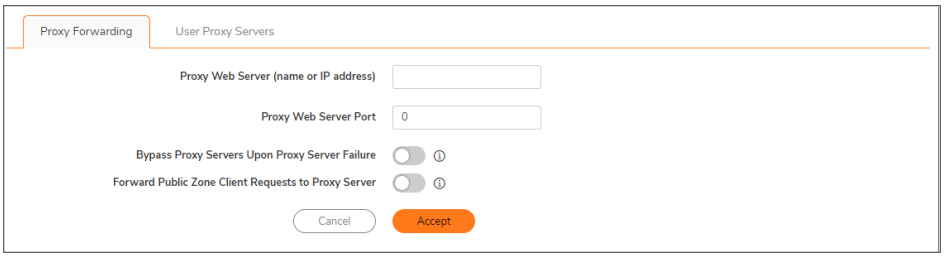
Setting up a Web proxy server on a network can be cumbersome, because each computer on the network must be configured to direct Web requests to the server.

If there is a proxy server on the SonicWall appliance's network, you can move the appliance between the network and the proxy server, and enable **Web Proxy Forwarding**. This forwards all WAN requests to the proxy server without requiring the computers to be individually configured.

ⓘ | **NOTE:** The proxy server must be located on the WAN or DMZ; it cannot be located on the LAN.

To configure a Proxy Web server:

1. Navigate to the **NETWORK | System > Web Proxy** page.



2. Type the name or IP address of the proxy server in the **Proxy Web Server (name or IP address)** field.
3. Type the proxy IP port in the **Proxy Web Server Port** field.
4. To bypass the Proxy Servers if a failure occurs, enable **Bypass Proxy Servers Upon Proxy Server Failure**. This option allows clients behind the appliance to bypass the Web proxy server in the event it becomes unavailable. Instead, the client's browser accesses the Internet directly as if a Web proxy server is not specified.
5. To force clients on public zones to use the proxy server as well, enable **Forward Public Zone Client Requests to Proxy Server**.
6. Click **Accept**.

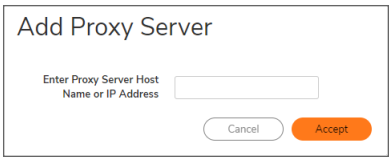
After the appliance has been updated, a message confirming the update displays.

Confirm the Description and Schedule.

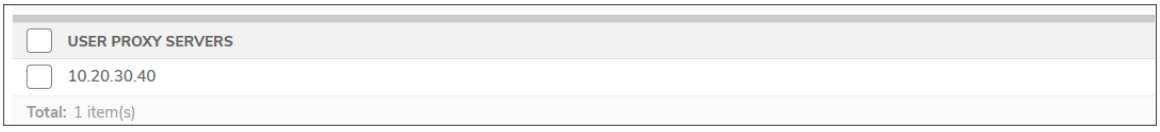
Adding User Proxy Servers

To add a Web Proxy server through which users' web request might come:

1. Navigate to the **NETWORK | System > Web Proxy** page.
2. In the **User Proxy Servers** tab, click **+ Add**. The **Add Proxy Server** dialog displays.



3. Enter a proxy server host name or IP address in the **Enter Proxy Server Host Name or IP Address** field.
4. Click **Accept**. The new proxy server populates in the **User Proxy Servers** table.

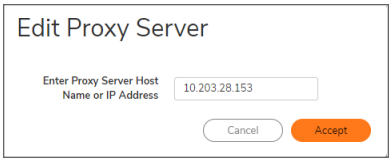


5. Click **Accept**.

Editing User Proxy Servers

To edit a Web Proxy server:

1. Navigate to the **NETWORK | System > Web Proxy** page.
2. In the **User Proxy Servers** table, select the proxy server to change and hover over the **Edit this entry** icon.
3. Click **Edit this entry**. The **Edit Proxy Server** dialog displays.



4. Make the change to the **Enter Proxy Server Host Name or IP Address** field.
5. Click **Accept**. The changed proxy server populates in the **User Proxy Servers** table.

Deleting User Proxy Servers

To delete a Web Proxy server:

1. Navigate to the **NETWORK | System > Web Proxy** page.
2. In the **User Proxy Servers** table, select the proxy server to delete and hover over the **Delete this entry** icon.
3. Click **Delete this entry**.
4. Click **OK**.

To delete all of the Web Proxy servers:

1. Navigate to the **NETWORK | System > Web Proxy** page.
2. Under the **User Proxy Servers** table, click the top left checkbox in the header. All user proxy servers are selected. **Delete all selected entries**.
3. Click **OK**.

8

PortShield Groups

A PortShield interface is a virtual interface with a set of ports, including ports on Dell Networking X-Series, or extended switches assigned to it. PortShield architecture enables you to configure some or all of the LAN ports into separate security contexts, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each context has its own wire-speed PortShield that enjoys the protection of a dedicated, deep packet inspection firewall. On the **NETWORK | System > PortShield Groups** page, you can manually group ports together that allow them to share a common network subnet as well as common zone settings.

TIP: Zones can always be applied to multiple interfaces in the **NETWORK | System > Interfaces** page, even without the use of PortShield groupings. These interfaces, however, do not share the same network subnet unless they are grouped using PortShield.

You can assign any combination of ports to a PortShield interface. All ports not assigned to a PortShield interface are assigned to the LAN interface.

NOTE: TZ series firewalls support Dell Networking X-Series switches and the Dell Networking X-Series Solution, which expand the capability of the firewalls, especially for portshielding interfaces. See *Configuring PortShield Interfaces for Dell Networking X-Series Switches*.

NOTE: For information about configuring PortShield interfaces for Dell networking X-Series switches, also see *Configuring PortShield Interfaces for Dell Networking X-Series Switches*.

NETWORK | System > PortShield Groups allows you to manage the assignments of ports to PortShield interfaces through:

- Port Graphics
- Port Configuration
- External Switch Configuration
- External Switch Diagnostics

SonicOS Support of X-Series Switches

Topics:

About the X-Series Solution

Critical network elements, such as a firewall and switch, need to be managed, usually individually. SonicOS allows unified management of the firewall and the switches using the appliance management interface and GMS.

The maximum number of interfaces available on the SonicWall firewalls varies depending on the model. The feature is supported on all SonicWall firewalls running SonicOS.

In certain deployments, the number of ports required might easily exceed the maximum number of interfaces available on the firewall. With the X-Series Solution, ports on switches are viewed as extended interfaces of the appliance, thereby increasing the number of interfaces available for use up to 192, depending on the switch. These extended ports can be portshielded and/or configured for High Availability (HA) and treated as any other interface on the appliance.

Performance Requirements

A SonicWall appliance can now:

- Be provisioned for a maximum of four switches.
- Manage an increased number of ports.

Key Features Supported with X-Series Switches

NOTE: For more information on these features, refer to the *SonicWall SonicOS X-Series Solution Deployment Guide* located on the Support portal at https://www.sonicwall.com/support/technical-documentation/ and choose **TZ Series** in the **Select A Product** field.

- Provisioning an X-Series switch as an extended switch
- PortShield functionality
- Configuring extended switch Interface settings
- Managing basic extended switch global parameters
- Managing the extended switch using GMS
- High Availability (HA) with PortShield functionality\

  Support for PortShield functionality in HA mode is available using Common Uplink. In this configuration, a link between the active/standby appliance and the switch serves as a common uplink to carry all the PortShield traffic. In this configuration, appliance interfaces that serve as PortShield hosts should be connected to a separate switch and not the same switch connected to the active and standby units. This avoids looping of packets for the same PortShield VLAN. The PortShield members can be connected to ports on the switch that is controlled by the active/standby appliance.
- Diagnostics support for extended switch
- Support for VLANs in a common uplink with SPM configuration
- Support for VLANs in a dedicated uplink configuration
- Single Point of Management over Common Uplink for VLAN Traffic

  VLANs are also supported with Common Uplink. This allows a single link between the appliance and the switch to carry management traffic of the appliance managing the switch plus PortShield traffic for the Interface Disambiguation through VLAN (IDV) VLANs corresponding to the firewall interfaces plus traffic for the VLAN sub-interfaces present under the Common Uplink interface.

  NOTE: Overlapping VLANs cannot exist under firewall interfaces configured as dedicated uplinks or common uplinks to the same switch. This is because the VLAN space is global on the switch.

  NOTE: PortShield of Extended Switch Interfaces to Common Uplink Interfaces without selecting any VLANs for access/trunk configuration is not supported.
- PoE/PoE+ and SFP/SFP+ functionality for appliances by certain X-Series switches.
- Batching configuration messages – To facilitate support of the X-Series switches, configuration messages can be batched before being sent to a switch.

PortShield Functionality and X-Series Switches

PortShield architecture allows configuration of appliance ports into separate security zones, thereby allowing protection of a deep-packet inspection firewall for traffic between devices across zones. For more information about PortShield functionality, see Configuring PortShield Interfaces on NETWORK | System > Interfaces.

The SonicWall X-Series Solution allows support for portshielding interfaces on the extended switch to appliance interfaces. X-Series switches are L2 switches, and by default, all ports on the extended switch are configured as access ports of the default VLAN 1. When ports of the extended switch are portshielded to appliance interfaces, the ports are reconfigured as access ports of the VLAN corresponding to the PortShield VLAN, also known as the IDV VLAN of the PortShield host interface.

Different Traffic Scenarios with PortShield

- Traffic between network devices connected to the ports on the extended switch that are part of the same PortShield group are switched automatically by the extended switch.
- Traffic between network devices connected to the ports on the extended switch and devices connected to ports on the firewall that are part of the same PortShield group are switched by the internal switch on the firewall.
- Traffic between network devices connected to the ports on the extended switch destined to firewall interfaces are handled by the data path in software. Such traffic might be subjected to firewall security services such as access rules, deep packet inspection, and intrusion prevention.
- Traffic between network devices connected to the ports on the extended switch and devices connected to ports on the firewall that are part of a different zone or part of a different PortShield group are forwarded by the data path in software. Such traffic is subjected to firewall security services in software.

Prerequisites for PortShielding X-Series Switches

IMPORTANT: If the topology has two or more switches, the switches can be cascaded or daisy chained, that is, one switch can be connected to another one that is connected to the appliance.

X-Series switches (excluding X1052/X1052P models) are delivered from the factory in unmanaged mode to avoid unauthorized access to the switch. You need to put the switch into Managed mode by pressing Mode, near the power plug, for at least seven seconds.

X1052/X1052P models delivered from the factory are by default in Managed mode.

During the initial set up of the switch, to ensure the X-Series switch's IP does not change dynamically when the DHCP server is enabled on the appliance interfaces, choose Static IP instead of Dynamic IP.

For more information on these features, refer to the *SonicWall SonicOS X-Series Solution Deployment Guide* located on the Support portal at https://www.sonicwall.com/support/technical-documentation/ and select **TZ Series** in the **Select A Product** field.

- Apart from the initial IP address, username/password configuration, which can be found on the switch, no other configuration is recommended to be performed on the X-Series switch directly through the switch's GUI/console. To do so results in the appliance being out-of-sync with the configuration state of the X-Series switch.
- To manage the X-Series switch from the appliance, one of the interfaces of the appliance must be in the same subnet as the X-Series switch. For example, to manage an X-Series switch with a default IP `192.168.2.1`, an interface of the appliance needs to be configured in the `192.168.2.0/24` subnet and connected to the X-Series switch.

- Ensure the appliance can reach the X-Series switch by pinging the X-Series switch from the appliance before provisioning/managing the switch from the appliance.
- VLAN support:
    - Support for VLANs is available on shared and common uplinks. For example, VLANs can be configured under the appliance interface, which is provisioned as the shared uplink for the X-Series switch.
    - For details on VLAN support, refer to the *SonicWall SonicOS X-Series/ Solution Deployment Guide* located on the Support portal at https://www.sonicwall.com/support/technical-documentation/ and select **TZ Series** in the **Select A Product** field. Overlapping VLANs cannot exist under appliance interfaces configured as dedicated uplinks. For example, if X3 and X5 are configured for dedicated uplinks, VLAN 100 cannot be present under both X3 and X5. Such a configuration is rejected.

Dell X-Series Daisy-Chaining Support

The SonicOS X-Series Daisy Chaining solution enables integration of a SonicWall appliance with switches connected in daisy-chained mode. Integration with all Dell switch models is supported in daisy-chain mode.

Daisy-chaining allows those with large facilities, such as warehouses, to deploy two switches more than 1000 ft apart on a given site, to be connected to each other through fiber, to have the first switch—the parent switch—connected to the appliance, and to manage both the switches from the appliance. This deployment also allows you access to an increased number of interfaces on the switch by using a single interface on the appliance. All the interfaces of the parent switch and the child switch are available to be managed from the appliance.

Topics:

Assumptions and Dependencies

- SonicOS switch daisy-chaining solution allows support for single level of chaining only. Multi-level chaining, where more than two switches are connected in series, is not supported. For example, the parent switch can be connected to a child switch, but the child switch cannot be connected to another child switch.
- There is a maximum limitation of four extended switches that can be provisioned. For example, a parent switch can have up to three child switches.
- In daisy-chaining mode, the only supported topology for the child switch is Common Uplink in which the child switch is connected to the parent switch through a single uplink. Other variations, such as dedicated uplinks, isolated links, and so on, are not supported for the child switch.

Daisy-chaining Support

Both switches connected in daisy-chained mode must have the IP address in the same subnet, and the appliance must be able to reach this subnet. Provisioning the switches in daisy-chained mode is a two-step process:

1. Provision the parent switch as a standalone switch.
2. Provision the child switch as a daisy-chained switch.

PoE/PoE+ and SFP/SFP+ Support

SonicWall appliances do not support PoE/PoE+, but this functionality can be added with certain switches, as shown in X-Series switch PoE/PoE+ and SFP/SFP+ support. This additional functionality enhances SonicWave usage by SonicWall appliances, especially for new SonicWaves supporting 802.11ac (supports up to 30W maximum power; 802.11a/b/g/h supports up to 15.4 W maximum power).

Some X-Series switches also support SFP/SFP+, as shown in X-Series switch PoE/PoE+ and SFP/SFP+ support.

Configuration of the PoE/PoE+ ports on the X-Series switch is managed from the UI of the X-Series switch and not through **NETWORK | System > PortShield Groups** on the SonicWall appliance.

This X-Series switch	Supports
X1008	1 PoE PD port; by default, port 8 is the PD port
X1008P	8 PoE ports, up to 123W total; by default, ports 1 through 8 support PoE
X1018	2 1GbE SFP ports; by default, ports 17 and 18 support SFP
X1018P	16 PoE ports, up to 246W total; by default, ports 1 through 16 support PoE 2 1GbE SFP ports; by default, ports 17 and 18 support SFP
X1026	2 1GbE SFP ports; by default, ports 25 and 26 support SFP
X1026P	24 PoE/12 PoE+ ports, up to 369W total; by default: • Ports 1 through 12 support PoE+ • Ports 13 through 24 support PoE 2 1GbE SFP ports; by default, ports 25 and 26 support SFP
X1052	4 10GbE SFP+ ports; by default, ports 49 through 52 support SFP+
X1052P	24 PoE/12 PoE+ ports, up to 369W total; by default: • Ports 1 through 12 support PoE+ • Ports 13 through 24 support PoE • Ports 25 through 48 support neither PoE nor PoE+ 4 10GbE SFP+ ports; by default, ports 49 through 52 support SFP+
X4012	12 10GbE SFP+ ports; by default, ports 1 through 12 support SFP+

IMPORTANT: A SonicWave AC without an external power source must be portshielded through ports 1 through 12 on an X1026P or X1052P X-Series switch.
Any SonicWave non-AC model without an external power source can be portshielded through ports 1 through 8 (X1008P), 1 through 16 (X1018P), or 1 through 24 (X1026P and X1052P).
Any SonicWave with an external power source can be portshielded to any Ethernet port.

X-Series Solution and SonicPoints

Ports on an extended switch can be portshielded to the WLAN zone of the appliance, and SonicPoints can be connected to these ports.

When connecting SonicPoints to an X-Series switch, it is important to consider the SonicPoint's power requirements. A SonicPoint ACe/ACi/N2 requires a minimum of 25.5 watts. If your switch model does not support PoE+, you must use a SonicPoint power injector. For which switches support PoE+, see PoE/PoE+ and SFP/SFP+ Support. For more information about managing SonicPoints, see the Knowledge Base article; *SonicWall TZ Series and SonicWall X-Series Solution managing SonicPoint ACe/ACi/N2 access points*.

Managing Extended Switches using GMS

The switch integration feature allows unified management of both the appliance and the switch using the SonicOS management interface and SonicWall GMS. GMS supports all configuration operations, such as provisioning of an extended switch, configuration of extended switch interface settings, and manageability of extended switch global parameters.

For more information, refer to the GMS administration documentation located on the Support portal. Go to https://www.sonicwall.com/support/technical-documentation/ and select GMS in the **Select A Product** field.

Extended Switch Global Parameters

Extended switch global parameters shows the extended switch global parameters that can be configured through the SonicOS Management Interface.

For more information, refer to the *SonicWall SonicOS X-Series Solution Deployment Guide* located on the Support portal at https://www.sonicwall.com/support/technical-documentation/ and select **TZ Series** in the **Select A Product** field.

EXTENDED SWITCH GLOBAL PARAMETERS

All Switches	Only X1026P and X1052P switches
STP Mode	PoE Alert Usage Threshold
STP State	PoE Traps
	PoE Power Limit Mode

About Links

Management (MGMT) links carry only management traffic and cannot be portshielded.

Data links carry all PortShield traffic. If all they carry are data, the links are called common links. In a few topologies, data links also carry management traffic, in which case they are called shared links.

Shared or common links can carry all the portshielded groups.

Dedicated links can carry only one portshielded group, and that group must be portshielded to the dedicated port on the appliance.

About Uplink Interfaces

Uplink interfaces can be viewed as “trunk” ports set up to carry tagged/untagged traffic. When an extended switch is added with appliance uplink and X-Switch uplink options, the port on the appliance configured as the SuperMassive uplink and the port on the extended switch configured as the switch uplink are set up automatically to receive/send tagged traffic for all IDV VLANs. The IDV VLAN of the tagged traffic allows the firmware to derive the PortShield host interface for the traffic.

Criteria for Configuring an Uplink Interface

- The interface must be a physical interface; virtual interfaces are not allowed.
- The interface must be a switch interface. (On some platforms, some appliance interfaces are not connected to the switch. Such interfaces are not allowed.)
- The interface cannot be a PortShield host (some other appliance interface cannot be portshielded to it) or a PortShield group member (cannot be portshielded to another appliance interface).
- The interface cannot be a bridge primary or bridge secondary interface.
- The interface cannot have any children (it cannot be a parent interface for other child interfaces).

Logging and Syslog Support

Support for logging critical configuration events such as addition/deletion of a switch, configuration of PortShield on an extended switch port, and network events such as port coming up/going down is available.

Supported Topologies

IMPORTANT: Before setting up the interface between the appliance and the switch, learn about provisioning, configuring, and setting up these topologies in the *SonicWall SonicOS X-Series Solution Deployment Guide* found on the Support portal at https://www.sonicwall.com/support/technical-documentation/ by selecting **TZ Series** in the **Select A Product** field.

NOTE: For basic details on configuring PortShield interfaces with X-Series switches, see *Managing Ports*.

The key supported topologies for X-Series switch support are:

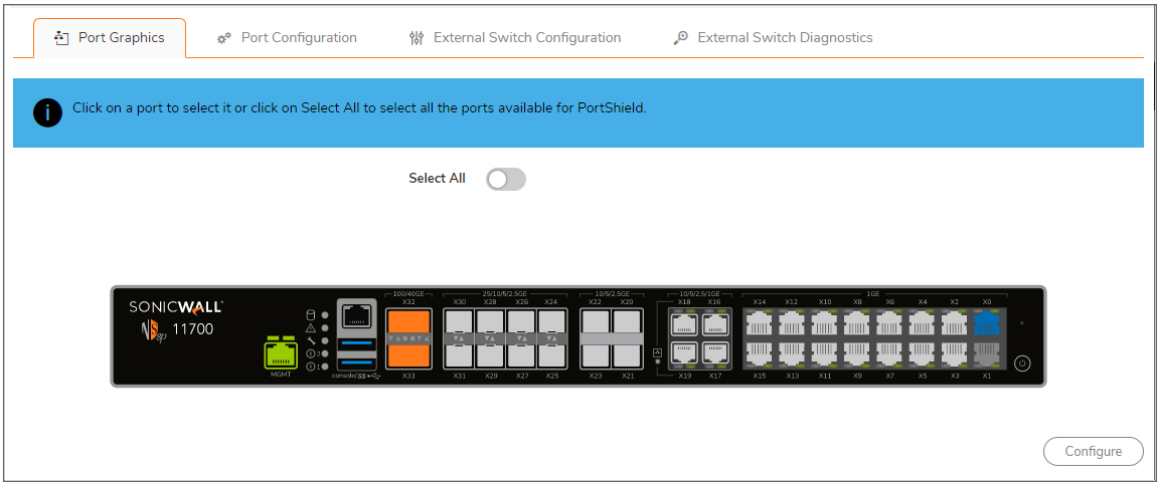
- Common uplink configuration
- Dedicated uplink configuration

NOTE: SonicPoints must be portshielded through the port that is part of the dedicated link.

- Hybrid configuration with common and dedicated uplink(s)
- Shared link configuration for both management and data traffic
- Isolated links for management and data uplinks
- HA and PortShield configurations with dedicated uplink(s)
- HA and PortShield configurations with a common uplink
- VLAN(s) with common uplinks through SPM configuration
- VLAN(s) with dedicated uplink(s) configuration
- Dedicated link for SonicPoint access

Port Graphics

Port Graphics displays the PortShield interfaces (ports) for your appliance. The large graphic represents the appliance's available interfaces. The interfaces are color coded to reflect their configuration:



COLOR CODE FOR INTERFACE CONFIGURATION

This color	Designates this type of interface
Black	Unassigned, that is, not part of a PortShield group.
Orange	Selected to be configured.
Greyed-out	Cannot be assigned, that is, added to a PortShield group.
Grey interfaces with a person graphic	Switch MGMT
Any (other than black, orange, or grey) with an UP arrow	Uplink
Same color (other than black, orange, or grey)	Part of a PortShield group, with the master interface having a white outline around the color.

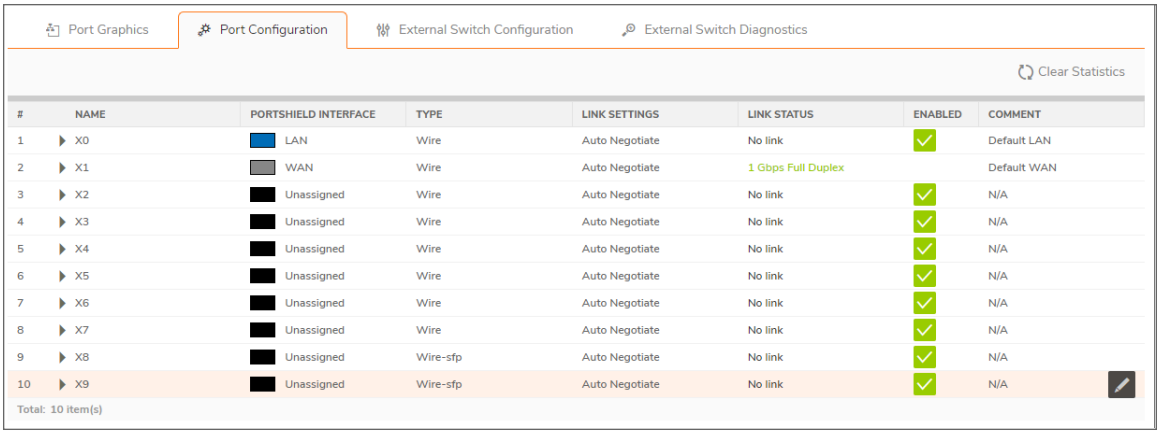
Each port graphic is labeled with its associated port name: X0 - Xn. When you select an interface or interfaces, you can configure them as described in *Configuring PortShield Groups*.

When one or more extended switches are provisioned, **Port Graphics** displays the PortShield interfaces (ports) for both the appliance and the switch(es):

- The first graphic displays the appliance's ports and is not labeled.
- The next graphic displays the ports for the first external switch, External Switch 1, which is labeled **SwitchModel External Switch 1**, for example, X1018P External Switch 1.
- If more external switches are provisioned, subsequent graphics display the ports for the other external switches in order of their ID, that is, External Switch 2, External Switch 3, and External Switch 4.

The color coding for external interfaces is the same as for the appliance; see Color Code for Interface Configuration.

Port Configuration



The Port Configuration table details more information about your PortShield interfaces:

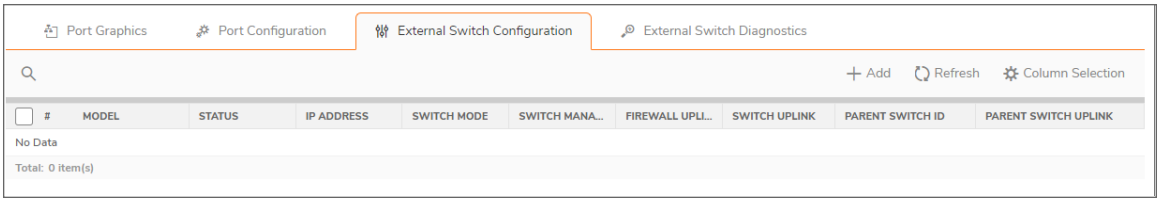
PORT CONFIGURATION TABLE

Name	Port name associated with the PortShield interface, such as X0 or X15. Ports for any external switches are shown in the format **ESs:n**, where ***s*** is the switch ID and ***n*** is the port number, as appropriate.
PortShield Interface	Color-coded graphic reflecting the PortShield interface's assignment and to which PortShield group it belongs. This graphic is a smaller version of the larger graphic(s) on **Port Graphics**.

Link Settings	Link speed: • **Auto Negotiate** • **1000 Mbps – Full Duplex** • **100 Mbps – Full Duplex** • **100 Mbps – Half Duplex** • **10 Mbps – Full Duplex** • **10 Mbps – Half Duplex**
Link Status	Displays either: • The current link speed, in green, for example, **1000 Mbps – Full Duplex**. • **No link**.
Enabled	Enable icon that is: • Green if the interface is enabled. • Dimmed grey if the interface is disabled.
Comment	Any comment entered when the interface was configured.
Configure	Contains one icon: • **Edit** – When clicked, displays the **Edit Switch Port** dialog. For more information about this dialog, see the procedure in *Configuring PortShield Interfaces* on **NETWORK | System > PortShield Groups**.

External Switch Configuration

ⓘ | **NOTE:** This table displays ***No Data*** when external switches have not been provisioned.



EXTERNAL SWITCH CONFIGURATION TABLE

ID #	ID number of the external switch: **1**, **2**, **3**, or **4**.
Model	Model number of the extended switch.

Status	Status of the switch: A green **Enabled** icon indicates the switch is up and available. ⓘ **NOTE:** When an extended switch has been powered off and then the appliance is restarted (rebooted), it might take up to five minutes before the appliance discovers the extended switch and reports the **Status** of the switch as up and available.
IP Address	IP address of the extended switch.
Switch Mode	Mode of the switch, such as **Standalone**.
Switch Management	Switch port used for management traffic.
Firewall Uplink	Port on the appliance configured as the appliance uplink. If no appliance port has been configured as the appliance uplink, the column displays None.
Switch Uplink	Port on the extended switch configured as the switch uplink. If no switch port has been configured as the switch uplink, the column displays **None**.
Parent Switch ID	For daisy-chained switches, the ID of the parent switch. If no switch port has been configured as the parent switch, the column displays **N/A**.
Parent Switch Uplink	Port on a daisy-chained parent switch configured as the switch uplink. If no switch port has been configured as the parent switch uplink, the column displays **N/A**.
Configure	Contains the: • **Edit** icon – Click to display the **Edit External Switch** dialog. • **Delete** icon – Click to delete the switch entry.

External Switch Configuration provides information about the external switches provisioned on the appliance and allows you to manage the switch. You can also configure or delete an extended switch. To configure an extended switch, see PortShield Groups; to delete an extended switch, see the *SonicWallX-Series Solution Deployment Guide*.

External Switch Diagnostics

External Switch Diagnostics allows you to:

- Restart the extended switch(es)
- Monitor statistics for the extended switch(es)
- Upload the firmware image and/or the boot image

External Switch Diagnostics displays statistics and other information about only one switch at a time. By default, the data for External Switch 1, ES1, is displayed. If you have two or more external switches, to display data about a different external switch, choose ES2, ES3, or ES4 from Switch Name.

Switch Information

IMPORTANT: When an extended switch has been powered off and then the appliance is restarted (rebooted), it might take up to five minutes before the appliance discovers the extended switch and reports the Status of the switch as **Connected**.

To restart an external switch:

1. Navigate to **NETWORK | System > PortShield Groups | External Switch Diagnostics**.
2. Select which external switch to restart from **Switch Name**.
3. Click **Restart Selected Switch**.

Statistics

The **Statistics** table displays a running tally of all statistics.

To restart statistics collection:

1. Click **Clear Statistics** to reset the counters.

STATISTICS TABLE

Name	Port name, 1 – n.
Status	Whether the port is Up or Down.
Rx Unicast Packets	Number of Unicast packets received on the port.
Rx Multicast Packets	Number of Multicast packets received on the port.
Rx Broadcast Packets	Number of Broadcast packets received on the port.
Rx Bytes	Number of bytes received on the port.
Rx Errors	Number of packets with errors received on the port.
Tx Unicast Packets	Number of Unicast packets transmitted on the port.
Tx Multicast Packets	Number of Multicast packets transmitted on the port.

Tx Broadcast Packets	Number of Broadcast packets transmitted on the port.
Tx Bytes	Number of bytes transmitted on the port.
FCS Errors	Number of packets with FCS (frame check sequence) errors received on the port.
Single Collision Frames	Number of frame collisions detected on the port.
Late Collisions	Number of frame collisions detected after the last frame bit was sent on the port.
Excessive Collisions	Number of frame collisions detected that exceeded the number of retries on the port.
Internal MAC Transmit Errors	Number of non-collision transmission errors detected on the port.
Oversized packets	Number of received packets larger than the port was expecting.
Rx Pause Frames	Number of pause frames received by the port.
Tx Pause Frames	Number of pause frames sent by the port.

Firmware Management

The **Firmware Management** table displays information about the external switch's firmware and boot code.

FIRMWARE MANAGEMENT TABLE

Type	Either **Firmware** or **Boot Code**.
Version	Version of firmware or boot code on the external switch.
Date Created	Date the firmware or boot code was created.
Time Created	Time the firmware or boot code was created.
Upload	Upload icon; for • **Firmware**, displays the **Upload External Switch Firmware** dialog. • **Boot Code**, displays the **Upload External Switch Boot Code** dialog.

To upload firmware or boot code:

1. Click **Upload** for either **Firmware** or **Boot Code**. The **Upload External Switch Firmware** or **Upload External Switch Boot Code** dialog displays.
2. Click **Browse**. The **File Upload** dialog displays.
3. Select the file.
4. Click **Upload**.

Configuring PortShield Groups

PortShield groups can be configured on several different pages in the SonicOS:

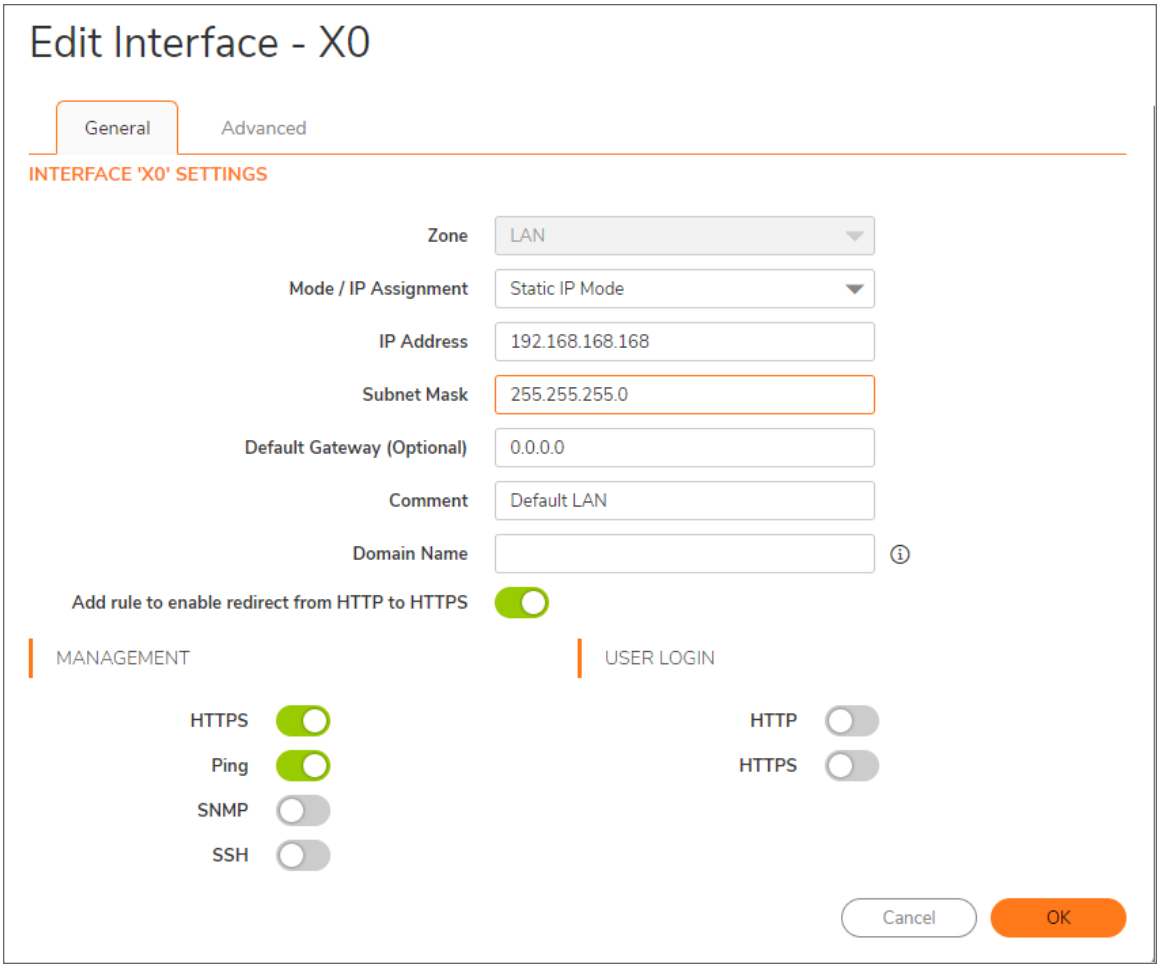
- Configuring PortShield Interfaces on **NETWORK | System > Interfaces**
- Configuring PortShield Interfaces with the PortShield Interface Guide (TZ Series Firewalls Only)
- Configuring PortShield Interfaces on **NETWORK | System > PortShield Groups**
- Configuring External Switch PortShield Groups from Port Graphics

Configuring PortShield Interfaces on NETWORK | System > Interfaces

ⓘ **IMPORTANT:** For a port to be an interface, it must be configured with an IP address. Otherwise, the port is not listed in **PortShield Interface**.

To configure a PortShield interface:

1. Navigate to **NETWORK | System > Interfaces**.
2. In the **Interface Settings** table, click the **Edit this entry** icon for the interface you want to configure. The **Edit Interface** dialog displays.



3. From **Zone**, select on a zone type option to which you want to map the interface. More options display.

ⓘ | **NOTE:** You can add PortShield interfaces only to **Trusted**, **Public**, and **Wireless** zones.

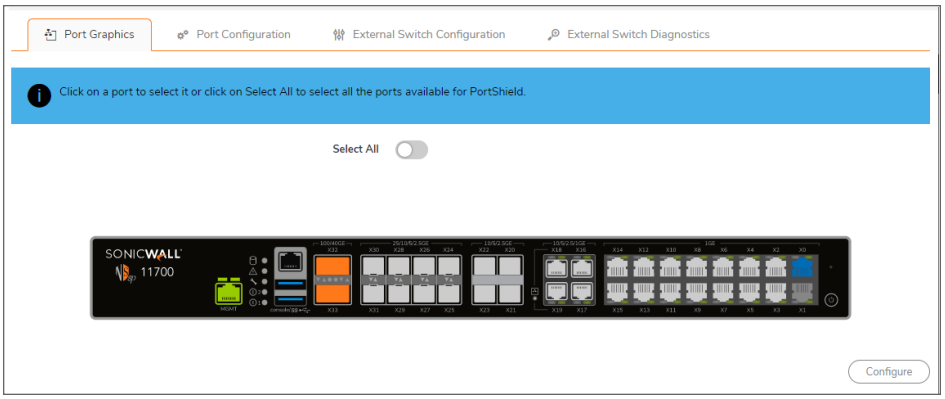
4. In the **Mode / IP Assignment** drop-down menu, select **PortShield Switch Mode**. The options change again.
5. From **PortShield to**, select the interface you want to map this port to. Only ports that match the zone you have selected are displayed.
6. Click **OK**.

Configuring PortShield Interfaces with the PortShield Interface Guide (TZ Series Firewalls Only)

You can configure PortShield interfaces through the *PortShield Interface Guide* as described in the *SonicOS Quick Configuration Guide*. You can access the *PortShield Interface Guide* in these ways:

- Clicking **Quick Configuration Guide** on any Management Interface page. The **Configuration Guide** displays; select **PortShield Interface Guide**.
- On the **NETWORK | System > Interfaces** page on a TZ Series firewall, click **PortShield Wizard** to display the *PortShield Interface Guide*.

Configuring PortShield Interfaces on NETWORK | System > PortShield Groups



Port Graphics displays a graphical representation of the current configuration of PortShield interfaces. For a description of the graphic display, see *Viewing Interfaces (Ports) on Port Graphics*.

You can manually group ports using the graphical PortShield Groups interface by clicking on the ports you want to group. Grouping ports allows them to share a common network subnet as well as common zone settings.

ⓘ | **NOTE:** Interfaces must be configured before being grouped with PortShield.

To configure PortShield groups:

1. In the port graphic, select the interface(s) you want to configure as part of a PortShield group. The interfaces turn yellow.
2. Click **Configure**. The **Edit Switch Port** dialog displays.

   ⓘ | **NOTE:** The name of the interface for this port is dimmed and cannot be changed.
3. From **Port Enable**, select whether you want to enable or disable the interfaces. The default is **Enabled**.
4. From **PortShield Interface**, select which interface you want to assign as the master interface for this PortShield interfaces. The default is **Unassigned**.

   ⓘ | **NOTE:** PortShield options might be disabled for external switch ports.
5. From **Link Speed**, select the link speed for the interfaces:
   - **Auto Negotiate** (default)
   - **1000 Mbps – Full Duplex**

- **100 Mbps – Full Duplex**
- **100 Mbps – Half Duplex**
- **10 Mbps – Full Duplex**
- **10 Mbps – Half Duplex**

6. Click **OK**.

Configuring External Switch PortShield Groups from Port Graphics

IMPORTANT: When an extended switch has been powered off and then the appliance is restarted (rebooted), it might take up to five minutes before the appliance discovers the extended switch and reports the **Status** of the switch as **Connected**.
When configuring extended switches in a PortShield group, it might take up to five minutes for the configuration to be displayed on **NETWORK | System > PortShield Groups**.

IMPORTANT: Interfaces must be configured before being grouped with PortShield.

NOTE: For more information, go to https://www.sonicwall.com/support/technical-documentation/ and search for the *SonicWall SonicOS X-Series Solution Deployment Guide* by selecting NSa Series and TZ Series in the Select A Product field.

NETWORK | System > PortShield Groups displays a graphical representation of the current configuration of PortShield interfaces on both the firewall and the extended (external) switch(es). If there is one external switch, there are two graphics; for two external switches, there are three graphics, and so on. The switch graphics are labeled with the switch model and the external switch ID: 1, 2, 3, 4.

You can manually group ports on the firewall and switches together using the graphical PortShield Groups interface by clicking on the ports you want to group. Grouping ports allows them to share a common network subnet as well as common zone settings.

To configure PortShield groups with external switches:

1. Configure the ports on the appliance by following the procedure in Configuring PortShield Interfaces on **NETWORK | System > PortShield Groups**.
2. In the port graphic for the external switch, select the interface(s) you want to configure as part of the PortShield group. The interfaces turn yellow.
3. Click **Configure**. The **Edit Multiple Switch Ports** dialog displays.

The **Name** field is dimmed and cannot be modified. It displays the names of both the appliance's and external switch's ports you selected (n is the selected port):

- Firewall ports are named **Xn**.
- External switch 1 ports are named **ES1 : n**.
- External switch 2 ports are named **ES2 : n**.

- External switch 3 ports are named **ES3 : n**.
- External switch 4 ports are named **ES4 : n**.

4. From **Port Enable**, select:

- **Disabled**
- **Enabled**
- **—Keep Current Settings—** (default) – By default, all ports on the extended switch are enabled.

5. From **PortShield Interface**, select which interface you want to assign as the master interface for these PortShield interfaces:

- **Unassigned**
- **Port name**

IMPORTANT: For a port to be an interface, it must be configured with an IP address. Otherwise, the port is not listed in PortShield Interface.

- **—Keep Current Settings—** (default)

NOTE: PortShield options could be disabled for external switch ports. Ports that are portshielded here are configured automatically as access VLANs for the corresponding PortShield VLAN.

6. From **Link Speed**, select the link speed for the interfaces:
    - **Auto Negotiate**
    - **1000 Mbps – Full Duplex**
    - **100 Mbps – Full Duplex**
    - **100 Mbps – Half Duplex**
    - **10 Mbps – Full Duplex**
    - **10 Mbps – Half Duplex**
    - **—Keep Current Settings—** (default) – By default, the link speed for all ports on the extended switch are set to **Auto Negotiate**.
7. Click **OK**.

9

PoE Settings

This feature is only available for TZ devices that include PoE support. If your TZ is designed for PoE support, the PoE ports must be enabled individually for powered device (PD) detection and classification.

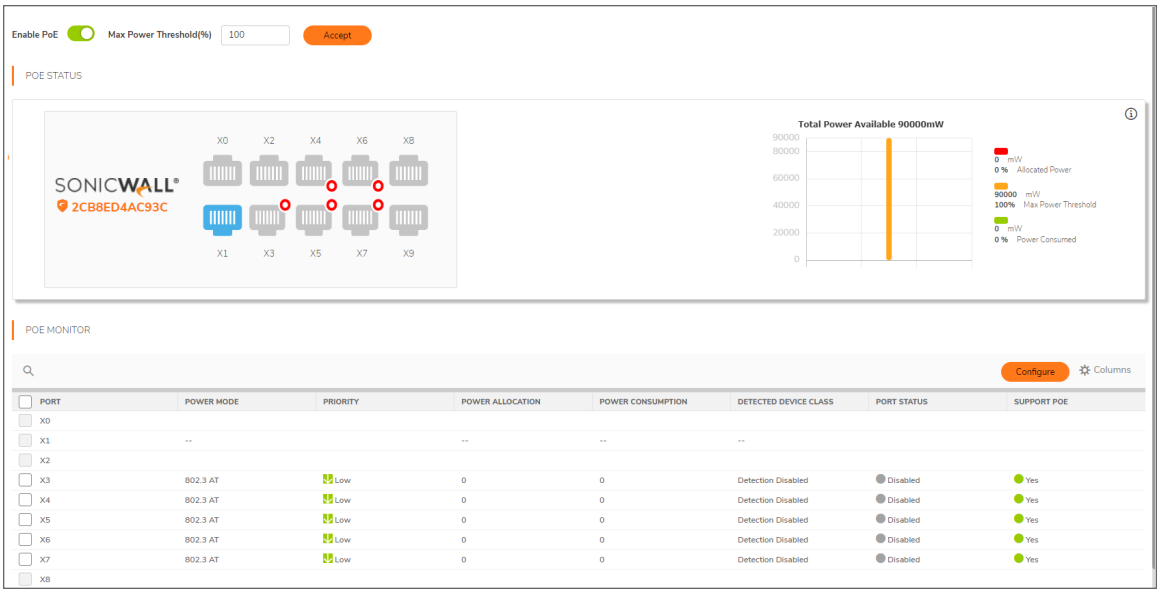
Topics:

Enabling PoE on the Appliance

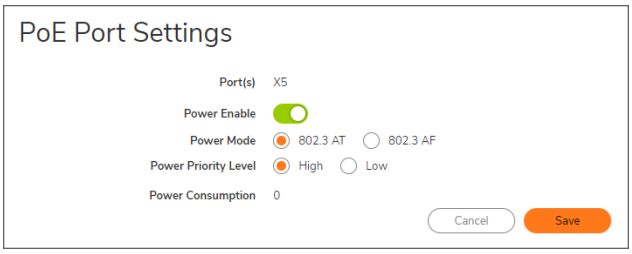
By default, the highest port number has the highest priority in powering on a PD. You can control the supplied power level and port priority from SonicOS.

To enable PoE and configure basic PoE settings:

1. Point your browser to the LAN or WAN IP address and log into the appliance as an administrator (default: admin / password).
2. Navigate to the **NETWORK | System | > PoE Settings** page.
3. Select **Enable PoE**. The display changes:



4. Accept the default of 100 in the **Max Power Threshold** field or type in a number between 1 and 100. This is the percentage of the maximum available power that the PoE controller allocates to the PoE ports on the appliance.
5. Click **Accept**.
6. The **NETWORK | System | > PoE Settings** page displays an interactive graphical representation of the PoE port status under **PoE Status**, with the PoE Monitor table showing the per port Power Mode (802.3 AT or 802.3 AF), Power Allocation, and Power Consumption.
7. To enable PoE power on a specific port, click the port image or checkbox of the port then click either **Configure** above the PoE Monitor table, or the **Edit** icon in the PoE Monitor table row for that port. The **Poe Port Settings** dialog displays the **Power Enable** option along with other options.



8. Select **Power Enable**, then set the desired options and click **Save**.
9. **Power Mode** – Changes to this option do not take effect unless a PoE device is connected to that port. The TZ detects the mode from the device, but you can change the mode here. For example, if the **Power Mode** is detected as 802.3 AT, you can change it to 802.3 AF if you know that the device requires a lower power level.
10. **Power Priority Level** – By default, this option is set to **Low** for all PoE ports and the highest numbered PoE port has the highest priority for power as distributed by the PoE controller. Set this option to **High** on a lower numbered port to give it a higher priority.

11. If the **Power Mode** is detected as 802.3 AT and then changed to 802.3 AF, the PoE device shuts down if its power consumption spikes above the 802.3 AF power budget for that port. Similarly, reducing the Max Power Threshold so that not all PoE ports have some power prevents devices connected to the lower priority ports from powering on.
12. Repeat Step 7 and Step 8 to enable PoE power on other ports, as needed.
13. The **PoE Status** display shows blue for the PoE port when an 802.3 AT device is connected. A green port is displayed when an 802.3 AF device is connected.

10

VLAN Translation

Topics:

The VLAN Translation (mapping) feature allows traffic arriving on a VLAN to a Wire Mode interface operating in Secure mode to be mapped to a different VLAN on the outgoing paired interface. Re-routing some of the traffic coming into the appliance onto different VLANS allows you to perform further analysis, processing, or merely remapping traffic. This feature is supported on all Wire Mode-capable devices.

An advantage of Wire Mode, is that you can preprovision the VLAN mapping. This allows you to have the mapping in place before the interface receives traffic. You also can add and delete mapping on an active Wire Mode interface.

ⓘ | **NOTE:** VLAN Translation is available on all platforms that support Wire Mode.

ⓘ | **NOTE:** VLAN Translation and Wire Mode over VLAN interfaces cannot be enabled at the same time.

Mapping Modes

You can create a VLAN mapping in these modes:

- **Unidirectional mapping** – For example, use to:
  - Secure printing from a less-secure network to a high-secure network
  - Transfer application and operating system updates from a less-secure network to a high-secure network
  - Monitor multiple networks in a SOC (security operations center)
  - Provide time synchronization in high-secure networks
  - Transfer files
  - Provide a “you have mail” alert to a high-secure network from a less-secure network

- **Bidirectional mapping** – For example, use to setup a two-way connection to and from devices through the appliance, for example, TCP.

Mapping Persistence

The VLAN map created for a pair of interfaces is persistent over reload and is stored as part of the configuration. If the wire-mode pair (secure mode) have mapping associated with them, the wire mode cannot be changed unless the mapping policy is deleted.

Map Multiple Interface Pairs

You can create VLAN mapping for multiple pairs of interfaces at the same time. These interfaces must form part of an existing Secure Wire Mode pair at the time of the VLAN mapping creation. You can also create mappings for an interface with multiple interfaces, but only the mappings for the current active Wire Mode pair are in use at any given time.

If the paired interface is changed, the message, `Cannot change wire-mode pair interface when WireMode VLAN entries exist for the interface`, displays.

Example

MULTIPLE INTERFACE PAIRS MAPPING

In Multiple interface pairs mapping, a mapping exists for X12 to X13 (policy 1) as well as X12 to X15 (policy 2).

As only X12 and X13 (policies 1 and 3) and X14 and X15 (policies 4 and 6) are currently forming a Wire Mode pair, only policies 1, 3, 4, and 6 are active as indicated by the green checkmark in the active column.

ⓘ | **NOTE:** The wire-mode pair interfaces cannot change if Wire Mode VLAN entries exist for the interface.

Creating and Managing VLAN Maps

Topics:

NETWORK | System > VLAN Translation allows you to create and manage the VLAN mapping of interfaces.

+Add	Displays the **Add VLAN Translation** dialog.

Delete icon	Displays the **Delete** drop-down menu: • **Delete Selected** • **Delete All**
Search field	Allows you to display only those VLAN translations of interest.
Refresh icon	Refreshes the VLAN Translation table.
Policy number and checkbox	Number of the policy and its associated checkbox.
Ingress Interface	Name of the incoming interface.
Ingress VLAN	VLAN tag of the incoming interface.
Egress Interface	Name of the interface to which traffic is mapped.
Egress VLAN	VLAN tag of the interface to which traffic is mapped.
Reverse Translation	Indicates whether the mapping is unidirectional or bidirectional: • **Disabled** – Unidirectional; column blank. • **Enabled** – Bidirectional; green checkmark.
Active	Status of the mapped pair: • **Active** – The Wire Mode pair is mapped and active; green checkmark. • **Inactive** – The Wire Mode pair is mapped but not active (pre-provisioned); column blank.
Configure	Displays **Edit** and **Delete** icons for a mapped pair.

Creating a VLAN Map

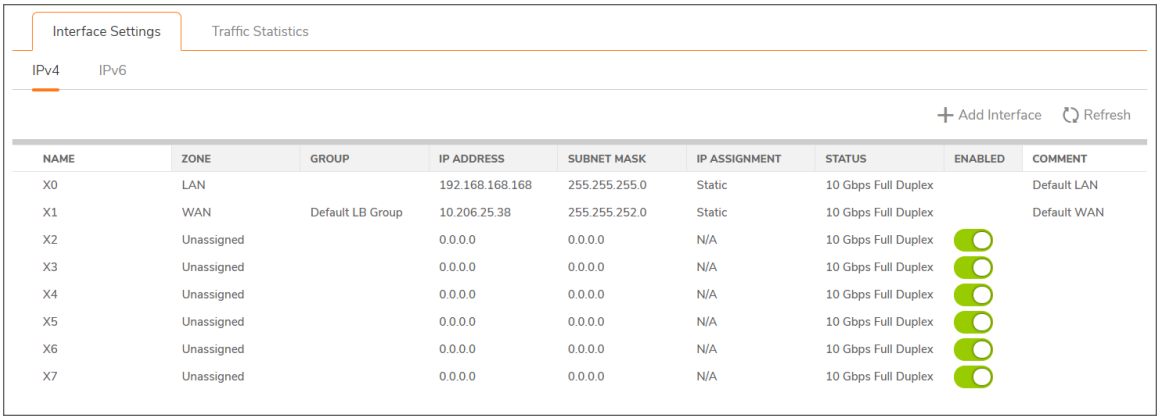
You can create a unidirectional VLAN map before or after a Wire Mode pair. Creating a VLAN map is a two-step process:

1. Creating a Wire Mode Pair in Secure Mode
2. Creating the VLAN Mapping

Creating a Wire Mode Pair in Secure Mode

To create a Wire Mode pair in secure mode:

1. Navigate to **NETWORK | System > Interfaces**.



2. Click the **Edit** icon for the interface to be part of the Wire Mode pair. The **Edit Interface** dialog displays.
3. Select the zone for the Wire Mode pair from **Zone**. The options change.
4. Select **Wire Mode (2-Port Wire)** from **Mode / IP Assignment**. The options change again.
5. Select **Secure (Active DPI of Inline Traffic)** from **Wire Mode Type**.
6. Select the interface to pair with the current interface from the **Paired Interface** drop-down menu.

   ⓘ | **TIP:** Ensure the interface you pair with is unassigned.
7. Select the zone for the paired interface from **Paired Interface Zone**. The default is **LAN**.
8. Configure the other options as if configuring a regular Wire Mode pair as described in Configuring Wire and Tap Mode.
9. Click **OK**. The **NETWORK | System > Interfaces** page is updated.

Creating the VLAN Mapping

To create a VLAN mapping:

1. Navigate to **NETWORK | System > VLAN Translation**.
2. Click **+Add**. The **Add VLAN Translation** dialog displays.
3. Select the Wire Mode interface in the pair on which you expect to receive traffic from **Ingress Interface**.
4. Set **Ingress VLAN** to the VLAN on which you expect to receive traffic for mapping.
5. Select the Wire Mode interface in the pair on which you want to map traffic to the **Egress Interface** drop-down menu.
6. Set **Egress VLAN** to the VLAN to which you expect to map traffic.
7. To create a:

- Unidirectional mapping, ensure **Reverse Translation** is not selected. For example, to map VLAN X on interface A to VLAN Y on interface B.

  ⓘ | **NOTE:** This option is selected by default.

- Bidirectional mapping, select **Reverse Translation**. For example, to map VLAN Y on interface B to VLAN X on interface A as well as map VLAN X on interface A to VLAN Y on interface B.

8. Click **Add**. The **Wiremode VLAN Translation** table is updated.

Managing VLAN Mappings

Topics:

Editing Mappings

To edit a mapping, click its **Edit** icon in the **Configuration** column. The **Edit VLAN Translation** dialog displays. You can change any of the mappings except the **Reverse Translation** setting.

Filtering Mappings

If you have a lot of VLAN mappings, you can display only those of interest by:

1. Entering an interface name or VLAN tag in the **Search** field.
2. Pressing **Enter**.

Only those mappings meeting the search criterion are displayed.

To redisplay all the mappings:

1. Delete the criterion from the **Search** field.
2. Press **Enter**.

Deleting Mappings

To delete mappings:

1. To delete:
   A single mapping by:
   - Clicking its **Delete** icon in the **Configuration** column.

     A confirmation message displays.
   - Clicking its **Selection** checkbox and then selecting **Delete Selected** from the **Delete** drop-down menu.

A confirmation message displays.

- Multiple mappings by clicking their **Selection** checkboxes and then selecting **Delete Selected** from the **Delete** drop-down menu.

  A confirmation message displays.

- All mappings by selecting **Delete Selected** from the **Delete All** drop-down menu.

  A confirmation message displays:

2. Click **OK**.

If a policy is bidirectional, then both directions are deleted if one is deleted.

11

IP Helper

Topics:

Using IP Helper

Topics:

About IP Helper

ⓘ | **IMPORTANT:** IP Helper is not supported for WAN interfaces or for interfaces that are configured for NAT.

Many User Datagram Protocols (UDP) rely on broadcast/multicast to find its respective server, usually requiring their servers to be present on the same broadcast subnet. To support cases where servers lie on different subnets than clients, a mechanism is needed to forward these UDP broadcasts/multicasts to those subnets. This mechanism is referred to as UDP broadcast forwarding. IP Helper helps broadcast/multicast packets to cross an

appliance's interface and be forwarded to other interfaces based on policy. IP Helper allows the appliance to forward DHCP requests originating from its interfaces to a centralized DHCP server.

IP Helper supports user-defined protocols and extended policies. IP Helper provides better control on existing NetBIOS/DHCP relay applications. Some of the built-in applications that have been extended are:

EXTENDED BUILT-IN RELAY APPLICATIONS

Protocol	UDP Port Number
DHCP	67/68
DHCPv6	546, 547
Net-Bios NS	137
Net-Bios Datagram	138
DNS	53
Time Service	37
Wake on LAN (WOL)	
mDNS	5353 Multicast address: `224.0.0.251`

VPN Tunnel Interface Support for IP Helper

The VPN Tunnel Interface can support IP Helper. DHCP Replay in IP Helper with Tunnel Interface Support shows a simple example of DHCP replay in IP Helper:

- PC is the device needed to get an IPv4 address from the DHCP protocol.
- GatewayA is the gateway-enabled IP helper.
- GatewayB is the gateway with a DHCP server.

DHCP REPLAY IN IP HELPER WITH TUNNEL INTERFACE SUPPORT

To configure IP Helper with a VPN Tunnel Interface:

NOTE: The numbers in DHCP Replay in IP Helper with Tunnel Interface support correspond to the numbered tasks.

1. In PC:
    a. Connect to the LAN (X0) subnet of GatewayA.
    b. Set to obtain an IP address through DHCP mode.

2. Set up a VPN tunnel between GatewayA and GatewayB.
    a. Add a VPN Tunnel Interface.
3. In Gateway B:
    a. Add a route entry from the Tunnel Interface's IP address to GatewayA's X0 interface.
    b. Add the outbound interface of the Tunnel Interface.
    c. Add an IP address range as the DHCP scope for PC.
4. In Gateway A:
    a. Enable IP Helper.
    b. Add an IP Helper DHCP relay protocol from X0 to GatewayB's Tunnel Interface address. The protocol is DHCP.

DHCPv6 Relay

Topics:

About DHCPv6 Relay

SonicOS supports DHCPv6 Relay. A DHCP relay agent is a node that acts as an intermediary to deliver DHCP messages between clients and server, and is on the same link as the client. A DHCPv6 relay agent is used to relay messages between the client and the server when they are not on the same IPv6 link. The DHCPv6 relay agent operation is transparent to the client.

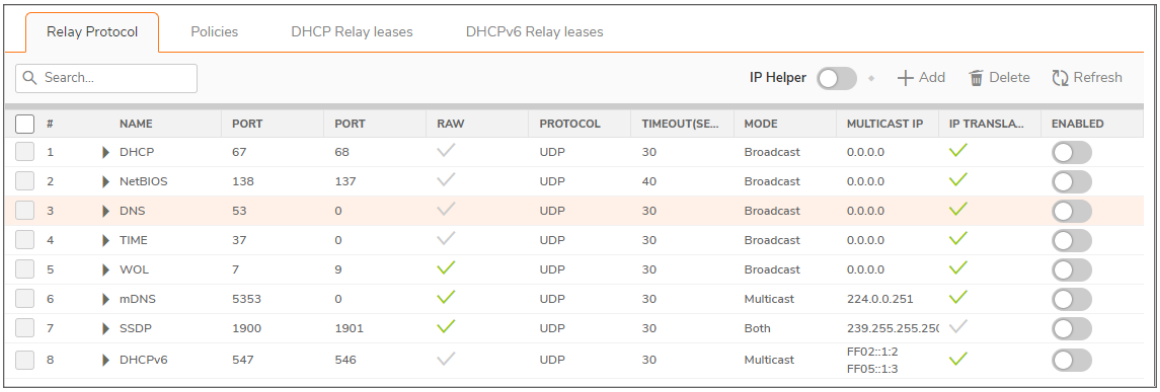
In SonicOS, supported destination addresses can be global addresses or link-local addresses, but not multicast addresses.

DHCPv6 relay can be enabled on both physical and virtual interfaces. DHCPv6 is a built-in application in IP Helper protocols.

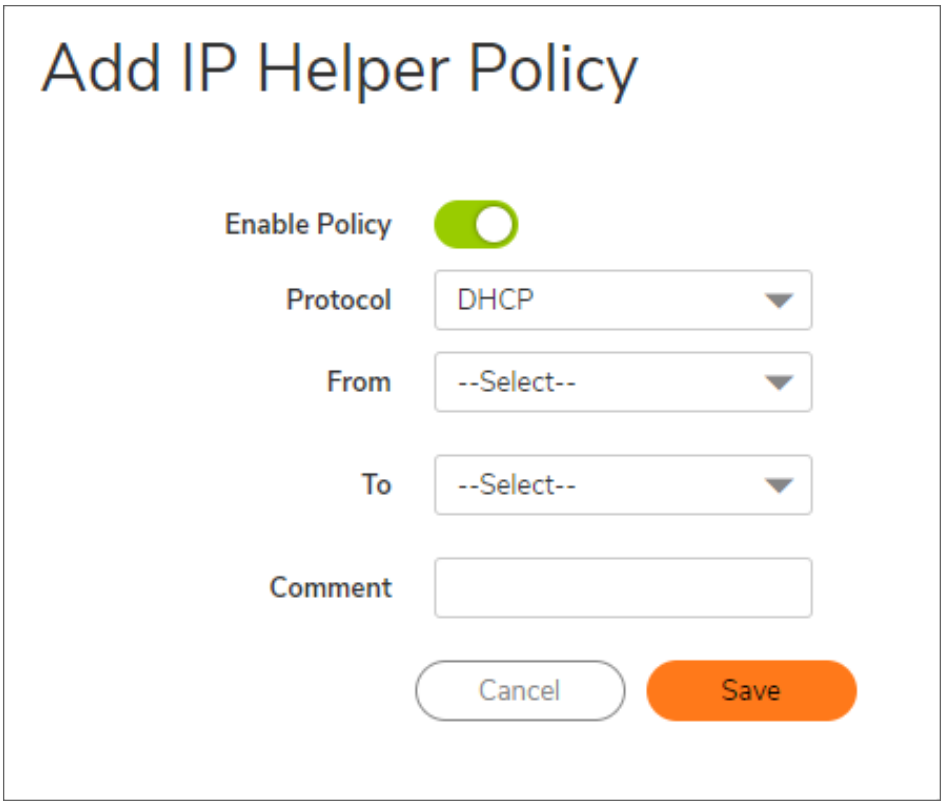
Configuring DHCPv6 Relay

To configure DHCPv6 Relay:

1. Navigate to the **NETWORK | System > IP Helper** page.



2. Click the **Policies** view.
3. Click **+Add**. The **Add IP Helper Policy** dialog displays.

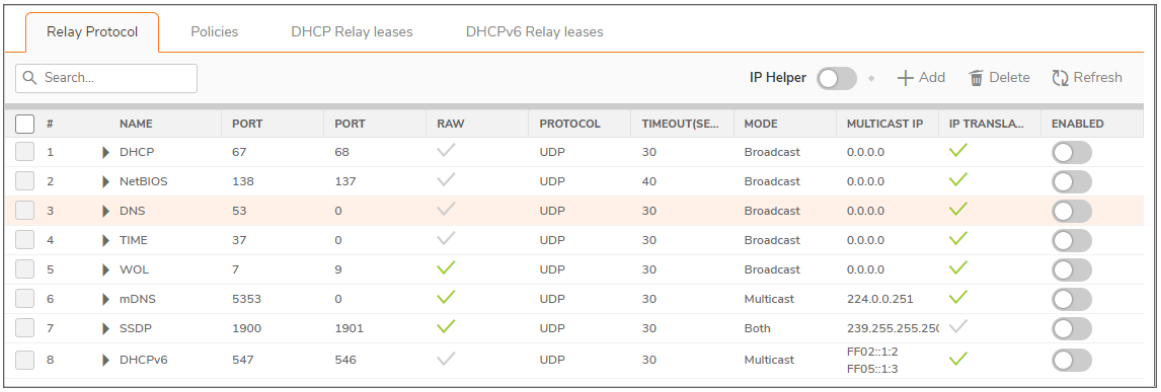


4. Select **DHCPv6** from **Protocol**.
5. Select the desired interface from **From**.
6. In the **To** field, type in the destination IPv6 address. This can be a list of destination addresses, which might include unicast addresses, or other addresses you select. The address cannot be a multicast address.

7. If the destination in the **To** field is a:
    - Global address, there is no need to select an egress interface. Go to Step 8.
    - Link-local address, select an egress interface from **Egress Interface**.
8. Click **Save**.

    A new DHCP lease appears in the **DHCPv6 Relay Leases** section of the page when the client gets a new IP address from the server.

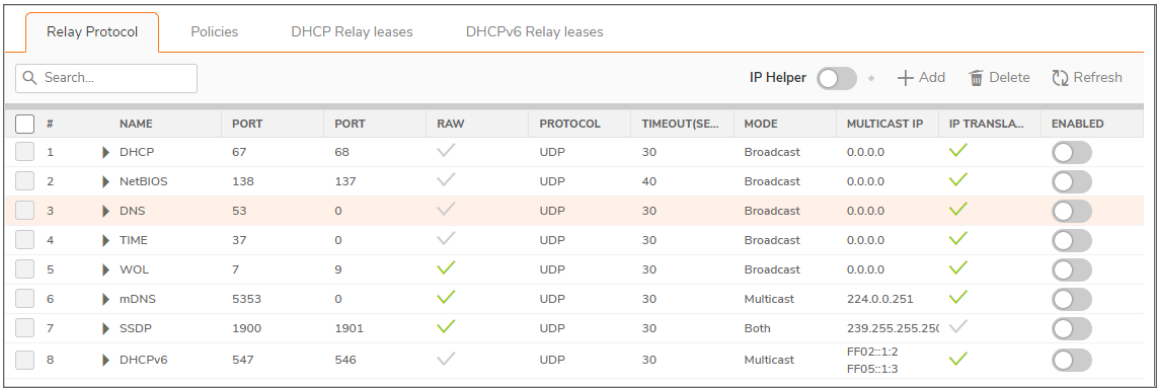
IP Helper Settings



Topics:

- Relay Protocols
- Policies
- DHCP/DHCPv6 Relay Leases

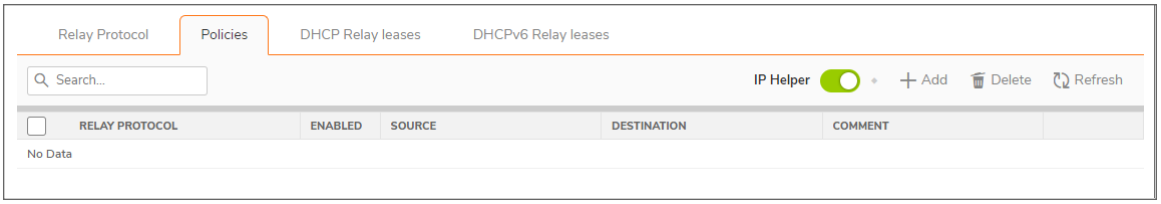
Relay Protocols



Name	IP Helper application name.

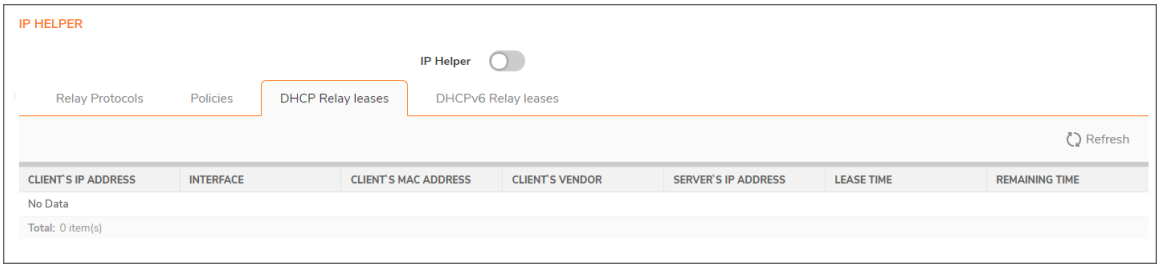
Port	First UDP port number for the IP Helper application.
Port	Optional second UDP port number for the IP Helper application.
Raw	Indicates whether raw mode was selected when the IP Helper application was configured. Timeout is ignored if this option is enabled.
Protocol	UDP.
Timeout (secs)	Timeout for the IP Helper cache. **N/A** indicates Raw mode is selected and the timeout is ignored.
Mode	Indicates the mode the protocol supports: • **Broadcast** • **Multicast** • **Both**
Multicast IP	Multicast IP the protocol uses.
IP Translation	Indicates whether the source IP address is translated when packets are forwarded by an IP Helper policy.
Enable	Indicates whether the IP Helper policy is enabled.
Configure	Contains the **Statistics**, **Edit**, and **Delete** icons for the entries. ⓘ | **NOTE:** Only user-generated Relay protocols can be deleted.

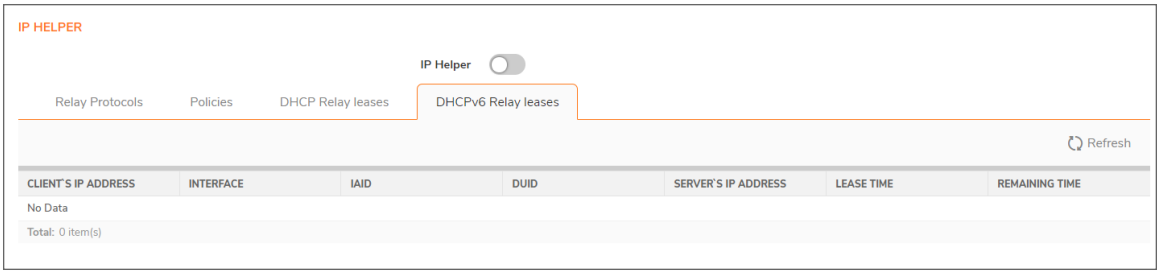
Policies



Relay Protocol	Protocol for the policy.
Enable	Indicates whether the IP Helper policy is enabled.
Source	Interface or zone for the policy.
Destination	Network destination.
Comment	Comment entered when the policy was configured.
Configure	Contains the **Edit** and **Delete** icons for each entry.

DHCP/DHCPv6 Relay Leases





Client's IP Address	IP address of the client device.
Interface	Receiving interface on the appliance.
DHCP Relay Leases:	
• **Client's MAC Address**	MAC address of the client device.
• **Client's Vendor**	Manufacturer of the client device.
DHCPv6 Relay Leases:	
• **IAID**	Interface ID; an Interface Association Identifier that is a binding between the interface and one or several IP addresses.
• **DUID**	Device (host) ID; a DHCP Unique Identifier for a DHCP participant.
Server's IP Address	IP address of the DHCP server.
Lease Time	Time of the relay lease.
Remaining Time	Time remaining on the relay lease.

To refresh the DHCP Relay Leases table:

1. Click **Refresh**.

Configuring IP Helper

Topics:

Enabling IP Helper

To activate IP Helper features:

1. Navigate to **NETWORK | System > IP Helper**.
2. Select enable **IP Helper**in the top banner.

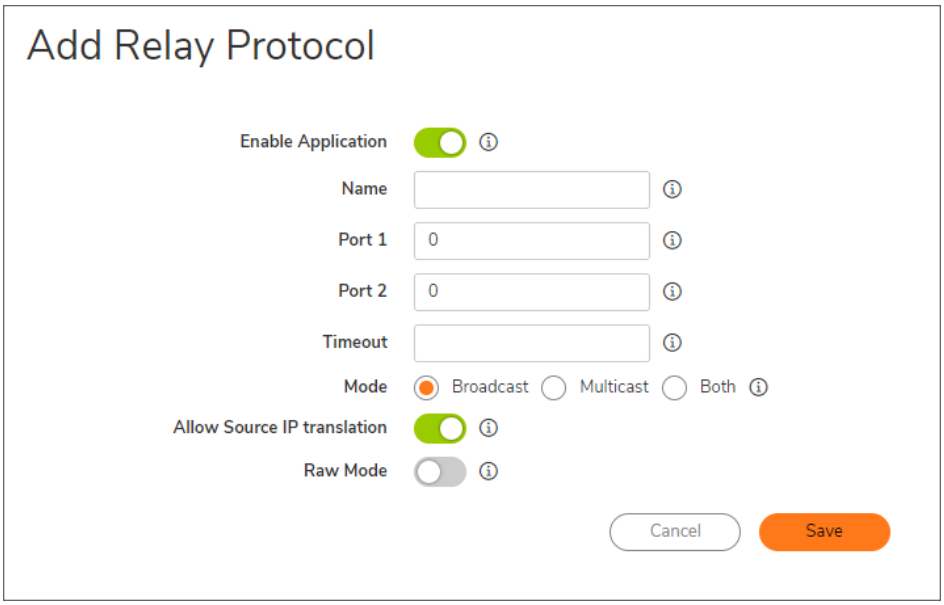
Managing Relay Protocols

Topics:

Adding User-Defined Relay Protocols

To add a relay protocol:

1. Navigate to **NETWORK | System > IP Helper**.
2. Click **+Add** in the **Relay Protocols** view. The **Add Relay Protocol** dialog displays.



3. Enable the IP Helper application by selecting **Enable Application**.
   ⓘ | **NOTE:** If this option is disabled, all IP Helper cache is deleted.
4. Enter a unique, case-sensitive name for the IP Helper application in the **Name** field.
5. In the **Port 1** field, specify a unique UDP port number for the application.
6. Optionally, in the **Port 2** field, specify a second unique UDP port number for the application.
7. Optionally, specify the IP Helper cache timeout, in seconds, in an increment of 10 from 10 to 60, in the **Timeout** field. If a timeout is not specified, a default value of **30** seconds is selected.
   ⓘ | **TIP:** This field is ignored if **Raw Mode** is selected.
8. Choose a **Mode** to specify whether this protocol supports:
   - **Broadcast**
   - **Multicast**
   - **Both**
9. If you selected **Multicast** or **Both** for **Mode**, specify a valid multicast IP that this protocol is used in the **Multicast IP** field.
10. To allow the source IP address to be translated when a packet is forwarded by an IP Helper policy, select **Allow Source IP Translation**. This option is selected by default.

11. To prevent a cache from being created when a packet is forwarded by an IP Helper policy, select **Raw Mode**. Unidirectional forwarding is supported. This option is not selected by default.

    ⓘ | **NOTE:** Any time set in the **Timeout** field is ignored.

12. Click **Save**.

Deleting Custom Protocols

To delete a custom protocol:

1. Navigate to **NETWORK | System > IP Helper**.
2. Select the **Delete** icon for that protocol.

To delete one or more custom relay protocols:

1. Navigate to **NETWORK | System > IP Helper**.
2. Select the left-most checkbox(es) (by the protocol name) of the desired protocol(s). **Delete** becomes available.
3. Click **Delete**.

To delete all custom relay protocols:

1. Navigate to **NETWORK | System > IP Helper**.
2. Select the checkbox in the **Relay Protocols** table header. **Delete**becomes available.
3. Click **Delete**.

Managing IP Helper Policies

IP Helper policies allow you to forward DHCP and NetBIOS broadcasts from one interface to another interface.

ⓘ | **IMPORTANT:** IP Helper is not supported for WAN interfaces or for interfaces that are configured for NAT.

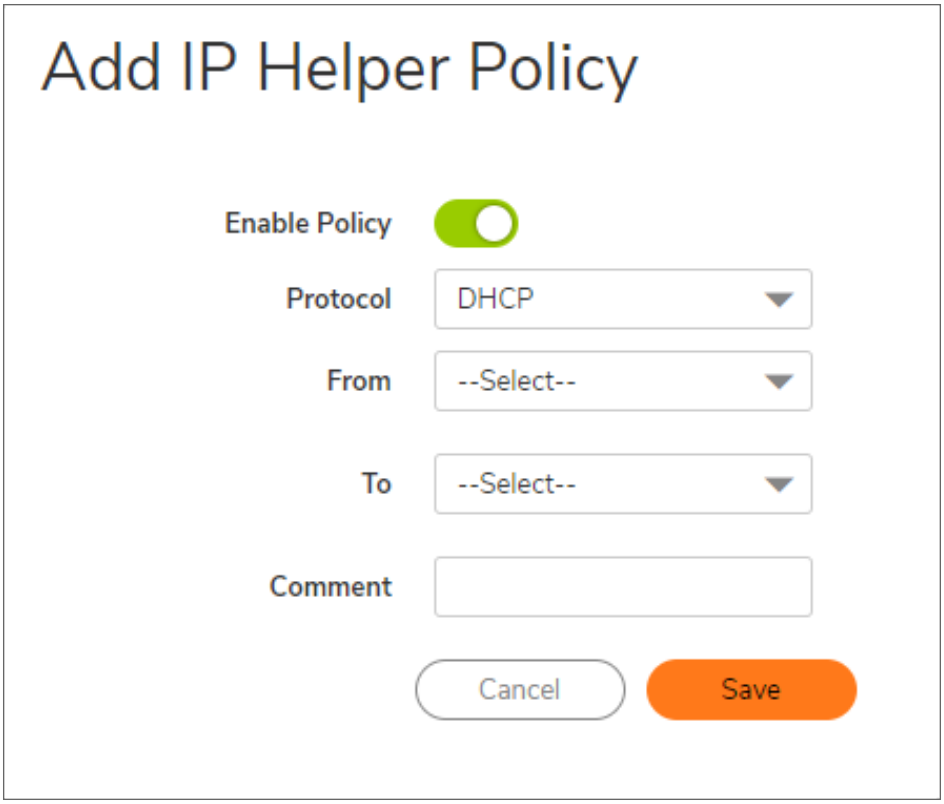
Topics:

Adding an IP Helper Policy

You can add up to 256 policies.

To add an IP Helper policy:

1. Navigate to **NETWORK | System > IP Helper | Policies**.
2. Click **+Add**. The **Add IP Helper Policy** dialog displays.



3. The policy is enabled by default. To configure the policy without enabling it, disable **Enable Policy**.
4. Select a protocol from the **Protocol** menu. The default is **DHCP**.
5. Select a source interface or zone from **From**.
6. From **To**, select either:
   - A destination Address Group or Address Object.
   - **Create New Network** to create a new Address Object. The **Add Address Object** dialog displays.
7. Enter an optional comment in the **Comment** field.
8. Click **Save**.

Editing an IP Helper Policy

To edit an IP Helper policy:

1. Navigate to **NETWORK | System > IP Helper**.
2. Click the **Edit** icon in the **Configure** column of the entry in the **IP Helper Policies** table. The **Edit IP Helper Policy** dialog displays.
3. The settings are the same as the **Add IP Policy** dialog. For information about the dialog, see Adding an IP Helper Policy.

Deleting IP Helper Policies

To delete a custom policy:

1. Navigate to **NETWORK | System > IP Helper**.
2. Select the **Delete** icon in the **Policies** table for that policy.

To delete one or more custom policies:

1. Navigate to **NETWORK | System > IP Helper**.
2. Select the left-most checkbox(es) (by the relay protocol) of the desired policies. **Delete** becomes available.
3. Click **Delete**.

To delete all custom policies:

1. Navigate to **NETWORK | System > IP Helper**.
2. Select the checkbox in the **Policies** table header. **Delete** becomes available.
3. Click **Delete**.

Filtering which DHCP Relay Leases are Displayed

You can display only a specific device(s) in the **Anti-Spoof Cache** and **Spoof Detected List** tables by using the **Filter** function.

To filter the table display:

1. Navigate to **NETWORK | System > MAC-IP Anti-Spoof**.
2. In the **Filter** field below the table to be filtered, specify either the device's IP address, interface, MAC address, host name, or name. The field must be filled using the appropriate syntax for operators shown in Filter Operator Syntax Options.

FILTER OPERATOR SYNTAX OPTIONS

Operator	Syntax Options
Value with a type	• Ip=1.1.1.1 or ip=1.1.1.0/24 • Mac=00:01:02:03:04:05 • Iface=x1
String	• X1 • 00:01 • Tst-mc • 1.1.
AND	Ip=1.1.1.1;iface=x1 Ip=1.1.1.0/24;iface=x1;just-string
OR	Ip=1.1.1.1,2.2.2.2,3.3.3.0/24 Iface=x1,x2,x3
Negative	!ip=1.1.1.1;!just-string !iface=x1,x2
Mixed	Ip=1.1.1.1,2.2.2.2;mac=00:01:02:03:04:05; just-string;!iface=x1,x2

Displaying IP Helper Cache from TSR

The TSR shows all the IP Helper caches, current policies, and protocols:

```
#IP_HELPER_START
IP Helper
-----IP Helper Global Run-time Data-------
IP Helper is OFF
IP Helper - DHCP Relay is OFF
IP Helper - Netbios Relay is OFF
Total Number Of Fwded Packets :0
Total Number Of Dropped Packets :0
Total Number Of Passed Packets :0
Total Number Of Unknown Packets :0
Total Number Of record create failure :0
Total Number Of element create failure :0User-defined
-----IP Helper Applications -------
Name: DHCP
Port: 67, 68, Max Record: 4000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 8000, Timeout: 3, index: 1, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: NetBIOS
Port: 138, 137, Max Record: 4000, Status: OFF
```

```
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 8000, Timeout: 4, index: 2, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: DNS
Port: 53, 0, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 16000, Timeout: 3, index: 3, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: TIME
Port: 37, 0, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 16000, Timeout: 3, index: 4, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: WOL
Port: 7, 9, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: YES
Max Element: 16000, Timeout: 3, index: 5, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: mDNS
Port: 5353, 0, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: YES
Max Element: 16000, Timeout: 3, index: 6, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
----------GEN APP Relay Policy-----------
---------------------------------Record Table----------------------------
Record(hash)[ClientIP, ClientIf, ClientMac, Proto, Vpn, transId, Age(pkts)]
Elmnt(hash)[serverIp, serverIf, srcIp, dhcpMac, transId, Vpn, proto(fm,to)]
-------------------------------------------------------------------------
----------DHCP Relay Policy-----------
--------NETBIOS Relay Policy-----------
#IP_HELPER_END
```

12

Dynamic Routing

A router running a dynamic routing protocol can change its routing table to a better path when the primary route goes down.

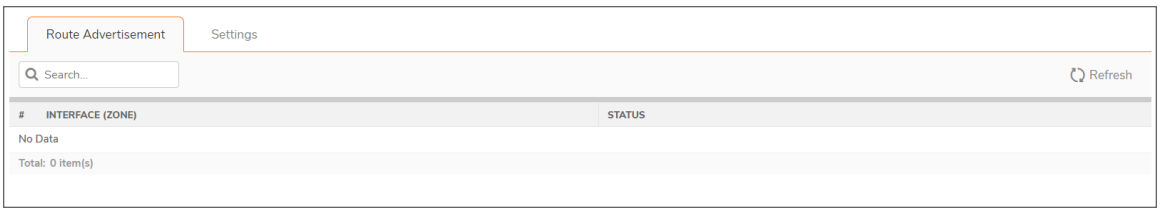
Topics:

Route Advertisement

SonicWall firewalls use RIPv1 or RIPv2 to advertise its ***static*** and ***dynamic*** routes to other routers on the network. Changes in the status of VPN tunnels between the firewall and remote VPN gateways are also reflected in the RIPv2 advertisements. Based on your router's capabilities or configuration, choose between:

- RIPv1, which is an earlier version of the protocol, has fewer features, and sends packets through broadcast instead of multicast.
- RIPv2, which is a later version of the protocol, includes subnet information when multicasting the routing table to adjacent routers and route tags for learning routes. RIPv2 packets are backwards compatible and can be accepted by some RIPv1 implementations that provide an option of listening for multicast packets. The RIPv2 Enabled (broadcast) selection, which broadcasts packets instead of multicasting them, is for heterogeneous networks with a mixture of RIPv1 and RIPv2 routers.

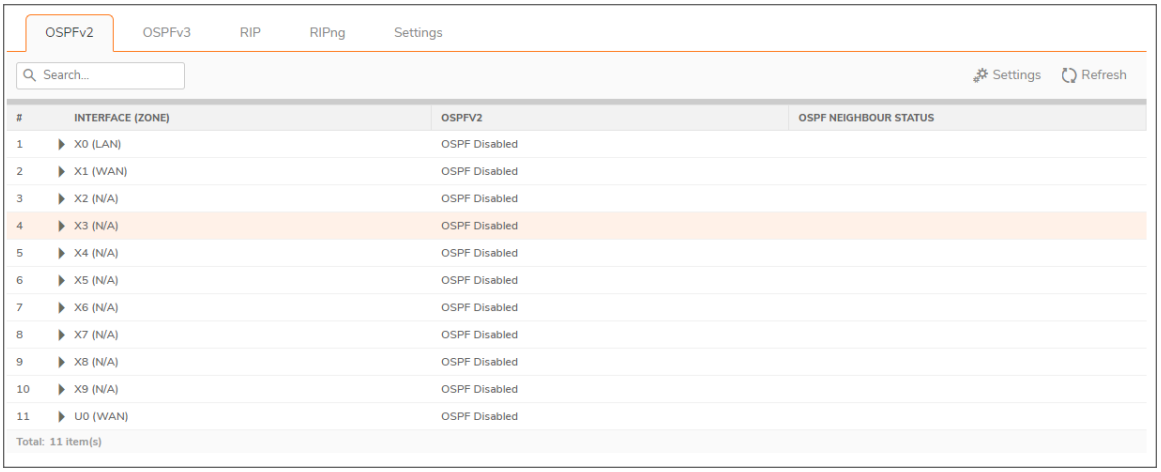
1. **NETWORK | System > Dynamic Routing | Route Advertisement** displays only when **Advanced Routing Mode** is disabled in **Settings**.



Interface (Zone)	Interfaces configured for route advertisement. If a zone has not been configured for an interface, the (**Zone**) designation is (**N/A**).
Status	Either **Enabled** or **Disabled**.
Configure	Contains the **Edit** icon.

OSPFv2

NETWORK | System > Dynamic Routing > OSPFv2, which displays only when **Advanced Routing Mode** is enabled on the **Settings** tab, shows the status of OSPFv2 and allows you to configure OSPFv2 for an interface.



Settings	Icon from the top right portion of the page that displays the **Settings** pop-up for configuring the metrics for default routes. See General Settings.
Interface (Zone)	Interfaces and their zone configured for OSPFv2. If a zone has not been configured for an interface, the (Zone) designation is (N/A).
OSPFv2	Indicates whether OSPF is enabled on an interface: • **OSPF Enabled** • **OSPF Enabled (passive)** • **OSPF Disabled**
OSPF Neighbor Status	Displays the **Status** icon, which indicates whether there are active or inactive neighbors; clicking the icon displays the **Interface OSPFv2 Area Neighbors** pop-up for detail about the interface's neighbors.
Configure	Displays the **Edit OSPFv2 Configuration** icon for the interface.

Interface OSPFv2 Area Neighbors

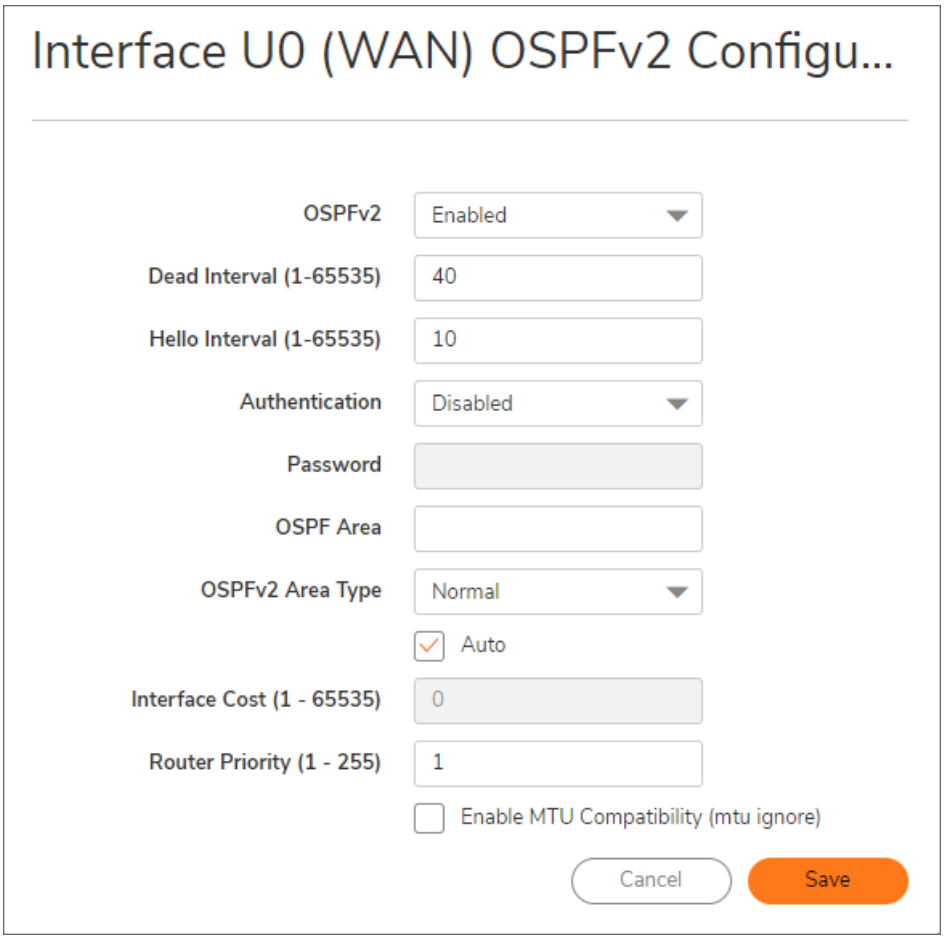
Display this pop-up by clicking the **Status** icon for the interface. (OSPFv2 must be enabled on the **Configuration** dialog.)

Router-ID	Neighbor's router ID.
Current State	State of the OSPFv2 neighborhood when it is established: • **Init** • **2-way** • **ExStart** • **Exchange** • **Loading** • **Full**
Priority	Neighbor's router's priority.
IP Address	IP address of neighbor's router.

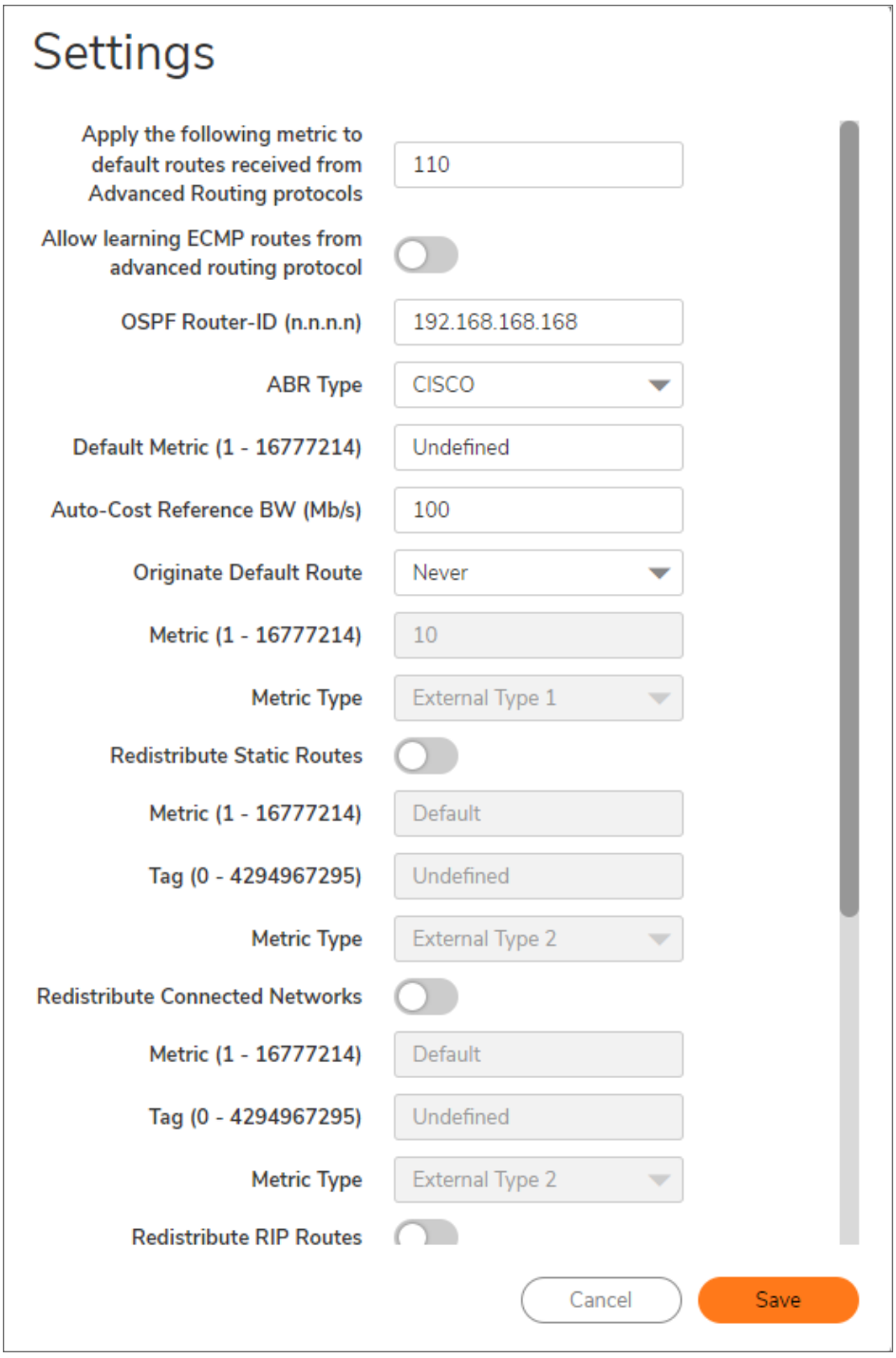
General Settings

To enable Dynamic Routing General Settings:

1. Navigate to **NETWORK | System > Dynamic Routing | Settings** tab.
2. Enable and confirm **Advanced Routing Mode**. Click the **OSPFv2** tab. Click the **Edit OSPFv2 Configuration** icon for the Interface Configuration with the relevant Routes or Networks to be distributed.
3. In the dialog that appears, set **OSPFv2** to **Enabled** and input the following information: **Dead Interval**, **Hello Interval**, and **OSPF Area**. This information must match across all firewalls or the routes and networks are not distributed correctly.



4. Click **Save**.
5. Each firewall must also have a unique Router ID, which is typically the interface IP address. However, you can set it to any local, unused IP address.
6. Navigate to **NETWORK | System > Dynamic Routing** and then click on the **Settings** icon in the top banner to enter all that information.



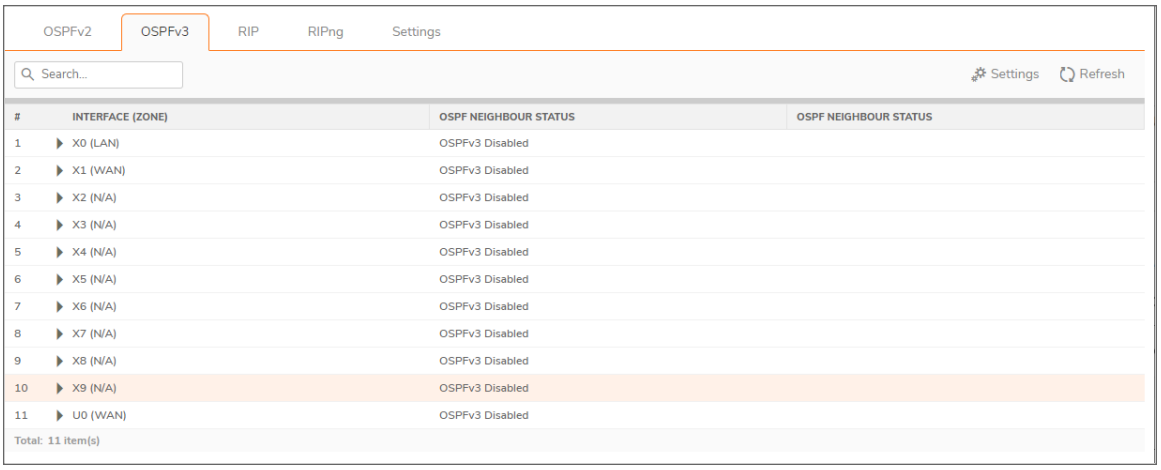
7. Set the **ABR Type** to Cisco.
8. Finally, select which, if any, of the relevant options will be redistributed: **Static Routes**, **Connected Networks**, **RIP Routes**, and **Remote VPN Networks**.

After the configuration is complete on all the area devices, you can set the metric for routes learned through the advanced routing protocols. To do so, edit the **Apply the following metric to default routes received from Advanced Routing protocols** field. The default value is 110.

After everything is configured, you will see OSPF Neighbor Status on **NETWORK | System > Dynamic Routing | OSPFv2**. A green bubble indicates that the neighbors are able to communicate, a red bubble indicates a failure. You can check the firewall's Logs under **DEVICE | Log > Settings > Network > Advanced Routing** for more information about failed peering.

OSPFv3

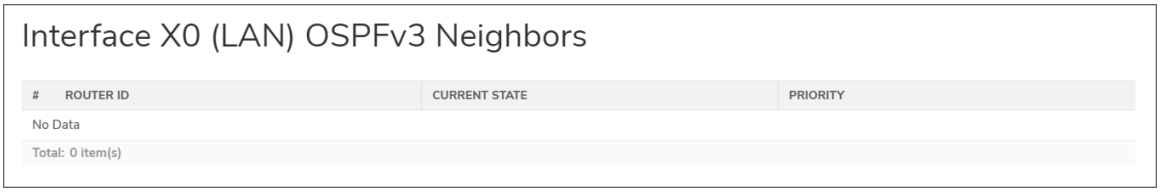
NETWORK | System > Dynamic Routing > OSPFv3, which displays only when **Advanced Routing Mode** is enabled on the **Settings** tab, shows the status of OSPFv3 and allows you to configure OSPFv3 for an interface.



Settings	Icon that displays the **Settings** pop-up for configuring the metrics for default routes. See General Settings.
Interface (Zone)	Interfaces and their zone configured for OSPFv3. If a zone has not been configured for an interface, the **(Zone)** designation is **(N/A)**.
OSPFv3	Indicates whether OSPFv3 is enabled on an interface: • **OSPFv3 Enabled** • **OSPFv3 Enabled (passive)** • **OSPFv3 Disabled**
Configure OSPFv3	Displays the **Edit** icon for the interface.
OSPFv3 Neighbor Status	Displays the **Status** icon, which indicates whether there are active or inactive neighbors; clicking the icon displays the **Interface OSPFv3 Area Neighbors** pop-up for more detail about the interface's neighbors. See **NETWORK	System > Dynamic Routing > OSPFv3**> Interface OSPFv3 Neighbors.

Interface OSPFv3 Neighbors

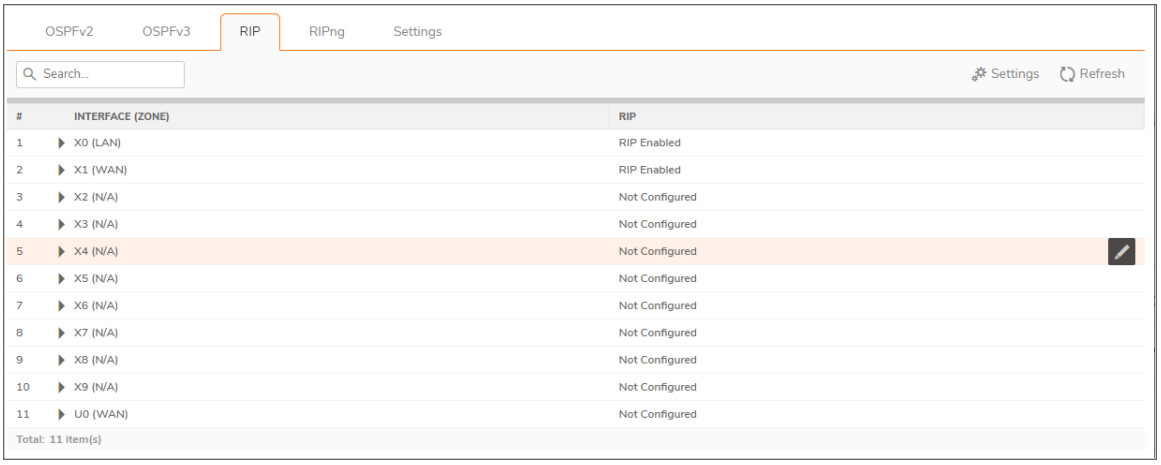
Display this pop-up by clicking the **Status** icon for the interface. (OSPFv3 must be enabled on the **Configuration** dialog.)



Router-ID	Neighbor's router ID.
Current State	State of the OSPFv3 neighborhood when it is established: • **Init** • **2-way** • **ExStart** • **Exchange** • **Loading** • **Full**
Priority	Neighbor's router's priority.

RIP

NETWORK | System > Dynamic Routing > RIP, which displays only when **Advanced Routing Mode** is enabled on the **Settings** tab, shows the status of RIP and allows you to configure RIP for an interface.

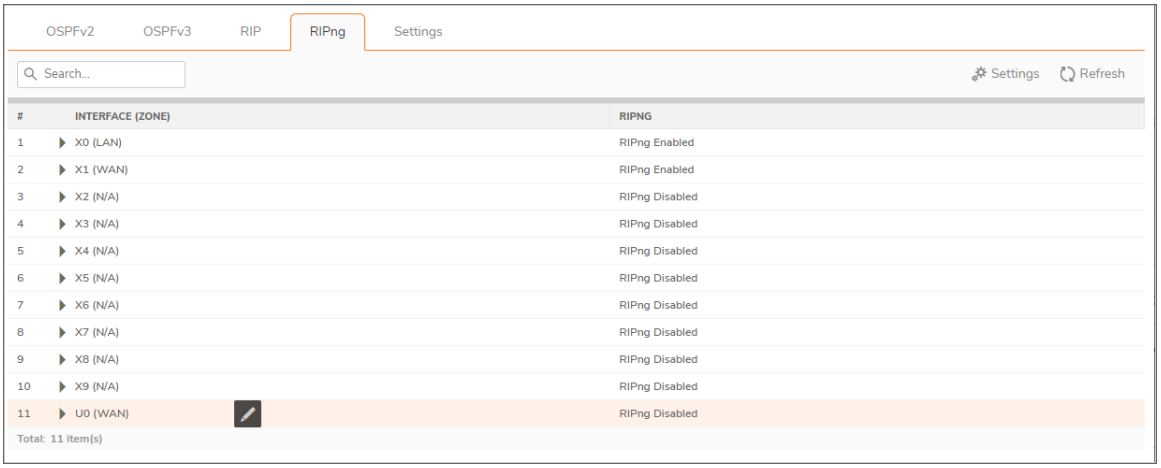


Settings	Icon that displays the **Settings** pop-up for configuring the metrics for default routes. See General Settings.

Interface (Zone)	Interfaces and their zone configured for RIP. If a zone has not been configured for an interface, the **(Zone)** designation is **(N/A)**.
RIP	Indicates whether RIP is enabled on an interface: • **RIP Enabled** • **RIP Enabled (passive)** • **RIP Disabled**
Configure RIP	Displays the **Edit** icon for the interface.

RIPng

NETWORK | System > Dynamic Routing > RIPng, which displays only when **Advanced Routing Mode** is enabled on the **Settings** tab, shows the status of RIPng and allows you to configure RIPng for an interface.

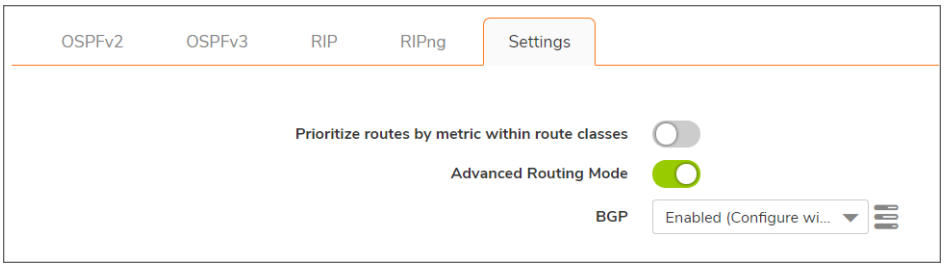


Settings	Icon that displays the **Settings** pop-up for configuring the metrics for default routes. See General Settings.
Interface (Zone)	Interfaces and their zone configured for RIPng. If a zone has not been configured for an interface, the **(Zone)** designation is **(N/A)**.
RIPng	Indicates whether RIPng is enabled on an interface: • **RIPng Enabled** • **RIPng Enabled (passive)** • **RIPng Disabled**
Configure RIPng	Displays the **Edit** icon for the interface.

Settings

To enable Dynamic Routing Settings:

1. Navigate to **NETWORK | System > Dynamic Routing | Settings**.



2. Enable **Prioritize routes by metric within route classes** if desired.
3. To switch to advanced routing mode, select **Advanced Routing Mode**. A confirmation message displays.
4. To enable BGP, select **Enabled (Configure with CLI)** from **BGP**. The default is **Disabled**. A confirmation message displays.

13

DHCP Server

The appliance includes a DHCP (Dynamic Host Configuration Protocol) server to distribute IP addresses, subnet masks, gateway addresses, and DNS server addresses to your network clients. **NETWORK | System > DHCP Server | DHCP Server Settings** includes settings for configuring the appliance's DHCP server.

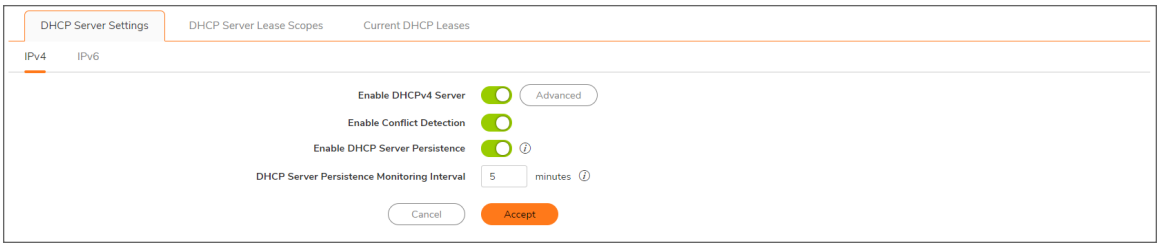
IMPORTANT: You can use the appliance's DHCP server or use existing DHCP servers on your network. If your network uses its own DHCP servers, make sure **Enable DHCP Server** is disabled.

Topics:

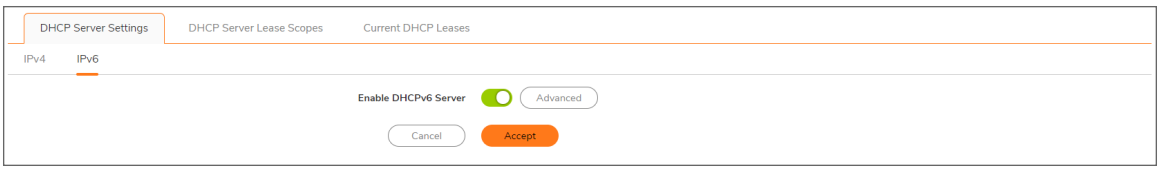
Configuring a DHCP Server

There are only minor differences between the IPv6 and IPv4 versions of **NETWORK | System > DHCP Server | DHCP Server Settings > IPv4/IPv6**. Differences are noted within procedures.

IPV4 DHCP SERVER SETTINGS



IPV6 DHCP SERVER SETTINGS



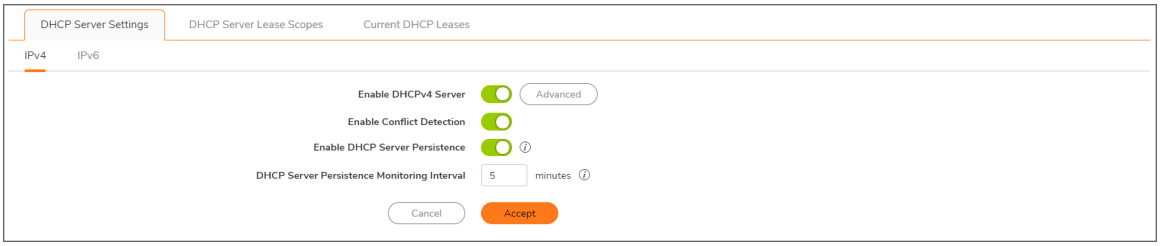
The number of address ranges and IP addresses that the firewall's DHCP server can assign depends on the model, operating system, and licenses of the appliance.

Configuring the DHCP Server Settings

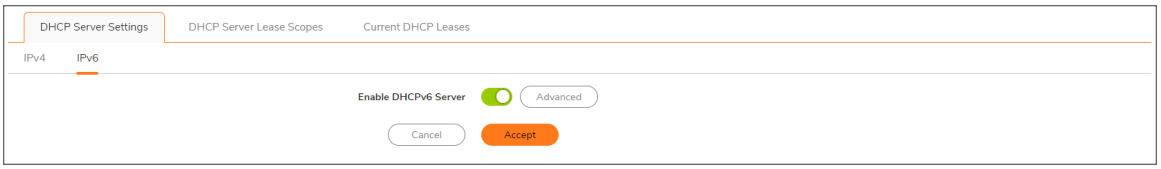
To use the SonicWall firewall's DHCP server:

1. Navigate to **NETWORK | System > DHCP Server | DHCP Server Settings**.
2. Choose which IP version to use (IPv4 or IPv6):

   IPV4

   IPV6

3. To distribute IP addresses, subnet masks, gateway addresses, and DNS server addresses to your network clients, select **Enable DHCPv4/6 Server**. This option is selected by default. For IPv4, **Advanced** and other server settings options become available.
4. For configuring DHCPv6, skip to Step 7.

5. To turn on automatic DHCP scope conflict detection on each zone when another DHCP server is present, select **Enable Conflict Detection**. This option is selected by default.

   Currently, DHCP server performs server-side conflict detection when this feature is enabled. The advantage of server-side conflict detection is that it detects conflicts even when the DHCP client does not run client-side conflict detection. However, if there are a lot of DHCP clients on the network, server-side conflict detection can result in longer wait times for a full IP address allocation to complete.

   NOTE: Conflict detection is not performed for an IP address that belongs to a “relayed” subnet scope. The DHCP server only performs a conflict detection ICMP check for a subnet range attached to its interface.

6. To allow the current state of the DHCP leases in the network to be periodically written to Flash, select **Enable DHCP Server Persistence**. At reboot, the system restores the previous DHCP server network DHCP allocation knowledge based on the IP. Lease times stored in Flash. This option is selected by default. When this option is selected, the **DHCP Server Persistence Monitoring Interval** option is available.

   - To control how often changes in the network are examined and, if necessary, written to Flash, enter the time, in minutes, in **DHCP Server Persistence Monitoring Interval**. The default is **5** minutes, the minimum is five minutes, and the maximum is 1440 minutes (24 hours).

7. To configure **Option Objects**, **Option Groups**, and **Trusted Agents**, click **Advanced**. For detailed information on configuring these features, see *Configuring Advanced Options*.
8. Click **Accept**.

Topics:

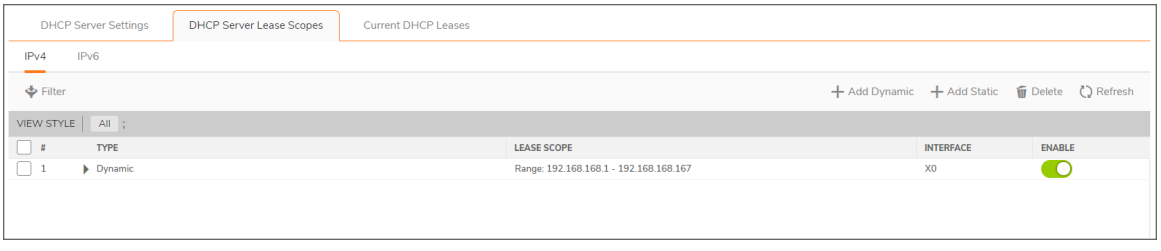
- Configuring the DHCP Server for DNS Proxy

Configuring the DHCP Server for DNS Proxy

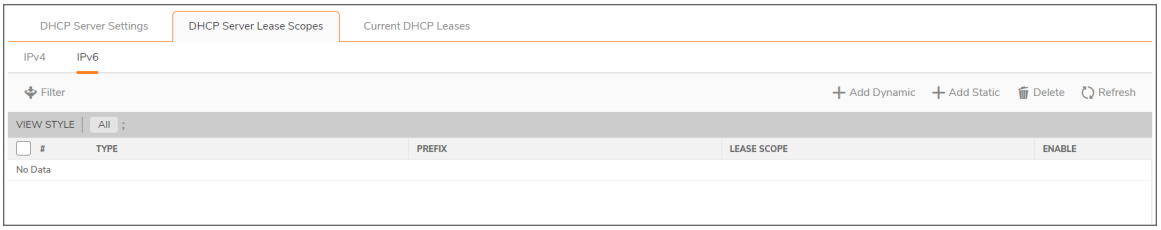
When DNS proxy is enabled on an interface, the device needs to push the interface IP as a DNS server address to clients, so you need to configure the DHCP server manually; use the interface address as the DNS Server 1 address in the DHCP server settings on the **DNS/WINS** tab. The **Interface Are-populate** checkbox on the DHCP page makes this easy to configure; if the selected interface has enabled DNS proxy, the DNS server IP is auto-added into the **DNS/WINS** page.

Configuring DHCP Server Lease Scopes

DHCPV4 SERVER LEASE SCOPES



DHCPV6 SERVER LEASE SCOPES



The **DHCP Server Lease Scopes** table displays the currently configured DHCP IP ranges:

DHCP SERVER LEASE SCOPES

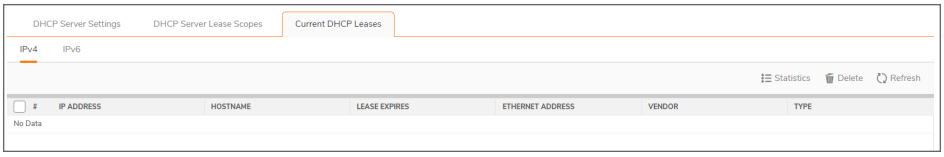
Type	**Dynamic** or **Static**
Prefix	IPv6 only.
Lease Scope	The IP address range, for example, `172.16.31.2` - `172.16.31.254`.
Interface	IPv4 only. The Interface the range is assigned to.
Details	Detailed information about the lease, displayed as a tool tip when you hover the mouse pointer over the **Comment** icon.
Enable	Select the checkbox to enable the DHCP range. Clear it to disable the range.
Configure	Contains the **Configure** and Delete icons for the table entry.

Current DHCP Leases

Topics:

- Current DHCP Leases IPv4
- Current DHCP Leases IPv6

Current DHCP Leases IPv4



The current DHCP lease information is displayed in the **Current DHCP Leases** table. Each binding entry displays the:

- **IP Address**
- **Hostname**
- **Lease Expires**
- **Ethernet Address**
- **Vendor**

- **Type** of binding (**Dynamic**, **Dynamic BOOTP**, or **Static BOOTP**)
- **Delete** icon

To delete a binding that frees the IP address on the DHCP server:

1. Click the **Delete** icon next for the entry. For example, use the **Delete** icon to remove a host when it has been removed from the network and you need to reuse its IP address.
2. Click **Accept**.

Current DHCP Leases IPv6

The current DHCP lease information is displayed in the **Current DHCP Leases** table. Each binding entry displays the:

- **IP Address**
- **Lease Expires**
- **IAID**
- **DUID**
- **Type** of binding (**Dynamic**, **Dynamic BOOTP**, or **Static BOOTP**)
- **Delete** icon

To delete a binding, which frees the IP address on the DHCP server:

1. Click the **Delete** icon next for the entry. For example, use the **Delete** icon to remove a host when it has been removed from the network and you need to reuse its IP address.
2. Click **Accept**.

DHCPv6 Relay

SonicOS supports DHCPv6 Relay. For information about DHCPv6 relay in SonicOS, see *DHCPv6 Relay*.

Configuring Advanced Options

NOTE: Configuring DHCP server options is essentially the same for both IPv4 and IPv6. Exceptions are noted in the procedures.

Topics:

- Configuring DHCP Option Objects
- Configuring DHCP Option Groups
- Configuring a Trusted DHCP Relay Agent Address Group (IPv4 Only)
- Enabling Trusted DHCP Relay Agents

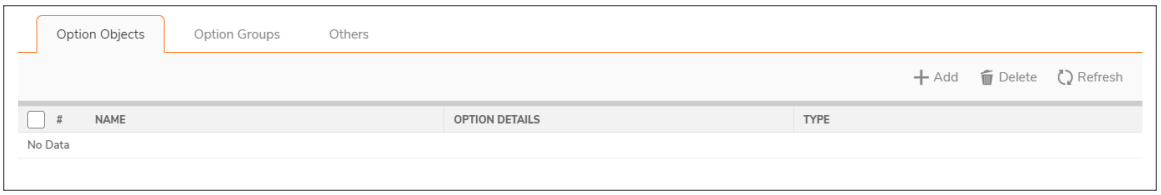
RFC-Defined DHCP Option Numbers provides a list of DHCP options by RFC-assigned option number.

Configuring DHCP Option Objects

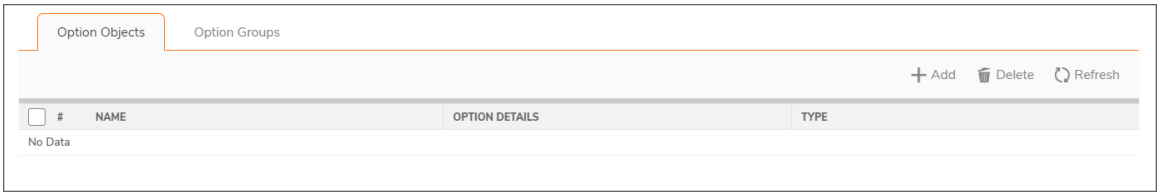
To configure DHCP option objects:

1. Navigate to **NETWORK | System > DHCP Server | DHCPv4/6 Server Settings**.
2. Click **Advanced**. The DHCP Advanced Settings dialog displays. The dialogs for IPv4 and IPv6 are slightly different; see *IPv4 DHCP Advanced Settings* and *IPv6 DHCP Advanced Settings*.

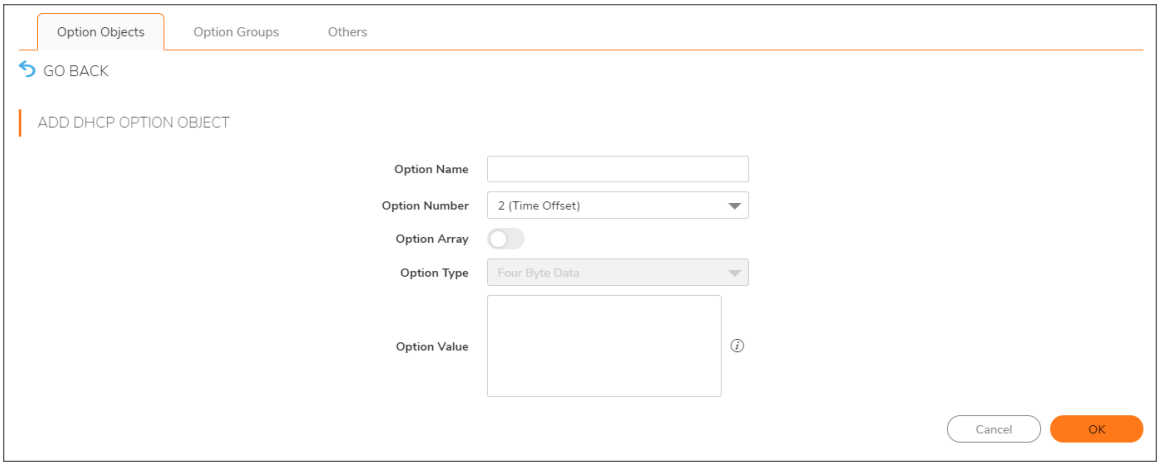
   IPV4 DHCP ADVANCED SETTINGS

   IPV6 DHCP ADVANCED SETTINGS

3. Click **+Add**. The **Add DHCP Option Object** dialog displays.



4. Type a name for the option in the **Option Name** field.
5. From **Option Number**, select the option number that corresponds to your DHCP option. For a list of option numbers, names, and descriptions, refer to *RFC-Defined DHCP Option Numbers*.

   NOTE: Available options differ depending on whether you are configuring an IPv4 or IPv6 option.

6. If:
   - Only one option type is available, for example, for **Option Number 2 (Time Offset)**, **Option Array** is dimmed. Go to Step 7.
   - There are multiple option types available, for example, for **77 (User Class Information)**, **Option Type** becomes available and lists allowable types of the option, such as **IP Address**, **Two-Byte Data**, **String**, or **Boolean**. Select the option type.
7. Type the option value, for example, an IP address, in the **Option Value** field. If **Option Array** is checked, multiple values can be entered, separated by a semi-colon (;).
8. Click **OK**. The object displays in the **Option Objects** table.

Configuring DHCP Option Groups

To configure DHCP option groups:

1. Navigate to **NETWORK | System > DHCP Server | DHCPv4/6 Server Settings**.
2. Click **Advanced**. The **DHCP Advanced Settings** dialog displays.

   NOTE: Available options differ depending on whether you are configuring an IPv4 or IPv6 option (see IPv6 DHCP Advanced Settings or IPv4 DHCP Advanced Settings).

3. Click **Option Groups**.
4. Click **Add Group**. The **Add DHCP/v6 Option Group** dialog displays.
5. Enter a name for the group in the **Name** field.

6. Select an option object from the left column and click the **Right Arrow** to add the option object to the In Group. To select multiple option objects at the same time, hold the Ctrl key while selecting the option objects.
7. Click **Save**. The group displays in the **Option Groups** table.

Configuring a Trusted DHCP Relay Agent Address Group (IPv4 Only)

To configure the **Default Trusted Relay Agent List** Address Group, you must first configure an Address Object for each trusted relay agent, then add these Address Objects to the **Default Trusted Relay Agent List** Address Group or to a custom Address Group.

Address Objects and Address Groups are configured in **OBJECT | Match Objects > Addresses | Address Objects**. For more information on how to configure Address Objects and Address Groups, see the *SonicOS Object Administration Guide*.

Enabling Trusted DHCP Relay Agents

In the **DHCP Advanced Settings** dialog, you can enable the **Trusted Relay Agent List** option using the **Default Trusted Relay Agent List** Address Group or create another Address Group using existing Address Objects.

ⓘ **NOTE:** When a server is assigned as the internal DHCP server for DHCP over VPN Central Gateway, DHCP messages that come from the VPN tunnel are always bypassed.

To enable the Trusted Relay Agent List option and select the desired Address Group:

1. Navigate to **NETWORK | System > DHCP Server | DHCPv4 Settings**.
2. Click **Advanced**. The **DHCP Advanced Settings** dialog displays.
3. Click the **Others** view.
4. Select **Enable Trusted DHCP Relay Agent List**. This option is not selected by default. **Trusted Relay Agent List** becomes available.
5. Select the Address Group from **Default Trusted Relay Agent List**. This option includes all existing address groups as well as the **Create New Address Object Group** option.
6. To create a custom Address Group for this option, select **Create New Address Object Group**. The **Add Address Object Group** dialog displays. For information on how to configure Address Groups, see the *SonicOS Object Administration Guide*.
7. Click **OK** to enable the **Trusted Relay Agent List** option with the selected Address Group.

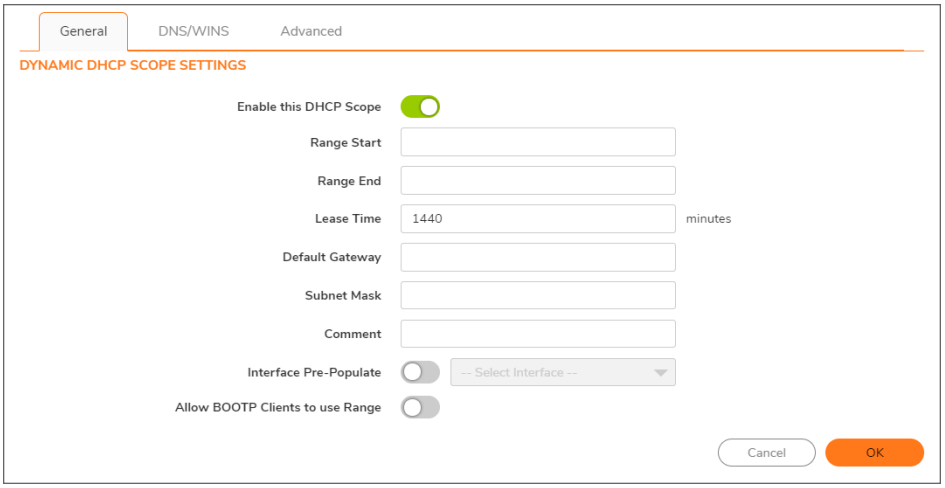
Configuring IPv4 DHCP Servers for Dynamic Ranges

Because SonicOS allows multiple DHCP scopes per interface, there is no requirement that the subnet range is attached to the interface when configuring DHCP scopes.

To configure IPv4 DHCP servers for dynamic IP address ranges:

1. Navigate to **NETWORK | System > DHCP Server | DHCP Server Lease Scopes**.
2. Click **+Add Dynamic**.
    - The **Dynamic Range Configuration** dialog displays. Go to Add DHCP Dynamic Scope

Add DHCP Dynamic Scope



To add a dynamic scope:

1. From the **General** view, to enable this scope, ensure **Enable this DHCP Scope** is selected. This option is selected by default.
2. To populate the **Range Start**, **Range End**, **Default Gateway**, and **Subnet Mask** fields:
    a. With default values for a certain interface:
        1. Select **Interface Pre-Populate** near the bottom of the dialog. The selections become available. This option is not selected by default.
        2. Select the interface. The populated IP addresses are in the same private subnet as the selected interface.

    ⓘ **IMPORTANT:** To select an interface from **Interface Pre-Populate**, the interface must first be fully configured and it must be either:

- Of the zone type LAN, WLAN, or DMZ.
- A VLAN subinterface
    - Go to Step 3.

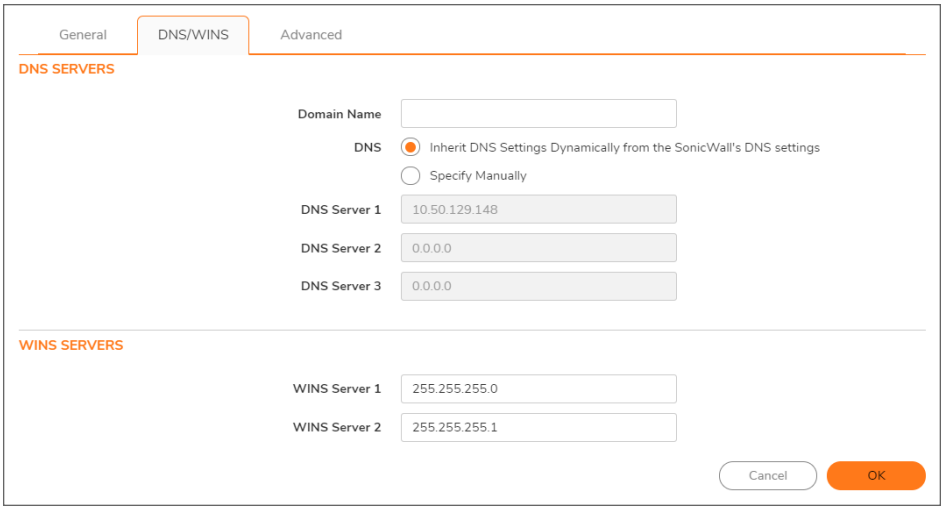
b. Manually:

1. Type in your own IP address range.
2. Enter the number of minutes an IP address is leased by the scope before it is issued another IP address in the Lease Time (minutes) field. The minimum is 0, the maximum is 71582789, and 1440 minutes (24 hours) is the default.
3. Enter the IP address of the gateway into the **Default Gateway** field.
4. Enter the gateway subnet mask into the **Subnet Mask** field.

3. Optionally, enter a comment in the **Comment** field.
4. The **Interface Pre-Populate** option populates the DHCP scope configuration with information from the selected interface. After the scope has been added, you might notice that the Interface reads “N/A.”
5. Select **Allow BOOTP Clients to use Range** if you have BOOTP Clients on your network. This option is not selected by default.

   BOOTP stands for bootstrap protocol, which is a TCP/IP protocol and service that allows disables workstations to obtain their IP address, other TCP/IP configuration information, and their boot image file from a BOOTP server.
6. Click **DNS/WINS** to continue configuring the DHCP Server feature.

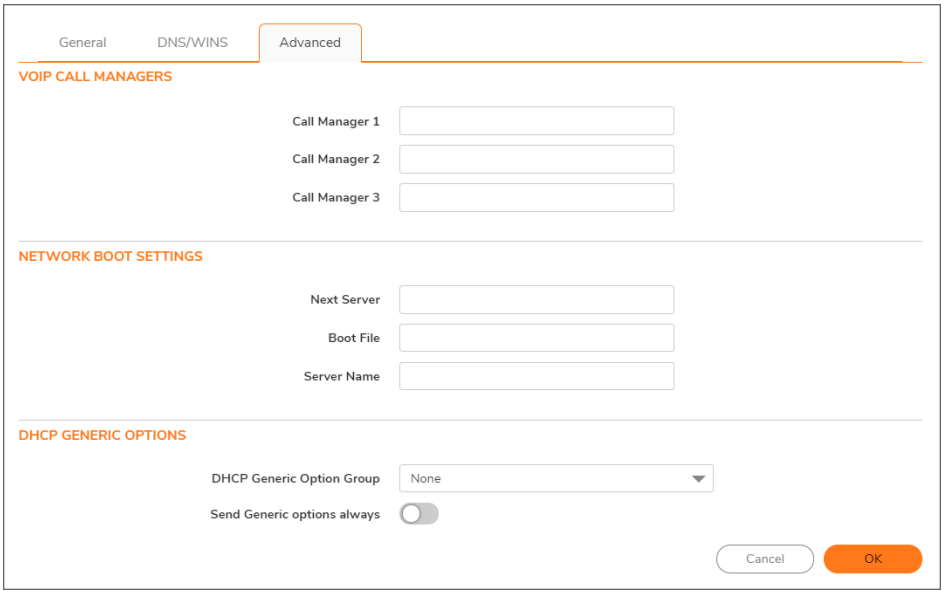
DNS/WINS



To configure DNS/WINS servers:

1. If you have a domain name for the DNS server, enter it in the **Domain Name** field.
2. Choose whether to:
    - **Inherit DNS Settings Dynamically from the SonicWall's DNS settings**; go to Step 4.
    - **Specify Manually**. The **DNS Server 1/2/3** fields become available.
3. Enter the IP address(es) of the DNS server(s) in the respective **DNS Server 1/2/3** field(s).
4. If you have WINS running on your network, type the WINS server IP address in the **WINS Server 1** field. You can add an additional WINS server.
5. Click **Advanced**. The **Advanced** options allow you to configure the DHCP server to send the Cisco Call Manager information to VoIP clients on the network.

Advanced



To configure advanced settings:

1. Under **VoIP Call Managers**, enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager 1** field. You can add two additional VoIP Call Manager addresses.
2. Under **Network Boot Settings**, in the **Next Server** field, enter the IP address of the PXE boot server (TFTP server) that a PXE client uses during the next stage of the boot process.

    ⓘ **IMPORTANT:** The fields under **Network Boot Settings** are used in a Pre-boot Execution Environment (PXE), in which the client boots up using files obtained over a network interface. The PXE client obtains the IP address and name of the PXE boot server, and the boot file name, from the DHCP server.
    When using these options, select **PXE** under **DHCP Generic Options**.

3. In the **Boot File** field, enter the name of the boot file that the PXE client can get over TFTP from the PXE boot server.
4. In the **Server Name** field, enter the DNS host name of the PXE boot server (TFTP server).
5. For information on configuring **DHCP Generic Options** see Configuring DHCP Generic Options for DHCP Lease Scopes.
6. Click **OK**.
7. Click **Accept** for the settings to take effect on the firewall.

For more information on VoIP support features on the SonicWall firewall, see *VoIP*.

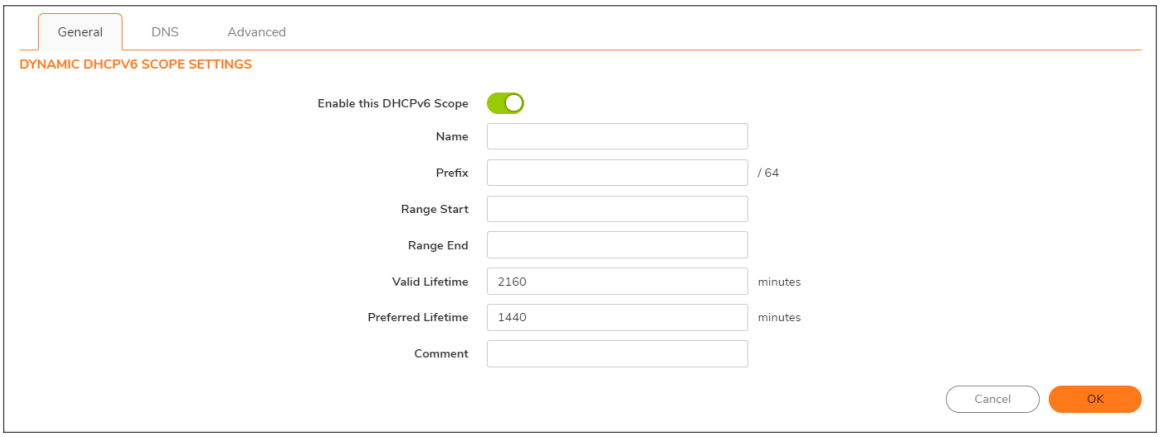
Configuring IPv6 DHCP Servers for Dynamic Ranges

Because SonicOS allows multiple DHCP scopes per interface, there is no requirement that the subnet range is attached to the interface when configuring DHCP scopes.

To configure IPv6 DHCP servers for dynamic IP address ranges:

1. Navigate to **NETWORK | System > DHCP Server | DHCPv6 Server Lease Scopes**.
2. Click **+Add Dynamic**.
    - The **Add DHCPv6 Dynamic Scope** dialog displays. Go to *Add DHCPv6 Dynamic Scope*.
    - IPv4, the **Dynamic Range Configuration** dialog displays. Go to *Dynamic Range Configuration*.

Add DHCPv6 Dynamic Scope

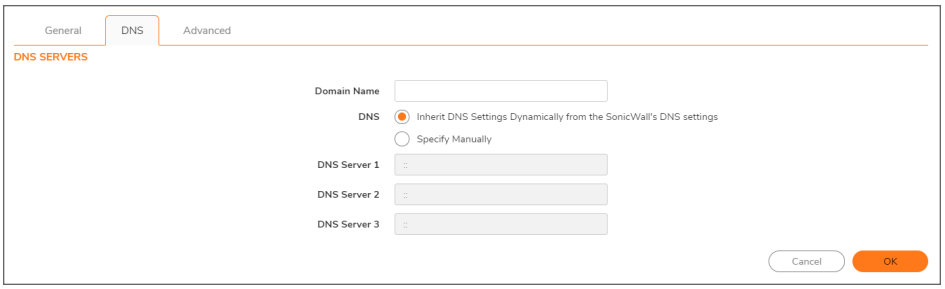


To add a dynamic scope:

1. To enable this scope, ensure **Enable this DHCP Scope** is selected. This option is selected by default.
2. Enter a name for the scope in the **Name** field.
3. Enter the prefix the scope uses to distribute IPv6 addresses in the **Prefix** field.

4. Enter the range start and range end in the **Range Start** and **Range End** fields, respectively. Both addresses must fall within the scope of the prefix.
5. Enter the valid lifetime of an IPv6 address leased by the scope, in minutes, in the **Valid Lifetime** field. The minimum is 0, the maximum is 71582789, and the default is **2160**.
6. Enter the preferred lifetime of an IPv6 address leased by the scope, in minutes, in the **Preferred Lifetime** field. The minimum is 0, the maximum is 71582789, and the default is **1440**.
7. Optionally, enter a comment in the **Comment** field.
8. Click **DNS**.

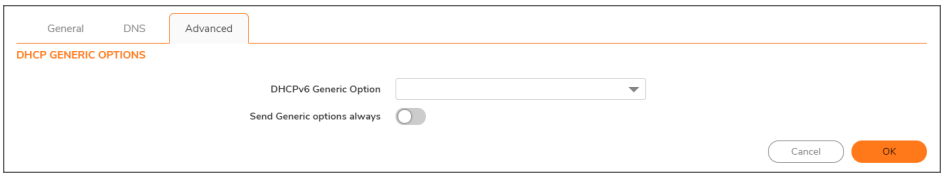
DNS



To add a DNS server:

1. Enter a domain name in the **Domain Name** field.
2. Choose whether to:
    - **Inherit DNS Settings Dynamically from the SonicWall's DNS settings**; go to Step 4.
    - **Specify Manually**. The **DNS Server 1/2/3** fields become available.
3. Enter the IP address(es) of the DNS server(s) in the respective **DNS Server 1/2/3** field(s).
4. Click **Advanced**.

Advanced



To configure generic DHCP options:

1. Select a DHCP Option Object or Group from DHCPv6 Generic Option. The default is **None**. To configure a new DHCPv6 Option or Group, see Configuring DHCP Option Objects and/or Configuring DHCP Option

Groups.

2. To send all configured DHCPv6 options for this scope regardless of the Option Request Option contained in the message from the DHCPv6 client, enable **Send Generic Options Always**. This option is not selected by default.
3. Click **OK**.

Configuring IPv4 DHCP Static Ranges

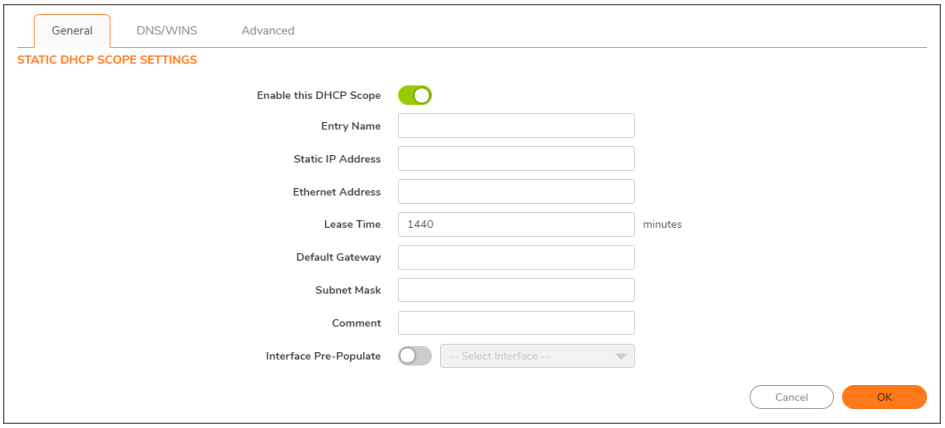
Static ranges are IP addresses assigned to servers requiring permanent IP settings. Because SonicOS allows multiple DHCP scopes per interface, there is no requirement that the subnet range is attached to the interface when configuring DHCP scopes.

To configure static ranges:

1. Navigate to **NETWORK | System > DHCP Server | DHCP Server Lease Scopes** table, click **+Add Static**.

   The **Static Range Configuration** dialog displays. Go to Adding Static Range Configuration Settings.

Adding Static Range Configuration Settings



To enable this scope:

1. Ensure **Enable this DHCP Scope** is enabled. This option is selected by default.
2. Enter a name for the static entry in the **Entry Name** field.
3. Enter the device IP address in the **Static IP Address** field.
4. Enter the device Ethernet (MAC) address in the **Ethernet Address** field.
5. To populate the **Lease Time**, **Default Gateway**, and **Subnet Mask** fields with default values for a certain interface, select **Interface Pre-Populate** near the bottom of the dialog. The drop-down menu becomes

available. This option is not selected by default.

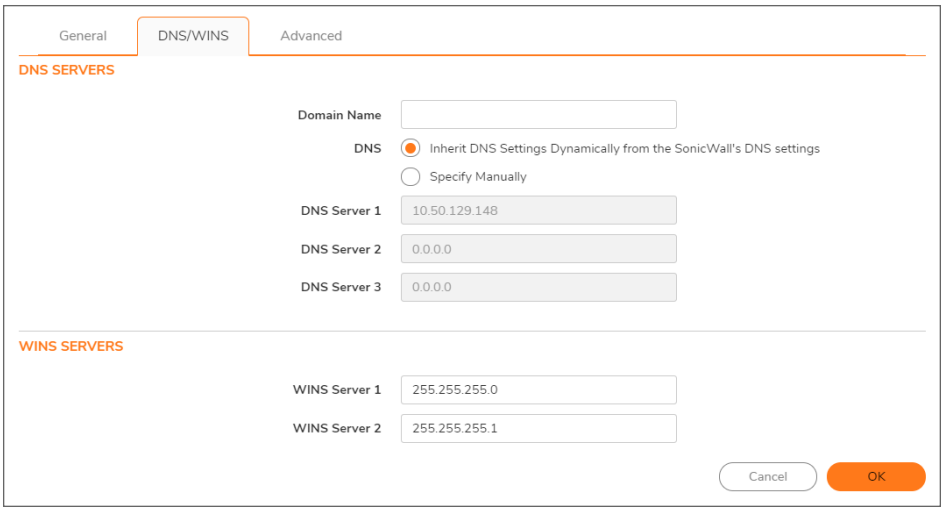
a. Select the interface from the drop-down menu. The populated IP addresses are in the same private subnet as the selected interface.

IMPORTANT: To select an interface from the Interface menu, it must first be fully configured and it must be of the zone type, LAN, WLAN, or DMZ, or be a VLAN subinterface.

6. Enter the number of minutes an IP address is leased by the scope before it is issued another IP address in the **Lease Time (minutes)** field. The minimum is 0, the maximum is 71582789, and **1440** minutes (24 hours) is the default.
7. Use the populated gateway address or enter the IP address of the gateway into the **Default Gateway** field.
8. Use the populated subnet mask or enter the gateway subnet mask into the **Subnet Mask** field.
9. Optionally, enter a comment in the **Comment** field.
10. For how to configure **DNS/WINS** and **Advanced** settings, see DNS/WINS and Advanced, respectively.
11. Click **OK** to add the settings to the firewall.
12. Click **Accept** for the settings to take effect on the firewall.

For more information on VoIP support features on the SonicWall firewall, see *VoIP*.

DNS/WINS

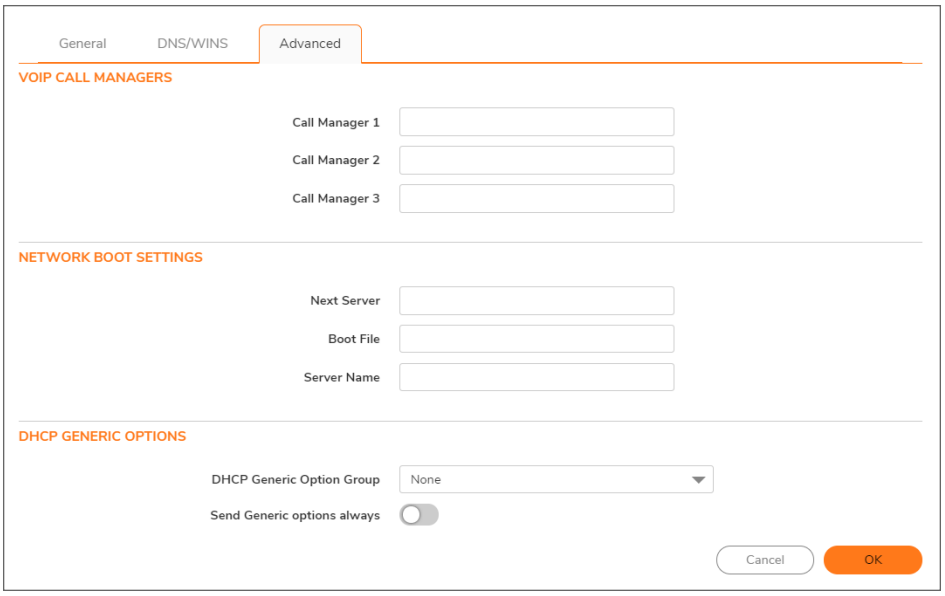


To configure DNS/WINS servers:

1. If you have a domain name for the DNS server, enter it in the **Domain Name** field.
2. Choose whether to:
   - **Inherit DNS Settings Dynamically from the SonicWall's DNS settings**; go to Step 4.
   - **Specify Manually**. The **DNS Server 1/2/3** fields become available.

3. Enter the IP address(es) of the DNS server(s) in the respective **DNS Server 1/2/3** field(s).
4. If you have WINS running on your network, type the WINS server IP address in the **WINS Server 1** field. You can add an additional WINS server.
5. Click **Advanced**. The **Advanced** options allow you to configure the DHCP server to send the Cisco Call Manager information to VoIP clients on the network.

Advanced



To configure advanced settings:

1. Under **VoIP Call Managers**, enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager 1** field. You can add two additional VoIP Call Manager addresses.
2. Under **Network Boot Settings**, in the **Next Server** field, enter the IP address of the PXE boot server (TFTP server) that a PXE client uses during the next stage of the boot process.

   ⓘ **IMPORTANT:** The fields under **Network Boot Settings** are used in a Pre-boot Execution Environment (PXE), in which the client boots up using files obtained over a network interface. The PXE client obtains the IP address and name of the PXE boot server, and the boot file name, from the DHCP server.
   When using these options, select **PXE** under **DHCP Generic Options**.
3. In the **Boot File** field, enter the name of the boot file that the PXE client can get over TFTP from the PXE boot server.
4. In the **Server Name** field, enter the DNS host name of the PXE boot server (TFTP server).
5. For information on configuring **DHCP Generic Options** see Configuring DHCP Generic Options for DHCP Lease Scopes.

6. Click **OK**.
7. Click **Accept** for the settings to take effect on the firewall.

For more information on VoIP support features on the SonicWall firewall, see *VoIP*.

Configuring IPv6 DHCP Static Ranges

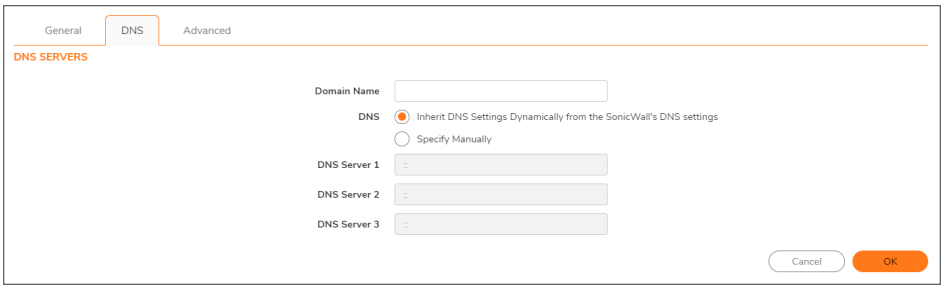
Static ranges are IP addresses assigned to servers requiring permanent IP settings. Because SonicOS allows multiple DHCP scopes per interface, there is no requirement that the subnet range is attached to the interface when configuring DHCP scopes.

To configure static ranges:

1. Navigate to **NETWORK | System > DHCP Server | DHCPv6 Server Lease Scopes** table, click **+Add Static**.

   The **Add DHCPv6 Static Scope** dialog displays. Go to Adding Static Range Configuration Settings.

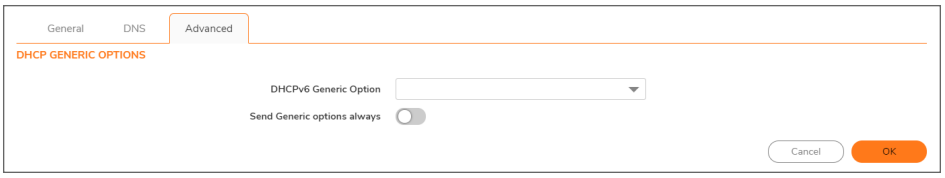
DNS



To add a DNS server:

1. Enter a domain name in the **Domain Name** field.
2. Choose whether to:
   - **Inherit DNS Settings Dynamically from the SonicWall's DNS settings**; go to Step 4.
   - **Specify Manually**. The **DNS Server 1/2/3** fields become available.
3. Enter the IP address(es) of the DNS server(s) in the respective **DNS Server 1/2/3** field(s).
4. Click **Advanced**.

Advanced



To configure generic DHCP options:

1. Select a DHCP Option Object or Group from DHCPv6 Generic Option. The default is **None**. To configure a new DHCPv6 Option or Group, see Configuring DHCP Option Objects and/or Configuring DHCP Option Groups.
2. To send all configured DHCPv6 options for this scope regardless of the Option Request Option contained in the message from the DHCPv6 client, enable **Send Generic Options Always**. This option is not selected by default.
3. Click **OK**.

Configuring DHCP Generic Options for DHCP Lease Scopes

This section provides configuration tasks for DHCP generic options for lease scopes.

NOTE: Before generic options for a DHCP lease scope can be configured, a static or dynamic DHCP server lease scope must be created.

The *RFC-Defined DHCP Option Numbers* provides a list of DHCP options by RFC-assigned option number.

To configure DHCP generic options for DHCP server lease scopes:

1. If:
    a. Modifying an existing DHCP lease scope:
        1. Locate the lease scope under DHCP Server Lease Scopes on **NETWORK | System > DHCP Server**.
        2. Click the **Configure** icon.
        3. Click **Advanced** on the displayed dialog.
    b. Creating a new DHCP lease scope:
        1. Click the **Advanced** view after configuring the options under the **General** and **DNS/WINS** tabs (see Configuring DHCP Server for Dynamic Ranges or Configuring Static DHCP Entries).

2. Select a DHCP option or option group in the **DHCP Generic Option Group** drop-down menu.

   When the **Network Boot Settings** fields are configured for use with PXE, select **PXE** here.
3. To always use DHCP options for this DHCP server lease scope, check **Send Generic options always**.
4. Click **OK**.

RFC-defined DHCP Option Numbers

Option Number	IPv6 √	Name	Description
2		Time Offset	Time offset in seconds from UTC
3		Router	N/4 router addresses
4		Time Servers	N/4 time server addresses
5		Name Servers	N/4 IEN-116 server addresses
6		DNS Servers	N/4 DNS server addresses
7		Log Servers	N/4 logging server addresses
8		Cookie Servers	N/4 quote server addresses
9		LPR Servers	N/4 printer server addresses
10		Impress Servers	N/4 impress server addresses
11		RLP Servers	N/4 RLP server addresses
12	√	Host Name	Hostname string- such as (Server Unicast)
13		Boot File Size	Size of boot file in 512-byte chunks
14		Merit Dump File	Client to dump and name of file to dump to
15		Domain Name	DNS domain name of the client
16		Swap Server	Swap server addresses
17		Root Path	Path name for root disk
18		Extension File	Patch name for more BOOTP info
19		IP Layer Forwarding	Enable or disable IP forwarding
20		Src route enabler	Enable or disable source routing
21	√	Policy Filter (IPv4) SIP Servers Domain Name List (IPv6)	Routing policy filters (IPv4) Enables listing of SIP Servers domain names (IPv6)
22	√	Maximum DG Reassembly Size (IPv4) SIP Servers IPv6 Address List (IPv6)	Maximum datagram reassembly size (IPv4) Enables listing of SIP Servers IPv6 Addresses (IPv6)

Option Number	IPv6 √	Name	Description
23	√	Default IP TTL (IPv4) DNS Recursive Name Server (IPv6)	Default IP time-to-live (IPv4) Enables listing of DNS Recursive Name servers (IPv6)
24	√	Path MTU Aging Timeout (IPv4) Domain Search List (IPv6)	Path MTU aging timeout (IPv4) Enables listing of domain names for searching (IPv6)
25		MTU Plateau	Path MTU plateau table
26		Interface MTU Size	Interface MTU size
27	√	All Subnets Are Local (IPv4) Network Information Service (NIS) Servers (IPv6)	All subnets are local (IPv4) Enables listing of Network Information Service (NIS) servers (IPv6)
28	√	Broadcast Address (IPv4) Network Information Service V2 (NIS+) Servers (IPv6)	Broadcast address (IPv4) Enables listing of Network Information Service V2 (NIS+) servers (IPv6)
29	√	Perform Mask Discovery (IPv4) Network Information Service (NIS) Domain Name (IPv6)	Perform mask discovery (IPv4) Enables listing of Network Information Service (NIS) domain names (IPv6)
30	√	Provide Mask to Others (IPv4) Network Information Service V2 (NIS+) Domain Name (IPv6)	Provide mask to others (IPv4) Enables listing of Network Information Service V2 (NIS+) domain names (IPv6)
31	√	Perform Router Discovery (IPv4) Simple Network Time Protocol (SNTP) Servers (IPv6)	Perform router discovery (IPv4) Enables listing of Simple Network Time Protocol (SNTP) servers (IPv6)
32	√	Router Solicitation Address (IPv4) Information Refresh Time (IPv6)	Router solicitation address (IPv4) Information refresh time (IPv6)
33		Static Routing Table	Static routing table
34		Trailer Encapsulation	Trailer encapsulation
35		ARP Cache Timeout	ARP cache timeout
36		Ethernet Encapsulation	Ethernet encapsulation
37		Default TCP Time to Live	Default TCP time to live
38		TCP Keepalive Interval	TCP keepalive interval
39		TCP Keepalive Garbage	TCP keepalive garbage
40		NIS Domain Name	NIS domain name
41		NIS Server Addresses	NIS server addresses
42		NTP Servers Addresses	NTP servers addresses
43		Vendor Specific Information	Vendor specific information
44		NetBIOS Name Server	NetBIOS name server
45		NetBIOS Datagram Distribution	NetBIOS datagram distribution

Option Number	IPv6 √	Name	Description
46		NetBIOS Node Type	NetBIOS node type
47		NetBIOS Scope	NetBIOS scope
48		X Window Font Server	X window font server
49		X Window Display Manager	X window display manager
50		Requested IP address	Requested IP address
51		IP Address Lease Time	IP address lease time
52		Option Overload	Overload “sname” or “file”
53		DHCP Message Type	DHCP message type
54		DHCP Server Identification	DHCP server identification
55		Parameter Request List	Parameter request list
56		Message	DHCP error message
57		DHCP Maximum Message Size	DHCP maximum message size
58		Renew Time Value	DHCP renewal (T1) time
59		Rebinding Time Value	DHCP rebinding (T2) time
60		Client Identifier	Client identifier
61		Client Identifier	Client identifier
62		Netware/IP Domain Name	Netware/IP domain name
63		Netware/IP sub Options	Netware/IP sub options
64		NIS+ V3 Client Domain Name	NIS+ V3 client domain name
65		NIS+ V3 Server Address	NIS+ V3 server address
66		TFTP Server Name	TFTP server name
67		Boot File Name	Boot file name
68		Home Agent Addresses	Home agent addresses
69		Simple Mail Server Addresses	Simple mail server addresses
70		Post Office Server Addresses	Post office server addresses
71		Network News Server Addresses	Network news server addresses
72		WWW Server Addresses	WWW server addresses
73		Finger Server Addresses	Finger server addresses
74		Chat Server Addresses	Chat server addresses
75		StreetTalk Server Addresses	StreetTalk server addresses
76		StreetTalk Directory Assistance Addresses	StreetTalk directory assistance addresses
77		User Class Information	User class information
78		SLP Directory Agent	Directory agent information
79		SLP Service Scope	Service location agent scope

Option Number	IPv6 √	Name	Description
80		Rapid Commit	Rapid commit
81		FQDN-Fully Qualified Domain Name	Fully qualified domain name
82		Relay Agent Information	Relay agent information
83		Internet Storage Name Service	Internet storage name service
84		Undefined	N/A
85		Novell Directory Servers	Novell Directory Services servers
86		Novell Directory Server Tree Name	Novell Directory Services server tree name
87		Novell Directory Server Context	Novell Directory Services server context
88		BCMCS Controller Domain Name List	CMCS controller domain name list
89		BCMCS Controller IPv4 Address List	BCMCS controller IPv4 address list
90		Authentication	Authentication
91-92		Undefined	N/A
93		Client System	Client system architecture
94		Client Network Device Interface	Client network device interface
95		LDAP Use	Lightweight Directory Access Protocol
96		Undefined	N/A
97		UUID/GUID-based Client Identifier	UUID/GUID-based client identifier
98		Open Group’s User Authentication	Open group’s user authentication
99-108		Undefined	N/A
109		Autonomous System Number	Autonomous system number
110-111		Undefined	N/A
112		NetInfo Parent Server Address	NetInfo parent server address
113		NetInfo Parent Server Tag	NetInfo parent server tag
114		URL:	URL
115		Undefined	N/A
116		Auto Configure	DHCP auto-configuration
117		Name Service Search	Name service search
118		Subnet Collection	Subnet selection
119		DNS Domain Search List	DNS domain search list
120		SIP Servers DHCP Option	SIP servers DHCP option
121		Classless Static Route Option	Classless static route option
122		CCC- CableLabs Client Configuration	CableLabs client configuration
123		GeoConf	GeoConf
124		Vendor-Identifying Vendor Class	Vendor-identifying vendor class

Option Number	IPv6 √	Name	Description
125		Vendor Identifying Vendor Specific	Vendor-identifying vendor specific
126-127		Undefined	N/A
128		TFTP Server IP Address	TFTP server IP address for IP phone software load
129		Call Server IP Address	Call server IP address
130		Discrimination String	Discrimination string to identify vendor
131		Remote Statistics Server IP Address	Remote statistics server IP address
132		802.1Q VLAN ID	IEEE 802.1Q VLAN ID
133		802.1Q L2 Priority	IEEE 802.1Q layer 2 priority
134		Diffserv Code Point	Diffserv code point for VoIP signaling and media streams
135		HTTP Proxy For Phone Applications	HTTP proxy for phone-specific applications
136-149		Undefined	N/A
150		TFTP Server Address- Etherboot-GRUB Config	TFTP server address- Etherboot- GRUB configuration
151-174		Undefined	N/A
175		Ether Boot	Ether Boot
176		IP Telephone	IP telephone
177		Ether Boot PacketCable and CableHome	Ether Boot PacketCable and CableHome
178-207		Undefined	N/A
208		`pxelinux.magic` (string) = `241.0.116.126`	`pxelinux.magic` (string) = `241.0.116.126`
209		`pxelinux.configfile` (text)	`pxelinux.configfile` (text)
210		`pxelinux.pathprefix` (text)	`pxelinux.pathprefix` (text)
211		`pxelinux.reboottime`	`pxelinux.reboottime`
212-219		Undefined	N/A
220		Subnet Allocation	Subnet allocation
221		Virtual Subnet Allocation	Virtual subnet selection
222-223		Undefined	N/A
224-254		Private Use	Private use

DHCP and IPv6

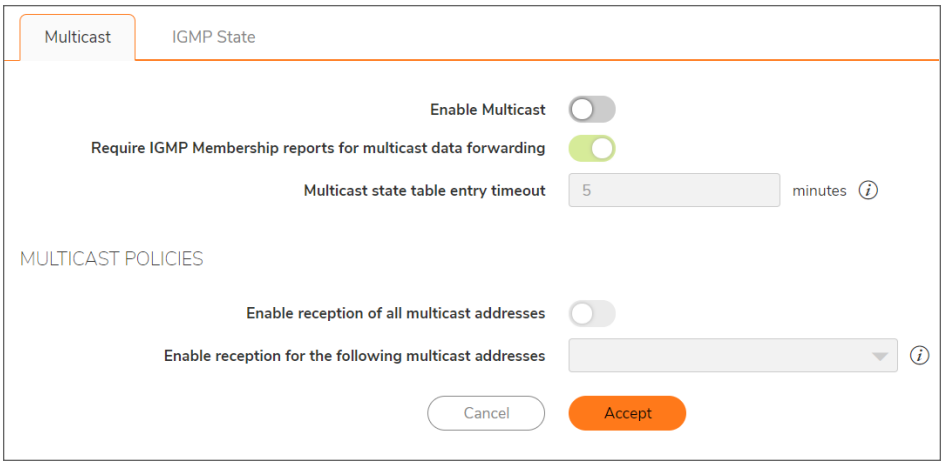
For complete information on the SonicOS implementation of IPv6, see *IPv6*.

14

Multicast

IP multicasting is a method for sending one Internet Protocol (IP) packet simultaneously to multiple hosts. Multicast is suited to the rapidly growing segment of Internet traffic - multimedia presentations and video conferencing. For example, a single host transmitting an audio or video stream and ten hosts that want to receive this stream. In multicasting, the sending host transmits a single IP packet with a specific multicast address, and the 10 hosts simply need to be configured to listen for packets targeted to that address to receive the transmission. Multicasting is a point-to-multipoint IP communication mechanism that operates in a connectionless mode - hosts receive multicast transmissions by “tuning in” to them, a process similar to tuning in to a radio.

The **NETWORK | System > Multicast** page allows you to manage multicast traffic on the firewall.



- **Enable Multicast** - Select this option to support multicast traffic. This option is not selected by default.
- **Require IGMP Membership reports for multicast data forwarding** - Select this option to improve performance by regulating multicast data to be forwarded to only interfaces joined into a multicast group address using IGMP. This option is available only if Multicast is enabled. This option is selected by default.

- **Multicast state table entry timeout (minutes)** - Set the number of minutes that the entries in the multicast table are valid, after which the table must be regenerated. This field has a default of **5**. The value range for this field is 5 to 60 (minutes). Update the default timer value in the following conditions:
  - You suspect membership queries or reports are being lost on the network.
  - You want to reduce the IGMP traffic on the network and currently have a large number of multicast groups or clients. This is a condition where you do not have a router to route traffic.
  - You want to synchronize the timing with an IGMP router.

Topics:

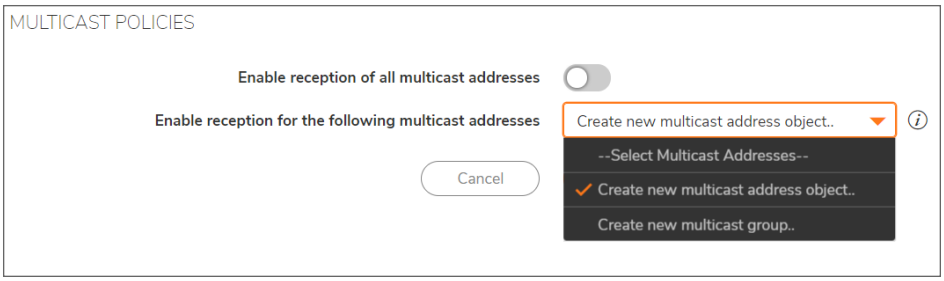
Multicast Policies

ⓘ | **TIP:** Multicast must be enabled for these options to be available.

- **Enable reception of all multicast addresses** - This radio button is not enabled by default. Select this radio button to receive all (class D) multicast addresses.

  ⓘ | **NOTE:** Receiving all multicast addresses might cause your network to experience performance degradation.

- **Enable reception for the following multicast addresses** - Select an existing multicast object/group. You can also create a new multicast object or a new multicast group to have it listed in the drop-down menu. In the drop-down menu, select **Create a new multicast address object** or **Create new multicast group.**



  ⓘ | **NOTE:** Only address objects and groups associated with the MULTICAST zone are available to select. Only addresses from 224.0.0.1 to 239.255.255.255 can be bound to the MULTICAST zone.

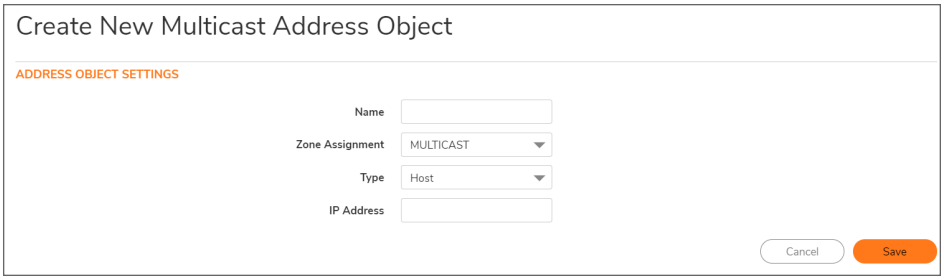
  ⓘ | **NOTE:** You can specify up to 200 total multicast addresses.

Topics:

Creating a Multicast Address Object

To create a Multicast Address Object:

1. **Enable reception for the following multicast addresses** - In the drop-down menu, select **Create a new multicast address object**. The **Create New Multicast Address Object** dialog displays.

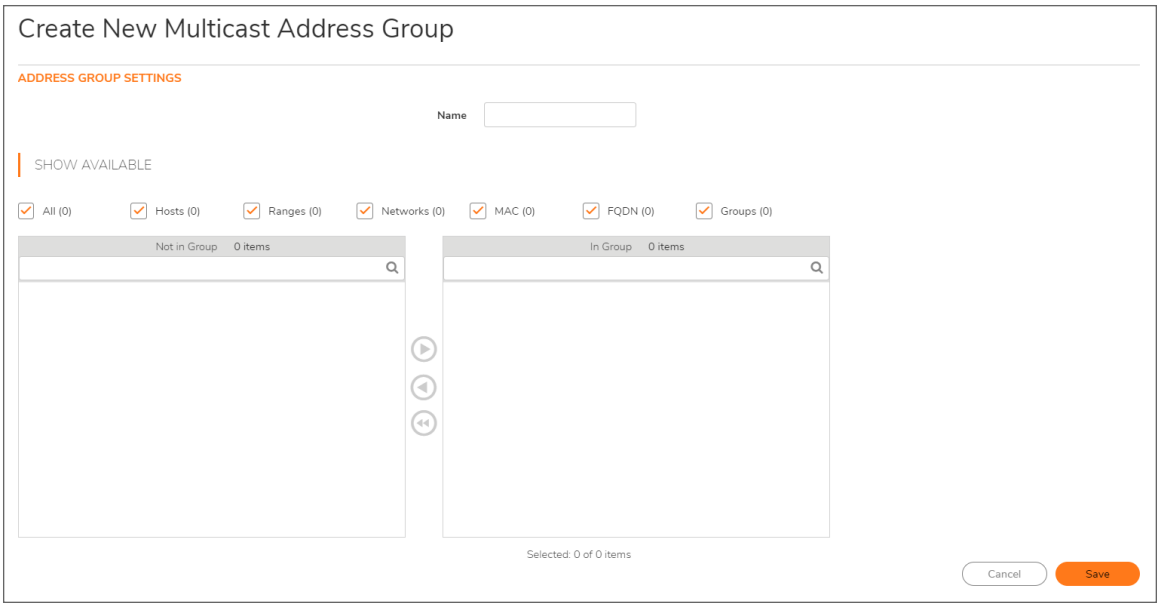


2. Configure the name of the address object in the **Name** field.
3. From the **Zone Assignment** drop-down menu, select **MULTICAST**.
4. From the **Type** drop-down menu, select Host, Range, Network, MAC, or FQDN.
5. Depending on your **Type** selection, the options on the dialog change. If you select:

Type	Option(s) displayed
Host	**IP Address** – Enter the IP address of the host or network. The IP address must be in the range for multicast: 224.0.0.0 to 239.255.255.255.
Network	• **Network** – Enter the IP address of the host or network. The IP address must be in the range for multicast: 224.0.0.0 to 239.255.255.255. • **Netmask/Prefix Length** – Enter the netmask for the network.
Range	**Starting IP Address and Ending IP Address** – Enter the starting and ending IP address for the address range. The IP addresses must be in the range for multicast: 224.0.0.1 to 239.255.255.255.
MAC	• **MAC Address** – Enter the MAC address of the host or network. • **Multi-homed Host** – Select if the MAC address is for a multihomed host. This option is selected by default.
FQDN	• **FQDN Hostname** – Enter the fully qualified domain name for the host. • **Manually set DNS entries' TTL … (120~86400s)** – Select to enter the time-to-live (TTL or hop limit) for DNS entries. This option is not selected by default. When selected, the TTL field becomes active. The range is 120 - 86400 seconds.

6. Click **Save.**

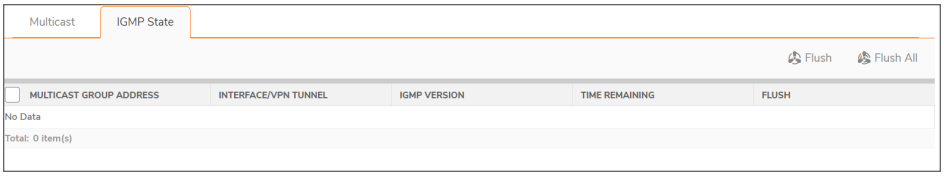
Creating a New Multicast Address Group



- Configure the name of the address group in the **Name** field.
- In **Show Available**, select options to filter IPs for All, Hosts only, Ranges only, Networks only, MACs only, FQDNs only, or existing Groups or combinations of these.
- Move the selected IPs to the right window to include the selections in the Multicast address group.
- Click **Save**.

IGMP State

This section provides descriptions of the fields in the IGMP State Table.



- **Multicast Group Address**—Provides the multicast group address the interface is joined to.
- **Interface / VPN Tunnel**—Provides the interface (such as LAN) for the VPN policy.
- **IGMP Version**—Provides the IGMP version (such as V2 or V3).
- **Time Remaining**—Provides the remaining time details.

- **Flush** — Provides an icon to flush that particular entry.
- **Flush** and **Flush All** icons—To flush a specific entry immediately, check the box to the left of the entry and click **Flush**. Click **Flush All** to immediately flush all entries.

Enabling Multicast

This section provides information on how to enable the multicast through a VPN and on a LAN dedicated interface.

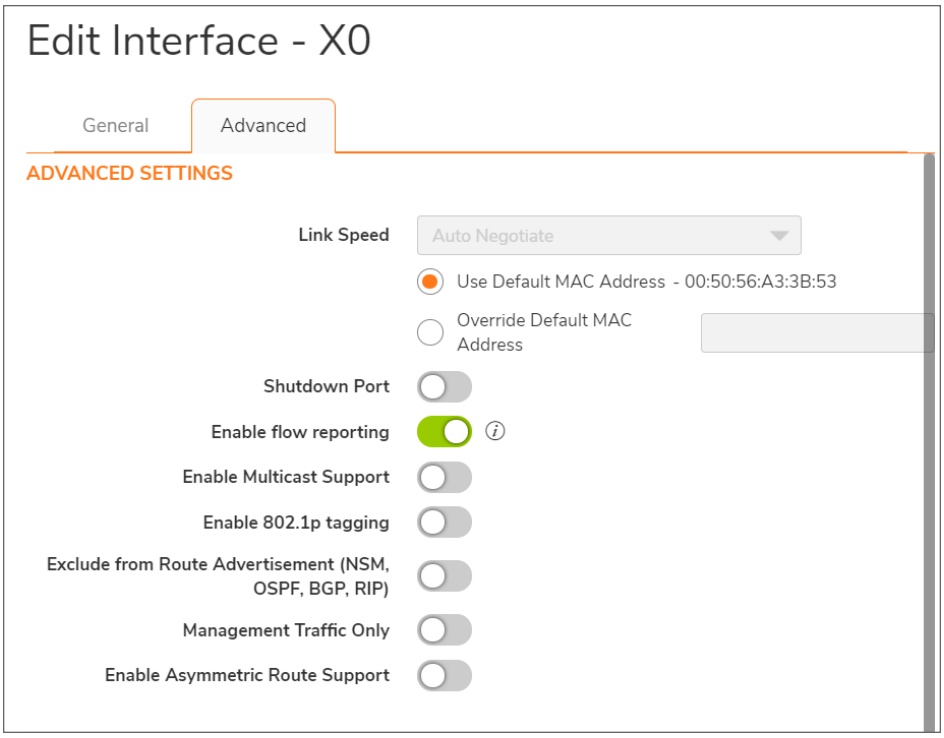
Topics:

- Enabling Multicast on a LAN-Dedicated Interface
- Enabling Multicast Support for Address Objects over a VPN Tunnel

Enabling Multicast on a LAN-Dedicated Interface

To enable multicast support on the LAN-dedicated interfaces of your firewall:

1. Navigate to **NETWORK | System > Multicast** page.
2. Under **Multicast** , select **Enable Multicast**.
3. Under **Multicast Policies**, select **Enable the reception of all multicast addresses**.
4. Click **Accept**.
5. Navigate to **NETWORK | System > Interfaces** page.
6. Click the **Edit** icon for the LAN interface you want to configure. The **Edit Interface** dialog displays.
7. Click **Advanced.**
8. Select **Enable Multicast Support**.



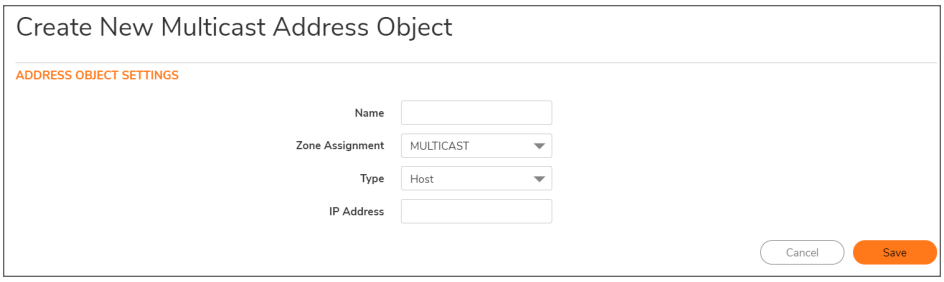
9. Click **OK**.
10. Click **Accept**.

Enabling Multicast Support for Address Objects over a VPN Tunnel

To enable multicast support for address objects over a VPN tunnel:

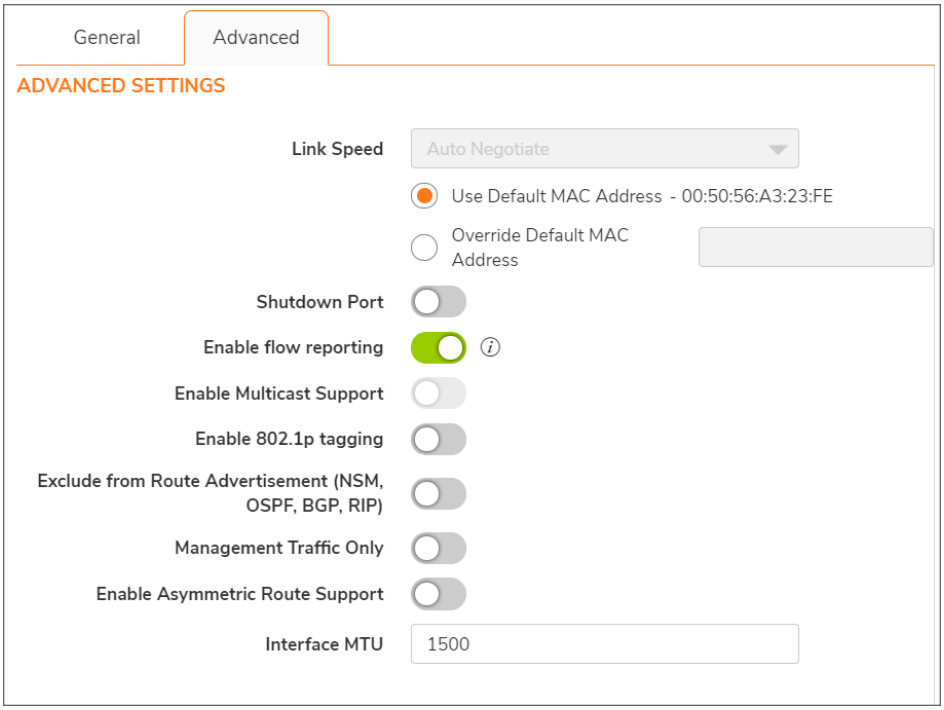
1. Navigate to **NETWORK | System > Multicast** page.
2. Under **Multicast**, select **Enable Multicast**.

3. Under **Multicast Policies**, from the **Enable the reception for the following multicast addresses** drop-down menu, select **Create new multicast address object**. The **Create New Multicast Address Object** dialog displays.



4. In the **Name** field, enter a name for your multicast address object.
5. From the **Zone Assignment** drop-down menu, select a zone: DMZ, LAN, MULTICAST, SSLVPN, VPN, WAN.
6. When you select a type from the **Type** drop-down menu, the other options change, depending on the selection. If you select:
    - **Host**: enter an IP address in the **IP Address** field.
    - **Range** : enter the starting and ending IP addresses in the **Starting IP Address** and the **Ending IP Address**field.
    - **Network**: enter the network IP address in the **Netmask** field and a netmask or prefix length in the **Netmask/Prefix Length** field.
    - **MAC**: enter the MAC address in the **MAC Address** field and select the Multi-homed host checkbox (which is selected by default).
    - **FQDN**: enter the FQDN hostname in the **FQDN Hostname** field.
7. Click **Save**.
8. Navigate to **NETWORK | System > Interfaces** page.
9. Click the **Edit** icon for the Group VPN policy you want to configure. The VPN Policy dialog displays.
10. Click **Advanced.**

11. In the **Advanced Settings** section, select **Enable Multicast Support.**



12. Click **OK.**

15

Network Monitor

The Network in the top navigation menu consists of Network Monitor services that provide a flexible mechanism for monitoring network path viability. The results and status of this monitoring are displayed dynamically on the **Network Monitor** page, and are also provided to affected client components and are logged into the system log.

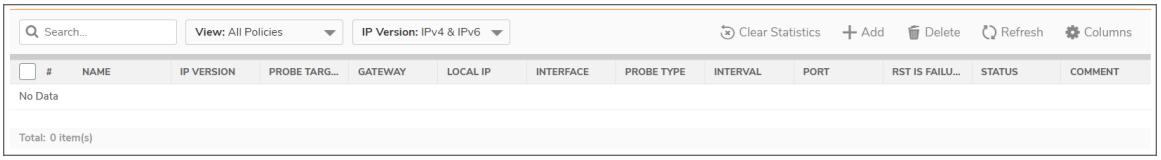
Each custom NM (Network Probe) policy defines a destination Address Object to be probed. This Address Object can be a Host, Group, Range, or FQDN. When the destination Address Object is a Group, Range, or FQDN with multiple resolved addresses, Network Monitor probes each probe target and derives the NM Policy state based on the results.

Topics:

About Network Monitor Policies

Network path performance metrics are determined using Network Monitor probes. SonicOS supports ICMP and TCP probe types. For more information, see Configuring Network Monitor Policies.

The **NETWORK | System > Network Monitor** page shows the dynamic performance data (latency/jitter/packet loss) and probe status for each path (interface) in the address object group, in both tabular and graphic displays. The display can show data for the last minute (default), last day, last week, or last month.



#	Number of the probe. The Collapse/Expand icon toggles the display of the graphs.
Name	Name of the Network Monitor Policy.
IP Version	IPv4 or IPv6

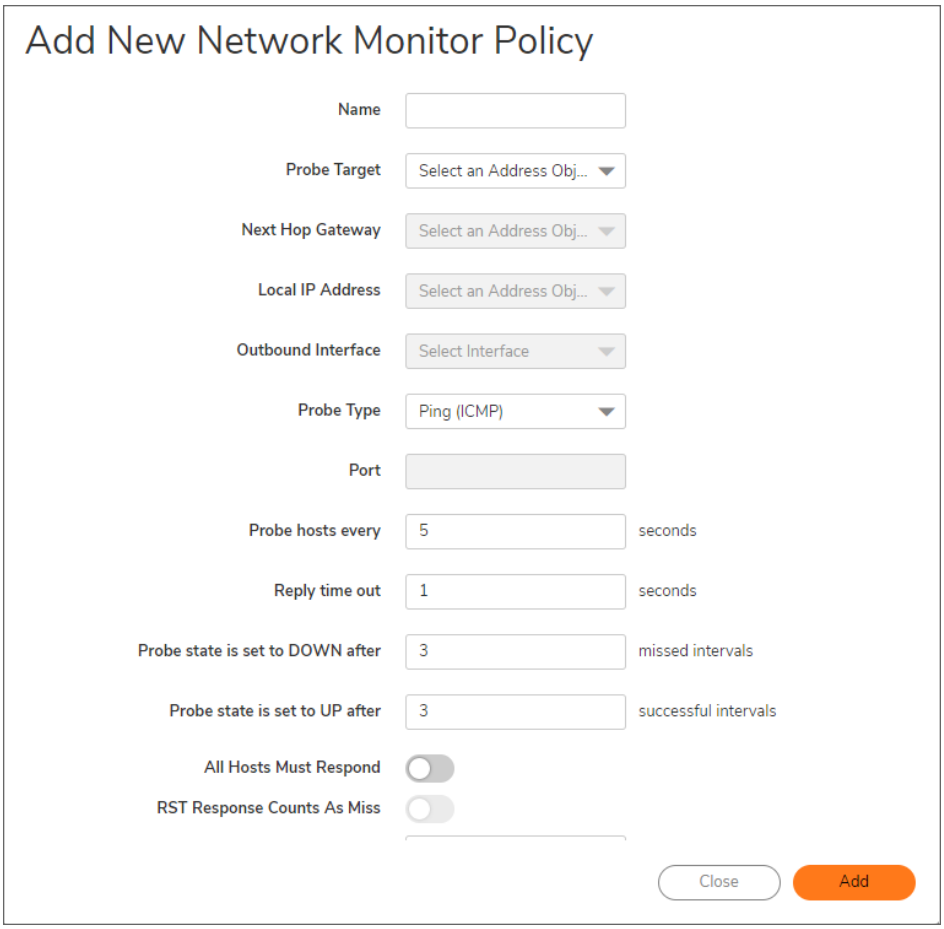
Probe Target	When logical probing is enabled, test packets can be sent to a remote probe target to verify WAN path availability.
Gateway	Gateway where the traffic originated.
Local IP	Address object you select
Interface	Round trip delay for the probes sent through a particular path/interface to reach the probe target and acknowledge back, in milliseconds. This is also displayed as a graph below the probe's entry in the Network Monitor policy table.
Probe Type	Type of network monitor: • **Ping** – Explicit Route • **TCP** – Explicit Route ⓘ **NOTE:** When - TCP – Explicit Route is selected along with the RST Response Counts as Miss field, the Port field also becomes available.
Interval	Time between SD-WAN performance probes, in seconds.
Port	Port for the SD-WAN performance probe. The minimum/maximum values are 1 to 65535. Ports are displayed only for TCP - Explicit Route probe types. A hyphen (–) displays for Ping - Explicit Route probe types.
Response Timeout	Maximum delay for a response.
Failure Threshold	Number of missed intervals before the probe state is set to DOWN.
Success Threshold	Number of successful intervals until the probe state is set to UP.
All Must Respond	Enabled or Disabled
RST Is Failure	For probe types of **TCP – Explicit Route**, whether RST responses count as misses.
Status	Shows whether the monitor is up or down.
UUID	UUID/GUID-based Client Identifier
Comment	Any comment entered when the interface was configured.

When configuring Network Monitor, default row(s) are created for each of the interfaces used by the groups established on the Network Monitor Policies screen.

Configuring Network Monitor Policies

To add a new Network Monitor policy:

1. Navigate to **NETWORK | System > Network Monitor**.
2. Click **+Add**. The **Add New Network Monitor Policy dialog** displays.



3. Enter a meaningful name in the **Name** field.
4. Select an address object from **Probe Target**.
5. From **Probe Type**, select:
   - **Ping (ICMP) - Explicit Route** (default); go to Step 7.
   - **TCP - Explicit Route**; the **Port** field and other options become available.
6. Enter the port number of the explicit route in the **Port** field.

7. Enter the interval between probes in the **Probe hosts every … seconds** field. The minimum is **1** second, the maximum is **3600** seconds, and the default is **3** seconds.

   ⓘ | **TIP:** The probe interval must be greater than the reply timeout.

8. Enter the maximum delay for a response in the **Reply time out … seconds** field. The minimum is **1** second, the maximum is **60** seconds, and the default is **1** second.
9. Enter the maximum number of missed intervals before the performance probe is set to the DOWN state in the **Probe state is set to DOWN after … missed intervals** field. The minimum number is 1, the maximum is 100, and the default is 3.
10. Enter the maximum number of successful intervals before the performance probe is set to the UP state in the **Probe state is set to UP after … successful intervals** field. The minimum number is 1, the maximum is 100, and the default is 1.
11. If you selected **TCP - Explicit Route** for **Probe Type**, the **RST Response Counts As Miss** option becomes available. Select the option to count RST responses as missed intervals. This option is not selected by default.
12. Enable or disable if you would like to force a response from all hosts with the **All Host Must Respond** option.
13. Enable or Disable **RST Response Counts As Miss** (for Probe Types of **TCP – Explicit Route**), whether RST responses count as misses.
14. Optionally, enter a comment in the **Comment** field.
15. Click **ADD**.
16. Repeat Step 3 through Step 14 to add more probes.
17. Click **Close**.

Deleting Network Monitor Policies

To delete Network Monitor Policies:

1. To delete:
   A single Network Monitor policy by:
   - Clicking its **Delete** icon in the **Configuration** column.

     A confirmation message displays.

   - Multiple Network Monitor policies by clicking their **Selection** checkboxes and then selecting **Delete**.

     A confirmation message displays.

2. Click **OK**.

16

AWS Configuration

The firewall integration with Amazon Web Services (AWS) enables Logs to be sent to AWS CloudWatch Logs, Address Objects and Groups to be mapped to EC2 Instances and VPNs created to allow connections to Virtual Private Clouds (VPCs). For an overview and links to pages describing how to use the individual firewall GUI pages, refer to the *SonicOS AWS User Guide*.

In order that the firewall can communicate with the various Application Programming Interfaces (APIs) of the Amazon Web Services (AWS), and thereby implement the integration with AWS, it is necessary to configure the firewall with the relevant AWS Security Credentials. The information required includes an AWS Identity and Access Management (IAM) User's Access Key, the corresponding Secret Access Key and a default region. The default region is used by the AWS Logs page, and for initialization of the AWS Objects and AWS VPN pages though different regions can be selected on those two pages.

AWS Security Credentials

The general features of AWS Security are beyond the scope of this article. Any AWS user should become familiar with details of AWS Identity and Access Management (IAM). Here, the focus is merely on what is needed to enable the firewall to be integrated with the AWS services that are supported by SonicOS.

IAM Group and User

IAM Identities, including Users and Groups, can be created and managed from the IAM page in the AWS Management Console.

Assuming that the AWS Account is already created and that an Administrator with either Root access or widespread privileges is logged into that account, it is then necessary to create an IAM User, if one does not already exist, that is used by the firewall to access the various AWS APIs for the services supported by the firewall.

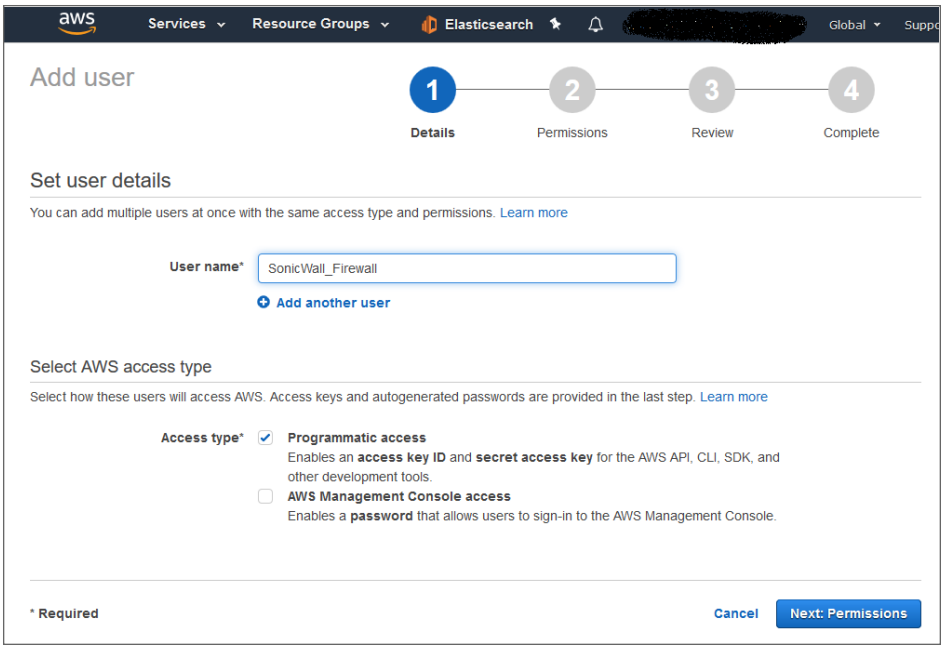
You need certain permissions to access the different services. These permissions can either be granted directly to the user or included in a security access policy assigned to an IAM Group and then the user added to that group.

The security policy used, either for a group to which the user belongs or attached to the user directly, must include the following permissions:

AmazonEC2FullAccess	For AWS Objects and AWS VPN
CloudWatchLogsFullAccess	For AWS Logs

Creating a group is described in the IAM Documentation. It is not strictly necessary to create a group; the permissions can be assigned directly to a user, however, it is common practice to define such a group so that it can be used for multiple users.

A user must be created. That user can be created specifically for use by the firewall alone. However, if the same user is going to access the AWS Management Console, the relevant checkbox must be ticked. In either case, the user must have "programmatic access."



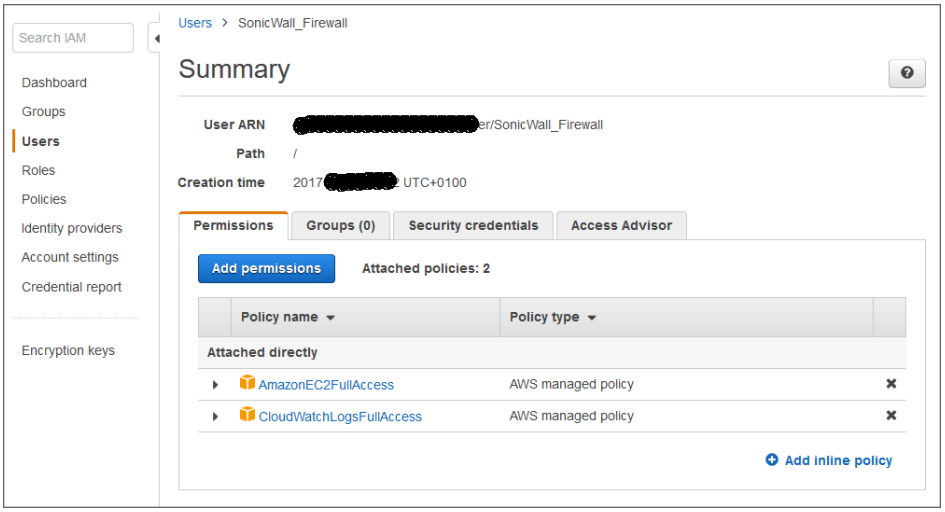
The second step of the **Add User** wizard determines which permissions the user has assigned, either through adding the user to a group or attaching the permission policies directly.

After reviewing the details of the user to be created and pressing **Create User**, there is a final and critical stage.

DO NOT LEAVE THE ADD USER WIZARD

You must retrieve the **Secret Access Key** that has been created for the user. The **Secret Access Key** together with the **Access Key** is used in the configuration of the firewall. It is needed for all API access to AWS. You should either copy it to a safe location or download the CSV file and keep that in a safe, secure location.

Finally, the newly created user with their required permissions can be seen in the IAM Users section of the AWS Console.

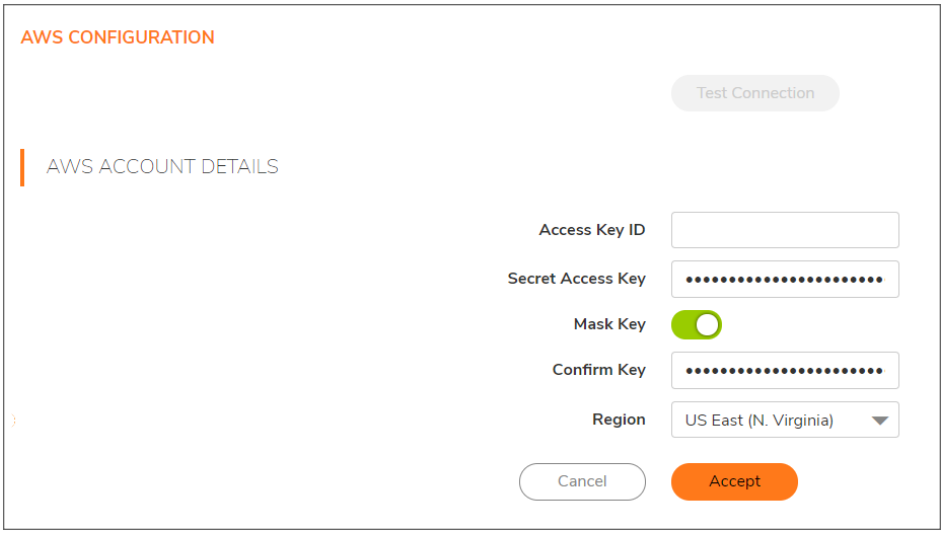


If you miss getting the Secret Access Key, it is possible to create another access Key from the User section of the IAM Console. Indeed, it is considered good practice to rotate Access Keys.

Firewall Configuration

Having obtained the Access Key and Secret Access Key for the user account that is used to enable the firewall to access the AWS APIs, the basic configuration of the firewall itself is straightforward.

1. Navigate to **NETWORK | System > AWS Configuration**.



2. Enter the **Access Key ID**, the **Secret Access Key**, **Confirm Key**, and select a default **Region**.

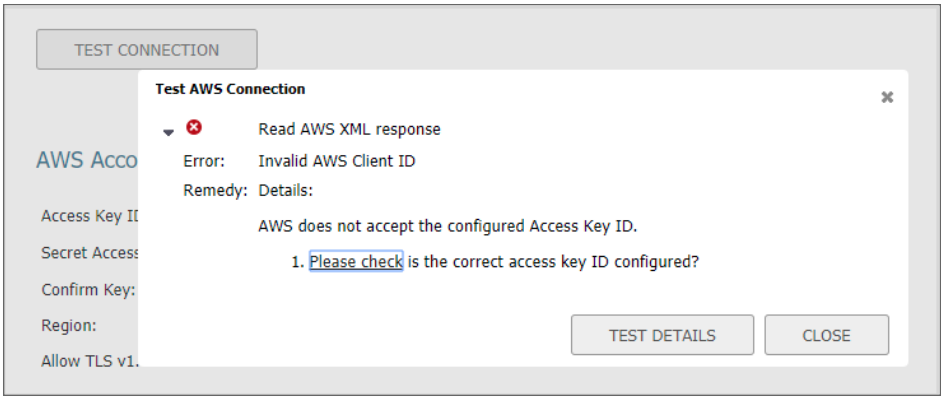
The default Region is only used for initialization of the AWS Objects and AWS VPN pages. However, it is the region that is used when sending firewall event logs to AWS CloudWatch Logs and, consequently, it is affected by changes on the **AWS Logs** page.

After all the settings have been entered, press **Accept** to save the configuration.

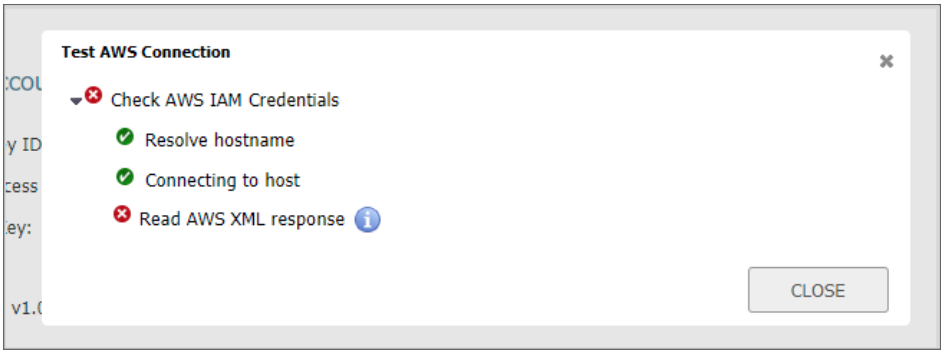
Test Connection

To test that the submitted credentials are acceptable and that the firewall can successfully communicate with AWS, press **Test Connection**. This results in a number of tests being run from the firewall with the feedback being shown.

For example, suppose an invalid Access Key had been entered, the resulting pop-up dialog would show something like this:



Clicking **Test Connection** provides more information about the tests that were conducted, highlighting the failed task.



After closing the chain of pop-up dialogs, correcting the invalid **Access Key** and saving the new configuration, the **Test Connection** can be run again. If successful, the pop-up dialog would indicate that.

The configuration of AWS credentials is now complete. You can proceed to configure the firewall to send log events to AWS Cloud Watch Logs on the AWS Logs page, map EC2 Instances to Address Objects and Groups on the AWS Objects page and connect the firewall to Virtual Private Clouds (VPCs) on the AWS VPN page.

17

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. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall Professional Services at https://sonicwall.com/pes.
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

SonicOS System Administration Guide
Updated - December 2023
Software Version - 7.1
232-005870-00 Rev A

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