SonicWall™ SonicOS 6.5.0.0

Release Notes

October 2017

These release notes provide information about the SonicWall™ SonicOS 6.5.0.0 release.

Topics:

About SonicOS 6.5.0.0

SonicWall SonicOS 6.5.0.0 is a major release that provides more than 60 new features, with multiple wireless enhancements including Access Points Floor Plan View, Topology View, Band Steering, Airtime Fairness, MiFi Extender, Captive Portal enhancements, and Device Fingerprinting and Reporting.

SonicOS 6.5 introduces support for one new firewall platform and three new wireless access point platforms. For details, see the New Hardware Support section.

The SonicOS 6.5 web management interface is completely redesigned from top to bottom with the best user experience in mind. For more information about each of the new features, see the New Features section.

Supported Platforms

SonicOS 6.5.0.0 is supported on the following SonicWall appliances:

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2650
- NSA 2600
- TZ600
- TZ500 / TZ500 Wireless
- TZ400 / TZ400 Wireless
- TZ300 / TZ300 Wireless
- SOHO Wireless

Supported Wireless Access Points

SonicOS 6.5 is supported with the following SonicWall access points:

- SonicWave 432e
- SonicWave 432i
- SonicWave 432o
-
- SonicPoint ACe
- SonicPoint ACi
- SonicPoint N2
-
- SonicPoint N Dual Radio
- SonicPoint Ne
- SonicPoint Ni
- SonicPoint Dual Band

> ⓘ **NOTE:** SonicWall GMS management of SonicWall security appliances running SonicOS 6.5.0.0 requires GMS 8.4 for management of firewalls using the new features in SonicOS 6.5.0.0.

See the New Hardware Support section for more information about the new hardware platforms supported by this release.

New Hardware Support

SonicOS 6.5 supports one new network security appliance and three new wireless access point platforms:

- NSA 2650

  The SonicWall NSA 2650 appliance addresses the growing trends in web encryption and mobility by delivering a solution that meets the need for high-speed threat prevention. The NSA 2650 features:

  - Increased port density and maximum connections
  - Increased processor speeds and counts for fast deep packet inspection performance
  - Enhanced processor architecture that aids stateful and deep packet inspections
  - Pre-populated storage module
  - Optional redundant power supply

  > ⓘ **NOTE:** SFP interfaces on the NSA 2650 currently support only 1Gb link speed.

- SonicWave 432e / 432i / 432o

  The SonicWall SonicWave Series includes two indoor platforms, one with external antennas (432e) and one with internal antennas (432i), and a third platform specifically designed for outdoor use (432o). All three SonicWave wireless access points support 802.11ac Wave 2 specifications to support higher throughputs:

- More spatial streams—4X4 multiple-input and multiple-output, (MU-MIMO) for the 802.11ac radio, where the capacity of a radio link is multiplied using multipath propagation.
- Wider channels—80 MHz-wide channels for the 802.11ac radio, while continuing to support 20 / 40 MHz channels. This allows for dynamic per packet negotiation of channel widths so that when there is interference, the SonicWave can temporarily fall back to 40 or 20MHz channels.
- More antennas—The SonicWave 432e and 432o provide four antennas for the 5 GHz radio, and four more for the 2.4 GHz radio.

> ⓘ **NOTE:** The *SonicWall SonicWave 432e and SonicWave 432i Getting Started Guide* shows frequency bands 5250-5350 MHz and 5500-5700 MHz on page 37. These frequency bands are not enabled in the current SonicWave software, but will be enabled after all regulatory approvals are obtained.

For more product information, see https://www.sonicwall.com.

New Features

This section describes the new features introduced in SonicOS 6.5.

Topics:

- Enhanced User Experience / UI Refresh
- Access Point / Wireless / 4G Features
- User and Authentication Features
- Networking Features
- Investigation Features
- Security Services Features
- Deployment and Maintenance Features
- VoIP Features
- IPv6 Features

Enhanced User Experience / UI Refresh

The SonicOS 6.5 user interface (UI) is completely redesigned and the user experience is improved, based on a SonicWall study of the biggest usability issues facing SonicOS users. While these users have different needs, their needs align with the roles they play in their company and are organized into high level tasks.

These high-level tasks are:

- **Monitor** — Dashboards and graphs provide overall status of device and traffic statistics along with threat prevention summary for overall traffic that is traversing the appliance. This is used by IT personnel and network administrators to monitor the network.
- **Investigate** — Logs, reports and some investigative tools such as packet monitor. This is used to identify and remedy a network or security incident.
- **Manage** — This is all the setup and configuration for the entire unit. It is used during initial setup, renewals, upgrades, and is where the admin can apply any remedies discovered during an investigation. The **Quick Configuration** wizards service this task as well.

The SonicOS 6.5 UI has been reorganized in accordance with these main, high-level tasks.

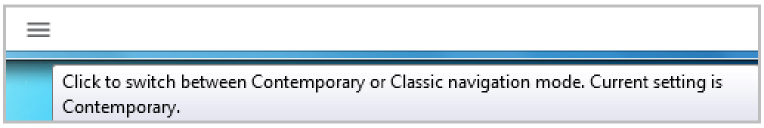
The improved user interface includes updated colors, general layout, typography, buttons, tables, tabs and numerous component styling.

Improved Navigation

The navigation is updated to support user roles and tasks. This adds a top level menu to the header, which in turn loads a relative left-hand navigation menu when clicked. Further, the items in the navigation menu have been reorganized and grouped under labels for easier navigation, some have been renamed.

The new interface provides three top-level sections, **MONITOR**, **INVESTIGATE**, and **MANAGE**, along with **QUICK CONFIGURATION** which invokes a selection of wizards. This functional breakdown makes it easier to complete tasks without switching between the top-level sections, and to determine the correct section at the start of each new task.

> **NOTE:** SonicOS 6.5 still supports classic SonicOS navigation. To switch back and forth between classic and contemporary navigation, click the settings icon ≡ located at the bottom of the left navigation pane.



≡

Click to switch between Contemporary or Classic navigation mode. Current setting is Contemporary.

Improved Dashboards

A new default **Dashboard** page is added to SonicOS 6.5. It replaces *Multi-Core Monitor* as the default dashboard. The dashboard summarizes much of the data from the Capture Threat Assessment report. This dashboard provides the “here’s what's going on, and here’s what was blocked” information needed by network security administrators. In addition, the top of the dashboard provides general system and network health information to support the administrator’s investigation tasks. Finally, the dashboard brings the wealth of security services and features available in the firewall to the forefront.

The large majority of the data relies on *Real-time Data Collection* and *Aggregate AppFlow Report Data Collection* being enabled. If one or both of these functions is not enabled, the dashboard will present some empty states.

Access Point / Wireless / 4G Features

Topics:

- Wireless Feature Support Matrix
- Access Point Floor Plan Management View
- Access Point Topology View
- RED Compliance and Certification
- Access Point Band Steering
- Wireless Device Fingerprinting and Reporting
- Access Point AirTime Fairness
- Wireless Forensic Packet Capturing
- WDS Mode / Wireless Repeater Support
- Access Point Dynamic VLAN Support
- Access Point 3G/4G/LTE MiFi Extender
- Extended Wireless SNMP MIB
- Wireless Traffic Bandwidth Utilization and Distribution Visualization

- Native Bridge Support
- Hi-Link 4G/LTE USB Modem Support

Wireless Feature Support Matrix

This matrix specifies the SonicWall access point platforms that support each wireless feature available in SonicOS 6.5.

Wireless Feature Support by Access Point Type

Feature Name	SonicWave	SonicPoint ACe/ACi	SonicPoint N2	SonicPoint Ne/Ni/NDR/N
SonicPoint BandSteering	Yes	Yes	Yes	**No**
SonicPoint AirTime Fairness	Yes	Yes	Yes	**No**
SonicPoint Wireless Forensic Packet Capturing	Yes	**No**	**No**	**No**
Wireless Built-in Radio Repeater Mode	For TZ wireless only	For TZ wireless only	For TZ wireless only	For TZ wireless only
Wireless Built-in Radio WDS Mode	For TZ wireless only	For TZ wireless only	For TZ wireless only	For TZ wireless only
SonicPoint WDS AP Support	Yes	Yes	Yes	**No**
SonicPoint Floor Plan View	Yes	Yes	Yes	Yes
SonicPoint Topology View	Yes	Yes	Yes	Yes
SonicPoint SSLVPN Concentrator	Yes	Yes	Yes	Yes
SonicPoint Real Time Monitoring Visualization	Yes	Yes	Yes	**No**
SonicPoint Dynamic VLAN	Yes	Yes	Yes	**No**
SonicPoint 3G/4G/LTE Extender	Yes	Yes	Yes	**No**
SonicPoint Client Fingerprinting and Reporting	Yes	Yes	Yes	**No**
SonicPoint SNMP MIB Extension	Yes	Yes	Yes	Yes
SonicPoint GRE management multi-core Support	Yes	Yes	Yes	Yes
SonicPoint Restful API Support	Yes	Yes	Yes	**No**
Guest Service: IP-based guest authentication bypass network	Yes	Yes	Yes	Yes
Guest Service: Cyclic quota for guest user group	Yes	Yes	Yes	Yes
Native Bridge support	Yes	Yes	Yes	Yes

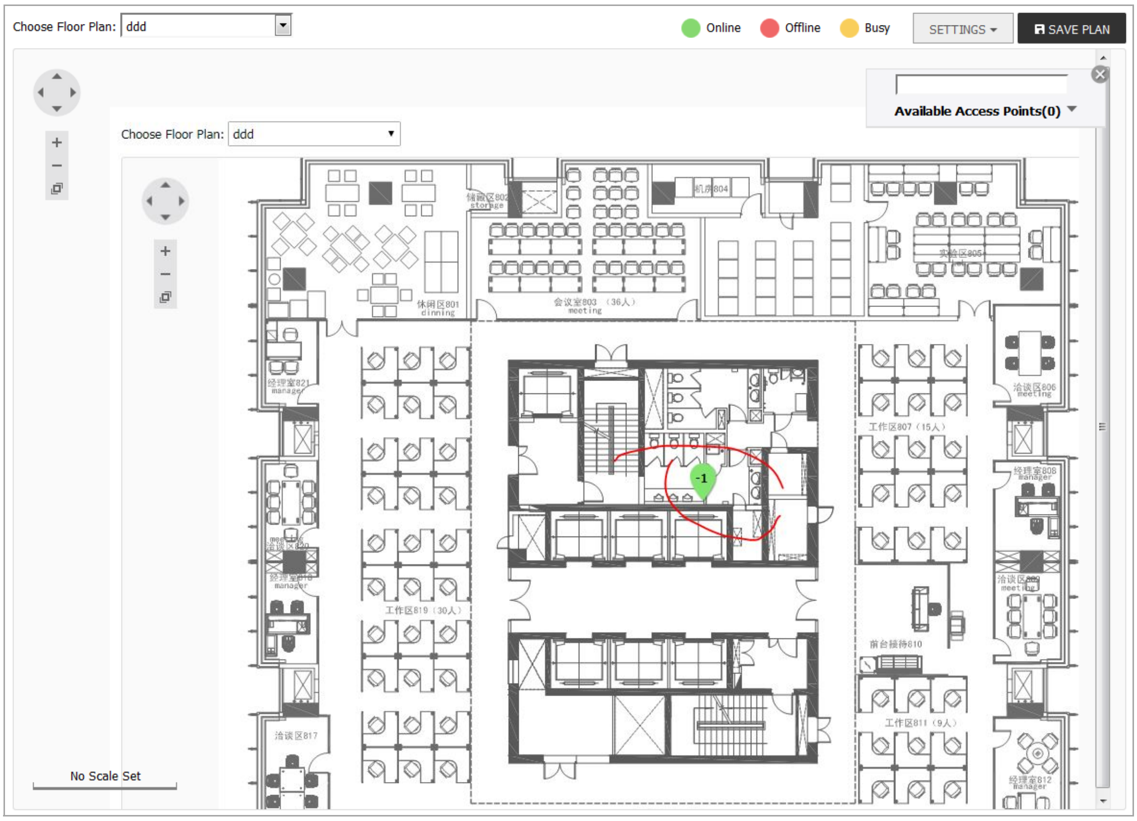
Access Point Floor Plan Management View

Floor Plan Management View in SonicOS user interface allows for a more visual approach to managing large numbers of SonicWave and SonicPoint devices. You can also track physical location and real-time status.

The Floor Plan Management View (FPMV) is an add-on to the existing wireless access point management suite in SonicOS that provides a real-time picture of the actual wireless radio deployment environment of your wireless network and improves your ability to estimate the wireless coverage of new deployments. The FPMV also provides the single-pane-of-glass console to be able to check access point statistics, monitor access point real-time status, configure access points, remove access points and even show the access point RF coverage from the consolidated the context menu.

ⓘ **NOTE:** You must first add your floor plan to SonicOS in order to use this feature.

The figure below shows a sample of a typical floor plan view.



In the FPMV, the following colors indicate the status of an access point:

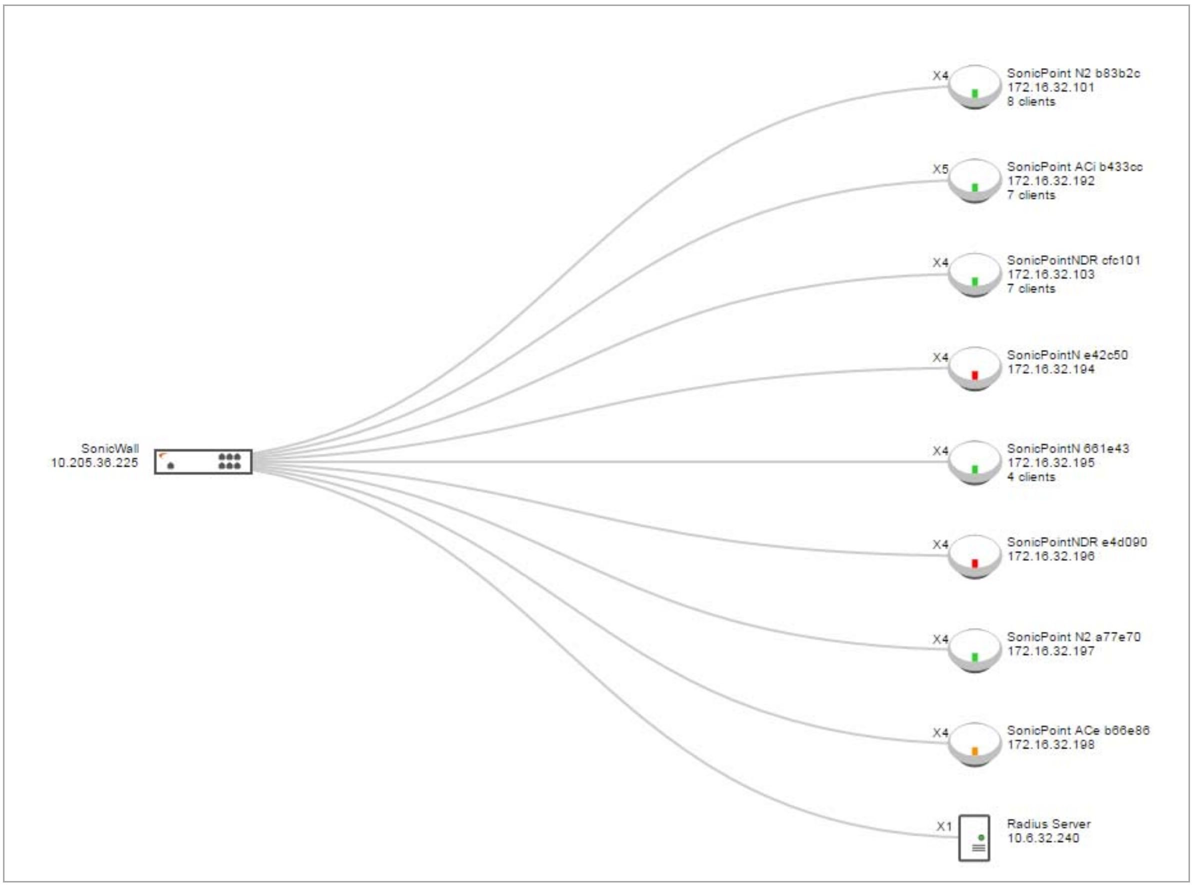
Color	Status	Definition
Green	Online	Access point is in an operational state.
Red	Offline	Access point is in initialization or non-responsive state.
Yellow	Busy	Firmware synchronization or configuration provisioning and scanning is in progress on the access point.

Access Point Topology View

Access point devices can be managed by the new Topology View feature in SonicOS 6.5. The Topology View can present the network topology from the SonicWall firewall to the wireless access point. The access point real-time status can be monitored, and the context menu also provides the access point configuration options.

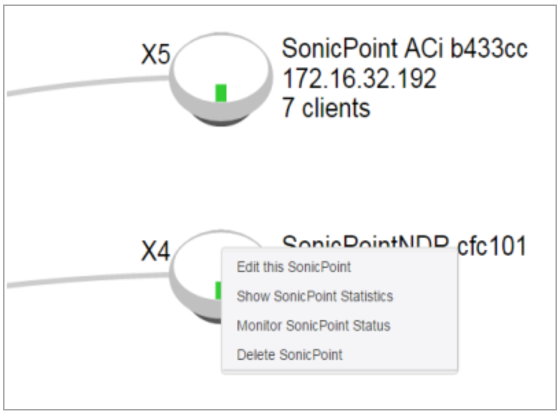
This feature shows the logical relationship among all WLAN zone devices, and provides a way to manage devices directly in the Topology View.

The **Access Points > Topology View** page displays a tree-like diagram showing connected devices known to the firewall and their relationships, similar to the figure below:



Topology View management provides a graphic presentation of the WLAN network for administrators with the most often used information and status. The devices are drawn as nodes on a tree and the tree is zoomable with the mouse and mouse wheel. Information shown in the tree includes device type, IP address, interface connected to, name, number of clients, and a simulated LED light on certain device shows working status. A tooltip bubble shows detailed information about a device.

The context menu is accessible by right-clicking on the access point ellipse-shaped icon as shown below:



RED Compliance and Certification

The SonicWall TZ and SOHO Wireless appliances and SonicWall SonicWave and SonicPoint wireless access points demonstrate compliance with the European Union's Radio Equipment Directive (RED). See the *Radio Equipment Directive (RED) Addendum* on the SonicWall Support portal under Technical Documentation:
https://www.sonicwall.com/Support/Technical-Documentation/Radio-Equipment-Directive-(RED)-Addendum

Access Point Band Steering

Band steering is implemented only for SonicWave access points in SonicOS 6.5. On the SonicWave, dual radio must be enabled with the same SSID for both radios and the VAP configuration must be the same on both radios.

Band Steering is a radio management technique to improve capacity, throughput, and the experience for users of crowded wireless networks. Usually the 5 GHz band has less interference than the 2.4 GHz band, since there are more devices that work in the 2.4 GHz band, such as microwaves and bluetooth devices.

Dual band operation with Band Steering detects wireless clients capable of 5 GHz operation and steers them to that frequency which leaves the more crowded 2.4 GHz band available for legacy clients. This helps improve end user experience by reducing channel utilization, especially in high density environments. Dual band operation with Band Steering is only available for networks with dual-band access points (those with at least 2 radios) and is configured on a per-SSID basis.

Sometimes the 2.4 GHz signal conditions or signal strength are better than 5 GHz. SonicOS provides settings on the **General** tab of the access point configuration dialog to take this into account. The available modes include **Disable**, **Auto**, **Prefer 5GHz**, **Force 5GHz** and **None**. If set to **Disable**, the Band Steering feature is disabled. The connection state is displayed, indicating whether the client is steered.

Wireless Device Fingerprinting and Reporting

This feature enhances the wireless access point station status display in SonicOS 6.5. The station physical mode information, hostname, and device type are displayed in the **Access Point Stations** page in the **MONITOR** interface. The physical mode information contains radio, channel bandwidth, and protocol. The device type information includes the client OS type and device type, such as laptop, phone or tablet.

Access Point AirTime Fairness

Air Time Fairness (ATF) gives equal amounts of air time (rather than an equal number of frames) to each client regardless of its theoretical data rate. This ensures higher download speed to the latest devices when slower devices are connected to the same access point.

802.11 standards have evolved over time. Over a decade ago, 11 Mbps was the fastest speed available over WiFi. The current 802.11ac devices provide speeds in the range of 2500 Mbps. Older, slower devices take relatively longer times to transmit and receive data compared to faster and newer devices. This gives less time to faster devices and disproportionately longer times to slow transmitting devices. Similar behaviors in air time can be observed if a device is farther away from an access point relative to other clients.

To enable Air Time Fairness:

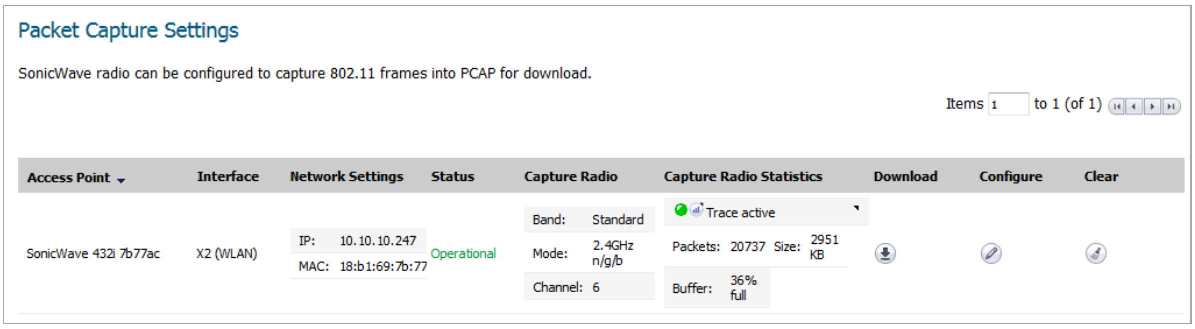
1. In the **MANAGE** interface, navigate to **Connectivity |Access Points > Base Settings**.
2. Under **SonicPoint / SonicWave Provisioning Profiles**, click the Configure button for the **SonicWave** profile or another (custom) **SonicWave** profile.
3. On the **Radio 0 Advanced** or **Radio 1 Advanced** tab, select the **Enable Air Time Fairness** checkbox.

Wireless Forensic Packet Capturing

The Wireless Forensic Packet Capturing feature provides an in-depth type of wireless troubleshooting that you can use to gather wireless data from a client site and output the captured information into a readable file format. Wireshark™ can be used to read the file.

> **NOTE:** Because the antenna of the scan radio is 1x1, some data frames cannot be captured by the scan radio due to hardware restrictions.

A new **Packet Capture** page is added to the SonicOS 6.5 management interface under **Access Points** for this feature. The capture view on the **Access Points > Packet Capture** page shows the status of the access point, the number of packets captured, and the size of the packet buffer. At the right, the **Configure** column provides buttons you can click to configure the capture settings for each access point.



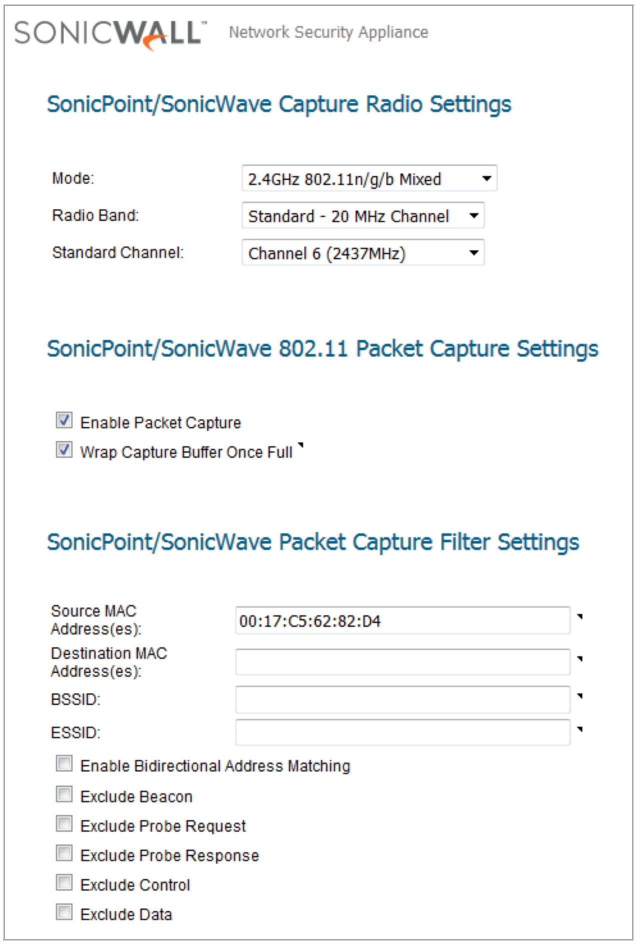
Packet Capture Settings

SonicWave radio can be configured to capture 802.11 frames into PCAP for download.

Items 1 to 1 (of 1)

Access Point	Interface	Network Settings	Status	Capture Radio	Capture Radio Statistics	Download	Configure	Clear
SonicWave 432i 7b77ac	X2 (WLAN)	IP: 10.10.10.247 MAC: 18:b1:69:7b:77	Operational	Band: Standard Mode: 2.4GHz n/g/b Channel: 6	Trace active Packets: 20737 Size: 2951 KB Buffer: 36% full			

You can configure the mode, band and channel settings in the configuration dialog, allowing you to capture wireless packets in a specific channel. You can configure up to five source and destination MAC addresses.



SONICWALL Network Security Appliance

SonicPoint/SonicWave Capture Radio Settings

Mode: 2.4GHz 802.11n/g/b Mixed

Radio Band: Standard - 20 MHz Channel

Standard Channel: Channel 6 (2437MHz)

SonicPoint/SonicWave 802.11 Packet Capture Settings

☑ Enable Packet Capture

☑ Wrap Capture Buffer Once Full

SonicPoint/SonicWave Packet Capture Filter Settings

Source MAC Address(es): 00:17:C5:62:82:D4

Destination MAC Address(es):

BSSID:

ESSID:

☐ Enable Bidirectional Address Matching

☐ Exclude Beacon

☐ Exclude Probe Request

☐ Exclude Probe Response

☐ Exclude Control

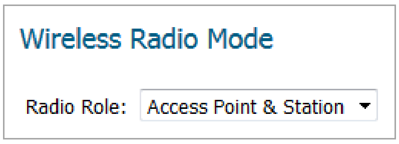
☐ Exclude Data

To capture the data for one of configured access point radios, click the **Download** button for that row on the **Access Points > Packet Capture** page. The capture file is named with the format, “wirelessCapture_[SW name].cap”, where “SW name” is the SonicWall access point name. Wireshark™ can be used to read the file.

WDS Mode / Wireless Repeater Support

The Wireless Distribution System (WDS) is supported on all SonicWall wireless TZ and SOHO platforms, as well as on all SonicWave and SonicPoint access points.

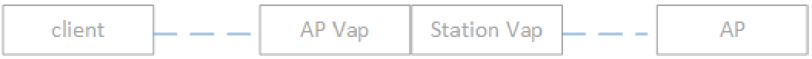
When two or more hosts need to connect to each other over the IEEE 802.11 protocol and the distance is too long for a direct connection to be established, a wireless repeater is used to bridge the gap. WDS Mode support allows SonicWall TZ Wireless and SOHO Wireless appliances to work in repeater mode with a new **Radio Role** mode called **Access Point & Station**, which supports Access Point mode and Station mode at the same time. This is configured on the **Wireless > Base Settings** page.



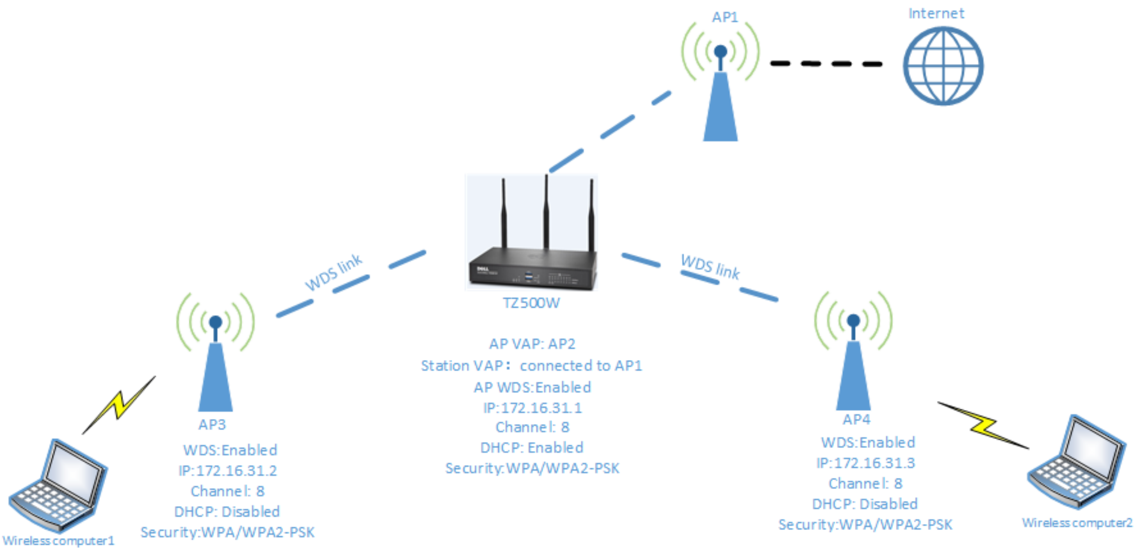
Wireless Radio Mode

Radio Role: Access Point & Station

While in **Access Point & Station** mode, one virtual access point (VAP) functions as a normal wireless access point, and another VAP is created as the *station*, which connects to the other wireless access point or appliance (a TZ/SOHO wireless or SonicWave/SonicPoint access point). In this mode, you can also set the virtual interface which the station VAP uses as the WAN interface.



WDS allows you to connect multiple access points. With WDS, access points communicate with one another without wires in a standardized way. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required.



You can enable WDS mode for an access point by selecting the **Enable WDS AP** checkbox in the **Wireless > Base Settings** page or in the SonicWave/SonicPoint **Radio 0/1 Advanced** configuration. On the TZ or SOHO Wireless appliance, the **Enable Station Mode** and **Enable WDS Station** settings are available for configuring station mode.

WDS mode requires the wireless client, the AP that the wireless client is connected to, the WDS station, and the WDS AP to all be in the same subnet.

Access Point Dynamic VLAN Support

In SonicOS 6.5, the Access Point Dynamic VLAN feature supports a very flexible deployment in which wireless clients can connect to the same SSID, but still be assigned unique VLAN IDs and IP subnets which have different security service offerings. The same SSID can be shared and broadcast by multiple access points connected to the same SonicWall firewall.

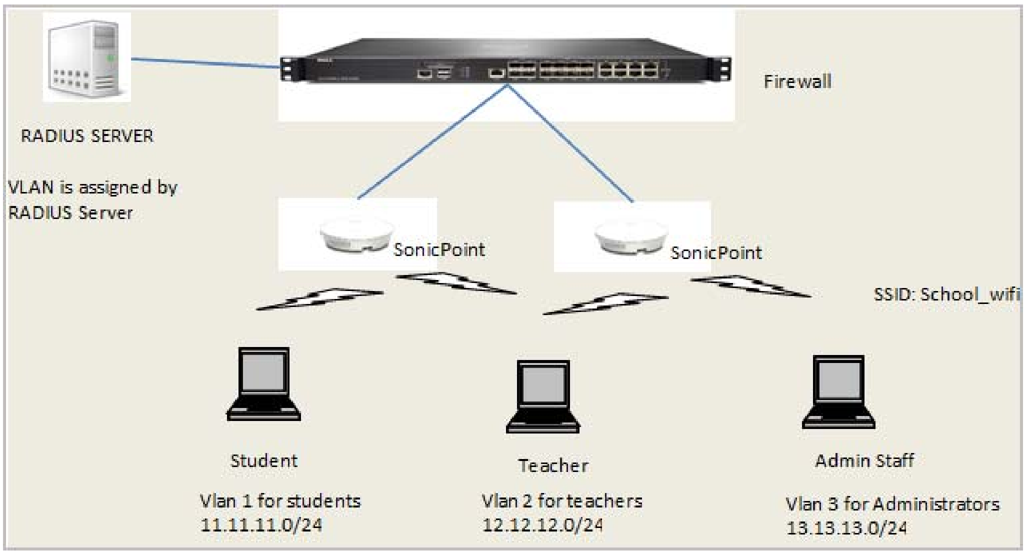
Dynamic VLAN is supported on all SonicWall firewalls running SonicOS 6.5 with the following access points:

- SonicWave 432e / 432i / 432o
- SonicPoint ACe / ACi / N2

The RADIUS Server takes the central control role in assigning wireless clients to various VLAN IDs and subnets according to the wireless client user login ID, user group membership, and RADIUS server policy. In previous

SonicOS versions, the WLAN service provider must create multiple dedicated SSIDs to offer the same services individually.

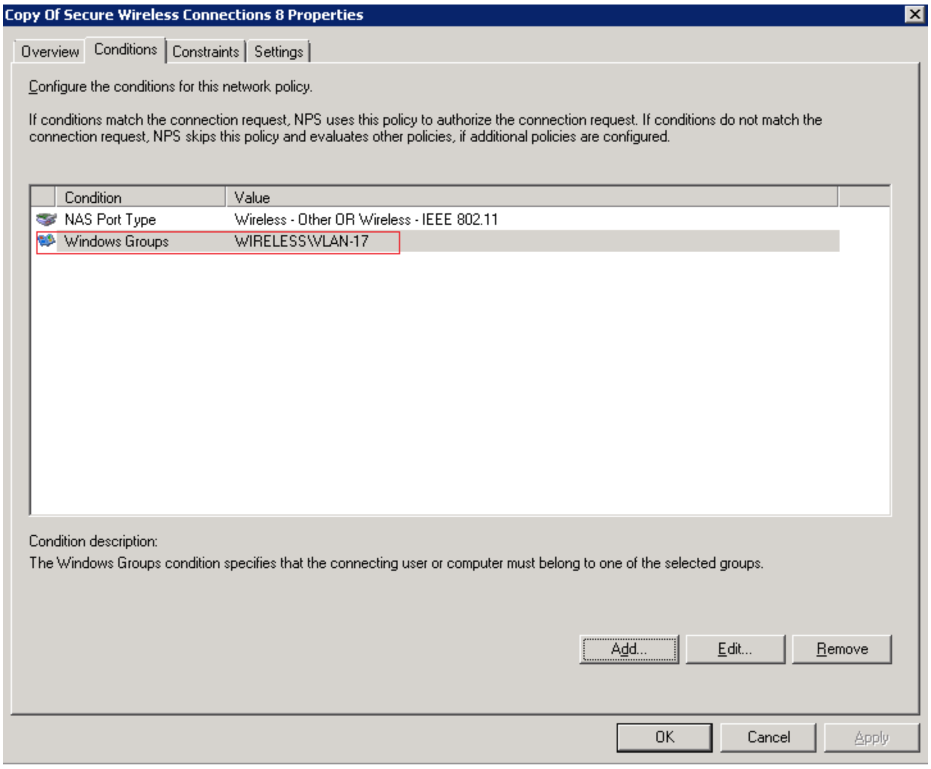
For example, a school could broadcast a single SSID such as *School_wifi*. Students, teachers, and administration staff connect to that same SSID, and the RADIUS server assigns them to different zones/subnets by their login ID.


RADIUS SERVER
Firewall
VLAN is assigned by RADIUS Server
SonicPoint
SonicPoint
SSID: School_wifi
Student
Teacher
Admin Staff
Vlan 1 for students 11.11.11.0/24
Vlan 2 for teachers 12.12.12.0/24
Vlan 3 for Administrators 13.13.13.0/24

RADIUS Server Configuration

This feature depends on correct configuration of the RADIUS server, along with the host Windows Server configuration. The examples below show key points of the network policy configuration in Windows Server 2008.

- Add user group for the network policy:



Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

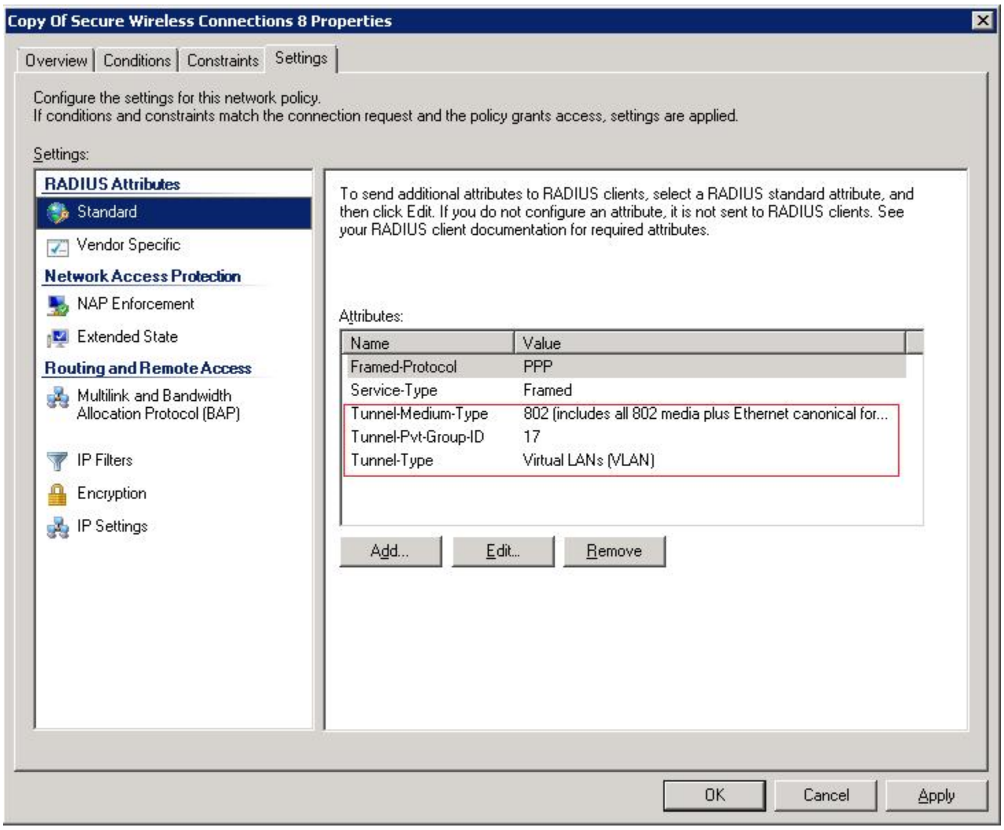
Condition	Value
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11
Windows Groups	WIRELESS\VLAN-17

Condition description:
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

- Configure Tunnel Type, Tunnel Medium Type and Tunnel Private Group ID for the network policy. The Tunnel-Private-Group-ID Attribute will be included in the Access-Request packet if authentication comes from a user in the group.

  The RADIUS server assigns a VLAN ID to a user using the following Tunnel attributes:

  - IETF 64 (Tunnel Type) - Set this to VLAN.
  - IETF 65 (Tunnel Medium Type) - Set this to 802.
  - IETF 81 (Tunnel Private Group ID) - Set this to VLAN ID.



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	17
Tunnel-Type	Virtual LANs (VLAN)

SonicOS Configuration

On the firewall, the configuration includes VLAN interface configuration, access point radio Dynamic VLAN configuration, and VAP Dynamic VLAN configuration.

Virtual interfaces should be configured in advance for the Dynamic VLAN IDs. Each VLAN ID can only be used once, either for one VAP object or one radio.

Radio Dynamic VLAN Configuration

When Dynamic VLAN is enabled on a radio, Virtual Access Point settings are disabled for the radio. A Dynamic VLAN list must be configured for the radio. Dynamic VLANs for radio 0 should not overlap with those for radio 1.

To configure access point radio Dynamic VLAN settings:

1. In the **MANAGE** view, navigate to **Connectivity | Access Points > Base Settings**.
2. Scroll down to the **SonicPoint / SonicWave Objects** section and click the Configure button for the access point you wish to configure.
3. On the **General** screen, scroll down to the **Dynamic VLAN ID Assignment** section.
4. Select the **Enable Dynamic Vlan ID Assignment for Radio 0** checkbox (or the checkbox for Radio 1).

ⓘ **NOTE:** Dynamic VLAN can only be configured when the Authentication Type is EAP.

5 Click the **EDIT** button next to the checkbox.

6 In the **Edit Dynamic VLAN ID** dialog, use the arrow buttons to move the desired VLANs from the **VLANs not in the list** box to the **VLANs included in the list** box.

7 Click **OK**.

VAP Dynamic VLAN Configuration

Dynamic VLAN can be enabled for each Virtual Access Point (VAP). When Dynamic VLAN is enabled for a VAP, VLAN ID settings are disabled. VLAN IDs should not overlap those of VAPs in the same group.

To configure VAP Dynamic VLAN settings:

1 In the **MANAGE** view, navigate to **Connectivity | Access Points > Virtual Access Point**.

2 Scroll down to the **Virtual Access Points** section and click **ADD** to display the **Add/Edit Virtual Access Point** dialog.

3 On the **General** screen, select the **Enable Dynamic Vlan ID Assignment** checkbox.

ⓘ **NOTE:** You can only select the option if Authentication Type is EAP.

4 Click the **EDIT** button next to the checkbox.

5 In the **Add/Edit Dynamic VLAN ID** dialog, use the arrow buttons to move the desired VLANs from the **VLANs not in the list** box to the **VLANs included in the list** box.

6 Click **OK**.

Access Point 3G/4G/LTE MiFi Extender

A MiFi is a mobile wireless hotspot. In SonicOS 6.5, the SonicPoint 3G/4G/LTE MiFi Extender feature allows SonicWall wireless access points to connect into 3G or 4G cellular networks and create a wireless hotspot that can be shared among mobile devices such as smartphones, laptops, and tablets. This WWAN solution allows multiple end users and mobile devices to share a 3G or 4G mobile broadband internet connection.

To use this feature, you plug a USB device into the SonicWave or SonicPoint and it then connects to the internet over 3G/4G. In SonicOS, you bind a VLAN Interface to the USB modem.

This feature is supported on all SonicWall firewalls running SonicOS 6.5 and all SonicWave and SonicPoint access points with USB interfaces. A USB device that supports 3G (PPP), 4G (Hi-Link), or the QMI protocol is required.

Use the following settings for the VLAN configuration:

- Set the Zone to WAN.
- Set the parent interface to the physical interface to which access points are connected.
- For a 3G USB modem, the IP Assignment should be Static, and assign a private IP address to it. Leave the gateway and DNS servers fields blank, they will be filled automatically after the provisioning for the access point is completed.
- For 4G and QMI Modem, the IP Assignment should be DHCP. It will get the DHCP lease from the USB modem server after the modem is connected.

This feature uses connection profiles provided by the SonicOS 3G/4G module. Go to the **Connectivity | 3G/4G Modem** pages to add the right profiles for the 3G USB modem being used.

To configure the access point:

1 In the **MANAGE** view, navigate to **Connectivity | Access Points > Base Settings**.

2 Under **SonicPoint / SonicWave Objects**, click the Configure button for the access point you wish to use.

3 Click the **3G/4G/LTE WWAN** button.

> ⓘ **NOTE:** You can click the **3G/4G/LTE WWAN WIZARD** button at the bottom of this page to have the wizard assist you in creating or selecting a VLAN interface and a 3G/4G/LTE connection profile.

4 Select the **Enable 3G/4G/LTE Modem** checkbox.

5 Select the VLAN you created for the USB device from the **Bound to WAN VLAN Interface** drop-down list.

6 To use a specific connection profile, select the **Enable Connection Profile** checkbox and fill in the related fields. In many cases, the default connection profile can be used, in which case this step is optional.

7 Click **OK**.

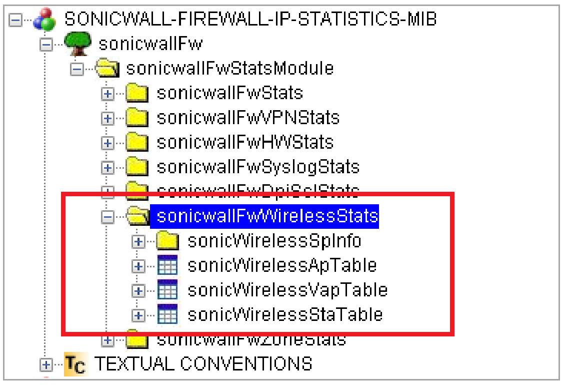
The settings are pushed to the access point. You can view basic status in the **MANAGE** view on the **Connectivity | Access Points > 3G/4G/LTE WWAN** page.

When multiple access points and 3G/4G modems (at least two for each) are available, SonicOS can make use of them simultaneously and perform load balancing among them. First, assign a unique VLAN to each SonicPoint and modem pair. Then add these VLAN interfaces to a LB group on the **System Setup | Network > Failover & Load Balancing** page.

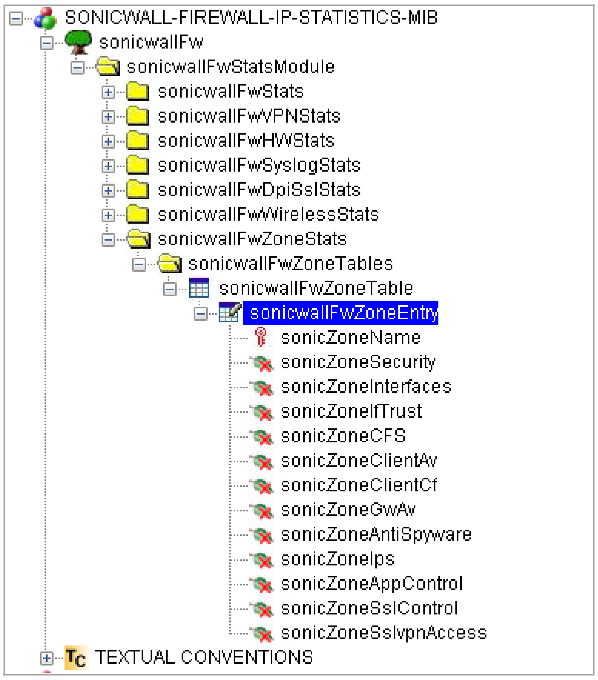
Extended Wireless SNMP MIB

The SNMP MIB for SonicOS 6.5 includes new elements for wireless access points and zone monitoring and reporting. SNMPv2C is supported.

SONICWALL-FIREWALL-IP-STATISTICS-MIB.MIB is extended by adding wireless and zone OIDs, specifically by adding scalars of wirelessSpInfo and three tables: sonicWIrelessApTable, sonicWirelessVapTable and sonicWirelessStaTable.



SONICWALL-FIREWALL-IP-STATISTICS-MIB.MIB is extended by adding the zone table: sonicwallFwZoneTable.



- SONICWALL-FIREWALL-IP-STATISTICS-MIB
  - sonicwallFw
    - sonicwallFwStatsModule
      - sonicwallFwStats
      - sonicwallFwVPNStats
      - sonicwallFwHWStats
      - sonicwallFwSyslogStats
      - sonicwallFwDpiSslStats
      - sonicwallFwWirelessStats
      - sonicwallFwZoneStats
        - sonicwallFwZoneTables
          - sonicwallFwZoneTable
            - sonicwallFwZoneEntry
              - sonicZoneName
              - sonicZoneSecurity
              - sonicZoneInterfaces
              - sonicZoneIfTrust
              - sonicZoneCFS
              - sonicZoneClientAv
              - sonicZoneClientCf
              - sonicZoneGwAv
              - sonicZoneAntiSpyware
              - sonicZoneIps
              - sonicZoneAppControl
              - sonicZoneSslControl
              - sonicZoneSslvpnAccess
  - TEXTUAL CONVENTIONS

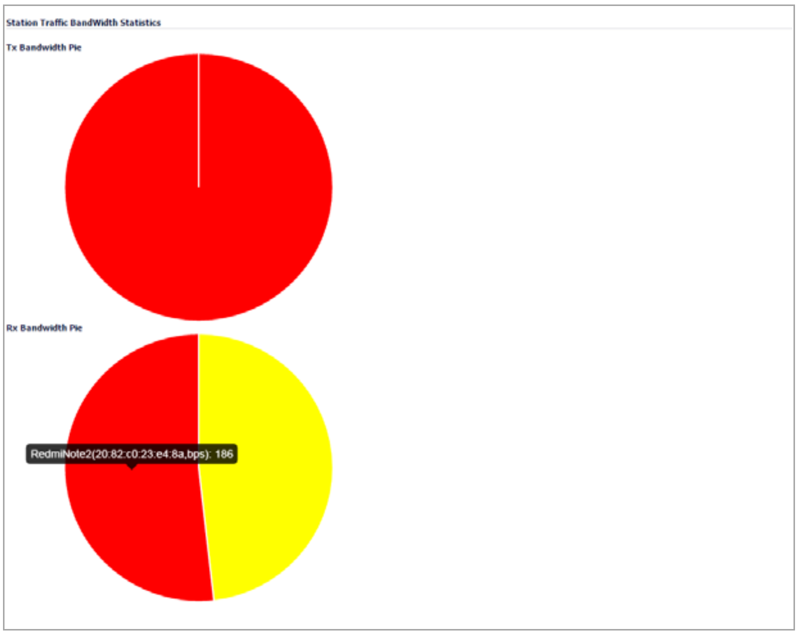
Wireless Traffic Bandwidth Utilization and Distribution Visualization

This feature enhances the current access point traffic distribution and utilization presentation feature to display the stations' real time traffic bandwidth. It can display information from different stations of one access point or from different access points. This feature allows you to see the proportional station traffic information in the graphical display.

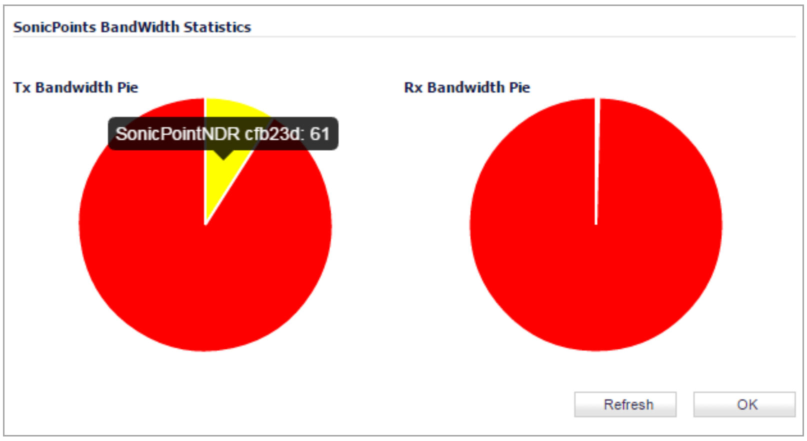
No new options or settings are introduced with this feature. It is supported on SonicOS 6.5 with all SonicWave and SonicPoint access points.

The Bandwidth display includes two different factors:

- The bandwidth rate of different wireless client stations connected to the same access point; two client stations are shown in the example below. The station represented by red is using all the transmission bandwidth and about half of the received bandwidth.


Station Traffic BandWidth Statistics
Tx Bandwidth Pie
Rx Bandwidth Pie
RedmiNote2(20:82:c0:23:e4:8a,bps): 186

- The bandwidth rate of different access points connected to the same firewall; two SonicPoints are shown in the example below:

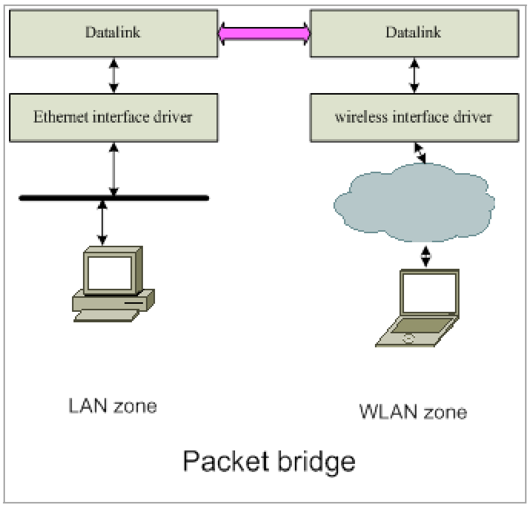


Click on the picture to display the SonicPoint information.

Native Bridge Support

SonicOS 6.5 introduces Native Bridge Mode to support multiple bridges between the WLAN and other zones, and allows the WAN zone to be a native bridge host for bridging traffic to other zones.

In Layer 2 bridging, if two hosts belong to the same subnet, a Layer 2 network device such as a SonicWall firewall can connect these two hosts. The network device bridges the packets from one host to another. This type of packet bridging works, for example, if the wireless interface and LAN ethernet interface are assigned to the same subnet.



Previous versions of SonicOS provide L2 Bridge and Portshield support to provide some extent of Layer 2 bridging among LAN, WAN and other applicable zones. TZ Wireless and SOHO Wireless appliances support the WLAN Layer2 bridge feature. However, the WLAN Layer 2 bridge feature permits clients connected to the TZ/SOHO internal wireless to share an IP subnet with only LAN and DMZ zones, and only one-to-one Layer2 bridging is supported.

With Native Bridging, you can bridge multiple virtual WLAN interfaces and virtual LAN interfaces together, and bridge between more than just WLAN and LAN/DMZ zones.

In this release, only WLAN, DMZ, and LAN zone interfaces and unassigned interfaces are supported for Native Bridge mode. WAN zone interfaces are not allowed to join a Native Bridge as a *member*, but other interfaces can be native-bridged to a WAN interface, making the WAN interface a Native Bridge host. The Native Bridge feature works with WLAN zones on TZ/SOHO Wireless appliances and on all SonicWall platforms with a SonicWave or SonicPoint wireless access point.

A new **IP Assignment** is added to support this feature, called ***NativeBridge Mode***. An interface placed into this mode becomes a NativeBridge member interface of the native bridge. The resulting bridge members and host work like a multi-port bridge with full Layer 2 transparency, and all IP traffic that passes through can be configured to be, or not to be, subjected to full stateful and deep-packet inspection.

You can select **NativeBridge Mode** on a WLAN, DMZ, or LAN zone interface or on an unassigned interface. As this mode is a pure Layer 2 bridge scheme, after **NativeBridge Mode** is selected, the zone value of, for example, WLAN is changed to *unassigned*. This WLAN interface inherits the zone settings and IP settings of the native bridge *host* and becomes a native bridge *member*. You can configure **IP Assignment** to **NativeBridge Mode** when editing an interface in the **MANAGE** view, on the **System Setup | Network > Interfaces** page.

Hi-Link 4G/LTE USB Modem Support

SonicOS 6.5 implements a new *Hi-Link* interface to work with the newer 4G/LTE USB modems.

4G/LTE USB modem vendors are implementing Hi-Link mode to provide an Ethernet interface with a direct IP address for the host operating system, allowing the host OS to use the standard IP protocol to access the USB internal web server, fetch the dynamic IP address, manage the USB modem device, establish the connection to the high speed 4G/LTE network, and monitor device status as well as data usage. Previously, PPP was used widely by legacy 3G USB modem devices to establish a direct connection to the cellular mobile network. With the 4G/LTE high speed technology, PPP is no longer suitable.

When a Hi-Link USB modem is plugged into a SonicWall firewall, SonicOS detects the model and displays the U0 interface in the **MANAGE** view, **System Setup | Network > Interfaces** page. A dedicated **4G/LTE** page is displayed and allows the user to access modem configuration settings. To use the modem, connect the USB device to the network by clicking the **Connect** button in the **Connection Manager**.

The U0 4G/LTE interface belongs to the WAN zone by default and can be used in **Network > Failover & Load Balancing**. The USB modem WAN interface address and DNS address are assigned by the ISP's DHCP server. SonicOS uses this DHCP IP address for the U0 interface IP address.

User and Authentication Features

Topics:

- Authentication Partitioning / Multi-LDAP
- RADIUS Accounting Client Support
- Captive Portal Authentication
- Cyclic Quota for Guest User Group
- IP-Based Guest Authentication Bypass Network

Authentication Partitioning / Multi-LDAP

SonicOS 6.5 introduces support for user authentication partitioning and multiple LDAP servers. Authentication partitioning and multiple LDAP servers are supported on NSA 2650, NSA 3600 and above, and on SuperMassive platforms. Authentication partitioning is a high-end feature that is only relevant in networks that are big enough to encompass multiple Active Directory forests.

User authentication partitioning provides a mechanism for LDAP, RADIUS, and/or Single-Sign On (SSO) authentication in an environment where you manage multiple non-interconnected domains. Such an environment needs users in a particular domain to be authenticated via the specific:

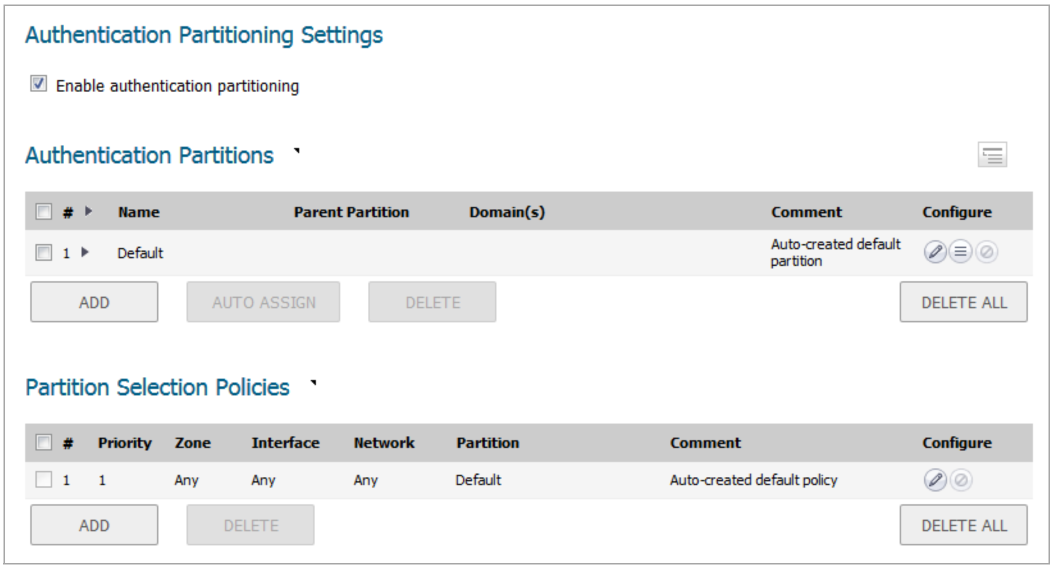
- LDAP/RADIUS server for that domain
- SSO agent(s) located in that domain

User authentication partitioning means:

- First, partitioning your network(s) into separate partitions, each with its own authentication servers/agents/clients
- Then, authenticating each user against the relevant servers/agents/clients according to the authentication partition in which the user is located

An authentication partition typically corresponds to one or more domains; for example, in a Windows domain, a partition usually corresponds to an Active Directory forest. Each partition has separate LDAP servers, RADIUS servers, SSO agents, and/or Terminal Service agents (TSAs).

In the **MANAGE** view, a new **System Setup | Users > Partitions** page is added in SonicOS 6.5.



Authentication Partitioning Settings

☑ Enable authentication partitioning

Authentication Partitions

□	#	Name	Parent Partition	Domain(s)	Comment	Configure
□	1	Default			Auto-created default partition	

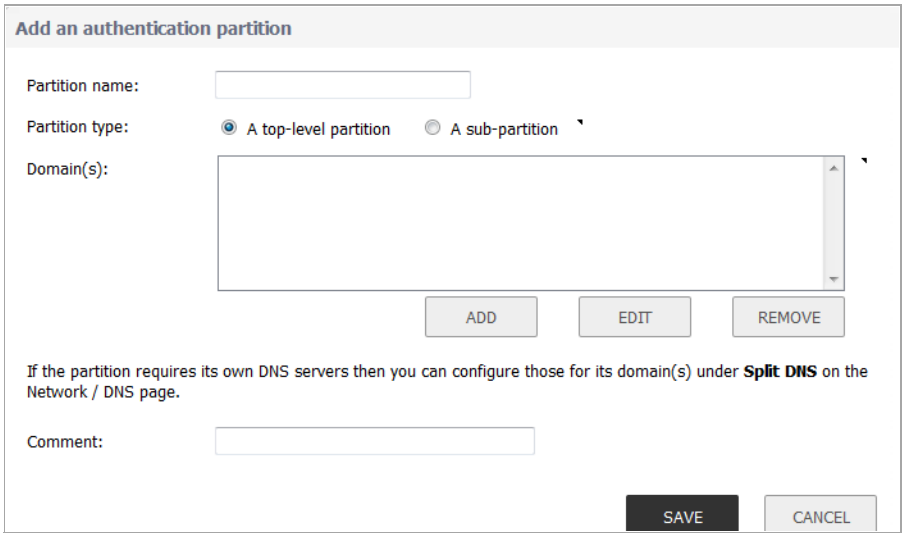
Partition Selection Policies

□	#	Priority	Zone	Interface	Network	Partition	Comment	Configure
□	1	1	Any	Any	Any	Default	Auto-created default policy	

The partitions configured under **Authentication Partitions** control which authentication servers are used for which users, where those users are in different network partitions.

The policies configured under **Partition Selection Policies** define the selection of the above partitions based on the physical location of users being authenticated. When authenticating users whose domain names are not available for matching against those in the above partitions, the users' partitions are selected based on their physical locations as set by these policies. These policies are also used for auto-assigning authentication devices to partitions based on physical location of the devices.

By clicking **ADD** under **Authentication Partitions**, you can add either a top level partition or a sub-partition.



Add an authentication partition

Partition name:

Partition type: ● A top-level partition ○ A sub-partition

Domain(s):

If the partition requires its own DNS servers then you can configure those for its domain(s) under **Split DNS** on the Network / DNS page.

Comment:

Authentication partitions select the LDAP servers, RADIUS servers, SSO agents, and TSAs used to authenticate particular users. In addition to assigning the servers and agents to a partition, it may be necessary to assign certain of them to different subsets of the users in the partition. ***Sub-partitions*** allow assigning particular agents for certain subsets of a partition's users if specific ones need to be used for them. If an authentication partition is set as a sub-partition of another one, then agents specific to the top level, or parent, authentication partition's users can be assigned to the sub-partition. The sub-partition's agents are used when relevant, but the servers and agents of the parent partition can be used as appropriate.

Multiple primary LDAP servers can be configured, one for each authentication partition, plus a list of additional servers for each. More than two RADIUS servers can also be configured.

When adding an authentication server or SSO/Terminal Services/RADIUS Accounting agent in the **Users > Settings** page, you must select the authentication partition if more than one partition is configured.

Multiple authentication partitions will usually require using different DNS servers to resolve the host names in the different partitions. In SonicOS 6.5, the ***Split DNS*** feature is separated from ***DNS Proxy*** to accommodate this configuration. The **Split DNS** configuration is moved from the **DNS Proxy** page to the main **Network > DNS** page. DNS servers configured in **Split DNS** are now used directly for DNS lookups of host names in internal domains.

RADIUS Accounting Client Support

SonicOS 6.5 introduces RADIUS Accounting Client support, which allows you to track accounting information from user sessions and associate network resource usage that is necessary for the billing process. The SonicOS implementation follows the RADIUS accounting client specification in RFC 2866.

After a user authenticates successfully, SonicOS sends an Accounting Start message to the RADIUS accounting server if it is configured. The Accounting Start message describes the type of service and the user being connected to the firewall. At intervals, SonicOS then sends an Accounting Interim message to periodically update the server with user session information. When the user session terminates, SonicOS sends an Accounting Stop message, along with a code indicating the reason that the session ended.

To enable and configure RADIUS Accounting for clients:

1. In the **MANAGE** view, navigate to **System Setup | Users > Settings**.
2. On the **Accounting** screen, select the **Send RADIUS Accounting information** checkbox. The page changes to display more settings.
3. If no RADIUS Accounting server is configured, click **ADD** to add one. The RADIUS Accounting server is configured separately from any RADIUS Authentication server.
4. Configure other options as desired, and then click **ACCEPT**.

Captive Portal Authentication

Captive Portal Authentication is a new feature in SonicOS 6.5 which allows users to gain access after being authenticated and authorized by a Network Authentication/Authorization Server (NAS). A user who seeks web access to a network is redirected to the authentication web login page hosted on the captive portal server that is integrated with the RADIUS server.

This authentication method is an extension to SonicWall Lightweight Hotspot Messaging (LHM) support. LHM deployment requires all authentications to be handled by an external LHM server. With Captive Portal Authentication, there is no need to set up an LHM server, but uses the SonicWall firewall itself to communicate with the RADIUS Server to complete the authentication process.

Captive Portal Authentication is available on all platforms running SonicOS 6.5.

This feature provides the following major components:

- **Internal Captive Portal Authentication** – SonicOS provides an internal captive portal authentication portal and vendor URL, so you can easily add your desired portal content into the SonicOS authentication page. This way, you can focus on the portal page content and leave the rest of the authentication framework to SonicOS. When a user accesses the URL in a browser, the web page is redirected to the SonicOS authentication page with the Captive Portal content embedded.
- **External Captive Portal Authentication** – SonicOS provides an external captive portal authentication vendor URL, so you can host all captive portal pages in your own portal server without SonicOS authentication page leverage. This method gives you more flexibility in portal page design and management. However, you need to be sure to post the required information (user name and password) back to the SonicWall firewall for authentication. When a user accesses the URL in a browser, the web page is redirected to the external captive portal page and parameters are dynamically added to the URL so that the portal server receives the firewall identification along with the user identification and initial landing URL being requested.

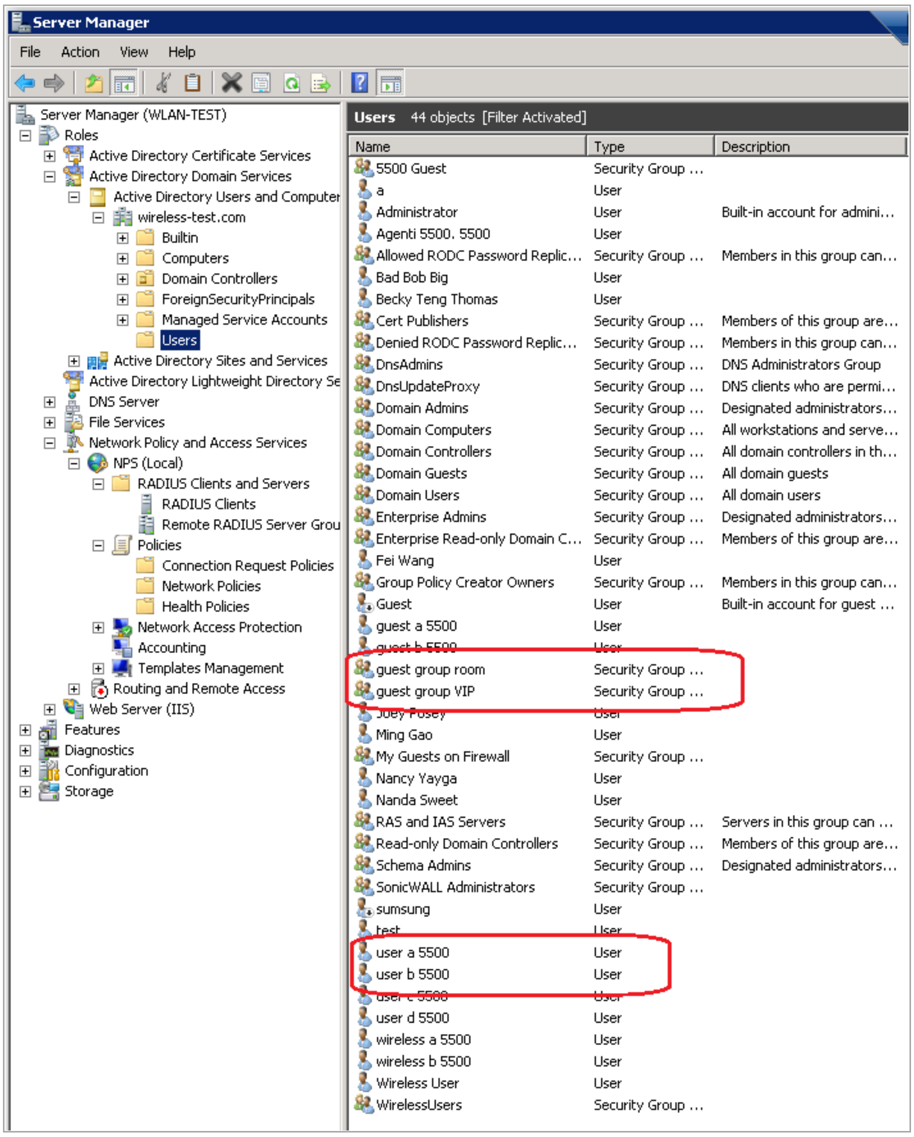
- **RADIUS server API** – SonicOS defines the interface for the RADIUS server to communicate with SonicOS to pass the URL, idle time out, and session time out information back to the firewall. This allows SonicOS to control the login session and run central session management from the RADIUS Server side for highly efficient deployment.

Portal and RADIUS Server Configuration

This feature depends on the correct configuration of the portal server, RADIUS server, and firewall.

The Portal server hosts web pages based on configuration of either internal or external captive portal URL. The Portal server decodes and processes user information passed in from SonicOS, including the client IP address, MAC address, firewall identifier, and firewall management URL. A guest account must be created on the RADIUS server with this information before authentication.

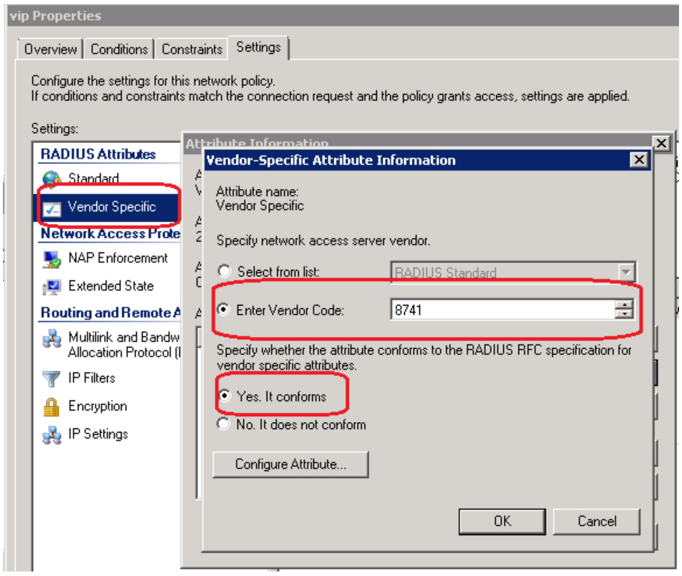
The RADIUS server must have the user information and user group information. The group name is returned to SonicOS with the ACCEPT message. The group name has to match a group name configured on the firewall which has guest privileges.


Server Manager
File
Action
View
Help
Server Manager (WLAN-TEST)
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Users and Computer
wireless-test.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Active Directory Sites and Services
Active Directory Lightweight Directory Se
DNS Server
File Services
Network Policy and Access Services
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Grou
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Templates Management
Routing and Remote Access
Web Server (IIS)
Features
Diagnostics
Configuration
Storage

Users 44 objects [Filter Activated]

Name	Type	Description
5500 Guest	Security Group ...	
a	User	
Administrator	User	Built-in account for admini...
Agenti 5500. 5500	User	
Allowed RODC Password Replic...	Security Group ...	Members in this group can...
Bad Bob Big	User	
Becky Teng Thomas	User	
Cert Publishers	Security Group ...	Members of this group are...
Denied RODC Password Replic...	Security Group ...	Members in this group can...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators...
Enterprise Read-only Domain C...	Security Group ...	Members of this group are...
Fei Wang	User	
Group Policy Creator Owners	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
guest a 5500	User	
guest b 5500	User	
guest group room	Security Group ...	
guest group VIP	Security Group ...	
Joey Posey	User	
Ming Gao	User	
My Guests on Firewall	Security Group ...	
Nancy Yayga	User	
Nanda Sweet	User	
RAS and IAS Servers	Security Group ...	Servers in this group can ...
Read-only Domain Controllers	Security Group ...	Members of this group are...
Schema Admins	Security Group ...	Designated administrators...
SonicWALL Administrators	Security Group ...	
sumsung	User	
test	User	
user a 5500	User	
user b 5500	User	
user c 5500	User	
user d 5500	User	
wireless a 5500	User	
wireless b 5500	User	
Wireless User	User	
WirelessUsers	Security Group ...	

Idle timeout and **session timeout** are attributes supported on RADIUS. These must be configured on the RADIUS server if they are to be returned in the ACCEPT message. The **Welcome URL** is a Vendor Specific attribute in RADIUS.



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Attribute name:
Vendor Specific

Specify network access server vendor.

○ Select from list: RADIUS Standard

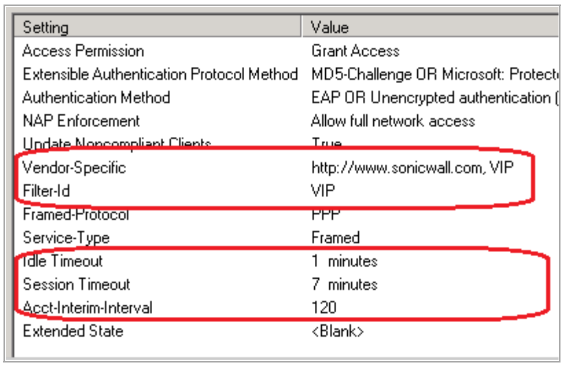
● Enter Vendor Code: 8741

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

● Yes. It conforms

○ No. It does not conform

If RADIUS Accounting is supported, the **interim interval** attribute must be set in the RADIUS server.



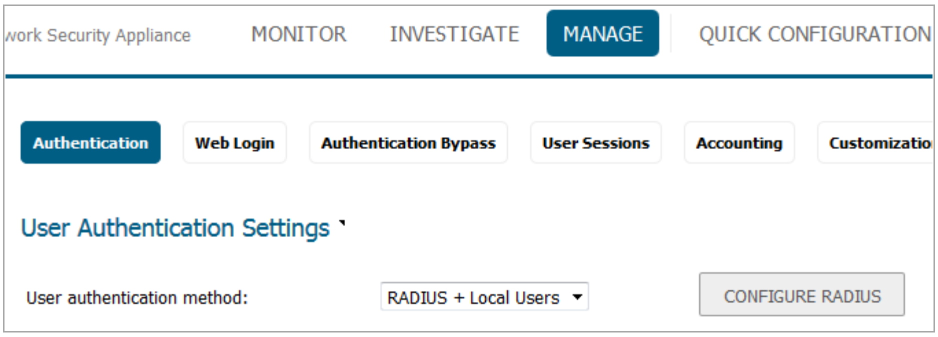
Setting	Value
Access Permission	Grant Access
Extensible Authentication Protocol Method	MD5-Challenge OR Microsoft: Protect
Authentication Method	EAP OR Unencrypted authentication (
NAP Enforcement	Allow full network access
Update Noncompliant Clients	True
Vendor-Specific	http://www.sonicwall.com, VIP
Filter-Id	VIP
Framed-Protocol	PPP
Service-Type	Framed
Idle Timeout	1 minutes
Session Timeout	7 minutes
Acct-Interim-Interval	120
Extended State	<Blank>

Prior to SonicOS 6.5, the **idle timeout**, **session timeout**, and **interim interval** RADIUS attributes were not supported by SonicOS. The **welcome URL** is not a default RADIUS attribute; its attribute number is defined as 5, and the SonicWall vendor code is 8741. The values of these attributes can be configured in SonicOS. If they are configured, SonicOS does not get them from the RADIUS server.

SonicOS Configuration

To configure the RADIUS server:

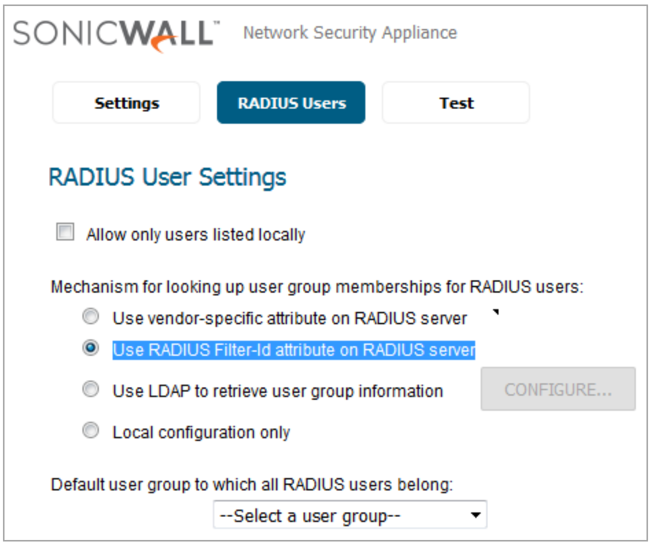
1 In the **MANAGE** view, navigate to **System Setup | Users > Settings**.



User Authentication Settings

User authentication method: RADIUS + Local Users

2 Select the **Use RADIUS Filter-Id attribute on RADIUS server** option.



RADIUS User Settings

□ Allow only users listed locally

Mechanism for looking up user group memberships for RADIUS users:

○ Use vendor-specific attribute on RADIUS server
● Use RADIUS Filter-Id attribute on RADIUS server
○ Use LDAP to retrieve user group information
○ Local configuration only

Default user group to which all RADIUS users belong: --Select a user group--

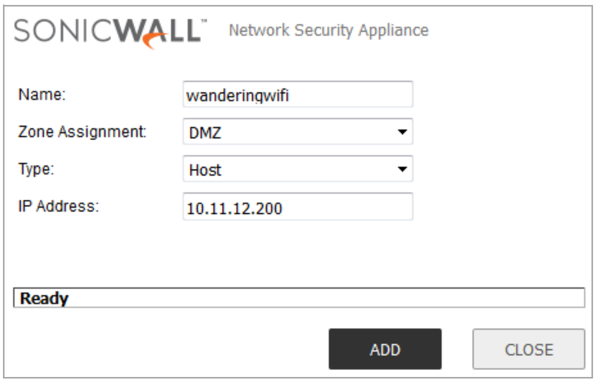
RADIUS attributes are configured along with the Captive Portal settings under **Guest Services**.

SonicOS uses an address object for the portal in the Guest Services configuration.

To configure the Portal URL address object:

1 In the **MANAGE** view, navigate to **Policies | Objects > Address Objects** and click **Add**.

2 Fill in the fields in the **Add Address Object** dialog and click **OK**.



Name: wanderingwifi
Zone Assignment: DMZ
Type: Host
IP Address: 10.11.12.200

Ready

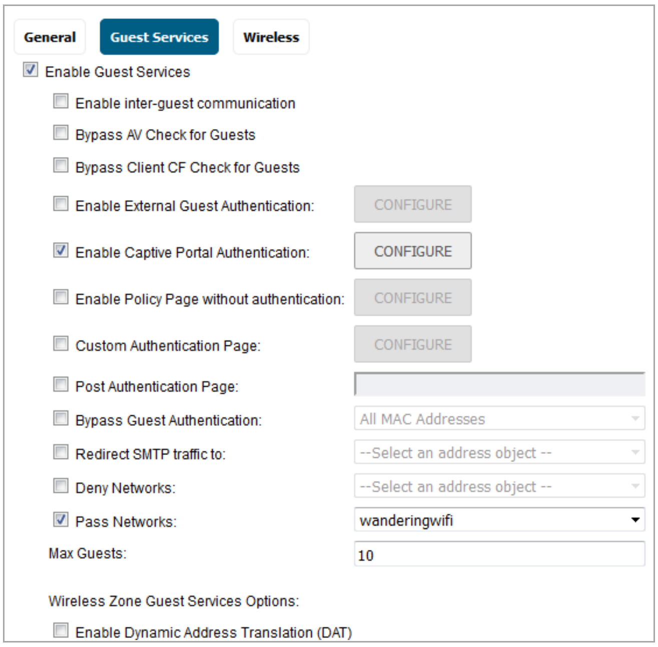
Captive Portal settings are configured under **Guest Services**.

To configure the Captive Portal settings:

1 In the **MANAGE** view, navigate to the **System Setup | Network > Zones** page.

2 Click the Configure button for the zone you want to configure, such as **WLAN**.

3 On the **Guest Services** tab, select the **Enable Guest Services** checkbox.



☑ Enable Guest Services

□ Enable inter-guest communication

□ Bypass AV Check for Guests

□ Bypass Client CF Check for Guests

□ Enable External Guest Authentication: CONFIGURE

☑ Enable Captive Portal Authentication: CONFIGURE

□ Enable Policy Page without authentication: CONFIGURE

□ Custom Authentication Page: CONFIGURE

□ Post Authentication Page:

□ Bypass Guest Authentication: All MAC Addresses

□ Redirect SMTP traffic to: --Select an address object --

□ Deny Networks: --Select an address object --

☑ Pass Networks: wanderingwifi

Max Guests: 10

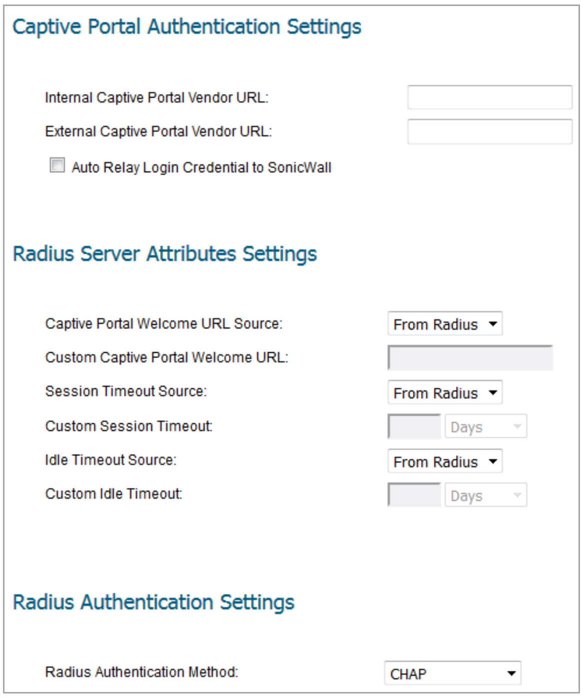
Wireless Zone Guest Services Options:

□ Enable Dynamic Address Translation (DAT)

4 Select the **Enable Captive Portal Authentication** checkbox.

5 For **Pass Networks**, select the address object for the portal, such as ***wanderingwifi***.

6 Click the **CONFIGURE** button next to the **Enable Captive Portal Authentication** checkbox. The **Customize Login Page** dialog is displayed.



Captive Portal Authentication Settings

Internal Captive Portal Vendor URL:

External Captive Portal Vendor URL:

□ Auto Relay Login Credential to SonicWall

Radius Server Attributes Settings

Captive Portal Welcome URL Source: From Radius

Custom Captive Portal Welcome URL:

Session Timeout Source: From Radius

Custom Session Timeout: Days

Idle Timeout Source: From Radius

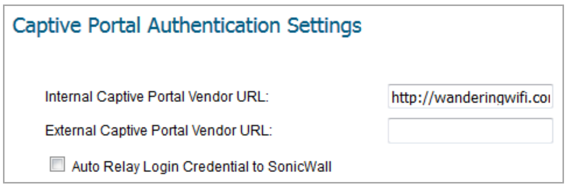
Custom Idle Timeout: Days

Radius Authentication Settings

Radius Authentication Method: CHAP

7 In the **Customize Login Page** dialog, enter the portal URL in one of the following fields:

- **Internal Captive Portal Vendor URL** – Enter the URL, such as **http://wanderwifi.com**.



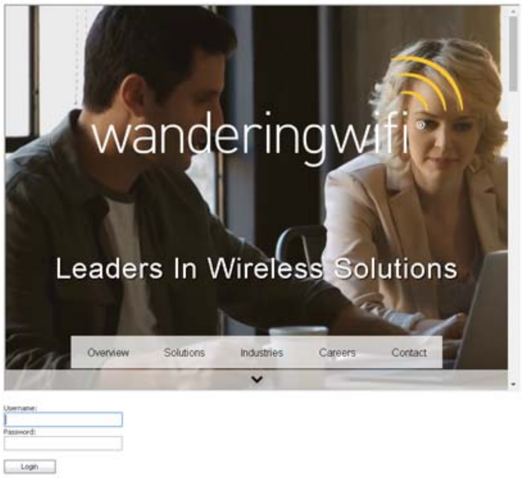
Captive Portal Authentication Settings

Internal Captive Portal Vendor URL: http://wanderingwifi.co

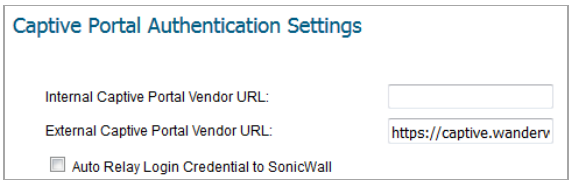
External Captive Portal Vendor URL:

□ Auto Relay Login Credential to SonicWall

This URL is displayed in an iframe to the firewall's authentication page as below.



- **External Captive Portal Vendor URL** – Enter the URL, such as **https://captive.wanderwifi.com**.



Captive Portal Authentication Settings

Internal Captive Portal Vendor URL:

External Captive Portal Vendor URL: https://captive.wanderv

□ Auto Relay Login Credential to SonicWall

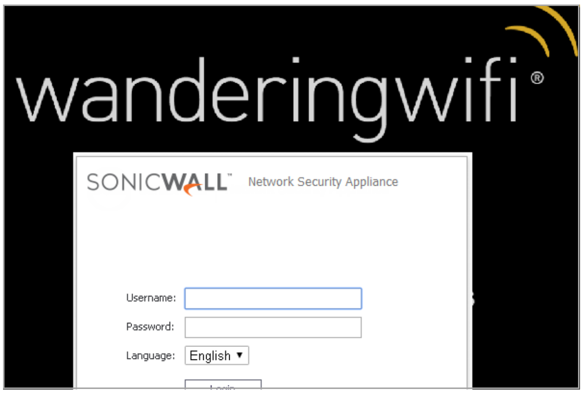
In this authentication path, clients are redirected to the portal server authentication page. User information can be passed to the captive portal server. The portal server either includes the SonicWall authentication URL as an iframe in the portal server page, or posts user authentication information to the firewall directly.

User information passed to the captive portal server:

If SonicOS passes the user information to the captive portal server, it automatically adds the user MAC address, user IP address, UFI (firewall serial number) and REQ (user client initial landing URL) to the end of the External Captive Portal Vendor URL. For example:

`http://captive.wanderingwifi.com/default.aspx?userMAC=34:e6:d7:25:0d:b3&userIP=18.18.18.194&UFI=18B169114528&REQ=http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?f95e30046a3679e3`

In this case, the SonicOS auth.html is iframed in the portal server authentication page. The client inputs user name and password as in an internal guest authentication.



Username:

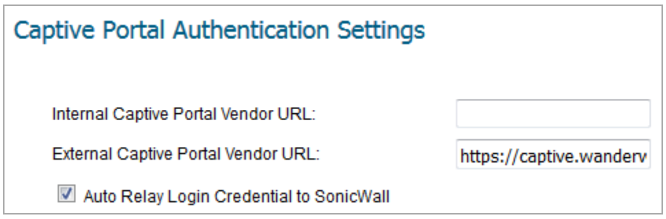
Password:

Language: English ▾

Captive portal server hosts its own authentication page, user information not passed:

If the captive portal server hosts its own authentication page, the client inputs user name and password and the server posts this information to SonicOS directly.

This case requires selecting the **Auto Relay Login Credential to SonicWall** option.



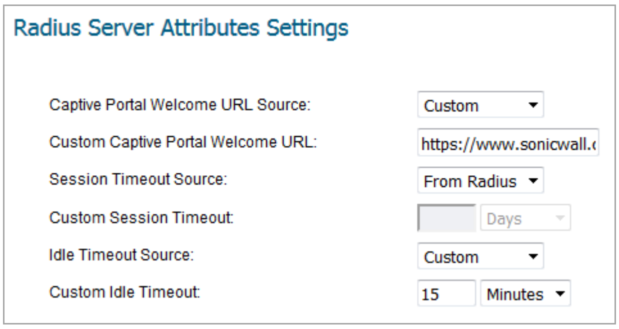
Captive Portal Authentication Settings

Internal Captive Portal Vendor URL:

External Captive Portal Vendor URL: https://captive.wanderv

☑ Auto Relay Login Credential to SonicWall

8 Under **RADIUS Server Attributes Settings**, select **Custom** to configure the attribute here, or select **From Radius** to use the value configured on the RADIUS server.



Radius Server Attributes Settings

Captive Portal Welcome URL Source:	Custom
Custom Captive Portal Welcome URL:	https://www.sonicwall.c
Session Timeout Source:	From Radius
Custom Session Timeout:	Days
Idle Timeout Source:	Custom
Custom Idle Timeout:	15 Minutes

9 Click **OK**.

10 Click **OK** in the **Edit Zone** dialog.

Cyclic Quota for Guest User Group

In previous SonicOS releases, after a guest user reaches his quota, he can no longer access the internet through your network. The quota setting for a guest account can only be used once, requiring the guest account to be repeatedly reconfigured in order to continue using it for internet access.

SonicOS 6.5 introduces cyclic quota control based on the guest account. After a guest user reaches his quota, he cannot access the internet any more in this cycle, but in the next cycle he gets a new quota to use. The quota cycle can be one day, one week, or one month.

This feature adds a new option accessed in the **MANAGE** view on **System Setup | User > Local Users & Groups**, **User > Guest Accounts**, or **Users > Guest Services**, by adding or editing the User, Guest Account, and Guest Profile accordingly.

Lightweight Hotspot Messaging also supports this feature. When a LHM user logs in or updates his session, the LHM server passes the Cycle quota setting to the firewall. Upon the LHM user logout, the firewall and LHM server synchronize the user's data usage and update the quota.

IP-Based Guest Authentication Bypass Network

SonicOS Guest Services allows guest users to have access through your network directly to the Internet without access to your protected network. In previous versions of SonicOS, Guest Services uses the MAC address of the user's computer for identification. In SonicOS 6.5, this feature enhances Guest Services with the ability to use the IP address of the user's computer.

Using the IP address as the identifier is useful when the guest user traffic passes through a network router, as this changes the source MAC address to that of the router. However, the user's IP address passes through unchanged.

If only the MAC address is used for identification, two clients behind the same router will have the same MAC upon reaching the firewall. When one client gets authenticated, the traffic from the other client will also be treated as authenticated and will bypass the guest service authentication.

By using the client IP address for identification, all guest clients behind the routed device are required to authenticate independently.

Networking Features

Topics:

- Dynamic LAG Using LACP
- Wire Mode over VLAN Interfaces
- Dell X-Series Daisy-Chaining Support
- ECMP Routing
- Policy Based TOS Routing
- PBR Metric-Based Priority
- BGP over Unnumbered Tunnel Interface

Dynamic LAG Using LACP

SonicOS 6.5 introduces support for Dynamic Link Aggregation using Link Aggregation Control Protocol (LACP). This feature is supported on SuperMassive and NSA platforms. The feature is not supported on platforms which do not support Advanced Switching features, including SOHO W, TZ300/W, TZ400/W, TZ500/W, and TZ600.

Link Aggregation allows you to inter-connect 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. Since multiple links are present between two devices, if one link fails, the traffic is transferred through other links without disruption. With multiple links being present, traffic can also be load balanced in such a way to achieve even distribution.

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. Dynamic LAG using LACP is already supported on SuperMassive 9800 platforms. With SonicOS 6.5, support for Dynamic LAG using LACP is available on current NSA (NSA 2650, NSA 3600, NSA 4600, NSA 5600, NSA 6600) and SuperMassive (SM 9200, SM 9400, SM 9600) platforms.

The two major benefits of LAG such as increased throughput and link redundancy can be achieved efficiently using LACP. LACP is the signalling protocol used between members in a LAG. It ensures links are only aggregated into a bundle if 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 will respond to the LACP PDUs received from the active side. If both sides are passive, LACP will fail to negotiate the bundle. Passive mode is rarely used in deployments.

SonicOS 6.5 only supports the Active mode of LACP.

In 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. Once 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 via LACP are displayed on the Switching > Link Aggregation page.

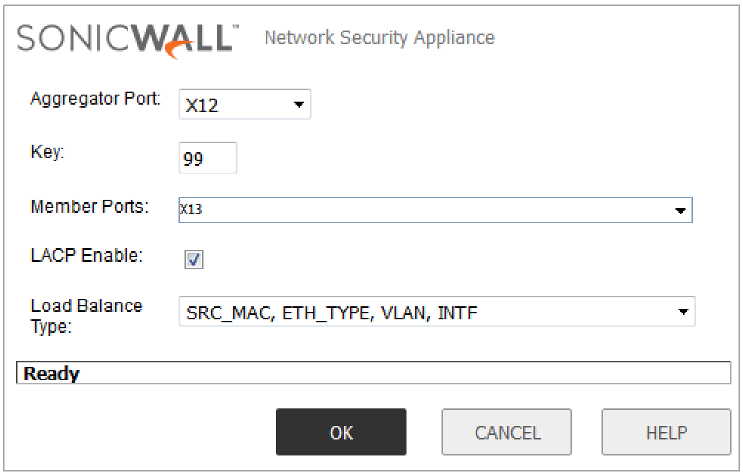
Six load balancing options are available for configuration. The load balancing option needs to be chosen during creation of a LAG when the Aggregator port is chosen. You cannot modify the load balancing option after the LAG is created.

- 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

To add a LAG port with LACP enabled:

1 In the **MANAGE** view, navigate to the **System Setup | Switching > Link Aggregation** page and click the **ADD** button.

2 In the **Add LAG Port** dialog, select the **Aggregator Port** from the drop-down list of available interfaces. This populates the list of available member ports.



Aggregator Port: X12

Key: 99

Member Ports: X13

LACP Enable: ☑

Load Balance Type: SRC_MAC, ETH_TYPE, VLAN, INTF

Ready

3 A **Key** value in the range of 1-255 is accepted.

4 Select one or more member ports from the **Member Ports** drop-down list.

5 Select the **LACP Enable** checkbox to enable exchange of LACP PDUs.

6 Select the **Load Balance Type** from the list.

To remove a LAG port with LACP enabled:

1 On the **Switching > Link Aggregation** page, click the **X** option with the "Delete this entry" tooltip corresponding to the port that needs to be deleted.

2 Click **OK** in the confirmation dialog box.

> **NOTE:** All member ports must be deleted from the LAG before deleting the Aggregator port.

Wire Mode over VLAN Interfaces

Wire mode between VLAN interfaces is very similar to wire mode between two physical interfaces. It is supported on NSA 2650, NSA 3600 and above, and on SuperMassive platforms. The feature functionality is as follows:

- Wire mode is supported for any two VLAN interfaces which have separate physical parent interfaces.
- Bypass mode, Inspect mode, and Secure mode are all supported.
- Disable Stateful Inspection is supported.
- Link Aggregation and Link State Propagation are ***not*** supported with wire mode over VLAN interfaces.
- Wire mode over VLAN interfaces and the VLAN Translation feature cannot be enabled at the same time.

Dell X-Series Daisy-Chaining Support

The Dell TZ-X Daisy Chaining solution enables integration of a SonicWall firewall with Dell X-Series Switches connected in daisy-chained mode. This feature is supported on GEN6 TZ wired/wireless platforms, on NSA and on SuperMassive platforms. This feature is not supported on NSA 2600 and SM 9800 platforms. Integration with all Dell X-Series Switch Models such as X1008/X1008P, X1018/X1018P, X1026/X1026P, X1052/X1052P and X4012 is supported in daisy-chain mode.

Support for this feature allows customers with large warehouses to deploy two X-series switches. The parameters allow the switches to be more than 1000 ft apart on a given site, to be connected to each other via fiber, to have the first switch—the parent switch—connected to the firewall, and to manage both the switches from the firewall. This deployment also allows customers access to an increased number of interfaces on the X-series switch by using a single interface on the firewall. All the interfaces of the parent switch and the child switch are available to be managed from the firewall.

Assumptions and Dependencies

- Dell X-series 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 4 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 via a single uplink. Other variations, such as dedicated uplinks, isolated links, etc. 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 firewall must be able to reach this subnet. Provisioning the switches in daisy-chained mode is a two step process. The first step is to provision the parent switch as a standalone switch. The second step is to provision the child switch as a daisy-chained switch.

ECMP Routing

SonicOS 6.5 introduces support for ECMP routing. Equal-cost multi-path (ECMP) is a routing technique for routing packets along multiple paths of equal cost. The forwarding engine identifies paths by next-hop. When forwarding a packet, the router must decide which next-hop (path) to use.

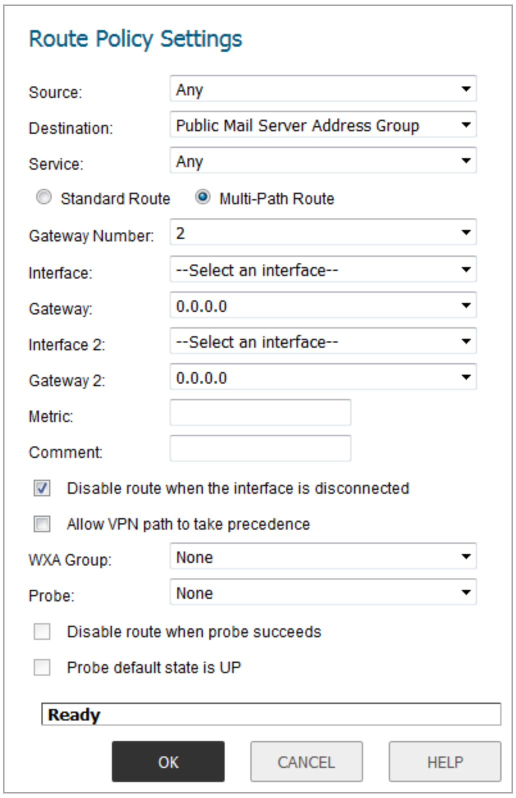
In SonicOS, an administrator can use ECMP routing to specify multiple next hops for a given route's destination. In environments with substantial requirements, there are several reasons for doing this. A router could just use one ISP most of the time, and switch to the other when the first one fails for some reason. Another application of multi-path is to keep a path on standby and enable it only when bandwidth requirements surpass a predefined threshold.

Various routing protocols, including Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (ISIS), explicitly allow ECMP routing. Some router implementations also allow equal-cost multi-path usage with RIP and other routing protocols.

SonicOS supports up to four next-hop paths.

To configure a multi-path route policy:

1. In the **MANAGE** view, navigate to the **System Setup | Network > Routing** page.
2. On the **Route Policies** screen, click **Add** to add a new policy.
3. In the **Add Route Policy** dialog, select values for the **Source**, **Destination**, and **Service** fields, and then select the **Multi-Path Route** radio button.



Route Policy Settings

Source: Any

Destination: Public Mail Server Address Group

Service: Any

○ Standard Route ● Multi-Path Route

Gateway Number: 2

Interface: --Select an interface--

Gateway: 0.0.0.0

Interface 2: --Select an interface--

Gateway 2: 0.0.0.0

Metric:

Comment:

☑ Disable route when the interface is disconnected

□ Allow VPN path to take precedence

WXA Group: None

Probe: None

□ Disable route when probe succeeds

□ Probe default state is UP

Ready

4. In the **Gateway Number** field, select the number of gateways used in the multiple paths. You can select 2, 3, or 4. The same number of **Interface** and **Gateway** fields are displayed for configuration.
5. Select a physical or VPN Tunnel interface from the **Interface** drop-down list or choose the **Create VPN Tunnel Interface** option. You can also select the **Drop_TunnelIf** option. This defines the egress interface used by this path.

6 Select an address object from the **Gateway** drop-down list. This defines the IP address of the gateway for this path.

7 Configure any other **Interface** and **Gateway** fields in the same way.

8 Configure the remaining fields in the same way you would for a standard route policy.

9 Click **OK**.

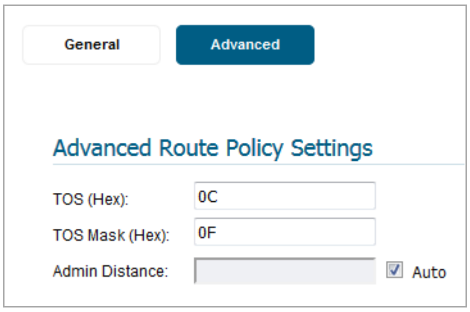
Policy Based TOS Routing

SonicOS 6.5 introduces two new options available when defining policy based routing (PBR) policies, a Type of Service (TOS) value and TOS mask. When defined, the TOS value and mask are compared against the associated IP packet's TOS/DSCP field in the IP header when finding a route match.

The options are found on the **Advanced** screen of the **Add/Edit Route Policy** dialog, accessed from the **MANAGE** view, **System Setup | Network > Routing** page. The new options are displayed as:

- **TOS (Hex)**
- **TOS Mask (Hex)**

Each option provides a field that accepts a two-digit hexadecimal number from 00 to FF. For example:



Advanced Route Policy Settings

TOS (Hex): 0C

TOS Mask (Hex): 0F

Admin Distance: ☑ Auto

Definition of the **TOS** value and **TOS Mask** is optional. Zero is the default for both (no value set). When no values are defined, policy routes result in the same behavior seen in previous SonicOS firmware.

The **TOS Mask** defines which bits (if any) will be examined for routing when a packet enters the firewall. An inbound IP packet's **TOS** field bits corresponding to unset bits in the **TOS Mask** are ignored.

When you configure any non-zero value for either the **TOS** or **TOS Mask**, the **TOS** and **TOS Mask** values are compared before submission to verify that they are consistent. Any **TOS** bits set must have a corresponding bit set in the **TOS Mask**. Conversely, **TOS Mask** bits may be set without the corresponding **TOS** value bit being set. This can be used when trying to match a zero-valued bit in the inbound packet.

The **TOS** value uses an 8-bit field in the IP packet header whose purpose has been redefined in RFC 2474 (Differentiated Services) and RFC 2168 (Explicit Congestion Notification). It can be used to define services relating to quantitative performance requirements (e.g., peak bandwidth) and those based on relative performance (e.g, class differentiation).

TOS routing differs from existing SonicOS QoS marking which does not affect the routing of a packet and cannot forward packets differently based on an inbound packet's TOS field. TOS Routing provides this capability by allowing policy routes to define a TOS Value / TOS Mask pair to be compared to inbound packets for differential forwarding. TOS routing only applies to packets as they enter the firewall.

With TOS routing, it is possible to define multiple policy routes with identical Source-IP, Destination-IP, and Service values, but differing **TOS/TOS Mask** values. This allows packets with marked TOS fields to be forwarded differently based on the value of the TOS field in the inbound packet.

Any PBR policy routes already defined will have no values defined for the TOS Value/TOS Mask after a firmware upgrade to SonicOS 6.5. Likewise, the default values for TOS Value/TOS Mask fields are zero (no values defined).

Policy routes with a **TOS** value other than zero are prioritized above all simple Destination-only routes, but below any policy routes that define a **Source** or **Service**. When comparing two TOS Policy routes, and assuming both have the same set of **Source**, **Destination**, and **Service** either defined or not defined, the TOS route with the greater number of **TOS Mask** bits set to 1 is prioritized above TOS routes with fewer **TOS Mask** bits set.

The general prioritization (high to low) of PBR routes is as follows, based on the policy fields defined as anything other than **Any**, or zero for **TOS**:

Destination, Source, Service, TOS

Destination, Source, Service

Destination, Source, TOS

Destination, Source

Destination, Service, TOS

Destination, Service

Destination, TOS

Destination

Source, Service, TOS

Source, Service

Source, TOS

Source

Service, TOS

Service

TOS

PBR Metric-Based Priority

SonicOS 6.5 introduces a new metric-weighted option for policy based routing (PBR) that allows the configured **Metric** to take precedence in route prioritization over the route specificity that is used by default. The new **Prioritize routes by metric within route classes** checkbox appears on the **Settings** screen of the **Network > Routing** page. Changing the option requires a restart of the system for the change to take effect.

The **Metric** is configured when you add a PBR route; it is a weighted cost assigned in the route policy. Metrics have a value between 0 and 255. Lower metrics are considered better and take precedence over higher ones.

The general prioritization (high to low) of PBR routes is as follows, based on the policy fields defined as anything other than **Any**, or zero for TOS:

Destination, Source, Service, TOS

Destination, Source, Service

Destination, Source, TOS

Destination, Source

Destination, Service, TOS

Destination, Service

Destination, TOS

Destination

Source, Service, TOS

Source, Service

Source, TOS

Source

Service, TOS

Service

TOS

Within these 15 classifications, routes are further prioritized based on the cumulative specificity of the defined route entries. For the source and destination fields, specificity is measured by counting the number of IP addresses represented in the address object. For example, the network address object 10.0.0.0/24 would include 256 IP addresses, while the network address object 10.0.0.0/20 would represent 4096. The longer /24 (24 bit) network prefix represents fewer host IP addresses and is more specific.

The new metric-weighted option allows the configured **Metric** to take precedence in prioritization over the route specificity. With the option enabled, the precedence used during prioritization is as follows (high to low):

1. Route class (determined by the combination of source, destination, service, and TOS fields with values other than **Any** or zero)
2. The value of the **Metric**
3. The cumulative specificity of the source, destination, service, and TOS fields

BGP over Unnumbered Tunnel Interface

BGP (Border Gateway Protocol) interfaces has been extended to support unnumbered tunnel interfaces, in addition to the numbered interfaces already allowed. This feature is supported on all platforms where BGP and unnumbered tunnel interfaces can be set up.

Investigation Features

Topics:

- Capture Threat Assessment Service Enhancements
- Packet Replay
- Advanced Flow Server
- Granular ZebOS Debug Control in CLI

Capture Threat Assessment Service Enhancements

Capture Threat Assessment (previously known as SWARM, SonicWall Application Risk Management) services are enhanced and improved for SonicOS 6.5:

- **SonicFlow Report File (SFR) posting and Capture Threat Assessment Report Generation** - This provides a one-click operation to send the SFR file to the SonicWall backend site for report generation. A download link is available in the management GUI when a report is available.
- **SFR Scheduled Auto-Emailing** - This allows scheduled emailing of SFR file to a user email account. The SFR file is attached to the email.
- **Additions to the SFR File data content**:
  - Real-Time data for applications, bandwidth, packets, connections, core usage that is useful to generate graphs and charts in the Capture Threat Assessment report
  - DPI-SSL visibility monitor mode statistics

Capture Threat Assessment interacts with several internal SonicOS modules for data gathering:

- Flow Reporting – aggregated data of Applications, threats, Geo-IP/Locations, botnets, Users, IP, etc.
- System – device system information and identification, license status information
- Interfaces – current interface bandwidth
- Peak information

- DPI-SSL – connection maximum and peak information
- Connection – connection cache maximum and peak
- Capture ATP – feature settings

ⓘ **NOTE:** Only a person with full administrative rights is allowed to send and generate reports.

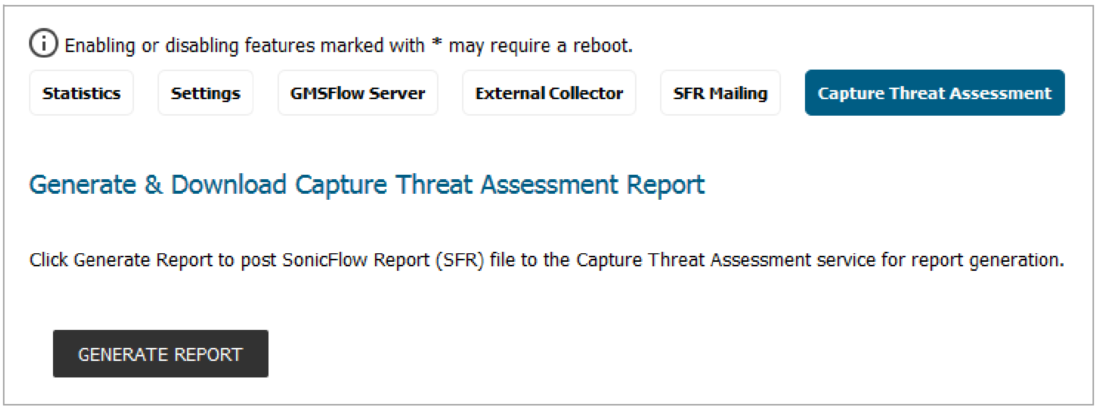
Feature Scope

This feature is available for all appliances that support SonicOS 6.5. However, bandwidth data information for SOHO-W may not be available in the SFR file due to certain limitations in Flow Reporting.

SFR Posting and Capture Threat Assessment Report Generation

Capture Threat Assessment report posting and generation is only available when the appliance is registered.

When registered, the **AppFlow Settings > Flow Reporting** page has a new tab named **Capture Threat Assessment Report**. Click the **GENERATE REPORT** button to initiate the creation, compression and encryption of SFR file that then gets posted via HTTPS to the threat report backend service.

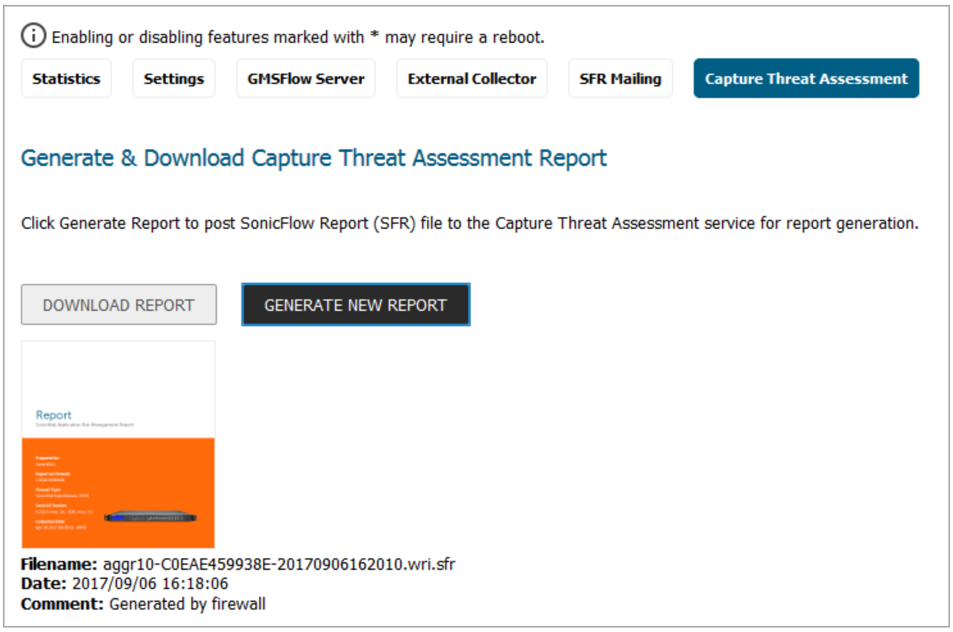


ⓘ Enabling or disabling features marked with * may require a reboot.

Generate & Download Capture Threat Assessment Report

Click Generate Report to post SonicFlow Report (SFR) file to the Capture Threat Assessment service for report generation.

Click the **DOWNLOAD REPORT** button to retrieve the generated report if it's available in the backend. A message is displayed if no report is available for download. Also you can select **Check Latest Report** to retrieve the latest information from the backend service.



ⓘ Enabling or disabling features marked with * may require a reboot.

Generate & Download Capture Threat Assessment Report

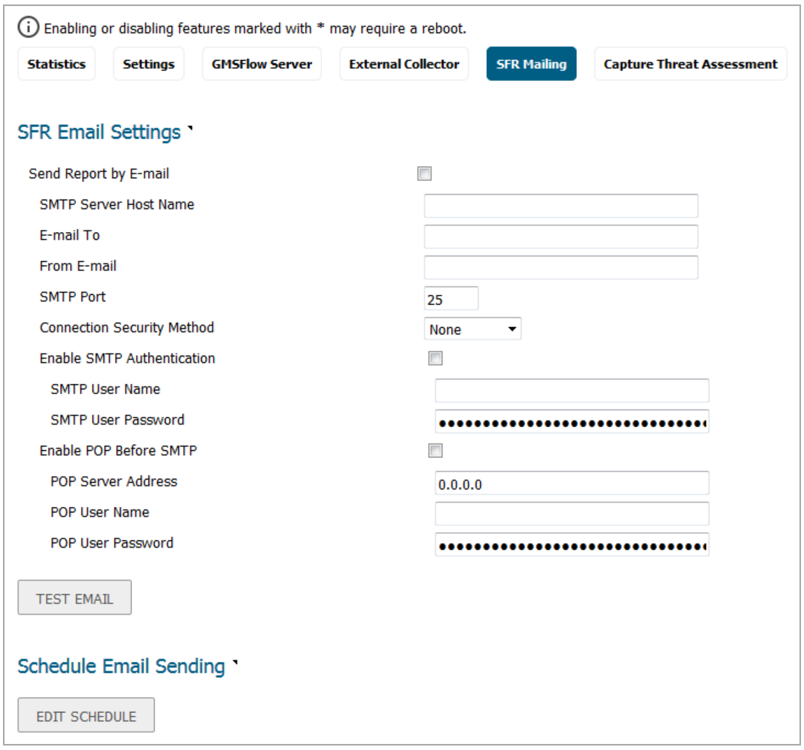
Click Generate Report to post SonicFlow Report (SFR) file to the Capture Threat Assessment service for report generation.

Filename: aggr10-C0EAE459938E-20170906162010.wri.sfr
Date: 2017/09/06 16:18:06
Comment: Generated by firewall

SFR Scheduled Email

Automatic emailing of SFR file allows you to set a schedule for sending the SFR file user email account. The email has SFR file attached to it. The user can then use this to upload to MySonicWall and use the offline Capture Threat Assessment tool to generate a report.

This feature can be enabled or disabled. If enabled, a schedule object **App Visualization Report Hours** is available for edit to schedule the mailing of SFR file. Go to **AppFlow Settings / Flow Reporting** and select the **SFR Mailing** tab.



ⓘ Enabling or disabling features marked with * may require a reboot.

SFR Email Settings

Send Report by E-mail	□
SMTP Server Host Name	
E-mail To	
From E-mail	
SMTP Port	25
Connection Security Method	None
Enable SMTP Authentication	□
SMTP User Name	
SMTP User Password	••••••••••••••••••••••••••••••••
Enable POP Before SMTP	□
POP Server Address	0.0.0.0
POP User Name	
POP User Password	••••••••••••••••••••••••••••••••

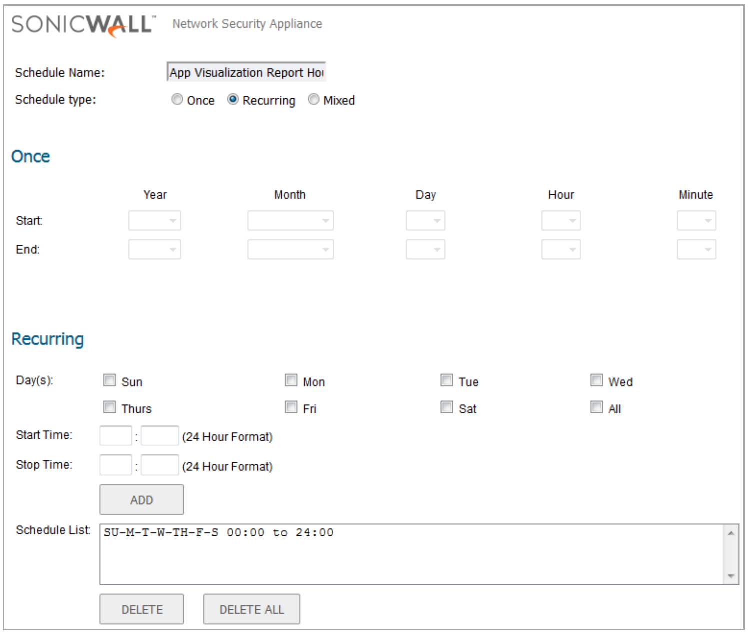
Schedule Email Sending

The first section of the screen prompts the user to configure email server settings:

- **Send Report by E-mail** – checkbox to enable/disable sending of SFR email
- **SMTP Server Host Name** – host name or IP address of SMTP server to use
- **E-mail To** – email account to receive the SFR file
- **From E-mail** – email name to denote the sender
- **SMTP Port** – TCP port use by the SMTP server
- **Connection Security Method** – specifies whether to use secure (select protocol) or non-secure email
- **Enable SMTP Authentication** – specifies whether SMTP server requires authentication
- **SMTP User Name** – user name to use for SMTP authentication
- **SMTP User Password** – password to use for SMTP authentication
- **Enable POP Before SMTP** – specifies if POP authorization is needed for sending email
- **POP Server Address** – IP address of POP server
- **POP User Name** – user name to use for POP authorization
- **POP User Password** – password to use for POP authorization

At any point of time even if the above parameters are not yet saved, you can test the email send function by clicking on the **Test Email** button. This uses the values set in the current form, validates them and tries to send the email. An alert message pops up for either a successful or failed email transaction.

To schedule the email, select **Edit Schedule** button. A popup window to edit the **App Visualization Report Hours** schedule object appears.



Schedule Name: App Visualization Report Hou

Schedule type: ○ Once ● Recurring ○ Mixed

Day(s): □ Sun □ Mon □ Tue □ Wed □ Thurs □ Fri □ Sat □ All

Start Time: _ : _ (24 Hour Format)

Stop Time: _ : _ (24 Hour Format)

Schedule List: SU-M-T-W-TH-F-S 00:00 to 24:00

Like any other schedule object, you can edit this to be one-time, recurring or mixed scheduling. However, this is a system created object so you cannot delete this object.

Updated SFR File Contents

Two new sections are added to the SFR file report format:

- Real-Time Monitor history data
- DPI-SSL Visibility monitor statistics

Packet Replay

SonicOS 6.5 introduces Packet Replay as an integrated tool in SonicOS for testing and debugging purposes. A new **Packet Replay** page is provided in SonicOS 6.5 in the **Investigate** view, under **Tools**.

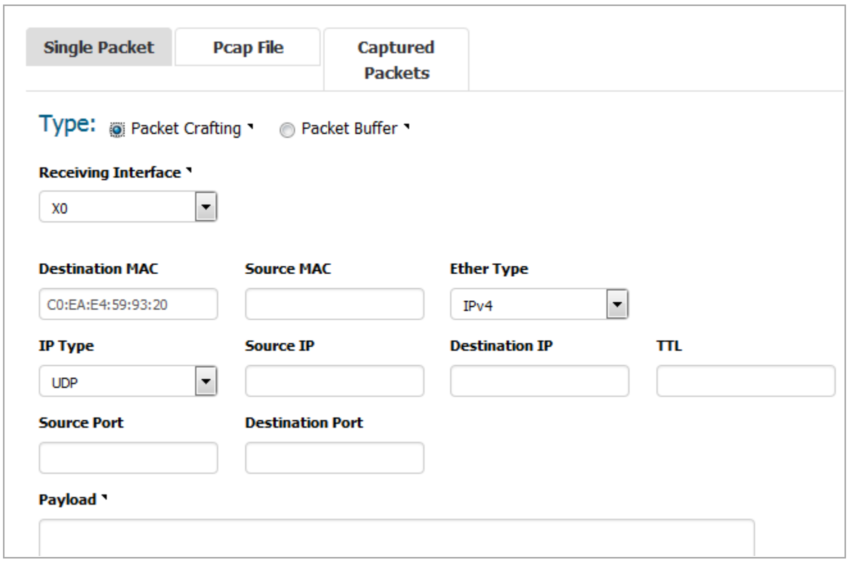
Replayed packets are restrained from travelling outside the firewall, meaning that they are dropped before being transmitted through interfaces.

The **Captured Packets** tab displays the packet data and provides a selection of file formats for exporting the data:

- **PcapNG** (new in SonicOS 6.5)
- **Libpcap**
- **Html**
- **Text**
- **App Data**

There are three ways you can replay packets from the **Packet Replay** page:

1 **Packet Crafting** – Specify packet header fields and payload on the **Single Packet** tab, then click **Send**.



Type: ● Packet Crafting ○ Packet Buffer

Receiving Interface: X0

Destination MAC: C0:EA:E4:59:93:20

Source MAC:

Ether Type: IPv4

IP Type: UDP

Source IP:

Destination IP:

TTL:

Source Port:

Destination Port:

Payload:

Depending on the selected **IP Type**, a few fields change. **IP Type** choices are:

- **UDP** (default)
- **ICMP**
- **IGMP**

The fields for an **IP Type** of **UDP** are:

- **Receiving Interface** - the interface from which the packet is assumed to be received
- **Destination MAC** - destination MAC address
- **Source MAC** - source MAC address
- **Ether Type** - protocol type in Ethernet frame (default IPv4)
- **IP Type** - UDP
- **Source IP** - source IP address
- **Destination IP** - destination IP address
- **TTL** - IP header TTL (Time to Live) field
- **Source Port** - UDP source port number
- **Destination Port** - UDP destination port number
- **Payload** - payload hex data is copied or typed here

When ready to replay the packet, click the **Send** button.

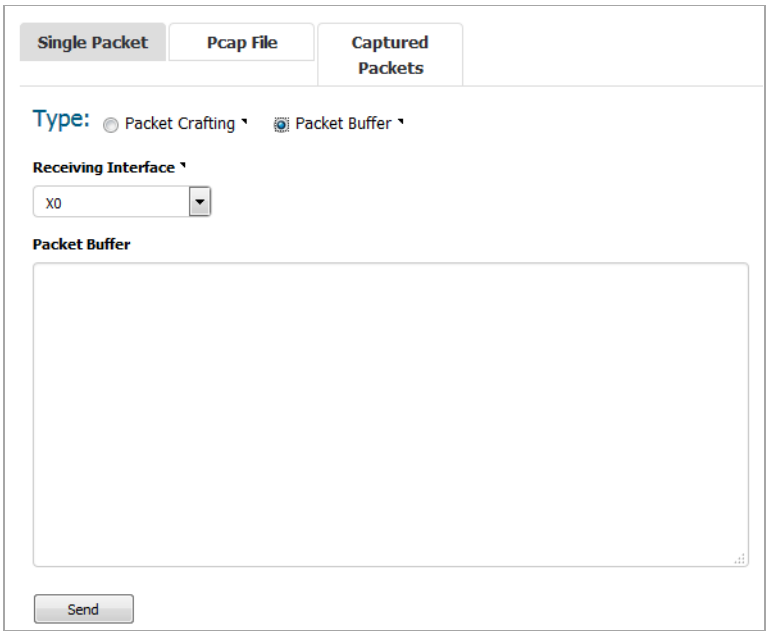
For an **IP Type** of **ICMP**, most fields are the same as above, except the following:

- **ICMP Type** - select **Echo Request** or **Echo Response**
- **ID** - ICMP identifier
- **Sequence** - ICMP sequence number

For an **IP Type** of **IGMP**, most fields are the same as above, except the following:

- **IGMP Type** - select IGMP type (default **Membership Query**)
- **Max Response** - IGMP max response timeout in seconds
- **Group address** - IGMP group IP address for query

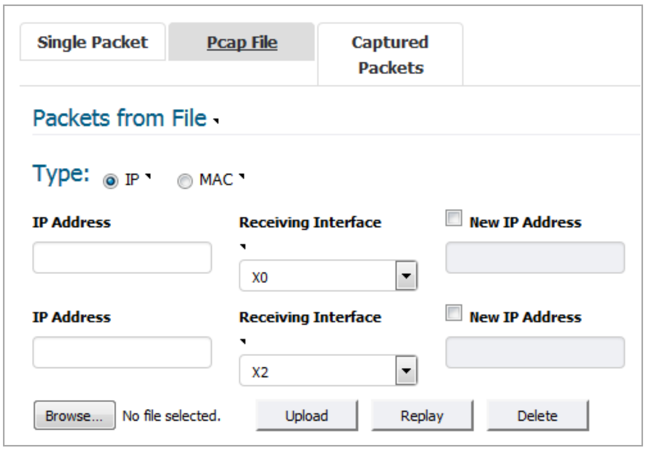
2 **Packet Buffer** – Copy a hex dump of the packet from Wireshark™ and paste into the **Packet Buffer** field on the **Single Packet** tab, then click **Send**.



Type: ○ Packet Crafting ● Packet Buffer

Receiving Interface: X0

3 **Replay Pcap File** - Upload a Pcap file on the **Pcap File** tab, select **IP** or **MAC** as the **Type**, configure settings, and click **Replay**.



Type: ● IP ○ MAC

Receiving Interface: X0

Receiving Interface: X2

Two IP or MAC filters are provided.

The fields and button functions are:

- For both IP filters:

  IP Address or **MAC Address** - the destination address to be looked up

  Receiving Interface - the interface from which the packets with the above destination address are assumed to arrive

  New IP Address - this IP address replaces the filtered destination IP address when replaying packets (only available with **Type** set to **IP**)

- **Browse** - selects a Pcap file to be replayed
- **Upload** - uploads the selected file
- **Replay** - replays the packets in the uploaded Pcap file
- **Delete** - deletes the uploaded Pcap file from memory

Advanced Flow Server

The the AppFlow Server Address and the External Collector's Server Address have been enhanced to accept address objects in addition to accepting an IP address. This feature adds:

- Support for address objects in **Flow Server IP Configuration** screens.
- Support for FQDN address objects.
- The ability for the user to choose input method for flow server to be of type **IP address** or **Address object** to maintain backward compatibility.
- **Advanced** tab in the **Flow Server Configuration** screens that has two flow server modes: **active/standby** and **load balancing**.

Granular ZebOS Debug Control in CLI

The Granular ZebOS Debug feature provides granular control of debug output to the CLI user. At a minimum, it provides a binary mode which allows granular ZebOS debug control at the expense of blocking logging output for Advanced Routing. It may, however, provide granular debug control without limiting the events that are made available to the logging/syslog component.

This feature is supported on all platforms running SonicOS 6.5.

Security Services Features

Topics:

- Dynamic CFS Categories
- CFS Keyword Filtering
- Dynamic Botnet List

Dynamic CFS Categories

Beginning with SonicOS 6.5, the categories defined for Content Filtering Services (CFS) are no longer limited to a static list. The CFS categories are now built and managed dynamically from the backend server. The maximum number of categories is extended from 64 to 255 so that new categories can be more easily added in the future. Categories can also be renamed or deleted more easily. This allows SonicWall appliances to access the latest categories without the need to load a new version of SonicOS firmware.

CFS Keyword Filtering

Since CFS 4.0, URI List Objects are used to do URI match when scanning web traffic. A token-based match algorithm is used, which means “torrent.com” does not match “seedtorrent.com”. To resolve this issue and make URI matching more flexible, a keywords list has been added to the URI List object.

When doing a web traffic filter, the URI list is scanned first. If no match is found, the keyword list is scanned next. The keyword list is used to match the host+path+query string, while the URI list is used to match the host+path. A match is made as long as one of those two lists matches the web traffic.

The following configuration and limits apply to keywords:

- Up to 100 keywords can be configured in each CFS URI list object.
- Each keyword can contain up to 255 printable ASCII chars.
- The whole length of keywords in one object should not be longer than 2048 (including the length of separator char ‘\n’ between each keyword).

The keywords can be edited in the **MANAGE** view, on the **Policies | Objects > Content Filter Objects** page, when adding or editing **URI List Objects**.

Dynamic Botnet List

SonicOS 6.5 provides the ability to maintain a dynamic list of botnets in the firewall. If enabled, an IP address is first looked up in the dynamic botnet list and then, if not found, looked up in the default list from the backend database.

To enable the dynamic botnet list:

1. In the **MANAGE** view, navigate to **Security Configuration | Security Services / Botnet Filter**.
2. On the **Settings** screen, select the **Enable Dynamic Botnet List** checkbox.
3. Click **ACCEPT**.

You can view, search, download, and flush the dynamic botnet list on the **Dynamic Botnet List** screen.

You can configure a dynamic botnet list server on the **Dynamic Botnet List Server** screen.

Deployment and Maintenance Features

Topics:

- Cloud Backup of Configuration Settings
- HTML5 Client Bookmarks
- GRE Management Multicore support
- OpenSSH 7.2 Support
- Federal Certification Support (UC-APL)

Cloud Backup of Configuration Settings

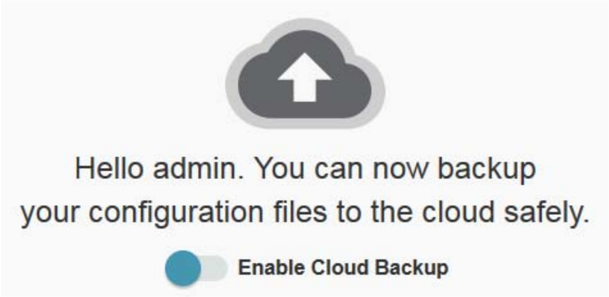
All SonicWall appliances have configuration settings that can be exported and saved to a file on your management computer. The filename has the extension `.exp`. This file serves as an external backup of the configuration settings, and can be imported to an appliance to give it the same configuration that was saved. For example, you can import the settings file into a replacement appliance, an appliance needing a similar configuration, or into the same appliance after rebooting the firmware with factory default settings. Restoring these configuration settings ensures the same functionality without any disruption.

System administrators generally save these configuration settings locally or in a network folder, and the file may be difficult to locate when needed.

In SonicOS 6.5, you can store exported settings files in the cloud, where they are accessible at any time just by logging into https://www.mysonicwall.com/.

ⓘ **NOTE:** Appliance configuration settings are also called preferences or prefs.

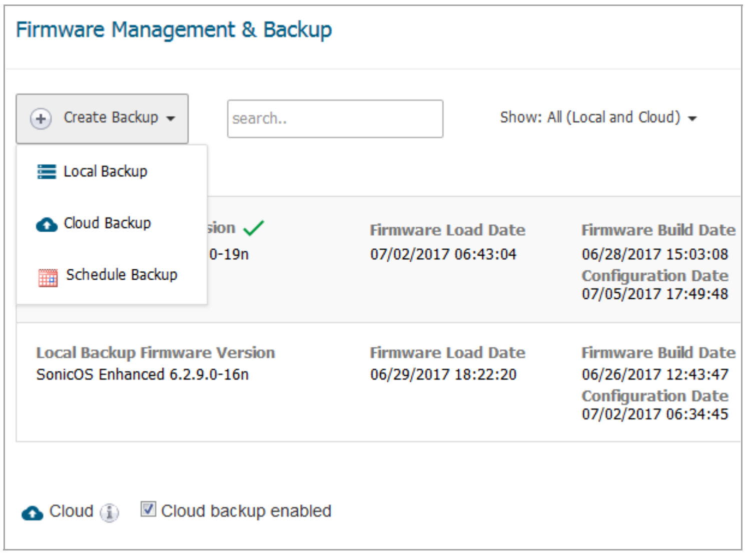
Cloud Backup is enabled and controlled in the **MANAGE** view, on the **Updates | Firmware & Backups** page.



Hello admin. You can now backup your configuration files to the cloud safely.

Simply click to enable Cloud Backup. The feature is disabled by default.

You can then use **Create Backup** to create local and cloud backups and create a backup schedule for cloud backups. The **Show** drop-down provides the lists of existing backups.



sion ✓
0-19n

Firmware Load Date
07/02/2017 06:43:04

Firmware Build Date
06/28/2017 15:03:08
Configuration Date
07/05/2017 17:49:48

Local Backup Firmware Version
SonicOS Enhanced 6.2.9.0-16n

Firmware Load Date
06/29/2017 18:22:20

Firmware Build Date
06/26/2017 12:43:47
Configuration Date
07/02/2017 06:34:45

☑ Cloud backup enabled

SonicWall recommends using **Schedule Backup** to configure a regular schedule for cloud backups.

There is a way to designate one cloud backup as the ***Gold Master*** backup, generally of a very strong configuration which could be used to resolve most issues.

The appliance transfer process in MySonicWall provides an option to delete or retain cloud backups. Backed up configurations are stored based on the appliance serial number, which is helpful when a new appliance administrator takes over within the same company or organization. The backup deletion option supports the case where an appliance is sold or transferred to a new owner.

The data retention policy currently allows 12 configuration backups per firmware version. When the limit is reached, a new automated backup causes the oldest automated backup to be deleted. Manual backups and designated automated backups are retained even if the limit is reached; they are not counted toward the limit.

When viewing the **Cloud** table, options are available to download a backup, delete a backup, delete all backups associated with a firmware version, change the comment on a backup, and designate a backup as Gold Master.

HTML5 Client Bookmarks

In previous SonicOS releases, VNC, RDP, SSH, and TELNET clients were implemented as Java or ActiveX plug-ins. Users had to install the clients in their systems before using them, while Java clients could cause security issues and have been abandoned by Apple on tablets.

SonicOS 6.5 implements these clients using HTML5, which is both more secure and more convenient. Most modern browsers support HTML5 and it eliminates the plug-ins previously required.

The new HTML5 clients are accessed by creating bookmarks for them in the **MANAGE** view on the **Connectivity | SSL VPN > Virtual Office** page.

With **HTML5-RDP**, you can set the **Screen Size**, use Single Sign-On, and access a **Settings** menu on the remote desktop that controls full screen, accesses the remote control keys like CTRL, ALT, and more, controls the clipboard in both directions, and shows the About information.

HTML5-VNC provides the **View Only** and **Share Desktop** options for the remote PC. The **Settings** menu provides the **Ctrl Alt Delete** and **Fit to Content** button options.

HTML5-SSHv2 starts a shell client on the remote system in which you can use terminal tools. The **Settings** menu provides options for **Full Screen** and **Exit**.

HTML5-TELNET is similar to the **HTML5-SSHv2** client. It starts a shell client on the remote system in which you can use terminal tools. The **Settings** menu provides options for **Full Screen** and **Exit**.

GRE Management Multicore support

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. GRE is a special protocol that is used in many scenarios, like IPv6 over IPv4 tunnel, PPTP, and wireless access point Layer 3 management and roaming support. Heavy GRE traffic passes through SonicOS, which can cause overly high utilization of a single core, impacting performance. SonicOS is enhanced to allow all cores to process GRE traffic to improve processing capability. This enhancement is implemented on all TZ, NSA, and SuperMassive non-multiblade platforms.

OpenSSH 7.2 Support

SonicOS 6.5 supports OpenSSH 7.2. OpenSSH is a 100% complete SSH protocol 2.0 implementation and includes SFTP client and server support.

Federal Certification Support (UC-APL)

SonicOS 6.5 supports a number of enhancements that are required for federal certification and UC-APL certification.

Topics:

- Role-based Administrator Support
- Pre-Login Policy Banner
- MSCHAPv2 and TLS Enforcement in RADIUS and LDAP Support
- Out-of-Band Management Support
- Audit Logging Enhancement Support
- CAC Support – Certificate Expiration Check and Certificate Cache Control
- FIPS 2K Signing Support
- Core Distribution Performance Enhancement
- IPv6 Network Monitoring / Probing
- IPv6 UDP/ICMP Flood Protection
- IPv6 DDNS Support

Role-based Administrator Support

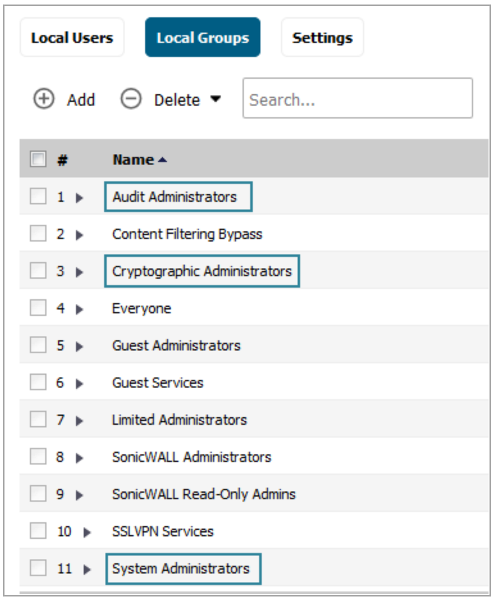
SonicOS supports multiple administrator roles as required for a UC-APL Certificate. Three new roles are added in SonicOS 6.5:

- **System Administrator** – able to access and edit all SonicOS pages except pages reserved for CAdmin and AAdmin
- **Cryptographic Administrator** (CAdmin) – able to access and edit VPN, SSLVPN and other cryptographic related pages
- **Audit Administrator** (AAdmin) – able to access and edit Dashboard, AppFlow, Log related pages

When viewed with previously existing administrator roles, the administrator levels from high to low are:
Full Admin -> System Admin -> CAdmin -> AAdmin -> Limit Admin -> Guest Admin

In the **MANAGE** view, on the **System Setup | Appliance > Base Settings** page, a new **Enable Multiple Administrative Roles** check box is added.

Three new user groups corresponding to the new admin roles are automatically created in **System Setup | Users > Local Users & Groups** if multiple administrators are enabled.

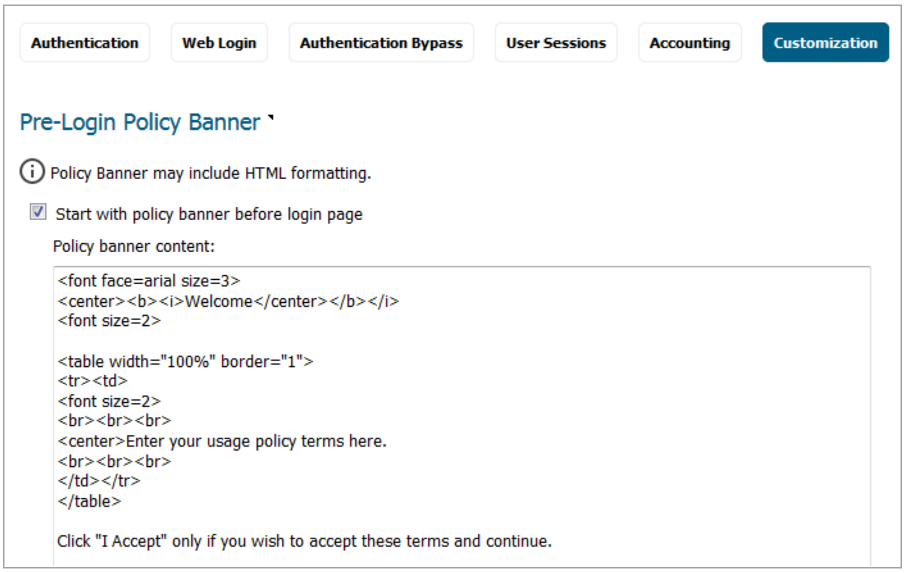


□	#	Name ▲
□	1 ▶	Audit Administrators
□	2 ▶	Content Filtering Bypass
□	3 ▶	Cryptographic Administrators
□	4 ▶	Everyone
□	5 ▶	Guest Administrators
□	6 ▶	Guest Services
□	7 ▶	Limited Administrators
□	8 ▶	SonicWALL Administrators
□	9 ▶	SonicWALL Read-Only Admins
□	10 ▶	SSLVPN Services
□	11 ▶	System Administrators

If a user belongs to one of these three groups, the user cannot belong to any other user groups. When one of these administrators logs in, a popup displays the corresponding access privileges and session duration. The SonicOS web management interface only displays the pages that the System, Crypto, or Audit administrator can access and edit. These administrators cannot preempt configuration mode from a Full administrator.

Pre-Login Policy Banner

Another federal requirement is the ability to configure and display a banner with a policy statement that users must agree to before logging in to access network resources. This is an enhancement to user authentication. You can configure the banner in the **System Setup | Users > Settings** page on the **Customization** screen.



Pre-Login Policy Banner

ⓘ Policy Banner may include HTML formatting.

☑ Start with policy banner before login page

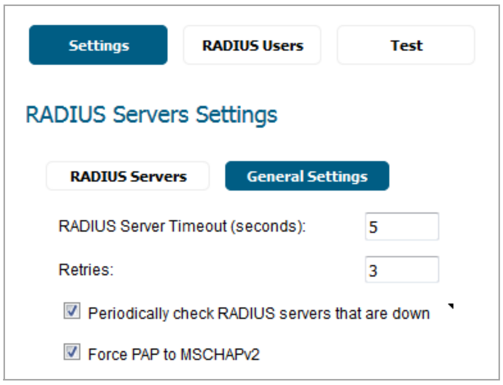
Policy banner content:

```
<font face=arial size=3>
<center><b><i>Welcome</center></b></i>
<font size=2>

<table width="100%" border="1">
<tr><td>
<font size=2>
<br><br><br>
<center>Enter your usage policy terms here.
<br><br><br>
</td></tr>
</table>

Click "I Accept" only if you wish to accept these terms and continue.
```

MSCHAPv2 and TLS Enforcement in RADIUS and LDAP Support

SonicOS 6.5 provides two new checkboxes to enforce MSCHAPv2 instead of using the PAP authentication protocol in RADIUS and LDAP authentication.

The **Force PAP to MSCHAPv2** checkbox is added in **System Setup | Users > Settings** on the **CONFIGURE RADIUS** page.



RADIUS Server Timeout (seconds): 5

Retries: 3

☑ Periodically check RADIUS servers that are down

☑ Force PAP to MSCHAPv2

Similarly, a **Force PAP to MSCHAPv2** checkbox is added in **System Setup | Users > Settings** on the **CONFIGURE LDAP** page.

Out-of-Band Management Support

In SonicOS 6.5, NTP, DNS, and SYSLOG traffic can be routed automatically through the out-of-band MGMT interface. A new **Enable Out of Band Management on management port** checkbox is added in support of this on the **System Setup | Appliance > Base Settings** page.

Audit Logging Enhancement Support

In SonicOS 6.5, all configuration updates can be logged along with the user who performed them. The **Enable Enhanced Audit Logging** checkbox is added on the **System Setup | Appliance > Base Settings** page to enable this enhancement. A log event starting with “Configuration changed:” is added to log configuration changes.

CAC Support – Certificate Expiration Check and Certificate Cache Control

The Common Access Card (CAC) is a United States Department of Defense (DoD) smart card issued as an identification card as well as for authentication to enable access to DoD computers, networks, and certain DoD facilities. The CAC enables encrypting and cryptographically signing email, facilitating the use of PKI authentication tools, and establishes an authoritative process for the use of identity credentials.

In SonicOS 6.5, OCSP provides client certificate status checks during the user login process and periodically. SonicOS also provides a periodical expiration check on customer imported CA certificates.

Settings for these functions are available on the **System Setup | Appliance > Base Settings** page under **Client Certificate Check**.

FIPS 2K Signing Support

SonicOS 6.5 meets the latest FIPS requirement for firmware image hash with SHA256 and signature verification with 112 bits of security strength, which uses a 2048 bit key. For backward compatibility, the firmware also includes a 1024 bit signature.

Core Distribution Performance Enhancement

The Core Distribution Performance Enhancement is an internal optimization on packet processing to improve the performance of SonicOS. It is enabled by default.

IPv6 Network Monitoring / Probing

Network Monitoring provides a flexible mechanism for monitoring network path viability. SonicOS 6.5 supports Network Monitor over IPv6 as well as IPv4. It is configured and viewed in the **INVESTIGATE** view on the **Tools | Network Probes** page.

IPv6 UDP/ICMP Flood Protection

SonicOS 6.5 supports UDP and ICMP Flood Protection for IPv6 as well as for IPv4. It is configured in the **MANAGE** view on the **Security Configuration | Firewall Settings > Flood Protection** page.

IPv6 DDNS Support

SonicOS 6.5 supports Dynamic DNS for IPv6 as well as for IPv4. You can add a Dynamic DNS profile in the **MANAGE** view on the **System Setup | Network > Dynamic DNS** page.

VoIP Features

Topics:

- SIP and H323 per Access Rule
- SIP TCP

SIP and H323 per Access Rule

H.323 and SIP traffic transformations can be applied globally to all traffic, or it can be applied to a select set of traffic as defined by a firewall rule. These settings can be defined in the **MANAGE** view on the **System Setup | VoIP** page and **Policies | Rules > Access Rules** page.

On the **System Setup | VoIP** page, under **SIP Settings** choose one of the following for SIP traffic:

- **Use global control to enable SIP Transformations**

  When selected, the option **Enable SIP Transformations** has to be selected to enable SIP transformation globally.

- **Use firewall Rule-based control to enable SIP Transformations**

  When selected, you need to also go to the **Rules > Access Rules** page to define the firewall rule that enables or disables SIP transformations.

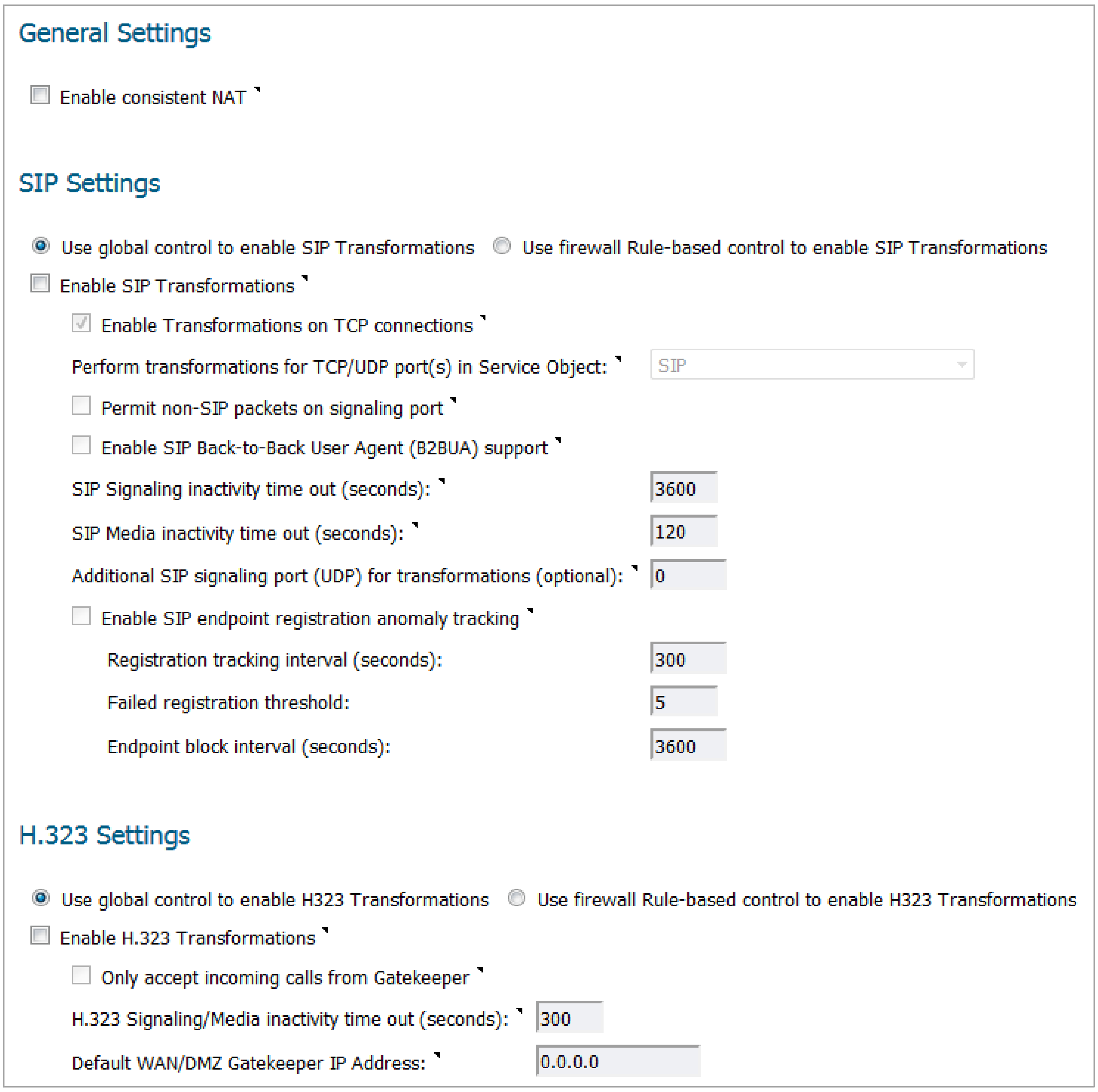
On the **System Setup | VoIP** page, for H.323 traffic go to **H.323 Settings** and choose one of the following:

- **Use global control to enable H323 Transformations**

  When selected, the option **Enable H.323 Transformations** has to be selected to enable H.323 transformation globally.

- **Use firewall Rule-based control to enable H323 Transformations**

When selected, you need to also go to the **Rules > Access Rules** page to define the firewall rule that enables or disables SIP transformations.



General Settings

□ Enable consistent NAT

SIP Settings

● Use global control to enable SIP Transformations ○ Use firewall Rule-based control to enable SIP Transformations

□ Enable SIP Transformations

☑ Enable Transformations on TCP connections

Perform transformations for TCP/UDP port(s) in Service Object: SIP

□ Permit non-SIP packets on signaling port

□ Enable SIP Back-to-Back User Agent (B2BUA) support

SIP Signaling inactivity time out (seconds): 3600

SIP Media inactivity time out (seconds): 120

Additional SIP signaling port (UDP) for transformations (optional): 0

□ Enable SIP endpoint registration anomaly tracking

Registration tracking interval (seconds): 300

Failed registration threshold: 5

Endpoint block interval (seconds): 3600

H.323 Settings

● Use global control to enable H323 Transformations ○ Use firewall Rule-based control to enable H323 Transformations

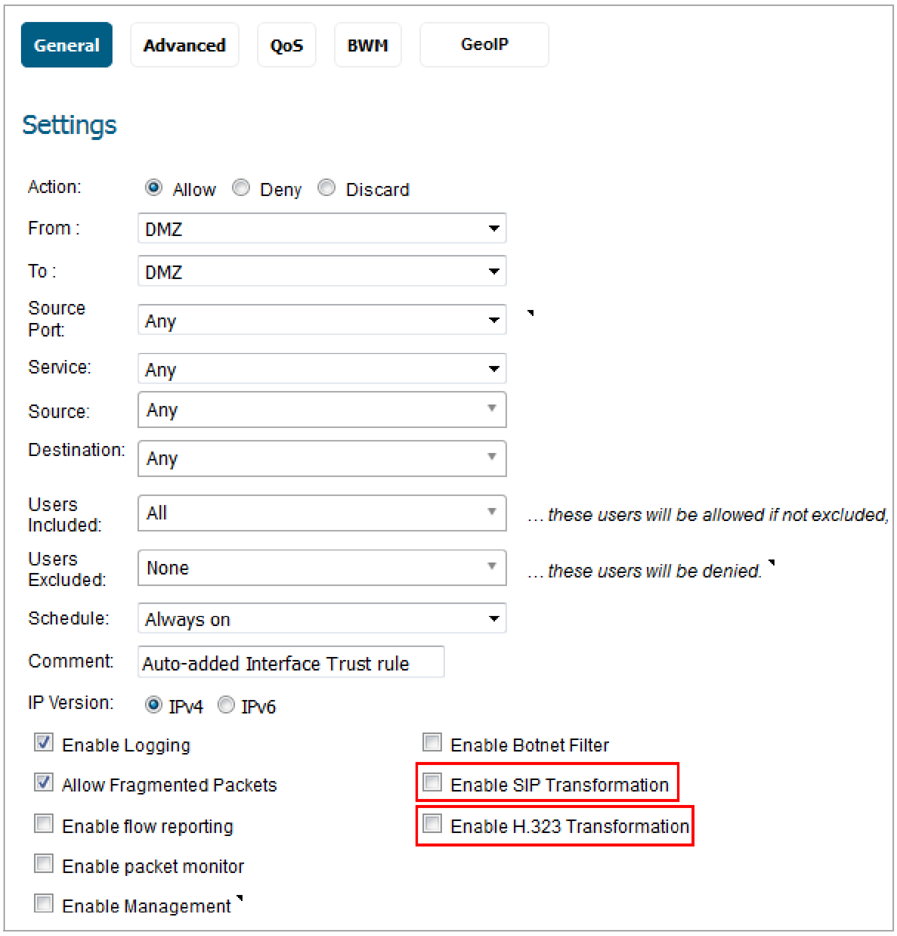
□ Enable H.323 Transformations

□ Only accept incoming calls from Gatekeeper

H.323 Signaling/Media inactivity time out (seconds): 300

Default WAN/DMZ Gatekeeper IP Address: 0.0.0.0

If you opt to manage SIP and H.323 transformations through firewall rules, you need to go to **Policies | Rules > Access Rules**. Click **Add** to launch the **Add Rule** dialog, and select the **Enable SIP Transformation** or **Enable H.323 Transformation** checkbox.



Settings

Action: ● Allow ○ Deny ○ Discard

From : DMZ

To : DMZ

Source Port: Any

Service: Any

Source: Any

Destination: Any

Users Included: All ... *these users will be allowed if not excluded,*

Users Excluded: None ... *these users will be denied.*

Schedule: Always on

Comment: Auto-added Interface Trust rule

IP Version: ● IPv4 ○ IPv6

☑ Enable Logging

☑ Allow Fragmented Packets

□ Enable flow reporting

□ Enable packet monitor

□ Enable Management

□ Enable Botnet Filter

□ Enable SIP Transformation

□ Enable H.323 Transformation

When configuring SIP transformations, consider the following guidelines:

- The **Enable SIP Transformation** box should not be checked if the **Use global control to enable SIP Transformations** is selected on the **System Setup | VoIP** page.
- The **Enable SIP Transformation** box is checked when the **Use firewall rule-based control to enable SIP Transformations** is selected on the **System Setup | VoIP** page.
- Select the option to enable SIP transformations for all the sessions permitted by this firewall access rule.
- Clear the option to disable SIP transformation for all the sessions permitted by this firewall access rule.

When configuring H.323 transformations, consider the following guidelines:

- The **Enable H.323 Transformation** box should not be checked if the **Use global control to enable H.323 Transformations** is selected on the **System Setup | VoIP** page.
- The **Enable H.323 Transformation** box is checked when the **Use firewall rule-based control to enable H.323 Transformations** is selected on the **System Setup | VoIP** page.
- Select the option to enable H.323 transformations for all the sessions permitted by this firewall access rule.
- Clear the option to disable H.323 transformation for all the sessions permitted by this firewall access rule.

SIP TCP

SonicOS 6.5 introduces support for the SIP protocol to work with TCP traffic. SIP is an industry standard VoIP protocol and is supported for both UDP and TCP. Some SIP applications, such as LYNC, are implemented only with TCP.

A new option, **Enable Transformations on TCP connections**, is available on the **System Setup | VoIP** page for this feature.

IPv6 Features

Topics:

- DS-Lite Tunnel / GRE 4to6 Tunnel
- IPv6 WAN Load Balancing
- IPv6 AppFlow Report
- IPv6 PPPoE
- IPv6 MAC Spoof
- IPv6 SIP
- IPv6 SSH
- IPv6 Geo-IP Reporting
- IPv6 SSL VPN on Data Plane
- IPv6 SNMP MIB

DS-Lite Tunnel / GRE 4to6 Tunnel

SonicOS 6.5 introduces support for Dual-Stack Lite (DS-Lite) Tunnel and IPv4 over IPv6 Generic Routing Encapsulation Tunnel (GRE 4to6 Tunnel). These tunneling features are closely related in SonicOS.

DS-Lite Tunnel

Dual-Stack Lite (DS-Lite), defined in RFC 6333, allows a service provider to share existing IPv4 address space and support both IPv6 and IPv4 clients utilizing an IPv6 infrastructure. It combines both tunneling and network address translation (NAT) technologies, and de-couples the service provider's access network from the public internet. This can simplify the migration to IPv6 by allowing incremental IPv6 deployment with the service provider's network while continuing to support legacy IPv4 clients.

DS-Lite is deployed across an all-IPv6 infrastructure, which natively supports IPv6 clients, and tunnels IPv4 packets using *softwires* to the ***AFTR***. A *softwire* is an IPv4-in-IPv6 tunnel, using the IPIP-0x04 protocol type, defined per RFC 2473.

Logically there are two components:

1. **B4 (Base Bridging BroadBand element)**: This component has an IPv6 connection to the IPv6 internet, and has a stateless IPv4-in-IPv6 tunnel to AFTR.

   When it receives IPv6 traffic, it routes the traffic to the IPv6 internet. When it receives IPv4 traffic, it sends it in IPv4-in-IPv6 tunnel to AFTR. The IPv4 traffic is encapsulated into the tunnel without NAT applied.

2. **AFTR (Address Family Transition Router element)**: This component maintains multiple IPv4-in-IPv6 tunnels with different B4s. It has public IPv4 address(es) and will translate the source IP of the IPv4 traffic from the tunnels for IPv4 internet access.

To configure a DS-Lite Softwire tunnel:

1. In the **MANAGE** view, on the **System Setup | Network > Interfaces** page, click the **Add Interface** drop-down list below the **Interface Settings** table and select **4ot6 Tunnel Interface**.
2. In the **Add DS-Lite Softwire Interface** dialog, the **Zone** is set to **WAN** and cannot be edited.
3. For **Tunnel Type**, select **DS-Lite Softwire**. Only four softwire tunnels can be configured on the appliance.
4. For **Name**, type in the interface name. It cannot be null and the max length is 25.
5. For **Bound to**, select the interface to which the tunnel is bound. It should be a physical WAN interface. If the bound interface link goes down, the softwire will be down as well. You cannot change the zone of the bound interface to a different zone.
6. Under **Local IPv6 Address** - As an interface may have various IPv6 addresses, select one of the following options for the local IPv6 address choice:
   - **Use Primary IPv6 Address** – This uses the bound Interface's IPv6 address as the Local Address. When the bound interface is using DHCPv6 or Autonomous Mode, it obtains a dynamic IP address (DHCPv6 IP or Autonomous IP) as the softwire local IPv6 address, and DHCP IP has a higher priority. Otherwise, if the bound interface is using Static or another mode, it uses the primary static IPv6 address as the softwire local IPv6 address. If the bound interface IP address is released or deleted, the IP address can be **::**.
   - **Specify the Local IPv6 Address** – Type in the IPv6 address to use.
7. Under **AFTR IPv6 Address** - The address is used as softwire's peer address. Select one of the following options:
   - **Configure Static Address** – Type in the IPv6 address to use.
   - **Configure FQDN** – For a FQDN, B4 attempts to resolve its AAAA record. If resolving fails, the softwire is considered to be down.
   - **Get via DHCP** – In this case, the bound interface must be in DHCPv6 client mode. If the bound interface is not in DHCP mode, or the AFTR address and name cannot be obtained from DHCP, the softwire is considered to be down.
8. On the **Advanced** screen, type in a value for the **Local IPv4 Address**. 192.0.0.0/29 is the reserved range for softwire interfaces, and 192.0.0.2 is reserved for B4 per RFC6333. The default softwire IPv4 address is 192.0.0.2. The subnet mask is 255.255.255.248 and cannot be modified. This IPv4 address will not take effect in most cases. The IPv4 addresses cannot overlap among different softwire interfaces.
9. Click **OK** when ready. Two address objects are automatically added, one for the IP and the other for the subnet of the softwire interface.

A softwire interface can be used in a Route entry, with NAT, and in an Access Control List (ACL).

GRE 4to6 Tunnel

The feature enables the delivery of IPv4 packets through an IPv6 network and allows the routing of IPv6 packets between private networks across public networks with globally routed IPv6 addresses.

A GRE tunnel is a static tunnel, that is, when creating a GRE tunnel, the endpoints must be specified. For point-to-point GRE tunnels, each tunnel interface requires a tunnel source IPv6 address and a tunnel destination IPv6 address when being configured. All packets are encapsulated with an outer IPv6 header and a GRE header.

To pass IPv4 packets through the IPv6 network, each IPv4 packet is encapsulated in an IPv6 packet at the ingress side of a tunnel. When the encapsulated packet arrives at the egress of the tunnel, the process is reversed.

To configure a GRE 4to6 tunnel:

1. In the **MANAGE** view, on the **System Setup | Network > Interfaces** page, click the **Add Interface** drop-down list below the **Interface Settings** table and select **4ot6 Tunnel Interface**.
2. In the **Add DS-Lite Softwire Interface** dialog, the **Zone** is set to **WAN** and cannot be edited.

3. For **Tunnel Type**, select **GRE 4to6 Tunnel**. Only four GRE 4to6 tunnels can be configured on the appliance.
4. For **Name**, type in the interface name. It cannot be null and the max length is 25.
5. For **IP Address**, type in the interface IPv4 address.
6. For **Subnet Mask**, type in the subnet mask.
7. For **Bound to**, select the interface to which the tunnel is bound. It should be a physical WAN interface. If the bound interface link goes down, the GRE 4to6 tunnel will be down as well. You cannot change the zone of the bound interface to a different zone.
8. Under **Local IPv6 Address** - As an interface may have various IPv6 addresses, select one of the following options for the local IPv6 address choice:
   - **Use Primary IPv6 Address** – This uses the bound Interface's IPv6 address as the Local Address. When the bound interface is using DHCPv6 or Autonomous Mode, it obtains a dynamic IP address (DHCPv6 IP or Autonomous IP) as the softwire local IPv6 address, and DHCP IP has a higher priority. Otherwise, if the bound interface is using Static or another mode, it uses the primary static IPv6 address as the tunnel local IPv6 address. If the bound interface IP address is released or deleted, the IP address can be **::**.
   - **Specify the Local IPv6 Address** – Type in the IPv6 address to use.
9. For **Remote IPv6 Address**, type in the remote address. The endpoints must be specified.
10. On the **Advanced** screen, the **Interface MTU** is the MTU effective for the IPv4 packet size before encapsulation. The GRE tunnel automatically calculates its MTU based on the bound interface's IPv6 MTU. If the bound IPv6 interface MTU changes, the tunnel's MTU is automatically updated.
11. Select the fragmentation settings you want to use. The default is **Fragment non-VPN outbound packets larger than this Interface's MTU**. Fragmentation happens AFTER encapsulation.
12. Click **OK** when ready. Two address objects are automatically added, one for the IP and the other for the subnet of the GRE tunnel.

A GRE 4to6 tunnel interface can be used in a Route entry, with NAT, and in an Access Control List (ACL).

IPv6 WAN Load Balancing

SonicOS 6.5 supports WAN Load Balancing (WLB) over IPv6, in addition to the IPv4 existing implementation. This feature is supported on all platforms.

In the **MANAGE** view, on the **System Setup | Network > Interfaces** page, you can choose the **IPv6** option for **View IP Version** to view the IPv6 WLB group.

IPv6 WLB supports the same four modes that are supported for IPv4:

- Basic Failover – The WAN interfaces use rank to determine the order of preemption when the **Preempt** checkbox has been enabled. Only a higher-ranked interface can preempt an Active WAN interface.
- Round Robin – This mode allows the user to re-order the WAN interfaces for Round Robin selection. The order is as follows: Primary WAN, Alternate WAN #1, Alternate WAN #2, and Alternate WAN #3; the Round Robin will then repeat back to the Primary WAN and continue the order.
- Spill-over – The bandwidth threshold applies to the Primary WAN. Once the threshold is exceeded, new traffic flows are allocated to the Alternates in a Round Robin manner. Once the Primary WAN bandwidth goes below the configured threshold, Round Robin stops, and outbound new flows will again be sent out only through the Primary WAN. Note that existing flows will remain associated with the Alternates (since they are already cached) until they timeout normally.
- Ratio – The percentages can be set for each WAN in the LB group. To avoid problems associated with configuration errors, ensure that the percentage correctly corresponds to the WAN interface it indicates.

When an IPv6 interface is configured in WAN zone in Static mode, SonicOS automatically adds an IPv6 default gateway address object for the interface, and dynamically changes it according to the gateway configuration. For an IPv6 interface, the default gateway address object only makes sense when the interface is in the WAN zone and in Static mode.

The IPv6 default gateway address object remains until the interface is deleted (for a VLAN) or unassigned. If the interface is changed from the WAN zone to a non-WAN zone, or the Primary Static Address is null, the default gateway address object is kept. But, when the interface is deleted, then the default gateway address object is deleted from address object table, and all the related Route/NAT/VPN/ACL items are also removed, including auto-added and manually created entries.

IPv6 AppFlow Report

SonicOS 6.5 enhances the AppFlow Reporting feature to display reports showing IPv6 flows on the **AppFlow Reports** page in the **INVESTIGATE** view. You can select whether to show IPv4 only, IPv6 only, or IPv4 and IPv6 flows.

When viewing the **Location** information in **AppFlow Reports**, the IPv6 location data is only displayed if Geo-IP is enabled for IPv6.

IPv6 PPPoE

SonicOS 6.5 supports PPPoE over IPv6. IPv6 PPPoE provides a point-to-point connection over Ethernet in the IPv6 network. It provides the ability to connect a network of hosts over a simple bridging access device to a remote Access Concentrator in the IPv6 network.

In SonicOS, IPv4 PPPoE and IPv6 PPPoE use the same interface, To avoid multiple PPPoE connections on the same interface, IPv6 PPPoE cannot be applied alone, it must be used with IPv4 PPPoE at the same time. That means you must configure PPPoE over IPv4 before you configure IPv6 PPPoE on the interface. Once the IPv6 PPPoE connection has been established, it also can pass IPv4 traffic.

After the initial IPv4 PPPoE interface is configured in the **MANAGE** view on the **System Setup | Network > Interfaces** page, and then you change **View IP Version** to **IPv6**, the interface is displayed as *PPPoEv6* in the **Network > Interfaces** page. You can configure it and select the PPPoEv6 address assignment:

- **Auto** – Provides a link local address.
- **Static** – You assign a static, global IPv6 address.
- **DHCPv6** – Obtain a global IPv6 address dynamically.

After the configuration is complete, click **Connect** in the **Interface Settings** table to establish the PPPoEv6 connection and communicate with the internet through the PPPoEv6 session.

IPv6 MAC Spoof

MAC address and IPv6 Address based spoofing attack are very common in a local area network. These attacks are commonly known as Man-in-the-middle, NDP poisoning, SPITS, unauthorized access, and so forth. There are many ways to limit these attacks.

IPv6 MAC-IP Anti-Spoof feature lowers the risk of these attacks and provides administrators different ways to control the access of the network along with managing the configuration of the network. It provides L2/L3 level admission control along with L2 (MAC) based anti-spoof or NDP Guard.

IPv6 MAC-IP Anti-Spoof feature can be deployed on a firewall to defend IPv6 MAC-IP Spoof attack for each IPv6 network interface. When it is enabled, the firewall watches IPv6 traffic pass through the firewall and detects IPv6 MAC-IP Spoof attacks. When the IP and MAC of IPv6 packets are not found in the Anti-Spoof Cache, the firewall records potential attack in the Spoof Detected List. When it is enforced, the firewall blocks this kind of traffic to protect potential victims.

Functions of the IPv6 MAC-IP Anti-Spoof feature include:

- Configure IPv6 MAC-IP Anti-Spoof settings – Provides UI to Display/Configure IPv6 MAC-IP Anti-Spoof settings.
- IPv6 MAC-IP Anti-Spoof Cache – Provide UI to Display/Configure IPv6 MAC-IP Anti-Spoof Cache.
- IPv6 MAC-IP Spoof Detected List – Provides UI Display IPv6 MAC-IP Spoof Detected List and Add Entry From Detected List to Anti-Spoof Cache.

The following interfaces are excluded from the list of IPv6 MAC-IP anti-spoof interface list:

- Non-Ethernet interfaces
- Port-shield member interfaces
- Layer2 bridge pair interfaces
- HA interfaces
- HA data interface
- Tunnel interface

IPv6 SIP

SonicOS 6.5 introduces support for the SIP protocol over IPv6. The SIP IPv6 implementation is completely transparent to users without any additional configuration needed. The SIP Application Layer Gateway functionality is enhanced and redesigned to be IPv6-aware.

With SIP IPv6, the SIP component within SonicOS is able to support both IPv4 and IPv6 address modes simultaneously. However, is cannot function like a bridge between IPv4 and IPv6 (NAT64). In other words, if an ingress SIP stream to the firewall is in IPv4 mode, it will stay in IPv4 mode on the egress side. The same is true for IPv6 mode. The associated media sessions (like audio and video sessions) as hosted by the SIP signaling stream have the same address mode as the SIP signaling session. For example, if the SIP signaling handshake is in IPv6 mode, all the RTP/RTCP streams generated from this SIP signaling stream will be in IPv6 mode as well.

IPv6 SSH

IPv6 SSH support in SonicOS 6.5 is a major enhancement of the original SSH feature, allowing you to connect to SonicWall firewalls using the SSH protocol with an IPv6 address.

SSH must be enabled on an interface before it can be used to access the appliance from that interface. Just like HTTP, HTTPS and Ping, SSH belongs to the management policies related to a network interface. Select the **SSH** checkbox when configuring the IPv6 interface to enable SSH management.

This feature is supported on all platforms running SonicOS 6.5.

IPv6 Geo-IP Reporting

The IPv6 Geo-IP reporting feature makes IPv6 addresses available for geographical information lookup and provides interfaces to other features which need IPv6 geographical information, including:

- AppFlow Monitor can display an IPv6 traffic group by countries
- AppFlow Reports and AppFlow Dash can display location statistics
- Geo-IP Filter can filter IPv6 traffic by countries

IPv6 Geo-IP reporting is supported on all SonicWall firewalls that support Flow Reporting and Geo-IP.

IPv6 SSL VPN on Data Plane

In SonicOS 6.5, IPv6 SSL VPN can run on the firewall’s data plane rather than only on the control plane. Running on the data plane provides better performance for the NetExtender client.

IPv6 SNMP MIB

SonicOS has been updated so RFC 4293 IP MIB and SNMPv2C Protocol Operations over IPv6 is supported.

Resolved Issues

This section provides a list of resolved issues in this release.

Gateway Anti-Virus

Resolved issue	Issue ID
Capture ATP does not process email attachments; SMTP email is not processed regardless of the attached file type. Also, Gateway Anti-Virus does not block email attachments, such as VBA macros, that are configured to be blocked in the GAV settings. Occurs when the TCP Stream option is enabled for Outbound Inspection in the Gateway Anti-Virus settings.	188050

High Availability

Resolved issue	Issue ID
In a High Availability deployment with one unit down, the active appliance becomes unresponsive. Occurs when heavy, mixed traffic including SIP (H.323) traffic is passing through the active appliance, while the other unit in the HA pair is powered down.	190464

Networking

Resolved issue	Issue ID
The first 600 access rules are kept per any zone-to-zone rule list and the rest are deleted after upgrading to SonicOS 6.2.7.1. Occurs when there are more than the default number of access rules (Max Rule Count: 600 by default) in any zone to zone access rule list, and then the appliance is upgraded to SonicOS 6.2.7.1. Occurs even when Max Rule Count is set to a higher number before upgrading or importing the previous configuration.	190798
The Transparent IP Mode (Splice L3 Subnet) option is not available for the Mode/IP Assignment option in SonicOS 6.2.7.1. Occurs when configuring a virtual interface in SonicOS 6.2.7.1.	189827
The delete option to remove automatically added rules is always disabled. Occurs when the internal setting "Enable the ability to remove and fully edit auto-added access rules" is selected, which should enable the delete option.	188125
SonicWall GMS does not display the Vendor and Type fields when viewing the Network > ARP table or in other tables. Occurs when GMS is managing a firewall running SonicOS 6.2.7.1 which supports the Vendor and Type fields, but SonicOS does not pass the data to GMS.	186628
Wireless users connected to a SonicPoint are unable to access LAN or WAN destinations. Occurs when the SonicPoint is connected to a physical firewall interface with a VLAN or VAP configured and bridged with Layer 2 Bridging to an interface in the LAN zone.	185498

Users

Resolved issue	Issue ID
The SSO Agent does not trigger when traffic occurs on zones that have authentication enforced. Occurs when the **For other unidentified connections** option under **For logging of connections on which the user is not identified** is set to **Log user name: Unknown** in the user settings.	189771

VoIP

Resolved issue	Issue ID
VoIP phones behind a firewall running SonicOS 6.2.7.1 cannot make outbounds calls, although inbound calls and phone registration are working fine. Occurs when the internal SIP device uses a port that is different from the source port (the port associated with the Via or Contact fields), and when the remote device sends packets to this port, the firewall is not forwarding them to the internal device.	189231
VoIP inbound and outbound calls have no audio unless the SIP transformation settings are periodically disabled and re-enabled. Occurs when VoIP is working fine with a PBX (IPFX) server behind the firewall and then the firewall is upgraded to SonicOS 6.2.7.1.	188861

VPN

Resolved issue	Issue ID
Firewall1 fails to resolve the IPsec gateway domain whenever the WAN IP address changes on Firewall2. Occurs when a Tunnel Interface Site-to-Site VPN is configured between Firewall1 and Firewall2, where Firewall1 is using Dynamic WAN and DDNS, and Firewall2 is the IPsec gateway and is behind NAT with Keep Alive enabled and Initiator with FQDN set to the address of Firewall1.	190490
The firewall stops responding and stops passing traffic with a certain combination of VPN and DNS server configuration. Occurs when a site to site VPN with FQDN is configured as the WAN gateway, the primary DNS server is in a subnet behind the remote VPN, and a secondary DNS server is configured on the local side. If the VPN policy is disabled after adding it and then re-enabled, the firewall stops responding. It only occurs when the IP address is unresolved (0.0.0.0) in the VPN policy.	187008

Vulnerability

Resolved issue	Issue ID
A false positive PCI scan failure occurs for 80/tcp Web error message information leakage: /auth1.html. Occurs when the SonicWall appliance tries to send an error message related to One Time Password, which it shouldn't as the user did not try to login into the system.	189907

Wireless

Resolved issue	Issue ID
Multiple wireless clients cannot access the internet at the same time using Lightweight Hotspot Messaging. Occurs when one of following sequences takes place: • Wireless Client1 tries to access the internet, is redirected to the login page and logs in successfully. Wireless Client2 tries to access the internet, is redirected to the login page, but gets a “Session creation failed” error and cannot log in. • Wireless Client1 tries to access the internet, the page is redirected to the login page, but Client1 does not log in right away. Then, Wireless Client2 tries to access the internet, the page is redirected to the login page and Client2 logs in. The result is that Client1 is authenticated and can access the internet successfully, while Client2 is asked to log in every time while trying to access the internet.	190413

Known Issues

This section provides a list of known issues in this release.

3G/4G

Known issue	Issue ID
Traffic passes through the alternate WAN and it becomes the default gateway, although U0 was configured as the primary WAN and default gateway. Occurs when U0 is in Connect on Data mode and working fine as the primary WAN, with X1 connected and configured as the alternate WAN, and then the appliance is restarted.	190640

Application Firewall

Known issue	Issue ID
An application category match object is not added when using Application List Object, and an error popup is displayed, “Please add one or more applications.” Occurs when clicking **Add > Application List Object** on the **MANAGE | Objects > Match Objects** page, then selecting one or more categories on the **Category** screen and clicking **ACCEPT**.	187545

Command Line Interface

Known issue	Issue ID
The CLI does not display the item to delete for a custom list from the Geo-IP and Botnet configuration. Occurs when a custom Geo-IP list is added in the SonicOS web management interface and then the user attempts to delete it in the CLI, but the `no[TAB]` command from custom list mode does not cause the CLI to display anything to delete.	193210
Configuring a Geo-IP custom list results in the error “Error encountered processing command: geo-ip custom-list”. Occurs when configuring the Geo-IP custom list from the CLI.	193209

Content Filter Service

Known issue	Issue ID
A web site cannot be blocked by CFS for LDAP users with RADIUS Accounting. Occurs when a CFS policy is configured to block a category of web site, but an LDAP user authenticated by RADIUS Accounting is still able to access it.	192258

DPI-SSL

Known issue	Issue ID
In the **Common Name** screen of the **MANAGE | Decryption Services > DPI-SSL/TLS Client** page, the **Skip authenticating the server** option is selected when adding “cacert.org” as a common name, but it does not have the expected effect of skipping the authentication. Occurs when the **Always authenticate server for decrypted connections** option is enabled in the **General** screen, and then the user tries to access *https://cacert.org*, but the site is still authenticated as an untrusted site and blocked by DPI-SSL.	192439
In the **Common Name** screen of the **MANAGE | Decryption Services > DPI-SSL/TLS Client** page, the option **Skip CFS Category-based Exclusion** is selected when adding “bankofamerica.com” as a common name, but it does not have the expected effect of skipping such an exclusion. Occurs when a category such as “20. Online Banking” is selected for exclusion in the CFS Category-based Exclusion/Inclusion page, and then the user browses to *https://www.bankofamerica.com*, but the site is still excluded from inspection by DPI-SSL.	192438
The **Always authenticate server before applying exclusion policy** option in a custom exclusion policy for a common name such as *dropbox.com* is changed to disabled when saving the policy. Occurs when the **Always authenticate server before applying exclusion policy** option is set to the default setting **Use Global Setting** when adding the common name and saving it in the **Common Name** screen of the **MANAGE | Decryption Services > DPI-SSL/TLS Client** page.	192326

Networking

Known issue	Issue ID
Traffic cannot pass through a VLAN trunking interface because all incoming ARP requests are dropped. Occurs after removing the VLAN trunking interface from an LACP LAG. **Workaround**: Delete the VLAN trunk interface and then add the exact same configuration, or reboot the firewall.	191702
The broadcast/multicast packets generated by the Portshield port loop back and are received by the firewall again. Occurs when an interface is configured with a static IP in the LAN zone, a second interface is portshielded to it, and traffic is sent from the SonicOS diagnostic *ping* function to a PC connected to the static IP interface. The ARP request packets loop back to that interface.	189317
With two WAN interfaces configured, management traffic from the WAN side cannot reach the default gateway for the second WAN. Occurs when both WAN interfaces are configured with IPv6 static IP addresses, but the system default route from the interface IP to ANY was not created for the second WAN. **Workaround**: Manually add the route from the interface IPv6 IP to ANY for the second WAN.	189296

SonicWave / SonicPoint

Known issue	Issue ID
The **Floor Plan View** does not work in a High Availability deployment upon failover. Occurs when the Floor Plan information does not synchronize from the primary to the secondary unit in the HA pair.	193319

SSL VPN

Known issue	Issue ID
SSL VPN HTML5 bookmarks are not clickable, but are just text. Occurs when there is no port in the bookmark name when the access rule has a service limit to the bookmark. If the feature is used with default rules of ANY > ANY, the bookmarks work fine.	193657

Switching

Known issue	Issue ID
Unexpected failover occurs on a Stateful HA pair with Link Aggregation (LAG) configured. Occurs after deleting all the members and aggregate ports in the LAG.	193551
Traffic fails through L2 LAG. Occurs after upgrading from SonicOS 6.2.7 or 6.2.9 to 6.5.0.0 and then shutting down the aggregator port from the SonicOS management interface.	193305
Traffic fails through L2 LAG and a PC cannot get a dynamic IP address from the enabled DHCP server. Occurs when High Availability is enabled and then a LAG using Portshield mode or Trunk mode is created.	191790

User Interface

Known issue	Issue ID
“SIP” is displayed as a service object after upgrading to 6.5.0.0, but is a service group in factory default settings. Occurs after upgrading from SonicOS 6.2.7.1 or 6.2.9.0 to 6.5.0.0, when “SIP” was configured as a service object in the earlier version.	191327
The **MONITOR | User Sessions > Active Users** page continually refreshes when viewing a particular partition's status. Occurs when the default WAN interface is the only WAN interface, three partitions are added, some partition policies are configured, users log in from a partition, and then the user attempts to view a particular partition's status rather than viewing *All*.	190025

Users

Known issue	Issue ID
NTLM authentication fails for a domain PC with transparent domain user login enabled. Occurs when using Internet Explorer (IE 11) the second or third time that the user authenticates over NTLM.	193507
Mirrored LDAP user groups do not have the correct display name and cannot be edited. Upon opening the **Mirrored Groups** tab, all group names are formatted as “name@domain.com”. When editing a group, the error “Creating <domain>\<group-name>: Network Object not found” is displayed when **OK** is clicked. Occurs when the **Preferred display format for domain user/group names** option on the **Settings** screen in **Users > Local Users and Groups** is set to either of: • **Automatic (from the LDAP schema)** • **DOMAIN\name (Windows)** and user group mirroring is enabled in the LDAP settings.	193491

Users

Known issue	Issue ID
SonicOS displays “ERROR: Creating Mirrored Groups: Network Object not found” when adding or deleting a user to/from the Mirrored Groups, although the action is successfully applied. Occurs when the **Preferred display format for domain user/group names** option on the **Settings** screen in **Users > Local Users and Groups** is set to **Automatic (from the LDAP schema)** before mirroring is turned on.	193298
The browser does not redirect to the requested URL after NTLM authentication succeeds. Occurs about half of the time when using Firefox to browse to a website and NTLM is enabled for user authentication, RADIUS is configured, and there is an access rule requiring user authentication.	193291
In RADIUS Accounting configuration, the options on the **Forwarding** screen cannot be configured, which affects proper forwarding to all servers. Occurs when the **Try next on timeout** option cannot be disabled and the **Forward to all** option cannot be saved when enabled.	193214
SonicOS displays very high numbers for Intrusion Prevention in the **Threat Prevention Summary** table on the **MONITOR | Dashboard** page, and very high numbers for PING on the **Intrusions** screen of the **INVESTIGATE | AppFlow Reports** page. Occurs when there are only about 20 active users and seemingly not that many actual intrusions.	193137
The SSO agent/Terminal service agent/Radius Accounting client assigned to a partition are not moved to the default partition, but are still pointing to the old partition. Occurs after deleting the partition that had the agent/client assigned to it.	192825
The user authentication method is changed back to ***Local Users*** automatically after adding a new partition. Occurs after changing the user authentication method to **RADIUS**, **LDAP**, **RADIUS + Local Users**, or **LDAP+ Local Users** on the **Users > Settings** page.	192764
Partition domain names are not listed in the drop-down list on the SSL VPN portal page. Only ***LocalDomain*** is displayed in the list. Occurs after disabling and then re-enabling Authentication Partitioning. **Workaround**: Reboot the firewall or make some change to the partition domain name, then it will reappear.	192733
The Radius Accounting server denies an IPv4 SSL VPN user login sent by the RADIUS Accounting client with log message “User login denied due to bad credentials.” The user is not displayed on the User > Status page. Occurs after an IPv4 SSL VPN user logs in using correct credentials on the RADIUS Accounting client.	192554
Rebooting the firewall disables LDAP or RADIUS authentication for web, GVC, SSL VPN and L2TP client users. The **User authentication method** option reverts to ***Local Users***. Occurs only when Authentication Partitioning is enabled. **Workaround**: Enable the desired authentication again after restarting the appliance. In the **MANAGE** view, navigate to **Users > Settings**. On the **Authentication** screen, select the correct setting from the **User authentication method** drop-down list.	191014

Users

Known issue	Issue ID
After settings import, an additional “Any, Any, Any, Default” partition selection policy is created in **Users > Partitions** with the highest priority, causing partition authentication to fail. Occurs after the partition is working as expected, then the configuration settings are exported, and then the exp file is imported.	190377
Attempting to set the HTTPS port to 1443 results in an error that it is an invalid port. Changing it to 1444 works, but then the appliance allows login to SonicOS without the Authentication Required message on port 1444. Occurs when using SSH to connect to X0 and attempting to set the HTTPS port to one that has been successfully used in previous versions of SonicOS.	189580

X-Series

Known issue	Issue ID
The switch port cannot be discovered when connected to the child switch. Occurs when the IDV VLAN of a dedicated port is not allowed in the uplink ports between the parent and child switch.	193231
The port shield configuration of ports to a VLAN sub-interface is moved to parent interface in both parent and child switch. Occurs after failover in a dedicated uplink topology or with a common uplink.	193066
Importing configuration settings does not configure the primary switch uplink on the parent switch, all traffic fails, and the message “Unable to get port configuration from the external switch!” is displayed on the SonicWall appliance console. Occurs when importing settings from a topology with a common uplink and High Availability enabled.	192996
Adding a dedicated link in the parent switch does not program its native VLAN ID in the child switch and the message “unable to get etherlike counters from the external switch!” is displayed on the SonicWall appliance console. Occurs when using a dedicated uplink topology.	192920
A packet loop occurs after a failover with a certain topology. Occurs when an NSA 2650 HA pair is configured with a shared uplink and a dedicated uplink.	192807

System Compatibility

This section provides additional information about hardware and software compatibility with this release.

GMS Support

SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.5.0.0 requires GMS 8.4 for management of firewalls using the new features in SonicOS 6.5.0.0. SonicWall GMS 8.3 SP1 supports management of all other features in SonicOS 6.5.0.0 and earlier releases.

WAN Acceleration / WXA Support

The SonicWall WXA series appliances (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are supported for use with SonicWall security appliances running SonicOS 6.5.0.0. The recommended firmware version for the WXA series appliances is WXA 1.3.2.

Browser Support

SonicOS with Visualization uses advanced browser technologies such as HTML5, which are supported in most recent browsers. SonicWall recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS. This release supports the following Web browsers:

- Chrome 45.0 and higher
- Firefox 25.0 and higher
- IE Edge or IE 10.0 and higher
- Safari 10.0 and higher running on non-Windows machines

ⓘ **NOTE:** On Windows machines, Safari is not supported for SonicOS management.

ⓘ **NOTE:** Mobile device browsers are not recommended for SonicWall appliance system administration.

Product Licensing

SonicWall network security appliances must be registered on MySonicWall to enable full functionality and the benefits of SonicWall security services, firmware updates, and technical support. Log in or register for a MySonicWall account at https://mysonicwall.com.

Upgrading Information

For information about obtaining the latest firmware, upgrading the firmware image on your SonicWall appliance, and importing configuration settings from another appliance, see the *SonicOS 6.5 Upgrade Guide* available on the Support portal at https://www.sonicwall.com/en-us/support/technical-documentation.

SonicWall Support

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

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 video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- 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.

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

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

Legend

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

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

ⓘ **IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Last updated: 10/2/17

232-001703-00 Rev A