Release Notes

SonicOS

SonicOS 5.9.0.0 Release Notes

Contents

Release Purpose

SonicOS 5.9.0.0 is an Early Release for Dell SonicWALL NSA series network security appliances. It provides many new features.

Platform Compatibility

The SonicOS 5.9.0.0 release is supported on the following Dell SonicWALL Deep Packet Inspection (DPI) security appliances:

- NSA E8510
- NSA E8500
- NSA E7500
- NSA E6500
- NSA E5500
- NSA 5000
- NSA 4500
- NSA 3500

The Dell SonicWALL WXA series appliances (WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are also supported for use with Dell SonicWALL security appliances running SonicOS 5.9. The recommended firmware version for the WXA series appliances is 1.2.1.

Upgrading Information

For information about obtaining the latest firmware, upgrading the firmware image on your Dell SonicWALL appliance, and importing configuration settings from another appliance, see the *SonicOS 5.9 Upgrade Guide* available on MySonicWALL or on the www.sonicwall.com Product Documentation page for the NSA series:

http://www.sonicwall.com/us/en/support/3643.html

Browser Support

SonicOS with Visualization uses advanced browser technologies such as HTML5, which are supported in most recent browsers. Dell SonicWALL recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS.

This release supports the following Web browsers:

- Chrome 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 16.0 and higher
- Internet Explorer 8.0 and higher (do not use compatibility mode)
- Safari 5.0 and higher

Mobile device browsers are not recommended for Dell SonicWALL appliance system administration.

Known Issues

This section contains a list of known issues in the SonicOS 5.9.0.0 release. See the following categories:

3G/4G

Symptom	Condition / Workaround	Issue
The appliance can shut down or restart automatically if a 3G or 4G USB device is inserted or removed.	Occurs when inserting or removing a 3G/4G USB device while the appliance is powered on. Observed with a HuaWei E353 HSPA+ USB Stick. **Workaround**: The appliance should always be powered off when inserting or removing a USB device. Hot plug and play is not supported.	130973

Active/Active Clustering

Symptom	Condition / Workaround	Issue
The backup units do not synchronize with the updated configuration on the active units.	Occurs when all connection ports on both backup units are disconnected, then the CLI is used to configure X0 on an active unit to enable RIP and set “Send Only”, then the backup units are reconnected.	130316
No Virtual Group selection is available when using the Public Server Rule wizard on an Active/Active Clustering pair. The new policy is bound to Group 1.	Occurs when configuring a NAT policy and adding a public server for Group 2 from the Public Server Rule wizard. **Workaround**: Manually edit the NAT policy after using the wizard.	128631

Application Control

Symptom	Condition / Workaround	Issue
App Control policies do not block IPv6 traffic unless Intrusion Prevention Service (IPS) is enabled.	Occurs when IPS is disabled and an App Control policy is created from Firewall > App Control Advanced to block FTP traffic. A computer on the LAN side can still use an IPv6 IP address to connect to an FTP server. **Workaround**: Enable IPS. With IPS enabled, the App Control policy blocks the FTP connection	128410

DPI-SSL

Symptom	Condition / Workaround	Issue
The certificate from a secure website, such as https://mail.google.com, is not changed to the Dell SonicWALL DPI-SSL certificate when DPI-SSL is enabled, and the traffic cannot be inspected.	Occurs when a SonicPoint-N DR is connected to the appliance and Guest Services is enabled on the WLAN zone, and a wireless client connects via the SonicPoint, and the user logs into the guest account. Also, “Enable SSL Client Inspection” is set in the DPI-SSL > Client SSL page.	123097
An RDP remote desktop session cannot be established when DPI-SSL is enabled.	Occurs when the “Enable SSL Client Inspection” option is set in the DPI-SSL > Client SSL page, and a Windows 7 computer connects to the WLAN and then the user attempts to RDP to a Windows 7 computer on the LAN.	102701

High Availability

Symptom	Condition / Workaround	Issue
Logical monitoring and link aggregation features do not work when using High Availability probing.	Occurs when an IPv6 IP address is configured for the High Availability logical monitoring probe address. After the appliance is restarted, probing no longer works, causing issues with all logical monitoring and link aggregation.	131136

IPv6

Symptom	Condition / Workaround	Issue
An App Rules exclusion list configured with an IPv6 Address Object does not prevent the policy from blocking traffic.	Occurs when an IPv6 Address Object is configured with the IPv6 address of a computer on the LAN, and this AO is used when configuring an exclusion list for an App Rules policy. The IPv6 computer should be able to access IPv6 websites that match the policy, but they are still blocked by the App Rules policy.	128363

Log

Symptom	Condition / Workaround	Issue
After restarting the appliance, Syslog Format using Enhanced Syslog becomes the default.	Occurs when Enable Analyzer Settings is selected on the Log > Analyzer page and Enhanced Syslog is selected for Syslog Format on the Log > Syslog page. The Syslog Format using Enhanced Syslog setting persists across an appliance restart, although it should not.	130835

Networking

Symptom	Condition / Workaround	Issue
The value of ifHCInBroadcastPkts from an SNMP-GET differs from the value displayed for Rx Broadcast Packets in Network > Interfaces.	Occurs when comparing the Rx Broadcast Packets values shown in the Network > Interfaces page for each interface with the values obtained via SNMP.	131306
Wire Mode or Tap Mode cannot be configured because the IP Assignment field is disabled when editing an interface.	Occurs when editing an unassigned interface on a Stateful High Availability pair, and the WAN zone is selected. The IP Assignment field is set to Static and cannot be changed.	131050
SonicOS sends an “Unsupported Capability” error message and cannot connect to Amazon VPC.	Occurs when the “Use dynamic routing (requires BGP)” option is selected for the VPN connection in the Amazon WS VPC configuration. In SonicOS, BGP is configured to use a numbered tunnel interface with Amazon WS VPC.	127742
FTP and HTTP traffic does not pass through a pair of interfaces in Wire Mode, set to Secure. Ping still passes.	Occurs when using a Stateful High Availability pair with Active/Active DPI enabled. The Active/Active DPI data interface is set to X7, while the Wire Mode interfaces are X2 and X6 in the LAN zone. The traffic between X2 and X6 fails, but traffic passes on other, static, interfaces.	101359

Security Services

Symptom	Condition / Workaround	Issue
A Gateway Anti-Virus exclusion list does not prevent GAV from blocking downloads from excluded IP addresses.	Occurs when a FQDN Address Object is used when configuring the GAV exclusion list.	121984

SSL VPN

Symptom	Condition / Workaround	Issue
The WAN interface becomes unresponsive to Ping or HTTPS requests after a high number of NetExtender logins.	Occurs when 1000 NetExtender logins and logouts have taken place at a rate of one every 3 seconds, using a Linux NetExtender client, with the client inactivity timeout set to 10 minutes.	131421
NetExtender login fails with the log entry “'IP address in pool is exhausted” after 917 successful logins using NetExtender.	Occurs when 1000 NetExtender logins were previously successful and the client IP address pool has 1000 addresses in it.	131186

System

Symptom	Condition / Workaround	Issue
The administrator cannot access configuration mode on the LCD panel. The LCD panel displays an Invalid Code error message.	Occurs when the PIN code for the LCD panel is changed on the System > Administration page, and then the admin selects the configuration option on the LCD panel and enters the new PIN code.	130379
GMS 7.1 cannot synchronize with SonicOS after the appliance restarts following One Touch Configuration changes.	Occurs when password complexity is changed via One Touch Configuration from GMS. The One Touch Configuration options for Stateful Firewall Security require passwords containing alphabetic, numeric and symbolic characters. If the appliance has a simple password, such as the default “password”, GMS cannot log in after the restart, and cannot be prompted to change the password.	124998
The SonicOS management interface cannot be used to manage the appliance and large Ethernet packets are not forwarded.	Occurs when the management computer is connected to an H3C 10GE switch which is connected in Trunk mode to a second switch and then connected to an NSA E8510 10GE interface.	121657

User Interface

Symptom	Condition / Workaround	Issue
The LDAP configuration button is missing on the Users > Settings page.	Occurs when the user authentication method for login is set to Local Users, and Single Sign-On is enabled with its method for setting user group memberships configured as LDAP Lookup.	127691

Users

Symptom	Condition / Workaround	Issue
Single Sign-On (SSO) only works on Active-Active Clustering Virtual Group 1. SSO does not work on other Virtual Groups.	Occurs when SSO agents are configured in a clustered environment. Virtual Group 1 has a green status. However, all other Virtual Groups have a red status and do not work with the SSO Agent.	120202
Single Sign-On (SSO) does not work when Guest Services is enabled.	Occurs when both SSO and Guest Services are enabled. Guest Services blocks SSO authentication.	119001

VoIP

Symptom	Condition / Workaround	Issue
SonicOS drops SIP packets from the WAN to a Layer 2 Bridged LAN interface, and cannot establish a VoIP call. Ping works across the same path. The call can be established when using the primary LAN interface.	Occurs when interface X5 (LAN) is configured in L2 bridge mode and bridged to X0 (LAN). A Cisco phone is connected to X5 and is used to make a call to a phone on the WAN side, but the call cannot be established.	128225

VPN

Symptom	Condition / Workaround	Issue
An active IPv6 VPN tunnel is not displayed in the table on the VPN > Settings screen of the head-end firewall.	Occurs when two IPv6 VPN tunnels are created on both the head-end appliance and a remote appliance. The head-end VPN > Settings screen shows “2 Currently Active IPv6 Tunnels”, but only displays one tunnel in the Currently Active VPN Tunnels table.	128633
An OSPF connection cannot be established between an NSA 240 and an NSA 7500.	Occurs when a VPN tunnel is configured between the two appliances, with Advanced Routing enabled on the NSA 240 and a numbered tunnel interface is created on the NSA 7500 and bound to the VPN tunnel. A VLAN is created on the NSA 240 with an IP address in the same subnet as the Tunnel Interface on the NSA 7500. OSPF is enabled on both appliances, but the NSA 240 does not respond to the OSPF “Hello” packet, and the OSPF connection cannot be established.	128419
User cannot change a Manual Key VPN policy to an IKE policy.	Occurs when the user attempts to change a Manual Key VPN policy to an IKE policy. The following message appears, "Remote IKE ID must be specified." **Workaround:** Delete the Manual Key policy and add a new IKE policy with the same IPsec gateway and source/destination networks.	112988
OSPF routing does not work properly after the VPN policy is deleted and re-created unless the appliance is restarted.	Occurs when a Tunnel Interface VPN policy is deleted and then re-created, with OSPF properly configured. OSPF will not connect until the appliance or the HA pair is restarted.	101510

Supported Features by Appliance Series

The following table lists the key features in SonicOS 5.9 and shows which appliance series supports them.

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 215 Series	TZ 210 Series	TZ 205 Series	TZ 200 Series	TZ 105 Series	TZ 100 Series
Active-Active Clustering	✓	✗	✗	✗	✗	✗	✗	✗
Amazon VPC Support	✓	✓[1]	✗	✗	✗	✗	✗	✗
AppFlow Reports	✓	✓	✓	✓	✗	✗	✗	✗
App Rules Enhancement	✓	✓	✓	✓	✓	✗	✓	✗
ArcSight Syslog Format Support	✓	✓	✓	✓	✓	✗	✓	✗
Bandwidth Management Enhancement	✓	✓	✓	✓	✓	✓	✓	✓
BGP Advanced Routing	✓	✓[2]	✓[3]	✗	✗	✗	✗	✗
CLI Enhancements[4]	✓	✓	✓	✓	✓	✓	✓	✓
Common Access Card Support	✓	✓	✓	✓	✓	✓	✓	✓
IKEv2 Configuration Payload Support	✓	✓	✓	✓	✓	✓	✓	✓
IKE Dead Peer Detection	✓	✓	✓	✓	✓	✓	✓	✓
IPv6	✓	✓	✓	✓	✓	✗	✓	✗
LDAP User Group Monitoring	✓	✓	✓	✓	✓	✓	✓	✓
LDAP Group Membership by Organizational Unit	✓	✓	✓	✓	✓	✓	✓	✓
Logging Enhancement	✓	✓	✓	✓	✓	✓	✓	✓
MOBIKE	✓	✓	✓	✓	✓	✗	✓	✗
NetExtender WXAC Integration	✓	✓	✓	✓	✓	✓	✓	✓
Network Device Protection Profile (NDPP Mode)	✓	✓	✓	✓	✓	✓	✓	✓
Numbered Tunnel Interfaces for Route Based VPN	✓	✓[5]	✗	✗	✗	✗	✗	✗

[1] Not supported on NSA 240 or NSA 220 series.
[2] Not supported on NSA 240. NSA 250M series and NSA 220 series require a license for BGP.
[3] Requires License
[4] Limited CLI command set is supported on NSA 240 and all TZ models
[5] Supported only on NSA 250M and higher models; not supported on NSA 2400MX

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 215 Series	TZ 210 Series	TZ 205 Series	TZ 200 Series	TZ 105 Series	TZ 100 Series
One-Touch Configuration Overrides	✓	✓	✓	✓	✓	✗	✓	✗
OpenSSH Vulnerability Security Enhancements	✓	✓	✓	✓	✓	✓	✓	✓
Path MTU Discovery	✓	✓	✓	✓	✓	✓	✓	✓
Proxied Users Identification and login	✓	✓	✓	✓	✓	✓	✓	✓
Reassembly-Free Regular Expression for DPI Engine	✓	✓	✓	✓	✓	✗	✓	✗
SHA-2 in IPsec	✓	✓	✓	✓	✓	✓	✓	✓
SNMPv3	✓	✓	✓	✓	✓	✓	✓	✓
SSL-VPN Multi-Core Scalability	✓	✓	✓	✗	✓	✗	✗	✗
SSO RADIUS Accounting	✓	✗	✗	✗	✗	✗	✗	✗
TSR Enhancements	✓	✓	✓	✓	✓	✓	✓	✓
UDP/ICMP Flood Protection	✓	✓	✓	✓	✓	✗	✓	✗
Wire Mode 2.0	✓	✓[6]	✗	✗	✗	✗	✗	✗
WWAN 4G support	✓	✓	✓	✓	✓	✓	✓	✗
XD Lookup for Access Rules	✓	✓	✓	✓	✓	✓	✓	✓
YouTube for Schools Support	✓	✓	✓	✓	✓	✓	✓	✓

[6] Supported only on NSA 3500 and higher models

SonicPoint and Wireless Features

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 215 Series	TZ 210 Series	TZ 205 Series	TZ 200 Series	TZ 105 Series	TZ 100 Series
External Guest Service Apache / PHP support	✓	✓	✓	✓	✓	✓	✓	✓
External Guest Service FQDN support	✓	✓	✓	✓	✓	✓	✓	✓
Guest Admin Support	✓	✓	✓	✓	✓	✗	✓	✗
Internal Radio IDS scan scheduling[7]	✗	✓	✓	✓	✓	✓	✓	✓
SonicPoint 802.11e (WMM) QoS	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint Auto Provisioning	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint retain custom configuration	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint DFS support	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint Diagnostics Enhancement	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint FairNet Support	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint RADIUS Server Failover	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint WPA TKIP Countermeasures and MIC Failure Flooding Detection and Protection	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint Layer 3 Management	✓	✓[8]	✓	✗	✗	✗	✗	✗
Traffic Quota-based Guest Svc Policy	✓	✓	✓	✓	✓	✓	✓	✓
Virtual Access Point ACL Support	✓	✓	✓	✓	✓	✗	✓	✗
Virtual Access Point group sharing across dual radios	✓	✓	✓	✓	✓	✓	✓	✓
Virtual Access Point Layer 2 bridging	✓	✓	✓	✓	✓	✓	✓	✓
Virtual Access Point scheduling	✓	✓	✓	✓	✓	✗	✓	✗
Wireless Client Bridge Support[9]	✗	✓	✓	✓	✓	✓	✓	✓
Wireless PCI Rogue detect/prevention	✓	✓	✓	✓	✓	✓	✓	✓
Wireless Radio Built-in Scan Sched[10]	✗	✓	✓	✓	✓	✓	✓	✓

[7] Only supported on platforms with internal wireless radio

[8] Not supported on NSA 240

[9] Only supported on platforms with internal wireless radio

[10] Only supported on platforms with internal wireless radio

Key Features in SonicOS 5.9

The following are the key features in the SonicOS 5.9 release:

Active/Active Clustering in SonicOS

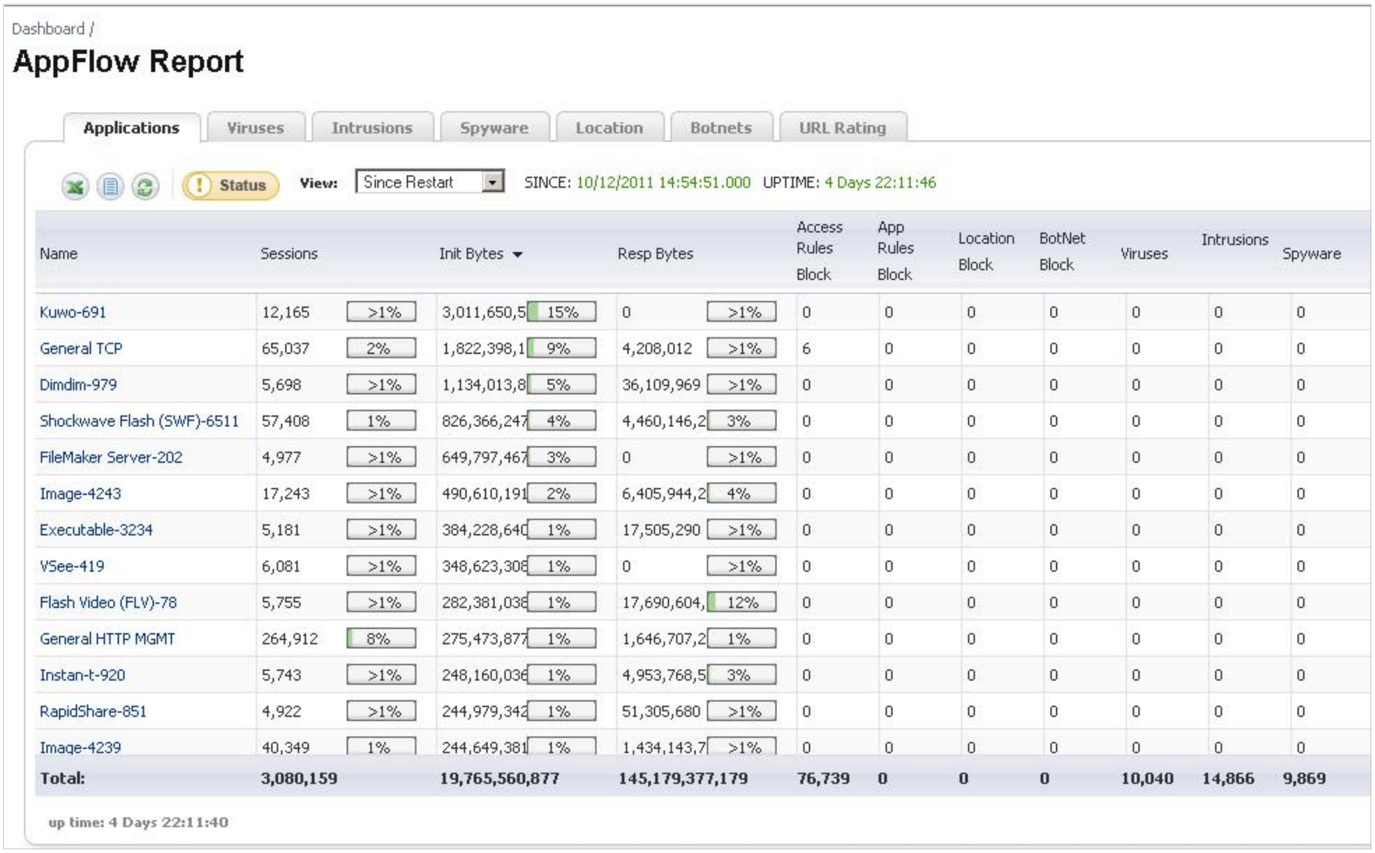
Active/Active Clustering is the most recent addition to the High Availability feature set in SonicOS. With Active/Active Clustering, you can assign certain traffic flows to each node in the cluster, providing load sharing in addition to redundancy, and supporting a much higher throughput without a single point of failure.

A typical recommended setup includes four firewalls of the same SonicWALL model configured as two Cluster Nodes, where each node consists of one Stateful HA pair. For larger deployments, the cluster can include eight firewalls, configured as four Cluster Nodes (or HA pairs). Within each Cluster Node, Stateful HA keeps the dynamic state synchronized for seamless failover with zero loss of data on a single point of failure. Stateful HA is not required, but is highly recommended for best performance during failover.

AppFlow Report

The **Dashboard > AppFlow Reports** page provides administrators with configurable scheduled reports by applications, viruses, intrusions, spyware, and URL rating. AppFlow Reports statistics enable network administrators to view a top-level aggregate report of what is going on in your network. This enables network administrators to answer the following questions with a quick glance:

- What are the top most used applications running in my network?
- Which applications in terms of total number of sessions and bytes consume my network bandwidth?
- Which applications have viruses, intrusions, and spyware?
- What website categories are my users visiting?



Dashboard /

AppFlow Report

View: Since Restart SINCE: 10/12/2011 14:54:51.000 UPTIME: 4 Days 22:11:46

Name	Sessions		Init Bytes ▼		Resp Bytes		Access Rules Block	App Rules Block	Location Block	BotNet Block	Viruses	Intrusions	Spyware
Kuwo-691	12,165	>1%	3,011,650,5	15%	0	>1%	0	0	0	0	0	0	0
General TCP	65,037	2%	1,822,398,1	9%	4,208,012	>1%	6	0	0	0	0	0	0
Dimdim-979	5,698	>1%	1,134,013,8	5%	36,109,969	>1%	0	0	0	0	0	0	0
Shockwave Flash (SWF)-6511	57,408	1%	826,366,247	4%	4,460,146,2	3%	0	0	0	0	0	0	0
FileMaker Server-202	4,977	>1%	649,797,467	3%	0	>1%	0	0	0	0	0	0	0
Image-4243	17,243	>1%	490,610,191	2%	6,405,944,2	4%	0	0	0	0	0	0	0
Executable-3234	5,181	>1%	384,228,640	1%	17,505,290	>1%	0	0	0	0	0	0	0
VSee-419	6,081	>1%	348,623,308	1%	0	>1%	0	0	0	0	0	0	0
Flash Video (FLV)-78	5,755	>1%	282,381,038	1%	17,690,604,	12%	0	0	0	0	0	0	0
General HTTP MGMT	264,912	8%	275,473,877	1%	1,646,707,2	1%	0	0	0	0	0	0	0
Instan-t-920	5,743	>1%	248,160,036	1%	4,953,768,5	3%	0	0	0	0	0	0	0
RapidShare-851	4,922	>1%	244,979,342	1%	51,305,680	>1%	0	0	0	0	0	0	0
Image-4239	40,349	1%	244,649,381	1%	1,434,143,7	>1%	0	0	0	0	0	0	0
Total:	**3,080,159**		**19,765,560,877**		**145,179,377,179**		**76,739**	**0**	**0**	**0**	**10,040**	**14,866**	**9,869**

up time: 4 Days 22:11:40

The report data can be viewed from the point of the last system restart, since the system reset, or by defining a schedule range. The page also provides the ability to schedule a report sent by FTP or by email.

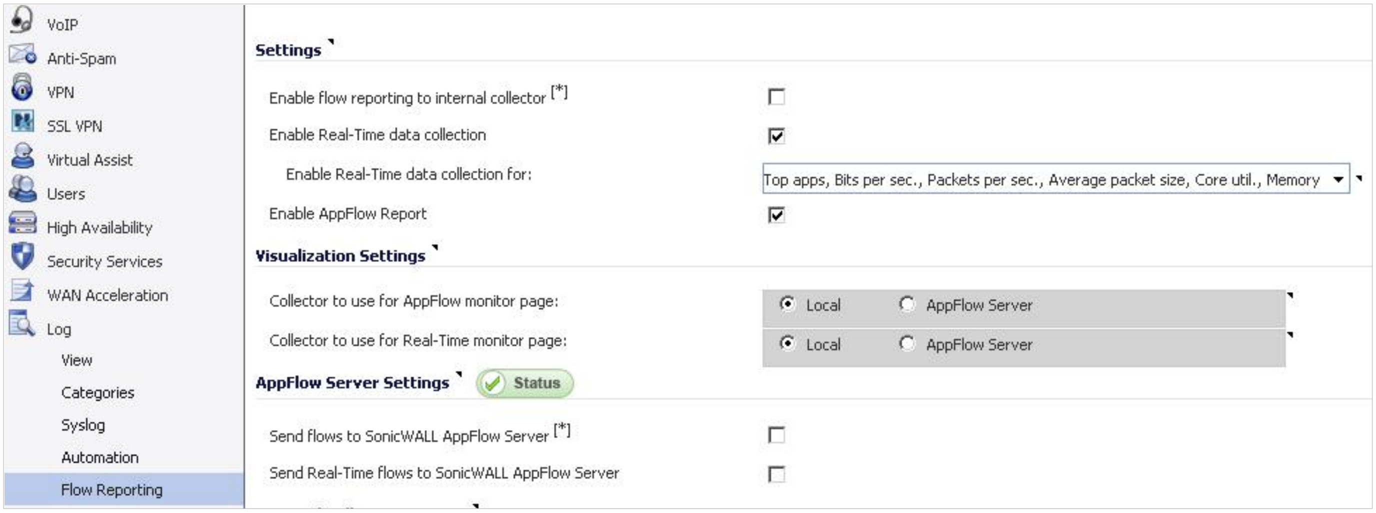
The following reports are currently supported:

- Applications
- Intrusions

- Viruses
- Spyware
- Botnet
- Locations
- Rating

NOTE: These features must be licensed and enabled in order to get a complete AppFlow report.

To enable this feature, select the **Enable AppFlow report** option on the **Log > Flow Reporting** page.



Settings

Enable flow reporting to internal collector [*] □

Enable Real-Time data collection ☑

Enable Real-Time data collection for: Top apps, Bits per sec., Packets per sec., Average packet size, Core util., Memory

Enable AppFlow Report ☑

Visualization Settings

Collector to use for AppFlow monitor page: ● Local ○ AppFlow Server

Collector to use for Real-Time monitor page: ● Local ○ AppFlow Server

AppFlow Server Settings Status

Send flows to SonicWALL AppFlow Server [*] □

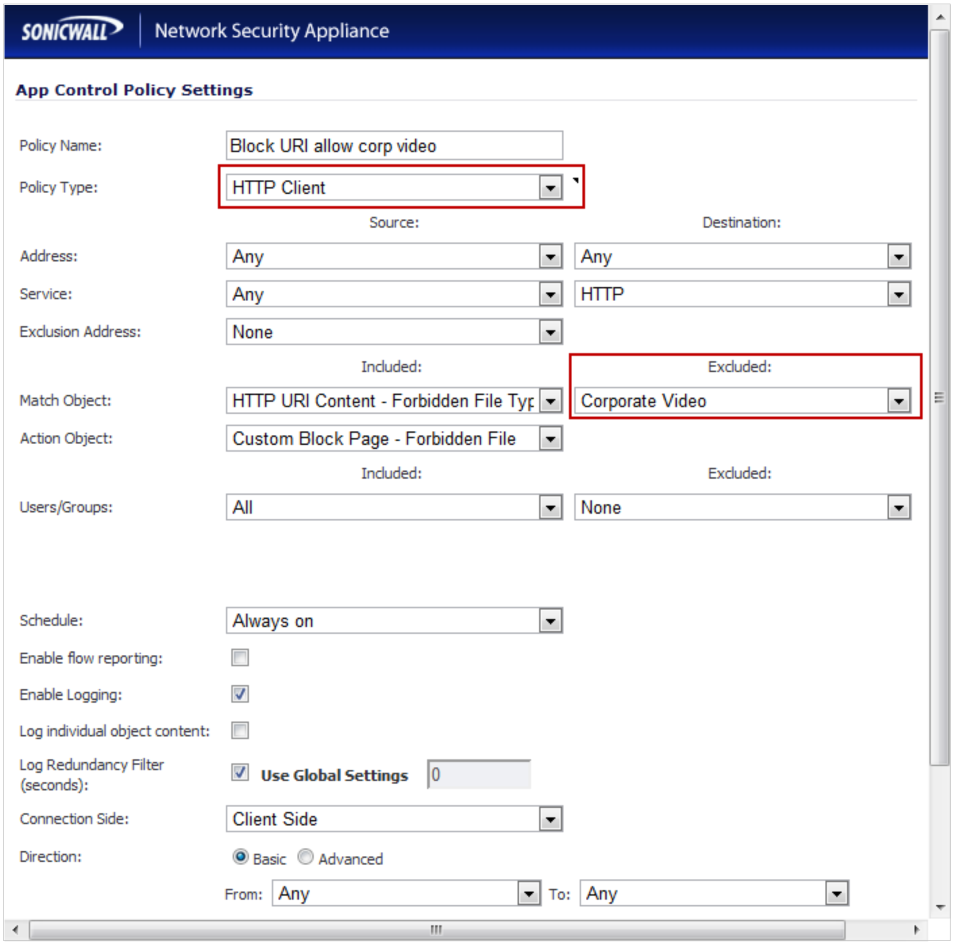
Send Real-Time flows to SonicWALL AppFlow Server □

App Rules Enhancements: Excluded and HTTP URL Match Objects

SonicOS 5.9 introduces the following enhancements to App Rule configuration:

- **HTTP Client Excluded Match Object –** When configuring an App Rule with the policy type HTTP Client, a new Excluded Match Objet option has been added to further refine the App Rule. The Excluded Match Object is used to exclude a certain object from the Match Object for the App Rule. For example, you could block all of sonicwall.com except for sales.sonicwall.com. To do so, you would create two HTTP Host objects with the host names sonicwall.com and sales.sonicwall.com. You would then create an App Rule with the following settings:
    - Policy Type: HTTP Client
    - Included Match Object: sonicwall.com
    - Excluded Match Object: sales.sonicwall.com

If the Action Object was set to block this App Rule, all of sonicwall.com would be blocked except for sales.sonicwall.com.



App Control Policy Settings

Policy Name:	Block URI allow corp video	
Policy Type:	HTTP Client	
	Source:	Destination:
Address:	Any	Any
Service:	Any	HTTP
Exclusion Address:	None	
	Included:	Excluded:
Match Object:	HTTP URI Content - Forbidden File Typ	Corporate Video
Action Object:	Custom Block Page - Forbidden File	
	Included:	Excluded:
Users/Groups:	All	None
Schedule:	Always on	
Enable flow reporting:	□	
Enable Logging:	☑	
Log individual object content:	□	
Log Redundancy Filter (seconds):	☑ Use Global Settings 0	
Connection Side:	Client Side	
Direction:	● Basic ○ Advanced	
	From: Any	To: Any

NOTE: The Excluded Match Object does not take affect when the Included Match Object is set to a Custom Object.

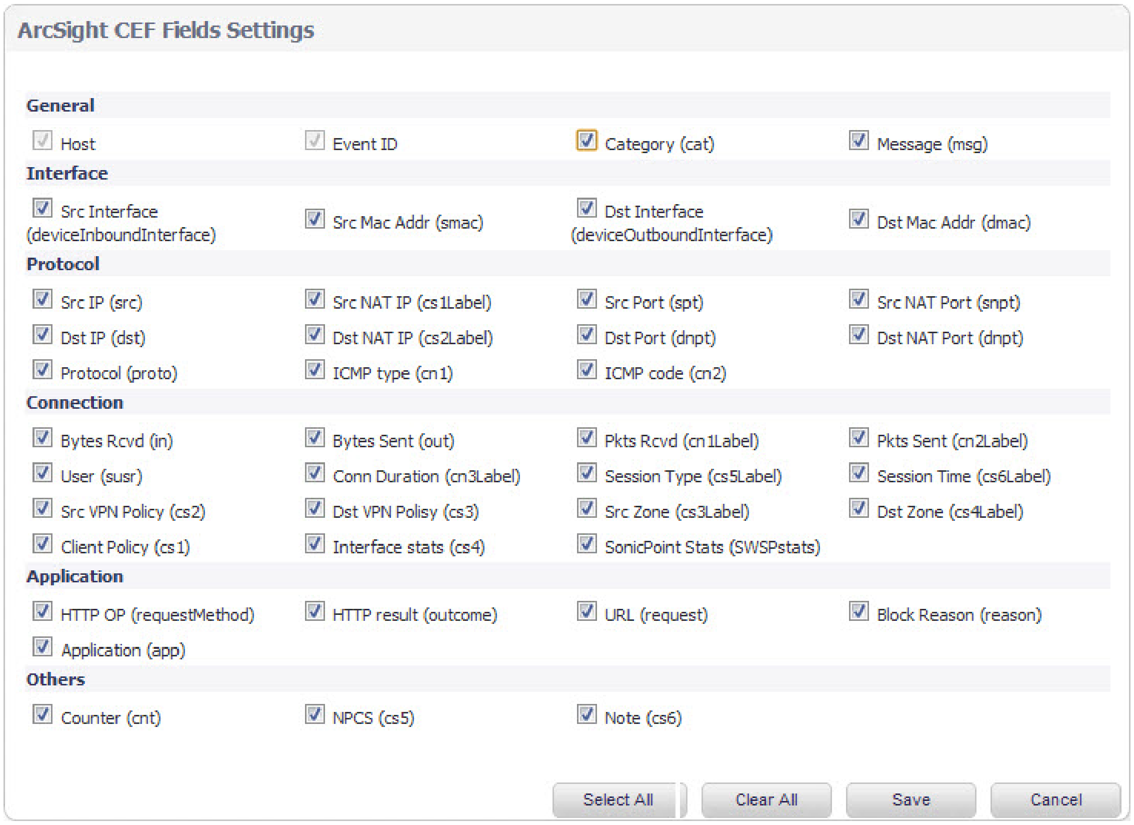
- **HTTP URL Match Object** – The new HTTP URL Match Object type matches both HTTP hosts and HTTP URI content.

ArcSight Syslog Format Support

SonicOS can now generate Syslog messages in the ArcSight format. To configure ArcSight Syslog, navigate to the **Log > Syslog** page, and select **ArcSight** for the **Syslog forma**t.

NOTE: To configure ArcSight syslog, both ViewPoint and Analyzer must be disabled (on the **Log > ViewPoint** and **Log > Analyzer** pages, respectively).

Click the configure icon to specify which categories of Syslog messages will be logged.



ArcSight CEF Fields Settings

General

☑ Host ☑ Event ID ☑ Category (cat) ☑ Message (msg)

Interface

☑ Src Interface (deviceInboundInterface) ☑ Src Mac Addr (smac) ☑ Dst Interface (deviceOutboundInterface) ☑ Dst Mac Addr (dmac)

Protocol

☑ Src IP (src) ☑ Src NAT IP (cs1Label) ☑ Src Port (spt) ☑ Src NAT Port (snpt)
☑ Dst IP (dst) ☑ Dst NAT IP (cs2Label) ☑ Dst Port (dnpt) ☑ Dst NAT Port (dnpt)
☑ Protocol (proto) ☑ ICMP type (cn1) ☑ ICMP code (cn2)

Connection

☑ Bytes Rcvd (in) ☑ Bytes Sent (out) ☑ Pkts Rcvd (cn1Label) ☑ Pkts Sent (cn2Label)
☑ User (susr) ☑ Conn Duration (cn3Label) ☑ Session Type (cs5Label) ☑ Session Time (cs6Label)
☑ Src VPN Policy (cs2) ☑ Dst VPN Polisy (cs3) ☑ Src Zone (cs3Label) ☑ Dst Zone (cs4Label)
☑ Client Policy (cs1) ☑ Interface stats (cs4) ☑ SonicPoint Stats (SWSPstats)

Application

☑ HTTP OP (requestMethod) ☑ HTTP result (outcome) ☑ URL (request) ☑ Block Reason (reason)
☑ Application (app)

Others

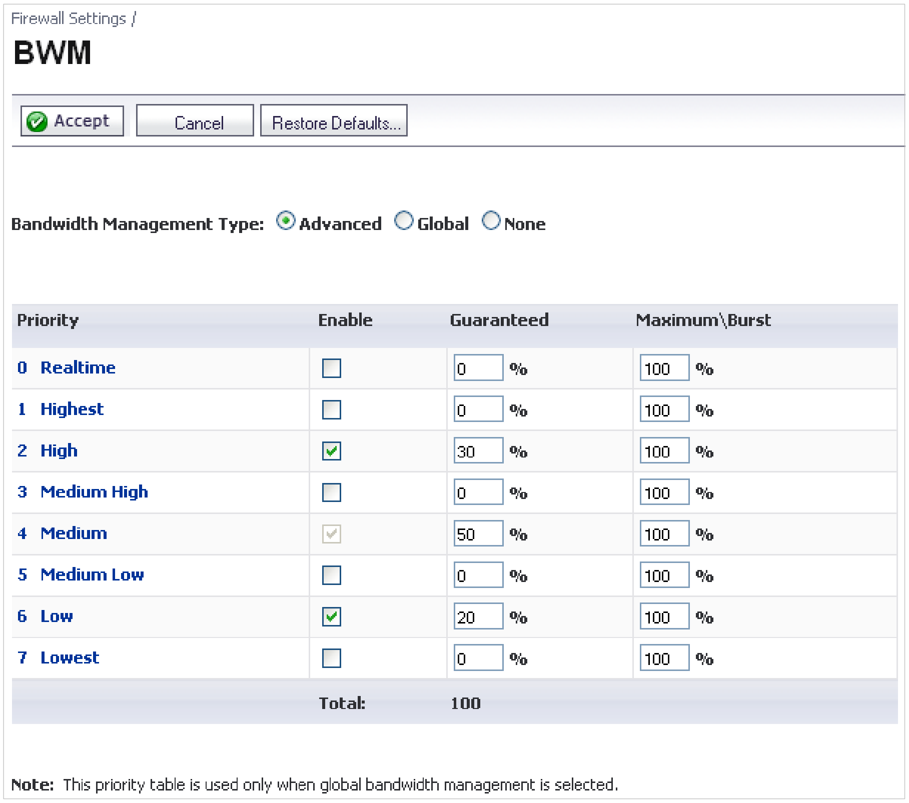
☑ Counter (cnt) ☑ NPCS (cs5) ☑ Note (cs6)

A Syslog server must be configured with the ArcSight Logger application to decode the ArcSight messages. ArcSight Logger runs on a Linux 64-bit platform with CentOS 5.4.

Bandwidth Management Enhancement

The Enhanced Bandwidth Management feature provides extensive enhancements to SonicOS BWM functionality, including the following:

- Advanced Bandwidth Management option – Provides a new priority table for configuring Bandwidth Management on the **Firewall Settings > BWM** page when the Bandwidth Management Type radio button is set to Advanced.

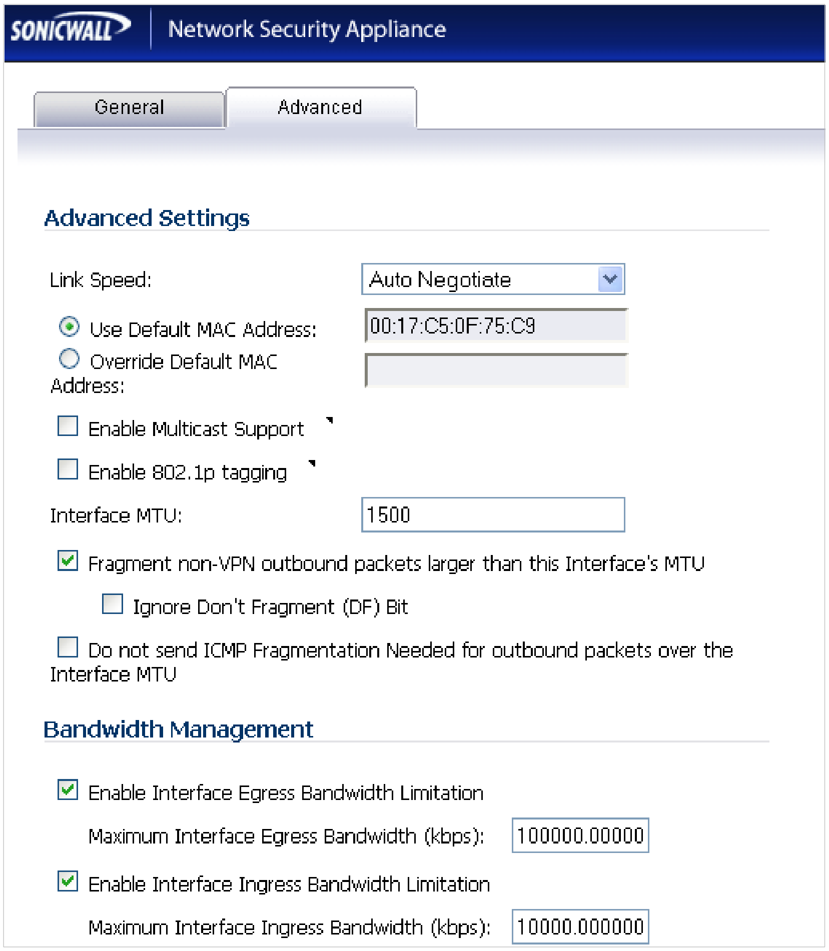


Bandwidth Management Type: ● Advanced ○ Global ○ None

Priority	Enable	Guaranteed	Maximum\Burst
0 Realtime	□	0 %	100 %
1 Highest	□	0 %	100 %
2 High	☑	30 %	100 %
3 Medium High	□	0 %	100 %
4 Medium	☑	50 %	100 %
5 Medium Low	□	0 %	100 %
6 Low	☑	20 %	100 %
7 Lowest	□	0 %	100 %
	Total:	100	

Note: This priority table is used only when global bandwidth management is selected.

- Interface Bandwidth Limitation – Provides the ability to edit Maximum Interface Egress/Ingress Bandwidth on a per interface basis.



Advanced Settings

Link Speed: Auto Negotiate

● Use Default MAC Address: 00:17:C5:0F:75:C9

○ Override Default MAC Address:

□ Enable Multicast Support

□ Enable 802.1p tagging

Interface MTU: 1500

☑ Fragment non-VPN outbound packets larger than this Interface's MTU

□ Ignore Don't Fragment (DF) Bit

□ Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU

Bandwidth Management

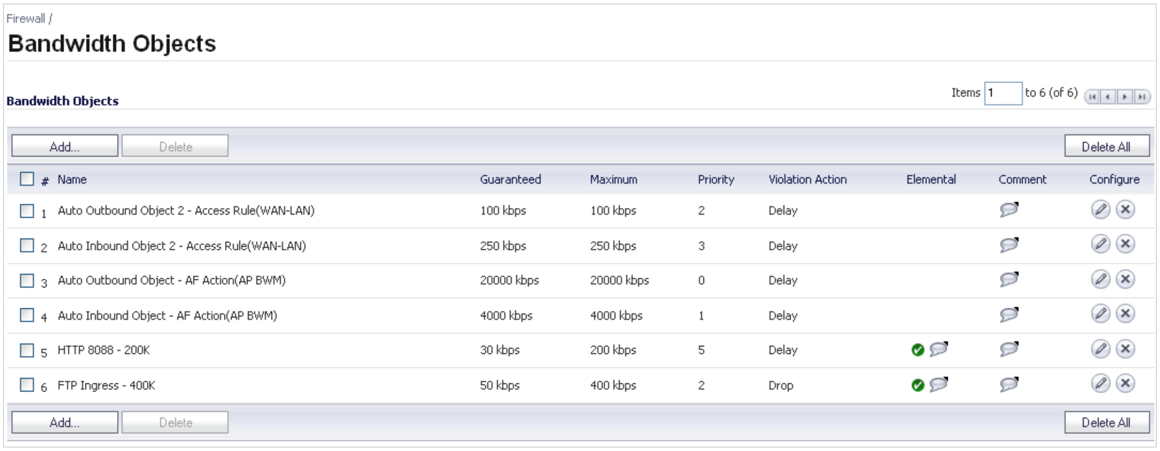
☑ Enable Interface Egress Bandwidth Limitation

Maximum Interface Egress Bandwidth (kbps): 100000.00000

☑ Enable Interface Ingress Bandwidth Limitation

Maximum Interface Ingress Bandwidth (kbps): 10000.000000

- Bandwidth Objects – Provides the ability to configure Bandwidth Objects that offer new granularity in bandwidth management configuration on the new **Firewall > Bandwidth Object** page.

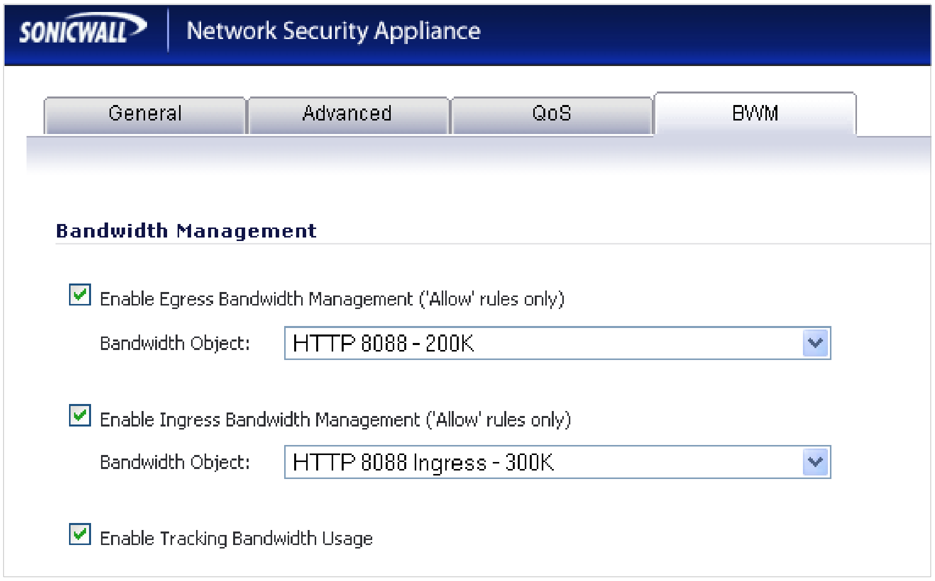


Bandwidth Objects

Bandwidth Objects

□ #	Name	Guaranteed	Maximum	Priority	Violation Action	Elemental	Comment	Configure
□ 1	Auto Outbound Object 2 - Access Rule(WAN-LAN)	100 kbps	100 kbps	2	Delay			
□ 2	Auto Inbound Object 2 - Access Rule(WAN-LAN)	250 kbps	250 kbps	3	Delay			
□ 3	Auto Outbound Object - AF Action(AP BWM)	20000 kbps	20000 kbps	0	Delay			
□ 4	Auto Inbound Object - AF Action(AP BWM)	4000 kbps	4000 kbps	1	Delay			
□ 5	HTTP 8088 - 200K	30 kbps	200 kbps	5	Delay	✓		
□ 6	FTP Ingress - 400K	50 kbps	400 kbps	2	Drop	✓		

- Access Rule BWM Settings – Provides the ability to edit bandwidth settings for Access Rules.



Bandwidth Management

☑ Enable Egress Bandwidth Management ('Allow' rules only)

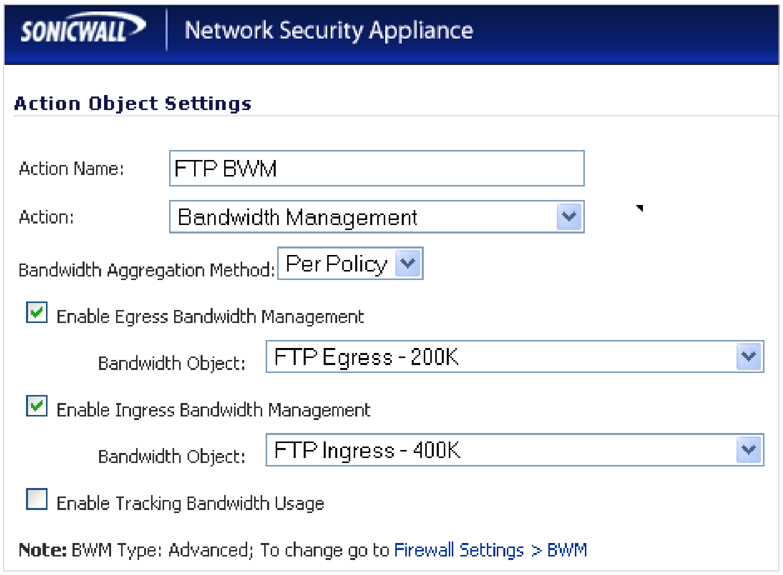
Bandwidth Object: HTTP 8088 - 200K

☑ Enable Ingress Bandwidth Management ('Allow' rules only)

Bandwidth Object: HTTP 8088 Ingress - 300K

☑ Enable Tracking Bandwidth Usage

- Edit Application Firewall Policy Settings – Provides the ability to edit bandwidth setting for Application Firewall policies.



Action Object Settings

Action Name: FTP BWM

Action: Bandwidth Management

Bandwidth Aggregation Method: Per Policy

☑ Enable Egress Bandwidth Management

Bandwidth Object: FTP Egress - 200K

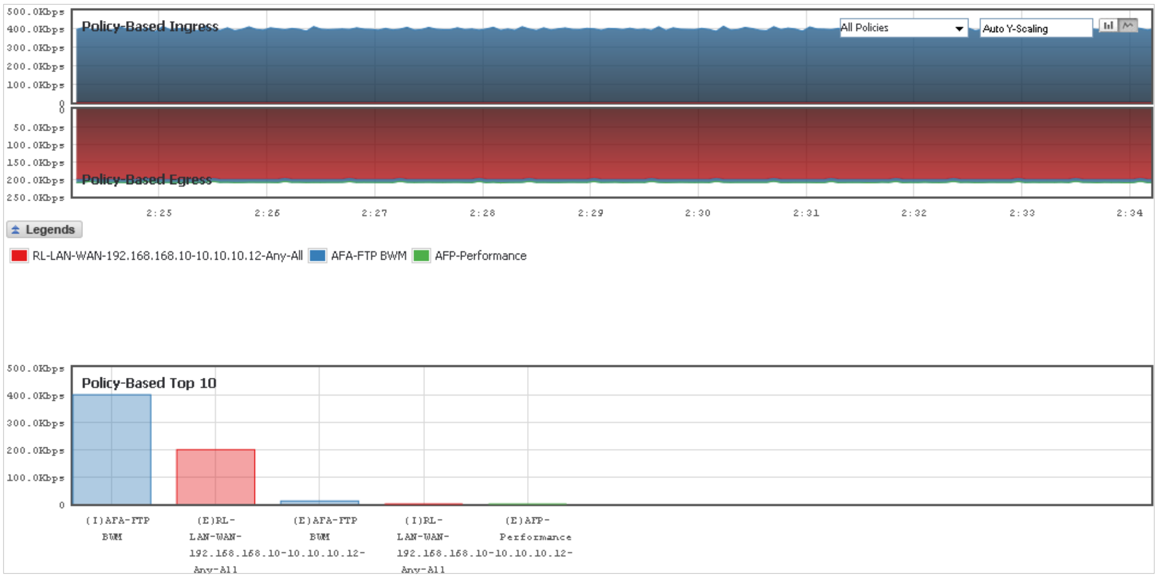
☑ Enable Ingress Bandwidth Management

Bandwidth Object: FTP Ingress - 400K

☐ Enable Tracking Bandwidth Usage

Note: BWM Type: Advanced; To change go to Firewall Settings > BWM

- Show Bandwidth Usage Statistics – Provide dynamic bandwidth usage reporting graphs on the new **Firewall > Bandwidth Reporting** page and as part of the AppFlow Monitor.



BGP Advanced Routing

Border Gateway Protocol (BGP) advanced routing is a large-scale routing protocol used to communicate routing information between Autonomous Systems (AS's), which are well-defined, separately administered network domains. The current SonicOS implementation of BGP is most appropriate for "single-provider / single-homed" environments, where the network uses one ISP as their Internet provider and has a single connection to that provider. SonicOS BGP is also capable of supporting "single-provider / multi-homed" environments, where the network uses a single ISP but has a small number of separate routes to the provider. Because BGP transmits packets in the clear, SonicOS supports using an IPsec tunnel for secure BGP sessions. The IPsec tunnel is configured independently within the VPN configuration section of the SonicOS Web-based management interface, while BGP is enabled on the **Network > Routing** page and then configured on the SonicOS Command Line Interface.

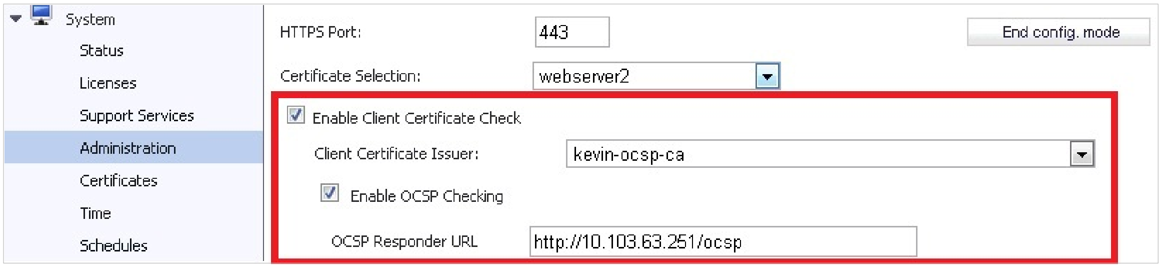
CLI Enhancements

SonicOS 5.9 introduces a new, more-robust, enterprise-level Command Line Interface (E-CLI). The CLI can be accessed via the console and SSH. The new CLI is designed to follow the organization of the SonicOS management GUI. New commands are available in the following categories:

- Commands for user authentication settings: These are commands to do with managing settings governing user authentication and maintenance of user sessions, as per settings on the Users / Settings page in the management GUI.
- Commands for local users and user groups: These are commands to do with users and user groups in the appliance's local database, as per settings on the Users / Local Users and Local Groups pages in the management GUI.
- Commands for displaying user status: These are commands to do with displaying information on current user sessions etc., equivalent to the information shown on the Users / Status page in the management GUI.
- Commands for guest services: These are commands to do with configuring guest services, as per settings on the Users / Guest Services and Guest Accounts pages in the management GUI.
- Commands for displaying guest status: These are commands to do with displaying information on current guest sessions, equivalent to the information shown on the Users / Guest Status page in the management GUI.
- Commands for user other authentication related features: These are commands for configuring and displaying information about the following other features related to user authentication (RADIUS, LDAP, Single Sign On).

Common Access Card Support

The Common Access Card (CAC) is a smart card issued by the United States Department of Defense (DoD). 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. Although this feature is developed to meet CAC requirements, it can be used for any scenario which requires client certificate in the HTTPS/SSL connection. CAC support is enabled on the System > Administration page by selecting the **Enable Client Certificate Check** option.



HTTPS Port: 443

Certificate Selection: webserver2

☑ Enable Client Certificate Check

Client Certificate Issuer: kevin-ocsp-ca

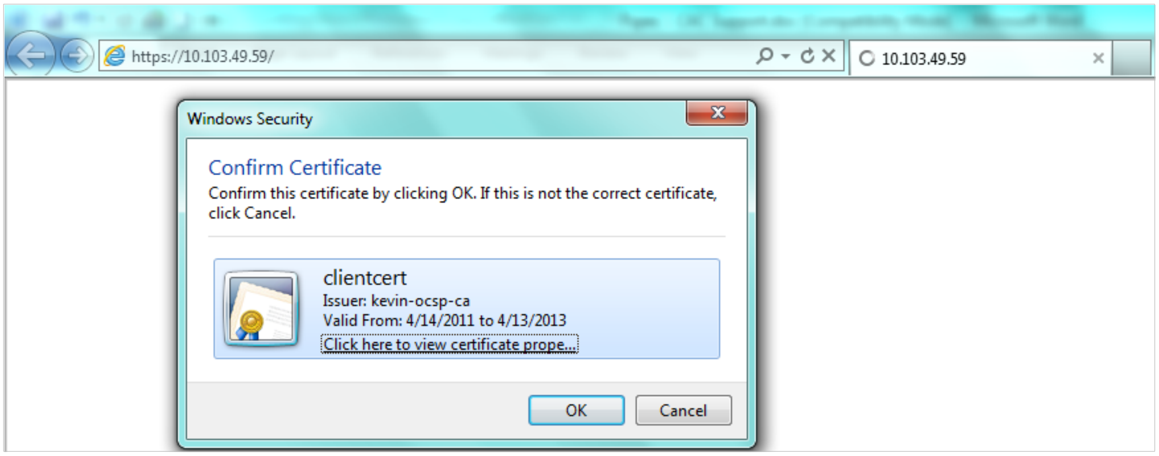
☑ Enable OCSP Checking

OCSP Responder URL http://10.103.63.251/ocsp

CAC is only supported for HTTPS management. Optionally, an additional Online Certificate Status Protocol (OSCP) check can verify the authenticity certificate.

Users do not need to perform any configuration. When the CAC Smart Card is inserted into the PC, the card imports client certificates to the Internet Explorer personal certificate store automatically. The certificate selection window pops up when customer initiates HTTPS management.

Note: The CAC card is designed to work automatically with Internet Explorer. CAC certificates can be manually imported into other browsers.



Confirm Certificate

Confirm this certificate by clicking OK. If this is not the correct certificate, click Cancel.

clientcert
Issuer: kevin-ocsp-ca
Valid From: 4/14/2011 to 4/13/2013
Click here to view certificate prope...

When the Dell SonicWALL security appliance receives the client certificate, it verifies it with the certificate issuer and then redirects the user to the regular admin login page. If OCSP is enabled, the browser will be redirect to an OCSP Pending page while the appliance performs the OSCP check.

IKEv2 Configuration Payload

In IKEv2, the configuration payload is used to exchange configuration between IKE peers. Most commonly occurring in the endpoint-to-security-gateway scenario, an endpoint may need an IP address in the network protected by the security gateway and may need to have that address dynamically assigned.

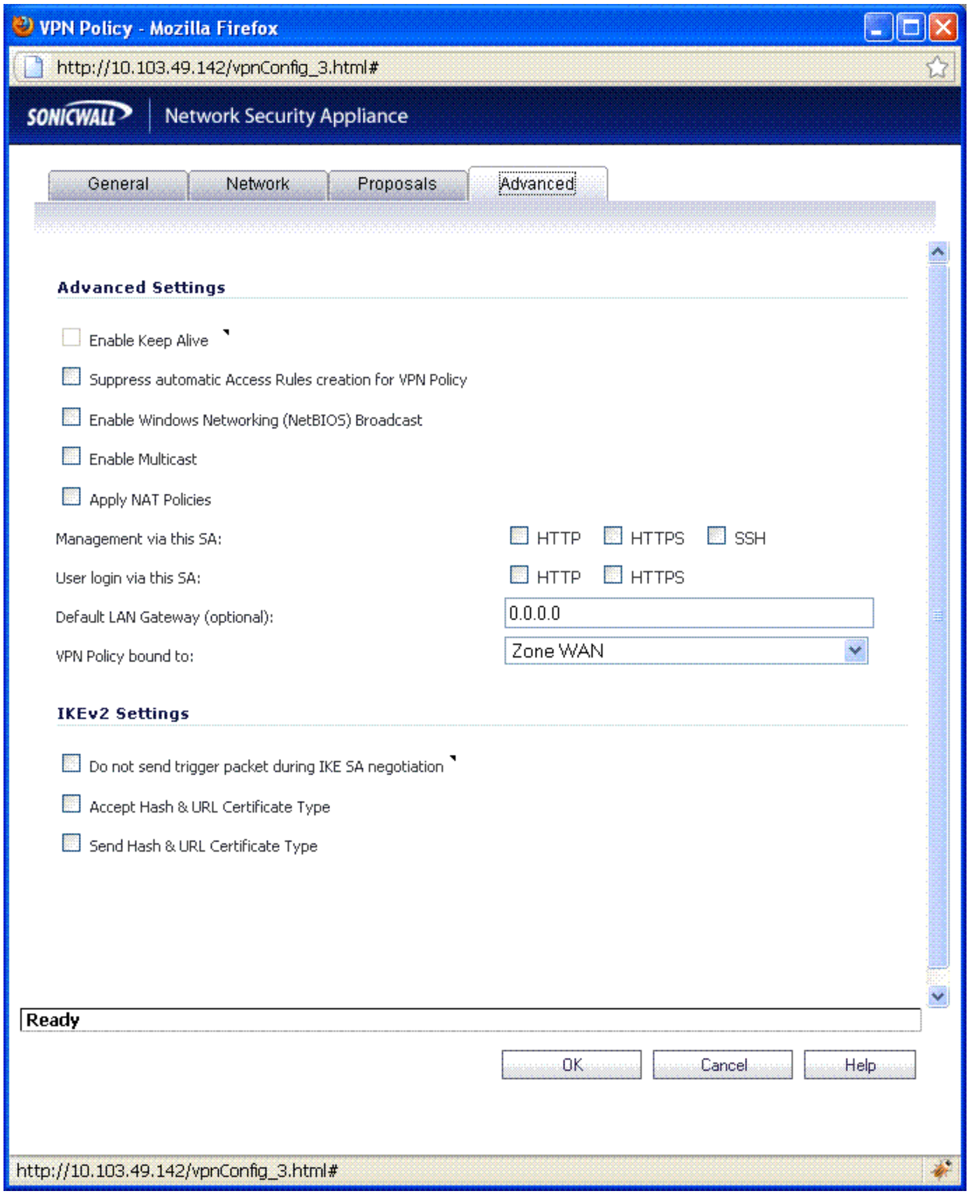
When IKEv2 is selected as the exchange type on the Proposals tab of the Edit VPN Policy window, the new **Use IKEv2 IP Pool** option is available on the Network tab. When this option is selected, the VPN policy is used as IRAS which can handle the CP IKEv2 payload. When firewall receives a CP from IKEv2 client, the firewall allocates an IP address from the IKEv2 IP Pool Address Object (which is selected in the **Use IKEv2 IP Pool** option).

Selecting the **Use IKEv2 IP Pool** option means that the IKEv2 client can only access the network included in Local Networks. If the destination IP address is not in the range of Local Networks, the packet will be dropped after it is decapsulated from ESP packet. When configuring the IP pool, the Address Object of the pool should not overlap with other IKEv2 IP pools or the Remote Networks of any other VPN policies.

When using IKEv2, the authentication method must be 3rd party certificates. The certificate installed on the remote access server should have the following values for fields in the certificate:

- Common Name (CN): This field should contain the fully qualified DNS name or IP address of the remote access server. If the server is located behind a NAT router, then the certificate must contain the fully qualified DNS name or IP address of the external connection of the NAT router (the address that the client computer sees as the address of the server).
- EKU: For a certificate to be used to authenticate an IKEv2 connection, the certificate must specify an EKU field that includes Server Authentication. If there is more than one server authentication certificate, the IP security IKE intermediate EKU should also be included. Only one certificate should have both EKU options, otherwise IPsec cannot determine which certificate to use, and may not use the correct certificate.

Several IKEv2 settings are added to the Advanced tab of the VPN Policy window.



http://10.103.49.142/vpnConfig_3.html#

Advanced Settings

☐ Enable Keep Alive

☐ Suppress automatic Access Rules creation for VPN Policy

☐ Enable Windows Networking (NetBIOS) Broadcast

☐ Enable Multicast

☐ Apply NAT Policies

Management via this SA: ☐ HTTP ☐ HTTPS ☐ SSH

User login via this SA: ☐ HTTP ☐ HTTPS

Default LAN Gateway (optional): 0.0.0.0

VPN Policy bound to: Zone WAN

IKEv2 Settings

☐ Do not send trigger packet during IKE SA negotiation

☐ Accept Hash & URL Certificate Type

☐ Send Hash & URL Certificate Type

Ready

http://10.103.49.142/vpnConfig_3.html#

IPv6

The following table summarizes the IPv6 features that are supported in SonicOS 5.9.

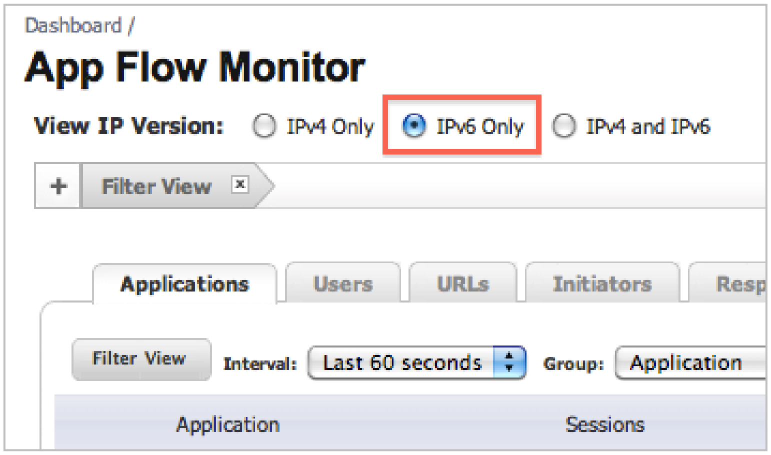
IPv6 Features Supported	**IPv6 Features Not Currently Supported**
• 6to4 tunnel (allows IPv6 nodes to connect to outside IPv6 services over an IPv4 network) • Access Rules • Address Objects • Anti-Spyware • Application Firewall • Attack prevention: o Land Attack o Ping of Death o Smurf o SYN Flood • Connection Cache • Connection Limiting for IPv6 connections • Connection Monitor • Content Filtering Service • DHCP • DNS client • DNS lookup and reverse name lookup • Dynamic Routing (RIPng and OSPFv3) • EPRT • EPSV • FTP • Gateway Anti-Virus • High Availability: o Connection Cache o FTP o IPv6 management IP address o NDP o SonicPoint • HTTP/HTTPS management over IPv6 • ICMP • IKEv2 • Intrusion Prevention Service • IP Spoof Protection • IPv4 Syslog messages, including messages with IPv6 addresses • Layer 2 Bridge Mode • Logging IPv6 events • Login uniqueness • Multicast Routing with Multicast Listener Discovery • NAT • Neighbor Discovery Protocol • NetExtender connections for users with IPv6 addresses • Packet Capture • Ping • Policy Based Routing • PPPoE • Remote management	• Anti-Spam • Command Line Interface • DHCP over VPN • DHCP Relay • Dynamic Address Objects for IPv6 addresses • Dynamic DNS • FQDN • Global VPN Client (GVC) • GMS • H.323 • High Availability: o Multicast o Oracle SQL/Net o RTSP o VoIP • IKEv1 • IPv6 Syslog messages • L2TP • LDAP • MAC-IP Anti-Spoof • NAT between IPv6 and IPv4 addresses • NAT High Availability probing • NAT load balancing • NetBIOS over VPN • NTP • QoS Mapping • RADIUS • RAS Multicast Forwarding • Route-based VPNs • Single Sign On • SIP • SMTP Real-Time Black List (RBL) Filtering • SSH • Transparent Mode • ViewPoint • Virtual Assistant • Web proxy • Wiremode

IPv6 Features Supported	IPv6 Features Not Currently Supported
• Security services for IPv6 traffic with DPI • Site-to-site IPv6 tunnel with IPsec for security • SonicPoint IPv6 support • SNMP • SSL VPN • Stateful inspection of IPv6 traffic • User status • Visualization • VLAN interfaces with IPv6 addresses • VPN policies • Wireless	

The IPv6 features supported in the SonicOS 5.9 release are described below:

- **IPv6 Visualization in AppFlow Monitor and Real-Time Monitor** — With the new visualization dashboard monitoring improvements, administrators are able to respond more quickly to network security vulnerabilities and network bandwidth issues. Administrators can see what websites their employees are accessing, what applications and services are being used in their networks and to what extent, in order to police content transmitted in and out of their organizations.

  The **AppFlow Monitor** page has two new options for the **View IP Version** selection. These allow you to monitor **IPv6 only** or **IPv4 and IPv6** traffic.


Dashboard /

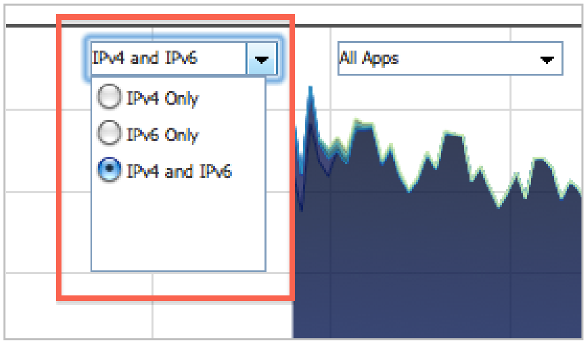
App Flow Monitor

View IP Version: ○ IPv4 Only ● IPv6 Only ○ IPv4 and IPv6

Interval: Last 60 seconds

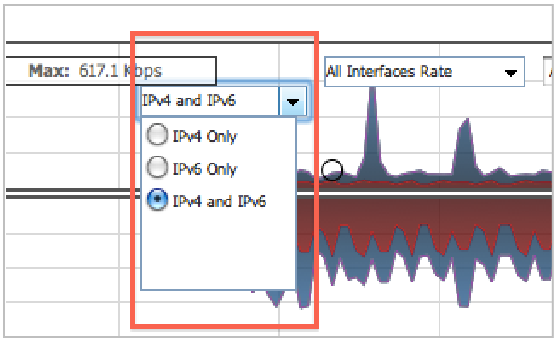
Group: Application

  The Real-Time Monitor page has the same two new options under the Interface drop-down menu in the **Applications** and **Bandwidth** panels.


IPv4 and IPv6

All Apps

○ IPv4 Only
○ IPv6 Only
● IPv4 and IPv6

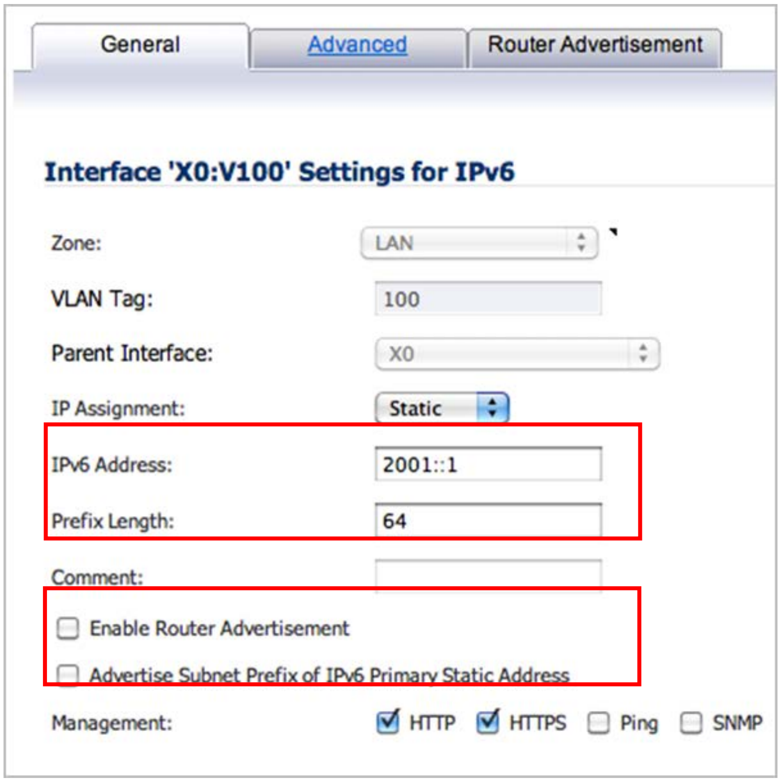

Max: 617.1 kbps

IPv4 and IPv6

All Interfaces Rate

○ IPv4 Only
○ IPv6 Only
● IPv4 and IPv6

- **IPv6 VLAN Support** – SonicOS 5.9 supports VLAN interfaces for IPv6 addresses, IPv6 NAT policies, and IPv6 IPsec policy on the IPv6 VLAN interfaces. The General tab has two new text fields, **IPv6 Address** and **Prefix Length**, and two new checkboxes, **Enable Router Advertisement** and **Advertise Subnet Prefix of IPv6 Primary Static Address**.



Interface 'X0:V100' Settings for IPv6

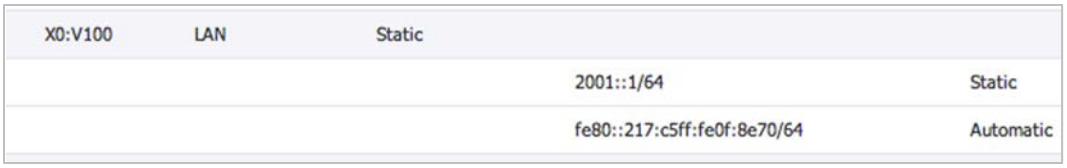
Zone:	LAN
VLAN Tag:	100
Parent Interface:	X0
IP Assignment:	Static
IPv6 Address:	2001::1
Prefix Length:	64
Comment:	

☐ Enable Router Advertisement

☐ Advertise Subnet Prefix of IPv6 Primary Static Address

Management: ☑ HTTP ☑ HTTPS ☐ Ping ☐ SNMP

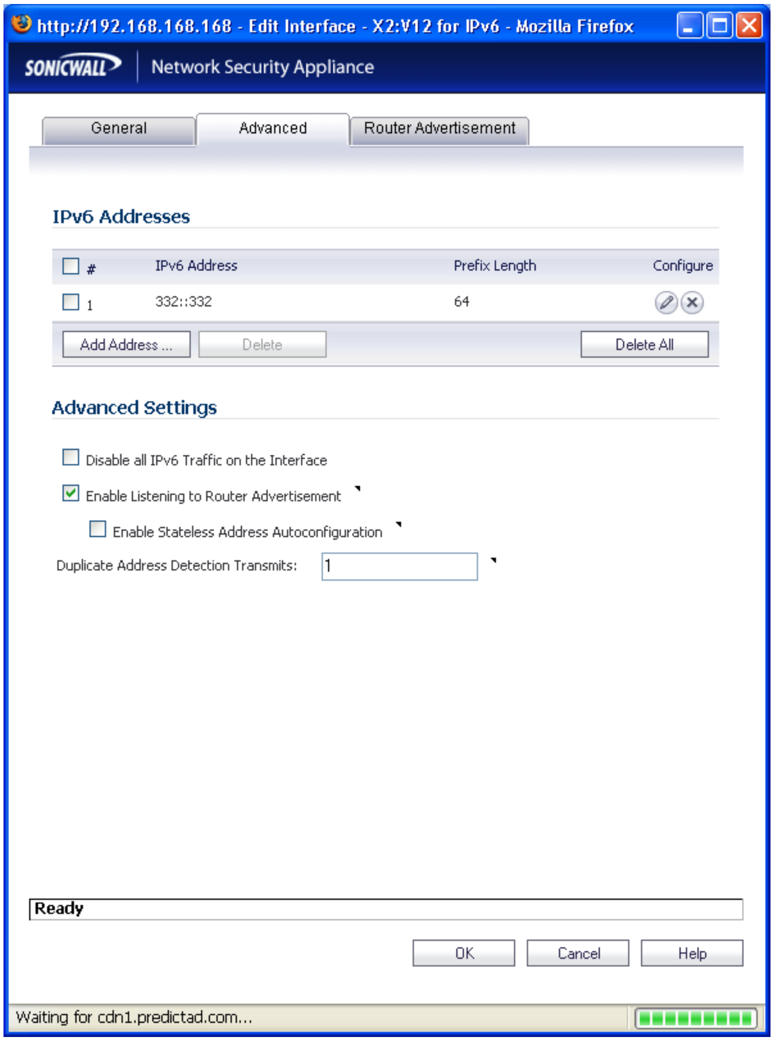
After you click **OK**, the VLAN will be displayed on the **Interface** page.



X0:V100	LAN	Static		
			2001::1/64	Static
			fe80::217:c5ff:fe0f:8e70/64	Automatic

NOTE: IPv6 sub-interfaces support Auto, Static, and DHCPv6 IP Assignment mode.

The **Advanced** tab has been modified as follows to fit the needs of configuring an IPv6 VLAN.



http://192.168.168.168 - Edit Interface - X2:V12 for IPv6 - Mozilla Firefox
SONICWALL
Network Security Appliance
General
Advanced
Router Advertisement

IPv6 Addresses

□ #	IPv6 Address	Prefix Length	Configure
□ 1	332::332	64	

Add Address ...
Delete
Delete All

Advanced Settings

□ Disable all IPv6 Traffic on the Interface

☑ Enable Listening to Router Advertisement

□ Enable Stateless Address Autoconfiguration

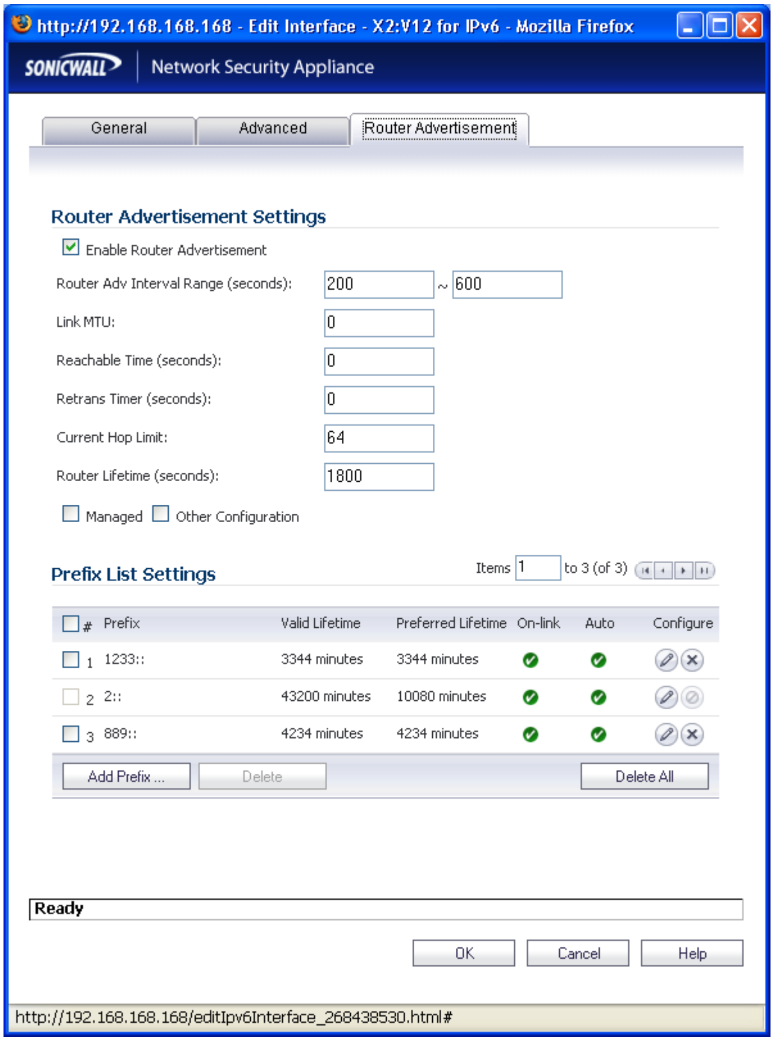
Duplicate Address Detection Transmits: 1

Ready

OK
Cancel
Help
Waiting for cdn1.predictad.com...

The **Router Advertisement** tab has been modified as follows to fit the needs of configuring an IPv6 VLAN with Router Advertisement. Consider the following when configuring Router Advertisement:

- Multiple IPv6 addresses can be configured on a sub-interface like they can be on a physical interface.
- The zone of any interface or VLAN sub-interface can only be changed in the IPv4 view of the item.


http://192.168.168.168 - Edit Interface - X2:V12 for IPv6 - Mozilla Firefox
SONICWALL
Network Security Appliance
General
Advanced
Router Advertisement
OK
Cancel
Help
Add Prefix ...
Delete
Delete All

Router Advertisement Settings

☑ Enable Router Advertisement

Router Adv Interval Range (seconds):	200 ~ 600
Link MTU:	0
Reachable Time (seconds):	0
Retrans Timer (seconds):	0
Current Hop Limit:	64
Router Lifetime (seconds):	1800

☐ Managed ☐ Other Configuration

Prefix List Settings

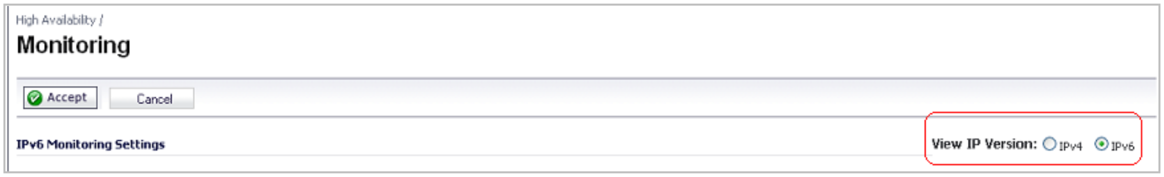
Items 1 to 3 (of 3)

☐ #	Prefix	Valid Lifetime	Preferred Lifetime	On-link	Auto	Configure
☐ 1	1233::	3344 minutes	3344 minutes	✓	✓	
☐ 2	2::	43200 minutes	10080 minutes	✓	✓	
☐ 3	889::	4234 minutes	4234 minutes	✓	✓	

Ready

http://192.168.168.168/editIpv6Interface_268438530.html#

- **IPv6 HA Monitoring Support** – Support for High Availability Monitoring through IPv6 address. A new **View IP Version:** option is added to the **High Availability > Monitoring** page.



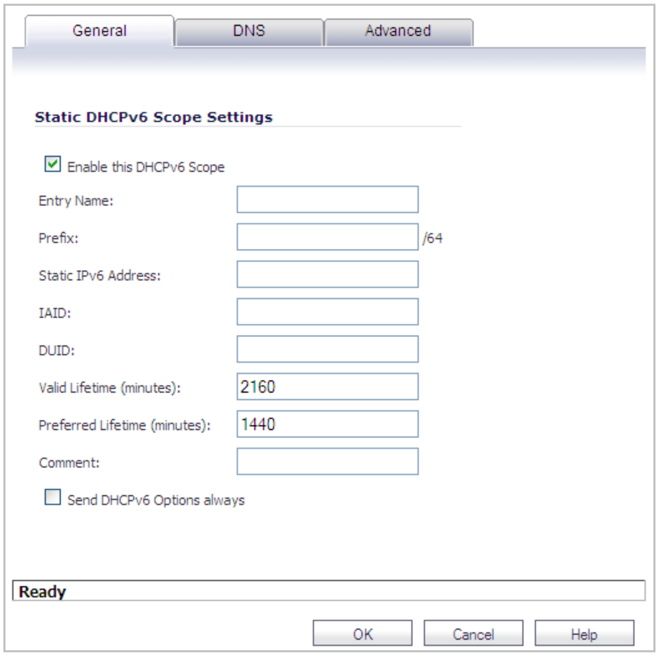
IPv6 Monitoring Settings

View IP Version: ○ IPv4 ● IPv6

Consider the following to make sure your IPv6 HA configuration works correctly:

- Primary/Backup IPv6 address must be in the same subnet of the interface, and it cannot be same as global IP and link-local-IP of primary and backup appliance.
- If primary/back monitoring IP is set (not ::), they cannot be same.
- If Management checkbox is enabled, the primary/backup monitoring IP cannot be unspecified (i.e., ::)
- If probe checkbox is enabled, the probe IP cannot be unspecified.

- **DHCPv6 Decline Message and Static DHCPv6** Support – Supports DHCPv6 static lease and Lease Persistent on the **Network > DHCP Server** page and **Network > DHCP Server > Add Static** page. The configuration page is modified so that DHCP IPv6 can be configured.



Static DHCPv6 Scope Settings

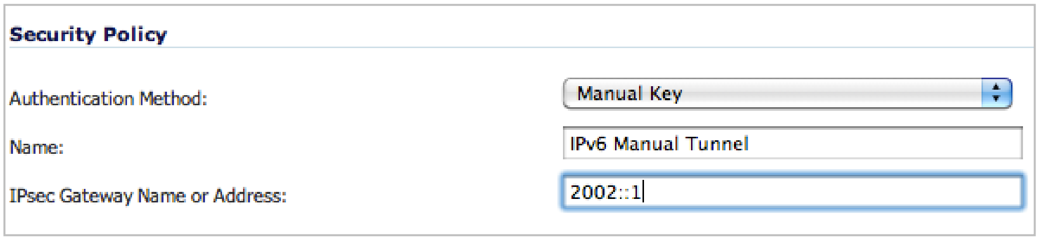
☑ Enable this DHCPv6 Scope

Entry Name:	
Prefix:	/64
Static IPv6 Address:	
IAID:	
DUID:	
Valid Lifetime (minutes):	2160
Preferred Lifetime (minutes):	1440
Comment:	

□ Send DHCPv6 Options always

Ready

- **IPv6 VPN Manual Key Policy** – Provides Manual Key Authentication for IPv6 VPN Policy.



Security Policy

Authentication Method:	Manual Key
Name:	IPv6 Manual Tunnel
IPsec Gateway Name or Address:	2002::1

LDAP User Group Mirroring

LDAP User Group Mirroring provides the ability to manage LDAP User Groups only on the LDAP server without needing to do any duplication of that on the Dell SonicWALL appliance. The groups and group-group memberships will be periodically read from the LDAP server via the existing import mechanism and local user groups will be created to mirror them.

The name of the local user group that is auto-created to mirror one on the LDAP server will include the domain where the group is located, formatted name@domain.com. This will ensure that we have a unique user group name when mirroring user groups from multiple domains.

The following will apply for these auto-created mirror user groups:

- They will not be user-deletable, and the group name and comment will not be editable (the latter will show as “Mirrored from LDAP”).
- The appliance administrator will be able to add local users to them as members, but will not be able to add any member groups (member groups can only be set on the LDAP server).
- They will allow setting VPN client access networks, CFS policy, SSLVPN bookmarks and other settings as per other user groups.
- They will be selectable in access rules, App rules, IPS policies, etc.
- If a user group is deleted on the LDAP server its mirror group will be automatically deleted if it is not being used by anything, but it will not be deleted if it has been set in any access rules, App rules, IPS policies, etc.
- On disabling LDAP user group mirroring the local mirror user groups will not be deleted, but they will be changed to be user-deletable. If it is subsequently re-enabled then they will be changed back.
- If a mirrored group name matches a user-created (non-mirrored) local user group the latter will not get replaced, but its group memberships will get updated to reflect any group nestings set on the LDAP server.
- If a user group name is found on the LDAP server with a name that matches one of the default user groups on the UTM appliance, then no local mirror user group will be created for it. Instead the memberships in that default user group will be updated to reflect any user group nestings present in the group read from LDAP.
- For backwards compatibility with local user groups created pre-user group mirroring, when setting memberships on login, if a local user group exists with a simple name (no domain component) that matches the LDAP user group name, the user will be given membership to that group as well as to the mirror group. For example, if a user is a member of Group1 in somedomain.com then there will be a mirror user group named Group1@somedomain.com which the user will get membership to. If a local user group named Group1 also exists then the user will get membership to that too.

LDAP Group Membership by Organizational Unit

The LDAP Group Membership by Organizational Unit feature provides the ability to set LDAP rules and policies for the users who are located in certain Organizational Units (OUs) on the LDAP server. This is accomplished through the new "Set membership for LDAP users at/under location" setting in local user groups. When a user logs in or is authenticated via SSO and user groups are being set via LDAP, when the user object is found on the LDAP server the user will be made a member of any such groups that its location matches.

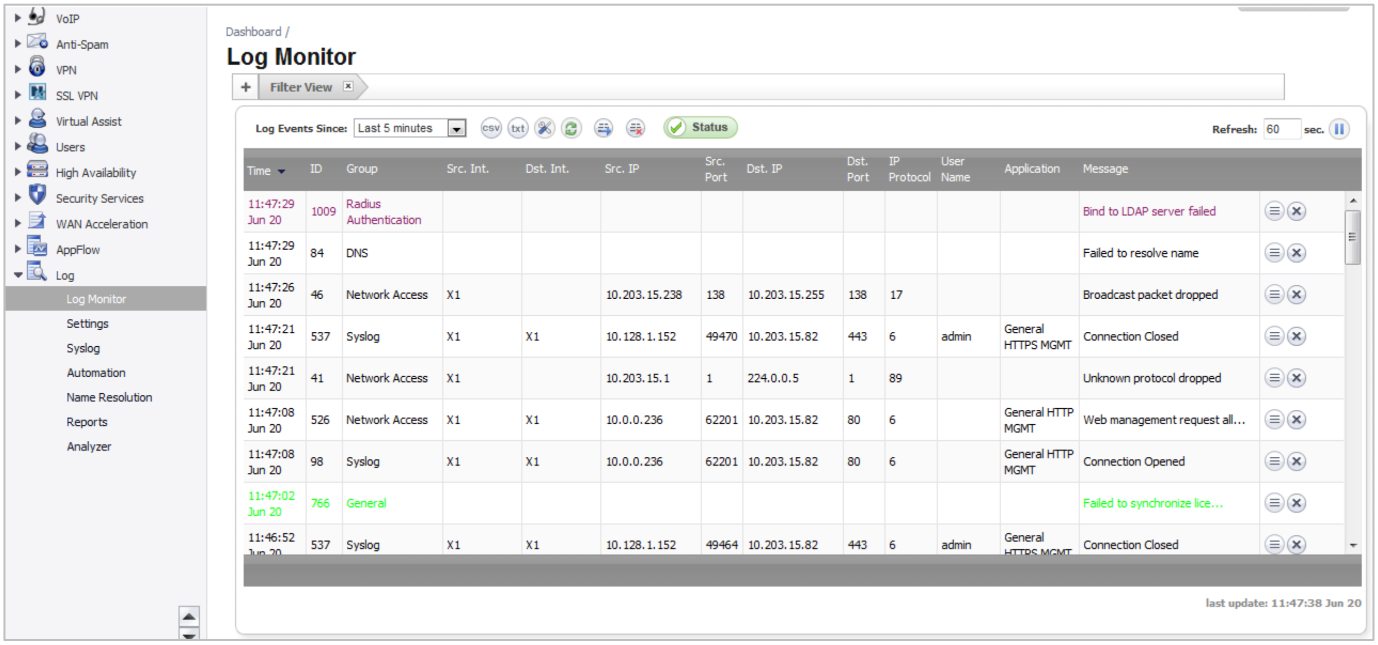
It will now be possible to set any local user group, including the default user groups (apart from Everyone or Trusted Users) as one whose member users are set from their location in the LDAP directory tree, and to configure the location in the group object.

When groups are configured this way:

- When a user's group memberships are looked up via LDAP during login or after SSO authentication, their location in the LDAP tree is learned. That will now be checked against any local user groups set this way. If it matches any then the user will be set as a member of those groups for the login session.
- On login success or failure, the event log will now include the user’s distinguished name in the notes when that has been learned from LDAP. This is to help with troubleshooting should a user fail to get memberships of these groups as expected.

Logging Enhancements

The new **Log Monitor** page overhauls the SonicOS approach to logging by providing a dynamic and intuitive interface for viewing and sorting log messages. The Categories display on the Log Monitor page groups the thousands of types of log events into a logical hierarchy that provides the administrator with the ability to quickly sort which types of log messages are to be displayed at various levels of priority and notification. Important events can be configured to trigger alerts or email notification. Log filters can be saved to allow for them to quickly be recalled.



Log Monitor

Log Events Since: Last 5 minutes

Refresh: 60 sec.

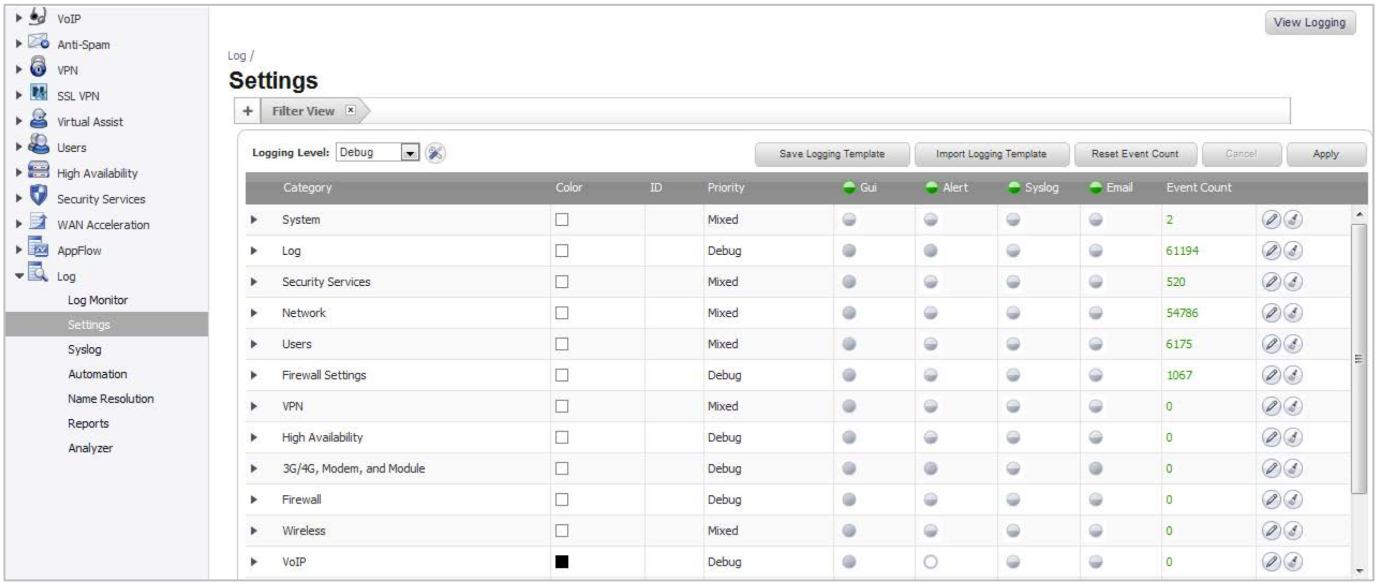
Time	ID	Group	Src. Int.	Dst. Int.	Src. IP	Src. Port	Dst. IP	Dst. Port	IP Protocol	User Name	Application	Message
11:47:29 Jun 20	1009	Radius Authentication										Bind to LDAP server failed
11:47:29 Jun 20	84	DNS										Failed to resolve name
11:47:26 Jun 20	46	Network Access	X1		10.203.15.238	138	10.203.15.255	138	17			Broadcast packet dropped
11:47:21 Jun 20	537	Syslog	X1	X1	10.128.1.152	49470	10.203.15.82	443	6	admin	General HTTPS MGMT	Connection Closed
11:47:21 Jun 20	41	Network Access	X1		10.203.15.1	1	224.0.0.5	1	89			Unknown protocol dropped
11:47:08 Jun 20	526	Network Access	X1	X1	10.0.0.236	62201	10.203.15.82	80	6		General HTTP MGMT	Web management request all...
11:47:08 Jun 20	98	Syslog	X1	X1	10.0.0.236	62201	10.203.15.82	80	6		General HTTP MGMT	Connection Opened
11:47:02 Jun 20	766	General										Failed to synchronize lice...
11:46:52 Jun 20	537	Syslog	X1	X1	10.128.1.152	49464	10.203.15.82	443	6	admin	General HTTPS MGMT	Connection Closed

last update: 11:47:38 Jun 20

Common Tasks for Event Log Management:

1. Online viewing of Log Events (not persistent, the run-time Event Log Database buffer may wrap-around so that older events will be over-written with new events)
   a. Can be viewed online using the SonicOS Log Monitor page – SonicOS grabs snapshots of the Event Log Database so the administrator can page forward/backwards using the browser
   b. Can be viewed in text format using the CLI – this shows only the current content of the Event Log Database
2. Customizing the Log Event display (Log > Monitor, display filtering)
3. Customizing the Log Event capture (Log > Settings, capture filtering)
4. Offline viewing of Log Events (also persistent due to external saving of events)
   a. Events can be viewed using your favorite email client by sending email alerts (an individual event is sent by email as soon as the event occurs) or an email digest (batches of events are sent periodically).
   b. Events can be viewed using a Syslog viewer after configuring the Syslog settings as well as Log > Settings capture
   c. Events can be viewed by GMS Syslogs
5. Exporting the current Event Log Database (use the export button)
6. Deleting entries from the run-time Event Log Database (Clear All button) – this permanently deletes entries, so proceed with caution. If no automation is enabled via Email/Syslogs, make sure to export the database first before using Clear All.
7. Deep Packet Forensics using a data recorder such as Solera. This is under Log > Automation after the selection of “interesting content” is done in Log > Settings.

The Log Settings page is shown below:

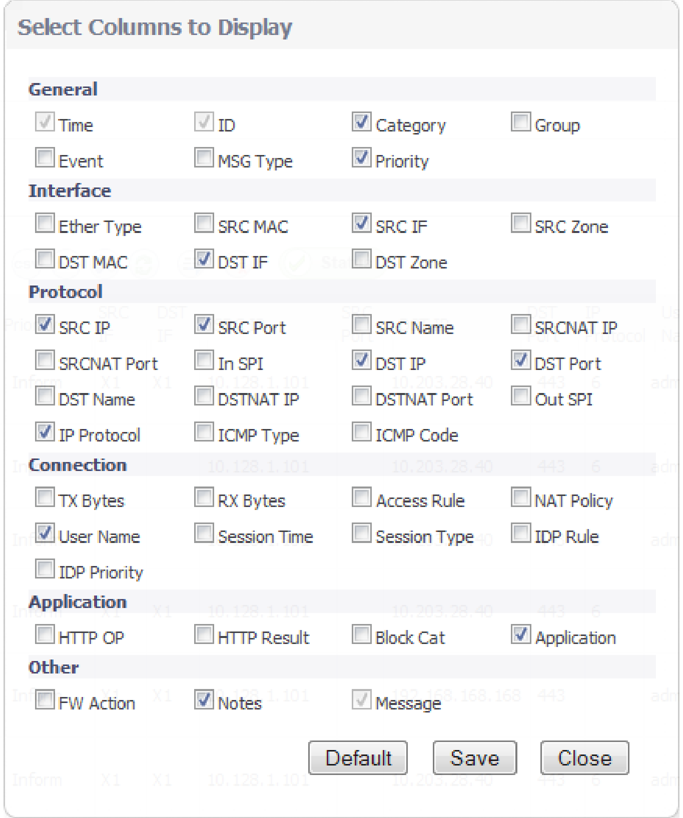


Settings

Logging Level: Debug

Category	Color	ID	Priority	Gui	Alert	Syslog	Email	Event Count
System	□		Mixed	●	●	●	●	2
Log	□		Debug	●	●	●	●	61194
Security Services	□		Mixed	●	●	●	●	520
Network	□		Mixed	●	●	●	●	54786
Users	□		Mixed	●	●	●	●	6175
Firewall Settings	□		Debug	●	●	●	●	1067
VPN	□		Mixed	●	●	●	●	0
High Availability	□		Debug	●	●	●	●	0
3G/4G, Modem, and Module	□		Debug	●	●	●	●	0
Firewall	□		Debug	●	●	●	●	0
Wireless	□		Mixed	●	●	●	●	0
VoIP	■		Debug	●	○	●	●	0

The updated Log Monitor view page provides enhanced flexibility with forty-nine separate columns that can be displayed or hidden.



Select Columns to Display

General

☑ Time ☑ ID ☑ Category □ Group
□ Event □ MSG Type ☑ Priority

Interface

□ Ether Type □ SRC MAC ☑ SRC IF □ SRC Zone
□ DST MAC ☑ DST IF □ DST Zone

Protocol

☑ SRC IP ☑ SRC Port □ SRC Name □ SRCNAT IP
□ SRCNAT Port □ In SPI ☑ DST IP ☑ DST Port
□ DST Name □ DSTNAT IP □ DSTNAT Port □ Out SPI
☑ IP Protocol □ ICMP Type □ ICMP Code

Connection

□ TX Bytes □ RX Bytes □ Access Rule □ NAT Policy
☑ User Name □ Session Time □ Session Type □ IDP Rule
□ IDP Priority

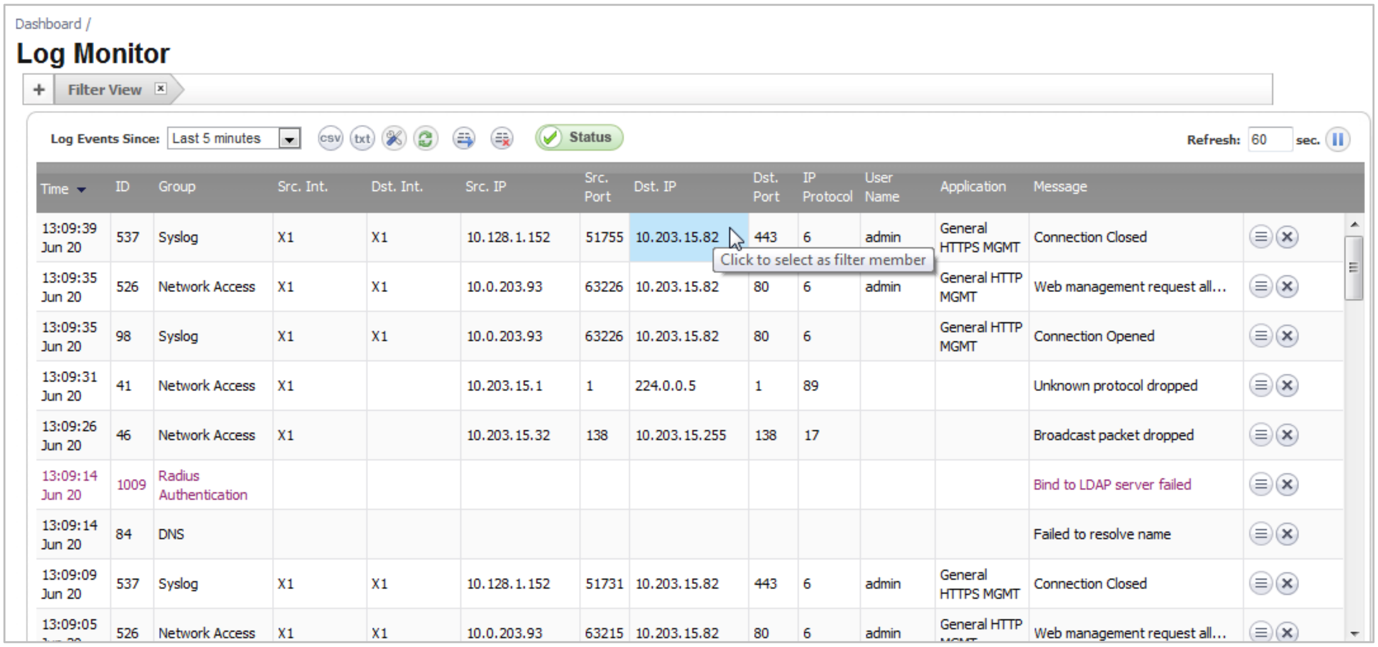
Application

□ HTTP OP □ HTTP Result □ Block Cat ☑ Application

Other

□ FW Action ☑ Notes ☑ Message

The Log Monitor view can be sorted by column and filtered dynamically by clicking on an entry, such as Destination IP address, as shown below.



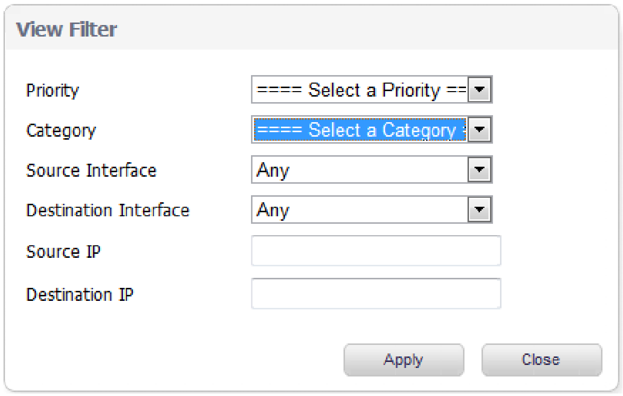
Log Monitor

Log Events Since: Last 5 minutes

Refresh: 60 sec.

Time	ID	Group	Src. Int.	Dst. Int.	Src. IP	Src. Port	Dst. IP	Dst. Port	IP Protocol	User Name	Application	Message
13:09:39 Jun 20	537	Syslog	X1	X1	10.128.1.152	51755	10.203.15.82	443	6	admin	General HTTPS MGMT	Connection Closed
13:09:35 Jun 20	526	Network Access	X1	X1	10.0.203.93	63226	10.203.15.82	80	6	admin	General HTTP MGMT	Web management request all...
13:09:35 Jun 20	98	Syslog	X1	X1	10.0.203.93	63226	10.203.15.82	80	6		General HTTP MGMT	Connection Opened
13:09:31 Jun 20	41	Network Access	X1		10.203.15.1	1	224.0.0.5	1	89			Unknown protocol dropped
13:09:26 Jun 20	46	Network Access	X1		10.203.15.32	138	10.203.15.255	138	17			Broadcast packet dropped
13:09:14 Jun 20	1009	Radius Authentication										Bind to LDAP server failed
13:09:14 Jun 20	84	DNS										Failed to resolve name
13:09:09 Jun 20	537	Syslog	X1	X1	10.128.1.152	51731	10.203.15.82	443	6	admin	General HTTPS MGMT	Connection Closed
13:09:05	526	Network Access	X1	X1	10.0.203.93	63215	10.203.15.82	80	6	admin	General HTTP	Web management request all...

When you click on the plus sign (+) next to the **Filter View** tab, a dialog opens where you can filter items by specific priority, category, or interfaces, etc. as shown below.



View Filter

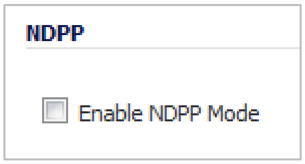
Priority	==== Select a Priority ==
Category	==== Select a Category
Source Interface	Any
Destination Interface	Any
Source IP	
Destination IP	

MOBIKE – IKEv2 Mobility and Multihoming Protocol

The IKEv2 Mobility and Multihoming Protocol (known as MOBIKE) provides the ability for maintaining a VPN session when a user moves from one IP address to another without the need for reestablishing IKE security associations with the gateway. For example, a user could establish a VPN tunnel while using a fixed Ethernet connection in the office. MOBIKE allows the user to disconnect the laptop and move to the office's wireless LAN without interrupting the VPN session. MOBIKE operation is transparent to the administrator and does not require any extra configuration by the administrator or consideration by users.

Network Device Protection Profile (NDPP)

SonicOS 5.9 provides an **Enable NDPP Mode** option on the System > Settings page of the management interface.



NDPP

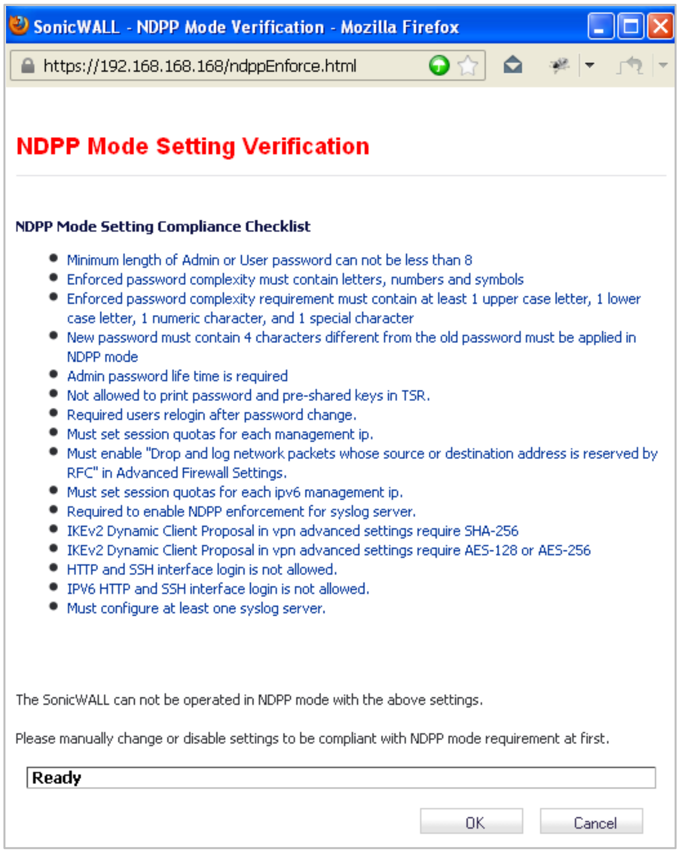
☐ Enable NDPP Mode

NDPP is a part of Common Criteria certification. The security objectives for a device that claims compliance to a Protection Profile are defined as follows:

> Compliant TOEs (Targets Of Evaluation) will provide security functionality that address threats to the TOE and implement policies that are imposed by law or regulation. The security functionality provided includes protected communications to and between elements of the TOE; administrative access to the TOE and its configuration capabilities; system monitoring for detection of security relevant events; control of resource availability; and the ability to verify the source of updates to the TOE.

Note: The **Enable NDPP Mode** checkbox cannot be enabled at the same time as the **Enable FIPS Mode** checkbox, which is also on the System > Settings page.

To configure the appliance for NDPP compliance, first select the **Enable NDPP Mode** checkbox on the System > Settings page. Once you do this, a popup window is displayed with the NDPP mode setting compliance checklist. The checklist displays every setting in your current SonicOS configuration that violates NDPP compliance, so that you can change these settings. You will need to navigate around the SonicOS management interface to make the changes. The checklist for an appliance with factory default settings is shown below:



SonicWALL - NDPP Mode Verification - Mozilla Firefox

https://192.168.168.168/ndppEnforce.html

NDPP Mode Setting Verification

NDPP Mode Setting Compliance Checklist

- Minimum length of Admin or User password can not be less than 8
- Enforced password complexity must contain letters, numbers and symbols
- Enforced password complexity requirement must contain at least 1 upper case letter, 1 lower case letter, 1 numeric character, and 1 special character
- New password must contain 4 characters different from the old password must be applied in NDPP mode
- Admin password life time is required
- Not allowed to print password and pre-shared keys in TSR.
- Required users relogin after password change.
- Must set session quotas for each management ip.
- Must enable "Drop and log network packets whose source or destination address is reserved by RFC" in Advanced Firewall Settings.
- Must set session quotas for each ipv6 management ip.
- Required to enable NDPP enforcement for syslog server.
- IKEv2 Dynamic Client Proposal in vpn advanced settings require SHA-256
- IKEv2 Dynamic Client Proposal in vpn advanced settings require AES-128 or AES-256
- HTTP and SSH interface login is not allowed.
- IPV6 HTTP and SSH interface login is not allowed.
- Must configure at least one syslog server.

The SonicWALL can not be operated in NDPP mode with the above settings.

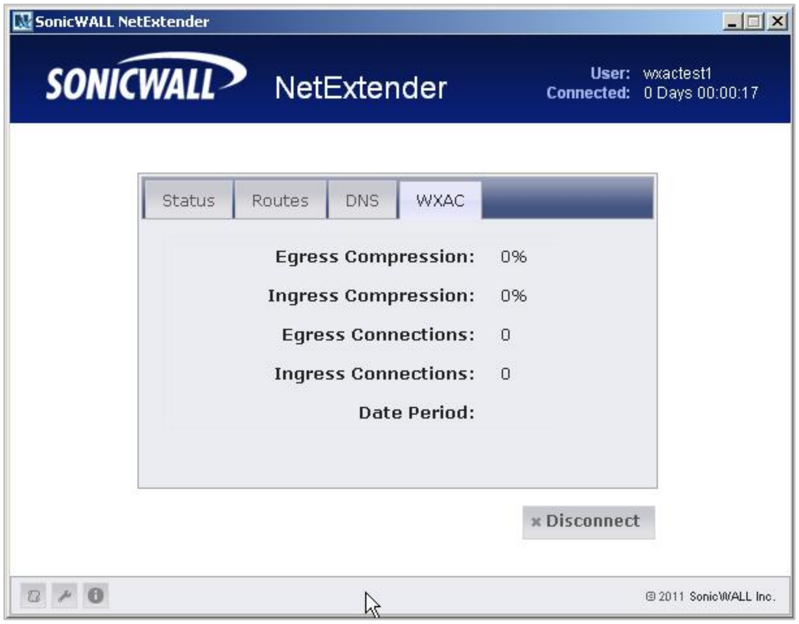
Please manually change or disable settings to be compliant with NDPP mode requirement at first.

Ready

You can leave the checklist window open while you make the configuration changes. If you click **OK** before all required changes are complete, the **Enable NDPP Mode** checkbox is automatically cleared upon closing the checklist window. Select the checkbox again to see what configuration changes are still needed for NDPP compliance.

NetExtender WAN Acceleration Client (WXAC) Integration

The SonicOS NetExtender feature now offers the integration of WAN Acceleration, allowing you to securely accelerate WAN traffic between a remote site and a central or branch office.



User: wxactest1
Connected: 0 Days 00:00:17

Egress Compression: 0%
Ingress Compression: 0%
Egress Connections: 0
Ingress Connections: 0
Date Period:

Numbered Tunnel Interfaces for Route Based VPN

In SonicOS 5.9, the routing protocol can use a numbered tunnel interface to establish a routing session. To support this requirement, the SonicOS administrator adds an interface in the VPN zone with an IP address from a private subnet assigned to it. This numbered tunnel interface can be used for the routing protocol session.

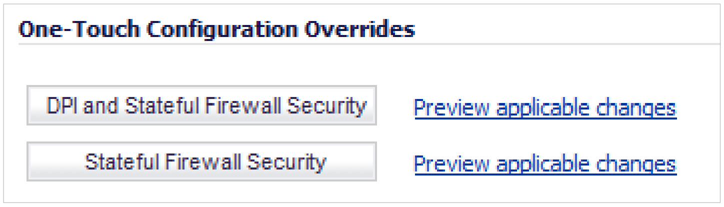
After a numbered tunnel interface is added to the interface list, a static route policy can use it as the interface in a static route policy configuration for a static route based VPN. Routing protocols (OSPF, RIP, and BGP) can use it for dynamic route based VPN.

Configuring a Numbered VPN Tunnel Interface is done in two parts:

- Configuring the VPN Policy
- Configuring the Tunnel Interface

One-Touch Configuration Overrides

The One-Touch Configuration Overrides section is found on the **System > Status** page and allows for automatic setting of a number of security features based on the deployment profile chosen.


One-Touch Configuration Overrides
DPI and Stateful Firewall Security
Preview applicable changes
Stateful Firewall Security
Preview applicable changes

A system restart is required for the One-Touch Configuration Overrides updates to take full effect.

OpenSSH Vulnerability Security Enhancements

Fixed the local private host key compromise on platforms without host – level randomness support (e.g. /dev/random) reported by Tomas Mraz. On hosts that did not have a randomness source configured in OpenSSL and were not configured to use EGD/PRNGd (using the--with-prngd-socket configure option), the ssh-rand-helper command was being implicitly executed by ssh-keysign with open file descriptors to the host private keys. An attacker could use ptrace(2) to attach to ssh-rand-helper and exfiltrate the keys.

Fixed the vulnerability in legacy certificate signing introduced in OpenSSH-5.6 and found by Mateusz Kocielski. Legacy certificates signed by OpenSSH 5.6 or 5.7 included data from the stack in place of a random nonce field. The contents of the stack do not appear to contain private data at this point, but this cannot be stated with certainty for all platform, library and compiler combinations. In particular, there exists a risk that some bytes from the privileged CA key may be accidentally included.

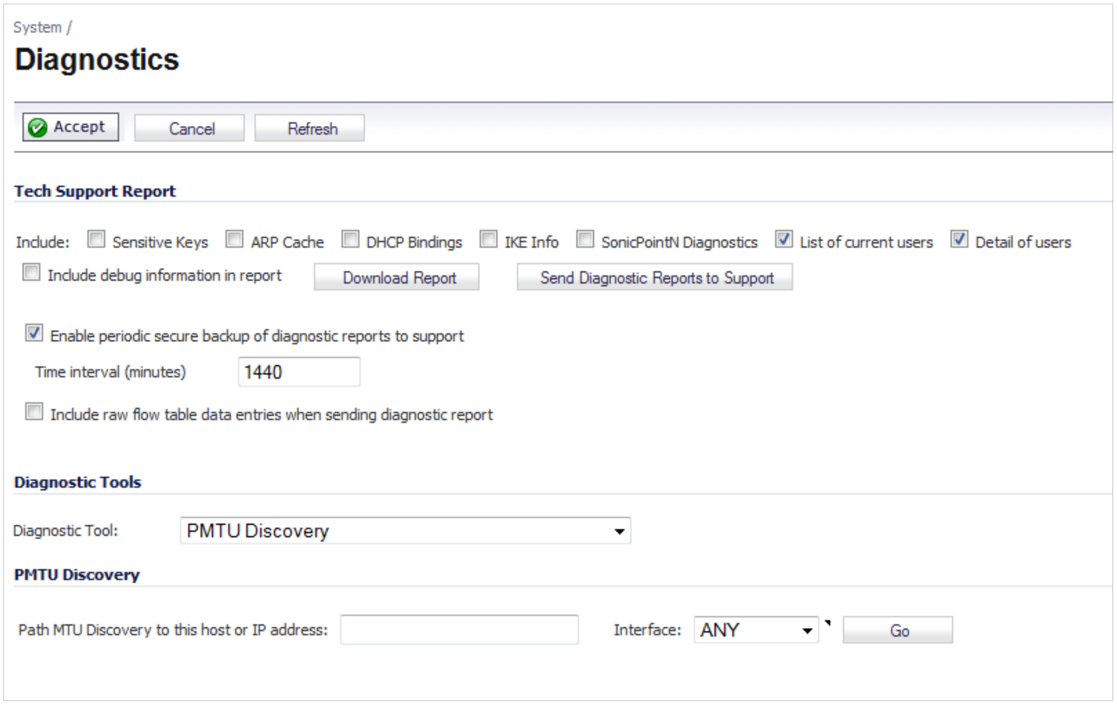
Path MTU Discovery

Path MTU Discovery is a diagnostic tool that determines the maximum transmission unit (MTU) on the network path between the Dell SonicWALL security appliance and a remote host. It is used to avoid IP fragmentation of traffic between the two hosts.

For IPv4 packets, Path MTU Discovery works by setting the "Don't Fragment" (DF) option bit in the IP headers of outgoing packets. When the DF option bit is set for a packet, and the packet traverses a device with an MTU smaller than the packet size, the device drops the packet and sends back an ICMP Fragmentation Needed message containing its MTU, allowing the source host to reduce its Path MTU appropriately. The process repeats until the MTU is small enough to traverse the entire path without fragmentation. IPv6 functions similarly, but the DF option bit is not required. IPv6 devices automatically send an ICMPv6 Packet Too Big message if the packet exceeds the devices MTU size.

By determining the MTU size on a network path and configuring the MTU for your Dell SonicWALL security appliance below the path MTU size, you avoid the potential delay caused by negotiation of the MTU size and other MTU-related network issues.

Path MTU Discovery is configured on the **System > Diagnostics** page by selecting **PMTU Discovery** for the Diagnostic Tool.



System /

Diagnostics

Tech Support Report

Include: □ Sensitive Keys □ ARP Cache □ DHCP Bindings □ IKE Info □ SonicPointN Diagnostics ☑ List of current users ☑ Detail of users

□ Include debug information in report

☑ Enable periodic secure backup of diagnostic reports to support

Time interval (minutes): 1440

□ Include raw flow table data entries when sending diagnostic report

Diagnostic Tools

Diagnostic Tool: PMTU Discovery

PMTU Discovery

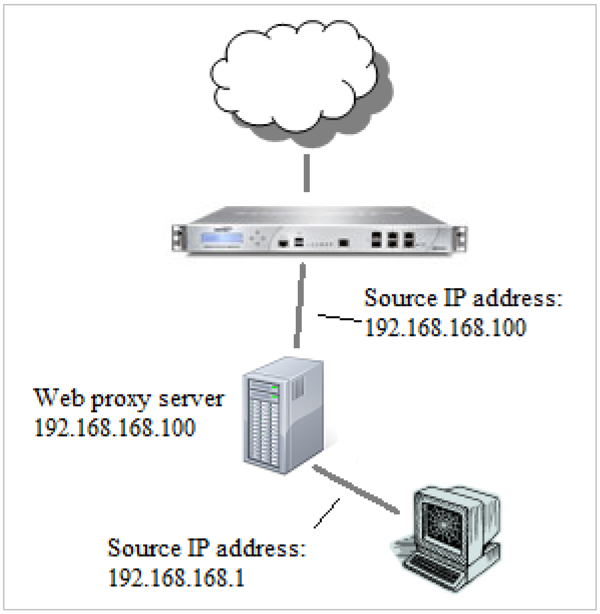
Path MTU Discovery to this host or IP address:

Interface: ANY

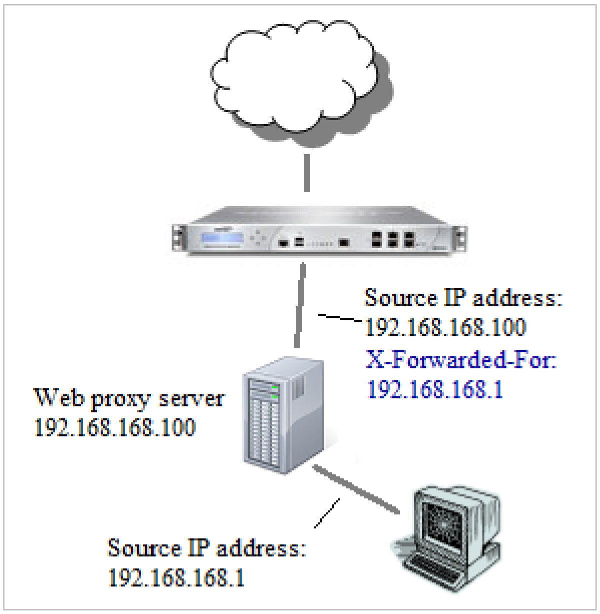
Enter the IP address or host name and click **Go**. When the **Interface** pulldown menu is set to **ANY**, the appliance chooses among all of its interfaces. Optionally, you can select one of the configured WAN interfaces to check the Path MTU for that interface.

Proxied Users Identification and Login

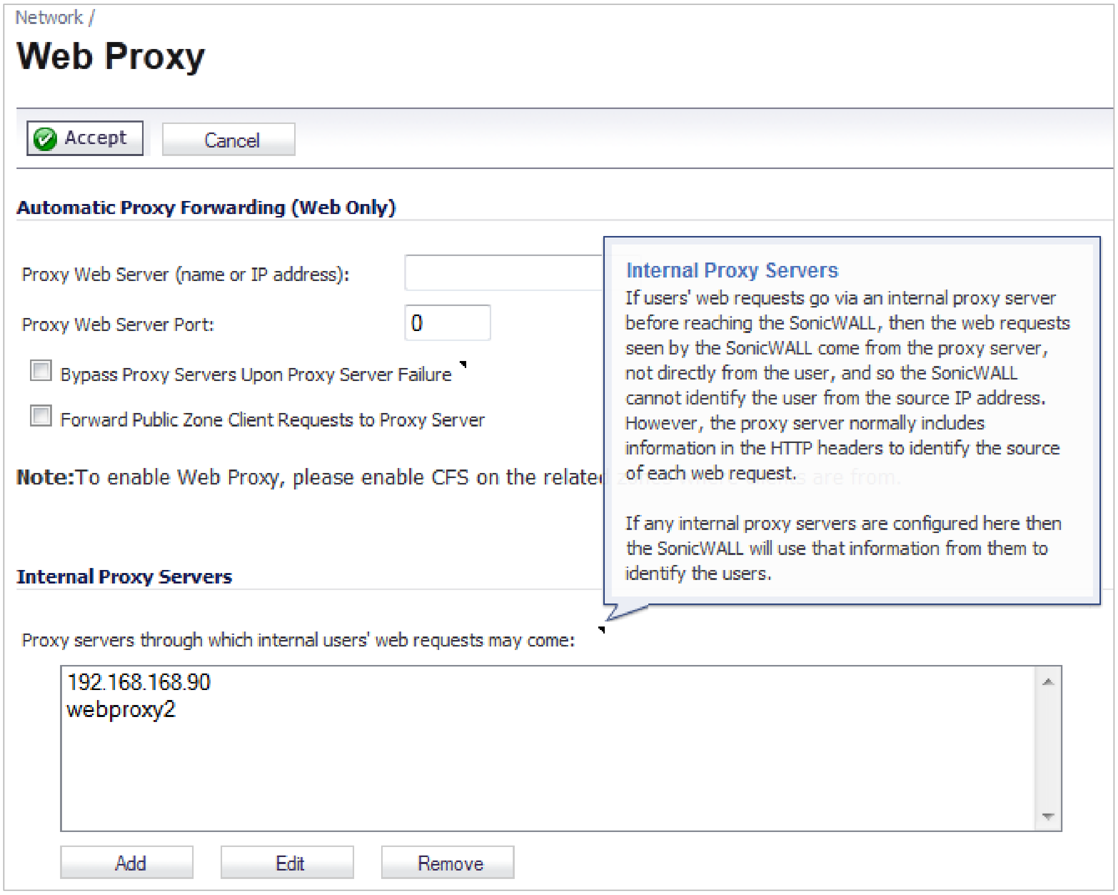
When users access the web through a proxy server that is located on the internal network (between the user and the UTM appliance), the HTTP/HTTPS connections, seen by the UTM appliance, originate from the proxy server, not from the user.



To identify the user for logging, policy enforcement, etc., the appliance must get the original source IP address of the connection from the user behind the proxy server. This is (optionally) provided by the proxy server in an **X-Forwarded-For** field in the HTTP header:



The Management GUI already includes a Network / Web Proxy page, where a proxy server can be configured for automatic proxy forwarding. On the same page, it is now possible to configure a list of up to 32 internal proxy servers (servers between the users and the appliance), identified by host name or IP address:



Automatic Proxy Forwarding (Web Only)

Proxy Web Server (name or IP address):

Proxy Web Server Port: 0

□ Bypass Proxy Servers Upon Proxy Server Failure

□ Forward Public Zone Client Requests to Proxy Server

Note: To enable Web Proxy, please enable CFS on the relate

Internal Proxy Servers

If users' web requests go via an internal proxy server before reaching the SonicWALL, then the web requests seen by the SonicWALL come from the proxy server, not directly from the user, and so the SonicWALL cannot identify the user from the source IP address. However, the proxy server normally includes information in the HTTP headers to identify the source of each web request.

If any internal proxy servers are configured here then the SonicWALL will use that information from them to identify the users.

Internal Proxy Servers

Proxy servers through which internal users' web requests may come:

192.168.168.90
webproxy2

RADIUS Accounting for SSO Overview

RADIUS Accounting is specified by RFC 2866 as a mechanism for a network access server (NAS) to send user login session accounting messages to an accounting server. These messages are sent at user login and logoff. Optionally, they can also be sent periodically during the user's session.

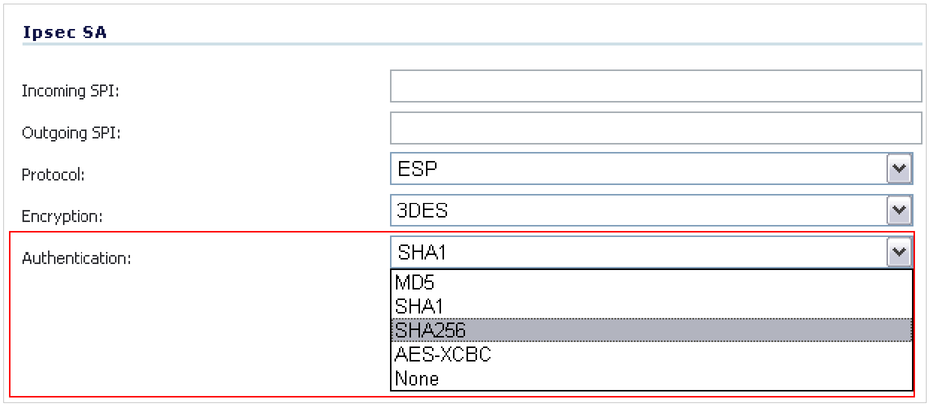
When a customer uses a third-party network access appliance to perform user authentication (typically for remote or wireless access) and the appliance supports RADIUS accounting, a Dell SonicWALL network security appliance can act as the RADIUS Accounting Server, and can use RADIUS Accounting messages sent from the customer's network access server for single sign-on (SSO) in the network.

Reassembly-Free Regular Expressions for DPI Engine

Dell SonicWALL has added reassembly-free regular expression functionality to the SonicOS Reassembly-Free Deep Packet Inspection (RF-DPI) engine. This proprietary implementation of regular expression matching does not require any buffering of the input content and works across packet boundaries. Users can now apply regular expressions to match objects in App Rules and use them across all currently supported application protocols and policy types. SonicOS supports Perl-compatible regular expressions syntax. A few typical regular expression features are not supported: In this release SonicOS does not support back-references and does not provide substitution or translation functionality since regular expressions are used only for inspection of network traffic—not for modifying any part of the traffic.

SHA-2 in IPsec

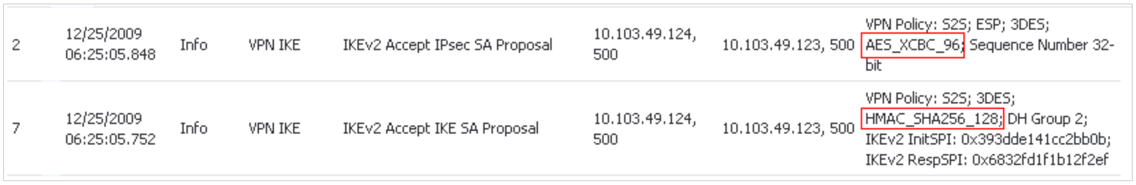
SHA-2 is a set of cryptographic algorithms used to secure IPsec traffic. SHA-2 provides a number of enhancements over its predecessor, SHA-1, to address potential security flaws. SonicOS has implemented the SHA256 variant of SHA-2.



Ipsec SA

Incoming SPI:	
Outgoing SPI:	
Protocol:	ESP
Encryption:	3DES
Authentication:	SHA1

SHA-2 can be used for Global VPN policies that are configured either manually or through the VPN wizard. If IKE is used for IPsec, SHA256 is available for both IKE and IKEv2. If the two phases are negotiated successful, the new algorithms will also be shown in the log page.



2	12/25/2009 06:25:05.848	Info	VPN IKE	IKEv2 Accept IPsec SA Proposal	10.103.49.124, 500	10.103.49.123, 500	VPN Policy: S2S; ESP; 3DES; AES_XCBC_96; Sequence Number 32-bit
7	12/25/2009 06:25:05.752	Info	VPN IKE	IKEv2 Accept IKE SA Proposal	10.103.49.124, 500	10.103.49.123, 500	VPN Policy: S2S; 3DES; HMAC_SHA256_128; DH Group 2; IKEv2 InitSPI: 0x393dde141cc2bb0b; IKEv2 RespSPI: 0x6832fd1f1b12f2ef

SNMPv3

Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are:

- Message integrity – Ensuring that a packet has not been tampered with in-transit.
- Authentication – Determining the message is from a valid source.
- Encryption – Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

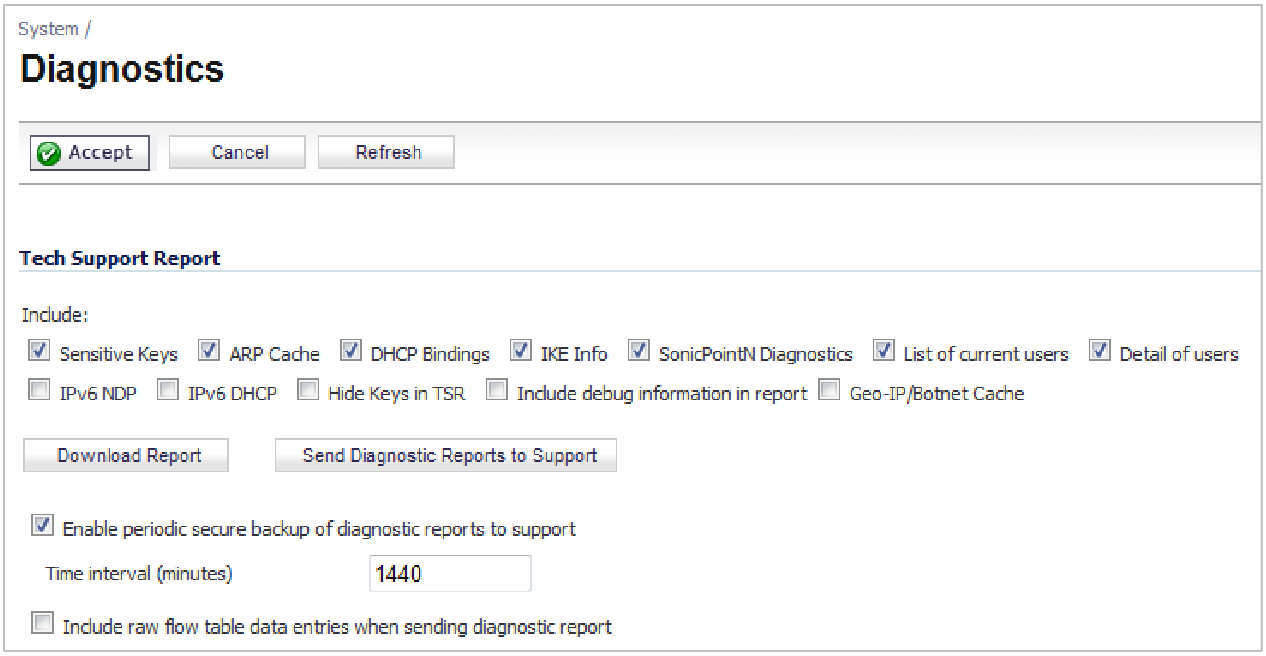
SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet. Three security models are available: SNMPv1, SNMPv2c, and SNMPv3.

The following Table identifies what the combinations of security models and levels mean:

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

TSR Enhancements

The Enhanced Technical Support Report (TSR) feature provides more options for the configuration of the TSR and reorganizes the TSR to make the report more readable and easier to use. The TSR is now organized using the second-level nodes of the SonicOS GUI main page. A substantial portion of the more difficult to read information in the TSR has been gathered at the end under the "Debug Info" category.



System /

Diagnostics

Tech Support Report

Include:

☑ Sensitive Keys ☑ ARP Cache ☑ DHCP Bindings ☑ IKE Info ☑ SonicPointN Diagnostics ☑ List of current users ☑ Detail of users

□ IPv6 NDP □ IPv6 DHCP □ Hide Keys in TSR □ Include debug information in report □ Geo-IP/Botnet Cache

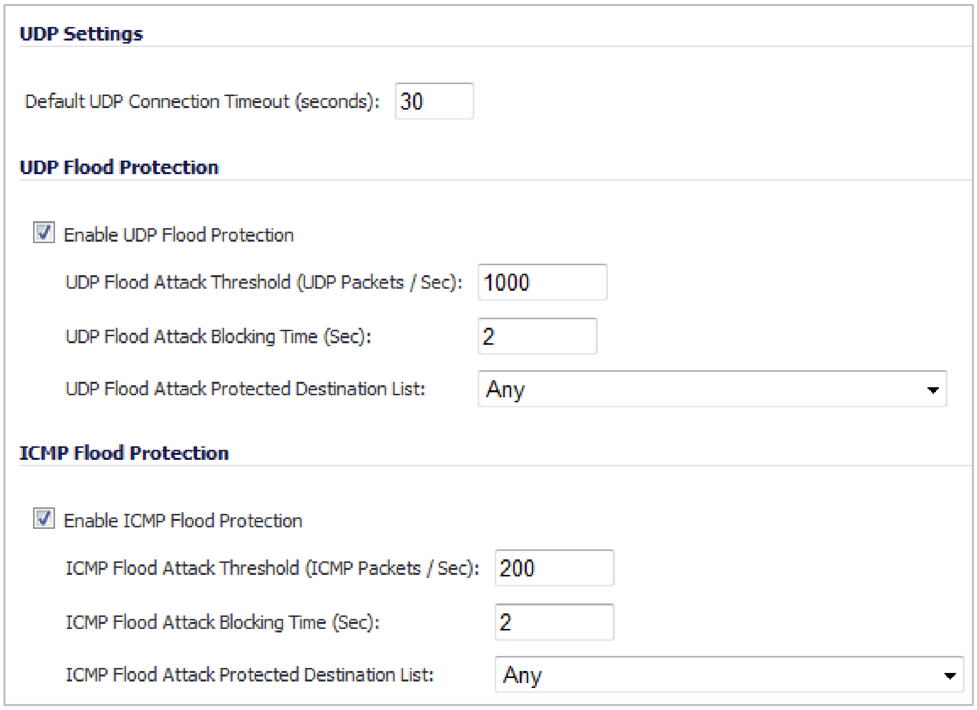
☑ Enable periodic secure backup of diagnostic reports to support

Time interval (minutes): 1440

□ Include raw flow table data entries when sending diagnostic report

UDP and ICMP Flood Protection

A UDP or ICMP Flood attack is type of denial-of-service (DoS) attack. It can be initiated by sending a large number of UDP packets to random ports on a remote host. The UDP and ICMP Flood Protection feature defends against these attacks by monitoring UDP and ICMP traffic that passes through the appliance for a UDP or ICMP Flood attack. UDP and ICMP Flood Protection are configured on the **Firewall Settings > Flood Protection** page:



UDP Settings

Default UDP Connection Timeout (seconds): 30

UDP Flood Protection

☑ Enable UDP Flood Protection

UDP Flood Attack Threshold (UDP Packets / Sec): 1000

UDP Flood Attack Blocking Time (Sec): 2

UDP Flood Attack Protected Destination List: Any

ICMP Flood Protection

☑ Enable ICMP Flood Protection

ICMP Flood Attack Threshold (ICMP Packets / Sec): 200

ICMP Flood Attack Blocking Time (Sec): 2

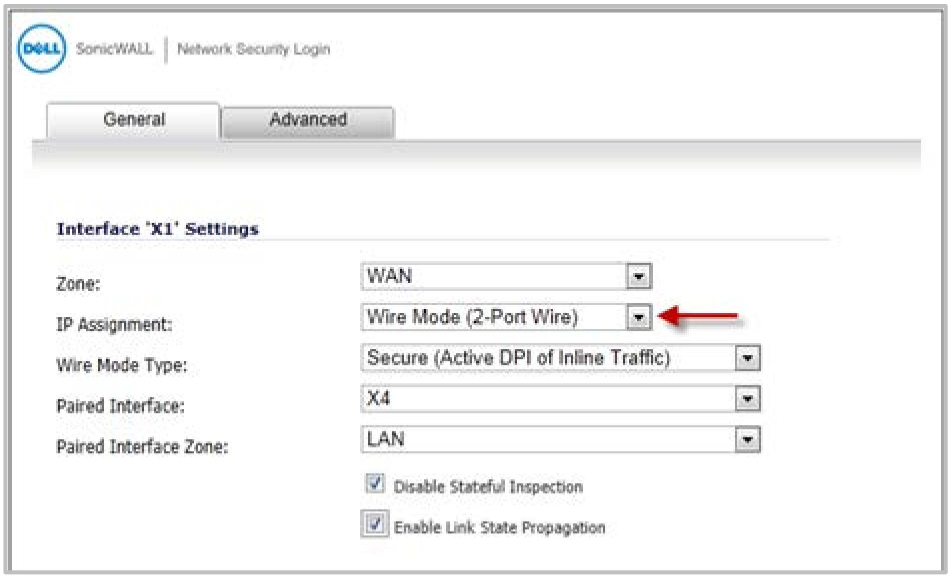
ICMP Flood Attack Protected Destination List: Any

The following UDP and ICMP Flood Protection settings are available:

- **Enable UDP Flood Protection / Enable ICMP Flood Protection** – Enables or disables UDP or ICMP Flood Protection.
- **UDP Flood Attack Threshold / ICMP Flood Attack Threshold** – Specifies the maximum number of allowed UDP or ICMP packets per second that can be sent to a Host, Range, or Subnet.
- **UDP Flood Attack Blocking Time / ICMP Flood Attack Blocking Time** – Specifies the number of seconds to block UDP or ICMP traffic after detecting a flood attack.
- **UDP Flood Attack Protected Destination List / ICMP Flood Attack Protected Destination List** – Specifies the destination addresses list which will be protected from a UDP or ICMP Flood attack. Select "Any" to apply the attack threshold to the sum of UDP or ICMP packets that pass through the firewall.
- **Default UDP Connection Timeout** – Moved to the Flood Protection page to be consistent with TCP settings.

Wire Mode 2.0

In SonicOS 5.9, Wire Mode can be configured on any zone (except Wireless zones), under **Network** > **Interfaces** > **Configure** > **General**, by setting the **IP Assignment:** to **Wire Mode (2-Port Wire)**. The rules that apply to the **Zone** also apply to the **Paired Interface Zone**. For example, when you select **Wire Mode** for a **WAN Zone** and set the **Paired Interface Zone** to **LAN**, then **WAN** rules are applied based on the direction of the traffic.



Interface 'X1' Settings

Zone: WAN

IP Assignment: Wire Mode (2-Port Wire)

Wire Mode Type: Secure (Active DPI of Inline Traffic)

Paired Interface: X4

Paired Interface Zone: LAN

☑ Disable Stateful Inspection

☑ Enable Link State Propagation

The **Disable Stateful Inspection** option is new in SonicOS 5.9. When **Disable Stateful Inspection** is selected, Stateful Packet Inspection (SPI) is turned off. When **Disable Stateful Inspection** is *not* selected, new connections can be established without enforcing a 3-way TCP handshake. **Disable Stateful Inspection** must be selected if asymmetrical routes are deployed.

The **Enable Link State Propagation** option is also new in SonicOS 5.9. This feature propagates the link status of an interface to its paired interface. If an interface goes down, its paired interface is forced down to mirror the link status of the first interface. Both interfaces in a Wire Mode pair always have the same link status.

WWAN 4G support

SonicOS 5.9 introduces support for 4G PC cards and USB devices. 4G interfaces in SonicOS function identically to 3G interfaces. To use a 3G/4G interface you must have a 3G/4G PC card and a contract with a wireless service provider. A 3G/4G service provider should be selected based primarily on the availability of supported hardware, which is listed at:

http://www.sonicwall.com/us/products/cardsupport.html

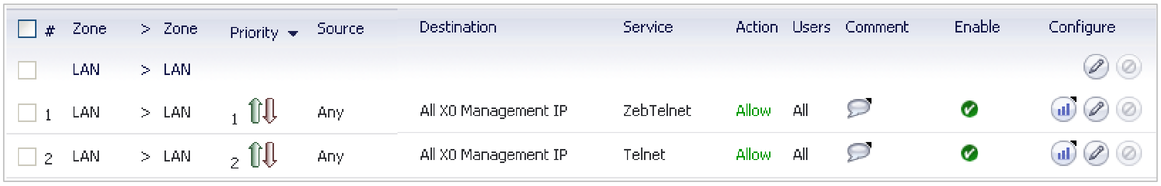
SonicOS 5.9.0.0-58o and higher includes support for the following additional 3G/4G devices:

- "T-Mobile Rocket 3.0" ZTE MF683 4G (USA)
- "AT&T Momentum" Sierra Wireless 313U 4G (USA)
- "Rogers Rocket Stick" Sierra Wireless 330U 4G (Canada)
- Kyocera 5005 (Asia/Europe)
- Huawei 398 (Asia/Europe)
- Huawei E353 (Asia/Europe)
- D-Link DWM156 (Asia/Europe)

XD Lookup for Access Rules

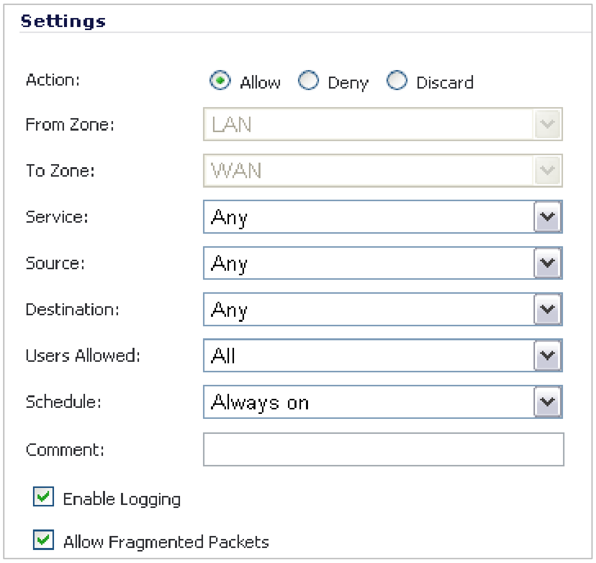
Under **Firewall** > **Access Rules**, the name of the **Dst Service** column has been modified to **Service**. When you pause your mouse over the **Service** column heading, the message reads as, "Click to sort by Service object".

Firewall > **Access Rules** GUI –



□ #	Zone	>	Zone	Priority ▾	Source	Destination	Service	Action	Users	Comment	Enable	Configure
□	LAN	>	LAN									
□ 1	LAN	>	LAN	1 ⇅	Any	All X0 Management IP	ZebTelnet	Allow	All	💬	✓	
□ 2	LAN	>	LAN	2 ⇅	Any	All X0 Management IP	Telnet	Allow	All	💬	✓	

Configure Dialog –



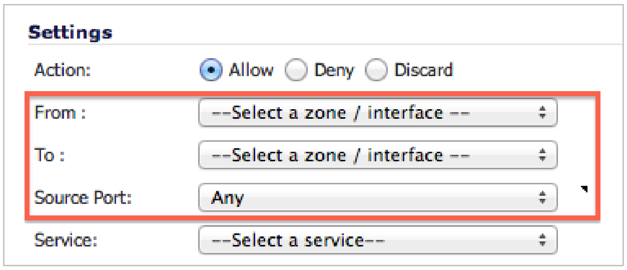
Settings

Action:	● Allow ○ Deny ○ Discard
From Zone:	LAN
To Zone:	WAN
Service:	Any
Source:	Any
Destination:	Any
Users Allowed:	All
Schedule:	Always on
Comment:	

☑ Enable Logging

☑ Allow Fragmented Packets

In the **Configure** dialog, in the **From Zone:** and **To Zone:** lists, **Zone** was changed to **Zone** / **Interface**. The **Source Port** list was added.



Settings

Action: ● Allow ○ Deny ○ Discard

From : --Select a zone / interface --

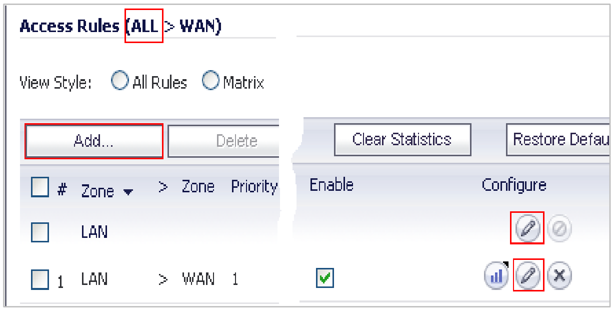
To : --Select a zone / interface --

Source Port: Any

Service: --Select a service--

The ability to select interfaces was added to the **From:** and **To: Select a zone / interface** lists. The available zones and interfaces that appear in the list, depends on the **View Style:** option.

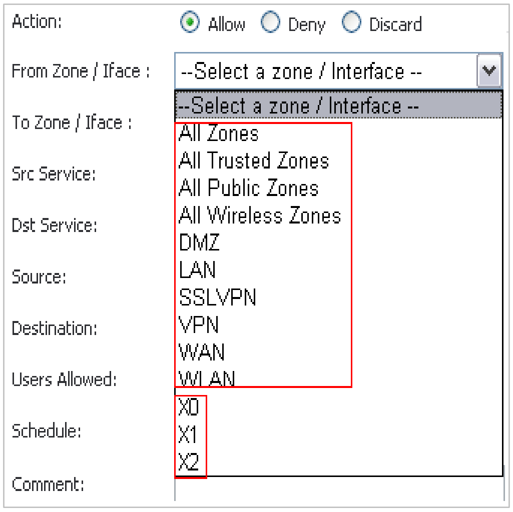
Firewall > **Access Rules** Screen with **All** selected –



Access Rules (ALL > WAN)

View Style: ○ All Rules ○ Matrix

□ #	Zone ▾	>	Zone	Priority	Enable	Configure
□	LAN					
□ 1	LAN	>	WAN	1	☑	

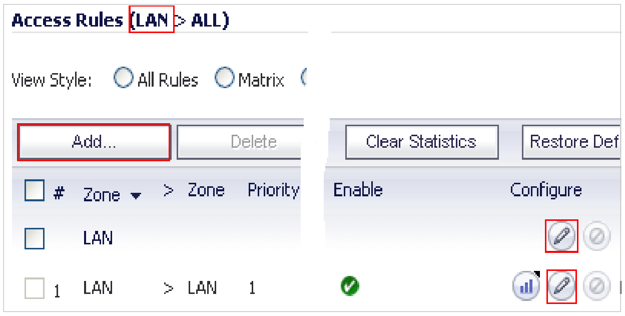


Action: ● Allow ○ Deny ○ Discard

From Zone / Iface : --Select a zone / Interface --

--Select a zone / Interface --
All Zones
All Trusted Zones
All Public Zones
All Wireless Zones
DMZ
LAN
SSLVPN
VPN
WAN
WLAN
X0
X1
X2

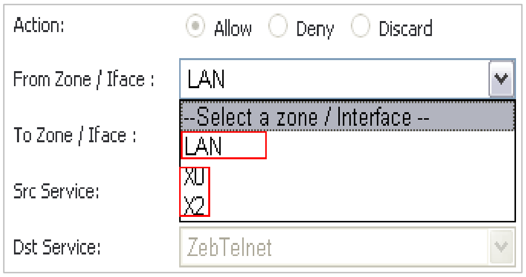
Firewall > **Access Rules** Screen with **LAN** selected –



Access Rules (LAN > ALL)

View Style: ○ All Rules ○ Matrix

□ #	Zone ▾	>	Zone	Priority	Enable	Configure
□	LAN					
□ 1	LAN	>	LAN	1	✓	



Action: ● Allow ○ Deny ○ Discard

From Zone / Iface : LAN

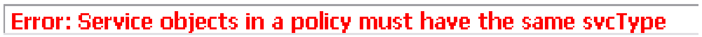
To Zone / Iface :

--Select a zone / Interface --
LAN
X0
X2

Src Service:

Dst Service: ZebTelnet

The list for **Source Port** is the same as the list for **Service**. If both **Source Port** and **Service** are set to anything other than **Any**, they both must have the same service type and it must be unique. Otherwise, the following error message is displayed.



Error: Service objects in a policy must have the same svcType

Note: Source Port is not listed in the **Access Rules** column headings.

YouTube for Schools Content Filtering Support

The YouTube for Schools feature was introduced in SonicOS 5.8.1.8.

YouTube for Schools is a service that allows for customized YouTube access for students, teachers, and administrators. YouTube Education (YouTube EDU) provides schools access to hundreds of thousands of free educational videos. These videos come from a number of respected organizations. You can customize the content available in your school. All schools get access to all of the YouTube EDU content, but teachers and administrators can also create playlists of videos that are viewable only within their school's network. Before configuring your Dell SonicWALL security appliance for YouTube for Schools, you must first sign up: www.youtube.com/schools

The configuration of YouTube for Schools depends on the method of Content Filtering you are using, which is configured on the **Security Services > Content Filter** page.

Membership in Multiple Groups

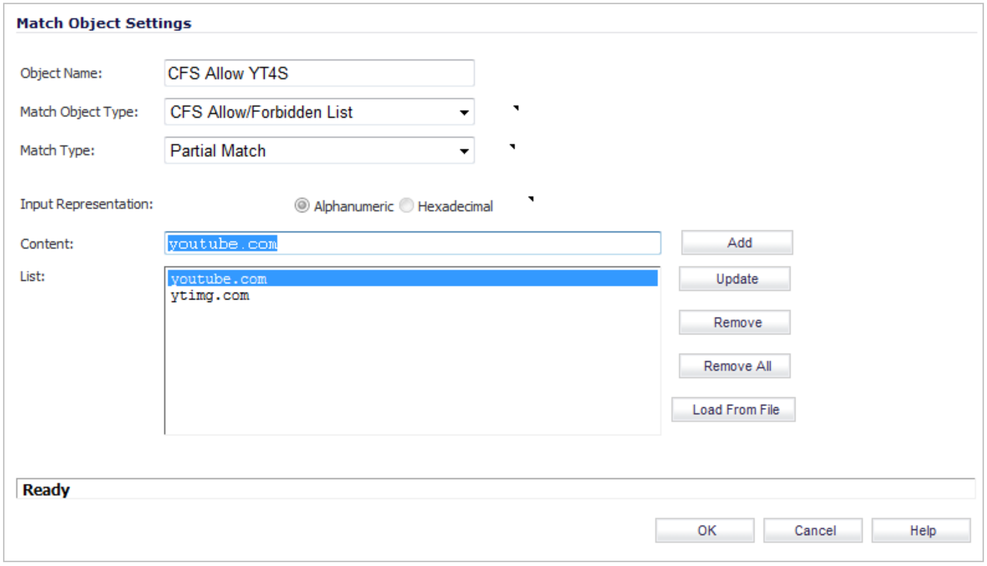
If a user is a member of multiple groups where one policy allows access to any part of YouTube and the other policy has a YouTube for Schools restriction, the user will be filtered by the YouTube for Schools policy and not be allowed unrestricted access to YouTube.

A user cannot be a member of multiple groups that have different YouTube for School IDs. While the firewall will accept the configuration, this is not supported.

Note: For more information on the general configuration of CFS, refer to the **Security Services > Content Filter** section in the *SonicOS Administrator's Guide*.

When the **CFS Policy Assignment** pulldown menu is set to **Via Application Control**, YouTube for Schools is configured as an App Control Policy.

1. Navigate to **Firewall > Match Objects** and click **Add New Match Object**.



Match Object Settings

Object Name: CFS Allow YT4S

Match Object Type: CFS Allow/Forbidden List

Match Type: Partial Match

Input Representation: ● Alphanumeric ○ Hexadecimal

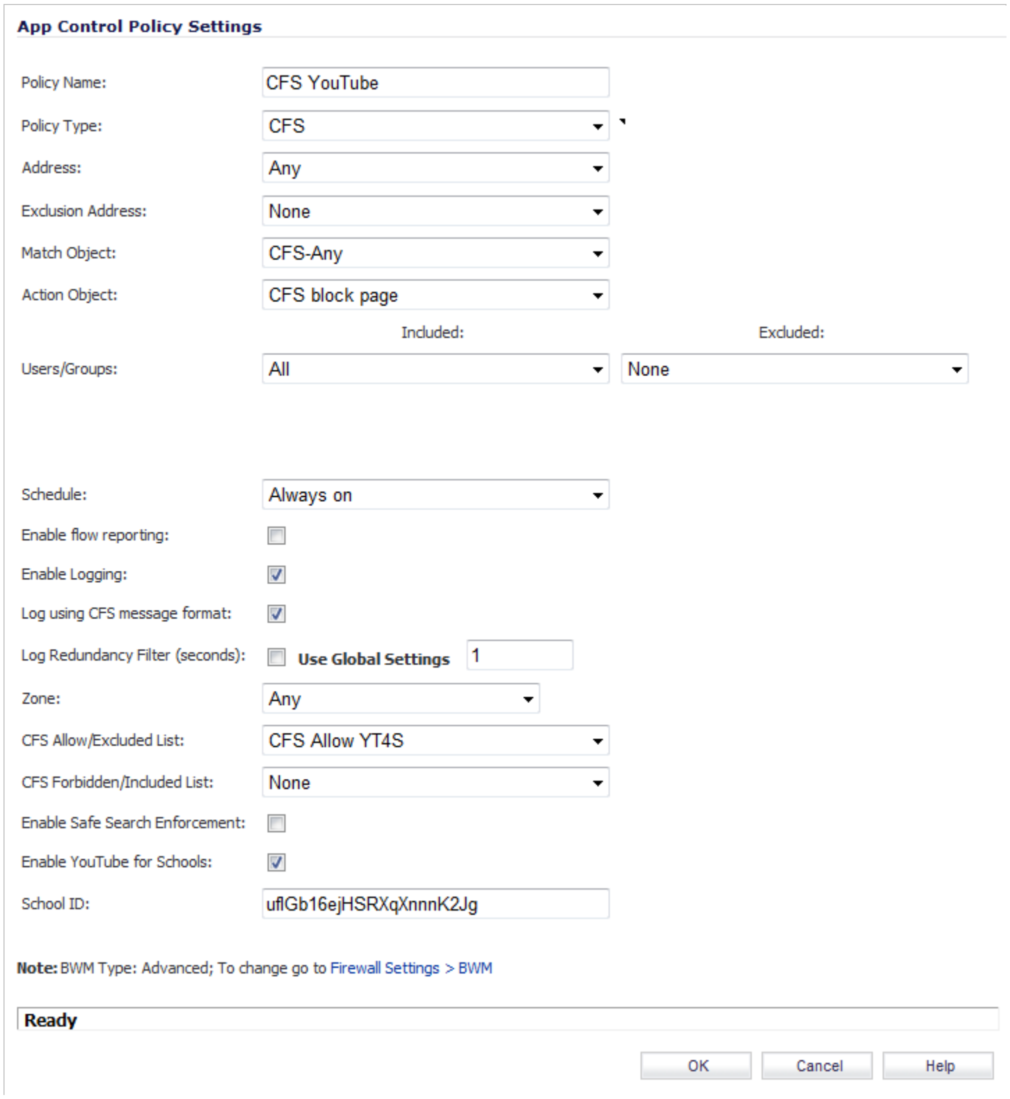
Content: youtube.com

List:
youtube.com
ytimg.com

Ready

2. Type in a descriptive name, and then select **CFS Allow/Forbidden List** as the **Match Object Type**.
3. Select **Partial Match** for the **Match Type**.
4. In the **Content** field, type in "youtube.com" and then click **Add**.
5. Type in "ytimg.com" and then click **Add**.
6. Click **OK** to create the Match Object.

7. Navigate to the **Firewall > App Rules** page and click **Add New Policy**.



App Control Policy Settings

Policy Name:	CFS YouTube	
Policy Type:	CFS	
Address:	Any	
Exclusion Address:	None	
Match Object:	CFS-Any	
Action Object:	CFS block page	
	Included:	Excluded:
Users/Groups:	All	None
Schedule:	Always on	
Enable flow reporting:	□	
Enable Logging:	☑	
Log using CFS message format:	☑	
Log Redundancy Filter (seconds):	□ **Use Global Settings** 1	
Zone:	Any	
CFS Allow/Excluded List:	CFS Allow YT4S	
CFS Forbidden/Included List:	None	
Enable Safe Search Enforcement:	□	
Enable YouTube for Schools:	☑	
School ID:	uflGb16ejHSRXqXnnnK2Jg	

Note: BWM Type: Advanced; To change go to Firewall Settings > BWM

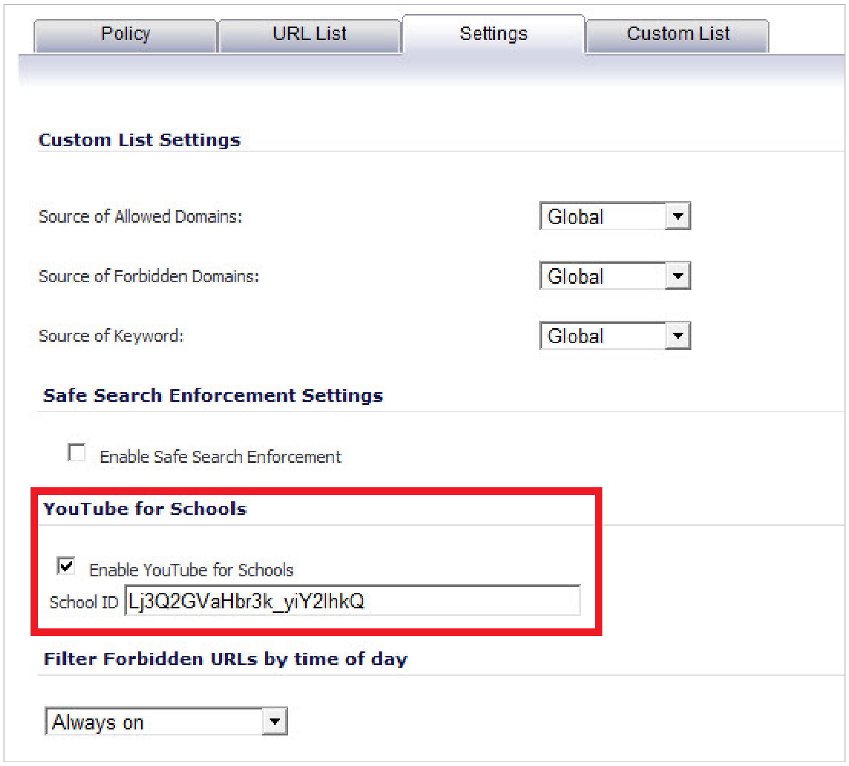
Ready

8. Type in a descriptive **Policy Name**.
9. For the **Policy Type**, select **CFS**.
10. Select the appropriate settings for **Match Object** and **Action Object**, based on your environment.
11. For **CFS Allow/Excluded List**, select the Match Object you just created (our example uses “CFS Allow YT4S”).
12. Select the **Enable YouTube for Schools** checkbox.
13. Paste in your **School ID**, which is obtained from www.youtube.com/schools
14. Click **OK** to create the policy.
    Note: Once the policy has been applied, any existing browser connections will be unaffected until the browser has been closed and reopened. Also, if you have a browser open as administrator on the firewall, you will be excluded from CFS policy enforcement unless you configure the firewall specifically not to exclude you (select the **Do not bypass CFS blocking for the Administrator** checkbox on the **Security Services > Content Filter** page).

When the **CFS Policy Assignment** pulldown menu is set to **Via User and Zone Screens**, YouTube for Schools is configured as part of the Content Filter policy.

On the Security Services > Content Filter page, select Content Filter Service for the Content Filter Type pulldown menu.

1. Click the Configure button.
2. On the Policy tab, click the Configure icon for the CFS policy on which you want to enable YouTube for Schools.
3. Click on the Settings tab, and select the Enable YouTube for Schools checkbox.
4. Paste in your School ID, which is obtained from www.youtube.com/schools.



Custom List Settings

Source of Allowed Domains: Global

Source of Forbidden Domains: Global

Source of Keyword: Global

Safe Search Enforcement Settings

☐ Enable Safe Search Enforcement

YouTube for Schools

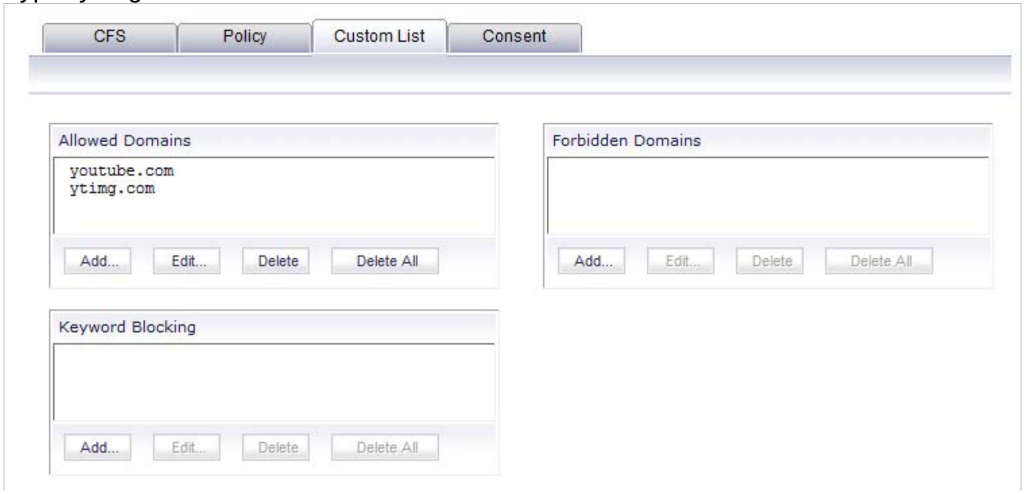
☑ Enable YouTube for Schools

School ID Lj3Q2GVaHbr3k_yiY2lhkQ

Filter Forbidden URLs by time of day

Always on

5. Click **OK**.
6. On the **Custom List** tab, click the **Add** button for **Allowed Domains**.
7. In the dialog box, type “youtube.com” into the **Domain Name** field and click **OK**.
8. Click **Add** again.
9. Type “ytimg.com” into the **Domain Name** field and click **OK**.



Allowed Domains

youtube.com
ytimg.com

Forbidden Domains

Keyword Blocking

10. Click **OK**.

    These settings will override any CFS category that blocks YouTube.

    Note: Once the policy has been applied, any existing browser connections will be unaffected until the browser has been closed and reopened. Also, if you have a browser open as administrator on the firewall, you will be excluded from CFS policy enforcement unless you configure the firewall specifically not to exclude you (select the **Do not bypass CFS blocking for the Administrator** checkbox on the **Security Services > Content Filter** page).

YouTube for Schools and HTTPS

The SonicOS CFS implementation of YouTube for Schools does not support HTTPS access to youtube.com. When youtube.com is accessed over HTTPS, the user will have unrestricted access to YouTube content. The following solutions can be implemented to work around this:

- Enable Client DPI-SSL with CFS inspection. DPI-SSL feature activation requires a separate license.
- Create a LAN (or DMZ) to WAN Access Rule as under:
    - Action: Deny
    - Service: HTTPS
    - Source: Any
    - Destination: Create an FQDN Address Object for youtube.com and ytimg.com

Issues:

DPI-SSL cannot be used to block https://youtube.com, but only to allow it. So the DPI section above should not be part of the solutions that can be implemented to work around this.

In creating the above rule to block https access to youtube.com or www.youtube.com and s.ytimg.com, we have found that https://www.google.com is now also blocked, as well as https://drive.google.com and https://play.google.com/ are blocked also.

Other google sites such as calendar.google.com and gmail work fine.

Creating fqdns for the blocked site and creating an allow rule for the group, also allows https youtube to be accessed.

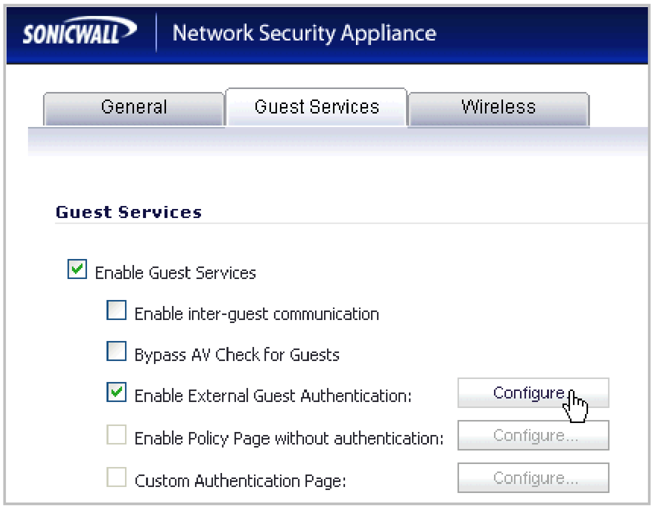
In summary, creating the deny rules for https>youtube fqdns also blocks other google ssl sites. So there is no way that we have found to use youtube for schools and block access to ssl youtube without blocking other google ssl sites. And there is no way to allow the other sites without also causing ssl youtube to be allowed as well.

SonicPoint and Wireless Enhancements

The following SonicPoint Enhancements are included in SonicOS 5.9:

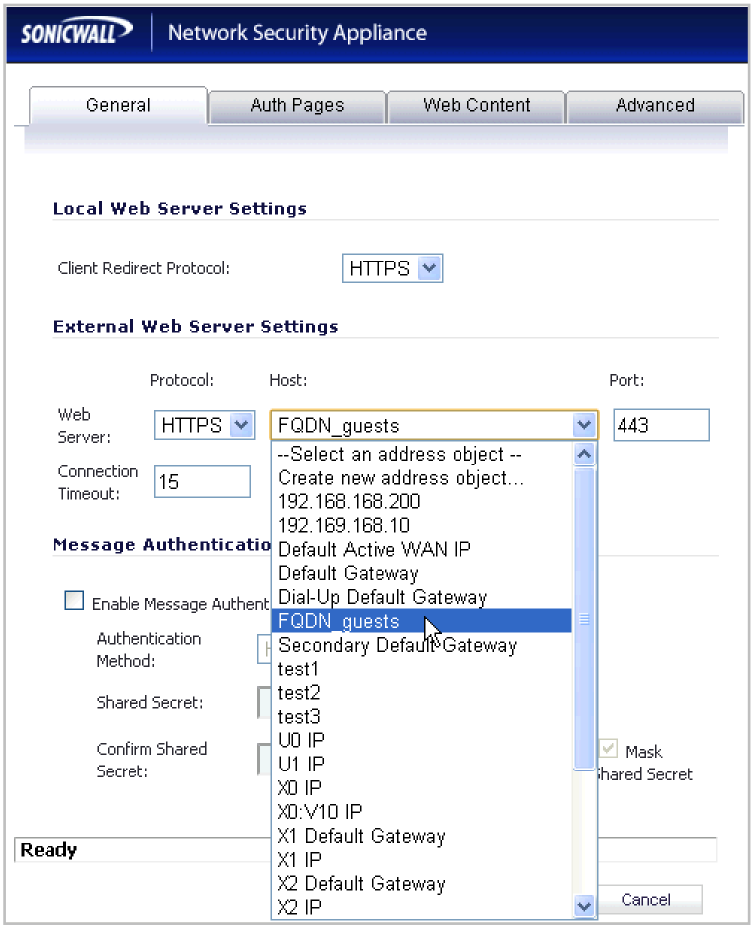
External Guest Service FQDN Support

Fully Qualified Domain Names are supported for Lightweight Hotspot Messaging (LHM) server configuration. To configure, navigate to the **Network > Zones** page and edit the **WLAN** zone. On the **Guest Services** tab of the configuration window, select the **Enable External Guest Authentication** checkbox and click the **Configure** button.



☑ Enable Guest Services
□ Enable inter-guest communication
□ Bypass AV Check for Guests
☑ Enable External Guest Authentication:
□ Enable Policy Page without authentication:
□ Custom Authentication Page:

In the configuration window under **External Web Server Settings**, you can select an **FQDN** address object in the **Host** drop-down list.



Local Web Server Settings

Client Redirect Protocol: HTTPS

External Web Server Settings

Web Server: Protocol: HTTPS Host: FQDN_guests Port: 443

Connection Timeout: 15

Message Authenticatio

□ Enable Message Authent

Authentication Method:

Shared Secret:

Confirm Shared Secret:

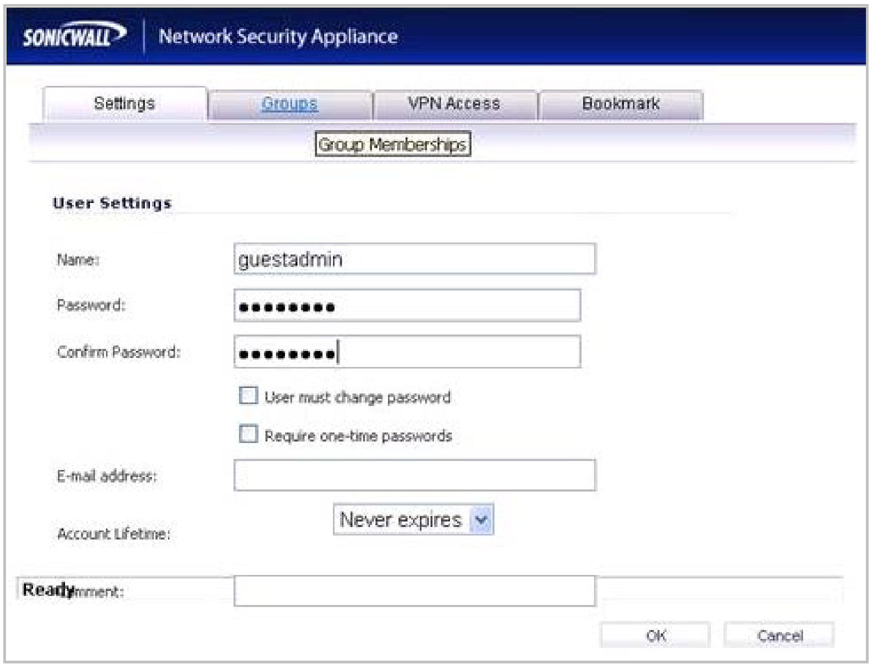
☑ Mask Shared Secret

Ready

Guest Administrator Support

A “Guest Administrator” privileges group is available to provide administrator access only to manage guest accounts and sessions.

To configure a Guest Administrator account, navigate to the **Users > Local Users** page and click **Add User**.



User Settings

Name: guestadmin

Password: ••••••••

Confirm Password: ••••••••

□ User must change password

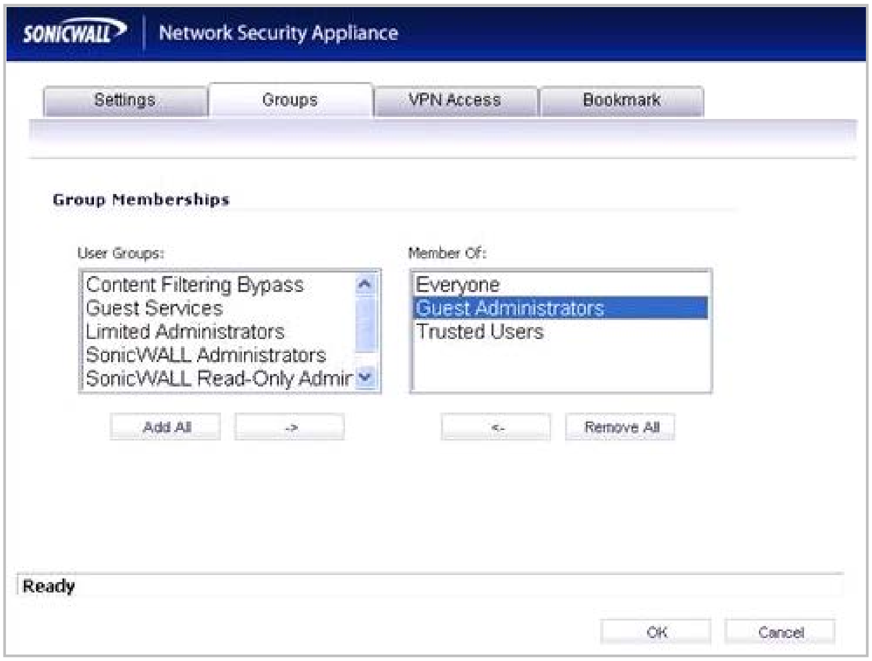
□ Require one-time passwords

E-mail address:

Account Lifetime: Never expires

Comment:

On the **Groups** tab, select **Guest Administrators** in the **User Groups** list and click the arrow to move it to the **Member Of** list. Click **OK**.



Group Memberships

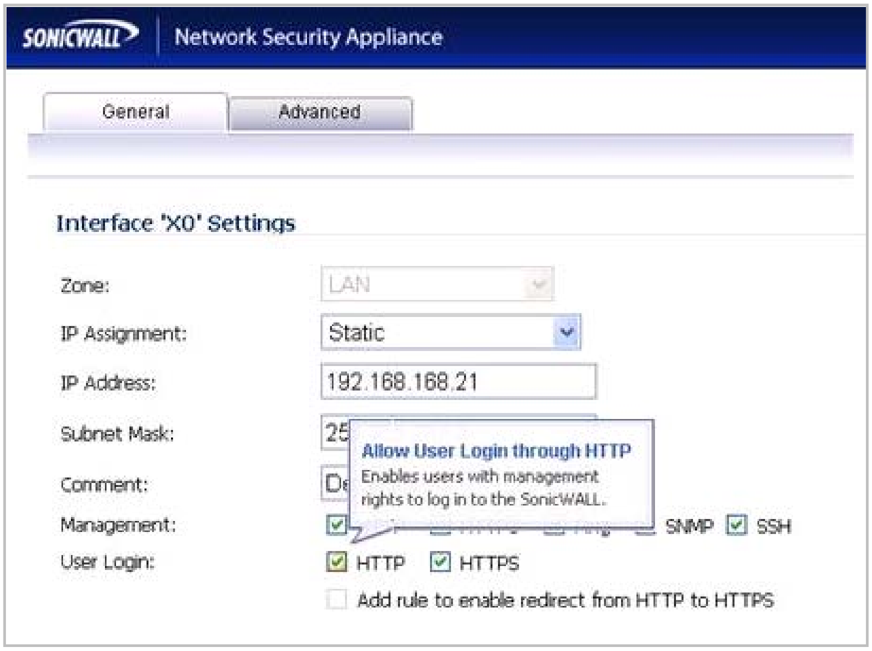
User Groups:

- Content Filtering Bypass
- Guest Services
- Limited Administrators
- SonicWALL Administrators
- SonicWALL Read-Only Admir

Member Of:

- Everyone
- Guest Administrators
- Trusted Users

On the **Network > Interfaces** page, edit the LAN interface. Enable **User Login** via **HTTP** and **HTTPS** to allow the Guest Administrator account to login to the appliance from the LAN.

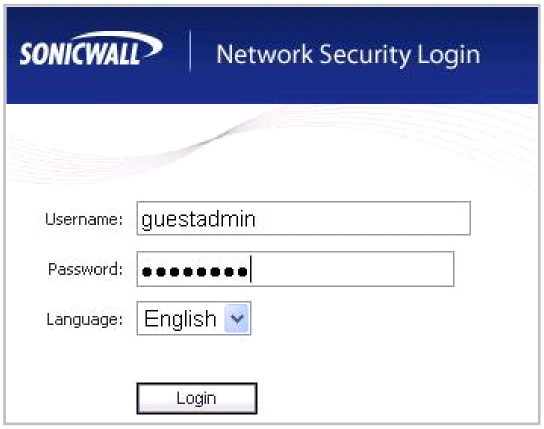


Interface 'X0' Settings

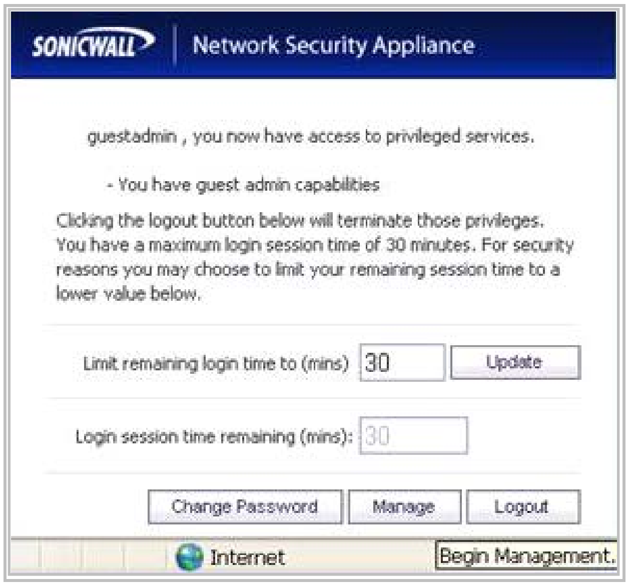
Zone:	LAN
IP Assignment:	Static
IP Address:	192.168.168.21
Subnet Mask:	25
Comment:	De
Management:	☑ □ □ □ SNMP ☑ SSH
User Login:	☑ HTTP ☑ HTTPS
	□ Add rule to enable redirect from HTTP to HTTPS

Allow User Login through HTTP
Enables users with management rights to log in to the SonicWALL.

The Guest Administrator logs in to the appliance and then clicks the **Manage** button.



Username:	guestadmin
Password:	••••••••
Language:	English



guestadmin , you now have access to privileged services.

- You have guest admin capabilities

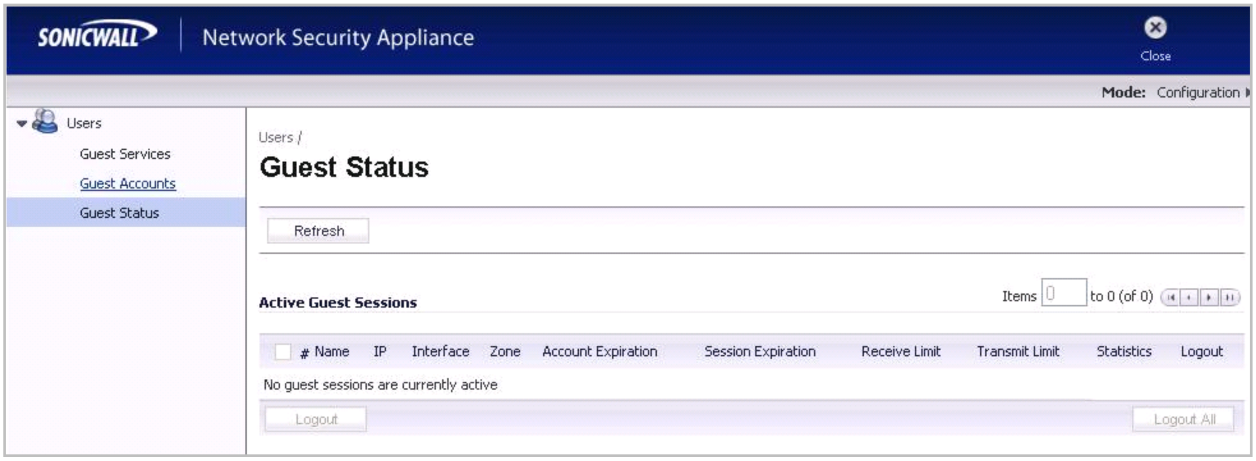
Clicking the logout button below will terminate those privileges. You have a maximum login session time of 30 minutes. For security reasons you may choose to limit your remaining session time to a lower value below.

Limit remaining login time to (mins) 30

Login session time remaining (mins): 30

Begin Management.

After logging in, the Guest Administrator can manage guest accounts and sessions, but cannot access any other resources or management interface pages.



Users /

Guest Status

Active Guest Sessions

Items 0 to 0 (of 0)

□	#	Name	IP	Interface	Zone	Account Expiration	Session Expiration	Receive Limit	Transmit Limit	Statistics	Logout

No guest sessions are currently active

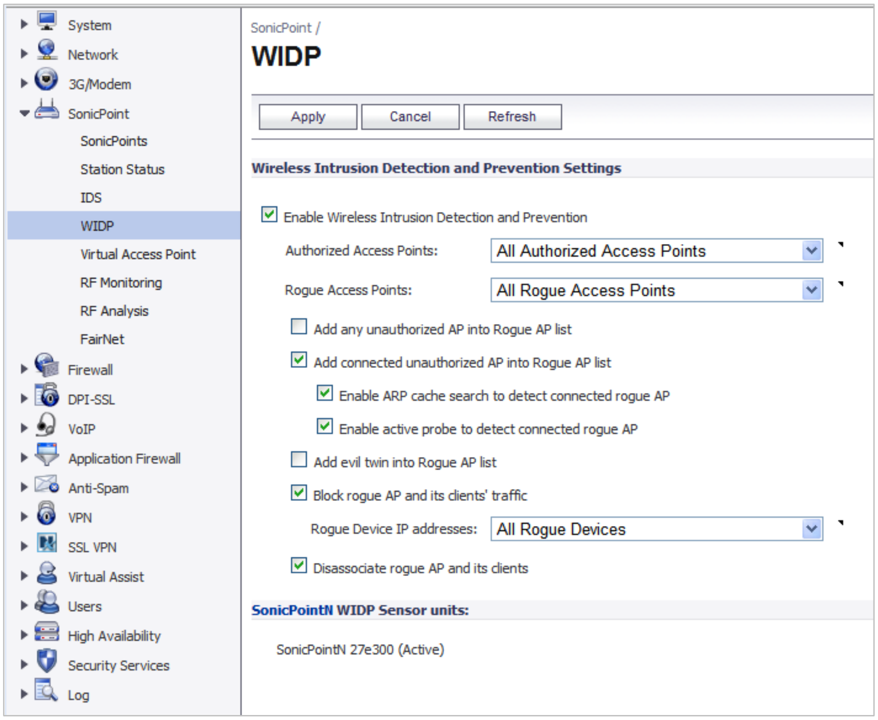
Internal Radio IDS Scan Scheduling

Wireless Intrusion Detection and Prevention (WIDP) monitors the radio spectrum for the presence of unauthorized access points (intrusion detection) and automatically takes counter measures (intrusion prevention). Previously, only a wireless scan was done. SonicOS 5.9 provides a solution that detects rogue access points and takes action according to the administrator settings.

SonicOS Wireless Intrusion Detection and Prevention is based on SonicPoint-N and cooperates with a Dell SonicWALL NSA gateway. This feature turns SonicPoint-Ns into dedicated WIDP sensors that detect unauthorized access points connected to a Dell SonicWALL network.

This feature is implemented on all G5 platforms and is available for single radio SonicPoint-N.

Under **SonicPoint**, a new GUI page was added with WIDP options.



SonicPoint /

WIDP

Wireless Intrusion Detection and Prevention Settings

☑ Enable Wireless Intrusion Detection and Prevention

Authorized Access Points: All Authorized Access Points

Rogue Access Points: All Rogue Access Points

□ Add any unauthorized AP into Rogue AP list

☑ Add connected unauthorized AP into Rogue AP list

☑ Enable ARP cache search to detect connected rogue AP

☑ Enable active probe to detect connected rogue AP

□ Add evil twin into Rogue AP list

☑ Block rogue AP and its clients' traffic

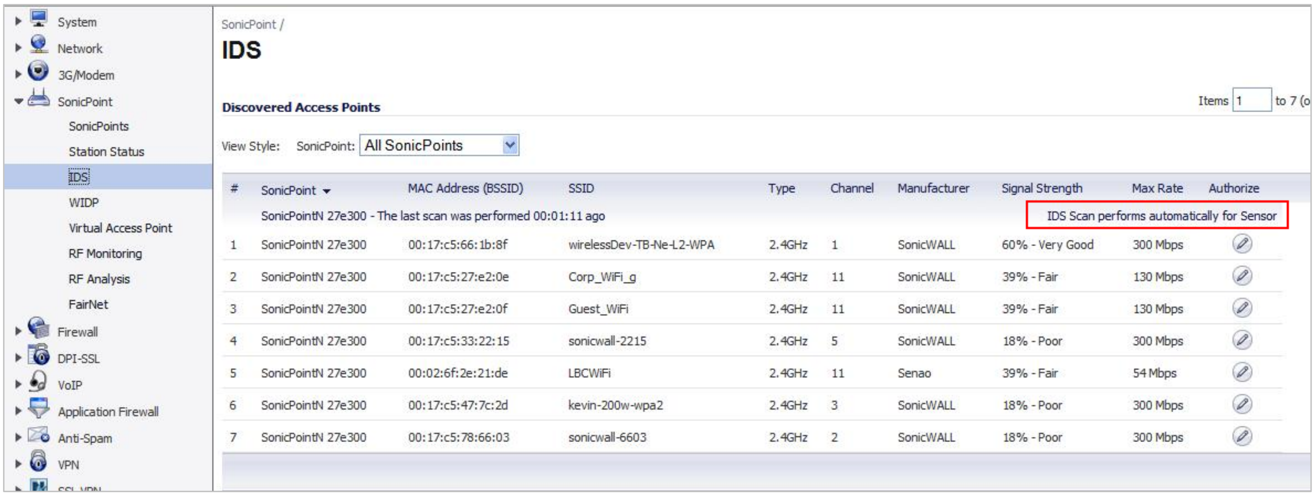
Rogue Device IP addresses: All Rogue Devices

☑ Disassociate rogue AP and its clients

SonicPointN WIDP Sensor units:

SonicPointN 27e300 (Active)

When a SonicPointN is configured as a WIDP sensor, it can no longer function as an access point. IDS scans are done automatically.



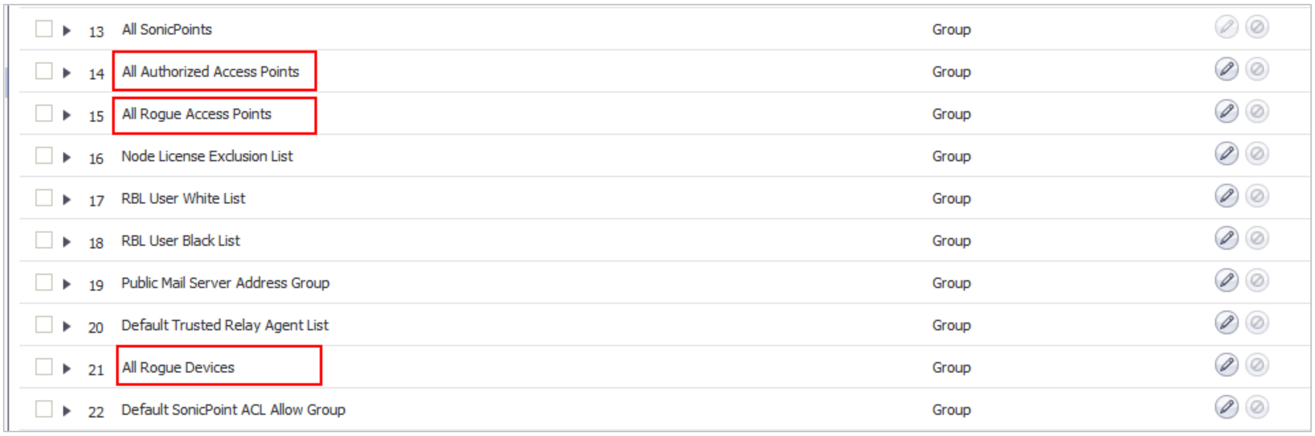
IDS

Discovered Access Points

SonicPoint: All SonicPoints

#	SonicPoint	MAC Address (BSSID)	SSID	Type	Channel	Manufacturer	Signal Strength	Max Rate	Authorize
	SonicPointN 27e300 - The last scan was performed 00:01:11 ago						IDS Scan performs automatically for Sensor		
1	SonicPointN 27e300	00:17:c5:66:1b:8f	wirelessDev-TB-Ne-L2-WPA	2.4GHz	1	SonicWALL	60% - Very Good	300 Mbps	✎
2	SonicPointN 27e300	00:17:c5:27:e2:0e	Corp_WiFi_g	2.4GHz	11	SonicWALL	39% - Fair	130 Mbps	✎
3	SonicPointN 27e300	00:17:c5:27:e2:0f	Guest_WiFi	2.4GHz	11	SonicWALL	39% - Fair	130 Mbps	✎
4	SonicPointN 27e300	00:17:c5:33:22:15	sonicwall-2215	2.4GHz	5	SonicWALL	18% - Poor	300 Mbps	✎
5	SonicPointN 27e300	00:02:6f:2e:21:de	LBCWiFi	2.4GHz	11	Senao	39% - Fair	54 Mbps	✎
6	SonicPointN 27e300	00:17:c5:47:7c:2d	kevin-200w-wpa2	2.4GHz	3	SonicWALL	18% - Poor	300 Mbps	✎
7	SonicPointN 27e300	00:17:c5:78:66:03	sonicwall-6603	2.4GHz	2	SonicWALL	18% - Poor	300 Mbps	✎

When an access point is identified as a rogue access point, its MAC address is added to the **All Rogue Access Points** group, and its source IP address is added to **All Rogue Devices** group.



□	▶	13	All SonicPoints	Group	✎ ⊘
□	▶	14	All Authorized Access Points	Group	✎ ⊘
□	▶	15	All Rogue Access Points	Group	✎ ⊘
□	▶	16	Node License Exclusion List	Group	✎ ⊘
□	▶	17	RBL User White List	Group	✎ ⊘
□	▶	18	RBL User Black List	Group	✎ ⊘
□	▶	19	Public Mail Server Address Group	Group	✎ ⊘
□	▶	20	Default Trusted Relay Agent List	Group	✎ ⊘
□	▶	21	All Rogue Devices	Group	✎ ⊘
□	▶	22	Default SonicPoint ACL Allow Group	Group	✎ ⊘

Figure 1 - All Rogue AP address object group

For SonicPointNs, no access point mode VAP is created. One station mode VAP is created, which is used to do IDS scans, and to connect to and send probes to unsecured access points.

SonicPoint 802.11e (WMM) QoS

SonicPoint access points now support Wi-Fi Multimedia (WMM) to provide a better Quality of Service experience on miscellaneous applications, including VoIP on Wi-Fi phones, and multimedia traffic on IEEE 802.11 networks. WMM is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard. It prioritizes traffic according to four access categories: voice, video, best effort, and background. Note that WMM does not provide guaranteed throughput. Supported on SonicPoint-N/Ni/Ne/NDR.

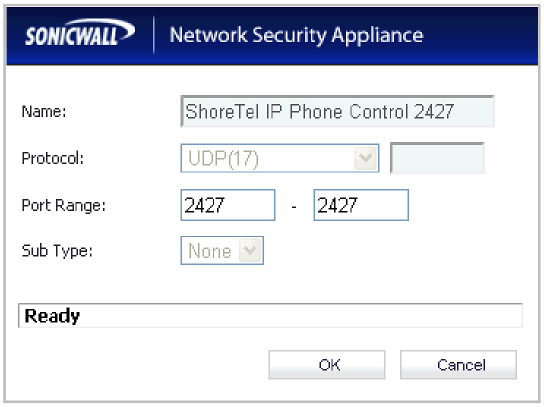
The following table shows the User Priority to Access Category mapping for the four access categories:

Priority	UP (Same as 802.1D user priority)	802.1D designation	AC	Designation (informative)
Lowest	1	BK	AC_BK	Background
	2	—	AC_BK	Background
	0	BE	AC_BE	Best Effort
↓	3	EE	AC_BE	Best Effort
	4	CL	AC_VI	Video
Highest	5	VI	AC_VI	Video
	6	VO	AC_VO	Voice
	7	NC	AC_VO	Voice

Each Access Category has its own transmit queue. WMM requires the SonicPoint-N to implement multiple queues for multiple priority access categories. The SonicPoint-N relies on either the application or the firewall to provide type of service (TOS) information in the IP data in order to differentiate traffic types. One way to provide TOS is through firewall services and access rules; another way is through VLAN tagging.

Firewall Services and Access Rules:

Services using a certain port can be prioritized and put into a proper transmit queue. For example, UDP traffic sending to port 2427 can be regarded as a video stream. The firewall administrator can add a custom service on the **Firewall > Services** page, similar to the following:



Name: ShoreTel IP Phone Control 2427

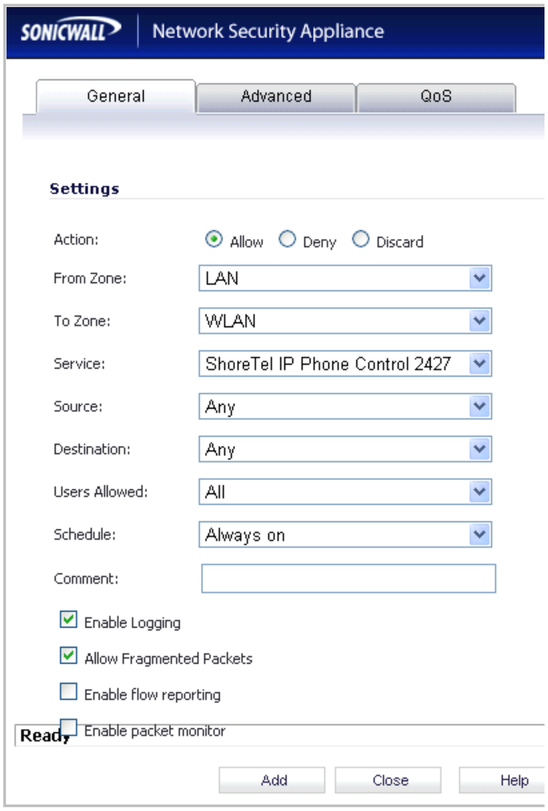
Protocol: UDP(17)

Port Range: 2427 - 2427

Sub Type: None

Ready

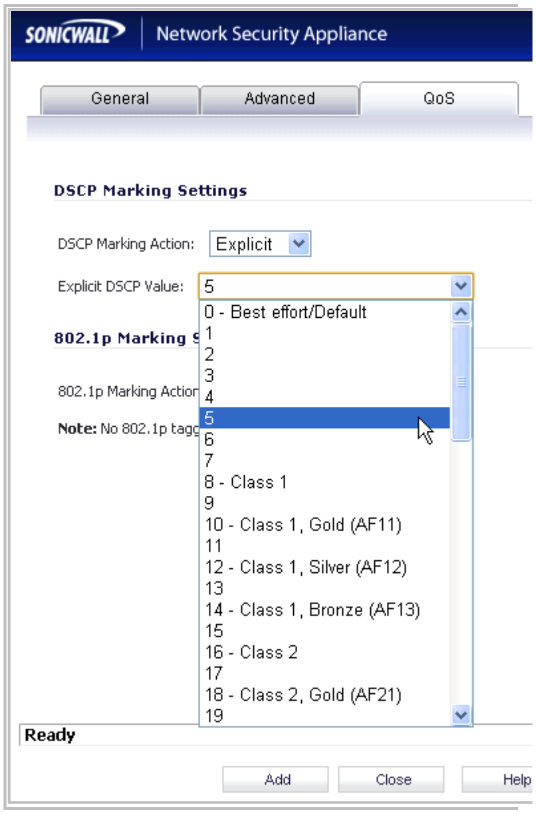
At least one access rule should be added on the **Firewall > Access Rules** page for the new service. For example, when such a service happens from a station on the LAN zone to a wireless client on the WLAN zone, an access rule can be inserted. In the QoS setting tab, an explicit DSCP value is defined. Later, when packets are sent to the SonicPoint-N via the firewall using UDP protocol with destination port 2427, their TOS fields are set according to the QoS setting in the access rule. The General and QoS tabs of an example access rule are shown below:



Settings

Action: ● Allow ○ Deny ○ Discard
From Zone: LAN
To Zone: WLAN
Service: ShoreTel IP Phone Control 2427
Source: Any
Destination: Any
Users Allowed: All
Schedule: Always on
Comment:
☑ Enable Logging
☑ Allow Fragmented Packets
□ Enable flow reporting
□ Enable packet monitor

Ready



DSCP Marking Settings

DSCP Marking Action: Explicit
Explicit DSCP Value: 5

0 - Best effort/Default
1
2
3
4
5
6
7
8 - Class 1
9
10 - Class 1, Gold (AF11)
11
12 - Class 1, Silver (AF12)
13
14 - Class 1, Bronze (AF13)
15
16 - Class 2
17
18 - Class 2, Gold (AF21)
19

802.1p Marking S

802.1p Marking Actior

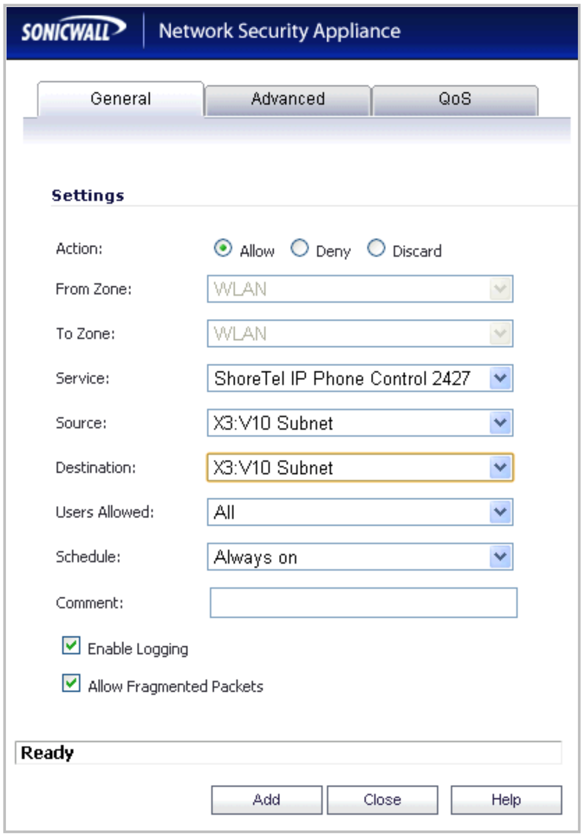
Note: No 802.1p tagg

Ready

VLAN Tagging:

Prioritization is possible in VLAN over Virtual Access Point (VAP), because the SonicPoint-N allows a VAP to be configured to connect with a VLAN by using same VLAN ID. You can set priority for VLAN traffic through a firewall access rule.

The firewall access rule is similar to that shown above to set priority for a UDP service destined to a port such as 2427, but is configured with a VLAN (VLAN over VAP) interface, such as X3:V10 Subnet, as the **Source** and **Destination**, and is a WLAN to WLAN rule.



Settings

Action: ● Allow ○ Deny ○ Discard

From Zone: WLAN

To Zone: WLAN

Service: ShoreTel IP Phone Control 2427

Source: X3:V10 Subnet

Destination: X3:V10 Subnet

Users Allowed: All

Schedule: Always on

Comment:

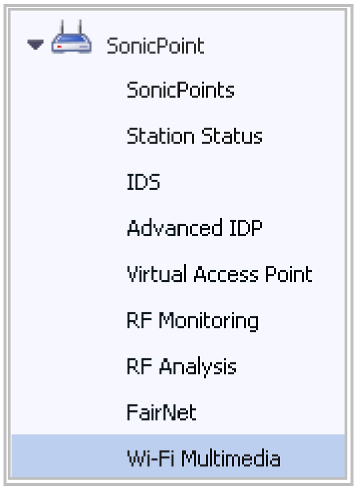
☑ Enable Logging

☑ Allow Fragmented Packets

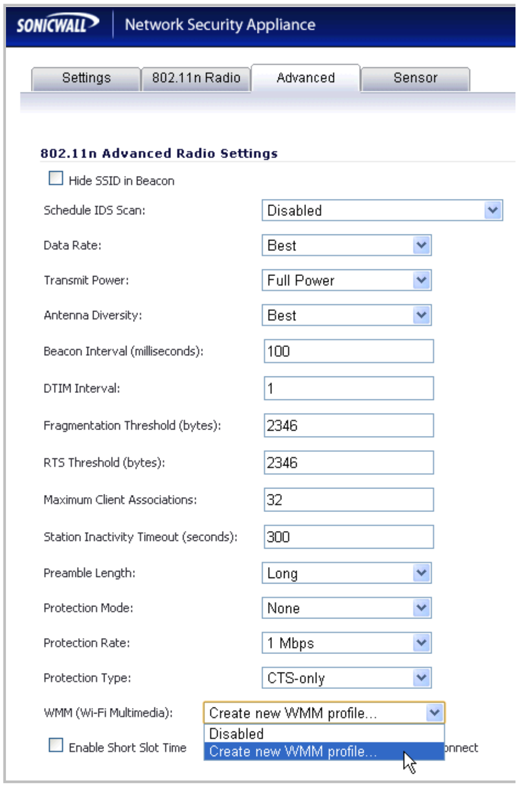
Ready

SonicPoint WMM Configuration

The **SonicPoint > Wi-Fi Multimedia** page provides a way to configure WMM profiles, including parameters and priority mappings.



You can also create a WMM profile or select an existing WMM profile when configuring a SonicPoint-N or a SonicPoint-N Profile from the **SonicPoint > SonicPoints** page. The configuration window provides a WMM **(Wi-Fi Multimedia)** drop-down list on the **Advanced** tab with these options.



802.11n Advanced Radio Settings

□ Hide SSID in Beacon

Schedule IDS Scan: Disabled

Data Rate: Best

Transmit Power: Full Power

Antenna Diversity: Best

Beacon Interval (milliseconds): 100

DTIM Interval: 1

Fragmentation Threshold (bytes): 2346

RTS Threshold (bytes): 2346

Maximum Client Associations: 32

Station Inactivity Timeout (seconds): 300

Preamble Length: Long

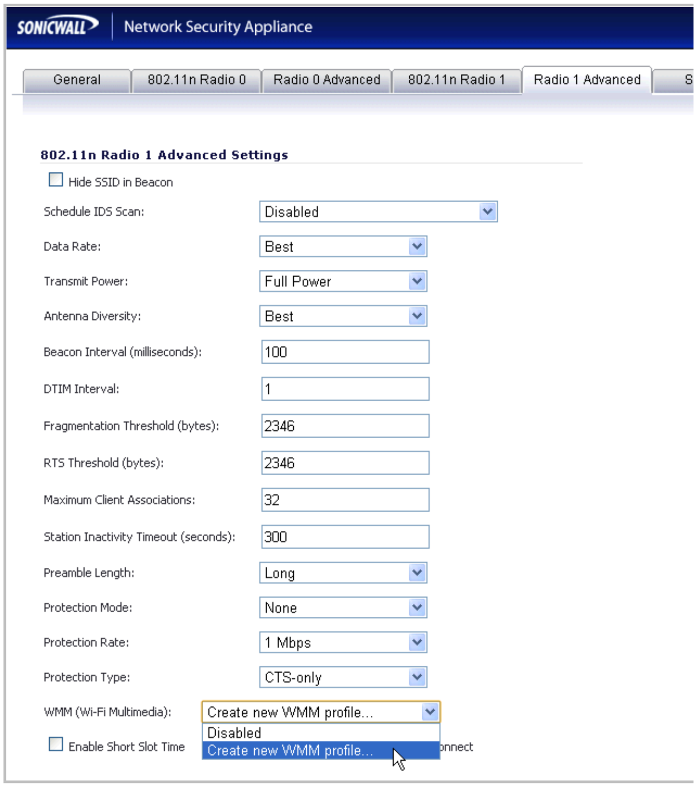
Protection Mode: None

Protection Rate: 1 Mbps

Protection Type: CTS-only

WMM (Wi-Fi Multimedia): Create new WMM profile...

□ Enable Short Slot Time



802.11n Radio 1 Advanced Settings

□ Hide SSID in Beacon

Schedule IDS Scan: Disabled

Data Rate: Best

Transmit Power: Full Power

Antenna Diversity: Best

Beacon Interval (milliseconds): 100

DTIM Interval: 1

Fragmentation Threshold (bytes): 2346

RTS Threshold (bytes): 2346

Maximum Client Associations: 32

Station Inactivity Timeout (seconds): 300

Preamble Length: Long

Protection Mode: None

Protection Rate: 1 Mbps

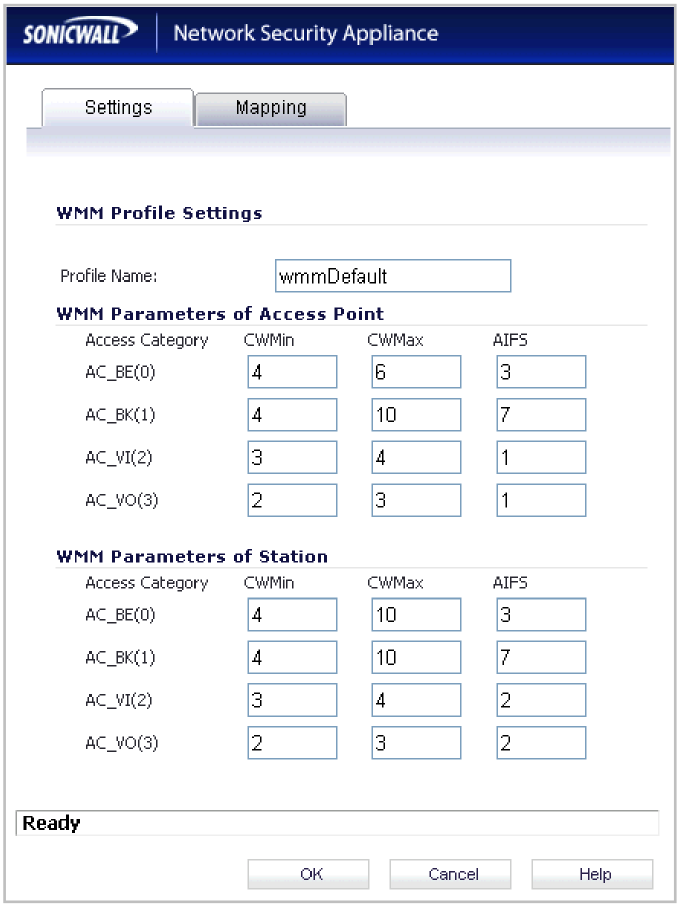
Protection Type: CTS-only

WMM (Wi-Fi Multimedia): Create new WMM profile...

□ Enable Short Slot Time

When configuring the WMM profile, on the **Settings** tab, the administrator can configure the size of the contention window (CWMin/CWMax) and the arbitration interframe space (AIFS) number when creating a WMM profile. These values can be configured individually for each priority, AC_BK, AC_BE, AC_VI, and AC_VO on the Access Point (SonicPoint-N) and for the Station (firewall).

The **Mapping** tab allows you to map priority levels to DSCP values. The default DSCP values are as same as the ones in **Firewall > Access Rules**, **QoS** mapping.



WMM Profile Settings

Profile Name: wmmDefault

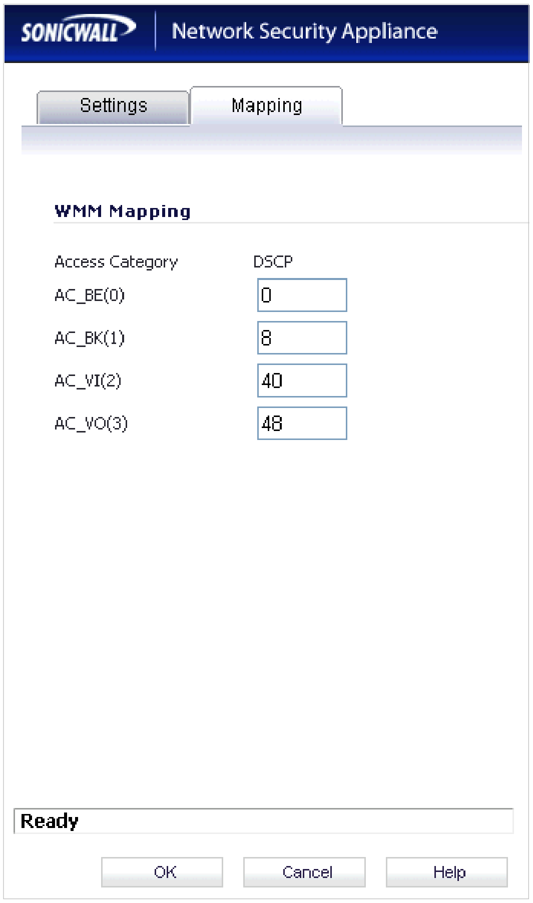
WMM Parameters of Access Point

Access Category	CWMin	CWMax	AIFS
AC_BE(0)	4	6	3
AC_BK(1)	4	10	7
AC_VI(2)	3	4	1
AC_VO(3)	2	3	1

WMM Parameters of Station

Access Category	CWMin	CWMax	AIFS
AC_BE(0)	4	10	3
AC_BK(1)	4	10	7
AC_VI(2)	3	4	2
AC_VO(3)	2	3	2

Ready



WMM Mapping

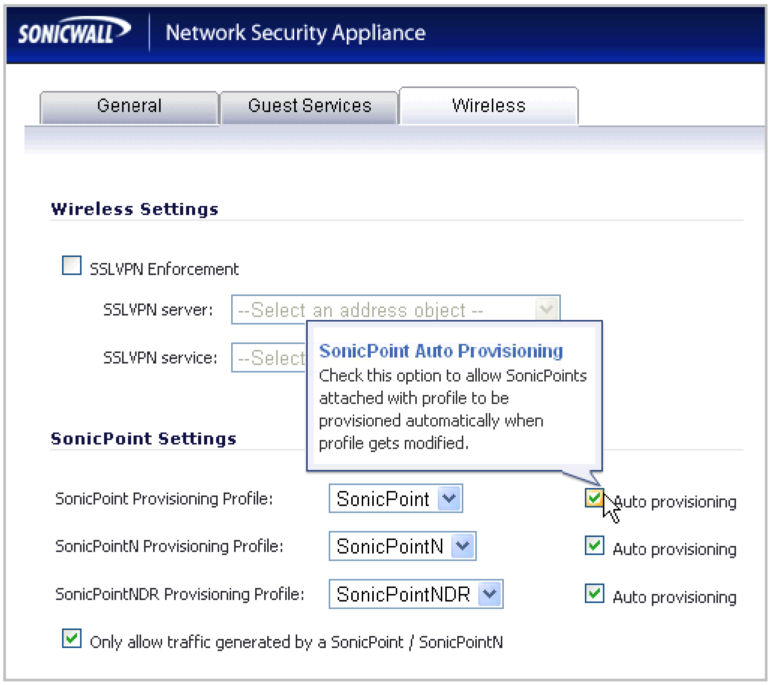
Access Category	DSCP
AC_BE(0)	0
AC_BK(1)	8
AC_VI(2)	40
AC_VO(3)	48

Ready

SonicPoint Auto Provisioning

A SonicPoint can be re-provisioned automatically according to a wireless zone profile. This increases management efficiency and ease of use, as previously a SonicPoint had to be deleted and re-added in order to be re-provisioned with a modified profile. Supported on SonicPoint-N/Ni/Ne/NDR/a/g.

To enable automatic provisioning, navigate to the **Network > Zones** page and click the Configure icon for the WLAN zone. In the Edit Zone window on the **Wireless** tab, select the **Auto provisioning** checkbox for each type of **SonicPoint Provisioning Profile** listed there, and then click **OK**.



Wireless Settings

☐ SSLVPN Enforcement

SSLVPN server: --Select an address object --

SSLVPN service: --Select

SonicPoint Auto Provisioning
Check this option to allow SonicPoints attached with profile to be provisioned automatically when profile gets modified.

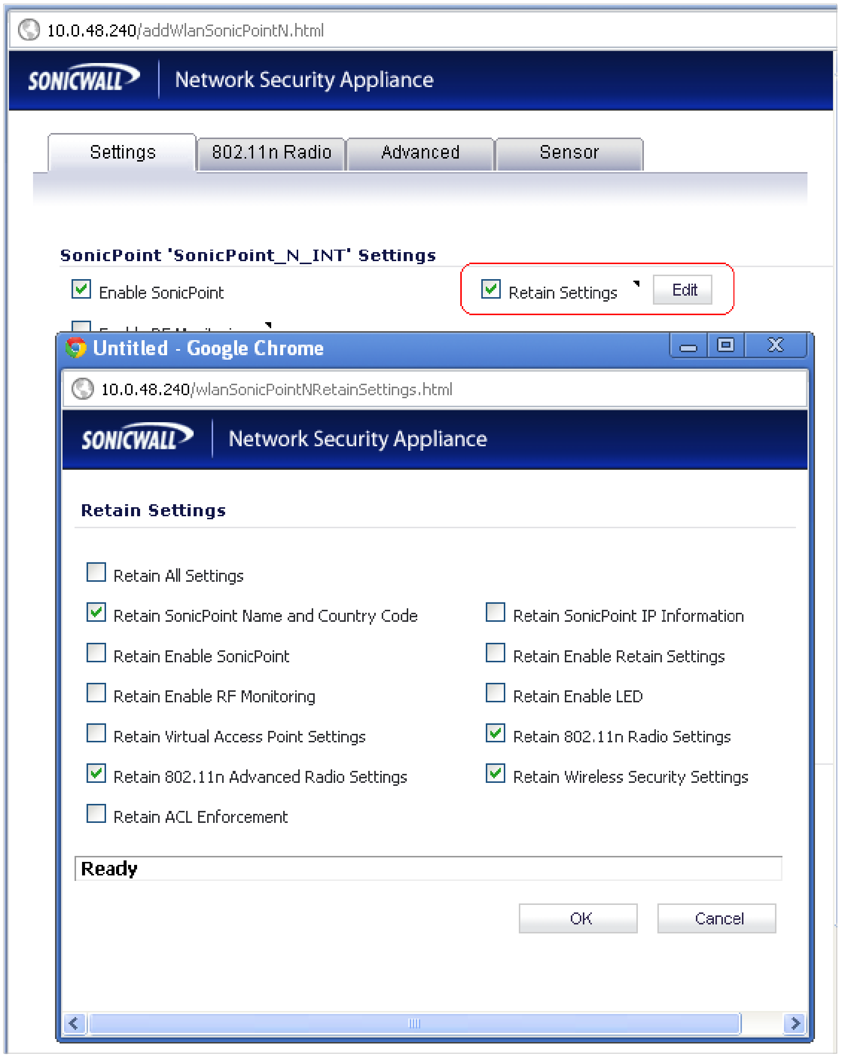
SonicPoint Settings

SonicPoint Provisioning Profile:	SonicPoint	☑ Auto provisioning
SonicPointN Provisioning Profile:	SonicPointN	☑ Auto provisioning
SonicPointNDR Provisioning Profile:	SonicPointNDR	☑ Auto provisioning

☑ Only allow traffic generated by a SonicPoint / SonicPointN

SonicPoint Customized Configuration Retaining

SonicOS 5.9 introduces the ability to configure SonicPoint profiles so that the SonicPoints retain portions of their configuration after they are deleted and resynchronized. To configure this feature, navigate to the **SonicPoint > SonicPoints** page and click the **configure** icon for the appropriate SonicPoint profile. Enable the **Retain Settings** checkbox and click the **Edit** button to configure which settings will be retained.


10.0.48.240/addWlanSonicPointN.html
SONICWALL
Network Security Appliance
Settings
802.11n Radio
Advanced
Sensor
Untitled - Google Chrome
10.0.48.240/wlanSonicPointNRetainSettings.html
SONICWALL
Network Security Appliance
OK
Cancel
Edit

SonicPoint 'SonicPoint_N_INT' Settings

☑ Enable SonicPoint

☑ Retain Settings

Retain Settings

☐ Retain All Settings

☑ Retain SonicPoint Name and Country Code

☐ Retain Enable SonicPoint

☐ Retain Enable RF Monitoring

☐ Retain Virtual Access Point Settings

☑ Retain 802.11n Advanced Radio Settings

☐ Retain ACL Enforcement

☐ Retain SonicPoint IP Information

☐ Retain Enable Retain Settings

☐ Retain Enable LED

☑ Retain 802.11n Radio Settings

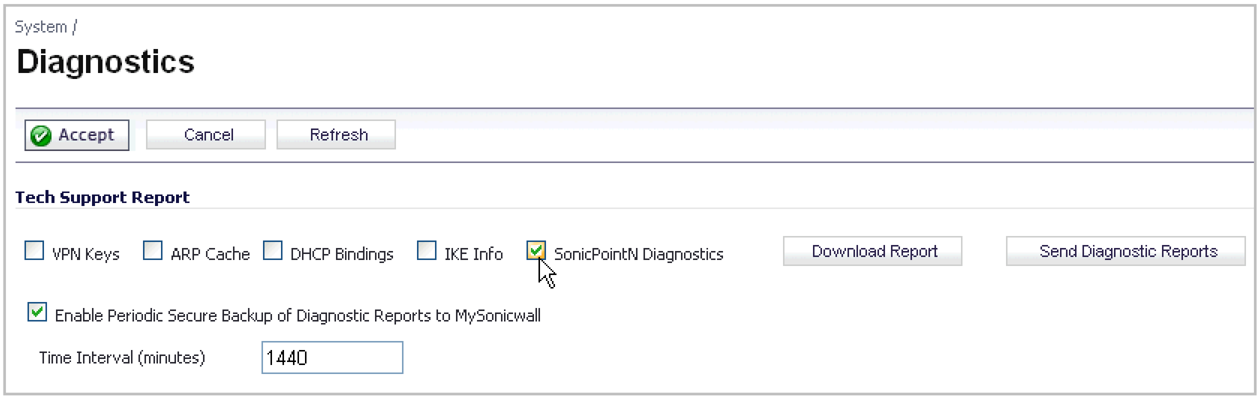
☑ Retain Wireless Security Settings

Ready

SonicPoint Diagnostics Enhancement

A SonicPoint can collect critical runtime data and save it into persistent storage. If the SonicPoint has a failure, the Dell SonicWALL managing appliance retrieves that data when the SonicPoint reboots, and incorporates it into the Tech Support Report (TSR). A subsequent SonicPoint failure will overwrite the data. Supported on SonicPoint-N/Ni/Ne/NDR.

To enable this feature, navigate to the **System > Diagnostics** page and select the **SonicPointN Diagnostics** checkbox in the **Tech Support Report** section, then click **Accept**.



System /

Diagnostics

Accept | Cancel | Refresh

Tech Support Report

□ VPN Keys □ ARP Cache □ DHCP Bindings □ IKE Info ☑ SonicPointN Diagnostics | Download Report | Send Diagnostic Reports

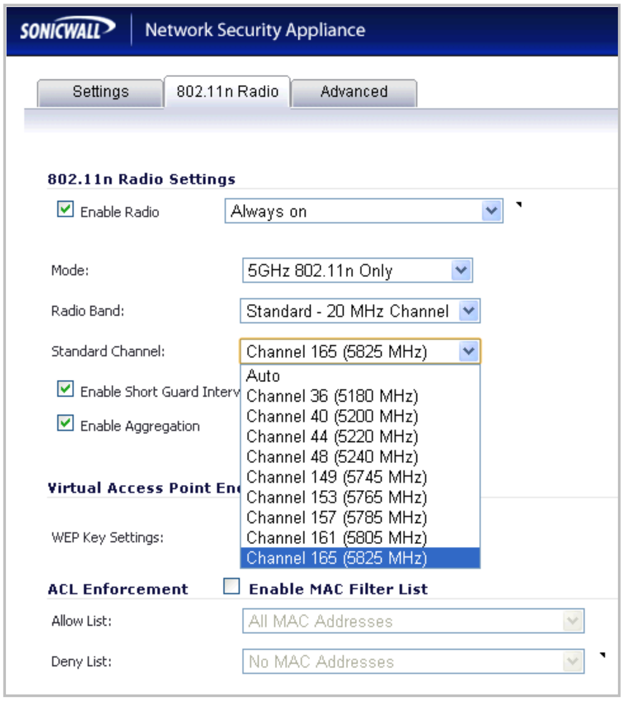
☑ Enable Periodic Secure Backup of Diagnostic Reports to MySonicwall

Time Interval (minutes): 1440

SonicPoint Dynamic Frequency Selection (DFS) Support

After a DFS certificate is issued, the SonicPoint-N can support dynamic frequency selection to allow a SonicPoint-N to be deployed in sensitive channels of the 5 GHz frequency band. Supported on SonicPoint-N.

To view and select from these 5 GHz channels, navigate to **SonicPoint > SonicPoints** and configure a SonicPoint-N Profile or an individual SonicPoint-N. On the **802.11n Radio** tab, select any 5 GHz setting in the **Mode** field, then select either Standard or Wide as the **Radio Band**. The **Standard Channel** or **Primary Channel** drop-down lists display a choice of sensitive channels.



SONICWALL | Network Security Appliance

Settings | 802.11n Radio | Advanced

802.11n Radio Settings

☑ Enable Radio: Always on

Mode: 5GHz 802.11n Only

Radio Band: Standard - 20 MHz Channel

Standard Channel: Channel 165 (5825 MHz)

Auto
Channel 36 (5180 MHz)
Channel 40 (5200 MHz)
Channel 44 (5220 MHz)
Channel 48 (5240 MHz)
Channel 149 (5745 MHz)
Channel 153 (5765 MHz)
Channel 157 (5785 MHz)
Channel 161 (5805 MHz)
Channel 165 (5825 MHz)

☑ Enable Short Guard Interv

☑ Enable Aggregation

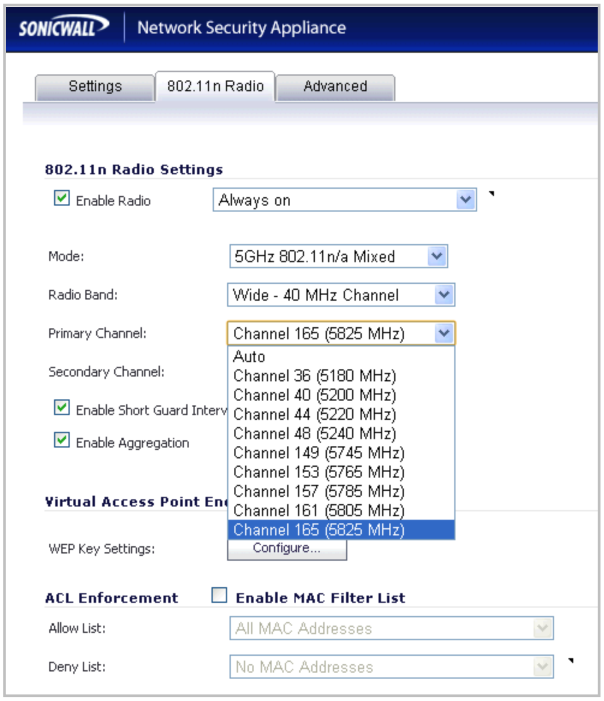
Virtual Access Point En

WEP Key Settings:

ACL Enforcement □ Enable MAC Filter List

Allow List: All MAC Addresses

Deny List: No MAC Addresses



SONICWALL | Network Security Appliance

Settings | 802.11n Radio | Advanced

802.11n Radio Settings

☑ Enable Radio: Always on

Mode: 5GHz 802.11n/a Mixed

Radio Band: Wide - 40 MHz Channel

Primary Channel: Channel 165 (5825 MHz)

Auto
Channel 36 (5180 MHz)
Channel 40 (5200 MHz)
Channel 44 (5220 MHz)
Channel 48 (5240 MHz)
Channel 149 (5745 MHz)
Channel 153 (5765 MHz)
Channel 157 (5785 MHz)
Channel 161 (5805 MHz)
Channel 165 (5825 MHz)

Secondary Channel:

☑ Enable Short Guard Interv

☑ Enable Aggregation

Virtual Access Point En

WEP Key Settings: Configure...

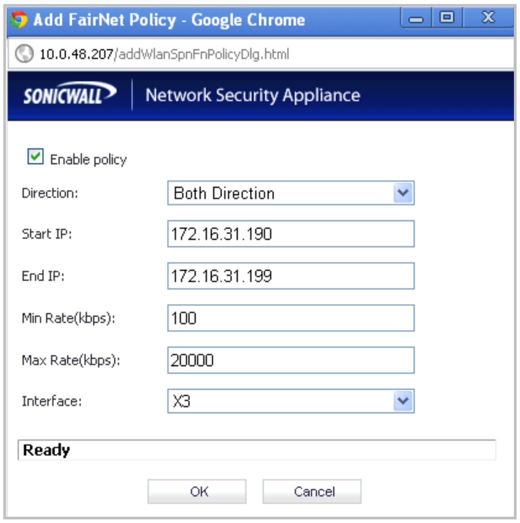
ACL Enforcement □ Enable MAC Filter List

Allow List: All MAC Addresses

Deny List: No MAC Addresses

SonicPoint FairNet Support

After optimizing the system resources, FairNet is now supported on the SonicPoint-Ni and SonicPoint-Ne to provide bandwidth fairness control in the WLAN. FairNet continues to be supported on SonicPoint-N and SonicPoint-N DR. To configure a FairNet policy, navigate to the **SonicPoint > FairNet** page and click the **Add** button.


Add FairNet Policy - Google Chrome
10.0.48.207/addWlanSpnFnPolicyDlg.html
SONICWALL
Network Security Appliance
OK
Cancel

☑ Enable policy

Direction: Both Direction

Start IP: 172.16.31.190

End IP: 172.16.31.199

Min Rate(kbps): 100

Max Rate(kbps): 20000

Interface: X3

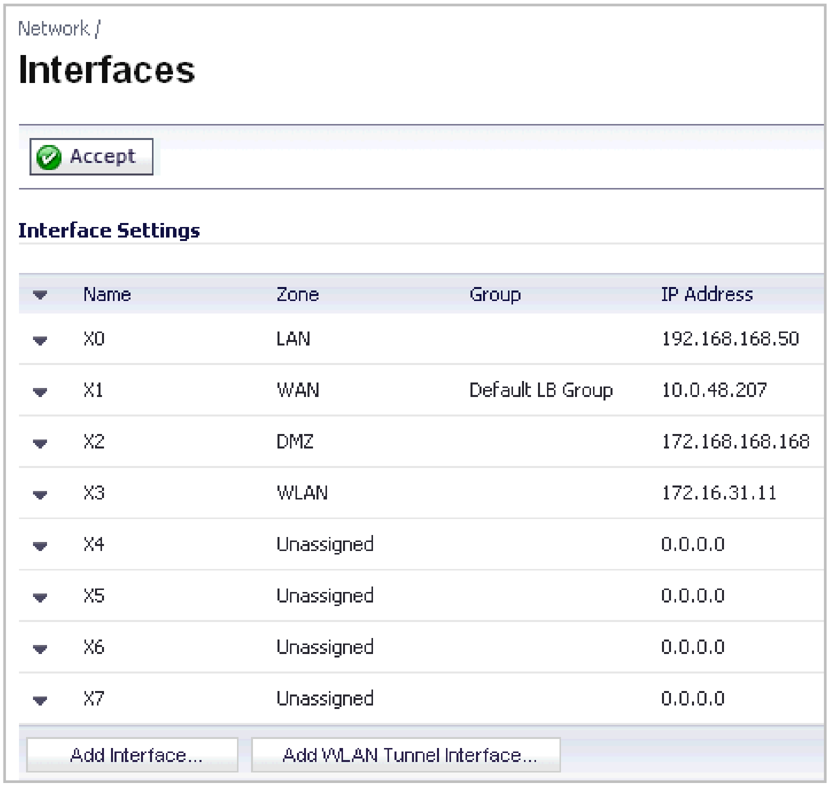
Ready

Use the **Start IP** and **End IP** fields to specify a subset of the SonicPoint DHCP range. The rates are per client; the minimum is 100 Kbps and the maximum is 300 Mbps (300,000 Kbps), although 20 Mbps might be a more typical **Max Rate** setting.

SonicPoint Layer 3 Management Phase I

This enhancement provides the DHCP and tunneling solution to support SonicPoint deployment in a Layer 3 network. SonicOS DHCP-based Discovery Protocol (SDDP) is based on the well-known DHCP protocol and allows the Dell SonicWALL gateway and SonicPoint to discover each other automatically across Layer 3 local networks. The remote network management protocol, SonicOS SSLVPN-based Management Protocol (SSMP), is based on SonicOS SSLVPN infrastructure to allow SonicPoints to be managed by a Dell SonicWALL network security appliance with the SSL-VPN option enabled. This feature is supported on SonicPoint-N/Ni/Ne/NDR wireless access points.

To configure the Layer 3 settings, navigate to the **Network > Interfaces** page and click the **Add WLAN Tunnel Interface** button below the **Interface Settings** table.



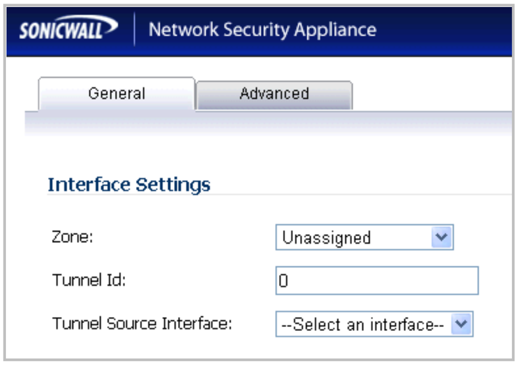
Network /

Interfaces

Interface Settings

Name	Zone	Group	IP Address
X0	LAN		192.168.168.50
X1	WAN	Default LB Group	10.0.48.207
X2	DMZ		172.168.168.168
X3	WLAN		172.16.31.11
X4	Unassigned		0.0.0.0
X5	Unassigned		0.0.0.0
X6	Unassigned		0.0.0.0
X7	Unassigned		0.0.0.0

When first displayed, the configuration page displays only three fields.



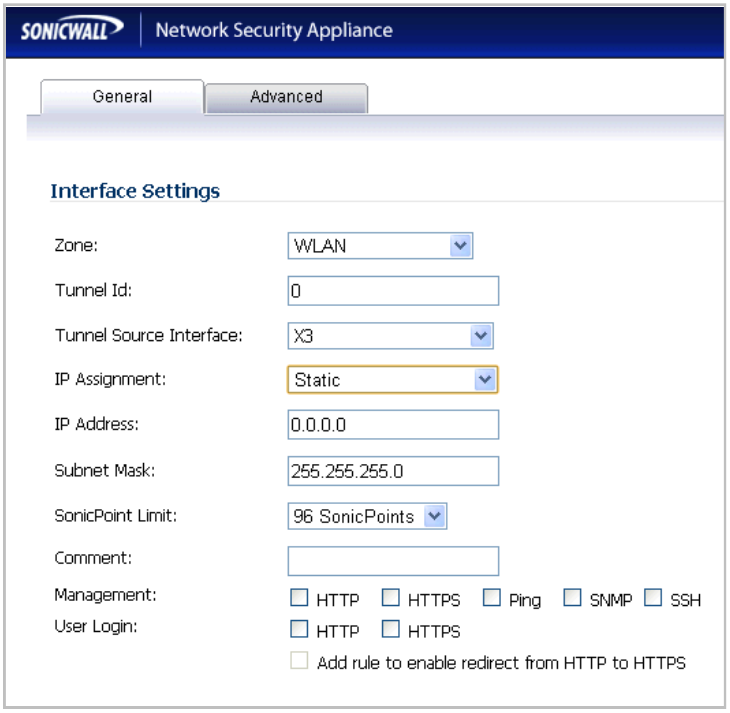
Interface Settings

Zone: Unassigned

Tunnel Id: 0

Tunnel Source Interface: --Select an interface--

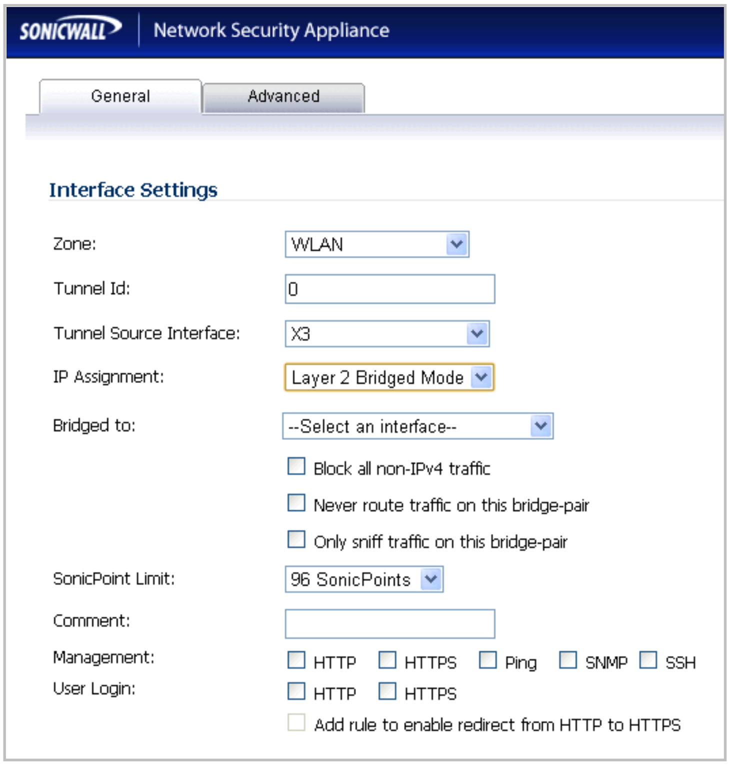
Select **WLAN** for the **Zone**. More fields are displayed. Select an interface that is connected to the SonicPoint-N from the **Tunnel Source Interface** drop-down list.



Interface Settings

Zone:	WLAN
Tunnel Id:	0
Tunnel Source Interface:	X3
IP Assignment:	Static
IP Address:	0.0.0.0
Subnet Mask:	255.255.255.0
SonicPoint Limit:	96 SonicPoints
Comment:	
Management:	□ HTTP □ HTTPS □ Ping □ SNMP □ SSH
User Login:	□ HTTP □ HTTPS
	□ Add rule to enable redirect from HTTP to HTTPS

You can choose an **IP Assignment** of either **Static** (shown above) or **Layer 2 Bridged Mode** (shown below). Fill in the **IP Address** or **Bridged to** interface and select the management options, then click **OK**.



Interface Settings

Zone:	WLAN
Tunnel Id:	0
Tunnel Source Interface:	X3
IP Assignment:	Layer 2 Bridged Mode
Bridged to:	--Select an interface--
	□ Block all non-IPv4 traffic
	□ Never route traffic on this bridge-pair
	□ Only sniff traffic on this bridge-pair
SonicPoint Limit:	96 SonicPoints
Comment:	
Management:	□ HTTP □ HTTPS □ Ping □ SNMP □ SSH
User Login:	□ HTTP □ HTTPS
	□ Add rule to enable redirect from HTTP to HTTPS

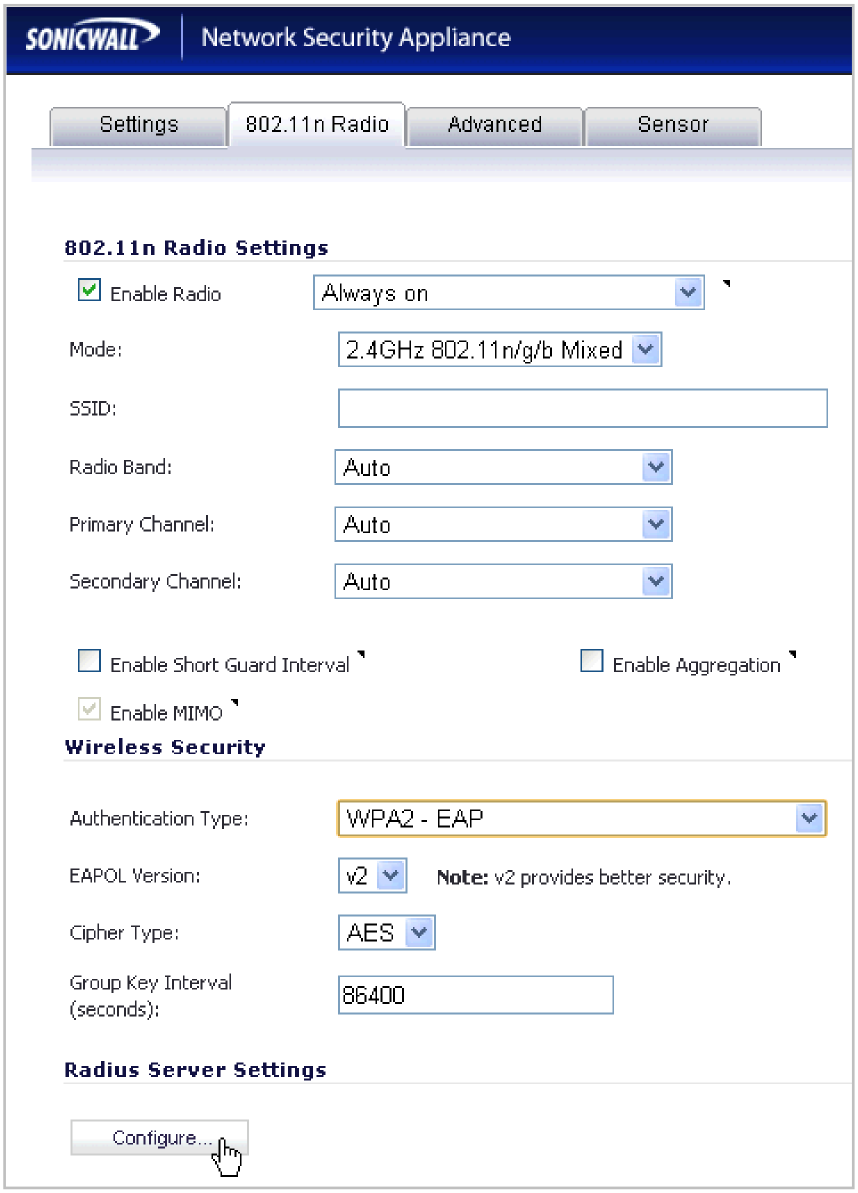
After completing the configuration, the **SonicPointNs** table on the **SonicPoint > SonicPoints** page shows **MGMT: Layer 3** in the **Network Settings** column.

SonicPoint RADIUS Server Failover

Provides round-robin algorithm and more flexibility to manage primary and secondary RADIUS servers of SonicPoint-N/Ni/Ne/NDR. To configure the RADIUS servers, navigate to the **SonicPoint > SonicPoints** page. Add or edit a SonicPoint or a SonicPoint Profile. On the **802.11n Radio** tab under **Wireless Security**, select one of the following for **Authentication Type**:

- WPA – EAP
- WPA2 – EAP
- WPA2 – Auto – EAP

The **Radius Server Settings** section appears in the window.



802.11n Radio Settings

☑ Enable Radio: Always on

Mode: 2.4GHz 802.11n/g/b Mixed

SSID:

Radio Band: Auto

Primary Channel: Auto

Secondary Channel: Auto

☐ Enable Short Guard Interval

☐ Enable Aggregation

☑ Enable MIMO

Wireless Security

Authentication Type: WPA2 - EAP

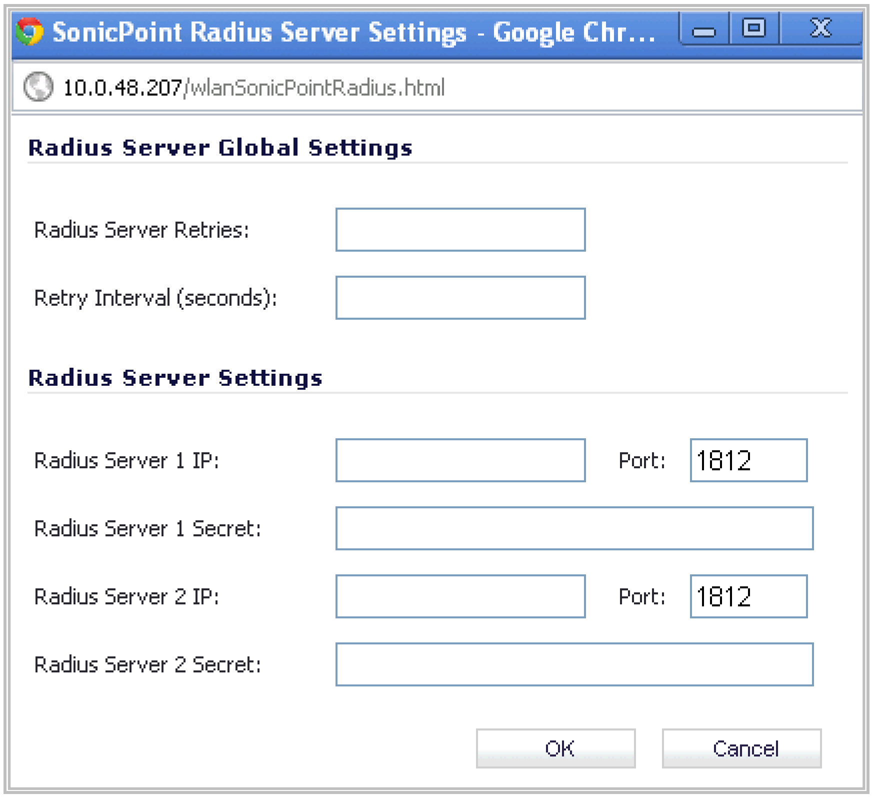
EAPOL Version: v2 **Note:** v2 provides better security.

Cipher Type: AES

Group Key Interval (seconds): 86400

Radius Server Settings

Click the **Configure** button to configure the RADIUS server settings.



SonicPoint Radius Server Settings - Google Chr...

10.0.48.207/wlanSonicPointRadius.html

Radius Server Global Settings

Radius Server Retries:

Retry Interval (seconds):

Radius Server Settings

Radius Server 1 IP: Port: 1812

Radius Server 1 Secret:

Radius Server 2 IP: Port: 1812

Radius Server 2 Secret:

You can set the **Radius Server Retries** to a value between **1** and **10**. This is the number of times the firewall will attempt to connect before it fails over to the other RADIUS server. The **Retry Interval** can be set to a value between **0** and **60** seconds, with a default of 0 meaning no wait between retries.

Under **Radius Server Settings**, enter the **IP** address, **Port**, and **Secret** for each RADIUS server.

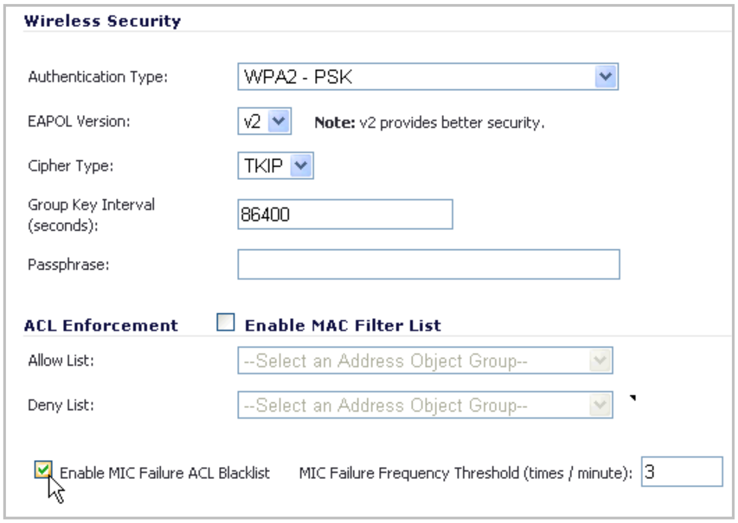
SonicPoint WPA TKIP Countermeasures and MIC Failure Flooding Detection and Protection

Wi-Fi Protected Access (WPA) TKIP countermeasures will lock down the entire Wireless LAN network in situations where an intruder launches a WPA passphrase dictionary attack to generate a Message Integrity Check (MIC) failure flood in an attempt to impact the WLAN functionality and performance. This SonicOS solution can detect a TKIP MIC failure flood and take action with TKIP countermeasures against the source to automatically block them by adding them to the runtime blacklist, protecting the overall system. Supported on SonicPoint-N/Ni/Ne/NDR.

To configure this feature, navigate to the **SonicPoint > SonicPoints** page. Add or edit a SonicPoint or a SonicPoint Profile. On the **802.11n Radio** tab under **Wireless Security**, select one of the following for **Authentication Type**:

- WPA – PSK
- WPA2 – PSK
- WPA2 – Auto – PSK

For the **Cipher Type**, select **TKIP**. Under **ACL Enforcement**, select the **Enable MIC Failure ACL Blacklist** checkbox. You can adjust the **MIC Failure Frequency Threshold** setting. The default is 3 times per minute. Once the threshold is reached, the source is blacklisted.



Wireless Security

Authentication Type: WPA2 - PSK

EAPOL Version: v2 **Note:** v2 provides better security.

Cipher Type: TKIP

Group Key Interval (seconds): 86400

Passphrase:

ACL Enforcement □ **Enable MAC Filter List**

Allow List: --Select an Address Object Group--

Deny List: --Select an Address Object Group--

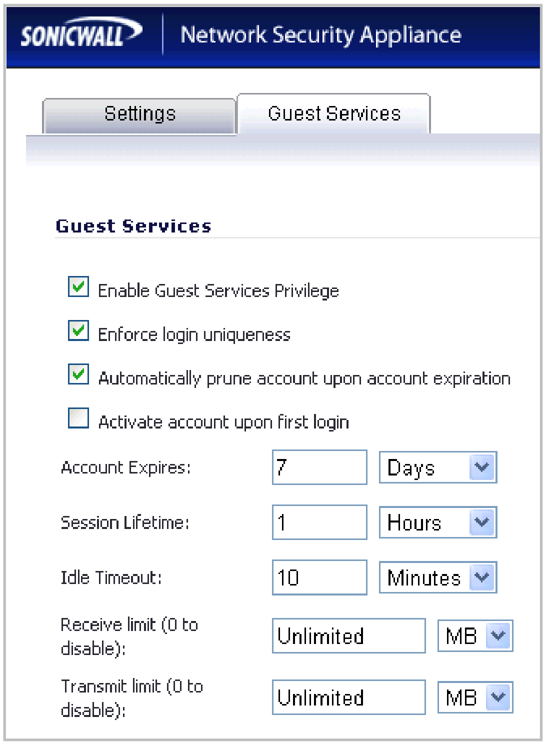
☑ Enable MIC Failure ACL Blacklist MIC Failure Frequency Threshold (times / minute): 3

When a source is blacklisted, it is added to the dynamically created **Default SonicPoint ACL Deny Group**. You can view this on the **Network > Address Objects** page.

Traffic Quota Based Guest Server Policy

Guest sessions can be controlled based on traffic quota policy for better usability. This allows you to configure different transmit/receive limits for different guest clients, possibly based on payment.

To configure a traffic quota based policy, navigate to the **Users > Guest Accounts** page and click the **Add Guest** button. In the Add Guest window on the **Guest Services** tab, set the desired number of megabytes in the **Receive limit** and **Transmit limit** fields. Set the fields to **0** to disable limits. Click **OK**.



Guest Services

☑ Enable Guest Services Privilege

☑ Enforce login uniqueness

☑ Automatically prune account upon account expiration

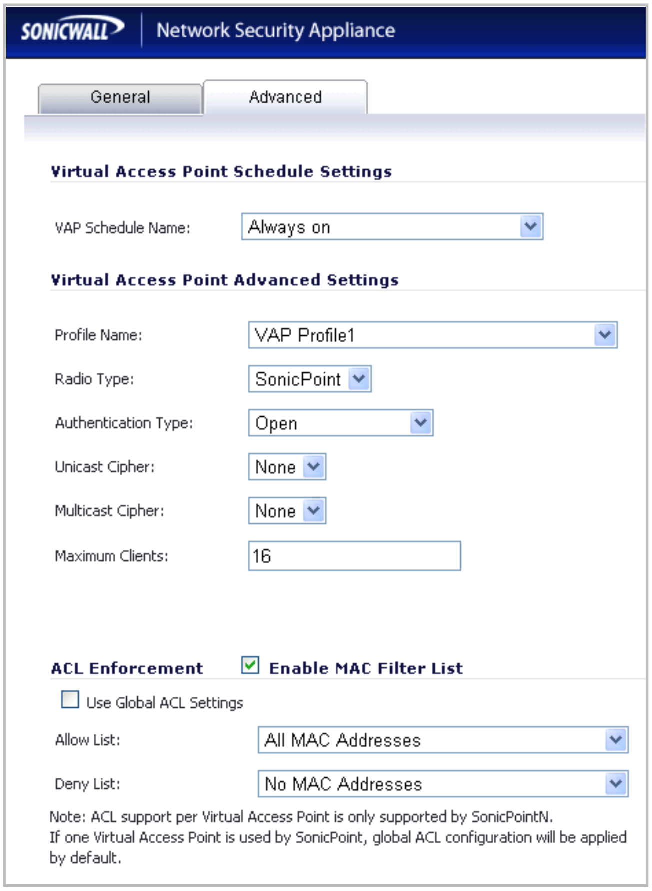
□ Activate account upon first login

Account Expires:	7	Days
Session Lifetime:	1	Hours
Idle Timeout:	10	Minutes
Receive limit (0 to disable):	Unlimited	MB
Transmit limit (0 to disable):	Unlimited	MB

Virtual Access Point ACL Support

Each Virtual Access Point can support an individual Access Control List (ACL) to provide more effective authentication control. Unified ACL support is provided for both SonicPoints and built-in wireless radio.

To enable this feature, navigate to the **SonicPoint > Virtual Access Point** page. Add or edit a Virtual Access Point and click the **Advanced** tab. In the **ACL Enforcement** section, select the **Enable MAC Filter List** checkbox.



Virtual Access Point Schedule Settings

VAP Schedule Name: Always on

Virtual Access Point Advanced Settings

Profile Name: VAP Profile1

Radio Type: SonicPoint

Authentication Type: Open

Unicast Cipher: None

Multicast Cipher: None

Maximum Clients: 16

ACL Enforcement ☑ Enable MAC Filter List

□ Use Global ACL Settings

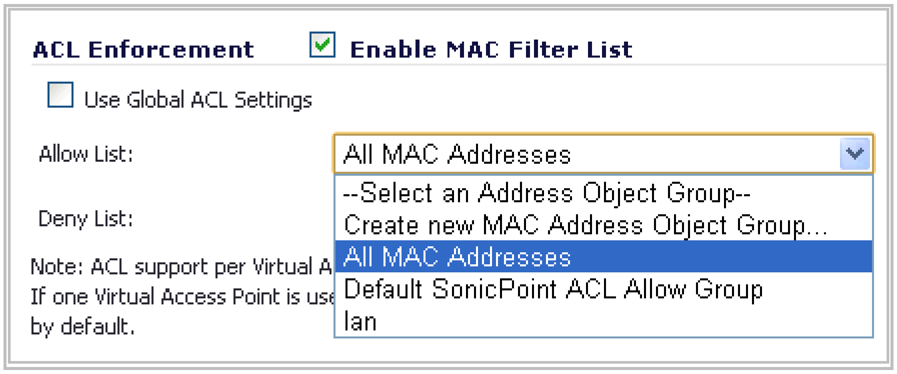
Allow List: All MAC Addresses

Deny List: No MAC Addresses

Note: ACL support per Virtual Access Point is only supported by SonicPointN.
If one Virtual Access Point is used by SonicPoint, global ACL configuration will be applied by default.

You can select the **Use Global ACL Settings** checkbox, or select an Address Group for both the **Allow List** and **Deny List**. You can also create a new, custom MAC Address Object Group.

Allow List options:


--Select an Address Object Group--
Create new MAC Address Object Group...
All MAC Addresses
Default SonicPoint ACL Allow Group
lan

ACL Enforcement ☑ Enable MAC Filter List

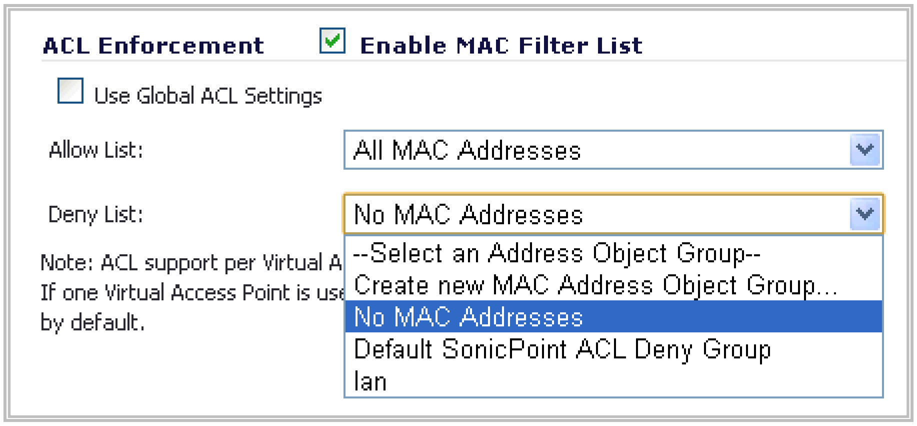
□ Use Global ACL Settings

Allow List: All MAC Addresses

Deny List:

Note: ACL support per Virtual A
If one Virtual Access Point is use
by default.

Deny List options:



ACL Enforcement ☑ **Enable MAC Filter List**

☐ Use Global ACL Settings

Allow List: All MAC Addresses

Deny List: No MAC Addresses

--Select an Address Object Group--
Create new MAC Address Object Group...
No MAC Addresses
Default SonicPoint ACL Deny Group
lan

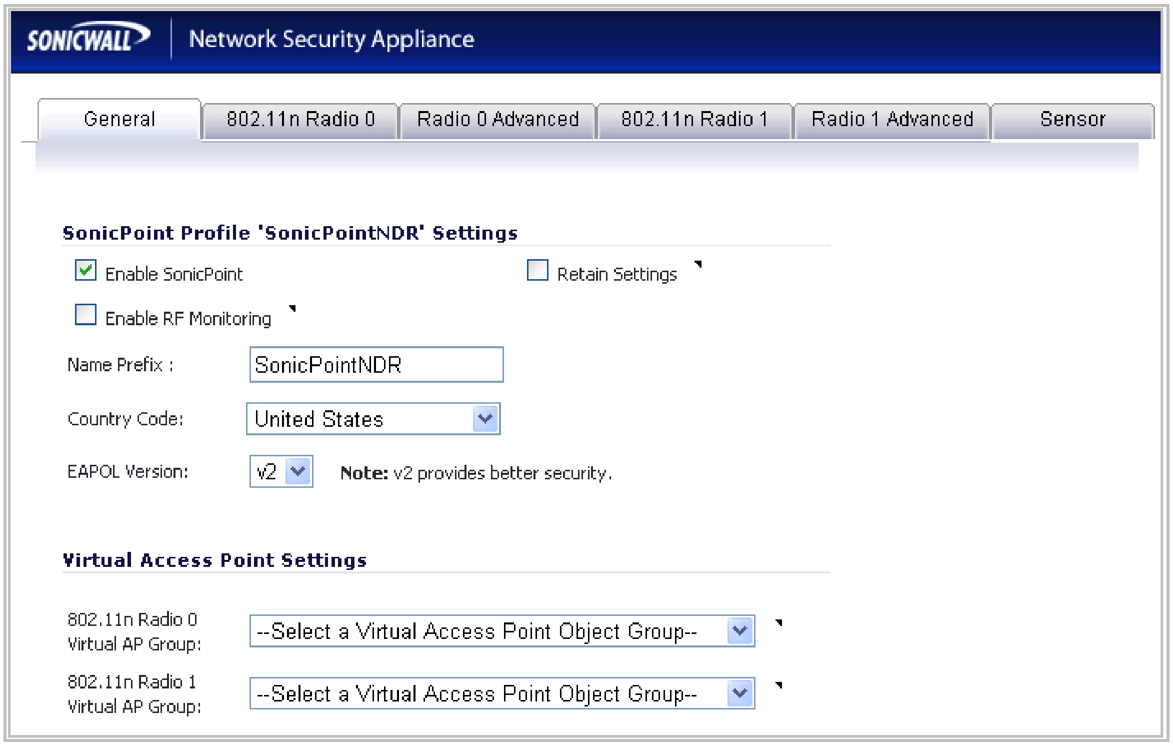
Note: ACL support per Virtual A
If one Virtual Access Point is use
by default.

See the **Network > Address Objects** page to view the ACL Allow and Deny groups.

Virtual Access Point Group Sharing on SonicPoint-N Dual Radios

The same Virtual Access Point / VLAN settings can be applied to dual radios. This allows you to use a unified policy for both radios, and to share a VLAN trunk in the network switch. Supported on the SonicPoint-N DR.

To apply the settings to both radios, navigate to the **SonicPoint > SonicPoints** page and edit a SonicPoint-N DR Profile or a SonicPoint-N DR. In the configuration window on the **General** tab, in the **Virtual Access Point Settings** section, select the same Virtual Access Point Group for both **Radio 0** and **Radio 1**. The drop-down list also provides the option to create the VAP Object Group.



SonicPoint Profile 'SonicPointNDR' Settings

☑ Enable SonicPoint ☐ Retain Settings

☐ Enable RF Monitoring

Name Prefix : SonicPointNDR

Country Code: United States

EAPOL Version: v2 **Note:** v2 provides better security.

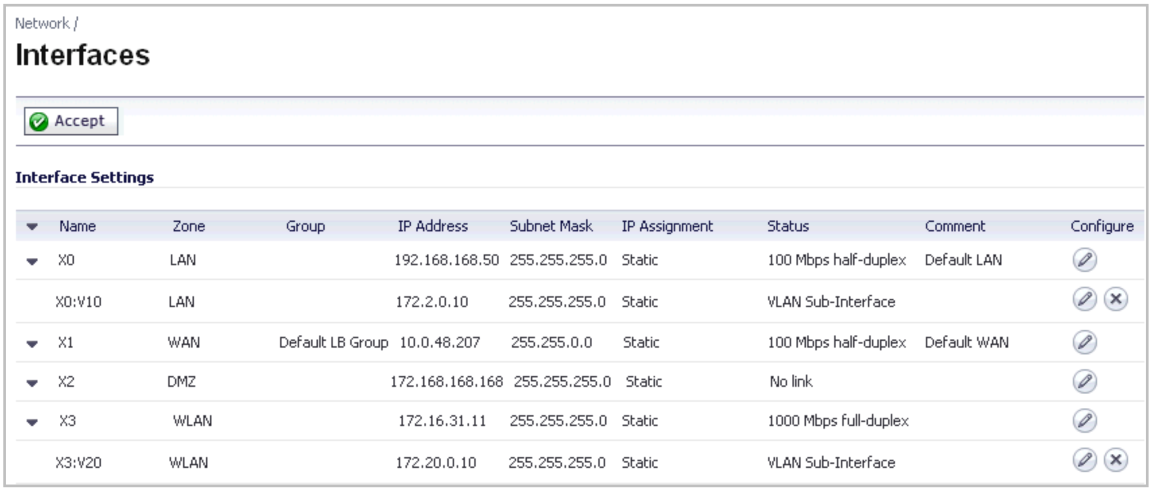
Virtual Access Point Settings

802.11n Radio 0 Virtual AP Group: --Select a Virtual Access Point Object Group--

802.11n Radio 1 Virtual AP Group: --Select a Virtual Access Point Object Group--

Virtual Access Point Layer 2 Bridging

Each Virtual Access Point can be bridged to a corresponding VLAN interface on the LAN zone, providing better flexibility. To configure a Virtual Access Point Layer 2 bridge, navigate to the **Network > Interfaces** page. If you have a Virtual Access Point configured, then you already have a VLAN interface under an interface, such as X3, in the WLAN zone, and your Virtual Access Point is configured to use that VLAN ID. Create a corresponding VLAN interface under the desired “bridge to” interface, such as **X0**.

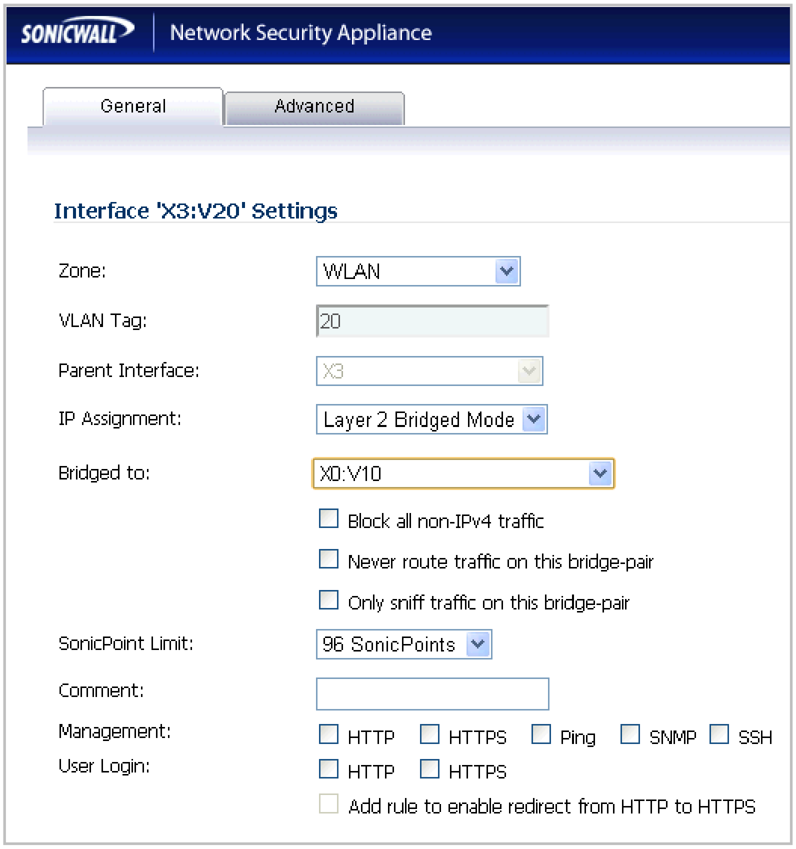


Network /
Interfaces

Interface Settings

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.168.50	255.255.255.0	Static	100 Mbps half-duplex	Default LAN	
X0:V10	LAN		172.2.0.10	255.255.255.0	Static	VLAN Sub-Interface		
X1	WAN	Default LB Group	10.0.48.207	255.255.0.0	Static	100 Mbps half-duplex	Default WAN	
X2	DMZ		172.168.168.168	255.255.255.0	Static	No link		
X3	WLAN		172.16.31.11	255.255.255.0	Static	1000 Mbps full-duplex		
X3:V20	WLAN		172.20.0.10	255.255.255.0	Static	VLAN Sub-Interface		

Next, edit the VLAN interface that is used by the VAP. For **IP Assignment**, select **Layer 2 Bridged Mode**, and for the **Bridged to** field, select the corresponding VLAN that you created under X0. Click **OK**.

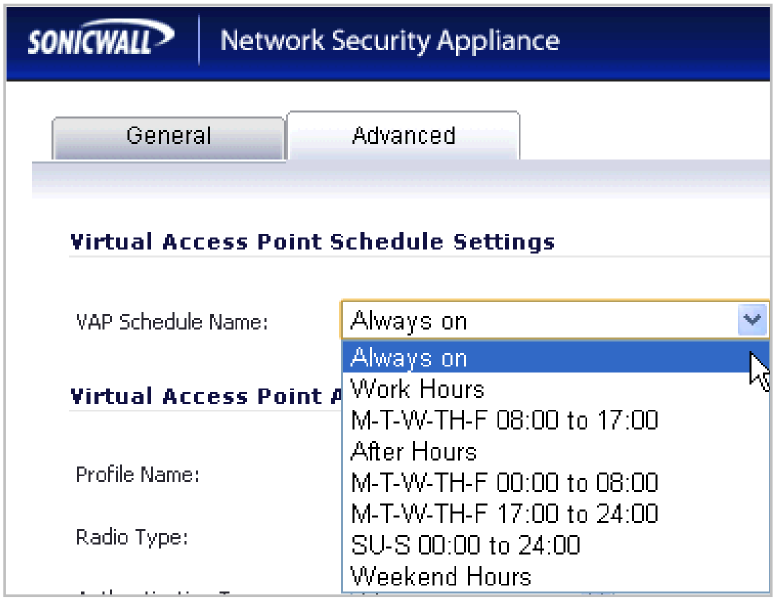


Interface 'X3:V20' Settings

Zone:	WLAN
VLAN Tag:	20
Parent Interface:	X3
IP Assignment:	Layer 2 Bridged Mode
Bridged to:	X0:V10
	□ Block all non-IPv4 traffic
	□ Never route traffic on this bridge-pair
	□ Only sniff traffic on this bridge-pair
SonicPoint Limit:	96 SonicPoints
Comment:	
Management:	□ HTTP □ HTTPS □ Ping □ SNMP □ SSH
User Login:	□ HTTP □ HTTPS
	□ Add rule to enable redirect from HTTP to HTTPS

Virtual Access Point Schedule Support

Each Virtual Access Point schedule can be individually enabled or disabled, for ease of use. To select a VAP schedule, navigate to the **SonicPoint > Virtual Access Point** page. Add or edit a Virtual Access Point. In the configuration window, click the **Advanced** tab. Select the desired schedule from the **VAP Schedule Name** drop-down list.


SONICWALL
Network Security Appliance
General
Advanced
Always on
Work Hours
M-T-W-TH-F 08:00 to 17:00
After Hours
M-T-W-TH-F 00:00 to 08:00
M-T-W-TH-F 17:00 to 24:00
SU-S 00:00 to 24:00
Weekend Hours

Virtual Access Point Schedule Settings

VAP Schedule Name: Always on

Virtual Access Point A

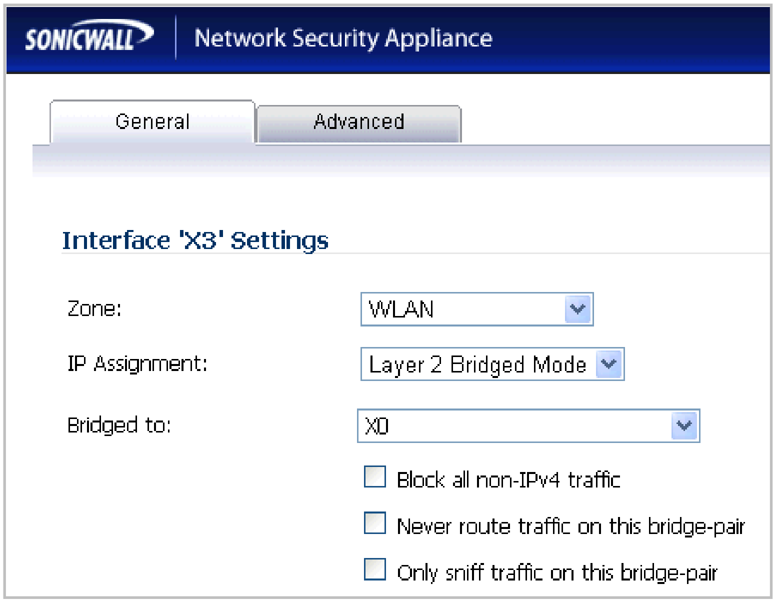
Profile Name:

Radio Type:

Wireless Client Bridge Support

A wireless bridge is supported in WLAN Layer 2 Bridge Mode to provide more flexibility. This feature allows you to bridge wired traffic wirelessly to another LAN.

To configure the bridge, edit the WLAN interface in **Network > Interfaces**. Set the **IP Assignment** field to **Layer 2 Bridged Mode**, and set the **Bridged to** interface to a LAN interface, such as **X0**.



Interface 'X3' Settings

Zone: WLAN

IP Assignment: Layer 2 Bridged Mode

Bridged to: X0

□ Block all non-IPv4 traffic

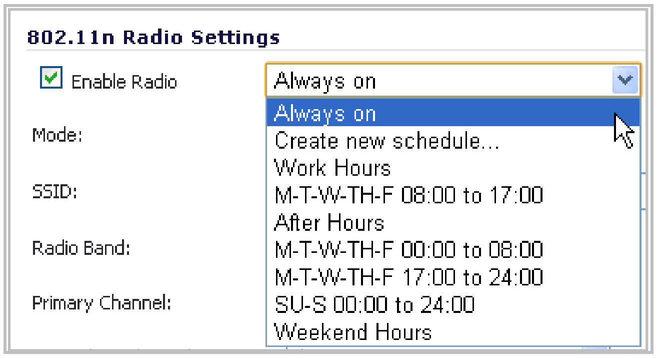
□ Never route traffic on this bridge-pair

□ Only sniff traffic on this bridge-pair

Wireless Radio Built-in Scan Schedule

The internal built-in radio on Dell SonicWALL TZ and NSA Wireless appliances can now be scheduled to perform Intrusion Detection/Prevention scanning with granular scheduling options to cover up to 24 hours a day, 7 days a week. The same scheduling options already exist on the **802.11n Radio** tab (or comparable tab) when editing SonicPoint profiles for all SonicPoint models.

The scheduling options are shown in the image below:



802.11n Radio Settings

☑ Enable Radio: Always on

Mode:

SSID:

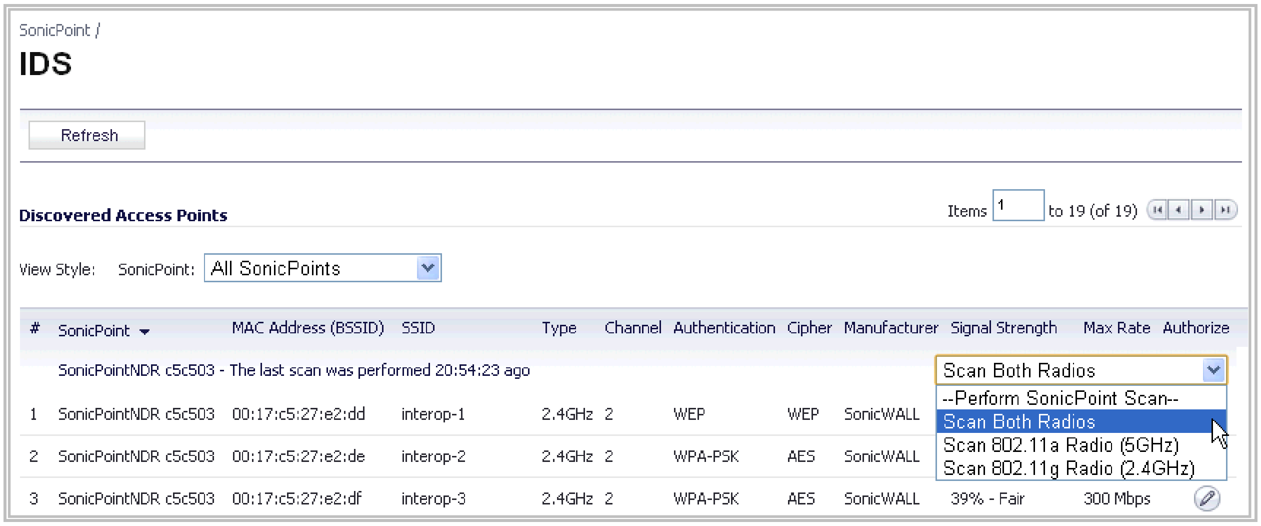
Radio Band:

Primary Channel:

Wireless Rogue Device Detection and Prevention

The SonicPoint-N can be configured in dedicated sensor mode to focus on rogue device detection and prevention, either passively or proactively on both the 2.4 GHz and 5 GHz bands. Both bands can be scanned even if only one is in use. The rogue device can be analyzed to report whether it is connected to the network and if it is blocked by a wired or wireless mechanism.

To scan rogue devices, navigate to the **SonicPoint > IDS** page. Select the type of scan to perform from the **Perform SonicPoint Scan** drop-down list.



SonicPoint /

IDS

Discovered Access Points

Items 1 to 19 (of 19)

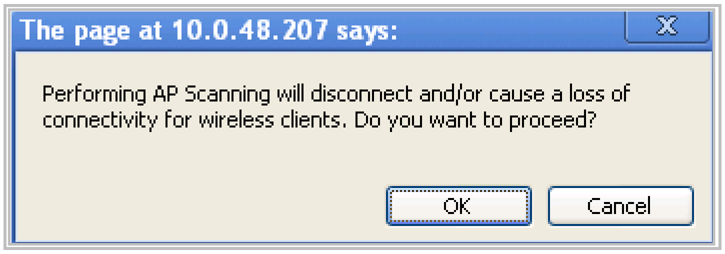
View Style: SonicPoint: All SonicPoints

SonicPointNDR c5c503 - The last scan was performed 20:54:23 ago — Scan Both Radios

#	SonicPoint	MAC Address (BSSID)	SSID	Type	Channel	Authentication	Cipher	Manufacturer	Signal Strength	Max Rate	Authorize
1	SonicPointNDR c5c503	00:17:c5:27:e2:dd	interop-1	2.4GHz	2	WEP	WEP	SonicWALL			
2	SonicPointNDR c5c503	00:17:c5:27:e2:de	interop-2	2.4GHz	2	WPA-PSK	AES	SonicWALL			
3	SonicPointNDR c5c503	00:17:c5:27:e2:df	interop-3	2.4GHz	2	WPA-PSK	AES	SonicWALL	39% - Fair	300 Mbps	✎

--Perform SonicPoint Scan--
Scan Both Radios
Scan 802.11a Radio (5GHz)
Scan 802.11g Radio (2.4GHz)

A pop-up message will warn you that performing the scan will cause all current wireless clients to be disconnected. Click **OK** to proceed with the scan.



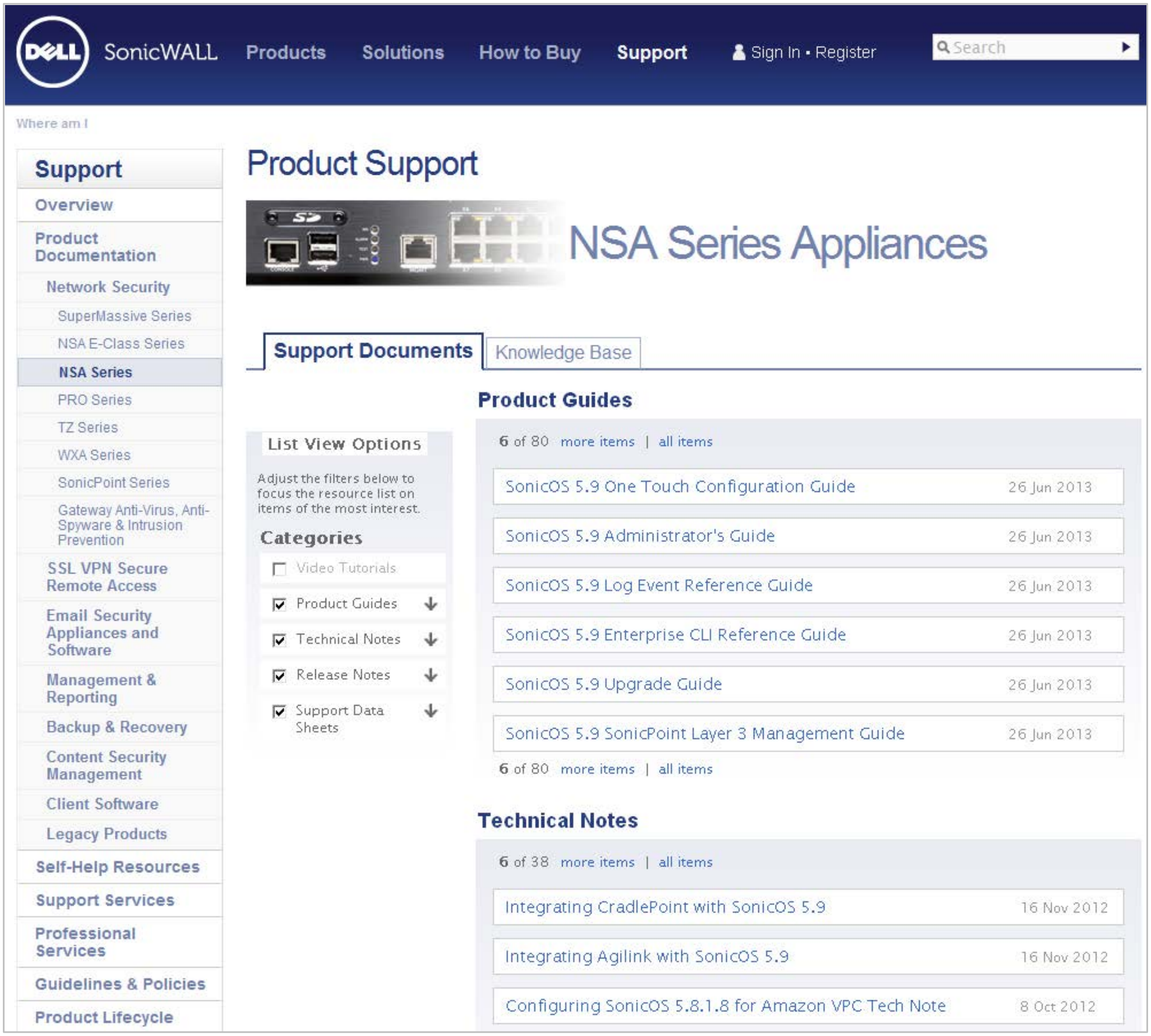
The page at 10.0.48.207 says:

Performing AP Scanning will disconnect and/or cause a loss of connectivity for wireless clients. Do you want to proceed?

Related Technical Documentation

Dell SonicWALL user guides and reference documentation is available at the Dell SonicWALL Technical Documentation Online Library: http://www.sonicwall.com/us/Support.html

For basic and advanced deployment examples, refer to SonicOS Guides and SonicOS TechNotes available on the website.



Product Support

NSA Series Appliances

List View Options

Adjust the filters below to focus the resource list on items of the most interest.

Categories

- □ Video Tutorials
- ☑ Product Guides
- ☑ Technical Notes
- ☑ Release Notes
- ☑ Support Data Sheets

Product Guides

6 of 80 more items | all items

SonicOS 5.9 One Touch Configuration Guide	26 Jun 2013
SonicOS 5.9 Administrator's Guide	26 Jun 2013
SonicOS 5.9 Log Event Reference Guide	26 Jun 2013
SonicOS 5.9 Enterprise CLI Reference Guide	26 Jun 2013
SonicOS 5.9 Upgrade Guide	26 Jun 2013
SonicOS 5.9 SonicPoint Layer 3 Management Guide	26 Jun 2013

6 of 80 more items | all items

Technical Notes

6 of 38 more items | all items

Integrating CradlePoint with SonicOS 5.9	16 Nov 2012
Integrating Agilink with SonicOS 5.9	16 Nov 2012
Configuring SonicOS 5.8.1.8 for Amazon VPC Tech Note	8 Oct 2012

Last updated: 7/8/2013