

# Release Notes

## Contents

---

<i>Release Purpose</i> .....	1
<i>Platform Compatibility</i> .....	1
<i>Upgrading Information</i> .....	1
<i>Browser Support</i> .....	1
<i>Known Issues</i> .....	2
<i>Supported Features by Appliance Series</i> .....	6
<i>Key Features in SonicOS 5.9</i> .....	9
<i>Related Technical Documentation</i> .....	71

## 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 3500
- NSA 4500
- NSA 5000

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](http://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.

# Release Notes

## Known Issues

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

3G/4G.....	2
Application Control.....	2
DPI-SSL.....	2
High Availability.....	3
IPv6.....	3
Log.....	3
Networking.....	3
Security Services.....	4
SSL VPN.....	4
System.....	4
User Interface.....	4
Users.....	5
VoIP.....	5
VPN.....	5

### 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. <b>Workaround:</b> The appliance should always be powered off when inserting or removing a USB device. Hot plug and play is not supported.	130973

### 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. <b>Workaround:</b> 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

# Release Notes

## 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

# Release Notes

## 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

# Release Notes

## 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." <b>Workaround:</b> 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

# Release Notes

## 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	✓	✓ <sup>1</sup>	✗	✗	✗	✗	✗	✗
AppFlow Reports	✓	✓	✓	✓	✗	✗	✗	✗
App Rules Enhancement	✓	✓	✓	✓	✓	✗	✓	✗
ArcSight Syslog Format Support	✓	✓	✓	✓	✓	✗	✓	✗
Bandwidth Management Enhancement	✓	✓	✓	✓	✓	✓	✓	✓
BGP Advanced Routing	✓	✓ <sup>2</sup>	✓ <sup>3</sup>	✗	✗	✗	✗	✗
CLI Enhancements <sup>4</sup>	✓	✓	✓	✓	✓	✓	✓	✓
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	✓	✓	✓	✓	✓	✓	✓	✓
One-Touch Configuration Overrides	✓	✓	✓	✓	✓	✗	✓	✗
OpenSSH Vulnerability Security Enhancements	✓	✓	✓	✓	✓	✓	✓	✓
Path MTU Discovery	✓	✓	✓	✓	✓	✓	✓	✓

<sup>1</sup> Not supported on NSA 240 or NSA 220 series.

<sup>2</sup> Not supported on NSA 240. NSA 250M series and NSA 220 series require a license for BGP.

<sup>3</sup> Requires License

<sup>4</sup> Limited CLI command set is supported on NSA 240 and all TZ models

# Release Notes

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
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	✓	✓ <sup>5</sup>	✗	✗	✗	✗	✗	✗
WWAN 4G support	✓	✓	✓	✓	✓	✓	✓	✗
XD Lookup for Access Rules	✓	✓	✓	✓	✓	✓	✓	✓
YouTube for Schools Support	✓	✓	✓	✓	✓	✓	✓	✓

<sup>5</sup> Supported only on NSA 3500 and higher models

# Release Notes

## 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 <sup>6</sup>	✗	✓	✓	✓	✓	✓	✓	✓
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	✓	✓ <sup>7</sup>	✓	✗	✗	✗	✗	✗
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 <sup>8</sup>	✗	✓	✓	✓	✓	✓	✓	✓
Wireless PCI Rogue detect/prevention	✓	✓	✓	✓	✓	✓	✓	✓
Wireless Radio Built-in Scan Schedule <sup>9</sup>	✗	✓	✓	✓	✓	✓	✓	✓

<sup>6</sup> Only supported on platforms with internal wireless radio

<sup>7</sup> Not supported on NSA 240

<sup>8</sup> Only supported on platforms with internal wireless radio

<sup>9</sup> Only supported on platforms with internal wireless radio



# Release Notes

## Key Features in SonicOS 5.9

---

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

<i>AppFlow Report</i> .....	10
<i>App Rules Enhancements: Excluded and HTTP URL Match Objects</i> .....	11
<i>ArcSight Syslog Format Support</i> .....	12
<i>Bandwidth Management Enhancement</i> .....	14
<i>BGP Advanced Routing</i> .....	17
<i>CLI Enhancements</i> .....	17
<i>Common Access Card Support</i> .....	18
<i>IKEv2 Configuration Payload</i> .....	18
<i>IPv6</i> .....	20
<i>LDAP User Group Mirroring</i> .....	26
<i>LDAP Group Membership by Organizational Unit</i> .....	26
<i>Logging Enhancements</i> .....	27
<i>MOBIKE – IKEv2 Mobility and Multihoming Protocol</i> .....	29
<i>Network Device Protection Profile (NDPP)</i> .....	30
<i>NetExtender WAN Acceleration Client (WXAC) Integration</i> .....	31
<i>One-Touch Configuration Overrides</i> .....	31
<i>OpenSSH Vulnerability Security Enhancements</i> .....	31
<i>Path MTU Discovery</i> .....	32
<i>Proxied Users Identification and Login</i> .....	33
<i>Reassembly-Free Regular Expressions for DPI Engine</i> .....	34
<i>SHA-2 in IPsec</i> .....	35
<i>SNMPv3</i> .....	36
<i>TSR Enhancements</i> .....	37
<i>UDP and ICMP Flood Protection</i> .....	37
<i>Wire Mode 2.0</i> .....	38
<i>WWAN 4G support</i> .....	39
<i>XD Lookup for Access Rules</i> .....	39
<i>YouTube for Schools Content Filtering Support</i> .....	41
<i>SonicPoint and Wireless Enhancements</i> .....	45

# Release Notes

## 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

Applications Viruses Intrusions Spyware Location Botnets URL Rating

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

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.

# Release Notes

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

The screenshot shows the SonicOS configuration interface for Flow Reporting. On the left is a navigation menu with options like VoIP, Anti-Spam, VPN, SSL VPN, Virtual Assist, Users, High Availability, Security Services, WAN Acceleration, Log, View, Categories, Syslog, Automation, and Flow Reporting (highlighted). The main area is titled 'Settings' and contains the following options:

- Enable flow reporting to internal collector [\*]
- Enable Real-Time data collection
- Enable Real-Time data collection for:
- Enable AppFlow Report

Below this is the 'Visualization Settings' section:

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

At the bottom is the 'AppFlow Server Settings' section, which includes a green 'Status' indicator and two options:

- 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 Object 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

# Release Notes

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

The screenshot shows the 'App Control Policy Settings' interface. Key fields include: Policy Name: Block URI allow corp video; Policy Type: HTTP Client; Address: Any; Service: Any; Exclusion Address: None; Match Object: HTTP URI Content - Forbidden File Type; Excluded Match Object: Corporate Video; Action Object: Custom Block Page - Forbidden File; Users/Groups: All; Schedule: Always on; Enable flow reporting: unchecked; Enable Logging: checked; Log individual object content: unchecked; Log Redundancy Filter (seconds): Use Global Settings (0); Connection Side: Client Side; Direction: Basic (selected).

**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 format**.

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

# Release Notes

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

### ArcSight CEF Fields Settings

<b>General</b>			
<input checked="" type="checkbox"/> Host	<input checked="" type="checkbox"/> Event ID	<input checked="" type="checkbox"/> Category (cat)	<input checked="" type="checkbox"/> Message (msg)
<b>Interface</b>			
<input checked="" type="checkbox"/> Src Interface (deviceInboundInterface)	<input checked="" type="checkbox"/> Src Mac Addr (smac)	<input checked="" type="checkbox"/> Dst Interface (deviceOutboundInterface)	<input checked="" type="checkbox"/> Dst Mac Addr (dmac)
<b>Protocol</b>			
<input checked="" type="checkbox"/> Src IP (src)	<input checked="" type="checkbox"/> Src NAT IP (cs1Label)	<input checked="" type="checkbox"/> Src Port (spt)	<input checked="" type="checkbox"/> Src NAT Port (snpt)
<input checked="" type="checkbox"/> Dst IP (dst)	<input checked="" type="checkbox"/> Dst NAT IP (cs2Label)	<input checked="" type="checkbox"/> Dst Port (dnpt)	<input checked="" type="checkbox"/> Dst NAT Port (dnpt)
<input checked="" type="checkbox"/> Protocol (proto)	<input checked="" type="checkbox"/> ICMP type (cn1)	<input checked="" type="checkbox"/> ICMP code (cn2)	
<b>Connection</b>			
<input checked="" type="checkbox"/> Bytes Rcvd (in)	<input checked="" type="checkbox"/> Bytes Sent (out)	<input checked="" type="checkbox"/> Pkts Rcvd (cn1Label)	<input checked="" type="checkbox"/> Pkts Sent (cn2Label)
<input checked="" type="checkbox"/> User (susr)	<input checked="" type="checkbox"/> Conn Duration (cn3Label)	<input checked="" type="checkbox"/> Session Type (cs5Label)	<input checked="" type="checkbox"/> Session Time (cs6Label)
<input checked="" type="checkbox"/> Src VPN Policy (cs2)	<input checked="" type="checkbox"/> Dst VPN Polisy (cs3)	<input checked="" type="checkbox"/> Src Zone (cs3Label)	<input checked="" type="checkbox"/> Dst Zone (cs4Label)
<input checked="" type="checkbox"/> Client Policy (cs1)	<input checked="" type="checkbox"/> Interface stats (cs4)	<input checked="" type="checkbox"/> SonicPoint Stats (SWSPstats)	
<b>Application</b>			
<input checked="" type="checkbox"/> HTTP OP (requestMethod)	<input checked="" type="checkbox"/> HTTP result (outcome)	<input checked="" type="checkbox"/> URL (request)	<input checked="" type="checkbox"/> Block Reason (reason)
<input checked="" type="checkbox"/> Application (app)			
<b>Others</b>			
<input checked="" type="checkbox"/> Counter (cnt)	<input checked="" type="checkbox"/> NPCC (cs5)	<input checked="" type="checkbox"/> Note (cs6)	

Select All Clear All Save Cancel

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.

# Release Notes

## ***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.

Firewall Settings /

### BWM

Bandwidth Management Type:  Advanced  Global  None

Priority	Enable	Guaranteed	Maximum\Burst
0 Realtime	<input type="checkbox"/>	0 %	100 %
1 Highest	<input type="checkbox"/>	0 %	100 %
2 High	<input checked="" type="checkbox"/>	30 %	100 %
3 Medium High	<input type="checkbox"/>	0 %	100 %
4 Medium	<input checked="" type="checkbox"/>	50 %	100 %
5 Medium Low	<input type="checkbox"/>	0 %	100 %
6 Low	<input checked="" type="checkbox"/>	20 %	100 %
7 Lowest	<input type="checkbox"/>	0 %	100 %
<b>Total:</b>		<b>100</b>	

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

# Release Notes

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

**SONICWALL** Network Security Appliance

General | **Advanced**

**Advanced Settings**

Link Speed:

Use Default MAC Address:

Override Default MAC Address:

Enable Multicast Support

Enable 802.1p tagging

Interface MTU:

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):

Enable Interface Ingress Bandwidth Limitation

Maximum Interface Ingress Bandwidth (kbps):

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

Firewall / **Bandwidth Objects**

Items 1 to 6 (of 6)

Add... Delete Delete All

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

Add... Delete Delete All

# Release Notes

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

The screenshot shows the SonicWall Network Security Appliance interface. At the top, there is a navigation bar with the SonicWall logo and the text "Network Security Appliance". Below this, there are four tabs: "General", "Advanced", "QoS", and "BWM". The "BWM" tab is selected. The main content area is titled "Bandwidth Management" and contains the following settings:

- 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.

The screenshot shows the SonicWall Network Security Appliance interface. At the top, there is a navigation bar with the SonicWall logo and the text "Network Security Appliance". Below this, there is a section titled "Action Object Settings". The settings are as follows:

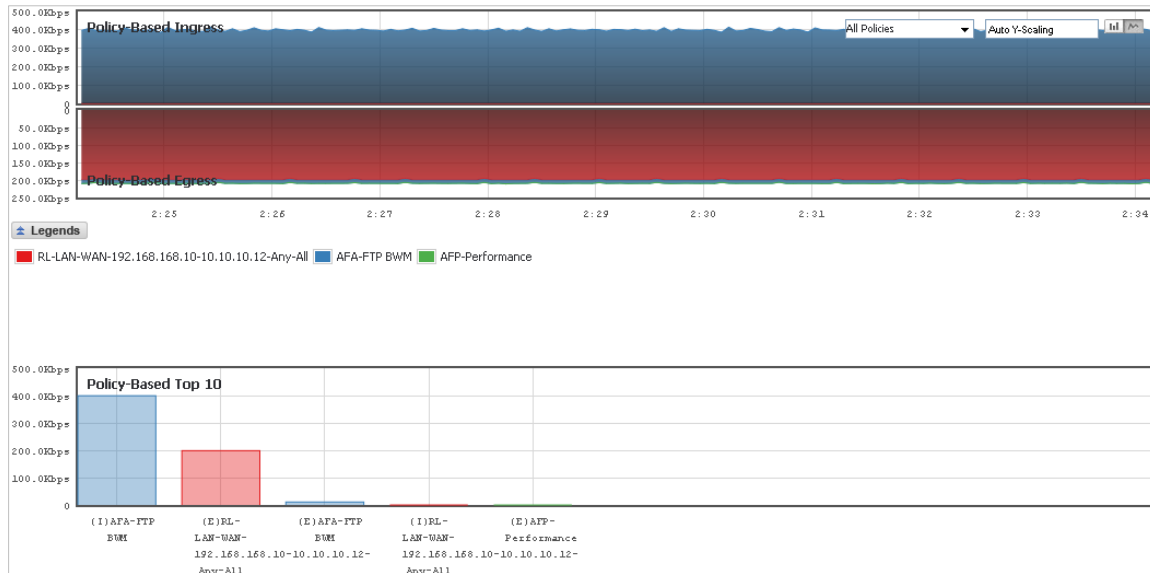
- Action Name: FTP BWM
- Action: Bandwidth Management
- Bandwidth Aggregation Method: Per Policy
- Enable Egress Bandwidth Management  
Bandwidth Object: FTP Egress - 200K
- Enable Ingress Bandwidth Management  
Bandwidth Object: FTP Ingress - 400K
- Enable Tracking Bandwidth Usage

**Note:** BWM Type: Advanced; To change go to [Firewall Settings > BWM](#)



# Release Notes

- 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

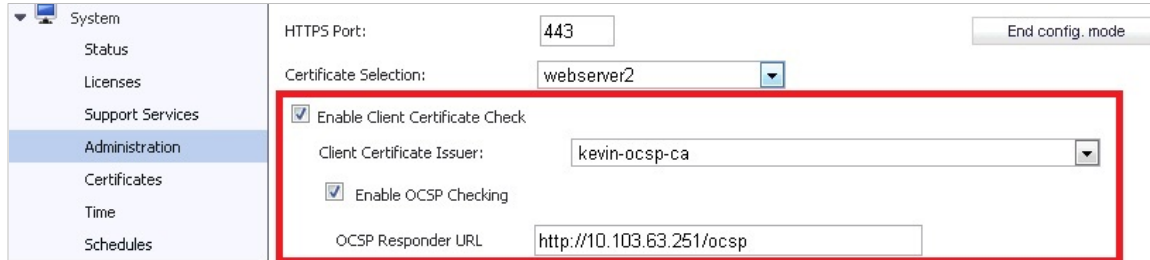
SonicOS 5.9 introduces a new, more-robust, enterprise-level Command Line Interface (E-CLI). The CLI can be accessed via the console and SSH. The new CLI is designed to follow the organization of the SonicOS management GUI. New commands are available in the following categories:

- 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).

# Release Notes

## Common Access Card Support

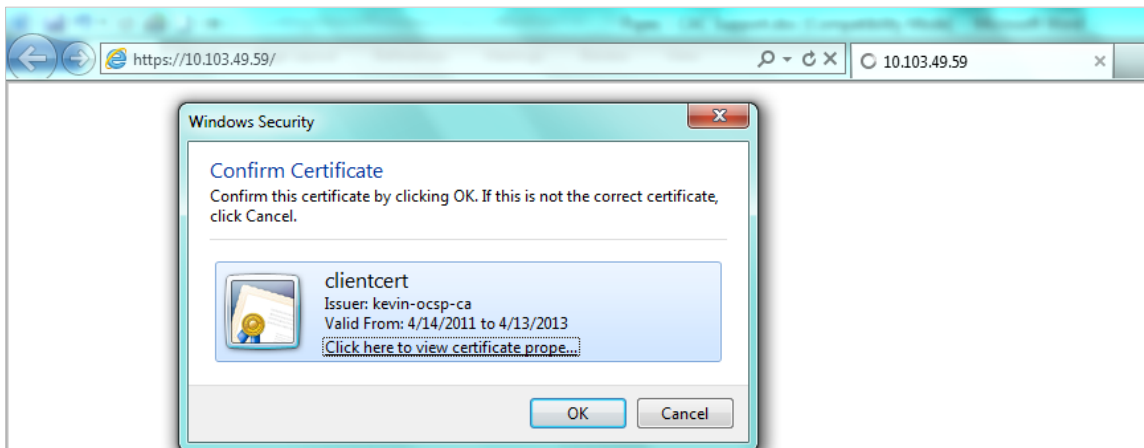
The Common Access Card (CAC) is a smart card issued by the United States Department of Defense (DoD). The CAC enables encrypting and cryptographically signing email, facilitating the use of PKI authentication tools, and establishes an authoritative process for the use of identity credentials. Although 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.



CAC is only supported for HTTPS management. Optionally, an additional Online Certificate Status Protocol (OCSP) 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.



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

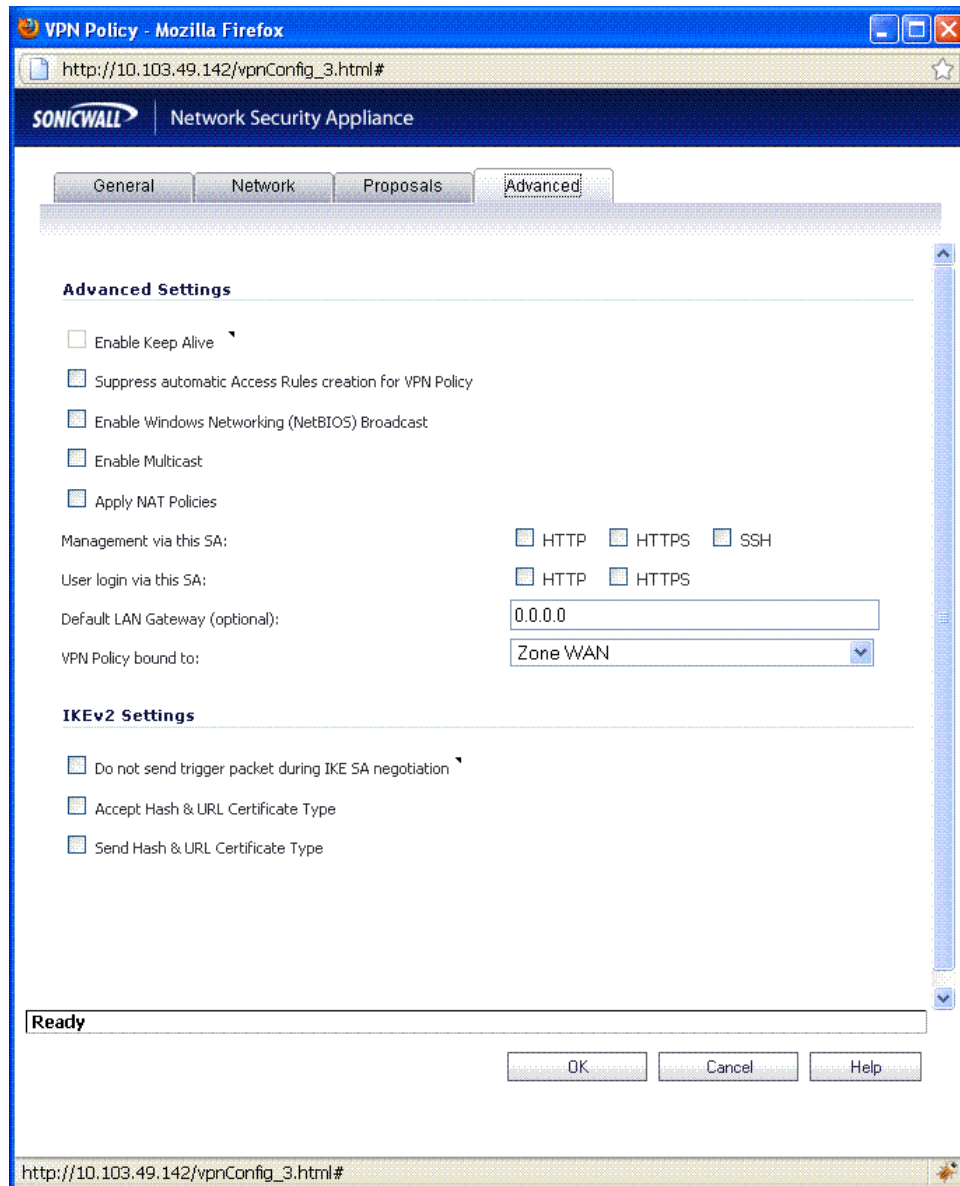
# Release Notes

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.



# Release Notes

## IPv6

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

IPv6 Features Supported	IPv6 Features Not Currently Supported
<ul style="list-style-type: none"> <li>• 6to4 tunnel (allows IPv6 nodes to connect to outside IPv6 services over an IPv4 network)</li> <li>• Access Rules</li> <li>• Address Objects</li> <li>• Anti-Spyware</li> <li>• Application Firewall</li> <li>• Attack prevention:               <ul style="list-style-type: none"> <li>○ Land Attack</li> <li>○ Ping of Death</li> <li>○ Smurf</li> <li>○ SYN Flood</li> </ul> </li> <li>• Connection Cache</li> <li>• Connection Limiting for IPv6 connections</li> <li>• Connection Monitor</li> <li>• Content Filtering Service</li> <li>• DHCP</li> <li>• DNS client</li> <li>• DNS lookup and reverse name lookup</li> <li>• Dynamic Routing (RIPng and OSPFv3)</li> <li>• EPRT</li> <li>• EPSV</li> <li>• FTP</li> <li>• Gateway Anti-Virus</li> <li>• High Availability:               <ul style="list-style-type: none"> <li>○ Connection Cache</li> <li>○ FTP</li> <li>○ IPv6 management IP address</li> <li>○ NDP</li> <li>○ SonicPoint</li> </ul> </li> <li>• HTTP/HTTPS management over IPv6</li> <li>• ICMP</li> <li>• IKEv2</li> <li>• Intrusion Prevention Service</li> <li>• IP Spoof Protection</li> <li>• IPv4 Syslog messages, including messages with IPv6 addresses</li> <li>• Layer 2 Bridge Mode</li> <li>• Logging IPv6 events</li> <li>• Login uniqueness</li> <li>• Multicast Routing with Multicast Listener Discovery</li> <li>• NAT</li> <li>• Neighbor Discovery Protocol</li> <li>• NetExtender connections for users with IPv6 addresses</li> <li>• Packet Capture</li> <li>• Ping</li> <li>• Policy Based Routing</li> <li>• PPPoE</li> <li>• Remote management</li> </ul>	<ul style="list-style-type: none"> <li>• Anti-Spam</li> <li>• Command Line Interface</li> <li>• DHCP over VPN</li> <li>• DHCP Relay</li> <li>• Dynamic Address Objects for IPv6 addresses</li> <li>• Dynamic DNS</li> <li>• FQDN</li> <li>• Global VPN Client (GVC)</li> <li>• GMS</li> <li>• H.323</li> <li>• High Availability:               <ul style="list-style-type: none"> <li>○ Multicast</li> <li>○ Oracle SQL/Net</li> <li>○ RTSP</li> <li>○ VoIP</li> </ul> </li> <li>• IKEv1</li> <li>• IPv6 Syslog messages</li> <li>• L2TP</li> <li>• LDAP</li> <li>• MAC-IP Anti-Spoof</li> <li>• NAT between IPv6 and IPv4 addresses</li> <li>• NAT High Availability probing</li> <li>• NAT load balancing</li> <li>• NetBIOS over VPN</li> <li>• NTP</li> <li>• QoS Mapping</li> <li>• RADIUS</li> <li>• RAS Multicast Forwarding</li> <li>• Route-based VPNs</li> <li>• Single Sign On</li> <li>• SIP</li> <li>• SMTP Real-Time Black List (RBL) Filtering</li> <li>• SSH</li> <li>• Transparent Mode</li> <li>• ViewPoint</li> <li>• Virtual Assistant</li> <li>• Web proxy</li> <li>• Wiremode</li> </ul>

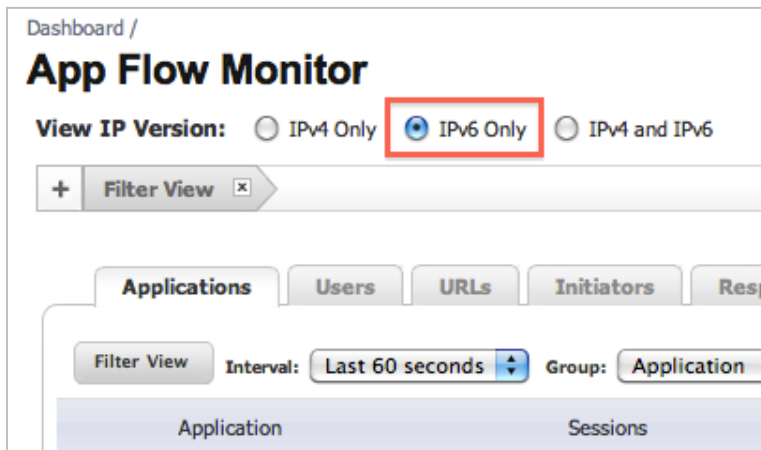
# Release Notes

IPv6 Features Supported	IPv6 Features Not Currently Supported
<ul style="list-style-type: none"><li>• Security services for IPv6 traffic with DPI</li><li>• Site-to-site IPv6 tunnel with IPsec for security</li><li>• SonicPoint IPv6 support</li><li>• SNMP</li><li>• SSL VPN</li><li>• Stateful inspection of IPv6 traffic</li><li>• User status</li><li>• Visualization</li><li>• VLAN interfaces with IPv6 addresses</li><li>• VPN policies</li><li>• Wireless</li></ul>	

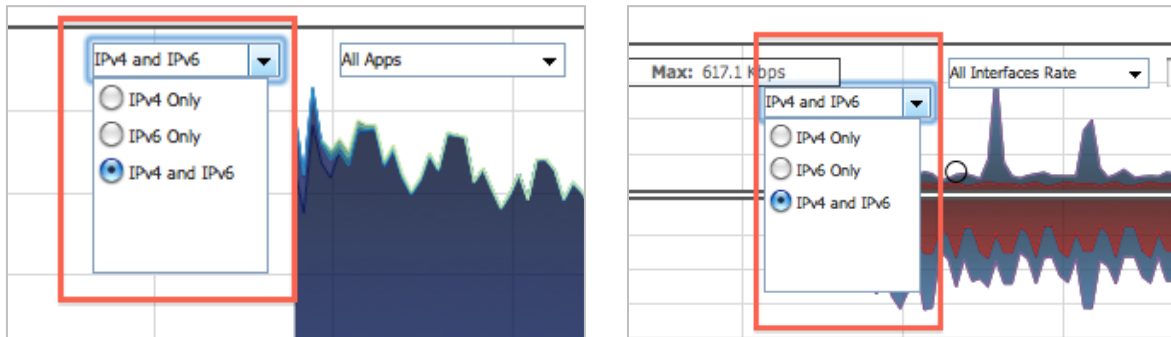
The IPv6 features supported in the SonicOS 5.9 release are described below:

- **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.



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



# Release Notes

- **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**.

General | **Advanced** | Router Advertisement

### 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

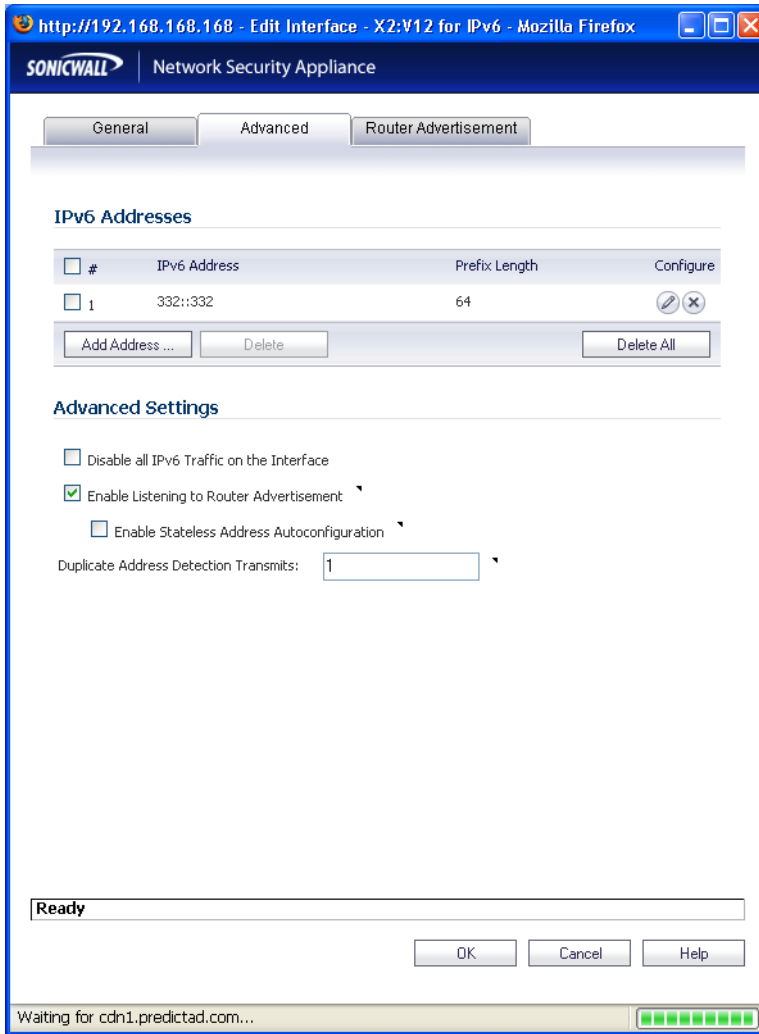
After you click **OK**, the VLAN will be displayed on the **Interface** page.

Interface	Zone	IP Assignment	IPv6 Address	IPv6 Prefix Length	IPv6 Address	IPv6 Prefix Length	IPv6 Address	IPv6 Prefix Length
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.

# Release Notes

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





# Release Notes

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.

The screenshot shows the SonicWall Network Security Appliance web interface. The browser address bar displays "http://192.168.168.168 - Edit Interface - X2:V12 for IPv6 - Mozilla Firefox". The interface has three tabs: "General", "Advanced", and "Router Advertisement", with "Router Advertisement" being the active tab. Below the tabs, the "Router Advertisement Settings" section includes a checked checkbox for "Enable Router Advertisement". Below this are several input fields: "Router Adv Interval Range (seconds)" with values 200 and 600, "Link MTU" with 0, "Reachable Time (seconds)" with 0, "Retrans Timer (seconds)" with 0, "Current Hop Limit" with 64, and "Router Lifetime (seconds)" with 1800. There are also checkboxes for "Managed" and "Other Configuration". The "Prefix List Settings" section shows "Items 1 to 3 (of 3)". Below this is a table with columns: "#", "Prefix", "Valid Lifetime", "Preferred Lifetime", "On-link", "Auto", and "Configure".

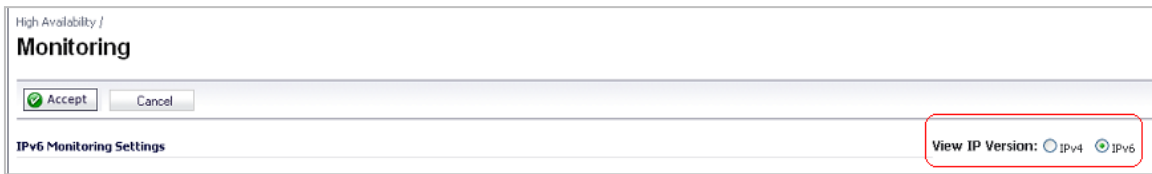
#	Prefix	Valid Lifetime	Preferred Lifetime	On-link	Auto	Configure
<input type="checkbox"/>	1 1233::	3344 minutes	3344 minutes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="edit"/> <input type="button" value="delete"/>
<input type="checkbox"/>	2 2::	43200 minutes	10080 minutes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="edit"/> <input type="button" value="delete"/>
<input type="checkbox"/>	3 889::	4234 minutes	4234 minutes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="edit"/> <input type="button" value="delete"/>

Below the table are buttons for "Add Prefix ...", "Delete", and "Delete All". At the bottom of the interface, there is a "Ready" status bar and "OK", "Cancel", and "Help" buttons. The footer of the browser window shows the URL "http://192.168.168.168/editipv6Interface\_268438530.html#".



# Release Notes

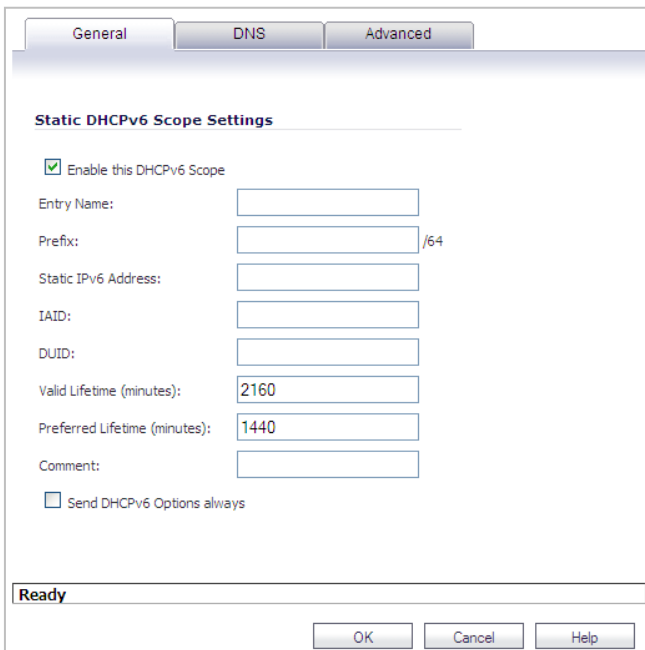
- **IPv6 HA Monitoring Support** – Support for High Availability Monitoring through IPv6 address. A new **View IP Version:** option is added to the **High Availability > Monitoring** page.



The screenshot shows the 'High Availability / Monitoring' configuration page. At the top, there are 'Accept' and 'Cancel' buttons. Below that, the 'IPv6 Monitoring Settings' section is visible, with a 'View IP Version:' label and two radio buttons: 'IPv4' (unselected) and 'IPv6' (selected). The 'IPv6' radio button is highlighted with a red box.

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.



The screenshot shows the 'Static DHCPv6 Scope Settings' configuration page. It has three tabs: 'General', 'DNS', and 'Advanced'. The 'General' tab is active. The page contains the following fields and options:

- Enable this DHCPv6 Scope
- Entry Name:
- Prefix:  /64
- Static IPv6 Address:
- IAID:
- DUID:
- Valid Lifetime (minutes):
- Preferred Lifetime (minutes):
- Comment:
- Send DHCPv6 Options always

At the bottom, there is a 'Ready' status bar and 'OK', 'Cancel', and 'Help' buttons.

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



The screenshot shows the 'Security Policy' configuration page. The 'Authentication Method' dropdown menu is set to 'Manual Key'. The 'Name' field contains 'IPv6 Manual Tunnel' and the 'IPsec Gateway Name or Address' field contains '2002::1'.

# Release Notes

## ***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.

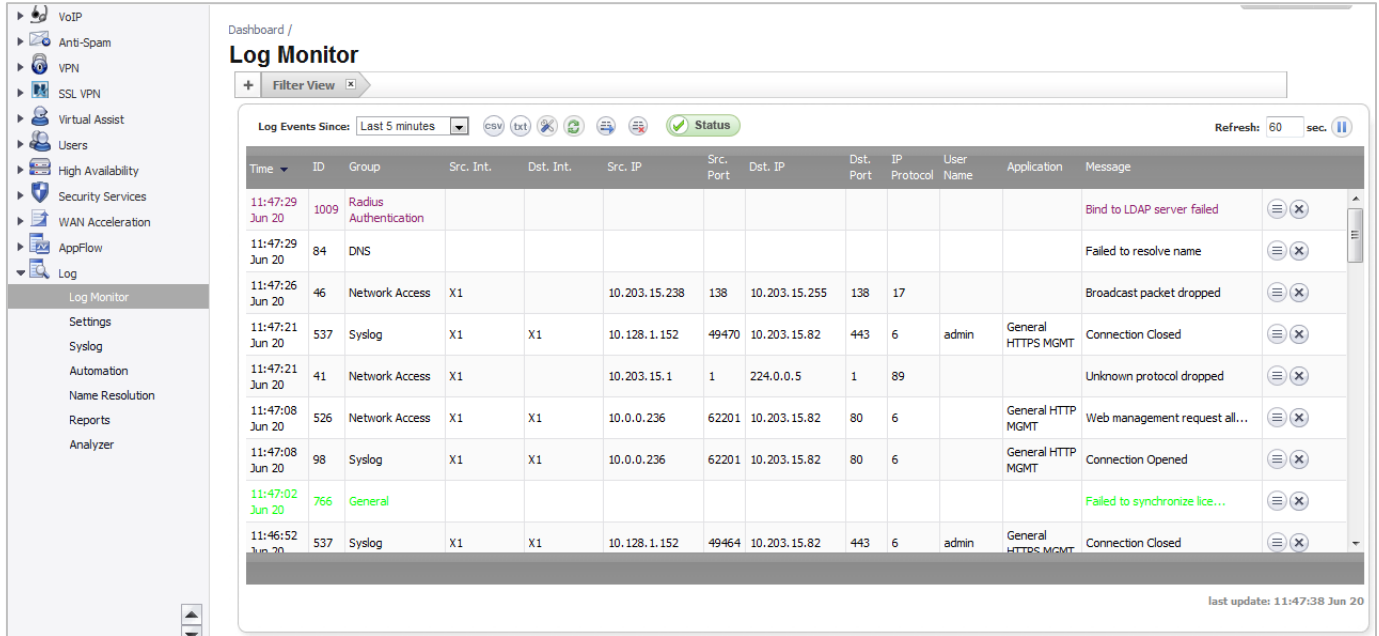
When groups are configured this way:

- 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.

# Release Notes

## 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.



The screenshot shows the SonicOS Log Monitor interface. On the left is a navigation menu with categories like VoIP, Anti-Spam, VPN, SSL VPN, Virtual Assist, Users, High Availability, Security Services, WAN Acceleration, AppFlow, and Log. The Log Monitor page displays a table of log events with columns for Time, ID, Group, Src. Int., Dst. Int., Src. IP, Src. Port, Dst. IP, Dst. Port, IP Protocol, User Name, Application, and Message. The table contains several entries, including RADIUS Authentication failures, DNS resolution failures, network access broadcasts, and connection events. A 'Filter View' button and a 'Status' indicator are visible at the top of the table area.

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

### 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.

# Release Notes

The Log Settings page is shown below:

Category	Color	ID	Priority	Gui	Alert	Syslog	Email	Event Count
System	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	2
Log	<input type="checkbox"/>		Debug	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	61194
Security Services	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	520
Network	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	54786
Users	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	6175
Firewall Settings	<input type="checkbox"/>		Debug	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	1067
VPN	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
High Availability	<input type="checkbox"/>		Debug	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
3G/4G, Modem, and Module	<input type="checkbox"/>		Debug	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
Firewall	<input type="checkbox"/>		Debug	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
Wireless	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0
VoIP	<input checked="" type="checkbox"/>		Debug	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0

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

# Release Notes

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.

Dashboard /  
**Log Monitor**  
+ Filter View x

Log Events Since: Last 5 minutes [csv] [txt] [Status] 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 Jun 20	526	Network Access	X1	X1	10.0.203.93	63215	10.203.15.82	80	6	admin	General HTTP MGMT	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: [ ]

Apply Close

## ***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.

# Release Notes

## Network Device Protection Profile (NDPP)

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

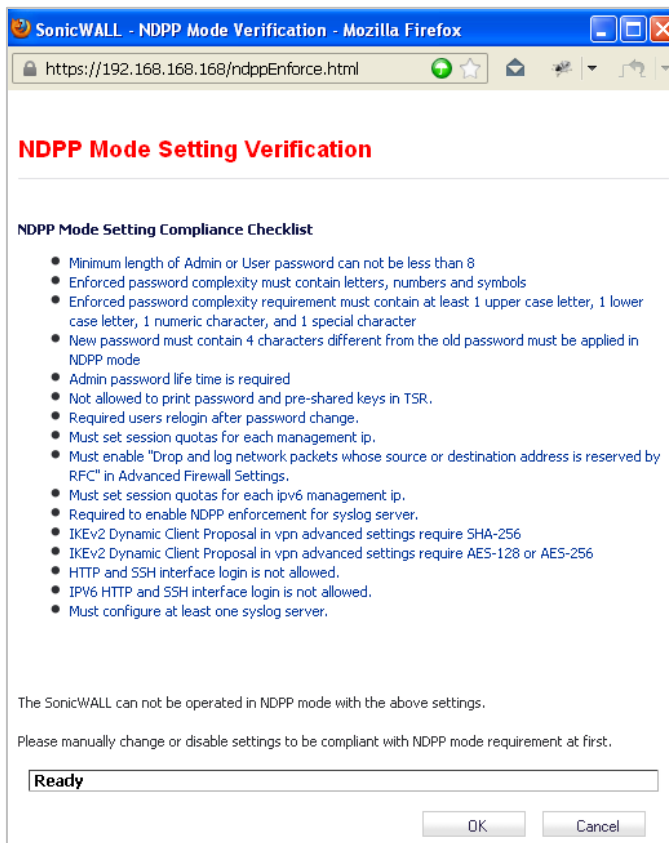


NDPP is a part of Common Criteria certification. The security objectives for a device that claims compliance to a Protection Profile are defined as follows:

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:



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.



# Release Notes

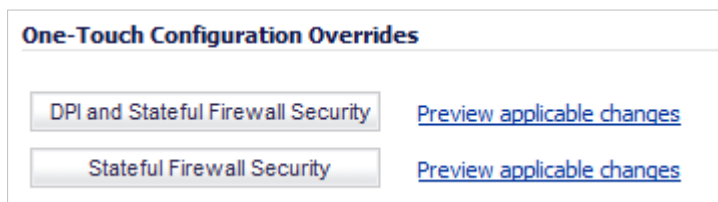
## NetExtender WAN Acceleration Client (WXAC) Integration

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.



## 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.



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.

# Release Notes

## 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.

The screenshot shows the 'System / Diagnostics' page. At the top, there are 'Accept', 'Cancel', and 'Refresh' buttons. Below is the 'Tech Support Report' section with various checkboxes for including sensitive keys, ARP cache, DHCP bindings, IKE info, SonicPointN diagnostics, list of current users, and detail of users. There are also buttons for 'Download Report' and 'Send Diagnostic Reports to Support'. A checkbox for 'Enable periodic secure backup of diagnostic reports to support' is checked, with a 'Time interval (minutes)' field set to '1440'. Another checkbox for 'Include raw flow table data entries when sending diagnostic report' is unchecked. The 'Diagnostic Tools' section has a dropdown menu set to 'PMTU Discovery'. The 'PMTU Discovery' section has a text input field for 'Path MTU Discovery to this host or IP address', a dropdown menu for 'Interface' set to 'ANY', and a 'Go' button.

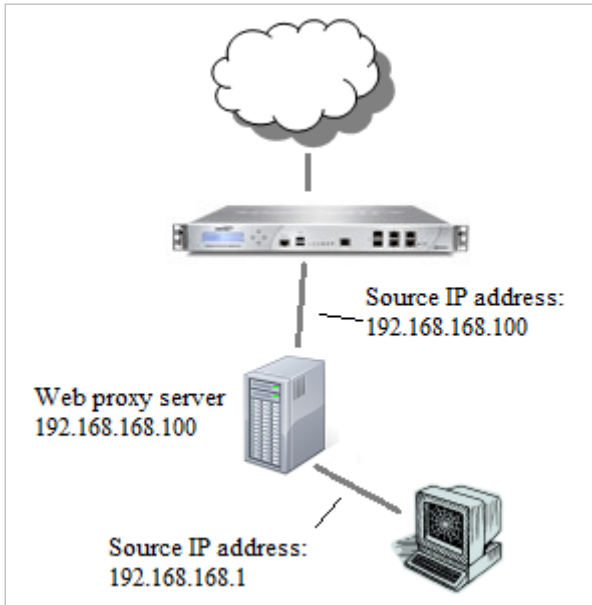
Enter the IP address or host name and click **Go**. When the **Interface** pulldown menu is set to **ANY**, the appliance chooses among all of its interfaces. Optionally, you can select one of the configured WAN interfaces to check the Path MTU for that interface.



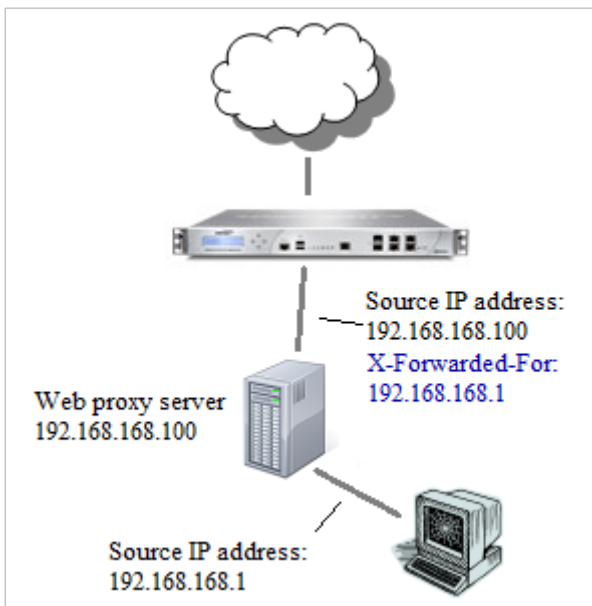
# Release Notes

## 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:



# Release Notes

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:

## 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.

# Release Notes

## 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:	<input type="text"/>
Outgoing SPI:	<input type="text"/>
Protocol:	ESP
Encryption:	3DES
Authentication:	SHA1
	MD5
	SHA1
	SHA256
	AES-XCBC
	None

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: S25; 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: S25; 3DES; HMAC_SHA256_128; DH Group 2; IKEv2 InitSPI: 0x393dde141cc2bb0b; IKEv2 RespSPI: 0x6832fd1f1b12f2ef

# Release Notes

## 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.

# Release Notes

## 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

Accept  Cancel  Refresh

### 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)

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):

### UDP Flood Protection

Enable UDP Flood Protection

UDP Flood Attack Threshold (UDP Packets / Sec):

UDP Flood Attack Blocking Time (Sec):

UDP Flood Attack Protected Destination List:

### ICMP Flood Protection

Enable ICMP Flood Protection

ICMP Flood Attack Threshold (ICMP Packets / Sec):

ICMP Flood Attack Blocking Time (Sec):

ICMP Flood Attack Protected Destination List:

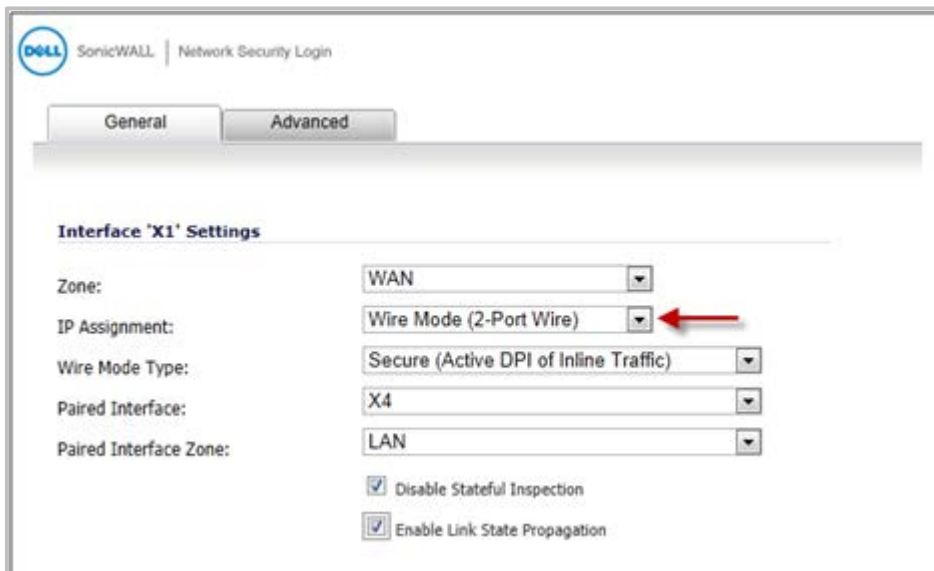
# Release Notes

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.



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.

# Release Notes

## 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 5.9.0.0-580 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 –

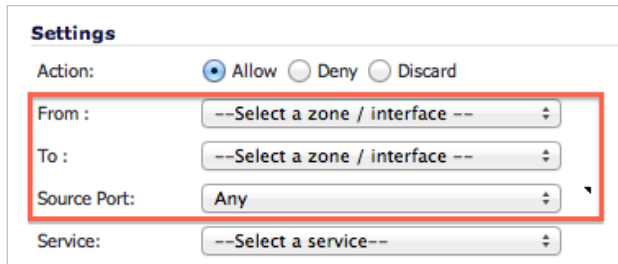
#	Zone	> Zone	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
	LAN	> LAN									 
1	LAN	> LAN	1 	Any	All XD Management IP	ZebTelnet	Allow	All			  
2	LAN	> LAN	2 	Any	All XD Management IP	Telnet	Allow	All			  

### Configure Dialog –

**Settings**  
Action:  Allow  Deny  Discard  
From Zone:   
To Zone:   
Service:   
Source:   
Destination:   
Users Allowed:   
Schedule:   
Comment:   
 Enable Logging  
 Allow Fragmented Packets

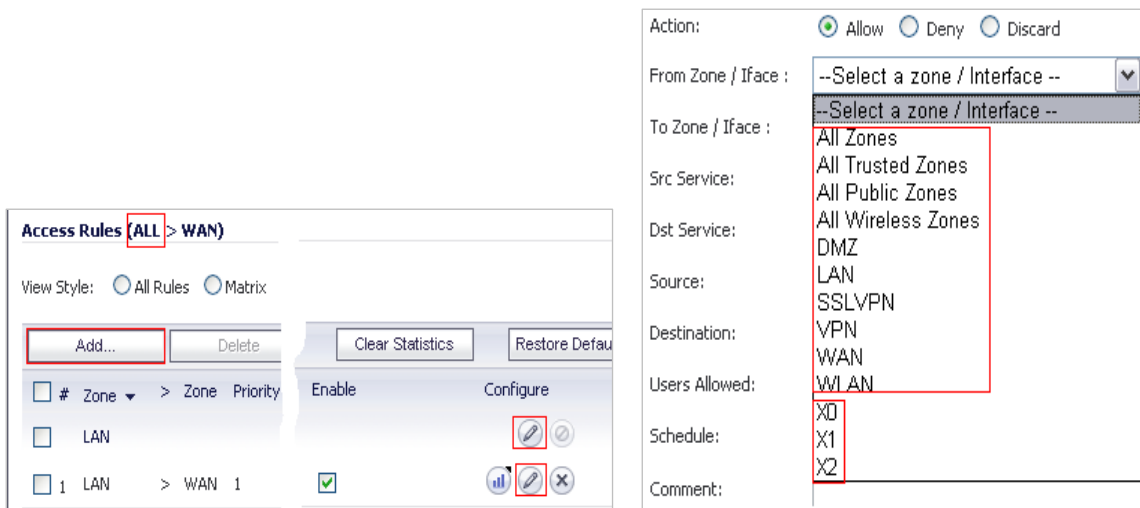
# Release Notes

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

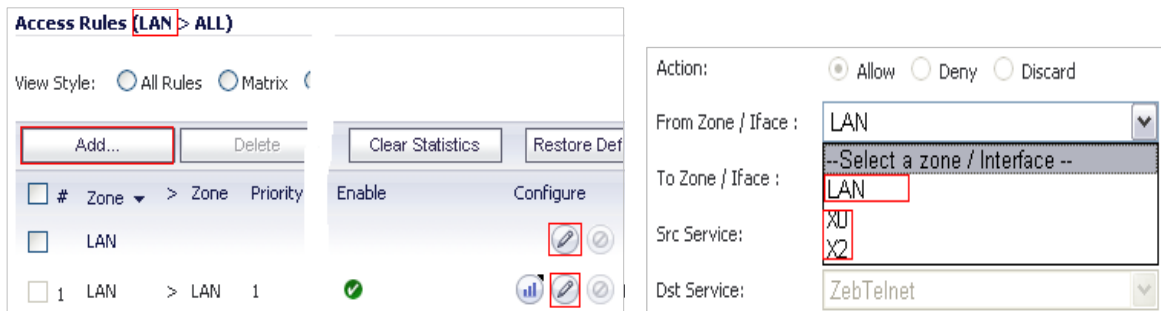


The ability to select interfaces was added to the **From:** and **To:** **Select a zone / interface** lists. The available zones and interfaces that appear in the list, depends on the **View Style:** option.

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



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



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.



# Release Notes

## **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](http://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**.

The screenshot shows the 'Match Object Settings' dialog box. It has the following fields and controls:

- Object Name:** Text input field containing 'CFS Allow YT4S'.
- Match Object Type:** Dropdown menu set to 'CFS Allow/Forbidden List'.
- Match Type:** Dropdown menu set to 'Partial Match'.
- Input Representation:** Radio buttons for 'Alphanumeric' (selected) and 'Hexadecimal'.
- Content:** Text input field containing 'youtube.com'. To its right is an 'Add' button.
- List:** A list box containing 'youtube.com' and 'yting.com'. To its right are 'Update', 'Remove', 'Remove All', and 'Load From File' buttons.
- Status:** A text field at the bottom left containing 'Ready'.
- Buttons:** 'OK', 'Cancel', and 'Help' buttons at the bottom right.

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 "yting.com" and then click **Add**.
6. Click **OK** to create the Match Object.

# Release Notes

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

**App Control Policy Settings**

Policy Name:

Policy Type:

Address:

Exclusion Address:

Match Object:

Action Object:

Users/Groups:  Included:  Excluded:

Schedule:

Enable flow reporting:

Enable Logging:

Log using CFS message format:

Log Redundancy Filter (seconds):  Use Global Settings

Zone:

CFS Allow/Excluded List:

CFS Forbidden/Included List:

Enable Safe Search Enforcement:

Enable YouTube for Schools:

School ID:

**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](http://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).

# Release Notes

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](http://www.youtube.com/schools).

The screenshot shows the 'Settings' tab of the Content Filter configuration. Under 'Custom List Settings', there are three dropdown menus for 'Source of Allowed Domains', 'Source of Forbidden Domains', and 'Source of Keyword', all set to 'Global'. Below this is the 'Safe Search Enforcement Settings' section with an unchecked checkbox for 'Enable Safe Search Enforcement'. The 'YouTube for Schools' section is highlighted with a red box and contains a checked checkbox for 'Enable YouTube for Schools' and a text field for 'School ID' containing the value 'Lj3Q2GVaHbr3k\_yiY2lhkQ'. At the bottom, the 'Filter Forbidden URLs by time of day' section has a dropdown menu set to '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 "yting.com" into the **Domain Name** field and click **OK**.

The screenshot shows the 'Custom List' tab of the Content Filter configuration. It features three main sections: 'Allowed Domains', 'Forbidden Domains', and 'Keyword Blocking'. The 'Allowed Domains' section contains a list with 'youtube.com' and 'yting.com', and buttons for 'Add...', 'Edit...', 'Delete', and 'Delete All'. The 'Forbidden Domains' section is currently empty and has the same set of buttons. The 'Keyword Blocking' section is also empty and has the same set of buttons. At the top, there are tabs for 'CFS', 'Policy', 'Custom List', and 'Consent'.

# Release Notes

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 yting.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](http://www.youtube.com) and s.yting.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](http://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.

# Release Notes

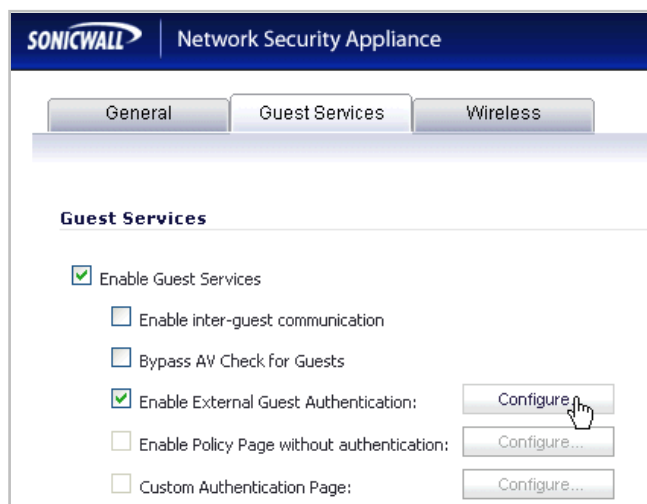
## SonicPoint and Wireless Enhancements

The following SonicPoint Enhancements are included in SonicOS 5.9:

<i>External Guest Service FQDN Support</i> .....	45
<i>Guest Administrator Support</i> .....	47
<i>Internal Radio IDS scan scheduling</i> .....	49
<i>SonicPoint 802.11e (WMM) QoS</i> .....	50
<i>SonicPoint Auto Provisioning</i> .....	56
<i>SonicPoint Customized Configuration Retaining</i> .....	57
<i>SonicPoint Diagnostics Enhancement</i> .....	58
<i>SonicPoint Dynamic Frequency Selection (DFS) Support</i> .....	58
<i>SonicPoint FairNet Support</i> .....	59
<i>SonicPoint Layer 3 Management Phase I</i> .....	59
<i>SonicPoint RADIUS Server Failover</i> .....	62
<i>SonicPoint WPA TKIP Countermeasures and MIC Failure Flooding Detection and Protection</i> .....	63
<i>Traffic Quota Based Guest Server Policy</i> .....	65
<i>Virtual Access Point ACL Support</i> .....	66
<i>Virtual Access Point Group Sharing on SonicPoint-N Dual Radios</i> .....	67
<i>Virtual Access Point Layer 2 Bridging</i> .....	68
<i>Virtual Access Point Schedule Support</i> .....	69
<i>Wireless Client Bridge Support</i> .....	69
<i>Wireless Radio Built-in Scan Schedule</i> .....	70
<i>Wireless Rogue Device Detection and Prevention</i> .....	70

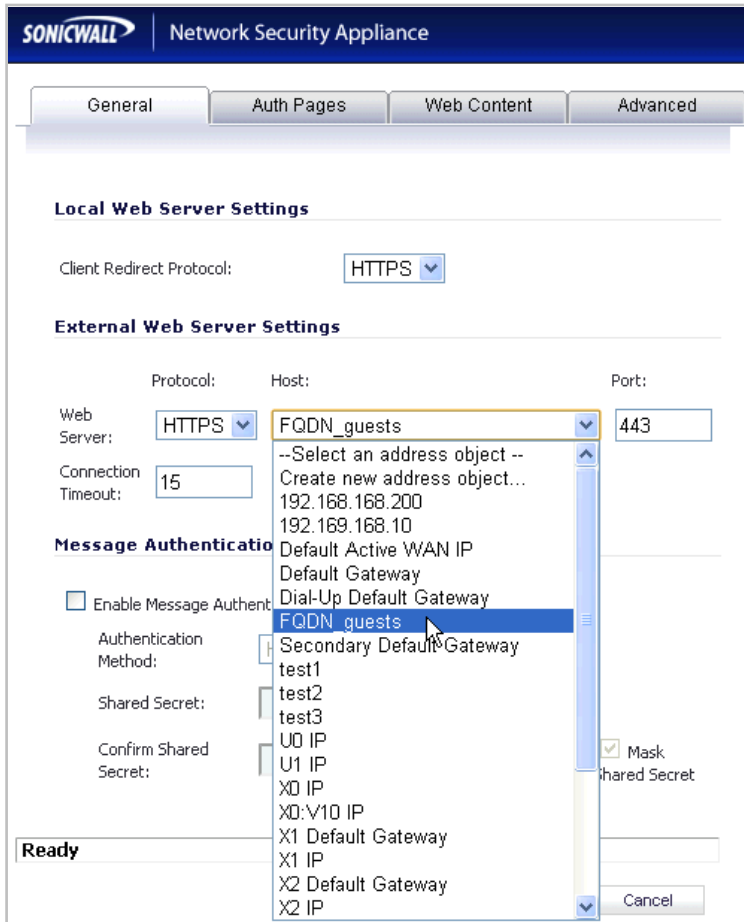
### External Guest Service FQDN Support

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.



# Release Notes

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



# Release Notes

## 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**.

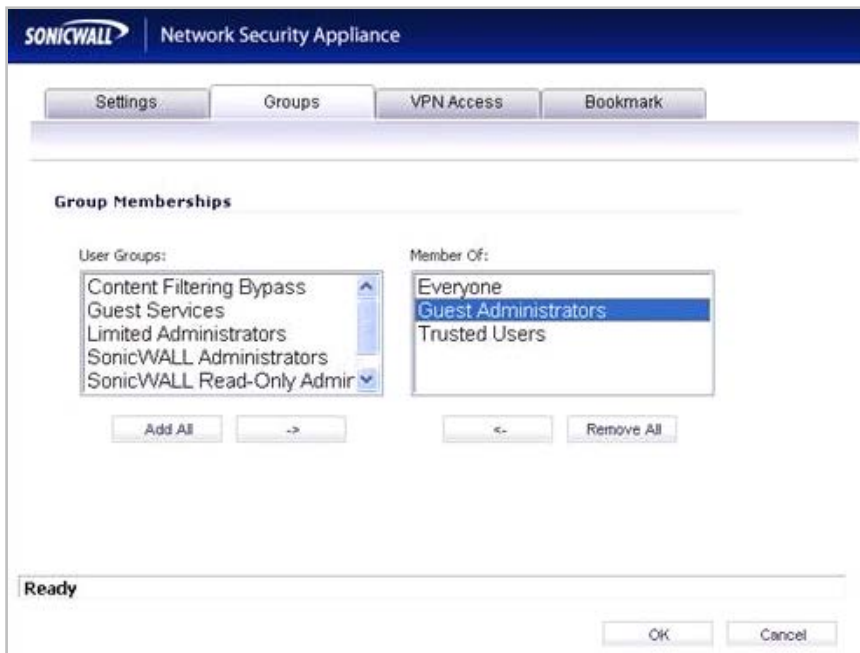


The screenshot shows the SonicWall Network Security Appliance web interface. The top navigation bar includes 'Settings', 'Groups', 'VPN Access', and 'Bookmark'. Below this is a sub-tab 'Group Memberships'. The main content area is titled 'User Settings' and contains the following fields and options:

- Name:
- Password:
- Confirm Password:
- User must change password
- Require one-time passwords
- E-mail address:
- Account Lifetime:
- Ready:

At the bottom right, there are 'OK' and 'Cancel' buttons.

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**.



The screenshot shows the SonicWall Network Security Appliance web interface with the 'Groups' tab selected. The sub-tab is 'Group Memberships'. The main content area is titled 'Group Memberships' and contains the following elements:

- User Groups: A list box containing 'Content Filtering Bypass', 'Guest Services', 'Limited Administrators', 'SonicWALL Administrators', and 'SonicWALL Read-Only Admin'.
- Member Of: A list box containing 'Everyone', 'Guest Administrators', and 'Trusted Users'. 'Guest Administrators' is highlighted.
- Buttons: 'Add All', '>', '<', and 'Remove All'.
- Ready:

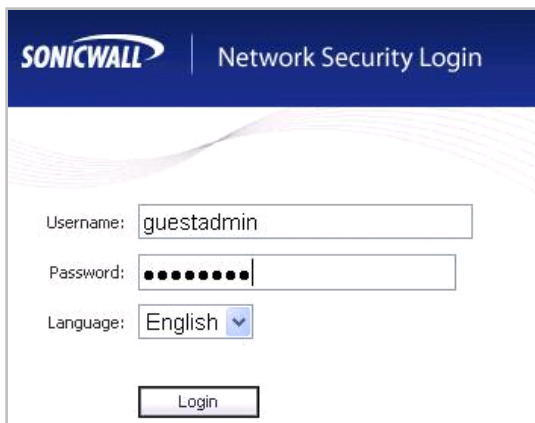
At the bottom right, there are 'OK' and 'Cancel' buttons.

# Release Notes

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.



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





# Release Notes

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



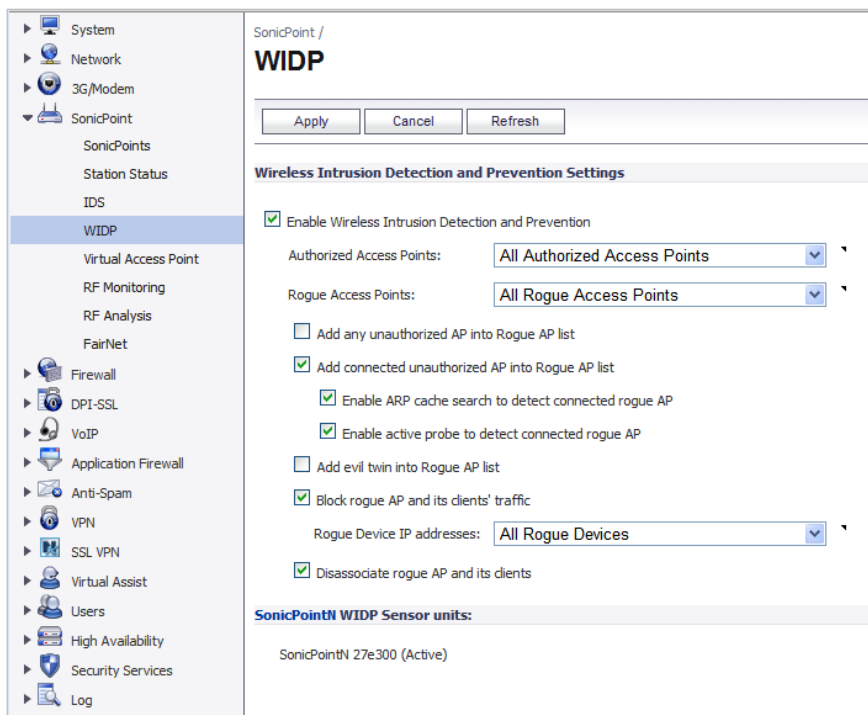
## Internal Radio IDS Scan Scheduling

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.



# Release Notes

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

SonicPointN /  
**IDS**

Discovered Access Points Items 1 to 7 (0)

View Style: 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									
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.

<input type="checkbox"/>	▶ 13	All SonicPoints	Group		
<input type="checkbox"/>	▶ 14	All Authorized Access Points	Group		
<input type="checkbox"/>	▶ 15	All Rogue Access Points	Group		
<input type="checkbox"/>	▶ 16	Node License Exclusion List	Group		
<input type="checkbox"/>	▶ 17	RBL User White List	Group		
<input type="checkbox"/>	▶ 18	RBL User Black List	Group		
<input type="checkbox"/>	▶ 19	Public Mail Server Address Group	Group		
<input type="checkbox"/>	▶ 20	Default Trusted Relay Agent List	Group		
<input type="checkbox"/>	▶ 21	All Rogue Devices	Group		
<input type="checkbox"/>	▶ 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.

# Release Notes

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 ↓ Highest	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
	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:

The screenshot shows the configuration interface for a service on a SonicWall Network Security Appliance. The service name is 'ShoreTel IP Phone Control 2427'. The protocol is set to 'UDP(17)'. The port range is '2427 - 2427'. The sub type is 'None'. The status is 'Ready'. There are 'OK' and 'Cancel' buttons at the bottom.

# Release Notes

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:

**SONICWALL** Network Security Appliance

General Advanced QoS

**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

Add Close Help

**SONICWALL** Network Security Appliance

General Advanced QoS

**DSCP Marking Settings**

DSCP Marking Action: Explicit

Explicit DSCP Value: 5

802.1p Marking Settings

802.1p Marking Action:

Note: No 802.1p tagging

Ready

Add Close Help

## 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.

# Release Notes

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.

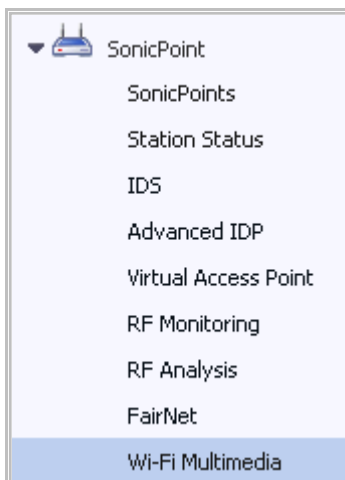
The screenshot shows the configuration page for a Network Security Appliance. The page has three tabs: General, Advanced, and QoS. The 'Settings' section is active and contains the following fields:

- 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: (empty text box)
- Enable Logging
- Allow Fragmented Packets

At the bottom, there is a 'Ready' status bar and three buttons: Add, Close, and Help.

## SonicPoint WMM Configuration

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



# Release Notes

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.

The screenshot shows the '802.11n Radio' configuration page in the 'Advanced' tab. The 'WMM (Wi-Fi Multimedia)' dropdown menu is open, showing three options: 'Create new WMM profile...', 'Disabled', and 'Create new WMM profile...'. A mouse cursor is pointing at the bottom option. Other settings include: Hide SSID in Beacon (unchecked), Schedule IDS Scan (Disabled), Data Rate (Best), Transmit Power (Full Power), Antenna Diversity (Best), Beacon Interval (100), DTIM Interval (1), Fragmentation Threshold (2346), RTS Threshold (2346), Maximum Client Associations (32), Station Inactivity Timeout (300), Preamble Length (Long), Protection Mode (None), Protection Rate (1 Mbps), Protection Type (CTS-only), and Enable Short Slot Time (unchecked).

The screenshot shows the '802.11n Radio 1' configuration page in the 'Radio 1 Advanced' tab. The 'WMM (Wi-Fi Multimedia)' dropdown menu is open, showing three options: 'Create new WMM profile...', 'Disabled', and 'Create new WMM profile...'. A mouse cursor is pointing at the bottom option. Other settings include: Hide SSID in Beacon (unchecked), Schedule IDS Scan (Disabled), Data Rate (Best), Transmit Power (Full Power), Antenna Diversity (Best), Beacon Interval (100), DTIM Interval (1), Fragmentation Threshold (2346), RTS Threshold (2346), Maximum Client Associations (32), Station Inactivity Timeout (300), Preamble Length (Long), Protection Mode (None), Protection Rate (1 Mbps), Protection Type (CTS-only), and Enable Short Slot Time (unchecked).

# Release Notes

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.

The screenshot shows the 'Settings' tab of the WMM configuration. It includes a 'Profile Name' field with the value 'wmmDefault'. Below are two tables for 'WMM Parameters of Access Point' and 'WMM Parameters of Station', each with columns for Access Category, CWMin, CWMax, and AIFS.

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

The screenshot shows the 'Mapping' tab of the WMM configuration. It displays a table for 'WMM Mapping' with columns for Access Category and DSCP.

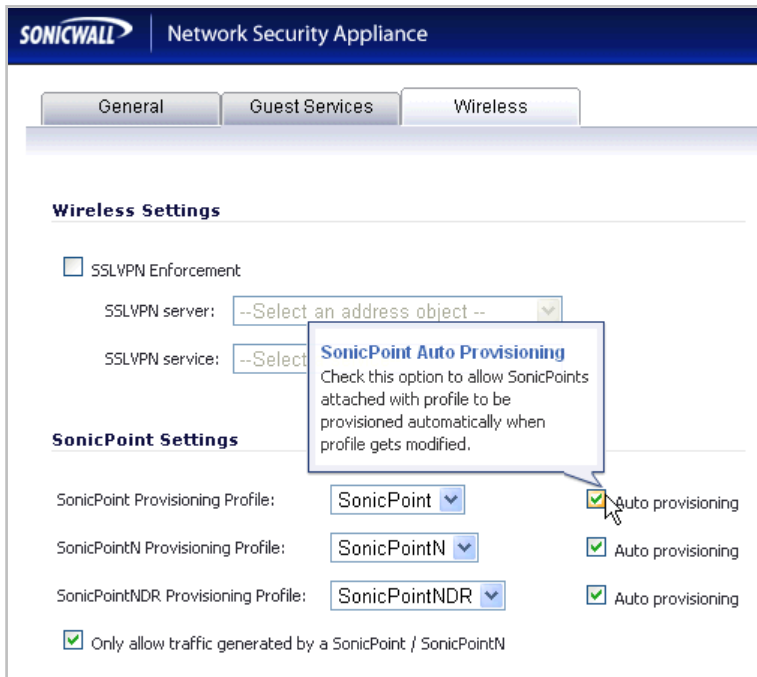
Access Category	DSCP
AC_BE(0)	0
AC_BK(1)	8
AC_VI(2)	40
AC_VO(3)	48

# Release Notes

## 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**.

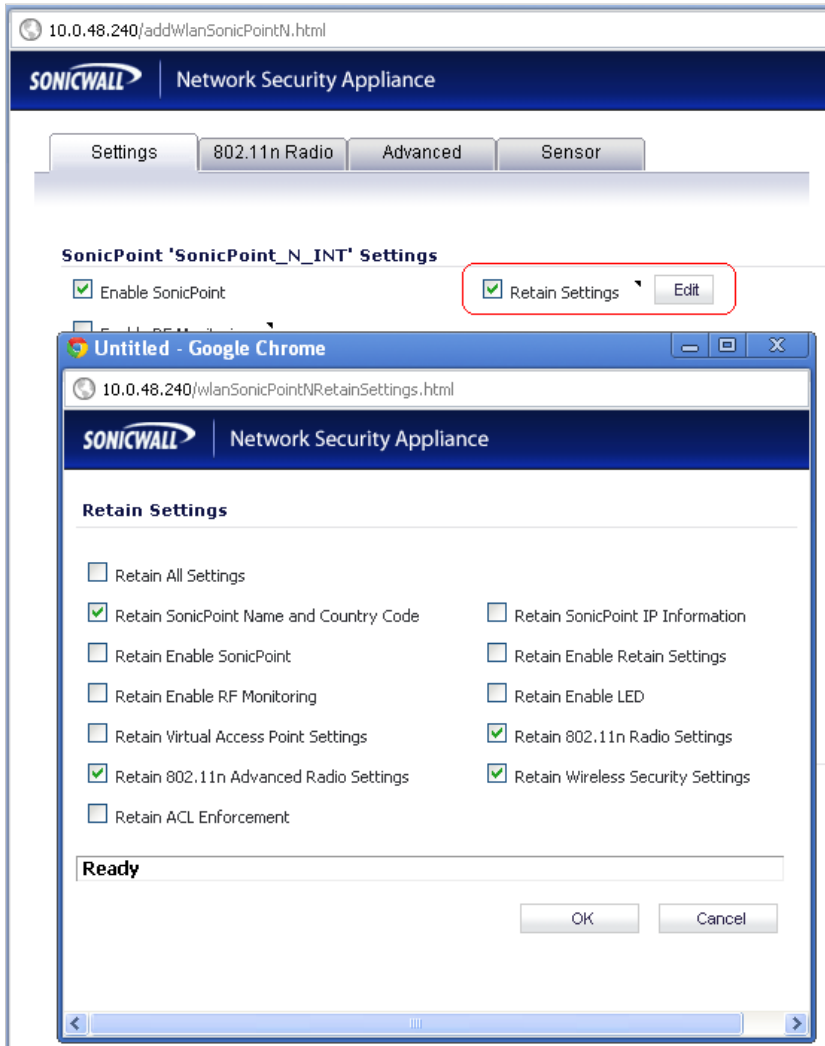




# Release Notes

## 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.



# Release Notes

## 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

Enable Periodic Secure Backup of Diagnostic Reports to MySonicwall

Time Interval (minutes)

## 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

Mode:

Radio Band:

Standard Channel:

Enable Short Guard Interval

Enable Aggregation

**Virtual Access Point En**

WEP Key Settings:

**ACL Enforcement**  Enable MAC Filter List

Allow List:

Deny List:

SONICWALL Network Security Appliance

Settings 802.11n Radio Advanced

**802.11n Radio Settings**

Enable Radio

Mode:

Radio Band:

Primary Channel:

Secondary Channel:

Enable Short Guard Interval

Enable Aggregation

**Virtual Access Point En**

WEP Key Settings:

**ACL Enforcement**  Enable MAC Filter List

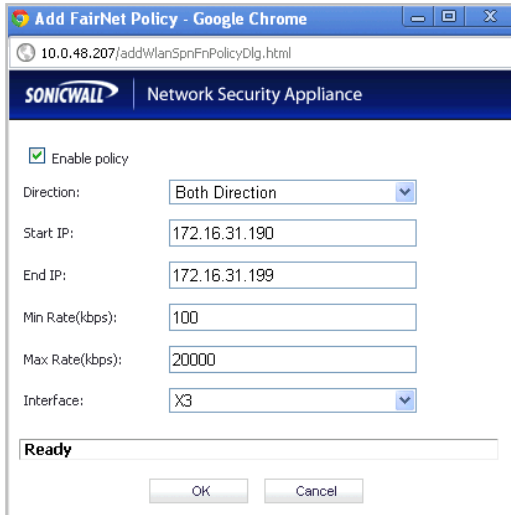
Allow List:

Deny List:

# Release Notes

## 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.



The screenshot shows a web browser window titled "Add FairNet Policy - Google Chrome" with the URL "10.0.48.207/addWlanSpnFnPolicyDlg.html". The page header displays the SonicWALL logo and "Network Security Appliance". The configuration form includes the following fields:

- Enable policy
- Direction: Both Direction (dropdown menu)
- Start IP: 172.16.31.190
- End IP: 172.16.31.199
- Min Rate(kbps): 100
- Max Rate(kbps): 20000
- Interface: X3 (dropdown menu)

At the bottom, there is a "Ready" status bar and "OK" and "Cancel" buttons.

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.

# Release Notes

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.

SONICWALL Network Security Appliance

General Advanced

### Interface Settings

Zone:

Tunnel Id:

Tunnel Source Interface:

# Release Notes

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.

The screenshot shows the 'Interface Settings' page in the SonicWall Network Security Appliance. The 'Zone' is set to 'WLAN'. The 'Tunnel Id' is '0'. The 'Tunnel Source Interface' is 'X3'. The 'IP Assignment' is 'Static'. The 'IP Address' is '0.0.0.0' and the 'Subnet Mask' is '255.255.255.0'. The 'SonicPoint Limit' is '96 SonicPoints'. The 'Management' options are 'HTTP', 'HTTPS', 'Ping', 'SNMP', and 'SSH'. The 'User Login' options are 'HTTP' and 'HTTPS'. There is a checkbox for '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**.

The screenshot shows the 'Interface Settings' page in the SonicWall Network Security Appliance. The 'Zone' is set to 'WLAN'. The 'Tunnel Id' is '0'. The 'Tunnel Source Interface' is 'X3'. The 'IP Assignment' is 'Layer 2 Bridged Mode'. The 'Bridged to' dropdown is set to '--Select an interface--'. There are three checkboxes: 'Block all non-IPv4 traffic', 'Never route traffic on this bridge-pair', and 'Only sniff traffic on this bridge-pair'. The 'SonicPoint Limit' is '96 SonicPoints'. The 'Management' options are 'HTTP', 'HTTPS', 'Ping', 'SNMP', and 'SSH'. The 'User Login' options are 'HTTP' and 'HTTPS'. There is a checkbox for '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.

# Release Notes

## 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.

The screenshot shows the SonicWall Network Security Appliance configuration interface. At the top, there is a navigation bar with the SonicWall logo and the text "Network Security Appliance". Below this, there are four tabs: "Settings", "802.11n Radio", "Advanced", and "Sensor". The "802.11n Radio" tab is selected.

The main content area is titled "802.11n Radio Settings". It contains the following fields and options:

- Enable Radio:** A checked checkbox and a dropdown menu set to "Always on".
- Mode:** A dropdown menu set to "2.4GHz 802.11n/g/b Mixed".
- SSID:** An empty text input field.
- Radio Band:** A dropdown menu set to "Auto".
- Primary Channel:** A dropdown menu set to "Auto".
- Secondary Channel:** A dropdown menu set to "Auto".
- Enable Short Guard Interval:** An unchecked checkbox.
- Enable Aggregation:** An unchecked checkbox.
- Enable MIMO:** A checked checkbox.

Below the "802.11n Radio Settings" section is the "Wireless Security" section, which contains:

- Authentication Type:** A dropdown menu set to "WPA2 - EAP".
- EAPOL Version:** A dropdown menu set to "v2". A note next to it says "Note: v2 provides better security."
- Cipher Type:** A dropdown menu set to "AES".
- Group Key Interval (seconds):** A text input field containing "86400".

At the bottom of the "Wireless Security" section is the "Radius Server Settings" section, which contains a "Configure..." button with a mouse cursor pointing to it.

# Release Notes

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

**Radius Server Global Settings**

Radius Server Retries:

Retry Interval (seconds):

**Radius Server Settings**

Radius Server 1 IP:  Port:

Radius Server 1 Secret:

Radius Server 2 IP:  Port:

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.

# Release Notes

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.



# Release Notes

## 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**.

The screenshot shows the SonicWall Network Security Appliance interface. At the top, there is a blue header with the SonicWall logo and the text "Network Security Appliance". Below the header, there are two tabs: "Settings" and "Guest Services". The "Guest Services" tab is selected. The main content area is titled "Guest Services" and contains several configuration options:

- Enable Guest Services Privilege
- Enforce login uniqueness
- Automatically prune account upon account expiration
- Activate account upon first login
- Account Expires:
- Session Lifetime:
- Idle Timeout:
- Receive limit (0 to disable):
- Transmit limit (0 to disable):

# Release Notes

## 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.

The screenshot shows the SonicWall Network Security Appliance configuration interface. The 'Advanced' tab is selected. Under 'Virtual Access Point Schedule Settings', the 'VAP Schedule Name' is set to 'Always on'. Under 'Virtual Access Point Advanced Settings', the 'Profile Name' is 'VAP Profile1', 'Radio Type' is 'SonicPoint', 'Authentication Type' is 'Open', 'Unicast Cipher' is 'None', 'Multicast Cipher' is 'None', and 'Maximum Clients' is '16'. In the 'ACL Enforcement' section, the 'Enable MAC Filter List' checkbox is checked. Below it, 'Use Global ACL Settings' is unchecked. The 'Allow List' is set to 'All MAC Addresses' and the 'Deny List' is set to 'No MAC Addresses'. A note at the bottom states: '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:

This close-up screenshot shows the 'ACL Enforcement' section with the 'Enable MAC Filter List' checkbox checked. The 'Use Global ACL Settings' checkbox is unchecked. The 'Allow List' dropdown menu is open, showing the following options: 'All MAC Addresses', '--Select an Address Object Group--', 'Create new MAC Address Object Group...', 'All MAC Addresses' (highlighted in blue), 'Default SonicPoint ACL Allow Group', and 'lan'. The 'Deny List' is set to 'No MAC Addresses'. The same note about ACL support is visible at the bottom.

# Release Notes

Deny List options:

**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 AP. If one Virtual Access Point is used by default.

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

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.

**SONICWALL** Network Security Appliance

General | 802.11n Radio 0 | Radio 0 Advanced | 802.11n Radio 1 | Radio 1 Advanced | Sensor

**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--

# Release Notes

## 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.

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

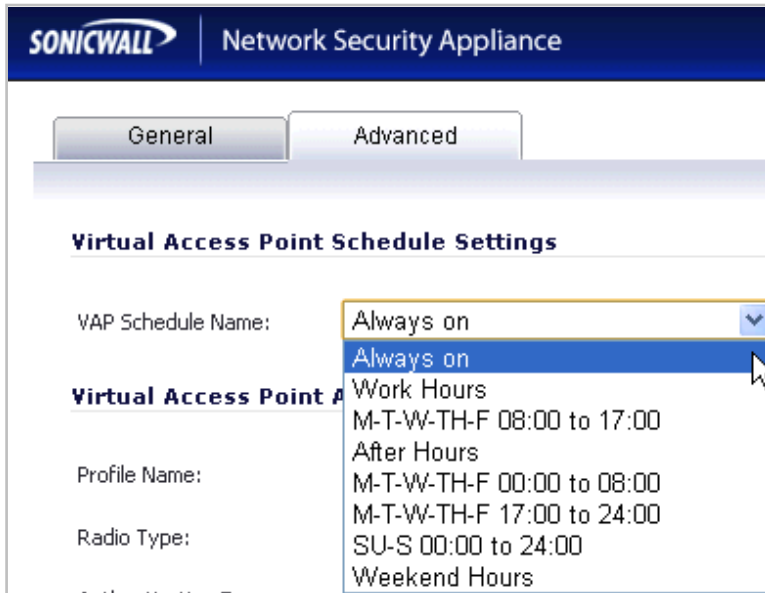
User Login:  HTTP  HTTPS

Add rule to enable redirect from HTTP to HTTPS

# Release Notes

## Virtual Access Point Schedule Support

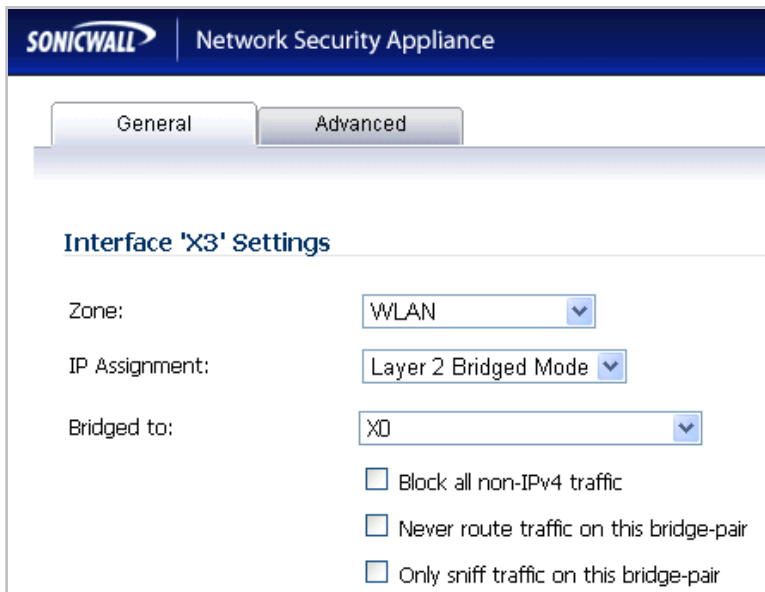
Each Virtual Access Point schedule can be individually enabled or disabled, for ease of use. To select a VAP schedule, navigate to the **SonicPoint > Virtual Access Point** page. Add or edit a Virtual Access Point. In the configuration window, click the **Advanced** tab. Select the desired schedule from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



## 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**.

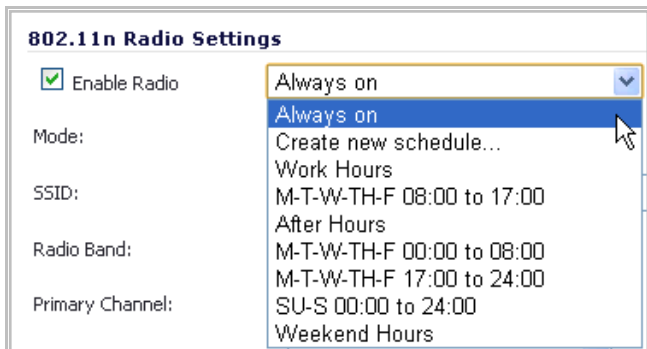


# Release Notes

## 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.

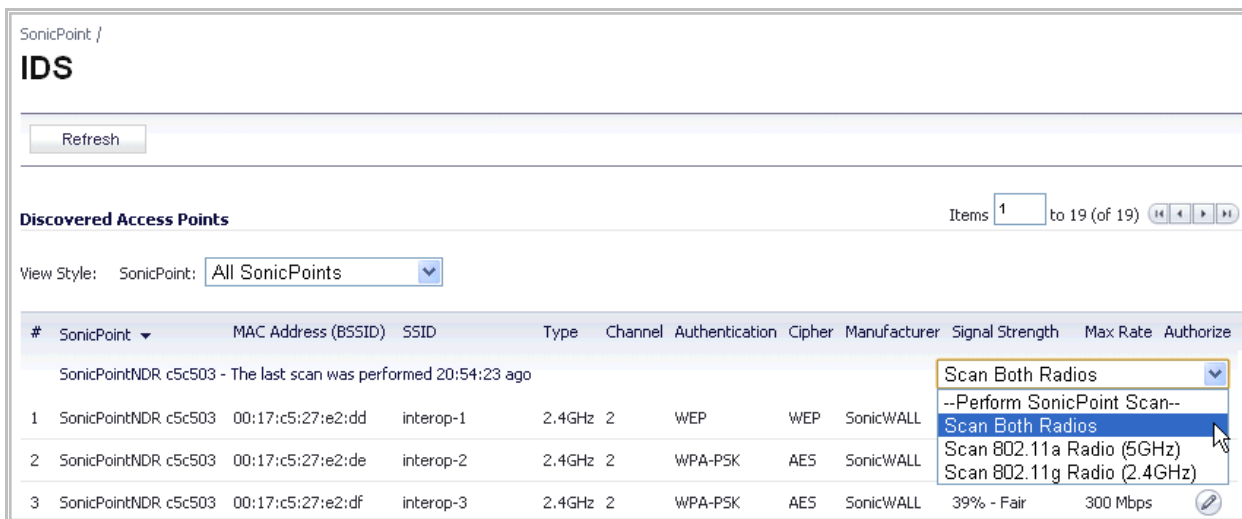
The scheduling options are shown in the image below:



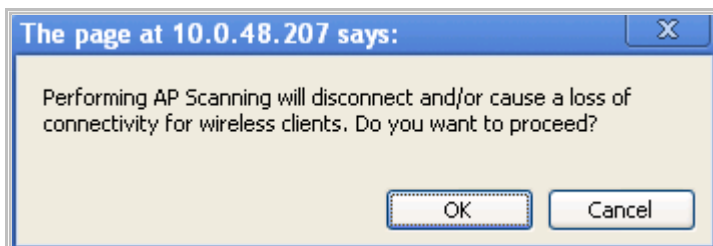
## Wireless Rogue Device Detection and Prevention

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.



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.



# Release Notes

## 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.

The screenshot displays the Dell SonicWALL Product Support page for NSA Series Appliances. The page features a navigation menu on the left with categories like Support, Product Documentation, Network Security, and NSA Series. The main content area is titled 'Product Support' and includes a search bar, 'Support Documents' and 'Knowledge Base' tabs, and a 'List View Options' section. Below these are sections for 'Technical Notes' and 'Release Notes', each displaying a list of documents with titles and dates.

**Support Documents**

Document Title	Date
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
Using a Windows Enterprise Root CA with DPI-SSL	22 Mar 2012
Integrating Agilink with SonicOS 5.8.1.5	1 Mar 2012
Integrating CradlePoint with SonicOS 5.8.1.5	1 Mar 2012

**Release Notes**

Document Title	Date
SonicWALL Mobile Connect for Android 2.0.8 Release Notes	13 Jun 2013
SonicOS 6.1.1.1 NSA 3600-6600 Release Notes	30 May 2013
Dell SonicWALL Directory Services Connector 3.6.11 Release Notes	18 May 2013
SonicOS 5.8.1.12 Release Notes	7 May 2013

Last updated: 6/25/2013