Release Notes

SonicOS | **SonicOS 5.9.0.2 Release Notes**

Contents

Release Purpose

SonicOS 5.9.0.2 is an Early Release for Dell SonicWALL NSA E-Class, NSA, and TZ series network security appliances. It provides several new features and resolves a number of issues found in earlier releases.

Platform Compatibility

The SonicOS 5.9.0.2 release is supported on the following Dell SonicWALL Deep Packet Inspection (DPI) security appliances:

- NSA E8510
- NSA E8500
- NSA E7500
- NSA E6500
- NSA E5500
- NSA 5000
- NSA 4500
- NSA 3500
- NSA 2400
- NSA 2400MX
- NSA 250M / NSA 250M Wireless
- NSA 240
- NSA 220 / NSA 220 Wireless
- TZ 215 / TZ 215 Wireless
- TZ 210 / TZ 210 Wireless
- TZ 205 / TZ 205 Wireless
- TZ 200 / TZ 200 Wireless
- TZ 105 / TZ 105 Wireless
- TZ 100 / TZ 100 Wireless

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 or higher.

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 the www.sonicwall.com Support/Product Documentation page for NSA or TZ 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.

WWAN 3G/4G Support

SonicOS 5.9 supports a variety of 3G and 4G PC cards and USB devices for Wireless WAN connectivity. 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

In addition to devices supported on previous releases, SonicOS 5.9 includes support for the following 3G/4G devices:

- “T-Mobile Rocket 3.0” ZTE MF683 4G (USA)
- “AT&T Momentum” Sierra Wireless 313U 4G (USA)
- “AT&T Beam AirCard” Sierra Wireless 340U 4G (USA) (supported with LTE network, not with HSPA+)
- Pantech UML290 4G (USA)
- “Rogers Rocket Stick” Sierra Wireless 330U 4G (Canada)
- Huawei E398
- Huawei E353
- Kyocera 5005 (Vodafone’s branded implementation of the Huawei E398)

Note: When connected to a Dell SonicWALL appliance, the performance and data throughput of most 3G/4G devices will be lower than when the device is connected directly to a personal computer. SonicOS uses the PPP interface rather than the proprietary interface for these devices. The performance is comparable to that from a Linux machine or other 4G routers.

Known Issues

This section contains a list of known issues in the SonicOS 5.9.0.2 release.

3G/4G

Symptom	Condition / Workaround	Issue
The 4G device is connected, but no traffic passes through it.	Occurs when interface U0 is configured as the final backup or as the primary WAN, and the AT&T Beam AirCard Sierra Wireless 340U 4G device is connected without an external antenna. Thus, it is only able to negotiate HSPA+. Traffic does pass when using an external antenna to negotiate with the faster LTE network.	133999
The firewall shuts down or restarts automatically when a 3G or 4G USB device is inserted or removed.	Occurs when inserting or removing a 3G/4G USB device (a HuaWei E353 HSPA+ USB Stick) when the appliance is powered on. **Workaround**: The appliance should always be powered off when inserting or removing a USB device. Hot plug and play is not supported.	130973

Active/Active Clustering

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

Application Control

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

DPI-SSL

Symptom	Condition / Workaround	Issue
The certificate from a secure website, such as https://mail.google.com, is not changed to a Dell SonicWALL DPI-SSL certificate as it should be, and traffic cannot be inspected.	Occurs when the “Enable SSL Client Inspection” option is set on the DPI-SSL > Client SSL page, a SonicPoint-NDR is connected to the appliance, Guest Services is enabled on the WLAN zone, a wireless client connects to the SonicPoint, and the user logs into the guest account.	123097
A Remote Desktop Protocol (RDP) session cannot be established.	Occurs when the “Enable SSL Client Inspection” option is set on the DPI-SSL > Client SSL page, and a user tries to connect, using RDP, from a Windows 7 computer on the WLAN to another Windows 7 computer on the LAN.	102701

Firewall

Symptom	Condition / Workaround	Issue
The App Rule Match Object cannot match a Filename.	Occurs during an FTP download or upload when the App Rule Match Object is set with the Prefix Match, Hexadecimal Representation, and Negative Match options enabled. **Workaround**: Do not enable the Negative Match option with the Prefix Match option.	135634

IPv6

Symptom	Condition / Workaround	Issue
A site-to-site VPN tunnel does not work if an IPv6 6rd tunnel is also configured.	Occurs when the Advertise Subnet Prefix of the IPv6 Primary Static Address option is enabled on one of the interfaces of the site-to-site VPN tunnel.	133750
An IPv6 Address Object in the Exclusion Address list of an App Rule policy is still blocked by that App Rule policy.	Occurs when a computer on the LAN with an IPv6 address that is included in the Exclusion Address list of an App Rule policy tries to connect to an IPv6 website that is blocked by that policy.	128363

Log

Symptom	Condition / Workaround	Issue
Log settings cannot be modified. The error message, “The format of the email address is incorrectly reported” is displayed.	Occurs when trying to modify the log settings in the Edit Log Category dialog on the Log > Settings page.	136248

Networking

Symptom	Condition / Workaround	Issue
Dynamic DNS always displays a network error status.	Occurs after configuring a DDNS profile on the Network > Dynamic DNS page. The page should display the online status.	135341
The value of the “ifHCInBroadcastPkts” field in an SNMP-GET packet is different from the value displayed for Rx Broadcast Packets on the Network > Interfaces page.	Occurs when comparing the Rx Broadcast Packet values for each interface shown on the Network > Interfaces page with the values obtained from SNMP.	131306
Wire Mode and Tap Mode are disabled and cannot be selected from the IP Assignment menu on the Edit Interface dialog. The IP Assignment menu is set to Static and cannot be changed.	Occurs when editing an unassigned interface in a Stateful High Availability pair, and WAN is selected from the Zone menu.	131050
FTP and HTTP traffic does not pass through a pair of interfaces in Wire Mode that is set to Secure. Pings still pass.	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 the other static interfaces.	101359

Security Services

Symptom	Condition / Workaround	Issue
SonicOS drops the Client CFS Ping reply packets, and Client CFS Enforcement does not work on the SSL VPN zone.	Occurs when the source IP address of the Client CFS Ping packet is the WAN interface IP address.	135585
The Gateway AV Exclusion List does not prevent some IP addresses from being blocked.	Occurs when an FQDN Address Object is included in the Gateway AV Exclusion List.	121984

System

Symptom	Condition / Workaround	Issue
The configuration mode on the LCD panel cannot be accessed and displays an Invalid Code error message.	Occurs when the administrator selects the Configuration option on the LCD panel and enters the new PIN code that was just changed on the System > Administration page.	130379
GMS 7.1 does not synchronize with SonicOS after making password changes in One Touch Configuration and then rebooting the appliance.	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 management computer cannot manage the firewall because SonicOS cannot forward Ethernet packets larger than 1496 KB.	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

Users

Symptom	Condition / Workaround	Issue
Single Sign-On (SSO) does not work for users behind a proxy server.	Occurs when SSO tries to authenticate users behind a proxy server from the “X-Forwarded-For HTTP” header. Two local IP addresses are being saved in the cache: the initiator IP address and the user IP address. Normally these should be the same IP address, but they are not because the user is behind a proxy server and the initiator IP address is that of the proxy server.	135558
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
Traffic goes to the wrong VPN tunnel.	Occurs when two VPN tunnel interfaces are configured with Amazon VPC, and we add two numbered tunnel interfaces and BGP neighbors based on the Amazon VPC configuration. When Tunnel 1 goes down, the traffic switches to Tunnel 2. When Tunnel 1 comes back up, the traffic stays on Tunnel 2. When Tunnel 2 goes down, the traffic switches to Tunnel 1. But when Tunnel 2 comes back up, the traffic stops. The route table shows that packets are going through Tunnel 1, but a packet capture shows that packets are going through Tunnel 2.	135205

Wizards

Symptom	Condition / Workaround	Issue
Setup Wizard cannot complete the initial setup configuration and the firewall must be restarted.	Occurs when trying to configure the initial setup using the Setup Wizard. The Setup Wizard stops on the WAN Settings page after the "Next" button is clicked, and the following message is displayed: “User:09/09 11:30:19.800: NOTICE: webSrvrThreadTimer:4598: Web server thread tWebMain02 has been busy for 31 seconds in state Active; fd 79 2291235280.49206.80.2291235472:-2102248124 -> port -2097387164” **Workaround**: Use the CLI to do the initial setup, or login to the firewall from the Web UI to do the configuration.	135211

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 it 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 an NSA 240 and an NSA 7500, with Advanced Routing enabled on the NSA 240. A numbered tunnel interface is created on the NSA 7500 and is 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 an OSPF connection cannot be established.	128419
User cannot change the Manual Key VPN policy to an IKE policy.	Occurs when the user attempts to change a Manual Key VPN policy to an IKE policy. The following message appears, "Remote IKE ID must be specified." **Workaround:** Delete the Manual Key policy and add a new IKE policy with the same IPsec gateway and source/destination networks.	112988
OSPF routing does not work properly.	Occurs when OSPF is configured, and a Tunnel Interface VPN policy is deleted and then re-created. OSPF will not connect until the appliance or the HA pair is restarted.	101510

Resolved Issues

This section contains a list of issues that are fixed in the SonicOS 5.9.0.2 release.

3G/4G

Symptom	Condition / Workaround	Issue
The 3G connection cannot obtain an IP address, preventing access to the Internet.	Occurs when trying to establish a 3G connection using a Huawei E398 card.	134756
The AT&T Beam 4G Aircard 340U needs to be supported by SonicOS.	Occurs when trying to establish a 4G connection using the AT&T Beam 4G Aircard 340U card for Wireless WAN connectivity.	132955

Anti-Spam

Symptom	Condition / Workaround	Issue
The System > Status page shows that Anti-Spam is licensed, but the Anti-Spam > Status page shows “Not Licensed".	Occurs when the firewall is rebooted and has been up for 5 minutes.	134472

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
Support for adding multiple IPv6 tunnel interfaces with remote IPv6 networks overlapped is requested.	Occurs when adding a default IPv6 tunnel interface for Internet traffic, and then attempting to add another tunnel interface for a specific network.	134545
Traffic cannot pass through IPv6 VPN tunnels.	Occurs when the primary WAN interface (X1) is disabled, and an IPv6 VPN tunnel is configured and bound to another WAN interface (X2). Negotiation is successful, but pings through the IPv6 tunnel are dropped.	134432
Traffic does not pass through an IPv6 SSL VPN tunnel to the WAN in Tunnel All mode. The remote administrator cannot connect to the IPv6 WAN address to manage the appliance.	Occurs when a remote client connects to the appliance using SSL VPN access and sends IPv6 traffic. IPv4 traffic works fine.	134344
Adding a second 6rd tunnel changes the 6rd address for the interface associated with the original 6rd tunnel. Deleting the second 6rd tunnel deletes that interface address. Adding the address again with original values results in an address using the second 6rd tunnel prefix.	Occurs when adding a second 6rd tunnel with a different prefix than the first 6rd tunnel. It causes the 6rd address of the interface for the first 6rd tunnel to change so that it corresponds to the prefix of the second 6rd tunnel.	134029

Symptom	Condition / Workaround	Issue
The IPv6 FTP Server cannot be accessed.	Occurs when the SYN Flood Protection Mode is set to Always proxy WAN client connections on the Firewall Settings > Flood Protection page.	131145
The IPv6 ACL does not appear in the IPv6 ACL list, but appears in the IPv4 ACL list.	Occurs when AppFlow is enabled, and a new IPv6 Access Control List (ACL) is added.	130522

Log

Symptom	Condition / Workaround	Issue
Log Automation does not work. SonicOS displays the error, “Problem connecting to SMTP server.”	Occurs when Log Automation is configured to send Email alerts, and the appliance is upgraded from 5.8 to 5.9.	134647
Multiple remote firewalls connected to an NSA 4500 by a site-to-site VPN shows the status as down.	Occurs when upgrading to 5.9 and the SNMP console queries the multiple remote firewalls connected to the NSA 4500 for statistics.	134282
The Syslog server configuration is lost.	Occurs after upgrading to 5.9 and checking the Syslog server settings. The Syslog server settings should be imported during the upgrade.	133053
Scrutinizer reports significantly understated results for Netflow (IPFIX w/ Extensions) data.	Occurs when Internal Flow Reporting (AFM) and External Flow Reporting are set to Scrutinizer, and the user downloads a large file such as a movie. AFM and Scrutinizer report significantly different results. Scrutinizer reports very little traffic. AFM reports more traffic than expected.	131330
The Enhanced Syslog format automatically becomes the default Syslog format.	Occurs when the appliance is restarted, and the “Enable Analyzer Settings” and “Enhanced Syslog” options were enabled on the Log > Syslog page before the restart. The “Enhanced Syslog” option is still enabled after the restart, although it should not be.	130835

Networking

Symptom	Condition / Workaround	Issue
An OSPF-originated default route disappears from the Route Policies table.	Occurs when OSPF is enabled on an interface connecting two firewalls, and the Originate Default Route option is set to Always on the first firewall. The OSPF-originated default route then appears in the Route Policies table on the second firewall. After changing the metric value for the “Apply the following metric to default routes received from Advanced Routing protocols” option on the second firewall, the OSPF-originated default route disappears from the Route Policies table.	134425
Throughput is reduced considerably when Deep Packet Inspection (DPI)is enabled.	Occurs when DPI is enabled and the connections to the client PCs are tested.	133249
The priority of NAT policies is changed or lost after rebooting.	Occurs when attempting to modify the priority of a NAT policy.	131806

SSL VPN

Symptom	Condition / Workaround	Issue
SSL VPN client routes disappear and the SSL VPN IPv6 pool becomes the default address object.	Occurs after upgrading to 5.9.	134506
The HTTP to HTTPS redirect on X0 does not work.	Occurs when you enable SSL VPN on a LAN interface, and the “Add rule to enable redirect from HTTP to HTTPS” option is selected on the “Edit Interface” dialog for X0.	130392

System

Symptom	Condition / Workaround	Issue
The firewall loses its port redundancy configuration on a VLAN-configured interface after an upgrade.	Occurs when upgrading from SonicOS 5.9.0.1.	134584
Valid hostnames with a numeric leading character cannot be added to the custom Network Time Protocol (NTP) list.	Occurs when trying to add an NTP server on the **System > Time** page.	134250

Users

Symptom	Condition / Workaround	Issue
LDAP traffic is incorrectly sourced from the WAN interface.	Occurs when LDAP traffic is sent over a site-to-site VPN tunnel to a host at the remote end of the tunnel.	135352
Users trying to login are not allowed membership into a trusted user group and cannot login to the firewall.	Occurs if LDAP is not configured, but is selected to read user group information. SSO domain users are put into the Unauthenticated User column and are only made members in the Everyone group. If LDAP is configured and selected to read user group information, but is still unable to connect, an error “LDAP cannot retrieve user group” is returned, but the user still gets membership in a trusted group and can login to the firewall.	134701

VPN

Symptom	Condition / Workaround	Issue
A tunnel routing policy cannot be configured for a route-based VPN.	Occurs when the user tries to create a tunnel-interface VPN policy. The Add Route Policy dialog times out, and the parameters cannot be entered.	135781
In an IPsec tunnel with WAN Failover, failback from the secondary interface to the primary interface does not occur for a while.	Occurs when the remote end connects to the head end. In the WAN failover, Primary (X1) to Secondary (X2), works, but failback, Secondary (X2) to Primary (X1), does not work. The VPN renegotiates on the remote end, but the head end active tunnel still lists the old tunnel information, and the ESP packets are dropped until dead peer detection is triggered and the tunnel is reinitiated, or the tunnel is manually disabled.	135720
NetBIOS traffic is dropped when the advanced settings for a NetBIOS broadcast on a VPN are enabled.	Occurs when the “Enable Windows Networking (NetBIOS) Broadcast” option is selected in a VPN policy under the Advanced tab.	135544
A Main Mode VPN tunnel cannot be established.	Occurs when OCSP and KeepAlive are both enabled on both sides of a connection.	131424
The Layer 2 Tunneling Protocol (L2TP) server cannot establish multiple L2TP sessions with multiple clients simultaneously.	Occurs when there are multiple L2TP clients behind the same NAT device. Only one session can be established at a time; otherwise, the Phase 2 Security Associations (SAs) are overridden.	52505

Wireless

Symptom	Condition / Workaround	Issue
SonicPointN provisioning fails.	Occurs in SonicPoint Layer 3 Management, when the maximum segment size (MSS) field for TCP is set to avoid packet fragmentation.	135332
The user is redirected to an interface IP instead of the FQDN, and security certificate warning is displayed.	Occurs when the User Web Login Settings on the Users > Settings page are configured to redirect the browser based on the name from the administration certificate or the configured domain name. Users are redirected to the FQDN and get the message, "Please wait while you are redirected to a secure login page." Users are then redirected to the interface IP of the firewall/auth.html.	134643
SonicPoint 5GHz channel configuration cannot be modified.	Occurs when trying to change a SonicPoint 5GHz channel from Auto to Manual 100.	133478
Wireless Authentication/Association for clients in the remote MAC address access list slows or fails.	Occurs the first time a client tries to connect to the RADIUS server.	108567

New Features in SonicOS 5.9.0.2

SonicOS 5.9.0.2 provides the following new features and enhancements:

Client CFS Enforcement

Client CFS Enforcement is a service that installs a Content Filtering Client on a Windows or Mac OS computer. The firewall performs enforcement according to the policies defined in the Enforced Client Policy and Reporting Server (EPRS), a server in the Dell SonicWALL data center.

Client CFS Enforcement is similar to Client Anti-Virus, such as McAfee Anti-Virus. Client CFS Enforcement is an independent feature and is not integrated with Client Anti-Virus. Client CFS Enforcement listens on a different port than Client Anti-Virus and is not aware of the Client Anti-Virus service.

Client CFS Enforcement is configured on the Security Services > Client CFS Enforcement page.

Note: Although Client CFS Enforcement is included in the UI, this feature is not yet available for licensing.

IPv6 BGP

IPv6 Border Gateway protocol (BGP) communicates IPv6 routing information between Autonomous Systems (ASs). A Dell SonicWALL security appliance with IPv6 BGP support can replace a traditional BGP router on the edge of a network's AS.

IPv6 BGP is enabled on the **Network > Routing** page, but must be configured on the SonicOS Command Line Interface (CLI).

Refer to Appendix B, “BGP Advanced Routing” of the *SonicOS 5.9 Administrator’s Guide* for the detailed CLI configuration procedures.

The following restrictions apply to IPv6 BGP in SonicOS 5.9.0.2:

- IPv6 BGP is supported only on NSA platforms.
- IPv6 BGP depends on IPv6 functions and ZebOS (Zebra OS).
- MPLS/VPN and multicast are not supported in IPv6 BGP.

IPv6 for Backend Servers

Dell SonicWALL provides backend servers that maintain IPv6 address records (AAAA records). Dell SonicWALL supports IPv6 on the following Dell SoniWALL backend servers:

- License Manager Servers
- Signature download Servers
- Content Filtering Service (CFS) Servers
- Dashboard Servers
- MySonicWALL Servers
- Online Help Servers
- Software Update Servers
- Auto Software Upgrade Servers
- Download NetExtender Servers
- Download SonicPoint Image Servers

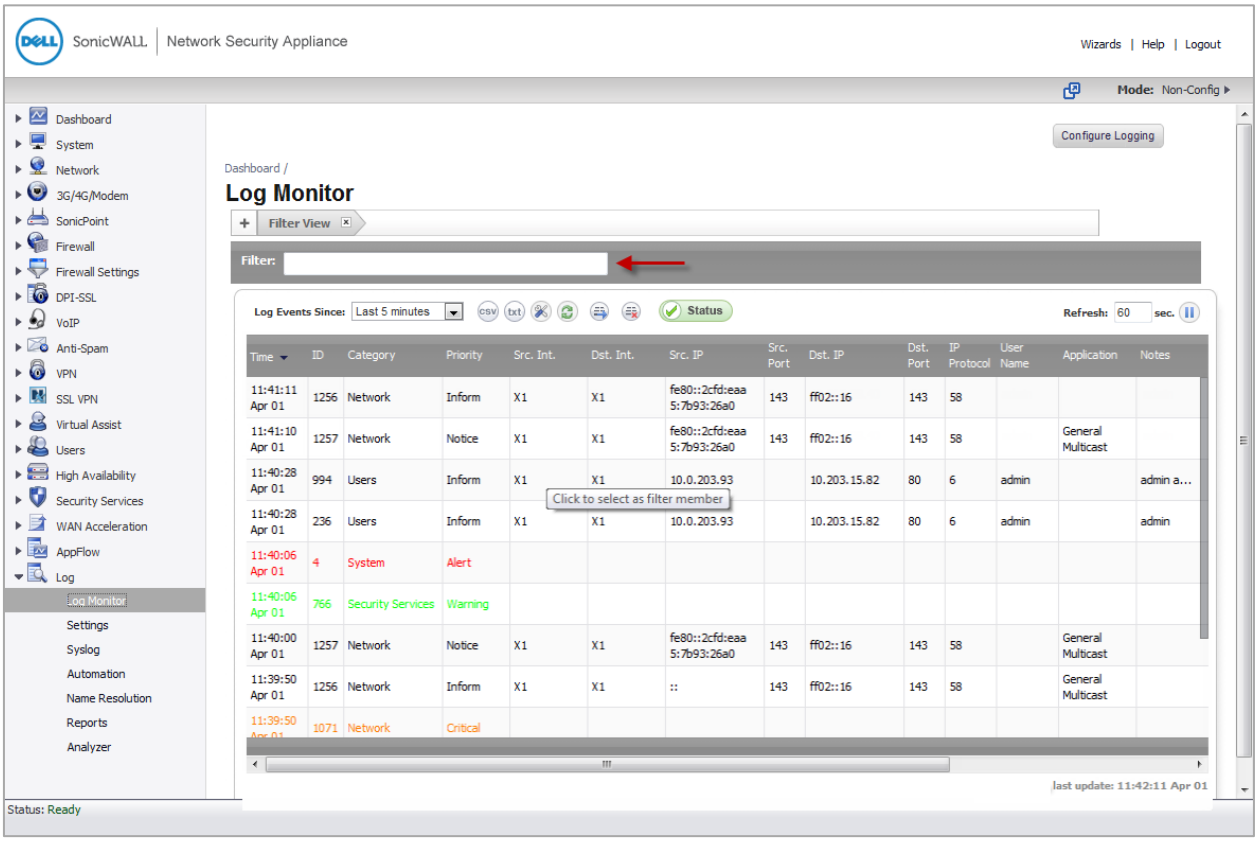
Dell SonicWALL does not support IPv6 on the following Dell SonicWALL backend servers:

- DRP Servers
- Responder Servers
- Anti-spam Servers
- Cloud AV Servers
- Enforce AV Servers
- Geo-IP Servers
- App Report Servers

A Dell SonicWALL network security appliance will use an IPv6 address to connect to a backend server only when no IPv4 address can be resolved.

Log Monitor Filter Input Box

The Filter input box at the top of the Log Monitor panel enables you to enter a search string that is used to filter the log events that are displayed in the Log Monitor panel.



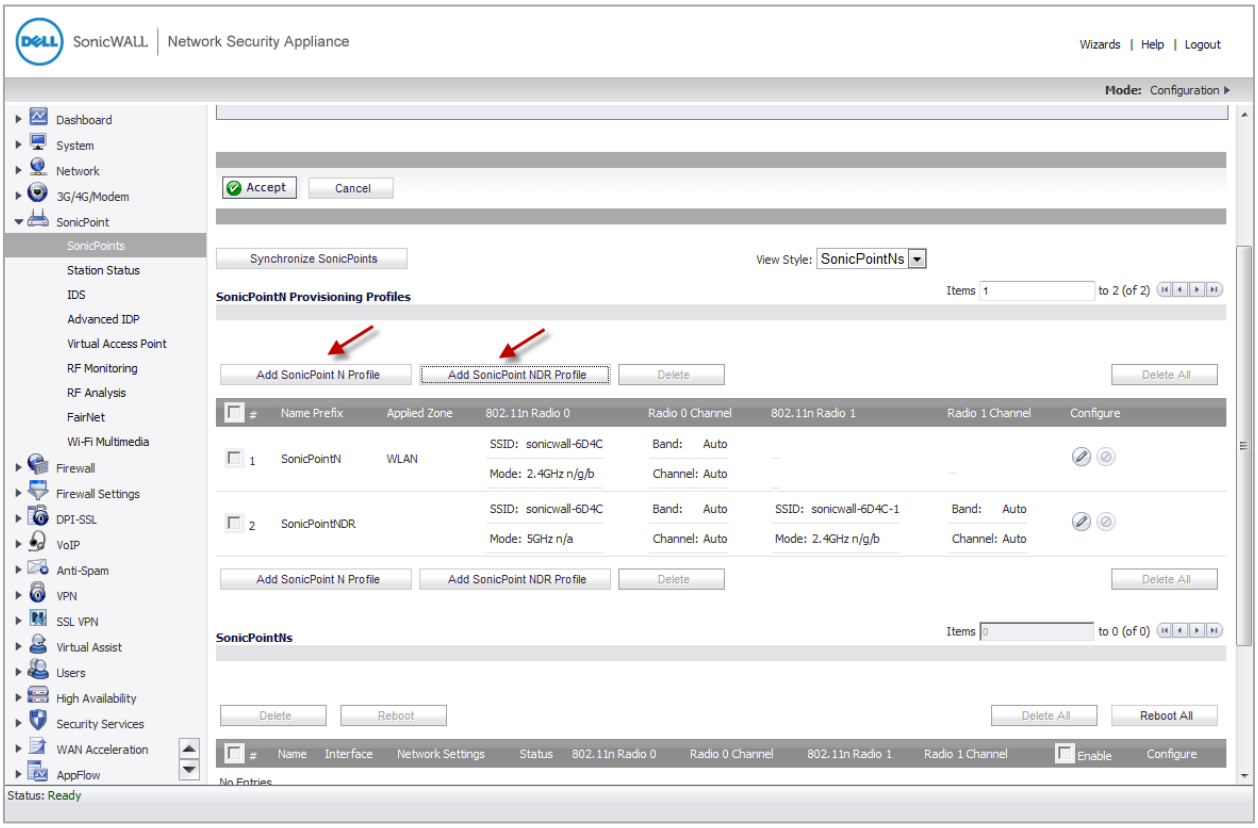
You can type any substring and press the Enter key to filter the Log Monitor panel. The Log Monitor will list only log events that contain matches for that substring.

Remote MAC Access Control

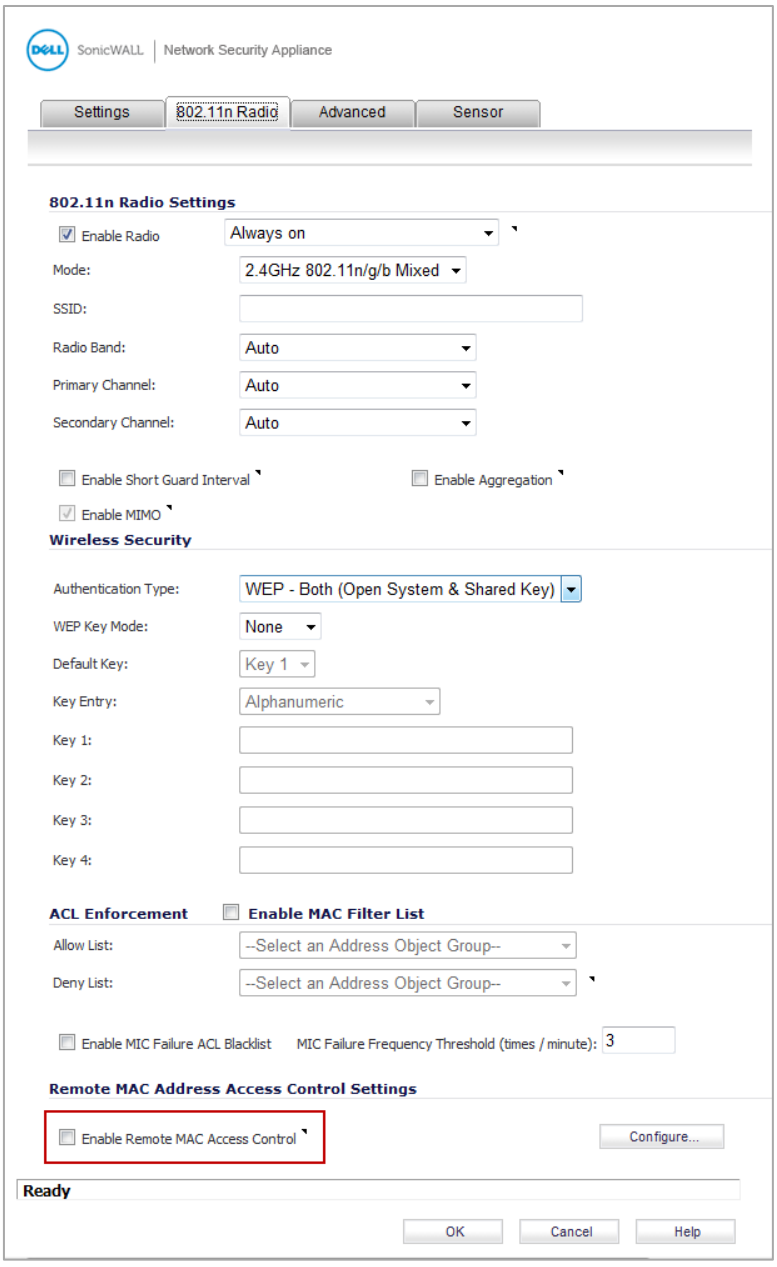
The Remote MAC Access Control option has been added for SonicPoints and for VAPs:

Remote MAC Access Control is a special feature that stores the MAC address of client computers in a remote Access Control List (ACL). This allows for a larger list than was previously possible when it was stored on the firewall itself. This feature is enforced using a 3rd party RADIUS server that can access and query the database where the MAC entries are stored.

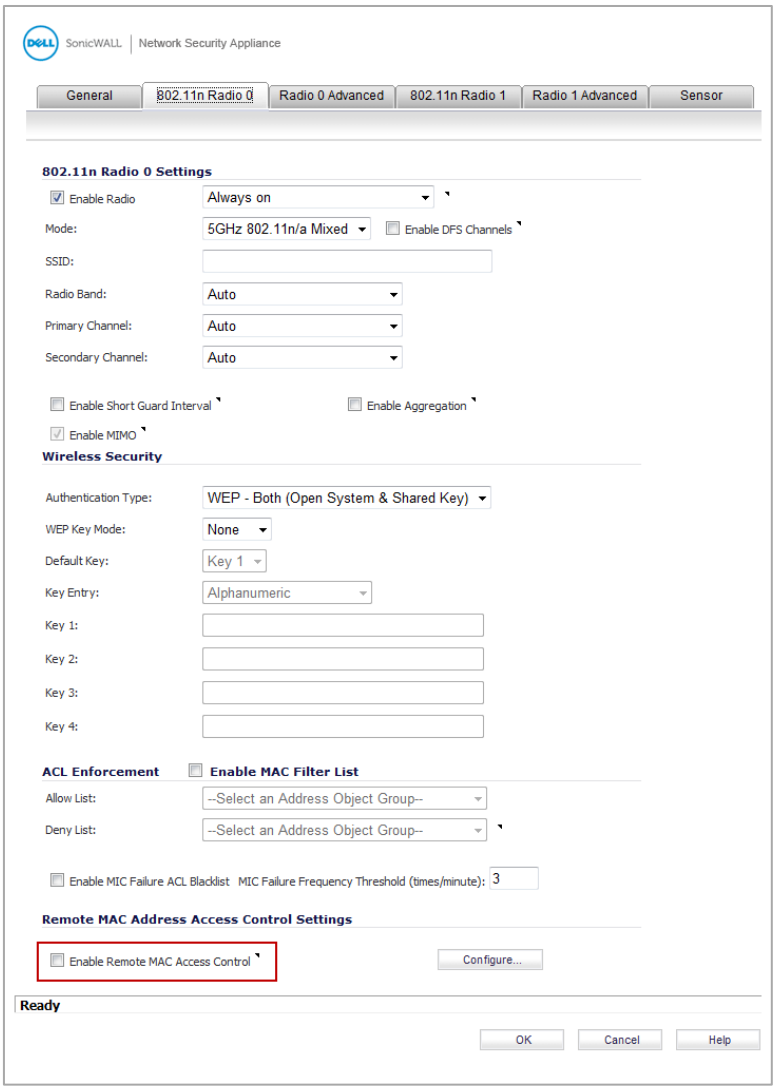
The **Enable Remote MAC Access Control** option has been added to the **Add SonicPoint N Profile** dialog and the **Add SonicPoint NDR Profile** dialog, accessed from the **SonicPoint** > **SonicPoints** page.



On the **SonicPoint** > **SonicPoints** page, in the **Add SonicPoint N Profile** dialog, under the **802.11n Radio** tab, the **Enable Remote MAC Access Control** option has been added under the **Remote MAC Address Access Control Settings** panel.

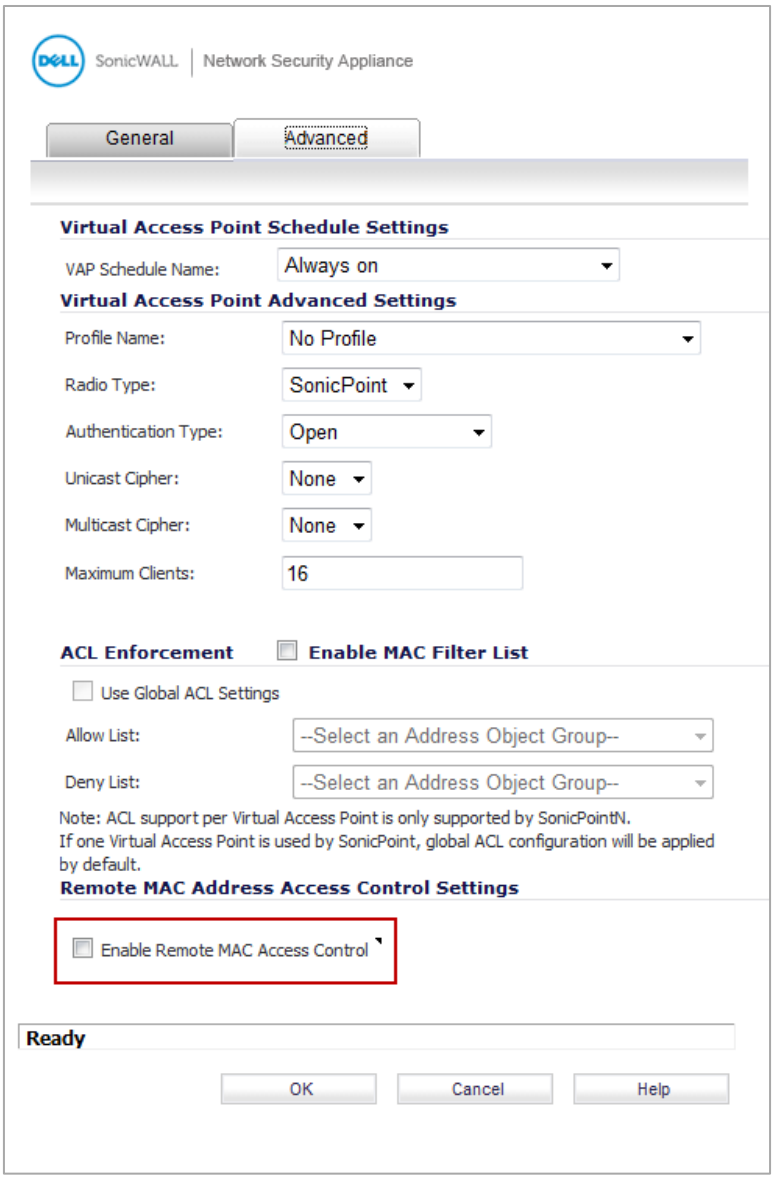


On the **SonicPoint** > **SonicPoints** page, in the **Add SonicPoint NDR Profile** dialog, under the **802.11n Radio 0** tab, the **Enable Remote MAC Access Control** option has been added under the **Remote MAC Address Access Control Settings** panel.



You cannot enable the **Remote MAC address access control** option at the same time that the **IEEE 802.11i EAP** is enabled. If you try to enable the **Remote MAC address access control** option at the same time that the **IEEE 802.11i EAP** is enabled, you will get the following error message:

The **Enable Remote MAC Access Control** option has also been added to the **Add Virtual Access Point** dialog, under the **Remote MAC Address Access Control Settings** panel, accessed from the .**SonicPoint** > **Virtual Access Point** page.



SSL VPN Mobile Connect Bookmark

Mobile Connect enables users to securely access their networks from a mobile device. Mobile Connect Bookmarks enhances the usability and experience for users by giving them quick access to their remote network resources.

When user bookmarks are defined, they are displayed on the **SSL VPN > Virtual Office** page. Users can modify or delete their own bookmarks, but cannot modify or delete bookmarks created by the administrator.

Refer to the “Configuring SSL VPN Bookmarks” section of the *SonicOS 5.9 Administrator’s Guide* for the steps to configure SSL VPN Bookmarks for Mobile Connect.

Supported Key Features

Supported Key Features by Platform

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

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 215 Series	TZ 210 Series	TZ 205 Series	TZ 200 Series	TZ 105 Series	TZ 100 Series
Active-Active Clustering	✓	✗	✗	✗	✗	✗	✗	✗
Amazon VPC Support	✓	✓[1]	✗	✗	✗	✗	✗	✗
App Rules Enhancement	✓	✓	✓	✓	✓	✗	✓	✗
AppFlow Reports	✓	✓	✓	✓	✗	✗	✗	✗
ArcSight Syslog Format Support	✓	✓	✓	✓	✓	✗	✓	✗
Bandwidth Management Enhancement	✓	✓	✓	✓	✓	✓	✓	✓
BGP Advanced Routing	✓	✓[2]	✓[3]	✗	✗	✗	✗	✗
CLI Enhancements[4]	✓	✓	✓	✓	✓	✓	✓	✓
Client CFS Enforcement	✓	✓	✓	✓	✓	✓	✓	✓
Common Access Card Support	✓	✓	✓	✓	✓	✓	✓	✓
IKE Dead Peer Detection	✓	✓	✓	✓	✓	✓	✓	✓
IKEv2 Configuration Payload Support	✓	✓	✓	✓	✓	✓	✓	✓
IPv6	✓	✓	✓	✓	✓	✗	✓	✗
IPv6 6rd	✓	✓	✓	✓	✓	✗	✓	✗
IPv6 BGP	✓	✓	✓	✓	✓	✗	✓	✗
IPv6 DHCP-PD	✓	✓	✓	✓	✓	✗	✓	✗
IPv6 for Backend Servers	✓	✓	✓	✓	✓	✗	✓	✗
LDAP Group Membership by Organizational Unit	✓	✓	✓	✓	✓	✓	✓	✓

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

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
LDAP User Group Monitoring	✓	✓	✓	✓	✓	✓	✓	✓
Log Monitor Filter Input Box	✓	✓	✓	✓	✓	✓	✓	✓
Logging Enhancement	✓	✓	✓	✓	✓	✓	✓	✓
MOBIKE	✓	✓	✓	✓	✓	✗	✓	✗
NetExtender WXAC Integration	✓	✓	✓	✓	✓	✓	✓	✓
Network Device Protection Profile (NDPP Mode)	✓	✓	✓	✓	✓	✓	✓	✓
Numbered Tunnel Interfaces for Route Based VPN	✓	✓[5]	✗	✗	✗	✗	✗	✗
One-Touch Configuration Overrides	✓	✓	✓	✓	✓	✗	✓	✗
OpenSSH Vulnerability Security Enhancements	✓	✓	✓	✓	✓	✓	✓	✓
Path MTU Discovery	✓	✓	✓	✓	✓	✓	✓	✓
Proxied Users Identification and login	✓	✓	✓	✓	✓	✓	✓	✓
Reassembly-Free Regular Expression for DPI Engine	✓	✓	✓	✓	✓	✗	✓	✗
SHA-2 in IPsec	✓	✓	✓	✓	✓	✓	✓	✓
SNMPv3	✓	✓	✓	✓	✓	✓	✓	✓
SSL VPN Mobile Connect Bookmark	✓	✓	✓	✓	✓	✓	✓	✓
SSL-VPN Multi-Core Scalability	✓	✓	✓	✗	✓	✗	✗	✗
SSO RADIUS Accounting	✓	✓[6]	✗	✗	✗	✗	✗	✗
TSR Enhancements	✓	✓	✓	✓	✓	✓	✓	✓
UDP/ICMP Flood Protection	✓	✓	✓	✓	✓	✗	✓	✗
Wire Mode 2.0	✓	✓[7]	✗	✗	✗	✗	✗	✗
WWAN 4G support	✓	✓	✓	✓	✓	✓	✓	✗

[5] Supported only on NSA 250M and higher models; not supported on NSA 2400MX
[6] Supported only on NSA 3500 and higher models
[7] Supported only on NSA 3500 and higher models

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
XD Lookup for Access Rules	✓	✓	✓	✓	✓	✓	✓	✓
YouTube for Schools Support	✓	✓	✓	✓	✓	✓	✓	✓

Supported SonicPoint and Wireless Features by Platform

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[8]	✗	✓	✓	✓	✓	✓	✓	✓
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	✓	✓[9]	✓	✗	✗	✗	✗	✗
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	✓	✓	✓	✓	✓	✓	✓	✓

[8] Only supported on platforms with internal wireless radio
[9] Not supported on NSA 240

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
Wireless Client Bridge Support[10]	✘	✓	✓	✓	✓	✓	✓	✓
Wireless PCI Rogue detect/prevention	✓	✓	✓	✓	✓	✓	✓	✓
Wireless Radio Built-in Scan Sched[11]	✘	✓	✓	✓	✓	✓	✓	✓

Supported/Unsupported IPv6 Features

The table in this section summarizes the key SonicOS 5.9 features that support IPv6.

To see which appliance platforms support IPv6, refer to the "Supported Key Features by Platform" section.

Features Available with IPv6	Features Not Available with IPv6

• 6to4 tunnel (allows IPv6 nodes to connect to outside IPv6 services over an IPv4 network)
• Access Rules
• Address Objects
• Anti-Spyware
• Application Firewall
• Attack prevention:
  o Land Attack
  o Ping of Death
  o Smurf
  o SYN Flood
• Connection Cache
• Connection Limiting for IPv6 connections
• Connection Monitor
• Content Filtering Service
• DHCP
• DNS client
• DNS lookup and reverse name lookup
• Dynamic Routing (RIPng and OSPFv3)
• EPRT
• EPSV
• FTP
• Gateway Anti-Virus
• High Availability:
  o Connection Cache
  o FTP
  o IPv6 management IP address
  o NDP
  o SonicPoint
• HTTP/HTTPS management over IPv6
• ICMP
• IKEv2
• Intrusion Prevention Service
• IP Spoof Protection
• IPv4 Syslog messages, including messages with
	• Anti-Spam
	• Command Line Interface
	• DHCP over VPN
	• DHCP Relay
	• Dynamic Address Objects for IPv6 addresses
	• Dynamic DNS
	• FQDN
	• Global VPN Client (GVC)
	• GMS
	• H.323
	• High Availability:
	  o Multicast
	  o Oracle SQL/Net
	  o RTSP
	  o VoIP
	• IKEv1
	• IPv6 Syslog messages
	• L2TP
	• LDAP
	• MAC-IP Anti-Spoof
	• NAT between IPv6 and IPv4 addresses
	• NAT High Availability probing
	• NAT load balancing
	• NetBIOS over VPN
	• NTP
	• QoS Mapping
	• RADIUS
	• RAS Multicast Forwarding
	• Route-based VPNs
	• Single Sign On
	• SIP
	• SMTP Real-Time Black List (RBL) Filtering
	• SSH
	• Transparent Mode

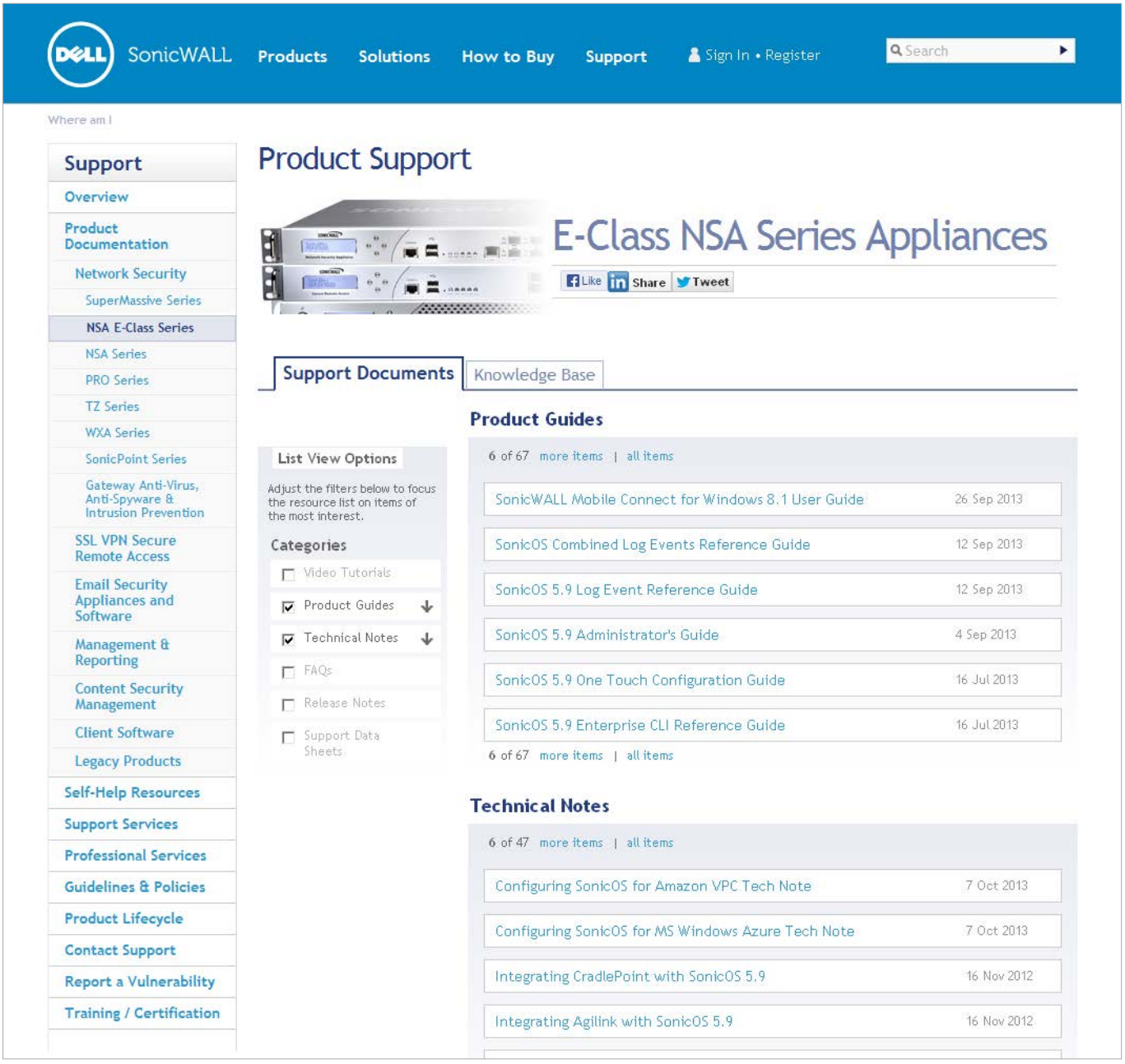
[10] Only supported on platforms with internal wireless radio
[11] Only supported on platforms with internal wireless radio

Features Available with IPv6	Features Not Available with IPv6
IPv6 addresses • IPv6 BGP • IPv6 for Backend Servers • Layer 2 Bridge Mode • Logging IPv6 events • Login uniqueness • Multicast Routing with Multicast Listener Discovery • NAT • Neighbor Discovery Protocol • NetExtender connections for users with IPv6 addresses • Packet Capture • Ping • Policy Based Routing • PPPoE • Remote management • Security services for IPv6 traffic with DPI • Site-to-site IPv6 tunnel with IPsec for security • SonicPoint IPv6 support • SNMP • SSL VPN • Stateful inspection of IPv6 traffic • User status • Visualization • VLAN interfaces with IPv6 addresses • VPN policies • Wireless	• ViewPoint • Virtual Assistant • Web proxy • Wiremode

Related Technical Documentation

Dell SonicWALL user guides and reference documentation are 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.



Last updated: 10/21/2013