

Dell™ SonicWALL™ SonicOS 5.9.1.7

Release Notes

August 2016, updated December 2016

These release notes provide information about the Dell™ SonicWALL™ SonicOS 5.9.1.7 release.

Topics:

- [About SonicOS 5.9.1.7](#)
- [Supported platforms](#)
- [Supported key features in SonicOS 5.9](#)
- [Resolved issues](#)
- [Known issues](#)
- [System compatibility](#)
- [Product licensing](#)
- [Upgrading information](#)
- [Technical support resources](#)
- [About Dell](#)

About SonicOS 5.9.1.7

SonicOS 5.9.1.7 provides all the features that were included in previous releases of SonicOS 5.9.1.x, and provides an option to disable RFC 5961 compliance to manage non-compliant legacy client systems. See issue #173655 in the [Known issues](#) section.

i **NOTE:** On SonicWALL TZ series and some smaller NSA series platforms such as the NSA 220, there might be an effect on performance after upgrading to SonicOS 5.9.1.7. This is due to the large number of features, enhancements, and vulnerability fixes provided in SonicOS 5.9, as compared to the SonicOS 5.8 releases. These features and updates are essential to better secure your network.

For more information about other releases, see the previous release notes, available on MySonicWALL or on the Support Portal at: <https://support.software.dell.com/release-notes-product-select>.

Supported platforms

The SonicOS 5.9.1.7 release is supported on the following Dell SonicWALL network security platforms:

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

Supported key features in SonicOS 5.9

See the tables in the following sections for supported feature information:

- [Supported key features by platform](#)
- [Supported SonicPoint and wireless features by platform](#)
- [Supported/unsupported IPv6 features](#)

Supported key features by platform

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

Table 1. Supported key 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	SOHO Series
Active-Active Clustering	Y	N	N	N	N	N	N	N	N
Amazon VPC Support ¹	Y	Y	Y	Y	Y	Y	Y	Y	Y
Guest Admin Support	Y	Y	Y	Y	Y	N	Y	N	Y

¹ Amazon VPC VPN connection using static routing is supported for all platforms. Amazon VPC VPN connection using dynamic routing is supported only on platforms that support BGP.

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	SOHO Series
App Rules Enhancement	Y	Y	Y	Y	Y	N	Y	N	Y
AppFlow Reports	Y	Y	Y	Y	N	N	N	N	N
ArcSight Syslog Format Support	Y	Y	Y	Y	Y	N	Y	N	Y
Bandwidth Management Enhancement	Y	Y	Y	Y	Y	Y	Y	Y	Y
BGP Advanced Routing	Y	Y ²	Y ³	N	N	N	N	N	N
CLI Enhancements ⁴	Y	Y	Y	Y	Y	Y	Y	Y	Y
Client CFS Enforcement	Y	Y	Y	Y	Y	Y	Y	Y	Y
Common Access Card Support	Y	Y	Y	Y	Y	Y	Y	Y	Y
Guest Admin Support	Y	Y	Y	Y	Y	N	Y	N	Y
IKE Dead Peer Detection	Y	Y	Y	Y	Y	Y	Y	Y	Y
IKEv2 Configuration Payload Support	Y	Y	Y	Y	Y	Y	Y	Y	Y
IPv6	Y	Y	Y	Y	Y	N	Y	N	Y
IPv6 6rd	Y	Y	Y	Y	Y	N	Y	N	Y
IPv6 BGP	Y	Y	Y	Y	Y	N	Y	N	Y
IPv6 DHCP-PD	Y	Y	Y	Y	Y	N	Y	N	Y
IPv6 for Backend Servers	Y	Y	Y	Y	Y	N	Y	N	Y
LDAP Group Membership by Organizational Unit	Y	Y	Y	Y	Y	Y	Y	Y	Y
LDAP User Group Monitoring	Y	Y	Y	Y	Y	Y	Y	Y	Y
Log Monitor Filter Input Box	Y	Y	Y	Y	Y	Y	Y	Y	Y

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

³ Requires a 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	SOHO Series
Logging Enhancement	Y	Y	Y	Y	Y	Y	Y	Y	Y
MOBIKE	Y	Y	Y	Y	Y	N	Y	N	Y
NetExtender WXAC Integration	Y	Y	Y	Y	Y	Y	Y	Y	Y
Network Device Protection Profile (NDPP Mode)	Y	Y	Y	Y	Y	Y	Y	Y	Y
Numbered Tunnel Interfaces for Route Based VPN	Y	Y ⁵	N	N	N	N	N	N	N
One-Touch Configuration Overrides	Y	Y	Y	Y	Y	N	Y	N	Y
OpenSSH Vulnerability Security Enhancements	Y	Y	Y	Y	Y	Y	Y	Y	Y
Path MTU Discovery	Y	Y	Y	Y	Y	Y	Y	Y	Y
Proxied Users Identification and login	Y	Y	Y	Y	Y	Y	Y	Y	Y
Reassembly-Free Regular Expression for DPI Engine	Y	Y	Y	Y	Y	N	Y	N	Y
SHA-2 in IPsec	Y	Y	Y	Y	Y	Y	Y	Y	Y
SNMPv3	Y	Y	Y	Y	Y	Y	Y	Y	Y
SSL VPN Mobile Connect Bookmark	Y	Y	Y	Y	Y	Y	Y	Y	Y
SSL-VPN Multi-Core Scalability	Y	Y	Y	N	Y	N	N	N	Y
SSO RADIUS Accounting	Y	Y ⁶	N	N	N	N	N	N	N

⁵ Supported only on NSA 250M and higher models; not supported on NSA 2400MX.

⁶ 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	SOHO Series
TSR Enhancements	Y	Y	Y	Y	Y	Y	Y	Y	Y
UDP/ICMP Flood Protection	Y	Y	Y	Y	Y	N	Y	N	Y
Wire Mode 2.0	Y	Y ⁷	N	N	N	N	N	N	N
WWAN 4G support	Y	Y	Y	Y	Y	Y	Y	N	Y
XD Lookup for Access Rules	Y	Y	Y	Y	Y	Y	Y	Y	Y
XD Lookup for Access Rules	Y	Y	Y	Y	Y	Y	Y	Y	Y

Supported SonicPoint and wireless features by platform

Table 4. Supported key 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	SOHO Series
External Guest Service Apache / PHP support	Y	Y	Y	Y	Y	Y	Y	Y	Y
External Guest Service FQDN support	Y	Y	Y	Y	Y	Y	Y	Y	Y
Internal Radio IDS scan scheduling ⁸	N	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint 802.11e (WMM) QoS	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint Auto Provisioning	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint retain custom configuration	Y	Y	Y	Y	Y	Y	Y	Y	Y

⁷ Supported only on NSA 3500 and higher models

⁸ Only supported on platforms with internal wireless radio

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	SOHO Series
SonicPoint DFS support	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint Diagnostics Enhancement	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint FairNet Support	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint RADIUS Server Failover	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint WPA TKIP Countermeasures and MIC Failure Flooding Detection and Protection	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint Layer 3 Management	Y	Y ⁹	Y	N	N	N	N	N	N
Traffic Quota-based Guest Svc Policy	Y	Y	Y	Y	Y	Y	Y	Y	Y
Virtual Access Point ACL Support	Y	Y	Y	Y	Y	Y	Y	Y	Y
Virtual Access Point ACL Support	Y	Y	Y	Y	Y	Y	Y	Y	Y
Virtual Access Point Layer 2 bridging	Y	Y	Y	Y	Y	Y	Y	Y	Y
Virtual Access Point scheduling	Y	Y	Y	Y	Y	Y	Y	Y	Y
Wireless Client Bridge Support ¹⁰	N	Y	Y	Y	Y	Y	Y	Y	Y
Wireless PCI Rogue detect / prevention	Y	Y	Y	Y	Y	Y	Y	Y	Y
Wireless Radio Built-in Scan Sched ¹¹	N	Y	Y	Y	Y	Y	Y	Y	Y

⁹ Not supported on NSA 240.

¹⁰ Only supported on platforms with internal wireless radio.

¹¹ Only supported on platforms with internal wireless radio.

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.

Table 5. IPv6 features

Features Available with IPv6	Features Not Available with IPv6
<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Land Attack • Ping of Death • Smurf • 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: <ul style="list-style-type: none"> • Connection Cache • FTP • IPv6 management IP address • NDP • SonicPoint • HTTP/HTTPS management over IPv6 • ICMP • IKEv2 • Intrusion Prevention Service • IP Spoof Protection • IPv4 Syslog messages, including messages with IPv6 addresses • IPv6 BGP • IPv6 for Backend Servers • Layer 2 Bridge Mode • Logging IPv6 events 	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Multicast • Oracle SQL/Net • RTSP • VoIP • IKEv1 • IPv6 Syslog messages • L2TP • LDAP • MAC-IP Anti-Spoof • NAT between IPv6 and IPv4 addresses • NAT High Availability probing • NetBIOS over VPN • NTP • QoS Mapping • RADIUS • RAS Multicast Forwarding • Route-based VPNs • Single Sign On • SIP • SMTP Real-Time Black List (RBL) Filtering • SSH • Transparent Mode • ViewPoint • Virtual Assistant • Web proxy

Features Available with IPv6

Features Not Available with IPv6

- Login uniqueness
- Multicast Routing with Multicast Listener Discovery
- NAT
- NAT load balancing
- 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
- WireMode

Resolved issues

This section describes an issue that is resolved in this release.

Networking

Resolved issue	Issue ID
<p>CPU utilization increases to greater than 90% after upgrading without any changes to the configuration settings. On a NSA E8510, data processing cores 2-15 show the CPU utilization at 90%, while on core 1 it stays lower, such as 15%.</p> <p>Occurs when the firewall is upgraded to SonicOS 5.9.1.6 with flood protection enabled, including the Always allow DELL SonicWALL management traffic option. In SonicOS 5.9.1.5 and 5.9.1.6, enhancements to flood protection for a better detection rate and protection control can result in thousands of TCP Resets (an RST flood).</p>	171624

Known issues

The following is a list of known issues in this release.

3G/4G

Known issue	Issue ID
The 3G/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 Wireless 3G/4G device is connected without an external antenna. Thus, it is only able to negotiate HSPA+ traffic when using an external antenna to negotiate with the faster LTE network.	133999

AppFlow

Known issue	Issue ID
The Create Rule option on the Users tab in Dashboard > AppFlow Monitor does not work correctly, and log messages are displayed on the console. Occurs when attempting to create a rule for a RADIUS user to block LAN to WAN access, when the user already belongs to a group that has LAN to WAN access.	167772
SSL VPN users are not displayed in Dashboard > AppFlow Monitor on the Users tab, only “unknown” users are shown. Occurs when several (10) SSL VPN users are connected to the firewall and AppFlow Reporting is enabled.	167149
IPv6 applications are not displayed in the AppFlow Monitor page. Occurs when some IPv6 streams have been triggered by visiting certain websites.	166912
The Dashboard > AppFlow Reports page does not display any entries on the Applications tab. Occurs when Flow Reporting , Real-Time Data Collection , and AppFlow To Local Collector are enabled, and some HTTP/FTP/ICMP connections are made on the LAN side. AppFlow Monitor shows some sessions.	164502

Application Control

Known issue	Issue ID
The App Rule Match Object cannot match a filename. Occurs during an FTP download or upload and the Match Type of the Firewall > Match Object is set to Prefix Match , the Input Representation is set to Hexadecimal Representation , and the Enable Negative Matching option is selected. Workaround: Do not enable the Negative Matching option with the Prefix Match option.	135634
App Control policies do not block IPv6 traffic unless Intrusion Prevention Service 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

Command Line Interface

Known issue	Issue ID
The CLI incorrectly indicates that Gateway Anti-Virus is not licensed. Occurs when using the <code>show status</code> CLI command while GAV is licensed on the appliance.	160800
Access Rules are not removed on the Backup device of an HA pair and further configuration is not synchronized with the Backup device. Occurs when the <code>access-rule restore-defaults</code> CLI command is issued.	141949

DPI-SSL

Known issue	Issue ID
The SSL proxied connection count cannot be cleared from the cache. Occurs when Client DPI-SSL is enabled and HTTPS traffic is passed through X0 and X2 which are configured in Layer 2 Bridge mode, and then X0 and X2 are changed to unassigned mode.	159332
The certificate from a secure website, such as <code>https://mail.google.com</code> , 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 are enabled on the WLAN zone, a wireless client connects to the SonicPoint, and the user logs into the guest account.	123097

IPv6

Known issue	Issue ID
A 6rd tunnel (IPv6 rapid deployment tunnel) is unexpectedly reported as UP although there is no available 6rd prefix. Occurs when the tunnel was previously UP and using DHCP mode, and then the DHCP server is disabled and the firewall is rebooted.	157034
IPv6 traffic that is sent over a 6rd interface is not forwarded. Occurs after rebooting the firewall. Workaround: Go to the Network > Interfaces page, open the Edit Interface dialog for the 6rd interface, and click OK without making any changes. Traffic will be forwarded after that.	143079
IPv6 packets exceeding the Maximum Transmission Unit (MTU) are dropped instead of being fragmented. Occurs when setting the MTU for an interface, and then sending IPv6 packets that exceed the MTU.	139108
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 in the Exclusion Address list of an App Rule policy tries to connect to an IPv6 website that is blocked by that policy.	128363

Known issue

Issue ID

The firewall has high CPU saturation and does not close connections, resulting in RST floods which are shown in the logs.

173655

Occurs when processing traffic from clients or servers which are not compliant with [RFC 5961](#), resulting in unusual TCP behaviors. The CPU saturation and logged RST floods are expected behaviors when protecting against vulnerability [CVE-2004-0230](#), as mandated by IETF [RFC 5961](#) to stop spoofed off-path TCP packet injection attacks. If connected client/server devices comply with RFC 5961, the firewall will not experience this issue.

Workaround: SonicOS 5.9.1.7 provides the following workaround for environments with legacy clients or servers that do not comply with [RFC 5961](#):

The ability to enable or disable enforcement of RFC 5961 compliance is added in SonicOS 5.9.1.7 in the **Firewall Settings > Flood Protection** page. The **Enforce strict TCP compliance with RFC 5961** option is enabled (checked) by default to enforce strict RFC 5961 compliance, but customers using legacy clients can disable (uncheck) it to turn off compliance.

CAUTION: Disabling this option is not recommended, as it can leave your network open to TCP packet injection attacks.

The screenshot shows the SonicWALL Network Security Appliance interface. The left sidebar contains navigation options: Dashboard, System, Network, 3G/4G/Modem, Wireless, SonicPoint, Firewall, Firewall Settings (expanded), Advanced, BWM, Flood Protection (selected), Multicast, QoS Mapping, SSL Control, DPI-SSL, VoIP, and Anti-Spam. The main content area is titled 'Firewall Settings / Flood Protection'. At the top, there are 'Accept' and 'Cancel' buttons. Below is the 'TCP Settings' section with the following options:

- Enforce strict TCP compliance with RFC 793, RFC 1122 and RFC 1323
 - Enable TCP handshake enforcement
 - Enforce strict TCP compliance with RFC 5961**
 - Enable TCP checksum enforcement
 - Drop TCP SYN packet with data
 - Enable TCP handshake timeout
 - TCP Handshake Timeout (seconds):
 - Default TCP Connection Timeout (minutes):
 - Maximum Segment Lifetime (seconds):

If your client devices comply with RFC 5961, leave the **Enforce strict TCP compliance with RFC 5961** option enabled.

If your client devices do not comply with RFC 5961 and your firewall is experiencing RST floods, you can disable the **Enforce strict TCP compliance with RFC 5961** option.

Changing the X1 interface from PPTP mode to static mode causes X1 to become inaccessible and changes its IP address to 0.0.0.0.

160164

Occurs when the X1 interface has obtained an IP address in PPTP mode and then the administrator reconfigures X1 in static mode and gives it a static IP address.

Workaround: Restart the firewall to make X1 accessible again.

Known issue	Issue ID
The WAN interface cannot be accessed with HTTPS or ping after restarting the firewall. Occurs when X0 (LAN) has a redundant port configured and X0 physical status is “no link”.	156619
The default route gateway is wrong after changing the WAN mode. Occurs when X1 is configured with IP Assignment in L2TP mode, then changed to PPTP mode, but the default route gateway is still the one learned from the L2TP server. After changing the WAN mode back to L2TP, the default route gateway is the one learned from the PPTP server.	154144
The paired interface does not go down when the other interface in the Wire Mode pair is brought down. Occurs when the Enable Link State Propagation option is enabled and a wire mode interface is brought down by performing a shutdown on the peer switch.	151827
There is no option to originate a default route for dynamic IPv6 routing via OSPFv3. Occurs when configuring OSPFv3 from the Network > Routing page. IPv6 default route origination via OSPFv3 is currently not supported.	150771
Disabling one DHCPv6 client also disables another DHCPv6 client. Occurs when both X1 and X2 are configured to DHCPv6 automatic mode, and then X1 is changed to static mode.	147542
Packets cannot pass through the Wire mode pair. Occurs when the destination link-local IPv6 address is the same as the Wire mode interface address.	144385
The default gateway cannot be configured. Occurs when X2 is configured as a WAN interface and the IP assignment is set to static.	141973
IPv6 NAT policies are not removed from the firewall as expected. Occurs when all the IPV6 custom policies have been deleted and the firewall is restarted.	141530
The Gateway Anti-Virus (GAV) may not work in IPv6 Wiremode > Secure mode. Occurs when using Wiremode > Secure mode with GAV enabled globally and per zone.	139250
Border Gateway Protocol (BGP) authentication does not work with IPv6 peers. Occurs when configuring an IPv6 peer between a firewall and a router, then enabling BGP authentication on each side.	138888

Security Services

Known issue	Issue ID
Excluding users for an individual Intrusion Prevention signature does not work as expected. Occurs when Security Services > Intrusion Prevention is enabled for all signatures, and IPS is also enabled for the WAN and LAN zones, and then the administrator configures a user in Excluded Users/Groups for a particular signature ID. When traffic containing that signature is sent by that user from the WAN side to a computer on the LAN, the log shows that the traffic was blocked by IPS and the user’s name appears in the log.	160458
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

SSL VPN

Known issue	Issue ID
SSLVPN Enforcement on the WLAN zone redirects users to the SSL VPN portal logon page, but the logon page does not open. Occurs when browsing any HTTP website from a WLAN client machine.	161300

System

Known issue	Issue ID
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
Dell SonicWALL GMS 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 the firewall 10GE interface.	121657

User Interface

Known issue	Issue ID
The Latest Alerts section of the System > Status page does not display any alerts. Occurs when interfaces are enabled or disabled, or when other events occur that are known to cause alerts.	160868
The hyperlink in “Click here for UTM management” does not work. Occurs when logged into the IPv6 address of the SSL VPN Virtual Office portal.	157523

VoIP

Known issue	Issue ID
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

Known issue	Issue ID
A client behind the central firewall can ping a LAN device behind the remote firewall even though the device is in the “excluded LAN devices” table. Occurs when the remote firewall is configured to use DHCP over VPN and the LAN device is first configured as a “static device on LAN” on the remote firewall and then added to the “excluded LAN devices” table.	166617

Known issue	Issue ID
<p>VPN negotiation fails and the log for the Initiator does not have an entry showing "IKEv2 negotiation complete".</p> <p>Occurs when the VPN policy is bound to an interface other than the interface for the default route. Observed when the VPN policy is bound to an IPv6 address on both ends.</p>	148167
<p>Traffic goes to the wrong VPN tunnel.</p> <p>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.</p> <p>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.</p>	135205
<p>An active IPv6 VPN tunnel is not displayed in the table on the VPN > Settings page of the head-end firewall.</p> <p>Occurs when two IPv6 VPN tunnels are created on both the head-end appliance and a remote appliance. The head-end VPN > Settings page shows "2 Currently Active IPv6 Tunnels", but it only displays one tunnel in the Currently Active VPN Tunnels table.</p>	128633
<p>An OSPF connection cannot be established between an NSA 240 and an NSA 7500.</p> <p>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.</p>	128419

System compatibility

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

Wireless 3G/4G broadband devices

SonicOS 5.9.1.6 provides support for a wide variety of PC cards, USB devices and wireless service providers. For the most recent list of supported devices, see <http://www.sonicwall.com/supported-wireless-broadband-cards-devices/>.

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.

GMS support

Dell SonicWALL Global Management System (GMS) 7.2 Service Pack 5 (or higher 7.2) or GMS 8.1 (or higher) are required for GMS management of Dell SonicWALL SOHO appliances running SonicOS 5.9.1.7.

WXA support

The Dell SonicWALL WXA series appliances (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are supported for use with Dell SonicWALL security appliances running SonicOS 5.9.1.7. The recommended firmware version for the WXA series appliances is WXA 1.3.2.

Browser support

SonicOS with Visualization uses advanced browser technologies such as HTML5, which are supported in most recent browsers. 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 9.0 and higher (do not use compatibility mode)
- Safari 5.0 and higher running on non-Windows machines

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

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

Product licensing

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

A number of security services are separately licensed features in SonicOS. When a service is licensed, full access to the functionality is available. SonicOS periodically checks the license status with the SonicWALL License Manager. The System > Status page displays the license status for each security service.

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 at <https://mysonicwall.com/> or on the Support portal at <https://support.software.dell.com/>.

IMPORTANT: If VPN tunnel interfaces are configured on your appliance running SonicOS 5.8, be sure to read the “Upgrading caveats for VPN tunnel interfaces” section in the *SonicOS 5.9 Upgrade Guide* before upgrading your appliance to SonicOS 5.9.

NOTE: On SonicWALL TZ series and some smaller NSA series platforms such as the NSA 220, there might be an effect on performance after upgrading to SonicOS 5.9.1.7. This is due to the large number of features, enhancements, and vulnerability fixes provided in SonicOS 5.9, as compared to the SonicOS 5.8 releases. These features and updates are essential to better secure your network.

Technical support resources

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

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system. To access the Support Portal, go to <http://support.software.dell.com>.

The Support Portal enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles at:
<https://support.software.dell.com/kb-product-select>
- Obtain product notifications
- View how-to videos at:
<https://support.software.dell.com/videos-product-select>
- Engage in community discussions

SonicOS Administration Guides and related documents are available on the Dell Software Support site at <https://support.software.dell.com/release-notes-product-select>.

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit <http://www.software.dell.com>.

Contacting Dell

For sales or other inquiries, visit <http://software.dell.com/company/contact-us.aspx> or call 1-949-754-8000.

Copyright 2016 Dell Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. Dell™, the Dell logo, and SonicWALL are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

For more information, go to <http://software.dell.com/legal/>.

Legend



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



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



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

Last updated: 12/14/2016

232-003354-00 Rev D