Release Notes

SonicOS | **SonicOS 5.9.0.4 Release Notes**

Contents

Release Purpose

SonicOS 5.9.0.4 provides several new features and resolves a number of issues found in earlier releases.

This release provides the same features and contains the same resolved issues as previous releases of SonicOS 5.9.0.x. For more information, see the previous release notes:

SonicOS 5.9.0.3 Release Notes	http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=RN&id=554
SonicOS 5.9.0.2 Release Notes	http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=RN&id=539
SonicOS 5.9.0.1 Release Notes	http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=RN&id=531
SonicOS 5.9.0.0 Release Notes	http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=RN&id=514

Platform Compatibility

The SonicOS 5.9.0.4 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 6000 Software, 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 WXA 1.3.0.

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 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)

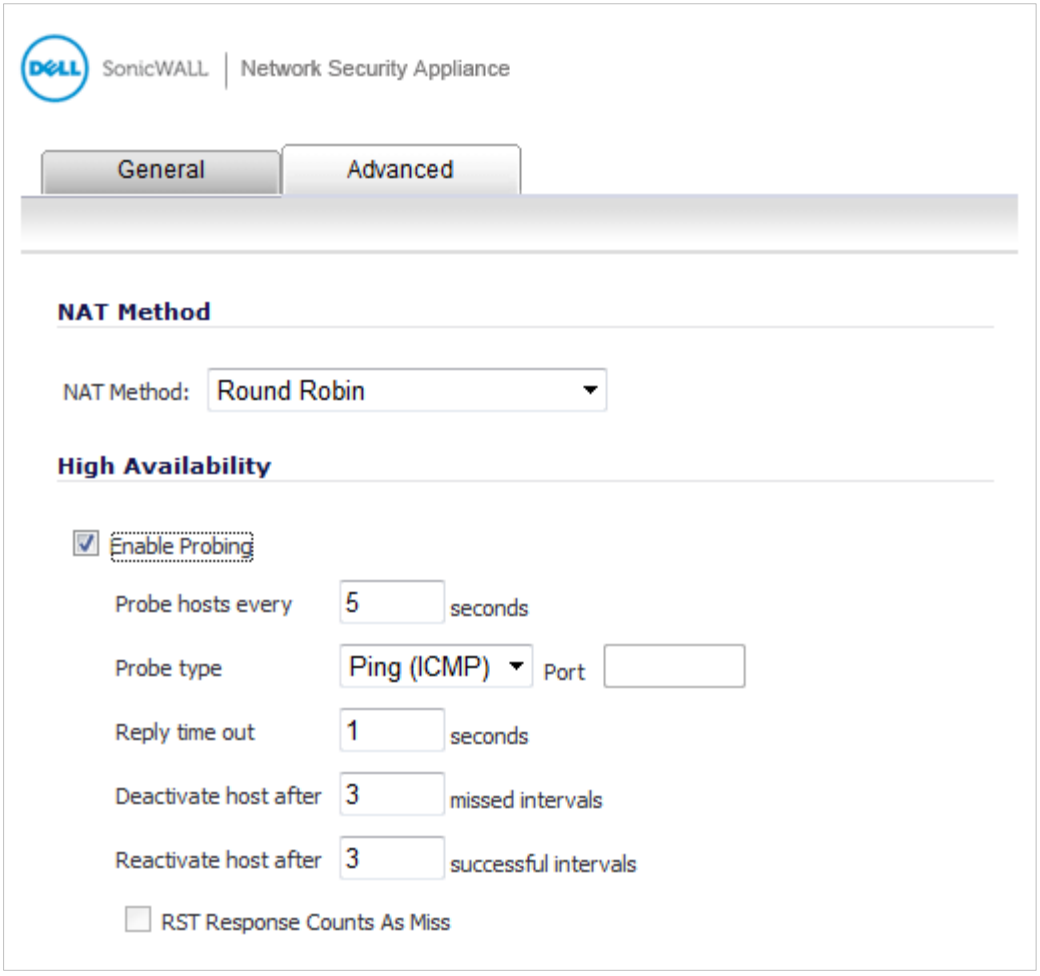
Note: When connected to a Dell SonicWALL appliance, the performance and data throughput of most 3G/4G devices will be lower than when the device is connected directly to a personal computer. SonicOS uses the PPP interface rather than the proprietary interface for these devices. The performance is comparable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

New Features in SonicOS 5.9.0.4

SonicOS 5.9.0.4 provides the following new features and enhancements:

IPv6 NAT Load Balancing

Support for IPv6 Network Address Translation (NAT) Load Balancing is integrated into SonicOS 5.9.0.4, balancing incoming IPv6 traffic across multiple, similar network resources. The IPv6 NAT Load Balancing methods (Sticky IP, Round Robin, Block Remap/Symmetrical Remap, Random Distribution) are configured in the “Advanced” tab of the NAT Polices configuration window:



Content Filtering – Removal of Category 42 (LGBT Rating)

Beginning in SonicOS 5.9.0.4, the Dell SonicWALL Content Filtering Service (CFS) no longer uses Category 42 as a rating for any websites. In previous releases, Category 42 was applied to websites with content relating to lesbian, gay, bisexual, or transgender (LGBT) topics.

These websites now receive an appropriate rating based on their content without consideration of any implied or explicit sexual orientation within the content. This policy is in accordance with ratings applied to other websites which contain gender based content, but are not categorized as “male” or “female”, for example.

For a list of the current Content Filtering Categories, refer to the following link:
http://www.sonicwall.com/us/en/products/Network_Security_Content_Filtering_Categories.html

Note: Upon upgrading to SonicOS 5.9.0.4, all CFS policies should be audited to ensure that the intended access restrictions are configured using the available categories.

Windows NetExtender 7.5.215

SonicOS 5.9.0.4 is supported to work with Windows operating systems using NetExtender 7.5.215.

Additional Signatures for TZ 105/105W

The large on-board signature base for the Security Services > Gateway Anti-Virus service is supported on the TZ 105 series.

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]	✗	✗	✗	✗	✗

[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

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
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	✓	✓	✓	✓	✓	✓	✓	✓
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	✓	✓	✓	✓	✓	✓	✓	✓

[4] Limited CLI command set is supported on NSA 240 and all TZ models
[5] Supported only on NSA 250M and higher models; not supported on NSA 2400MX

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 215 Series	TZ 210 Series	TZ 205 Series	TZ 200 Series	TZ 105 Series	TZ 100 Series
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	✓	✓	✓	✓	✓	✓	✓	✗
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	✓	✓	✓	✓	✓	✓	✓	✓

[6] Supported only on NSA 3500 and higher models
[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
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	✓	✓	✓	✓	✓	✓	✓	✓
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 5.9.0.4 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
	• 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

[9] Not supported on NSA 240
[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
• Connection Limiting for IPv6 connections • Connection Monitor • Content Filtering Service • DHCP • DNS client • DNS lookup and reverse name lookup • Dynamic Routing (RIPng and OSPFv3) • EPRT • EPSV • FTP • Gateway Anti-Virus • High Availability: o Connection Cache o FTP o IPv6 management IP address o NDP o SonicPoint • HTTP/HTTPS management over IPv6 • ICMP • IKEv2 • Intrusion Prevention Service • IP Spoof Protection • IPv4 Syslog messages, including messages with IPv6 addresses • IPv6 BGP • IPv6 for Backend Servers • Layer 2 Bridge Mode • Logging IPv6 events • 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	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 • 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

Known Issues

This section contains a list of known issues in the SonicOS 5.9.0.4 release.

3G/4G

Symptom	Condition / Workaround	Issue
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. For information on supported 3G/4G devices, refer to http://www.sonicwall.com/us/products/3190.html.	133999
The firewall shuts down or restarts automatically when a 3G/4G USB device is inserted or removed.	Occurs when inserting or removing a 3G/4G USB device 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. For information on supported 3G/4G devices, refer to http://www.sonicwall.com/us/products/3190.html.	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

Application Firewall

Symptom	Condition / Workaround	Issue
An application is blocked by the firewall even though the client IP address is in the “excluded IP address range” list.	Occurs when App Control is enabled and excluded traffic is sent through the firewall.	139176

CLI

Symptom	Condition / Workaround	Issue
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 access-rule restore-defaults CLI command is issued.	141949

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 are enabled on the WLAN zone, a wireless client connects to the SonicPoint, and the user logs into the guest account.	123097

Firewall

Symptom	Condition / Workaround	Issue
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

IPv6

Symptom	Condition / Workaround	Issue
IPv6 traffic that is sent over a 6rd interface is not forwarded.	Occurs after rebooting the firewall. **Workaround:** Go to the Network > Interfaces page and open the Edit Interface dialog for the 6rd interface and click OK without making any changes. Traffic should 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

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.	131932

Networking

Symptom	Condition / Workaround	Issue
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
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.	143144
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
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
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
A Web browser is automatically redirected the X1 WAN IP address of the SonicOS appliance instead of the X0 LAN IP address.	Occurs after a firmware upgrade when logging into the SonicOS appliance from the LAN zone.	140351
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 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

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
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

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

Resolved Issues

This section contains a list of issues that are fixed in the SonicOS 5.9.0.4 release.

CLI

Symptom	Condition / Workaround	Issue
The LDAP server configuration does not take effect.	Occurs when LDAP is configured in the command line interface after the firewall is booted with factory default settings.	140347

DPI-SSL

Symptom	Condition / Workaround	Issue
The “Web Page to Display when Blocking” that is provided on the Security Services > Content Filter page does not display when https websites are blocked.	Occurs when the “Enable SSL Client Inspection” option is enabled on the DPI-SSL > Client SSL page.	123676
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
Firewall becomes unresponsive, but returns to normal status after about one minute.	Occurs when the App Rule policy is changed, such as when a new Match Object is added.	140758
An App Rule policy is not enforced.	Occurs when the Match Object Type is Regex and the “Enable Negative Matching” option is selected in the Match Object dialog.	140245

GMS

Symptom	Condition / Workaround	Issue
Dell SonicWALL Global Management System cannot manage the firewall after upgrading.	Occurs when GMS is using the HTTPS Management method and the SonicOS appliance has WAN HTTPS Management disabled on the WAN interface.	139012

IPv6

Symptom	Condition / Workaround	Issue
IPv6 LAN and WAN packets are dropped by the firewall.	Occurs when the “Drop and log network packets whose source or destination address is reserved by RFC” option is selected on the Firewall Settings > Advanced page, under IPv6 Advanced Configurations.	143636
An IPv6 6rd interface cannot be deleted.	Occurs when manually adding an IPv6 6rd interface, and then trying to delete it.	138846

Networking

Symptom	Condition / Workaround	Issue
Dynamic DNS cannot connect to Dyn.com and reports a network error.	Occurs when configuring a DDNS profile to connect to Dyn.com with a free or paid account. The resolution includes adding the CyberTrust Root CA to the built-in certificate store.	144737
The secondary interface of an L2 Bridge cannot be configured.	Occurs when the “Disable all IPv6 Traffic on the Interface” option is enabled on the Network > Interfaces page, in the Edit dialog, under the Advanced tab.	141322
The IP assignment for the IPv6 X0 interface is changed from Static to Auto.	Occurs when the Release or Renew button is clicked for the X1 (DHCPv6) interface.	135871
The PPPOE connection becomes unstable and displays these error messages in the logs: • PPPOE Terminated • PPPOE Network Disconnected • PPPOE Client: Previous session was connected for 30 seconds • PPPOE LCP Link Down	Occurs when the firewall is rebooted with factory default settings.	134413
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

SSL VPN

Symptom	Condition / Workaround	Issue
NetExtender cannot connect to an external network.	Occurs when Tunnel All Mode is enabled on the SSL VPN > Client Settings page in the Edit Device Profile dialog under Client Routes, and the WAN RemoteAccess Networks option is added to Client Routes.	142003
The Tech Support Report (TSR) shows that SSL VPN licenses are being used when no users are logged in.	Occurs when users log in using Mobile Connect and then become inactive. Users are logged out on the mobile device but not on the firewall.	138063

Security Services

Symptom	Condition / Workaround	Issue
The System > Licenses page shows that the Kasperky Anti-Virus service is licensed, but the System > Status page does not show that the Kasperky Anti-Virus service is available.	Occurs when the firewall has been upgraded and booted to the factory default settings and the license registrations have been updated.	143105
The Secondary server does not become active when the Primary server becomes inactive.	Occurs when the Enable CFS Server Failover option is enabled in the Configure CFS dialog.	140433
Website browsing is very slow and has decreased throughput.	Occurs when CFS is enabled and the firewall is upgraded and rebooted. **Workaround:** Disable CFS on the firewall.	139807

SonicPoint

Symptom	Condition / Workaround	Issue
SonicPoints cannot get their configuration updates.	Occurs when a failover happens in a High Availability pair.	141105

System

Symptom	Condition / Workaround	Issue
IPv6 NAT configurations are changed, added, and deleted, and Access Rules are added.	Occurs after a reboot if there is an interface configured with a prefix length of 112. 113621 **Workaround:** Do not configure an interface with a prefix length of 112.	140884
A SonicOS appliance configured for use with the SNMP agent does not respond with proper interface data	Occurs when the SNMP agent does a query to the SonicOS appliance with "Getbulk Request Ifname".	140343
A 6 to 4 Auto Tunnel is not shown on the Network > Routing page in the Route Policies panel as it should be.	Occurs after rebooting the firewall with factory default settings and then importing the preferences. When trying to configure another Auto Tunnel, an error is displayed stating that only one Auto Tunnel is allowed. The routing table shows that a previous Auto Tunnel exists, but that it is bound to unknown.	140302

User Interface

Symptom	Condition / Workaround	Issue
The SonicOS management interface is slow to respond, or does not respond for a brief period of time.	Occurs when the WebListener task is in a loop waiting for more SSL data until it eventually times out. During this period, the tWebListen task may take 100% of the CPU time. **Note**: As a best practice, configure Access Control of the management interface on the WAN.	144909

Users

Symptom	Condition / Workaround	Issue
Two-factor authentication does not work on the firewall.	Occurs when two-factor authentication is used with a Dell Defender RADIUS server (RADIUS Access-Challenge).	141501
Inactive users are not being logged out after the time period that is specified by the "Age out inactive users after (minutes):" option on the Users > Settings page.	Occurs when SSO authenticated users have become inactive, but are not logged out yet.	140342
The firewall displays this message: "Recording error with no display string: err -1 module 1!"	Occurs when a pending SSO attempt is aborted due to a user deletion not being in sync.	139730
The user password cannot be changed on the System > Administration page.	Occurs when the password is set on the System > Administration page and special characters, such as ~!@#$%^&*()_+<>? , are used, and then the administrator, after logging out and logging back in, attempts to change the password to something different.	125369

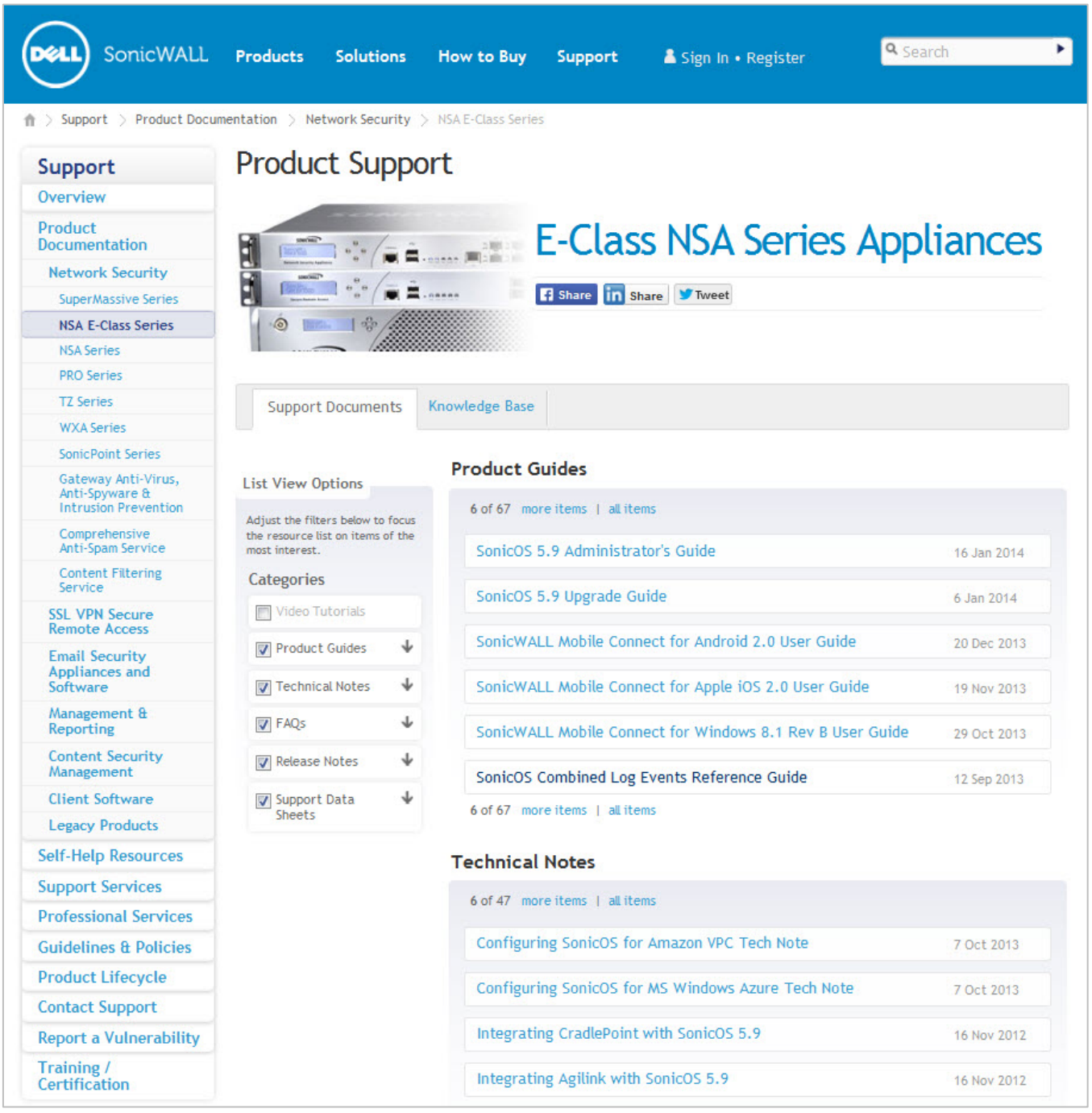
VPN

Symptom	Condition / Workaround	Issue
Clients on the remote gateway side of the VPN cannot access the network on the central gateway side of the VPN.	Occurs when the "Use this VPN Tunnel as default route for all Internet traffic" option is selected in the VPN Policy dialog of the VPN > Settings page, under the Network tab.	141183
The "Permit Acceleration" option in the Advanced tab of the VPN policy dialog is grayed out and cannot be selected.	Occurs when attempting to configure a VPN Policy after the firewall has been rebooted with factory default settings.	140501
The firewall generates a “Delete IPSec SA” when establishing a VPN.	Occurs when a site-to-site VPN is established, and then one of the sites is replaced with a different model firewall. **Workaround:** Disable the keepalive function on one of the two sites.	139456

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: 5/7/2014