



Dell SonicWALL™ SonicOS 5.9.1.5

Release Notes

December 2015, revised: January 2015

These release notes provide information about the Dell SonicWALL™ SonicOS 5.9.1.5 release.

- [About SonicOS 5.9.1.5](#)
- [Supported platforms](#)
- [Resolved Issues](#)
- [Known issues](#)
- [System compatibility](#)
- [Product licensing](#)
- [Upgrading information](#)
- [Technical support resources](#)
- [About Dell](#)

About SonicOS 5.9.1.5

SonicOS 5.9.1.5 is a maintenance release for the Dell SonicWALL network security appliances. A number of issues from previous releases are fixed in this release. See [Resolved Issues](#).

This release provides all the features and contains all the resolved issues that were included in previous releases of SonicOS 5.9.1.x. For more information, 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 5.9.1.5 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 | | | |

Resolved Issues

The following is a list of issues that are resolved in this release.

Application Control

| Resolved issue | Issue ID |
|---|----------|
| Traffic matching a regex (regular expression) is not blocked in some cases. Occurs when the regex uses any port rules when regex is also used in a specific port rule. For example: <ul style="list-style-type: none">• Create a rule with a regex for port 80 traffic.• Create a rule with a regex for any port traffic.• Pass traffic matching any of the above regexes. | 149448 |

Command Line Interface

| Resolved issue | Issue ID |
|--|----------|
| The “access-rule” CLI command does not exist in SonicOS 5.9 on some platforms, but exists on those platforms in SonicOS 5.8.1.15. Occurs when attempting to use the CLI to create access rules on a TZ 100/100W or 200/200W running SonicOS 5.9.0.x or 5.9.1.x. | 152394 |

Dashboard

| Resolved issue | Issue ID |
|---|----------|
| A scheduled AppFlow report sent to the FTP server is empty. Occurs when “Send Report by E-mail” is enabled together with “Send Report by FTP”. | 156817 |

DPI-SSL

| Resolved issue | Issue ID |
|--|----------|
| Server DPI-SSL does not block email with a malicious file attachment over SMTPS. Occurs when the SMTPS client is using STARTTLS for connection security (port 587 or 25), but SSL/TLS connection security does not have this issue. | 153364 |
| An App Rule fails to block attachments to gmail.com. Attachments are blocked the first 2-3 times, then not blocked. Occurs when using High Availability and Stateful Sync is enabled, and Client DPI-SSL is enabled. | 152034 |

Geo-IP / Botnet

| Resolved issue | Issue ID |
|---|----------|
| Some browsers do not accurately present the enabled/disabled state of Geo-IP Filtering. On the Geo-IP page, the "Block connections to/from countries listed in the table below" option is unchecked, even if the feature is on and actively working. Occurs when viewing the page from IE11 or Opera. Firefox and other versions of IE display the page correctly. | 154378 |

High Availability

| Resolved issue | Issue ID |
|--|----------|
| SonicOS displays multiple, recurring HA errors: <ul style="list-style-type: none">• Error synchronizing HA peer firewall (HTML post of main CGI)• Primary missed heartbeats from Backup• Primary received reboot signal from Backup Occurs when the HA Heartbeat is set to 1000ms instead of the recommended 5000ms, plus there are a lot of configuration settings including 300 unneeded NAT rules and 150 old address objects with associated NAT/Firewall rules. | 160515 |

Log

| Resolved issue | Issue ID |
|---|----------|
| Netflow traffic is not received by the external collector over a VPN tunnel interface. Occurs when using a Tunnel Mode VPN rather than a Site to Site VPN, and the remote firewall with the external collector behind it is running any of the following versions of SonicOS: <ul style="list-style-type: none">• 5.9.0.7 or earlier 5.9• 5.8.1.15 or earlier 5.8.1• 5.8.4.0 | 157207 |
| No data is shown on the Dashboard > AppFlow Monitor or AppFlow Reports pages and an error message is displayed, "Server responded with error [no such table: flow15]". Occurs when SonicOS cannot allocate additional memory for the AppFlow functions. | 143337 |

Modem

| Resolved issue | Issue ID |
|---|----------|
| After startup completes, VPN traffic triggers the dialup modem to dial even when there is an Ethernet interface (X1) available. It then continues to dial and seems to attempt to establish the VPN tunnel over the dialup interface. Occurs when a Zoom analog modem is connected to U0 on a TZ running SonicOS 5.9.0.7, WAN load-balancing is enabled, preempt and fallback to preferred interfaces when possible is set, X1 WAN is active and U0 is included on the final-backup. | 163423 |

Networking

| Resolved issue | Issue ID |
|--|----------|
| <p>The WAN PPPoE connection is not stable, but switches between two IP addresses. Occurs when the PPPoE packet has an illegal session ID, causing the packet to be dropped.</p> | 163824 |
| <p>An automatically created group address object becomes editable on the Network > Address Objects page and attempting to delete it causes an error message, "Error: Object is in use by an Access Rule" although it is not referenced by any ACL. Occurs when a group address object called "<custom zone name> Interface IPv6 Addresses" is created by the system after adding a custom zone in Network > Zones, and then the custom zone is deleted.</p> | 156481 |
| <p>Wildcard FQDN dynamic address object resolution generates excessive DNS traffic. Occurs when SonicOS generates DNS queries for wildcard subdomains (for example, *.sonicwall.com). The root domain (sonicwall.com) is resolved, and then a subdomain (sonicwall.com) is added, which is the same as the root domain. The DNS request times out when resolving the newly added subdomain and is sent again. The repetitive subdomains and related extra queries have been eliminated.</p> | 146856 |
| <p>Calls using Vertical Wave ISM 3.0.0 PBX in DMZ Transparent mode exhibit one way audio, causing SonicOS to see traffic using the same sequence number as a separate call and drop it due to a duplicate port error. Occurs when a client calls in and receives the automated attendant and prompt for extension and selections. After entering correct information, the call is transferred to the internal extension. When audio is passed outbound, the firewall NATs this traffic to a new source port deviating from the original transformation path. Inbound audio matching the original transformation path is then dropped on the WAN interface.</p> | 127260 |
| <p>If the Enable support for Oracle (SQLNet) option is selected, the connection to the Oracle server is lost after a few seconds. Occurs when an Oracle server is deployed behind a firewall and TCP port 1521 is open for accessing the server from the WAN interface. After the (child) data connection is sent to the client, the server closes the (parent) SQL*Net control connection on TCP port 1521. When the control connection state information is cleaned up, that data connection is also terminated by SonicOS.</p> | 115316 |
| <p>A firewall deployed in Wire Mode is not properly passing multicast traffic, causing issues for EIGRP or other multicast based protocols. Occurs when running SonicOS 5.8.1.0 - 5.8.1.5 on a firewall between Cisco routers in a network with thousands of EIGRP routes, using interface pairs configured in Layer2 Secure mode and with multicast traffic allowed/enabled under Firewall Advanced.</p> | 108635 |

Security Services

| Resolved issue | Issue ID |
|---|----------|
| <p>A CFS Custom Category cannot be added. After clicking Add to add a custom category, the dialog appears and the Name, Category, and Content fields can be populated, but when clicking on the Add button to add the website to the List field, nothing happens. Occurs when attempting to configure a CFS Custom Category on a TZ 100/100W or TZ 200/200W running SonicOS 5.9.1.0 or 5.9.1.1.</p> | 157751 |

SSL VPN

| Resolved issue | Issue ID |
|--|----------|
| <p>SSL VPN IP Pool exhaustion occurs when a single One-Time-Password user connects.</p> <p>Occurs when One-Time-Password is enabled for users attempting to log in with NetExtender, and the IPv4 IP address pool is limited to a single IP address.</p> | 165269 |
| <p>NetExtender displays the error, "Sending can't be completed in 10 seconds" for some One-Time Password connection attempts. This synchronization issue can cause a small SSL VPN IP address pool to become exhausted.</p> <p>Occurs when One-Time Password is enabled and the SMTP mail server causes a delay delivering the message, so that the OTP password is not received before it times out.</p> | 164847 |
| <p>A PCI compliance scan of the SSL VPN portal reports "This server's certificate chain is incomplete. Grade capped to B." The appliance does not send the complete certificate chain along with the server certificate.</p> <p>Occurs when a scan is run from https://www.ssllabs.com/ssltest/ on an appliance that has a server certificate from GoDaddy with a chain of 3 certificates including Root. The certificate is assigned on the SSL-VPN > Server Settings page.</p> | 163946 |
| <p>After disconnecting Mobile Connect from the firewall, a second attempt to connect gets stuck on "Verifying credentials" until 5-10 minutes have passed or the firewall or client machine is rebooted.</p> <p>Occurs when using Mobile Connect on Windows 8.1 related to a synchronization issue in the Microsoft VPN code.</p> | 159961 |
| <p>SonicOS Web management and SSH management over SSL VPN do not work.</p> <p>Occurs when SonicOS is configured to allow management over SSL VPN and a local user with SSL VPN service and administrator privileges tries to access the X0 subnet, but NetExtender attempts to connect to the default LAN IP address.</p> | 153399 |
| <p>A Qualys PCI compliance scan shows vulnerabilities to CVE-2014-0224, CVE-2011-3389 and CVE-2013-2566.</p> <p>Occurs when SonicOS does not support Suite B ciphers on port 443.</p> | 153072 |
| <p>One-Time Password login fails for SSL VPN users and the NetExtender logs display "Error sending one-time password. Sending can't be completed in 10 seconds."</p> <p>Occurs when an SSL VPN user tries to use NetExtender to log in and is required to enter a One-Time Password which is emailed to them.</p> | 151076 |
| <p>All SSL VPN connections simultaneously disconnect a couple of times a day. Some of the sessions automatically reconnect.</p> <p>Occurs when users are connected via NetExtender to a firewall running SonicOS 5.9.0.3 or 5.9.0.4. The inactivity timeout is set to 30 minutes, but the disconnection occurs before the timeout.</p> | 142546 |
| <p>SSL VPN does not provide a way for LDAP users to change expired passwords.</p> <p>Occurs when a user logs in via NetExtender and a message is displayed that their password is expired and to log into the portal and change it, but the portal does not provide a way to change the password.</p> | 135035 |

System

| Resolved issue | Issue ID |
|--|----------|
| <p>The SonicOS management interface becomes unresponsive after a VPN tunnel lifetime expires. The only way to recover is a warm reboot via SSH.</p> <p>Occurs when a SOHO or TZ is configured with L2B interface and VPN tunnel interface (600 sec lifetimes) to a larger firewall at the central site. IP Helper / DHCP policies use the central site DHCP server, and hosts are connected with settings for obtaining DHCP leases on the L2B interface of the SOHO. When the VPN lifetimes expire and renegotiate, the SOHO web UI cannot be accessed locally or via remote hosts.</p> | 165834 |
| <p>A network monitoring object does not work over a VPN Tunnel Interface and probing through the VPN says source is from 0.0.0.0.</p> <p>Occurs when the probe source IP address is supposed to be manually set by the administrator, but is left with the default 0.0.0.0.</p> | 163122 |
| <p>SonicOS certificate signing requests (CSR) use SHA-1 certificates, but need a way to do a SHA-256 CSR.</p> <p>Occurs when submitting a CSR request through the firewall to a Certificate Authority (CA).</p> | 163011 |
| <p>A custom admin username does not work after being imported and the firewall reverts to the default admin username, "admin".</p> <p>Occurs when configuration settings including the custom admin username are imported to a firewall.</p> | 161511 |
| <p>An SSL VPN local user login generates an IP Pool exhausted error.</p> <p>Occurs when a user logs in with NetExtender, using a One-Time Password, and receives an IP address from the SSL VPN IP pool twice and releases it once.</p> | 160068 |
| <p>The connection monitor shows UDP connections with a much higher value than the one allowed by the timeout value in the access rule.</p> <p>Occurs when random hosts in the LAN of the firewall create LAN to WAN UDP connections on port 443 with an expiry value in seconds much higher than the one configured (30 seconds).</p> | 155265 |
| <p>Extended Passive (EPSV) FTP for IPv4 is not working.</p> <p>Occurs when an FTP server is set up behind the firewall with the mode set to passive, and a client uses passive mode to connect to the FTP server through the firewall.</p> | 153146 |
| <p>After rebooting the firewall, some LDAP user groups disappear, SSO Agent configuration is lost, routes, VPN settings, and NAT policies are changed, and authenticated users show incorrectly. The configuration settings that disappear cause a ripple effect in App Rules, Access Rules, etc.</p> <p>Occurs when a configuration settings file is imported and then the firewall is rebooted. Network object update failures occur during prefs import and reboot.</p> | 151075 |
| <p>NAT policies and route table entries are corrupted after a reboot and in the secondary unit when a failover occurs, and there are certain address objects missing on the secondary unit corresponding to WXA appliance and SonicPoints.</p> <p>Occurs when running on a High Availability Pair with Stateful Sync enabled, after a reboot or failover occurs.</p> | 142858 |

User Interface

| Resolved issue | Issue ID |
|--|----------|
| <p>Botnet source (host/IP/user) identification is needed in AppFlow Monitor page.</p> <p>Occurs when attempting to determine the source of the reported Botnets shown in the AppFlow Reports page.</p> | 137844 |

Users

| Resolved issue | Issue ID |
|--|----------|
| <p>Attempting to delete a user group on the Users > Local Groups page results in the error message, "Error: Object is in use by an Access Rule".</p> <p>Occurs when trying to delete a local group which was already removed from the Firewall Access Rule in which it was previously among the included users.</p> | 148019 |
| <p>SonicOS blocks websites based on the Default CFS policy although the correct custom policies seem to be applied for the user based on user status.</p> <p>Occurs when the user is authenticated using TSA Agent 3.0.72 installed on Citrix XenApp 6.5, and the firewall is running SonicOS 5.9.0.2.</p> | 142324 |
| <p>SonicOS incorrectly reports previous/incorrect user information for a given IP address on the User > Status page, randomly resulting in incorrect CFS policies being assigned to users.</p> <p>Occurs when using physical and virtual PCs in a shared environment with DHCP enabled, all users log into the domain, approximately 100 Mac OS computers are also joined to the domain, and there are 3 Single Sign-On Agents (1 DC Logs Only, 2 WMI Only) on a virtual machine running SonicWALL Directory Services Connector 3.6.23.</p> | 139144 |
| <p>Single Sign-On (SSO) does not work for users behind a proxy server.</p> <p>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.</p> | 135558 |

VPN

| Resolved issue | Issue ID |
|---|----------|
| <p>After losing the WAN connection and then re-initializing it, many remote site to site tunnels are not automatically rebuilt. These tunnels stay down until they are manually disabled and re-enabled on the remote side.</p> <p>Occurs when KeepAlive is enabled on both the remote and head end sides and the VPN tunnels are bound to the WAN Load-Balancing (WLB) interface, and a WLB failover occurs. VPN best practices for large head end deployments say to have KeepAlive enabled only on the remote sides.</p> | 163773 |
| <p>SonicOS does not allow more than one concurrent L2TP client connection. If a second user tries to connect, it fails and logs show, "IKE Responder: IPsec proposal does not match (Phase 2)".</p> <p>Occurs when the firewall has been up and allowing multiple concurrent L2TP client connections for 2-3 weeks.</p> | 160786 |
| <p>Clients cannot connect to a remote NSA 3600 using SonicWALL Global VPN Client. The GVC IKE traffic is lost at the local firewall before egress on X1 WAN interface.</p> <p>Occurs when the client is connected to a local NSA 250MW running SonicOS 5.9.1.0, although it works with 5.9.0.7.</p> | 159481 |
| <p>One of three IPsec Phase 2 Security Associations (SAs) is lost on one side while traffic is still being sent.</p> <p>Occurs when many site to site VPN tunnels are configured between the E-Class NSA "hub" and the TZs which are the "spokes", and the E-Class NSA is the responder in aggressive mode. After the SA life time expires, logs show the SAs being negotiated, but the hub firewall does not list all of the SA networks. This is due to associating a phase2 tunnel to a wrong phase1 SA.</p> | 150055 |
| <p>When trying to acquire a firewall in GMS using a Management Tunnel, login attempts to the firewall are dropped.</p> <p>Occurs when the firewall is running SonicOS 5.8.1.12 and is behind NAT.</p> | 130301 |

It is not possible to export the Global VPN Client policy in RCF format and an error message is displayed, "The requested URL was not found on this server: /.rcf".
Occurs when the global IPsec index uses an incorrect value.

111513

Vulnerability

| Resolved issue | Issue ID |
|---|----------|
| Remote attackers may be able to obtain sensitive private-key information (OpenSSL advisory CVE-2015-3193). Occurs when the Montgomery squaring implementation in OpenSSL 1.0.2 before 1.0.2e on the x86_64 platform, as used by the BN_mod_exp function, mishandles carry propagation and produces incorrect output. | 167684 |
| SonicOS does not always drop the packet when an invalid port number is received from a malicious FTP client. This vulnerability is known as "FTP Bounce". Occurs when a malicious FTP client sends an FTP "PORT" command in an attempt to fool a vulnerable server into initiating a data connection to a victim host. | 166415 |
| Several OpenSSL vulnerabilities were reported, including a man-in-the-middle attack known as Logjam (CVE-2015-4000), malformed ECParameters that can cause an infinite loop (CVE-2015-1788), an exploitable out-of-bounds read (CVE-2015-1789), a PKCS7 crash with missing EnvelopedContent (CVE-2015-1790), a CMS verify infinite loop with unknown hash function (CVE-2015-1792), a race condition handling NewSessionTicket (CVE-2015-1791), and an invalid free in DTLS (CVE-2014-8176). Occurs when earlier versions of OpenSSL are used in the code. | 161863 |
| SonicOS needs the ability to block SSLv3 in SSL Control. Occurs when using SSL Control on an appliance running SonicOS 5.9.1.4 or earlier, in which only SSLv2 can be blocked. | 161805 |
| (CVE-2015-0204) The FREAK Client Test shows the FREAK vulnerability in SonicOS. This is a factoring attack on RSA-EXPORT keys exploiting a weakness in some versions of SSL/TLS that allow an attacker to decrypt secure communications between vulnerable clients and servers. Occurs when Client DPI-SSL is enabled. | 159277 |

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 |

| | |
|--|--------|
| <p>SSL VPN users are not displayed in Dashboard > AppFlow Monitor on the Users tab, only “unknown” users are shown.</p> <p>Occurs when several (10) SSL VPN users are connected to the firewall and AppFlow Reporting is enabled.</p> | 167149 |
| <p>IPv6 applications are not displayed in the AppFlow Monitor page.</p> <p>Occurs when some IPv6 streams have been triggered by visiting certain websites.</p> | 166912 |
| <p>The Dashboard > AppFlow Reports page does not display any entries on the Applications tab.</p> <p>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.</p> | 164502 |

Application Control

| Known issue | Issue ID |
|--|----------|
| <p>The App Rule Match Object cannot match a filename.</p> <p>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.</p> <p>Workaround: Do not enable the Negative Matching option with the Prefix Match option.</p> | 135634 |
| <p>App Control policies do not block IPv6 traffic unless Intrusion Prevention Service (IPS) is enabled.</p> <p>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.</p> <p>Workaround: Enable IPS. With IPS enabled, the App Control policy blocks the FTP connection.</p> | 128410 |

Command Line Interface

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

DPI-SSL

| Known issue | Issue ID |
|--|----------|
| <p>The SSL proxied connection count cannot be cleared from the cache.</p> <p>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.</p> | 159332 |
| <p>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.</p> <p>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,</p> <p>Guest Services are enabled on the WLAN zone, a wireless client connects to the SonicPoint, and the user logs into the guest account.</p> | 123097 |

IPv6

| Known issue | Issue ID |
|--|----------|
| <p>The firewall drops an "ICMPV6 packets too long" message, causing WLAN clients to be unable to connect to the WAN IPv6 server.</p> <p>Occurs when W0 is configured with an IPv6 address and an IPv6 NAT policy maps the W0 private address to the X1 IPv6 public address. The X1 IPv6 MTU is set to 1500 (default). A mobile phone connected to W0 attempts to launch the Facebook app, which fails when the WLAN client send some very large packets to the IPv6 remote server and then the IPv6 remote server responds with the "ICMPV6 packets too long" message.</p> | 167238 |
| <p>A 6rd tunnel (IPv6 rapid deployment tunnel) is unexpectedly reported as UP although there is no available 6rd prefix.</p> <p>Occurs when the tunnel was previously UP and using DHCP mode, and then the DHCP server is disabled and the firewall is rebooted.</p> | 157034 |
| <p>IPv6 traffic that is sent over a 6rd interface is not forwarded.</p> <p>Occurs after rebooting the firewall.</p> <p>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.</p> | 143079 |
| <p>IPv6 packets exceeding the Maximum Transmission Unit (MTU) are dropped instead of being fragmented.</p> <p>Occurs when setting the MTU for an interface, and then sending IPv6 packets that exceed the MTU.</p> | 139108 |
| <p>An IPv6 Address Object in the Exclusion Address list of an App Rule policy is still blocked by that App Rule policy.</p> <p>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.</p> | 128363 |

Networking

| Known issue | Issue ID |
|---|----------|
| <p>OSPF over a VPN tunnel does not establish adjacency.</p> <p>Occurs when using numbered tunnel interfaces for advanced routing in SonicOS 5.9, and the VPN tunnel interfaces are not part of the same subnet on both ends of the tunnel. This can also occur with a VPN tunnel between a numbered tunnel interface on an appliance running SonicOS 5.9 and an unnumbered tunnel interface on an appliance running 5.9 or another release.</p> | 166448 |
| <p>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.</p> <p>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.</p> <p>Workaround: Restart the firewall to make X1 accessible again.</p> | 160164 |
| <p>The WAN interface cannot be accessed with HTTPS or ping after restarting the firewall.</p> <p>Occurs when X0 (LAN) has a redundant port configured and X0 physical status is "no link".</p> | 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 |

VPN negotiation fails and the log for the Initiator does not have an entry showing "IKEv2 negotiation complete". 148167

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.

Traffic goes to the wrong VPN tunnel. 135205

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.

An active IPv6 VPN tunnel is not displayed in the table on the VPN > Settings screen of the head-end firewall. 128633

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.

An OSPF connection cannot be established between an NSA 240 and an NSA 7500. 128419

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.

System compatibility

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

Wireless 3G/4G broadband devices

SonicOS 5.9.1.5 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/>.

i **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 4 (or higher) or GMS 8.1 are required for GMS management of Dell SonicWALL SOHO appliances running SonicOS 5.9.1.5.

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 5.9.1.5. 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

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

i | **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/>.

i | **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.

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
- Chat with a support engineer

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 © 2015 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.

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: 1/12/2016

232-003125-00 Rev B