SonicWall® SonicOS 6.5.0.2

Release Notes

December 2017

These release notes provide information about the SonicWall® SonicOS 6.5.0.2 release.

Topics:

About SonicOS 6.5.0.2

SonicWall SonicOS 6.5.0.2 fixes a number of issues found in previous versions. For information, see the Resolved Issues section.

SonicOS 6.5.0.2 contains all the features and all the resolved issues that were included in previous SonicOS 6.5 releases. See the previous release notes on MySonicWall.

Supported Platforms

SonicOS 6.5.0.2 is supported on the following SonicWall appliances:

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2650
- NSA 2600
- TZ600
- TZ500 / TZ500 Wireless
- TZ400 / TZ400 Wireless
- TZ300 / TZ300 Wireless
- SOHO Wireless

Resolved Issues

This section provides a list of resolved issues in this release.

Access Point

Resolved issue	Issue ID
Wireless clients can not communicate with each other although in the same network segment with the same WT0 interface. Occurs when two SonicPoints are connected to a router which is connected to the firewall and Layer 3 management is configured in SonicOS for the SonicPoints, and a wireless client connects to each of the SonicPoints.	194957

CLI

Resolved issue	Issue ID
All SonicPoints reboot when selecting only one in the CLI command. Occurs when rebooting one SonicPoint from the CLI.	195878
The “show network-monitor policies” command does not show policies correctly. Occurs on a SuperMassive 9600.	186042

DPI-SSL

Resolved issue	Issue ID
A local user cannot be configured as the included user object. Occurs when configuring DDI-SSL Client on the Object screen.	195917

Log

Resolved issue	Issue ID
No log entries are entered and only “parsererror” is shown in the log monitor. Occurs when a GVC client connects to the firewall.	195850
Search displays data not relevant to the provided filter entry. Occurs when searching for an IP on the Logs > Event Logs page.	195470
Syslog messages do not show the msg field. Occurs when the firewall is sending syslogs in enhanced syslog format.	194831

Networking

Resolved issue	Issue ID
Ping to native bridge host from client of native bridge member fails. Occurs when the native bridge host is a VLAN interface or trunk VLAN interface and the link is down.	196918
OSPF page is blank in SonicOS management interface, and the CLI does not work to configure OSPF. Occurs when navigating to Network > Routing > Settings > Routing mode > Advanced routing > OSPFv2, after upgrading to 6.5 from 6.2.9.x and apostrophe characters existed in the comments of PBR routes configured in 6.2.9.	196652

Networking

Resolved issue	Issue ID
The “For users who are not identified via SSO, don't redirect to log in” checkbox cannot be enabled. Occurs when configuring options in the Firewall > Access Rules > Edit Rule screen.	196450
The firewall drops SYN,ACK packets with the error “Packet dropped - cache add cleanup drop the pkt” intermittently. Occurs when trying to access a server on a routed subnet from the X0 subnet.	195240
The error “Address Object is in use by a route Policy” is displayed when modifying an Address Group. Occurs when modifying a nested Address Group assigned to a route policy, only when an Address Group which contains other Address Groups is modified and a route policy is associated.	193260
Relay-forw packets are treated as normal DHCPv6 server packets and are consumed, passed to stack, but not forwarded through firewall even if they should be forwarded. Occurs when appliance receives DHCPv6 relay-forw/relay-reply packet with srcPort, dstPort both 547, and dst IP is this firewall or not.	193173
Traffic cannot pass through a VLAN trunking interface because all incoming ARP requests are dropped. Occurs after removing the VLAN trunking interface from an LACP LAG. **Workaround**: Delete the VLAN trunk interface and then add the exact same configuration, or reboot the firewall.	191702

Security Services

Resolved issue	Issue ID
Cannot create a MAC or FQDN type of Address Object. Occurs when adding an entry to the Client CF Enforcement lists.	196723
CFS objects (URI lists, action objects and profile objects) do not show up in the SonicOS UI and thus cannot be reconfigured. Occurs after upgrading from 6.2.9 to 6.5, while the CFS polices still show under Security Services > Content filter.	194442
Incorrectly formatted data is seen in a Geo_IP Filter. Occurs when adding a custom country such as Korea or N. Korea in Security Services > Geo_IP Filter on the Custom List screen.	183280

SSL VPN

Resolved issue	Issue ID
The Virtual Office portal does not display bookmarks added for an imported user. Occurs when the user was imported from Active Directory and added to the SSLVPN services group, and then the bookmark is added for that user and the user logs into the portal.	196878
SSL-VPN Cipher Preference stays enabled and there is no option to change it via CLI. Occurs after upgrading to 6.5.0.0.	194715
Delay/latency is observed in loading content. Occurs when connected to the computer via an RDP-Bookmark.	180711

Switching

Resolved issue	Issue ID
Traffic fails through L2 LAG. Occurs after upgrading from SonicOS 6.2.7 or 6.2.9 to 6.5.0.0 and then shutting down the aggregator port from the SonicOS management interface.	193305

System

Resolved issue	Issue ID
Service type of Bookmark should be included in TSR.	197009
Link is not detected on the 10G interfaces, X17, X18, and X19 for about four minutes after the firewall comes up. Occurs on a SuperMassive 9600 or NSA 6600 running SonicOS 6.5.0.1.	195622
SonicOS cannot export settings or create backup settings. Occurs when trying any actions on the System > Settings page, due to a JavaScript error.	195380
The firewall drops legitimate backup server traffic as Wrong fragmentation boundary and logs it as Nestea/Teardrop attack dropped. Occurs when the dropped traffic is shadow stream backup server traffic from WAN to LAN, using port forwarding to translate the traffic destination to the internal backup device.	191070
Need the ability to exclude/detect the aggregate Traffic (VPN and Non-VPN) from UDP and ICMP Flood Protection Configuration. Occurs when managing VOIP traffic across Site to Site VPN when UDP Flood Protection is enabled.	175461
Many “NTP Server response is none or invalid” alerts are displayed, especially after a reboot. Occurs when only the built-in NTP Servers are configured in SonicOS.	126655

User Interface

Resolved issue	Issue ID
SonicOS does not save after editing an URL, and the edit pop up cannot be closed. Occurs when adding the URL in user Authentication Bypass, then selecting the URL to edit and then clicking OK or Cancel.	194611
The **MONITOR | User Sessions > Active Users** page continually refreshes when viewing a particular partition's status. Occurs when the default WAN interface is the only WAN interface, three partitions are added, some partition policies are configured, users log in from a partition, and then the user attempts to view a particular partition's status rather than viewing *All*.	190025

Users

Resolved issue	Issue ID
External Guest Authentication is not working. Occurs after upgrade to 6.5 from 6.2.7.1.	195856
Importing a username results in “Error: name is not a simple name”. Occurs when importing a username from LDAP which has a dot/period symbol in its logon name.	195471
The firewall reports an error when trying to add VPN access for a default local group. Occurs when adding VPN access to the X0 subnet for a default user group such as Everyone.	193990

Vulnerability

Resolved issue	Issue ID
PCI scan failed with HTTP Security Header Not Detected on port 4433.	194474
OpenSSL issues with NULL pointer and memory.	170826

Known Issues

This section provides a list of known issues in this release.

3G/4G

Known issue	Issue ID
Traffic passes through the alternate WAN and it becomes the default gateway, although U0 was configured as the primary WAN and default gateway. Occurs when U0 is in Connect on Data mode and working fine as the primary WAN, with X1 connected and configured as the alternate WAN, and then the appliance is restarted.	190640

Access Point

Known issue	Issue ID
SonicWave access points are enabled and operational despite being disabled in SonicOS. Occurs when the Enable option is selected in SonicOS management settings when the SonicWave is first connected, then the option is disabled during the SonicWave reboot process.	197080

Content Filter Service

Known issue	Issue ID
A web site cannot be blocked by CFS for LDAP users with RADIUS Accounting. Occurs when a CFS policy is configured to block a category of web site, but an LDAP user authenticated by RADIUS Accounting is still able to access it.	192258

DPI-SSL

Known issue	Issue ID
The **Allow SSL without decryption (bypass) when connection limit exceeded** option does not work. Occurs when Client DPI-SSL is enabled on a SM 9600 with max DPI-SSL capacity set to 12,000 and then 15,000 HTTPS connections are attempted, but only 12,000 can be established and the bypass option does not take effect. Without Client DPI-SSL enabled, all 15,000 connections can be established.	197191
The NSA 2650 allows more DPI-SSL connections than it can reasonably support. Occurs when throughput drops significantly after 6000 DPI-SSL connections are established.	196979
In the **Common Name** screen of the **MANAGE | Decryption Services > DPI-SSL/TLS Client** page, the **Skip authenticating the server** option is selected when adding “cacert.org” as a common name, but it does not have the expected effect of skipping the authentication. Occurs when the **Always authenticate server for decrypted connections** option is enabled in the **General** screen, and then the user tries to access *https://cacert.org*, but the site is still authenticated as an untrusted site and blocked by DPI-SSL.	192439

DPI-SSL

Known issue	Issue ID
In the **Common Name** screen of the **MANAGE | Decryption Services > DPI-SSL/TLS Client** page, the option **Skip CFS Category-based Exclusion** is selected when adding “bankofamerica.com” as a common name, but it does not have the expected effect of skipping such an exclusion. Occurs when a category such as “20. Online Banking” is selected for exclusion in the CFS Category-based Exclusion/Inclusion page, and then the user browses to *https://www.bankofamerica.com*, but the site is still excluded from inspection by DPI-SSL.	192438
The **Always authenticate server before applying exclusion policy** option in a custom exclusion policy for a common name such as *dropbox.com* is changed to disabled when saving the policy. Occurs when the **Always authenticate server before applying exclusion policy** option is set to the default setting **Use Global Setting** when adding the common name and saving it in the **Common Name** screen of the **MANAGE | Decryption Services > DPI-SSL/TLS Client** page.	192326

High Availability

Known issue	Issue ID
Upon forced failover, not all connections are cleaned up on the new standby unit after all traffic is stopped. Occurs when more than 60%-70% of maximum connections are active for an hour or more on a SM 9600 HA pair with security services, SSO, AppFlow, and Capture traffic running, and then failover is forced and all traffic is stopped. Connections cleanup works fine on the newly active unit, but not on the standby unit.	197109
HA synchronization issues occur, including: • Standby unit shows CPU utilization although it should not. When the active is using 60%, the standby shows 30% in use. • After force failover, the standby unit stops responding, the admin cannot access UI and PING stops responding. • Active HA status shows a peer, but standby HA status shows no peer found. Occurs when an HA pair of SM 9600s has 99% of maximum connections passing traffic and 50%-60% of CPU in use.	195616

Log

Known issue	Issue ID
Server Facility and Syslog Facility settings for syslog servers on the Log > Syslog page are incorrectly changed from “Local use 0” to “Kernel”. Occurs after rebooting the appliance.	197151

Networking

Known issue	Issue ID
The default IPv4 access rule is placed after all the IPv6 rules for LAN to LAN, rather than after all IPv4 rules and before all IPv6 rules. Occurs when the default IPv4 rule is changed and then the **Restore** button is clicked.	197366
Consistent NAT does not work correctly with H323. Occurs when H323 signals a request for an RTP port for the call, but requests a different RTP port each time.	194555

Networking

Known issue	Issue ID
The broadcast/multicast packets generated by the Portshield port loop back and are received by the firewall again. Occurs when an interface is configured with a static IP in the LAN zone, a second interface is portshielded to it, and traffic is sent from the SonicOS diagnostic *ping* function to a PC connected to the static IP interface. The ARP request packets loop back to that interface.	189317
With two WAN interfaces configured, management traffic from the WAN side cannot reach the default gateway for the second WAN. Occurs when both WAN interfaces are configured with IPv6 static IP addresses, but the system default route from the interface IP to ANY was not created for the second WAN. **Workaround**: Manually add the route from the interface IPv6 IP to ANY for the second WAN.	189296

Packet Replay

Known issue	Issue ID
The Packet Replay function is affected by Packet Monitor. Occurs when duplicated ingress packets are replayed after starting packet monitoring.	195047

Switching

Known issue	Issue ID
IPv6 SSL VPN fails to connect to the interface IP in LACP group; connection fails with console message, “dp_stack_output:1259: Need to free this WQE!!!” Occurs when trying to connect from a PC on the WAN side, using IPv6 SSL VPN to the WAN interface of LACP, or with LAN/DMZ side LACP.	194566
Only one 10G interface is listed under the VLAN trunk port list on an appliance with multiple 10G interfaces, and a 1G port and 10G port can be configured as a Link Aggregation Group (LAG). Occurs on a NSA 6600, on which X16, X17, X18 and X19 are all 10G interfaces, when configuring a LAG, and when a 1G interface like X2 is configured as a trunk port and the same VLAN ID is enabled for both X2 and X17.	194004
Unexpected failover occurs on a Stateful HA pair with Link Aggregation (LAG) configured. Occurs after deleting all the members and aggregate ports in the LAG.	193551

SSL VPN

Known issue	Issue ID
Configured WINS Servers are not displayed in NetExtender on the DNS tab. Occurs when NetExtender is used on Windows 10 clients. The WINS Servers are displayed in NetExtender on Windows 7 clients.	197032

User Interface

Known issue	Issue ID
The first firewall in a VPN association does not show a SIP call, when the call is SIP/TCP/VPN. Occurs when a VPN is created between two firewalls, a SIP/TCPv4 call is sent over VPN, and the VoIP > Call status page is viewed.	193862

Users

Known issue	Issue ID
A user repeatedly gets the error message, “Incorrect Password” and cannot change their password. Occurs when the administrator creates the user credentials, adds the user to the SonicWall Administrators group, enables the **Force relogin after password change** option, and then the admin stays logged in while the new user logs in and is required to change their password.	196911
The field used to filter users by location when importing from LDAP is missing. Occurs when importing users from LDAP on the **MANAGE | Users > Local Users & Groups > Local Users** page and clicking the **Users at/at or under** option in the import dialog. The option should be followed by a field with LDAP locations, but the field is missing.	195781
SSO RADIUS accounting server does not create users with different user numbers after receiving TSA user info with SonicWall-Acct-Number attribute. On servers's User Sessions > Active Users page, only one TSA user from that IP is displayed. Occurs when multiple TSA users log on from the same IP address on a RADIUS accounting client, and the packet sent from RADIUS accounting client to server does carry the SonicWall-Acct-Number attribute.	194642
An IPv6 web-login user fails to log onto the RADIUS accounting server. Occurs when an IPv6 web-login user logs onto the RADIUS accounting client and should be automatically logged onto the RADIUS accounting server.	194581
A web user logs onto the RADIUS accounting client, but fails to log onto the RADIUS accounting server. Occurs when the User-Name attribute format is set to “user-name@domain” on the accounting server side, matching the format on the accounting client side.	194518
The browser does not redirect to the requested URL after NTLM authentication succeeds. Occurs about half of the time when using Firefox to browse to a website and NTLM is enabled for user authentication, RADIUS is configured, and there is an access rule requiring user authentication.	193291
SonicOS displays very high numbers for Intrusion Prevention in the **Threat Prevention Summary** table on the **MONITOR | Dashboard** page, and very high numbers for PING on the **Intrusions** screen of the **INVESTIGATE | AppFlow Reports** page. Occurs when there are only about 20 active users and seemingly not that many actual intrusions.	193137
Partition domain names are not listed in the drop-down list on the SSL VPN portal page. Only ***LocalDomain*** is displayed in the list. Occurs after disabling and then re-enabling Authentication Partitioning. **Workaround**: Reboot the firewall or make some change to the partition domain name, then it will reappear.	192733

VoIP

Known issue	Issue ID
After upgrading to SonicOS 6.5, it is necessary to change the SIP Service Object to allow SIP_TCP functionality to a SIP Proxy Server deployed on the LAN. Occurs when a SIP Proxy Server is deployed on the LAN before the upgrade to SonicOS 6.5. In earlier versions of SonicOS, only SIP_UDP was supported. To communicate the new SIP_TCP functionality to the SIP Proxy Server, the SIP Service Object must be changed to “SIP_GROUP”, which includes both SIP_UDP and SIP_TCP. Note that SIP_UDP and upstream SIP_TCP will work fine after the upgrade; only SIP_TCP to the server on the LAN requires the Service Object change.	195013

VPN

Known issue	Issue ID
One out of two clients does not receive IPsec/ESP packets. Occurs when using IPsec pass through with both clients using same VPN server.	196519

X-Series

Known issue	Issue ID
The switch port cannot be discovered when connected to the child switch. Occurs when the IDV VLAN of a dedicated port is not allowed in the uplink ports between the parent and child switch.	193231
The port shield configuration of ports to a VLAN sub-interface is moved to parent interface in both parent and child switch. Occurs after failover in a dedicated uplink topology or with a common uplink.	193066
Adding a dedicated link in the parent switch does not program its native VLAN ID in the child switch and the message “unable to get etherlike counters from the external switch!” is displayed on the SonicWall appliance console. Occurs when using a dedicated uplink topology.	192920
A packet loop occurs after a failover with a certain topology. Occurs when an NSA 2650 HA pair is configured with a shared uplink and a dedicated uplink.	192807

System Compatibility

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

Wireless 3G/4G Broadband Devices

SonicOS 6.5 provides support for a wide variety of PC cards, USB devices and wireless service providers. For the most recent list of supported devices, see:
https://www.sonicwall.com/en-us/support/knowledge-base/170505473051240

GMS Support

SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.5 requires GMS 8.4 for management of firewalls using the new features in SonicOS 6.5. SonicWall GMS 8.3 SP1 supports management of all features in SonicOS 6.2.9.2 and earlier releases.

WAN Acceleration / WXA Support

The SonicWall WXA series appliances (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are supported for use with SonicWall security appliances running SonicOS 6.5. 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. SonicWall recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS. This release supports the following Web browsers:

- Chrome 45.0 and higher
- Firefox 25.0 and higher
- IE Edge or IE 10.0 and higher
- Safari 10.0 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 SonicWall appliance system administration.

Product Licensing

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

Upgrading Information

For information about obtaining the latest firmware, upgrading the firmware image on your SonicWall appliance, and importing configuration settings from another appliance, see the *SonicOS 6.5 Upgrade Guide* available on the Support portal at https://www.sonicwall.com/en-us/support/technical-documentation.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products 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. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

Legend

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

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

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

Last updated: 12/29/17

232-004172-00 Rev A