SonicWall™ SonicOS 6.2.9.1

Release Notes

September 2017

These release notes provide information about the SonicWall™ SonicOS 6.2.9.1 release.

Topics:

About SonicOS 6.2.9.1

SonicWall SonicOS 6.2.9.1 is a maintenance release that fixes a number of issues found in previous releases. For more information, see the Resolved Issues section.

This release provides all the features and contains all the resolved issues that were included in SonicOS 6.2.9.0, 6.2.7.2, and releases prior to 6.2.7.2. For more information, see the previous release notes, available on MySonicWall at: https://mysonicwall.com.

Supported Platforms

SonicOS 6.2.9.1 is supported on the following SonicWall appliances:

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- 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.

Gateway Anti-Virus

Resolved issue	Issue ID
Capture ATP does not process email attachments; SMTP email is not processed regardless of the attached file type. Also, Gateway Anti-Virus does not block email attachments, such as VBA macros, that are configured to be blocked in the GAV settings. Occurs when the TCP Stream option is enabled for Outbound Inspection in the Gateway Anti-Virus settings.	188050

High Availability

Resolved issue	Issue ID
In a High Availability deployment with one unit down, the active appliance becomes unresponsive. Occurs when heavy, mixed traffic including SIP (H.323) traffic is passing through the active appliance, while the other unit in the HA pair is powered down.	190464

Networking

Resolved issue	Issue ID
The first 600 access rules are kept per any zone-to-zone rule list and the rest are deleted after upgrading to SonicOS 6.2.7.1. Occurs when there are more than the default number of access rules (Max Rule Count: 600 by default) in any zone to zone access rule list, and then the appliance is upgraded to SonicOS 6.2.7.1. Occurs even when Max Rule Count is set to a higher number before upgrading or importing the previous configuration.	190798
The Transparent IP Mode (Splice L3 Subnet) option is not available for the Mode/IP Assignment option in SonicOS 6.2.7.1. Occurs when configuring a virtual interface in SonicOS 6.2.7.1.	189827
The delete option to remove automatically added rules is always disabled. Occurs when the internal setting “Enable the ability to remove and fully edit auto-added access rules” is selected, which should enable the delete option.	188125
SonicWall GMS does not display the Vendor and Type fields when viewing the Network > ARP table or in other tables. Occurs when GMS is managing a firewall running SonicOS 6.2.7.1 which supports the Vendor and Type fields, but SonicOS does not pass the data to GMS.	186628
Wireless users connected to a SonicPoint are unable to access LAN or WAN destinations. Occurs when the SonicPoint is connected to a physical firewall interface with a VLAN or VAP configured and bridged with Layer 2 Bridging to an interface in the LAN zone.	185498

System

Resolved issue	Issue ID
The SonicWall appliance ceases to respond due to RADIUS task suspension. Occurs in some cases with the authentication of CLI logins with remotely authenticated administrators or during a GUI RADIUS test.	187930

Users

Resolved issue	Issue ID
The SSO Agent does not trigger when traffic occurs on zones that have authentication enforced. Occurs when the **For other unidentified connections** option under **For logging of connections on which the user is not identified** is set to **Log user name: Unknown** in the user settings.	189771

VoIP

Resolved issue	Issue ID
VoIP phones behind a firewall running SonicOS 6.2.7.1 cannot make outbounds calls, although inbound calls and phone registration are working fine. Occurs when the internal SIP device uses a port that is different from the source port (the port associated with the Via or Contact fields), and when the remote device sends packets to this port, the firewall is not forwarding them to the internal device.	189231
VoIP inbound and outbound calls have no audio unless the SIP transformation settings are periodically disabled and re-enabled. Occurs when VoIP is working fine with a PBX (IPFX) server behind the firewall and then the firewall is upgraded to SonicOS 6.2.7.1.	188861

VPN

Resolved issue	Issue ID
Firewall1 fails to resolve the IPsec gateway domain whenever the WAN IP address changes on Firewall2. Occurs when a Tunnel Interface Site-to-Site VPN is configured between Firewall1 and Firewall2, where Firewall1 is using Dynamic WAN and DDNS, and Firewall2 is the IPsec gateway and is behind NAT with Keep Alive enabled and Initiator with FQDN set to the address of Firewall1.	190490
The firewall stops responding and stops passing traffic with a certain combination of VPN and DNS server configuration. Occurs when a site to site VPN with FQDN is configured as the WAN gateway, the primary DNS server is in a subnet behind the remote VPN, and a secondary DNS server is configured on the local side. If the VPN policy is disabled after adding it and then re-enabled, the firewall stops responding. It only occurs when the IP address is unresolved (0.0.0.0) in the VPN policy.	187008

Vulnerability

Resolved issue	Issue ID
A false positive PCI scan failure occurs for 80/tcp Web error message information leakage: /auth1.html. Occurs when the SonicWall appliance tries to send an error message related to One Time Password, which it shouldn't as the user did not try to login into the system.	189907

Wireless

Resolved issue	Issue ID
Multiple wireless clients cannot access the internet at the same time using Lightweight Hotspot Messaging. Occurs when one of following sequences takes place: • Wireless Client1 tries to access the internet, is redirected to the login page and logs in successfully. Wireless Client2 tries to access the internet, is redirected to the login page, but gets a “Session creation failed” error and cannot log in. • Wireless Client1 tries to access the internet, the page is redirected to the login page, but Client1 does not log in right away. Then, Wireless Client2 tries to access the internet, the page is redirected to the login page and Client2 logs in. The result is that Client1 is authenticated and can access the internet successfully, while Client2 is asked to log in every time while trying to access the internet.	190413

Known Issues

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

3G/4G

Known issue	Issue ID
Web browsing and 1MB FTP downloads are slower on SonicOS 6.2.9.1 than on 6.2.6.0. Occurs when connected to WWAN with a Sprint 3G card.	183961

High Availability

Known issue	Issue ID
Failover occurs unexpectedly in an Active/Standby HA pair with link aggregation (L2 LAG with Trunk mode) enabled. Occurs when the “Active/Standby Failover only when ALL aggregate links are down” option is enabled on the High Availability > Advanced page and the aggregator port goes down. In this case, failover should not occur as long as at least one LAG member port is still up.	193086
Failover cannot be forced from the primary to the secondary unit in a Stateful HA pair. When attempted, the secondary unit displays a message that “peer has higher priority.” Occurs when the HA pair is running traffic using 99% of maximum connections.	192152

IPv6

Known issue	Issue ID
SonicOS sends IPv4 DNS requests when communicating with SonicWall backend servers such as MySonicWall or the License Manager. Occurs when the X1 (WAN) interface and the DNS server are only configured with IPv6 addresses.	183975

Networking

Known issue	Issue ID
Routes are not learned between two firewalls connected with VPN Tunnel Interfaces. Occurs when using advanced routing with RIPv1.	189538
When using NAT64, HTTPS traffic fails in some cases. Occurs when SSL Client Inspection is enabled.	184830
A specific sub-domain host IP address cannot be added into a FQDN Address Object. Occurs when a FQDN AO such as *.e.com is added, then the admin queries 1.e.com, 2.e.com, and 3.e.com on a computer connected to the firewall LAN zone and the IP addresses for those sub-domains are returned by the server. But, the FQDN AO still only contains the host IP address for e.com.	184156
A sub-VLAN interface configured in PPPoE/PPTP/L2TP mode and then changed cannot connect again during the enabled schedule. Occurs when the interface is changed to static mode while connected, and then changed back to iPPPoE/PPTP/L2TP mode.	183607

SonicPoint

Known issue	Issue ID
RADIUS Accounting can be configured with a SonicPoint NDR access point, but then no accounting messages reach the accounting server. Occurs when SonicOS allows configuration of the Radius Accounting settings with older SonicPoint platforms that are not officially supported.	181522

Switching / X-Series

Known issue	Issue ID
In an HA pair, importing settings after an X-series switch is deleted clears the VLAN configuration in the switch.	183564

VoIP

Known issue	Issue ID
VoIP service does not work for this H323 call sequence: Hook-OFF, Hook-ON and immediately do Hook-OFF again. The call does not pass. Occurs when the firewall is configured in NAT mode with the AVAYA hardware codec and AVAYA software codec in the LAN zone and the gatekeeper in the WAN zone.	192723

VPN

Known issue	Issue ID
VPN Auto Provisioning does not completely bring up the VPN Tunnel until traffic is initiated from behind the spoke (AP client side). Occurs when using VPN Auto Provisioning to negotiate and create the tunnel. Phase 1 negotiation is completed, but Phase 2 negotiation is not triggered until the client sends some traffic.	193235
A VPN policy which is already used in an existing Tunnel Interface is incorrectly shown in the drop-down list. Occurs when a new Tunnel Interface is being added and the policy choices are viewed in the VPN Policy drop-down list.	189220

VPN

Known issue	Issue ID
Only one of two protected subnets behind an Auto Provisioning (AP) client can establish a tunnel to the AP server. Occurs when the AP server policy has the **Require Authentication of VPN AP Clients via XAUTH** option enabled. If the **Allow Unauthenticated VPN AP Client Access** option is enabled instead, both subnets can establish a tunnel.	185074
The VPN Tunnel cannot be negotiated in some cases. Occurs when the Auto-Provisioned Server uses a certificate with a wildcard character in the DN and the DN also includes ID strings using “DC=”.	181322

Wireless

Known issue	Issue ID
TCP wireless traffic fails to connect 5 times, resulting in the message, “Error: TCP connect operation failed because of timeout...” Occurs when running mixed g mode layer 2 traffic from a testing tool and using the 2.4GHz radio on the wireless appliance.	192867
The internal wireless SSID cannot be found after restarting the firewall. Occurs when the wireless radio is enabled in the Wireless > Setting page and WP2-PSK/AES is selected and configuration is saved, then the firewall is restarted and the user attempts to connect to the known SSID.	192391

System Compatibility

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

Wireless 3G/4G Broadband Devices

SonicOS 6.2.9 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/.

GMS Support

SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.2.9 requires GMS 8.3.1 for management of firewalls using the new features in SonicOS 6.2.9. SonicWall GMS 8.3 supports management of all other features in SonicOS 6.2.9 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 6.2.9. 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 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 16.0 and higher
- Internet Explorer 9.0 and higher
- Safari 5.0 and higher running on non-Windows machines

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

NOTE: Mobile device browsers are not recommended for 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 6.2 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: 9/29/17

232-002584-00 Rev A