SonicWall® SonicOS 5.9.1.12

Release Notes

March 2019

These release notes provide information about the SonicWall® SonicOS 5.9.1.12 release.

Topics:

About SonicOS 5.9.1.12

SonicWall SonicOS 5.9.1.12 is a maintenance release that provides protection against a vulnerability. See the Resolved Issues section for more information.

SonicOS 5.9.1.12 provides all the features and resolved issues that were included in previous releases of SonicOS 5.9.1 and is a unified web post release with support for Gen5 platforms and SOHO.

NOTE: On SonicWall TZ series and some smaller NSA series platforms such as the NSA 220, performance may be affected after upgrading to SonicOS 5.9.1.12. This is due to the large number of features, enhancements, and vulnerability fixes provided in SonicOS 5.9 compared to the SonicOS 5.8 releases. These features and updates are essential to improving your network security.

For more information about other releases, see the previous release notes, available on MySonicWall at: https://www.mysonicwall.com/.

Supported Platforms

SonicOS 5.9.1.12 is supported on the following 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			

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

- Supported key features by platform
- Supported SonicPoint and wireless features by platform
- Supported/unsupported IPv6 features

Supported Key Features by Platform

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

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 215 Series	TZ 210 Series	TZ 205 Series	TZ 200 Series	TZ 105 Series	TZ 100 Series	SOHO Series
Active-Active Clustering	Y	N	N	N	N	N	N	N	N
Amazon VPC[a]	Y	Y	Y	Y	Y	Y	Y	Y	Y
App Rules Enhancement	Y	Y	Y	Y	Y	N	Y	N	Y
AppFlow Reports	Y	Y	Y	Y	N	N	N	N	N
ArcSight Syslog Format Support	Y	Y	Y	Y	Y	N	Y	N	Y
Bandwidth Management Enhancement	Y	Y	Y	Y	Y	Y	Y	Y	Y
BGP Advanced Routing	Y	Y[b]	Y[c]	N	N	N	N	N	N
CLI Enhancements[d]	Y	Y	Y	Y	Y	Y	Y	Y	Y
Client CFS Enforcement	Y	Y	Y	Y	Y	Y	Y	Y	Y
Common Access Card Support	Y	Y	Y	Y	Y	Y	Y	Y	Y

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 215 Series	TZ 210 Series	TZ 205 Series	TZ 200 Series	TZ 105 Series	TZ 100 Series	SOHO Series
Guest Admin Support	Y	Y	Y	Y	Y	N	Y	N	Y
IKE Dead Peer Detection	Y	Y	Y	Y	Y	Y	Y	Y	Y
IKEv2 Configuration Payload Support	Y	Y	Y	Y	Y	Y	Y	Y	Y
IPv6	Y	Y	Y	Y	Y	N	Y	N	Y
IPv6 6rd	Y	Y	Y	Y	Y	N	Y	N	Y
IPv6 BGP	Y	Y	Y	Y	Y	N	Y	N	Y
IPv6 DHCP PD	Y	Y	Y	Y	Y	N	Y	N	Y
IPv6 for Backend Servers	Y	Y	Y	Y	Y	N	Y	N	Y
LDAP User Group Monitoring	Y	Y	Y	Y	Y	Y	Y	Y	Y
LDAP User Group Monitoring	Y	Y	Y	Y	Y	Y	Y	Y	Y
Log Monitor Filter Input Box	Y	Y	Y	Y	Y	Y	Y	Y	Y
Logging Enhancement	Y	Y	Y	Y	Y	Y	Y	Y	Y
MOBIKE	Y	Y	Y	Y	Y	N	Y	N	Y
NetExtender WXAC Integration	Y	Y	Y	Y	Y	Y	Y	Y	Y
Network Device Protection Profile (NDPP Mode)	Y	Y	Y	Y	Y	Y	Y	Y	Y
Numbered Tunnel Interfaces for Route Based VPN	Y	Y[e]	N	N	N	N	N	N	N
One-Touch Configuration Overrides	Y	Y	Y	Y	Y	N	Y	N	Y
OpenSSH Vulnerability Security Enhancements	Y	Y	Y	Y	Y	Y	Y	Y	Y
Path MTU Discovery	Y	Y	Y	Y	Y	Y	Y	Y	Y

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 215 Series	TZ 210 Series	TZ 205 Series	TZ 200 Series	TZ 105 Series	TZ 100 Series	SOHO Series
Proxied Users Identification and Login	Y	Y	Y	Y	Y	Y	Y	Y	Y
Reassembly-Free Regular Expression for DPI Engine	Y	Y	Y	Y	Y	N	Y	N	Y
SHA-2 in IPsec	Y	Y	Y	Y	Y	Y	Y	Y	Y
SNMPv3	Y	Y	Y	Y	Y	Y	Y	Y	Y
SSL VPN Mobile Connect Bookmark	Y	Y	Y	Y	Y	Y	Y	Y	Y
SSL VPN Multi-Core Scalability	Y	Y	Y	N	Y	N	N	N	Y
SSO RADIUS Accounting	Y	Y[f]	N	N	N	N	N	N	N
TSR Enhancements	Y	Y	Y	Y	Y	Y	Y	Y	Y
UDP/ICMP Flood Protection	Y	Y	Y	Y	Y	N	Y	N	Y
Wire Mode 2.0	Y	Y[g]	N	N	N	N	N	N	N
WWAN 4G Support	Y	Y	Y	Y	Y	Y	Y	N	Y
XD Lookup for Access Rules	Y	Y	Y	Y	Y	Y	Y	Y	Y

a.Amazon VPC VPN connection using static routing is supported for all platforms. Amazon VPC VPN connection using dynamic routed is supported only on platforms that support BGP.
b.Not supported on NSA 240. NSA 250M series and NSA 220 series require a license for BGP.
c.Requires a license.
d.Limited CLI command set is supported on NSA 240 and all TZ models.
e.Supported only on NSA 250M and higher models; not supported on NSA 2400MX.
f.Supported only on NSA 3500 and higher models.
g.Supported only on NSA 3500 and higher models.

Supported SonicPoint and Wireless Features by Platform

The following table lists the SonicPoint and wireless 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	SOHO Series
External Guest Service Apache / PHP Support	Y	Y	Y	Y	Y	Y	Y	Y	Y
External Guides Service FQDN Support	Y	Y	Y	Y	Y	Y	Y	Y	Y
Guest Admin Support	Y	Y	Y	Y	Y	N	Y	N	Y
Internal Radio IDS Scan Scheduling[a]	N	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint 802.11e (WMM) OoS	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint Auto Provisioning	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint Retain Custom Configuration	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint DFS Support	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint Diagnostics Enhancement	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint FairNet Support	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint RADIUS Server Failover	Y	Y	Y	Y	Y	Y	Y	Y	Y
SoniPoint WPA TKIP Countermeasures and MIC Failure Flooding Detection and Protecton	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint Layer 3 Management	Y	Y[b]	Y	N	N	N	N	N	N
Traffic Quota-Based Guest Svc Policy	Y	Y	Y	Y	Y	Y	Y	Y	Y

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 215 Series	TZ 210 Series	TZ 205 Series	TZ 200 Series	TZ 105 Series	TZ 100 Series	SOHO Series
Virtual Access Point ACL Support	Y	Y	Y	Y	Y	Y	Y	Y	Y
Virtual Access Point ACL Support	Y	Y	Y	Y	Y	Y	Y	Y	Y
Virtual Access Point Scheduling	Y	Y	Y	Y	Y	Y	Y	Y	Y
Wireless Client Bridge Support[c]	N	Y	Y	Y	Y	Y	Y	Y	Y
Wireless PCI Rogue Detect Prevention	Y	Y	Y	Y	Y	Y	Y	Y	Y
Wireless Radio Built-In Scan Sched[d]									

a.Only supported on platforms with internal wireless radio.
b.Not supported on NSA 240.
c.Only Supported on platforms with internal wireless radio.
d.Only Supported on platforms with internal wireless radio.

Supported and Unsupported IPv6 Features

The table in this section summarizes the key SonicOS 5.9 features that support IPv6.

To see which appliance platforms support IPv6, refer to the section about Supported SonicPoint and Wireless Features by Platform.

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:
  • Land Attack
  • Ping of Death
  • Smurf
  • SYN Flood
• Connection Cache
• Connection Limiting for IPv6 connections
• Connection Monitor
• Content Filtering Service
• DHCP
• DNS client
	• 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:
	  • Multicast
	  • Oracle SQL/Net
	  • RTSP
	  • VoIP
	• IKEv1
	• IPv6 Syslog messages
	• L2TP

Features Available with IPv6	Features Not Available with IPv6

• DNS lookup and reverse name lookup
• Dynamic Routing (RIPng and OSPFv3)
• EPRT
• EPSV
• FTP
• Gateway Anti-Virus
• High Availability:
  • Connection Cache
  • FTP
  • IPv6 management IP address
  • NDP
  • SonicPoint
• HTTP/HTTPS management over IPv6
• ICMP
• IKEv2
• Intrusion Prevention Service
• IP Spoof Protection
• IPv4 Syslog messages, including messages with IPv6 addresses
• IPv6 BGP
• IPv6 for Backend Servers
• Layer 2 Bridge Mode
• Logging IPv6 events
• 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
	• LDAP
	• MAC-IP Anti-Spoof
	• NAT between IPv6 and IPv4 addresses
	• NAT High Availability probing
	• NetBIOS over VPN
	• NTP
	• QoS Mapping
	• RADIUS
	• RAS Multicast Forwarding
	• Route-based VPNs
	• Single Sign On
	• SIP
	• SMTP Real-Time Black List (RBL) Filtering
	• SSH
	• Transparent Mode
	• ViewPoint
	• Virtual Assistant
	• Web proxy

Features Available with IPv6	Features Not Available with IPv6
• VLAN interfaces with IPv6 addresses • VPN policies • Wireless • WireMode	

Resolved Issues

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

Encryption

Resolved issue	Issue ID
The TLS Padding (Zombie POODLE and GOLDENDOODLE) and ROBOT attack vulnerabilities exist in SonicOS. Occurs when a connection to the appliance uses cipher block-chaining (CBC).	215940

Known Issues

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

AppFlow

Known issue	Issue ID
The Create Rule option on the **Users** tab in **Dashboard > AppFlow Monitor** does not work correctly, and log messages are displayed on the console. Occurs when attempting to create a rule for a RADIUS user to block LAN to WAN access, when the user already belongs to a group that has LAN to WAN access.	167772
SSL VPN users are not displayed in **Dashboard > AppFlow Monitor** on the **Users** tab, only “unknown” users are shown. Occurs when several (10) SSL VPN users are connected to the firewall and AppFlow Reporting is enabled.	167149

Application Control

Known issue	Issue ID
The App Rule Match Object cannot match a filename. Occurs during an FTP download or upload and the **Match Type** of the **Firewall > Match Object** is set to **Prefix Match**, the **Input Representation** is set to **Hexadecimal Representation**, and the **Enable Negative Matching** option is selected. **Workaround:** Do not enable the Negative Matching option with the Prefix Match option.	135634
App Control policies do not block IPv6 traffic unless Intrusion Prevention Service is enabled. Occurs when IPS is disabled and an App Control policy is created from **Firewall > App Control Advanced** to block FTP traffic. A computer on the LAN side can still use an IPv6 IP address to connect to an FTP server. **Workaround:** Enable IPS. With IPS enabled, the App Control policy blocks the FTP connection.	128410

Command Line Interface

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

DPI-SSL

Known issue	Issue ID
The SSL proxied connection count cannot be cleared from the cache. Occurs when Client DPI-SSL is enabled and HTTPS traffic is passed through X0 and X2 which are configured in Layer 2 Bridge mode, and then X0 and X2 are changed to unassigned mode.	159332
The certificate from a secure website, such as `https://mail.google.com`, is not changed to a 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

Firmware

Known issue	Issue ID
Restore defaults button on Access not work.	182149

GVC Advanced Settings

Known issue	Issue ID
The address group cannot be added successfully. Occurs when configuring VPN policy, especially if Gateway Setup Destination Network obtains IP address using DHCP through a VPN Tunnel.	182239

High Availability

Known issue	Issue ID
The route polices added by OSPF/BGP/RIP route can't be deleted. Occurs when failover takes place.	182931

IPv6

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

Networking

Known issue	Issue ID
An administrator correctly receives an error message when attempting to delete a user defined IP-Helper protocol that is associated with an IP-Helper Policy. But if they also try to delete the policy followed by trying to add a new 'DNS' type policy, then the IP-Helper protocol and associated policy that they originally attempted to delete disappears.	183072
A DHCP ip-helper policy from ZONE VPN is not added from ZONE VPN. Occurs when a tunnel interface is added.	182751
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. Occurs when the X1 interface has obtained an IP address in PPTP mode and then the administrator reconfigures X1 in static mode and gives it a static IP address. **Workaround:** Restart the firewall to make X1 accessible again.	160164
The WAN interface cannot be accessed with HTTPS or ping after restarting the firewall. Occurs when X0 (LAN) has a redundant port configured and X0 physical status is "no link".	156619
The default route gateway is wrong after changing the WAN mode. Occurs when X1 is configured with IP Assignment in L2TP mode, then changed to PPTP mode, but the default route gateway is still the one learned from the L2TP server. After changing the WAN mode back to L2TP, the default route gateway is the one learned from the PPTP server.	154144
The paired interface does not go down when the other interface in the Wire Mode pair is brought down. Occurs when the **Enable Link State Propagation** option is enabled and a wire mode interface is brought down by performing a shutdown on the peer switch.	151827
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

Networking

Known issue	Issue ID
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
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
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

Upgrade

Known issue	Issue ID
NTP server authentication type changed from **MD5** to **No Auth**. Occurs after upgrade from 5.8.1.15 to 5.9.1.8.	183577

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". 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.	148167
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

VPN

Known issue	Issue ID
An active IPv6 VPN tunnel is not displayed in the table on the **VPN > Settings** page 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** page 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

System Compatibility

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

Wireless 3G/4G Broadband Devices

SonicOS 5.9 provides support for a wide variety of PC cards, USB devices and wireless service providers. For the most recent list of supported devices, see:
https://www.sonicwall.com/en-us/support/knowledge-base/170505473051240

NOTE: When connected to a 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

SonicWall Global Management System (GMS) 7.2 Service Pack 5 (or higher 7.2) or GMS 8.1 (or higher) are required for GMS management of SonicWall appliances running SonicOS 5.9.1.12.

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 5.9. The recommended firmware version for the WXA series appliances is WXA 1.3.2.

Browser Support

SonicWall recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS. This release supports the following web browsers:

- Chrome 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 16.0 and higher

- Internet Explorer 9.0 and higher (do not use compatibility mode)
- Safari 5.0 and higher running on non-Windows machines

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

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

Product Licensing

SonicWall network security platforms 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.

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 SonicWall appliance, and importing configuration settings from another appliance, see the *SonicOS 5.9 Upgrade Guide* available on the Support portal at https://www.sonicwall.com/support/technical-documentation.

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

NOTE: For SonicWall TZ series and some smaller NSA series platforms such as the NSA 220, performance may be affected after upgrading to SonicOS 5.9.1.12. This is due to the large number of features, enhancements, and vulnerability fixes provided in SonicOS 5.9, as compared to the SonicOS 5.8 releases. These features and updates are essential to better secure your network.

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: 3/22/19

232-004778-00 Rev A