

Release Notes

Contents

<i>Release Purpose</i>	1
<i>Platform Compatibility</i>	1
<i>Upgrading Information</i>	2
<i>Browser Support</i>	2
<i>WWAN 3G/4G Support</i>	2
<i>Known Issues</i>	3
<i>Resolved Issues</i>	8
<i>New Features in SonicOS 5.9.0.1</i>	11
<i>Supported Key Features</i>	15
<i>Related Technical Documentation</i>	20

Release Purpose

SonicOS 5.9.0.1 is an Early Release for Dell SonicWALL NSA E-Class, NSA, and TZ series network security appliances. It provides several new features and resolves a number of issues found in earlier releases.

Platform Compatibility

The SonicOS 5.9.0.1 release is supported on the following Dell SonicWALL Deep Packet Inspection (DPI) security appliances:

- NSA E8510
- NSA E8500
- NSA E7500
- NSA E6500
- NSA E5500
- NSA 5000
- NSA 4500
- NSA 3500
- NSA 2400
- NSA 2400MX
- NSA 250M / NSA 250M Wireless
- NSA 240
- NSA 220 / NSA 220 Wireless
- TZ 215 / TZ 215 Wireless
- TZ 210 / TZ 210 Wireless
- TZ 205 / TZ 205 Wireless
- TZ 200 / TZ 200 Wireless
- TZ 105 / TZ 105 Wireless
- TZ 100 / TZ 100 Wireless

The Dell SonicWALL WXA series appliances (WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are also supported for use with Dell SonicWALL security appliances running SonicOS 5.9. The recommended firmware version for the WXA series appliances is 1.2 or higher.

Release Notes

Upgrading Information

For information about obtaining the latest firmware, upgrading the firmware image on your Dell SonicWALL appliance, and importing configuration settings from another appliance, see the *SonicOS 5.9 Upgrade Guide* available on MySonicWALL or the www.sonicwall.com Support/Product Documentation page for NSA or TZ series:

<http://www.sonicwall.com/us/en/support/3643.html>

Browser Support



SonicOS with Visualization uses advanced browser technologies such as HTML5, which are supported in most recent browsers. Dell SonicWALL recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS.

This release supports the following Web browsers:

- Chrome 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 16.0 and higher
- Internet Explorer 8.0 and higher (do not use compatibility mode)
- Safari 5.0 and higher

Mobile device browsers are not recommended for Dell SonicWALL appliance system administration.

WWAN 3G/4G Support

SonicOS 5.9 supports a variety of 3G and 4G PC cards and USB devices for Wireless WAN connectivity. To use a 3G/4G interface you must have a 3G/4G PC card and a contract with a wireless service provider. A 3G/4G service provider should be selected based primarily on the availability of supported hardware, which is listed at:

<http://www.sonicwall.com/us/products/cardsupport.html>

In addition to devices supported on previous releases, SonicOS 5.9 includes support for the following 3G/4G devices:

- "T-Mobile Rocket 3.0" ZTE MF683 4G (USA)
- "AT&T Momentum" Sierra Wireless 313U 4G (USA)
- "AT&T Beam AirCard" Sierra Wireless 340U 4G (USA) (supported with LTE network, not with HSPA+)
- Pantech UML290 4G (USA)
- "Rogers Rocket Stick" Sierra Wireless 330U 4G (Canada)
- Kyocera 5005 (Asia/Europe)
- Huawei 398 (Asia/Europe)
- Huawei E353 (Asia/Europe)

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.

Release Notes

Known Issues

This section contains a list of known issues in the SonicOS 5.9.0.1 release.

3G/4G

Symptom	Condition / Workaround	Issue
With interface U0 configured as final backup or as primary WAN, the 4G device connects, but no traffic passes through it.	Occurs when using an "AT&T Beam AirCard" Sierra Wireless 340U 4G device without an external antenna and thus only able to negotiate HSPA+. Traffic can pass when using an external antenna to negotiate with the faster LTE network.	133999
Signal strength shown in the SonicOS 3G/4G Status page and in the 4G AT&T Beam AC340U LCD display can be inconsistent.	Occurs when the AT&T Beam makes its initial 4G connection after inserting it into the appliance and restarting. The AT&T Beam provides a single data channel which can be used to get the signal strength or to pass traffic. Upon startup, SonicOS gives priority to starting the WWAN connection over waiting for the device to report the correct signal strength. After the second connection, the signal strength displayed in SonicOS will match the LCD on the AT&T Beam.	133405
The appliance can shut down or restart automatically if a 3G or 4G USB device is inserted or removed.	Occurs when inserting or removing a 3G/4G USB device while the appliance is powered on. Observed with a HuaWei E353 HSPA+ USB Stick. Workaround: The appliance should always be powered off when inserting or removing a USB device. Hot plug and play is not supported.	130973

Active/Active Clustering

Symptom	Condition / Workaround	Issue
The backup units do not synchronize with the updated configuration on the active units.	Occurs when all connection ports on both backup units are disconnected, then the CLI is used to configure X0 on an active unit to enable RIP and set "Send Only", then the backup units are reconnected.	130316
No Virtual Group selection is available when using the Public Server Rule wizard on an Active/Active Clustering pair. The new policy is bound to Group 1.	Occurs when configuring a NAT policy and adding a public server for Group 2 from the Public Server Rule wizard. Workaround: Manually edit the NAT policy after using the wizard.	128631

Application Control

Symptom	Condition / Workaround	Issue
App Control policies do not block IPv6 traffic unless Intrusion Prevention Service (IPS) is enabled.	Occurs when IPS is disabled and an App Control policy is created from Firewall > App Control Advanced to block FTP traffic. A computer on the LAN side can still use an IPv6 IP address to connect to an FTP server. Workaround: Enable IPS. With IPS enabled, the App Control policy blocks the FTP connection	128410

Release Notes

DPI-SSL

Symptom	Condition / Workaround	Issue
The certificate from a secure website, such as https://mail.google.com, is not changed to the Dell SonicWALL DPI-SSL certificate when DPI-SSL is enabled, and the traffic cannot be inspected.	Occurs when a SonicPoint-N DR is connected to the appliance and Guest Services is enabled on the WLAN zone, and a wireless client connects via the SonicPoint, and the user logs into the guest account. Also, "Enable SSL Client Inspection" is set in the DPI-SSL > Client SSL page.	123097
An RDP remote desktop session cannot be established when DPI-SSL is enabled.	Occurs when the "Enable SSL Client Inspection" option is set in the DPI-SSL > Client SSL page, and a Windows 7 computer connects to the WLAN and then the user attempts to RDP to a Windows 7 computer on the LAN.	102701

High Availability

Symptom	Condition / Workaround	Issue
Logical monitoring and link aggregation features do not work when using High Availability probing.	Occurs when an IPv6 IP address is configured for the High Availability logical monitoring probe address. After the appliance is restarted, probing no longer works, causing issues with all logical monitoring and link aggregation.	131136

IPv6

Symptom	Condition / Workaround	Issue
Traffic does not pass through IPv6 VPN tunnels when the primary WAN is disabled.	Occurs when the primary WAN interface (X1) is disabled, and an IPv6 VPN tunnel is configured and bound to another WAN interface (X2). Negotiation is successful, but pings through the IPv6 tunnel are dropped.	134432
Traffic does not pass through an IPv6 SSL VPN tunnel to the WAN, in Tunnel All mode. The remote admin cannot connect to the IPv6 WAN address to manage the appliance.	Occurs when a remote client connects to the appliance using SSL VPN access and sends IPv6 traffic. IPv4 traffic works fine.	134344
Adding a second 6rd tunnel changes the 6rd address for the interface associated with the original 6rd tunnel. Deleting the second 6rd tunnel deletes that interface address. Adding the address again with original values results in an address using the second 6rd tunnel prefix.	Occurs when adding a second 6rd tunnel with a different prefix than the first 6rd tunnel. It causes the 6rd address of the interface for the first 6rd tunnel to change so that it corresponds to the prefix of the second 6rd tunnel.	134029
A Site-to-Site VPN tunnel does not work if an IPv6 6rd tunnel is also configured.	Occurs when the Advertise Subnet Prefix of IPv6 Primary Static Address option is enabled on one of the interfaces that connects the Site-to-Site tunnel.	133750
An App Rules exclusion list configured with an IPv6 Address Object does not prevent the policy from blocking traffic.	Occurs when an IPv6 Address Object is configured with the IPv6 address of a computer on the LAN, and this AO is used when configuring an exclusion list for an App Rules policy. The IPv6 computer should be able to access IPv6 websites that match the policy, but they are still blocked by the App Rules policy.	128363

Release Notes

Log

Symptom	Condition / Workaround	Issue
After restarting the appliance, Syslog Format using Enhanced Syslog becomes the default.	Occurs when Enable Analyzer Settings is selected on the Log > Analyzer page and Enhanced Syslog is selected for Syslog Format on the Log > Syslog page. The Syslog Format using Enhanced Syslog setting persists across an appliance restart, although it should not.	130835

Networking

Symptom	Condition / Workaround	Issue
An OSPF originated default route disappears from the Route Policies table of the firewall.	Occurs when OSPF is enabled on an interface used to connect two firewalls, the "Originate Default Route" option is set to "Always" on firewall #1, the originated default route appears in the Route Policies table on firewall #2, and then the value for "Apply the following metric to default routes received from Advanced Routing protocols" is changed on firewall #2.	134425
The value of ifHCInBroadcastPkts from an SNMP-GET differs from the value displayed for Rx Broadcast Packets in Network > Interfaces.	Occurs when comparing the Rx Broadcast Packets values shown in the Network > Interfaces page for each interface with the values obtained via SNMP.	131306
Wire Mode or Tap Mode cannot be configured because the IP Assignment field is disabled when editing an interface.	Occurs when editing an unassigned interface on a Stateful High Availability pair, and the WAN zone is selected. The IP Assignment field is set to Static and cannot be changed.	131050
FTP and HTTP traffic does not pass through a pair of interfaces in Wire Mode, set to Secure. Ping still passes.	Occurs when using a Stateful High Availability pair with Active/Active DPI enabled. The Active/Active DPI data interface is set to X7, while the Wire Mode interfaces are X2 and X6 in the LAN zone. The traffic between X2 and X6 fails, but traffic passes on other, static, interfaces.	101359

Security Services

Symptom	Condition / Workaround	Issue
A Gateway Anti-Virus exclusion list does not prevent GAV from blocking downloads from excluded IP addresses.	Occurs when a FQDN Address Object is used when configuring the GAV exclusion list.	121984

Release Notes

System

Symptom	Condition / Workaround	Issue
The administrator cannot access configuration mode on the LCD panel. The LCD panel displays an Invalid Code error message.	Occurs when the PIN code for the LCD panel is changed on the System > Administration page, and then the admin selects the configuration option on the LCD panel and enters the new PIN code.	130379
GMS 7.1 cannot synchronize with SonicOS after the appliance restarts following One Touch Configuration changes.	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 SonicOS management interface cannot be used to manage the appliance and large Ethernet packets are not forwarded.	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 an NSA E8510 10GE interface.	121657

Users

Symptom	Condition / Workaround	Issue
Single Sign-On (SSO) only works on Active-Active Clustering Virtual Group 1. SSO does not work on other Virtual Groups.	Occurs when SSO agents are configured in a clustered environment. Virtual Group 1 has a green status. However, all other Virtual Groups have a red status and do not work with the SSO Agent.	120202
Single Sign-On (SSO) does not work when Guest Services is enabled.	Occurs when both SSO and Guest Services are enabled. Guest Services blocks SSO authentication.	119001

VoIP

Symptom	Condition / Workaround	Issue
SonicOS drops SIP packets from the WAN to a Layer 2 Bridged LAN interface, and cannot establish a VoIP call. Ping works across the same path. The call can be established when using the primary LAN interface.	Occurs when interface X5 (LAN) is configured in L2 bridge mode and bridged to X0 (LAN). A Cisco phone is connected to X5 and is used to make a call to a phone on the WAN side, but the call cannot be established.	128225

Release Notes

VPN

Symptom	Condition / Workaround	Issue
An active IPv6 VPN tunnel is not displayed in the table on the VPN > Settings screen of the head-end firewall.	Occurs when two IPv6 VPN tunnels are created on both the head-end appliance and a remote appliance. The head-end VPN > Settings screen shows "2 Currently Active IPv6 Tunnels", but 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 the two appliances, with Advanced Routing enabled on the NSA 240 and a numbered tunnel interface is created on the NSA 7500 and 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 the OSPF connection cannot be established.	128419
User cannot change a Manual Key VPN policy to an IKE policy.	Occurs when the user attempts to change a Manual Key VPN policy to an IKE policy. The following message appears, "Remote IKE ID must be specified." Workaround: Delete the Manual Key policy and add a new IKE policy with the same IPsec gateway and source/destination networks.	112988
OSPF routing does not work properly after the VPN policy is deleted and re-created unless the appliance is restarted.	Occurs when a Tunnel Interface VPN policy is deleted and then re-created, with OSPF properly configured. OSPF will not connect until the appliance or the HA pair is restarted.	101510

Release Notes

Resolved Issues

This section contains a list of issues that are fixed in the SonicOS 5.9.0.1 release.

3G/4G

Symptom	Condition / Workaround	Issue
The appliance cannot connect to the Internet using a USB interface with a 4G device.	Occurs when using a 4G "AT&T Beam AirCard" Sierra Wireless 340U, which is not correctly detected by SonicOS 5.9.	132955
The Verizon U760 3G device is not recognized in SonicOS 5.9.0.0, preventing WWAN connectivity.	Occurs when using the Verizon U760 with a TZ 205W. Can occur when the 3G card is inserted and then the appliance is powered on. Can also occur after a successful WAN failover to the 3G device in interface U0, followed by restarting the firewall which then does not recognize the 3G device.	130802

Bandwidth Management

Symptom	Condition / Workaround	Issue
The Bandwidth management policy is not included in an access rule. The BWM tab is displayed in the Add access rule popup, but clicking the Add button does not apply the BWM policy to the rule.	Occurs when BWM is enabled globally and on the network interface, and an access rule for LAN to WAN or WAN to LAN is added.	127477

IPv6

Symptom	Condition / Workaround	Issue
The firewall displays a "Please wait" status for a long time, and when the page is refreshed it does not respond to management attempts for 10 minutes, then recovers and displays a Notice and a stack trace.	Occurs after attempting to ping an inaccessible IPv6 address from the System > Diagnostics page.	133974

Log

Symptom	Condition / Workaround	Issue
Dstname and arg values are missing in SonicOS 5.9 syslog messages, resulting in incomplete web activity reporting in GMS, Analyzer, and third party syslog reporting tools. Hostnames of the original URLs accessed are not logged or reported.	Occurs when an internal flow reporting collector is enabled on SonicOS 5.9.	133998
A syslog packet sent over a tunnel interface has zero for the source IP address.	Occurs when GMS is enabled on the local firewall and it sends syslog packets over a tunnel interface to a syslog host computer connected to the remote firewall LAN, and the GMS mode is HTTPS.	130488

Release Notes

Networking

Symptom	Condition / Workaround	Issue
Manually created access rules of the type "allow (or deny) Any Service from Any Source to Any Destination" are deleted after changing any configuration option for the source zone.	Occurs when the "Auto-generate Access Rules to allow traffic to zones with lower trust level" checkbox on the source zone page is initially cleared, and also when any other option is changed on the zone configuration page.	133585
Some routes disappear from the routing table after importing settings that include the routes.	Occurs when the routes reference tunnel interfaces with long names or when static routes are imported to a firewall that already has a number of static routes configured and the sum of the two sets of static routes exceeds the maximum limit, even though the imported routes are replacing the existing routes rather than adding to them.	128273
SonicOS incorrectly sends an Unsupported Capability Notification and resets the BGP connection.	Occurs when SonicOS receives a capability from the BGP peer (Amazon VPC, in this case) that it does not understand. Per RFC 5492, such capabilities must be ignored when received.	127742
Static routes added or modified with a network prefix not using 24 bits of the 32-bit IP address are not shown and redistributed until after restarting the appliance.	Occurs when modifying an address object used as the destination object in a PBR route, such as changing the network prefix from 24 to 23 bits, or from 23 to 24 bits.	127674

SSL VPN

Symptom	Condition / Workaround	Issue
SSLVPN Tunnel All mode does not pass traffic from the SSLVPN zone to the WAN zone.	Occurs when the primary WAN interface is not X1 and a remote SSLVPN client connects and attempts to send traffic to the WAN.	134088
Web based management and SSH management do not work over SSL VPN. Packets are dropped due to an IP spoof check.	Occurs when connecting to the appliance with the NetExtender SSL VPN feature and access is enabled from the SSL VPN zone to the LAN zone.	131811
The WAN interface becomes unresponsive to Ping or HTTPS requests after a high number of NetExtender logins.	Occurs when 1000 NetExtender logins and logouts have taken place at a rate of one every 3 seconds, using a Linux NetExtender client, with the client inactivity timeout set to 10 minutes.	131421
NetExtender login fails with the log entry "IP address in pool is exhausted" after 917 successful logins using NetExtender.	Occurs when 1000 NetExtender logins were previously successful and the client IP address pool has 1000 addresses in it.	131186

System

Symptom	Condition / Workaround	Issue
An internal web server behind the firewall becomes slow to respond and the firewall CPU utilization gets above 80%.	Occurs when hping3 is used to generate various TCP flood attacks aimed at the public NAT IP address of the web server.	131338

Release Notes

User Interface

Symptom	Condition / Workaround	Issue
The SonicOS administrator can be remotely logged out by an unauthenticated web browser.	Occurs under certain very rare circumstances when HTTP / HTTPS web management is enabled on the network interface.	133699
The LDAP configuration button is missing on the Users > Settings page.	Occurs when the user authentication method for login is set to Local Users, and Single Sign-On is enabled with its method for setting user group memberships configured as LDAP Lookup.	127691

Users

Symptom	Condition / Workaround	Issue
User authentication redirects result in certificate warnings.	Occurs when the appliance redirects the user to a secure login page at the local interface IP address, when the appliance has a registered certificate with a domain name as the common name. This is resolved by enhancements to the Users > Settings page, allowing the administrator to configure a domain name for the user redirect so that it will match the name in the certificate.	124551

Wireless

Symptom	Condition / Workaround	Issue
The SonicPoint > IDS page displays multiple entries for each SonicPoint.	Occurs when more than one SonicPoint is configured in the network.	133735
After upgrade, WLAN users bypassed from Guest Authentication on one firewall are unable to access resources behind a second firewall across a tunnel interface VPN.	Occurs when the first firewall is upgraded from 5.8.1.12 to 5.9.0.0.	133524

Release Notes

New Features in SonicOS 5.9.0.1

SonicOS 5.9.0.1 provides the following new features and enhancements:

<i>IPv6 DHCP Prefix Delegation</i>	11
<i>IPv6 6rd</i>	11
<i>Redirect to FQDN for User Web Login</i>	13
<i>SSL VPN Maximum Concurrent Users Increase</i>	14

IPv6 DHCP Prefix Delegation

IPv6 DHCP Prefix Delegation (DHCPv6-PD) is an extension to DHCPv6 (DHCP for IPv6). In DHCPv6, addresses are assigned by a DHCPv6 server to an IPv6 host. DHCPv6-PD is an additional subnet-configuration mode that co-exists with DHCPv6. In DHCPv6-PD, complete IPv6 subnet addresses and other parameters are assigned by a DHCPv6-PD server to a DHCPv6-PD client.

When DHCPv6-PD is enabled, it is applied to all DHCPv6 interfaces attached to the WAN zone.

The IPv6 address is a combination of the prefix provided by the DHCPv6-PD server and the suffix provided by the DHCPv6-PD client. The prefix length is 64 by default, but can be edited.

When the firewall starts, a default address object group called *Prefixes from DHCPv6 Delegation* is automatically created. Prefixes delegated from the upstream interface are members of this group.

DHCPv6 Prefix Delegation is configured on the following:

- An upstream interface
- One or more downstream interfaces

When the upstream interface learns the prefix delegation from the DHCPv6-PD server, SonicOS calculates and applies the IPv6 address prefixes to all the downstream interfaces, and the downstream interfaces advertise this information to all the hosts in their network segments.

IPv6 6rd

IPv6 Rapid Deployment (6rd) enables IPv6 to be deployed across an IPv4 network quickly and easily. 6rd utilizes a Service Provider's existing IPv6 address prefixes, ensuring that the 6rd operational domain is limited to the Service Provider's network and is under the Service Provider's direct control.

When 6rd is deployed, the IPv6 service is equivalent to native IPv6. 6rd mapping of IPv6 addresses to IPv4 addresses provides automatic determination of IPv4 tunnel endpoints from IPv6 prefixes, allowing stateless operation of 6rd.

A 6rd domain consists of several 6rd customer edge (CE) routers and one or more 6rd border relays (BRs). IPv6 packets encapsulated by 6rd follow the IPv4 routing topology within the service provider network. IPv6 packets traverse the border relays when they enter or exit a Service Provider's 6rd domain. Since 6rd is stateless, packets can be sent to the border relays using the Anycast method.

A 6rd domain can have only one 6rd prefix. Service Provider's may deploy 6rd in a single domain or in multiple domains.

On the Network > Routing page, in the Route Policies panel, there are four default route policies for 6rd tunnel interfaces.

Note: A 6rd tunnel interface must be bound to a physical or a virtual interface. In DHCP mode, the 6rd parameters are received from the bound interface. In Manual mode, the 6rd parameters must be configured manually.

The following four parameters can be set manually, or they can be set automatically by the DHCPv4 server.

- IPv4 Mask Length
- 6rd Prefix
- 6rd Prefix Length
- 6rdBRIPv4Address

Release Notes

A 6rd tunnel interface is configured in the same way as other IPv6 tunnel interfaces:

1. On the Network > Interfaces page, select the **IPv6** radio button.

Network /
Interfaces

Accept

Interface Settings View IP Version: IPv4 IPv6

Name	Zone	IP Assignment	IP Address/Prefix Length	IP Type	Status	Comment	Configure
X0	LAN	Static	fe80::217:c5ff:fe0f:6d4c/64	Automatic	No link	Default LAN	
X1	WAN	DHCPv6 <input type="button" value="Renew"/>	fe80::217:c5ff:fe0f:6d4d/64	Automatic	1 Gbps Full Duplex	Default WAN	
X2	Unassigned	N/A			No link		
X3	Unassigned	N/A			No link		
X4	Unassigned	N/A			No link		
X5	Unassigned	N/A			1 Gbps Full Duplex		
6rdTunnel	WAN	6rd Tunnel	2001::2/64	Static	Interface Down		

Add Interface: --Select Interface Type--

2. At the bottom of the Interface Settings table, select **Tunnel Interface** as the Interface Type in the **Add Interface** field. The Edit Interface configuration window is displayed.

Dell SonicWALL | Network Security Appliance

General

Interface Settings for IPv6

Zone:

Interface Type:

Tunnel Type:

Name:

Tunnel Interface IPv6 Address:

Prefix Length:

Bound to:

Configure Mode:

6rd Prefix:

6rd Prefix Length:

BR IPv4 Address:

IPv4 Mask Length:

Comment:

Add Default Route Automatically

Management: HTTP HTTPS Ping SNMP

Ready

3. In the configuration window, select **6rd Tunnel Interface** as the Tunnel Type.
4. Configure the other fields and click **OK**.

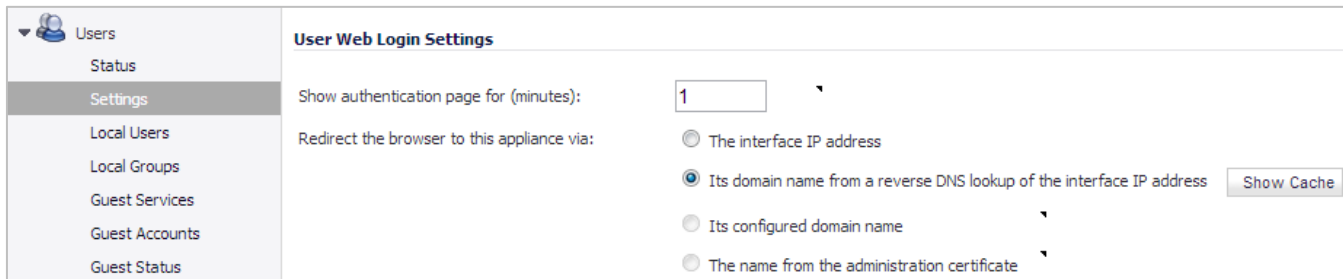
See the *SonicOS 5.9 Administrator's Guide* for the complete procedure.

Release Notes

Redirect to FQDN for User Web Login

When user authentication is enabled in SonicOS, a connecting user is redirected to a secure login page, using HTTPS. In previous releases, the administrator could only configure an appliance LAN IP address for the redirect. This redirect to “https://<local IP address>” could cause a certificate warning to display, requiring the user to click the option to continue to the website in order to log in.

SonicOS 5.9.0.1 provides additional options on the Users > Settings page, allowing the administrator to enable redirecting to a domain name as well as to an IP address.



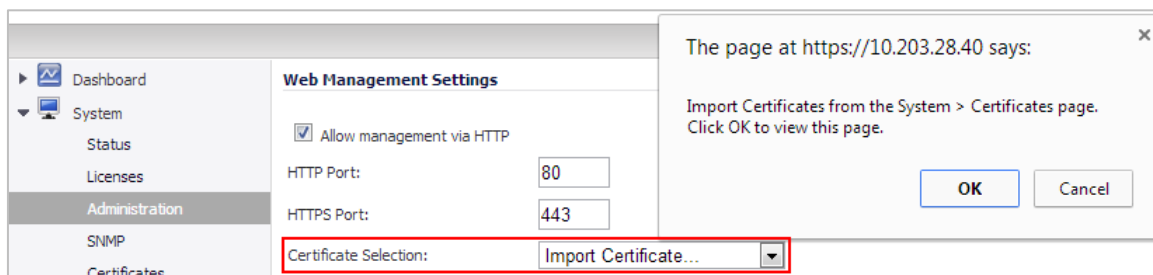
Options are available to redirect to the following:

- **The interface IP address** – This option redirects the user to the IP address of the interface to which his computer or local network is connected. This operates the same as in previous releases.
- **Its domain name from a reverse DNS lookup of the interface IP address** – This option causes the appliance to determine the Fully Qualified Domain Name of the interface IP address, and redirect the user to that domain name. For this to work, Reverse DNS must be enabled for the domain in the DNS server.
- **Its configured domain name** – This option redirects the user to the domain name that is configured on the System > Administration page. The firewall’s domain name must be configured there before this redirect can work, and in each zone that users will be logging in from, it must be a valid domain name that resolves to an interface IP address. Possible zones include LAN, WLAN, WAN, etc.



The domain name needs to be registered in the DNS server for each zone, and must resolve to the correct interface IP address for that zone. The domain name can be private, for internal users, or an externally registered domain name.

- **The name from the administration certificate** – This option redirects the user to the domain name (common name) in the certificate that was imported. The certificate must be imported on the System > Administration page before this redirect can work, and as above it must be a valid domain name in each zone that users will be logging in from.



A SAN (Subject Alternative Names) certificate can secure multiple domain names. Importing this type of certificate allows error-free user authentication redirects for several domains.

Release Notes

SSL VPN Maximum Concurrent Users Increase

The maximum number of SSL VPN concurrent users is increased in SonicOS 5.9.0.1. The following table shows the maximum number of SSL VPN concurrent users for each Dell SonicWALL network security appliance model:

Appliance Platform	Max Concurrent SSL VPN Users
NSA E8510	1500
NSA E8500	1500
NSA E7500	1000
NSA E6500	750
NSA E5500	500
NSA 5000	350
NSA 4500	350
NSA 3500	250
NSA 2400 / 2400MX	125
NSA 250M / 250MW	50
NSA 240	50
NSA 220 / 220W	50
TZ 215 / 215W	25
TZ 210 / 210W	25
TZ 205 / 205W	15
TZ 200 / 200W	10
TZ 105 / 105W	10
TZ 100 / 100W	5

Release Notes

Supported Key Features

Supported Key Features by Platform.....	15
Supported SonicPoint and Wireless Features by Platform.....	17
Supported/Unsupported IPv6 Features.....	18

Supported Key Features by Platform

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

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 215 Series	TZ 210 Series	TZ 205 Series	TZ 200 Series	TZ 105 Series	TZ 100 Series
Active-Active Clustering	✓	✗	✗	✗	✗	✗	✗	✗
Amazon VPC Support	✓	✓ ¹	✗	✗	✗	✗	✗	✗
AppFlow Reports	✓	✓	✓	✓	✗	✗	✗	✗
App Rules Enhancement	✓	✓	✓	✓	✓	✗	✓	✗
ArcSight Syslog Format Support	✓	✓	✓	✓	✓	✗	✓	✗
Bandwidth Management Enhancement	✓	✓	✓	✓	✓	✓	✓	✓
BGP Advanced Routing	✓	✓ ²	✓ ³	✗	✗	✗	✗	✗
CLI Enhancements ⁴	✓	✓	✓	✓	✓	✓	✓	✓
Common Access Card Support	✓	✓	✓	✓	✓	✓	✓	✓
IKEv2 Configuration Payload Support	✓	✓	✓	✓	✓	✓	✓	✓
IKE Dead Peer Detection	✓	✓	✓	✓	✓	✓	✓	✓
IPv6	✓	✓	✓	✓	✓	✗	✓	✗
IPv6 6rd	✓	✓	✓	✓	✓	✗	✓	✗
IPv6 DHCP-PD	✓	✓	✓	✓	✓	✗	✓	✗
LDAP User Group Monitoring	✓	✓	✓	✓	✓	✓	✓	✓
LDAP Group Membership by Organizational Unit	✓	✓	✓	✓	✓	✓	✓	✓
Logging Enhancement	✓	✓	✓	✓	✓	✓	✓	✓
MOBIKE	✓	✓	✓	✓	✓	✗	✓	✗

¹ Not supported on NSA 240 or NSA 220 series.

² Not supported on NSA 240. NSA 250M series and NSA 220 series require a license for BGP.

³ Requires License

⁴ Limited CLI command set is supported on NSA 240 and all TZ models

Release Notes

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
NetExtender WXAC Integration	✓	✓	✓	✓	✓	✓	✓	✓
Network Device Protection Profile (NDPP Mode)	✓	✓	✓	✓	✓	✓	✓	✓
Numbered Tunnel Interfaces for Route Based VPN	✓	✓ ⁵	✗	✗	✗	✗	✗	✗
One-Touch Configuration Overrides	✓	✓	✓	✓	✓	✗	✓	✗
OpenSSH Vulnerability Security Enhancements	✓	✓	✓	✓	✓	✓	✓	✓
Path MTU Discovery	✓	✓	✓	✓	✓	✓	✓	✓
Proxied Users Identification and login	✓	✓	✓	✓	✓	✓	✓	✓
Reassembly-Free Regular Expression for DPI Engine	✓	✓	✓	✓	✓	✗	✓	✗
SHA-2 in IPsec	✓	✓	✓	✓	✓	✓	✓	✓
SNMPv3	✓	✓	✓	✓	✓	✓	✓	✓
SSL-VPN Multi-Core Scalability	✓	✓	✓	✗	✓	✗	✗	✗
SSO RADIUS Accounting	✓	✓ ⁶	✗	✗	✗	✗	✗	✗
TSR Enhancements	✓	✓	✓	✓	✓	✓	✓	✓
UDP/ICMP Flood Protection	✓	✓	✓	✓	✓	✗	✓	✗
Wire Mode 2.0	✓	✓ ⁷	✗	✗	✗	✗	✗	✗
WWAN 4G support	✓	✓	✓	✓	✓	✓	✓	✗
XD Lookup for Access Rules	✓	✓	✓	✓	✓	✓	✓	✓
YouTube for Schools Support	✓	✓	✓	✓	✓	✓	✓	✓

⁵ Supported only on NSA 250M and higher models; not supported on NSA 2400MX

⁶ Supported only on NSA 3500 and higher models

⁷ Supported only on NSA 3500 and higher models

Release Notes

Supported SonicPoint and Wireless Features by Platform

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 215 Series	TZ 210 Series	TZ 205 Series	TZ 200 Series	TZ 105 Series	TZ 100 Series
External Guest Service Apache / PHP support	✓	✓	✓	✓	✓	✓	✓	✓
External Guest Service FQDN support	✓	✓	✓	✓	✓	✓	✓	✓
Guest Admin Support	✓	✓	✓	✓	✓	✗	✓	✗
Internal Radio IDS scan scheduling ⁸	✗	✓	✓	✓	✓	✓	✓	✓
SonicPoint 802.11e (WMM) QoS	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint Auto Provisioning	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint retain custom configuration	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint DFS support	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint Diagnostics Enhancement	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint FairNet Support	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint RADIUS Server Failover	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint WPA TKIP Countermeasures and MIC Failure Flooding Detection and Protection	✓	✓	✓	✓	✓	✓	✓	✓
SonicPoint Layer 3 Management	✓	✓ ⁹	✓	✗	✗	✗	✗	✗
Traffic Quota-based Guest Svc Policy	✓	✓	✓	✓	✓	✓	✓	✓
Virtual Access Point ACL Support	✓	✓	✓	✓	✓	✗	✓	✗
Virtual Access Point group sharing across dual radios	✓	✓	✓	✓	✓	✓	✓	✓
Virtual Access Point Layer 2 bridging	✓	✓	✓	✓	✓	✓	✓	✓
Virtual Access Point scheduling	✓	✓	✓	✓	✓	✗	✓	✗
Wireless Client Bridge Support ¹⁰	✗	✓	✓	✓	✓	✓	✓	✓
Wireless PCI Rogue detect/prevention	✓	✓	✓	✓	✓	✓	✓	✓
Wireless Radio Built-in Scan Sched ¹¹	✗	✓	✓	✓	✓	✓	✓	✓

⁸ Only supported on platforms with internal wireless radio

⁹ Not supported on NSA 240

¹⁰ Only supported on platforms with internal wireless radio

¹¹ Only supported on platforms with internal wireless radio

Release Notes

Supported/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 “Supported Key Features by Platform” section.

IPv6 Features Supported	IPv6 Features Not Currently Supported
<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ Land Attack ○ Ping of Death ○ Smurf ○ SYN Flood • Connection Cache • Connection Limiting for IPv6 connections • Connection Monitor • Content Filtering Service • DHCP • DNS client • DNS lookup and reverse name lookup • Dynamic Routing (RIPng and OSPFv3) • EPRT • EPSV • FTP • Gateway Anti-Virus • High Availability: <ul style="list-style-type: none"> ○ 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 • Layer 2 Bridge Mode • Logging IPv6 events • Login uniqueness • Multicast Routing with Multicast Listener Discovery • NAT • Neighbor Discovery Protocol • NetExtender connections for users with IPv6 addresses • Packet Capture • Ping • Policy Based Routing • PPPoE • Remote management 	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ Multicast ○ Oracle SQL/Net ○ RTSP ○ VoIP • IKEv1 • IPv6 Syslog messages • L2TP • LDAP • MAC-IP Anti-Spoof • NAT between IPv6 and IPv4 addresses • NAT High Availability probing • NAT load balancing • 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 • Wiremode

Release Notes

IPv6 Features Supported	IPv6 Features Not Currently Supported
<ul style="list-style-type: none">• Security services for IPv6 traffic with DPI• Site-to-site IPv6 tunnel with IPsec for security• SonicPoint IPv6 support• SNMP• SSL VPN• Stateful inspection of IPv6 traffic• User status• Visualization• VLAN interfaces with IPv6 addresses• VPN policies• Wireless	

Release Notes

Related Technical Documentation

Dell SonicWALL user guides and reference documentation are available at the Dell SonicWALL Technical Documentation Online Library: <http://www.sonicwall.com/us/Support.html>

For basic and advanced deployment examples, refer to SonicOS Guides and SonicOS TechNotes available on the website.

The screenshot shows the Dell SonicWALL Product Support page for E-Class NSA Series Appliances. The page features a navigation menu on the left with categories like Support, Product Documentation, and Self-Help Resources. The main content area includes a product image, social media sharing options, and sections for Support Documents, Product Guides, and Technical Notes. The Product Guides section lists several documents with their respective dates.

Document Title	Date
SonicOS Combined Log Events Reference Guide	12 Sep 2013
SonicOS 5.9 Log Event Reference Guide	12 Sep 2013
SonicOS 5.9 Administrator's Guide	4 Sep 2013
SonicOS 5.9 One Touch Configuration Guide	16 Jul 2013
SonicOS 5.9 Enterprise CLI Reference Guide	16 Jul 2013
SonicOS 5.9 Upgrade Guide	16 Jul 2013

Document Title	Date
Integrating CradlePoint with SonicOS 5.9	16 Nov 2012
Integrating Agilink with SonicOS 5.9	16 Nov 2012
Configuring SonicOS 5.8.1.8 for Amazon VPC Tech Note	8 Oct 2012

Last updated: 9/27/2013