Dell SonicWALL™ SonicOS 6.2.5.1

Release Notes

March 2016

These release notes provide information about the Dell SonicWALL™ SonicOS 6.2.5.1 release.

Topics:

About SonicOS 6.2.5.1

The SonicOS 6.2.5.1 release simplifies firmware management for Dell SonicWALL customers by offering a single consolidated software platform for the majority of the 6th generation Dell SonicWALL firewalls while also adding many new important features. For the complete list of features released with SonicOS 6.2.5.1, see New features.

Supported platforms

The SonicOS 6.2.5.1 release is supported on the following Dell SonicWALL network security appliances:

• SuperMassive 9600	• NSA 6600	• TZ600
• SuperMassive 9400	• NSA 5600	• TZ500 and TZ500 Wireless
• SuperMassive 9200	• NSA 4600	• TZ400 and TZ400 Wireless
	• NSA 3600	• TZ300 and TZ300 Wireless
	• NSA 2600	• SOHO Wireless

New features

This section describes the new features in the SonicOS 6.2.5.1 release.

- Dell X-Series switch integration
- DPI-SSL enhancements
- DPI-SSL Strengthened Encryption Methods
- Disable DPI Option for Firewall Access Rules
- Unified Capabilities Approved Product List (UC-APL) enhancements
- Firewall Sandwich support
- Wire Mode VLAN translation mapping
- Numbered VPN tunnel interfaces
- Change Auditor Support in AppFlow
- Botnet Source Identification in AppFlow Monitor
- Gateway Anti-Virus Detection Only Mode
- Control Plane Flood Protection
- Shutdown Port Option
- Port based network monitoring
- Disable Source Port Remapping option for NAT
- Suffix Option for HA/Clustered Firewalls
- Source/Destination IP address binding for Round Robin/Spillover load balancing
- SonicPoint ACe/ACi/N2 FCC new rule certification for DFS channels
- Feature support on TZ Series and SOHO Wireless appliances

Dell X-Series switch integration

Dell X-Series switches can now be managed easily within TZ series firewalls to offer a single pane of glass management of the entire network security infrastructure. This feature is supported on the following TZ series platforms:

- TZ600
- TZ500/TZ500 W
- TZ400/TZ400 W
- TZ300/TZ300 W

Supported X-Series switch models include:

- X1008/X1008P
- X1018/X1018P
- X1026/X1026P
- X1052/X1052P
- X4012

This feature allows unified management of both the firewall and the switch using the SonicOS management interface and Dell SonicWALL GMS.

IMPORTANT: GMS management of both the firewall and the switch requires GMS 8.1 Service Pack 1. This feature is not supported by lower versions of GMS.

The maximum number of interfaces available on the supported Dell SonicWALL TZ models range from 5 (TZ300) to 10 (TZ600). In certain deployments, the number of ports required might easily exceed the maximum number of interfaces available on the TZ. With the TZ/X-Series solution, ports on the X-Series switch can be viewed as "extended" interfaces of the firewall, thereby increasing the number of interfaces available for use.

Provisioning of an X-series switch is performed from SonicOS on the **Network > PortShield Groups** page.

Below is the key set of features supported with the TZ/X-Series solution:

- Provisioning of X-Series switch as Extended Switch
- PortShield functionality and protection propagated to the Extended Switch
- Configuration of Extended Switch interface settings
- Manageability of basic Extended Switch global parameters
- Manageability of Extended Switch using GMS
- High Availability and PortShield
- Diagnostics support for Extended Switch

For more information about Dell X-Series switch integration, see these Knowledge Base articles:

- Dell SonicWALL X-Series Solution: Dell SonicWALL integration with Dell X-Series Switches FAQ (KB 185430)
- Dell SonicWALL X-Series Solution Overview (KB 185439)
- Dell SonicWALL TZ - X solution: How to provision X-Series switches on SonicWALL TZ series firewalls (KB 185057)
- Dell SonicWALL X-Series Solution: How to provision Dell X-Series Switches on a SonicWALL TZ High Availability (HA) system (KB 186085)
- Dell SonicWALL X- Series Solution - How to manage Dell X-Series switch's admin credentials and management IP through the Dell X-Switch's UI (KB 185479)
- Dell SonicWALL X-Series Solution: Which models of Dell X-Switches has support for POE+ (KB 186709)
- Dell SonicWALL TZ Series and Dell SonicWALL X-Series solution managing SonicPoint ACe/ACi/N2 access points (SW13970)

DPI-SSL enhancements

The DPI-SSL enhancements in SonicOS 6.2.5.1 include:

Enhancement	Description
CFS category-based exclusion/inclusion	This feature enables DPI-SSL to use the CFS category list to exclude or include specific categories from or for DPI-SSL inspection. The CFS categories are provided on the **DPI-SSL > Client SSL** page and work in the same fashion. This feature is available when DPI-SSL is licensed.
Dynamic Exclusions	DPI-SSL dynamically determines if a connection should be intercepted (included) or excluded, based on policy or configuration. When DPI-SSL extracts the domain name for the connection, exclusion information is readily available for subsequent connections to the same server/domain.
TLS 1.2 support	DPI-SSL supports TLS 1.2, SHA-256 and Perfect Forward Secrecy.

Enhancement	Description
Increased default CA cert database	The default, or Built-In, CA-certificate database has been increased to 39 domains.
Management audit of default bypass behaviors	A new option on the **General** tab of the **DPI-SSL > Client SSL** page allows new built-in domain names to be examined before they are added to the Built-In, CA-certificate database for exclusion.
Troubleshoot connection failures with one-click exclude	SonicOS keeps a list of all client SSL connection failures and the reason for failure. This Connection Failure List allows quick inspection of connection failures and provides a one-click option to exclude a failed domain.
Granular policies per common name/domain name	This feature allows the administrator to exclude individual domains from the global authentication policy.
Customized default exemption database	To reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections, trusted domains can be added to the Built-In exclusion database.
Server certificate authentication (for exclusions and decryption)	Options on the **DPI-SSL > DPI Client** page allow server certificates to always be authenticated or before applying exclusion policies.
Proxy environment support (exclusions)	DPI-SSL supports proxy environments, where all client browsers redirect to a proxy server, including if an appliance sits between the client browsers and the proxy server. All DPI-SSL features are supported, including domain exclusions when the domain is part of a virtual hosting server, as part of a server farm fronted with a load balancer, or in some cloud deployments, wherein the same server IP can be used by multiple domains.
Subject alternate name support — `*.google.com` vs. `youtube.com`	DPI-SSL can be customized to support individual exclusion/inclusion of alternate names for a domain that is part of a list of domains supported by the same server (certificate). For example, excluding `youtube.com` while including `*.google.com`.
Refreshed UI	A new UI is available at **DPI-SSL > Client SSL** and **System > Licenses** pages to support all the new DPI SSL enhancements listed.

DPI-SSL session capacities

With SonicOS 6.2.5.1, DPI-SSL session capacities have been increased significantly on the 6th generation NSA and SM series appliances:

Platform	Max sessions	Platform	Max sessions	Platform	Max sessions
SuperMassive 9600	12,000	NSA 6600	6,000	TZ600	250
SuperMassive 9400	10,000	NSA 5600	4,000	TZ500/500W	250
SuperMassive 9200	8,000	NSA 4600	3,000	TZ400/400W	250
		NSA 3600	2,000	TZ300/300W	250
		NSA 2600	1,000	SOHO W	100

DPI-SSL Strengthened Encryption Methods

DPI-SSL now supports SHA-256 and TLS 1.2.

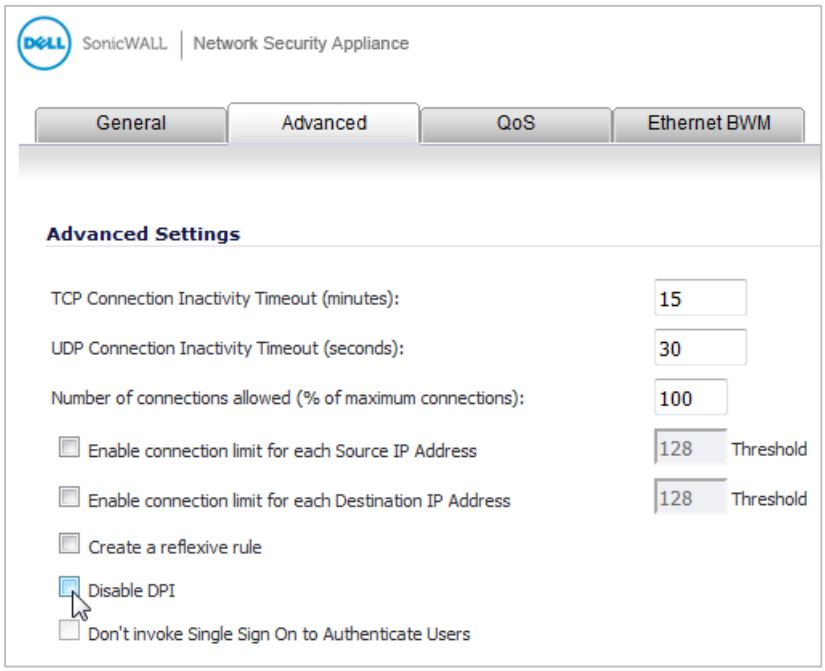
All the re-signed server certificates are now signed with the SHA-256 hash algorithm.

The TLS 1.2 communication protocol is now supported during SSL inspection/decryption between the firewall and the server (previously, TLS 1.2 was only supported between client and firewall) in DPI-SSL deployments. SonicOS already supports TLS 1.2 in other areas, as well.

Disable DPI Option for Firewall Access Rules

A new **Disable DPI** checkbox is provided on the **Advanced** tab when creating an access rule from the **Firewall > Access Rules** page. This allows the administrator to disable Deep Packet Inspection on a per-rule basis.

Disable DPI option



Unified Capabilities Approved Product List (UC-APL) enhancements

In addition to all FIPS and NDPP features from SonicOS 5.9.0/6.2.0, the UC-APL enhancements in SonicOS 6.2.5.1 include:

Enhancement	Description
New FIPS 2K certificate signing support	FIPS (Federal Information Processing Standards) 112 bits of security strength (2048 bits key) is supported while maintaining backward compatibility with previous signature modes.
Role-based administrator support	Adds these DoD UCR 4.2.3-defined administrator roles in addition to those already supported: • System Administrator • Cryptographic Administrator • Audit Administrator To support these new administrator roles, three new, editable user groups have been added, and an option has been added to the **Multiple Administrator** section of the **System > Administration** page.
OpenSSL 1.0.1h support	Open-source implementation for SSL and TLS protocols is supported.
TLS 1.1+ enforcement support	A new option in the **Web Management Settings** section on the **System > Administration** page allows enforcement of TLS 1.1 and above.
Web UI and E-CLI Login Banner compliance support	A new option in the **User Web Login Settings** section on the **Users> Settings** page enables display of a policy banner when a user logs in. The displayed policy must be accepted before the user can log in. The option has template and preview features.

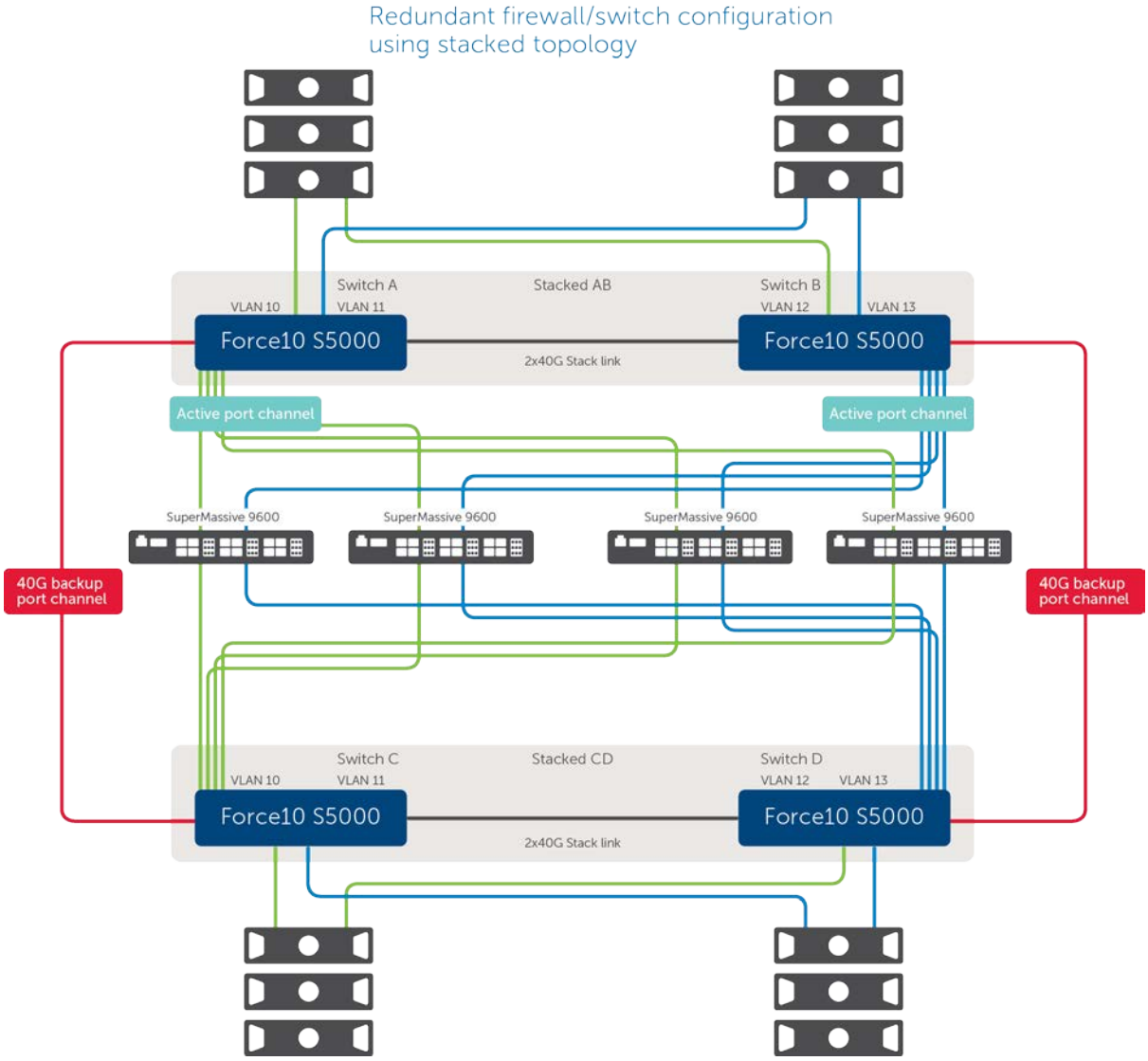
Enhancement		Description
Two factor authentication (CAC) enhancement		SonicOS had already provided client certificate status checking during the user login process. To support Common Access Card (CAC), SonicOS now also periodically performs an expiration check on a customer-imported certificate. To support this feature, a new option has been added to the **System > Administration** page.
LDAP TLS MS-CHAPv2 support		To support MS-CHAPv2 LDAP authentication, a new option has been added to the **Users > Settings > LDAP Configuration** dialog. Selecting this option enforces use of MS-CHAPv2 authentication. If a RADIUS server is also configured, it will provide authentication if LDAP authentication fails.
MS-CHAPv2 RADIUS authentication enforcement		To support MS-CHAPv2 RADIUS authentication, a new option has been added to the **Users > Settings > RADIUS Configuration** dialog. Selecting this option enforces use of MS-CHAPv2 authentication.
ICMPv6 Packet detection report and log support		SonicOS now validates packet extension headers and logs each invalid extension header in accordance with RFC2460. This function is configurable by two new options on the **Firewall Settings > Advanced** page.
Firewall obscures display after administrator times out		The management UI now logs out the administrator automatically when the administrator's session times out.
OOBM (Out-Of-Band-Management) support		A new option in the **Advanced Management** section of the **System > Administration** page enables automatic creation of a route policy for the MGMT interface, which works as an out-of-band interface. To avoid conflicts when deleting/creating route policies, enabling/disabling the OOBM option causes the appliance to reboot. This MGMT interface provides a trusted interface to manage the appliance. Network connections to this interface are very limited. If the NTP, DNS, and SYSLOG servers are configured in the MGMT subnet, the appliance uses the MGMT IP as the source IP and creates MGMT address object and route policies automatically. All traffic from the MGMT interface is routed by this policy. Created routes display on the **Network > Routing** page. The MGMT address object and route policies are created and updated using the IPv4 MGMT address IP. As the IPv6 management IP address object is created by default, this feature doesn't work with IPv6 management IP address object creation.
Certificate expiration notification		A new section on the **System > Administration** page, **Check certificate expiration settings**, enables periodic checking for expired certificates and allows the interval to be specified.
Client certificate cache control		In support of UC-APL, a Client Certificate Cache can be activated on the **System > Administration** page with a new option, **Enable Client Certificate Cache**.
Core Distribution Performance Enhancement		Core Distribution Performance Enhancement will improve Firewall performance, depending on network conditions and activated services.
IPv6	Network Monitoring support	Network Monitoring now supports monitoring of any remote host status in the local or remote network. SonicOS now checks the availability of the traffic between the appliance and the target host in real time, thus ensuring the target host can receive network traffic. SonicOS also displays the status of the monitored host on the **Network > Network Monitor** page.
	Extension header detection report and log support	SonicOS now validates packet extension headers and logs each invalid extension header in accordance with RFC2460. This function is configurable by two new options on the **Firewall Settings > Advanced** page.

Enhancement	Description
Extension header order check enforcement	An option on the **Firewall Settings > Advanced** page enables a check of the extension header order to ensure a packet with multiple extension headers have a valid order, in compliance with RFC2460. When this option is enabled, packets with an invalid extension order are dropped.
Hop-By-Hop Extension Header support	SonicOS provides an IPv6 hop-by-hop extension headers check. A hop limit can be configured through an option on the **Firewall Settings > Advanced** page.
Site-local address control to allow or disallow SLU	By default, IPv6 Site Local Unicast (SLU) addresses are used. As the nature of these addresses may adversely affect network security through leaks, ambiguity, and potential misrouting, an option on the **Firewall Settings > Advanced** page disables use of SLU addresses for IPv6 interfaces and router advertisement daemon (RADVD) prefixes.
Inbound type 0 routing header packet check	SonicOS provides a check of IPv6 extension routing headers of type 0 and can be configured to drop these headers through enabling an option on the **Firewall Settings > Advanced** page.
DDNS support	SonicOS supports dynamic DNS (DDNS) for IPv6 as well as IPv4.
UDP/ICMP Flood Protection support	SonicOS defends against UDP/ICMP flood attacks by monitoring IPv6 UDP/ICMP traffic flows to defined destinations. UDP/ICMP packets to a specified destination are dropped if one or more sources exceeds a configured threshold. The new option on the **Firewall Settings > Flood Protection** page enables this support.

Firewall Sandwich support

Dell SonicWALL firewalls running SonicOS 6.2.5.1 are compatible with Dell Force 10 switches in a configuration known as a firewall sandwich. A firewall sandwich deployment provides redundancy and improves availability, scalability, and manageability across the IT infrastructure.

Firewall Sandwich topology



Wire Mode VLAN translation mapping

This feature allows traffic arriving on a VLAN to a Wire Mode Interface operating in Secure mode to be mapped to a different VLAN on the outgoing paired interface. This feature, which is supported on all wire mode-capable devices, allows for easy rerouting of traffic for further analysis or processing.

The SonicOS administrator can create a VLAN mapping for a pair of interfaces that are not yet a wire mode pair, to pre-provision the VLAN mapping. This allows the admin to have the mapping in place before the traffic hits the interface. The admin can also add and delete mapping on an active wire mode interface.

The VLAN map created for a pair of interfaces is persistant over reload and is stored as part of the configuration. This feature also allows the creation of VLAN mapping for multiple pairs of interfaces at the same time. These interfaces may or may not form part of a wire mode pair at the time of the VLAN mapping creation. If the paired interface is changed and this new pair has pre-created mapping, those will go into effect immediately on the pair change.

Creating and managing VLAN mapping is done on the **Network > VLAN Translation** page. VLAN mapping can be created in two modes:

- Using a uni-directional map

  Applications of uni-directional traffic include:

  - Secure printing from a less secure network to a high secure network (reducing print costs)
  - Transferring application and operating system updates from a less secure network to a high secure network
  - Monitoring multiple networks in a SOC (security operations center)
  - Time synchronization in high secure networks
  - File transfer
  - Providing email alerts in a high secure network, from a less secure network

- Using a bi-directional map

  Bi-directional mapping is used when setting up a two way connection to and from devices through the firewall (TCP).

Numbered VPN tunnel interfaces

Routing protocols now can use a numbered tunnel interface to establish routing sessions. After a numbered tunnel interface is added to the interface list, a static route policy can use it as the interface in a static route policy configuration for a static route based VPN. Routing protocols (OSPF, RIP, and BGP) can use it for dynamic route-based VPN.

Numbered tunnel interfaces, as well as unnumbered tunnel interfaces, are supported on all platforms running SonicOS 6.2.5.1.

Change Auditor Support in AppFlow

AppFlow now includes support for Dell™ Change Auditor for SonicWALL, the automated auditing module that allows you to collect data on Internet web site and cloud activity. For more information about using Change Auditor with SonicOS appliances, see the *Change Auditor for SonicWALL User Guide*, available at https://support.software.dell.com/change-auditor-for-sonicwall/release-notes-guides.

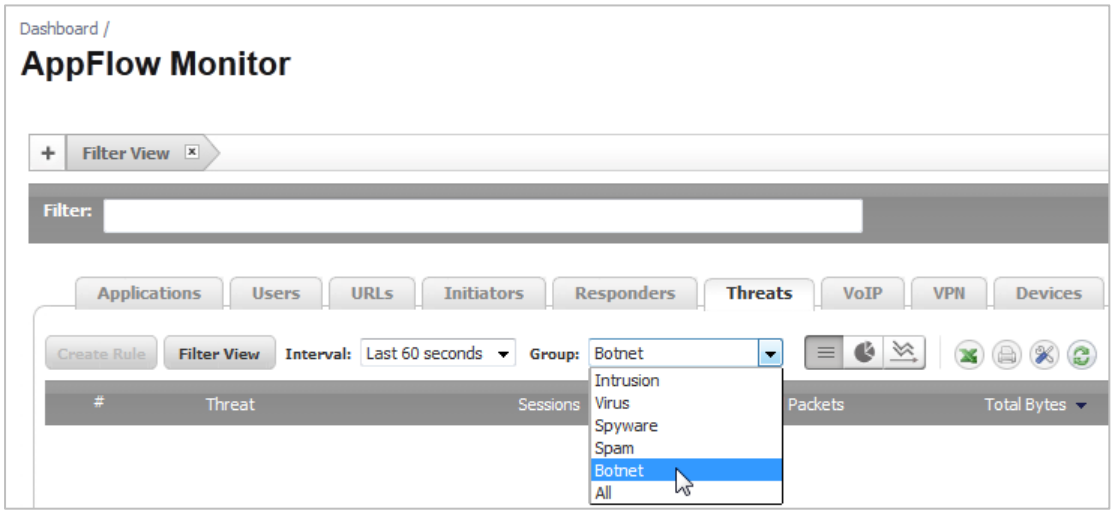
Botnet Source Identification in AppFlow Monitor

A Botnet filtering option and Botnet reporting columns is added to the **Dashboard > AppFlow Monitor** page to allow the administrator to filter for botnet traffic and view the individual user or IP address and associated detected applications.

A Botnet tab is added to the **Dashboard > AppFlow Reports** page.

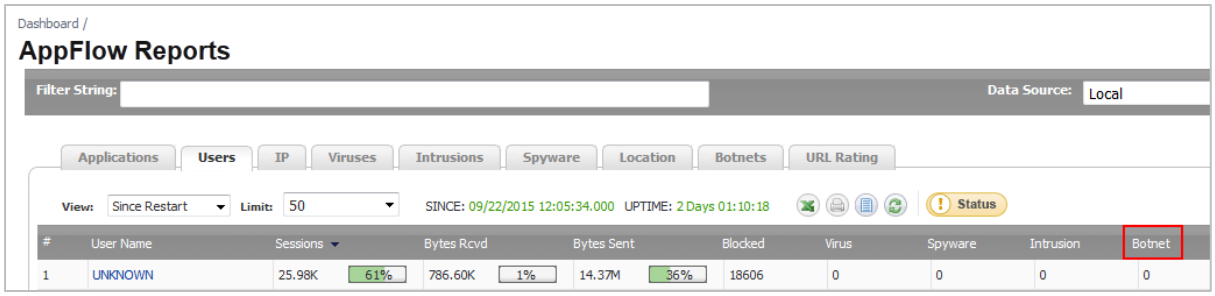
In **Dashboard > AppFlow Monitor** (and **AppFlow > AppFlow Monitor**), **Botnet** can now be selected for the **Group** option on the **Threats** tab.

Botnet option for Group



In **Dashboard > AppFlow Reports** (and **AppFlow > AppFlow Reports**), new Botnet columns are added to the **User** and **IP** tabs.

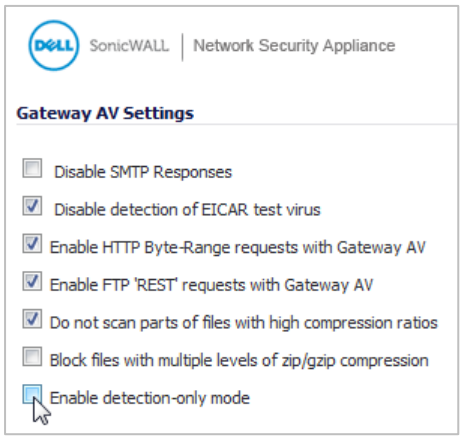
Botnet column in reports



Gateway Anti-Virus Detection Only Mode

A new **Enable detection-only mode** checkbox is available in the Gateway AV settings. Click the **Configure Gateway AV Settings** button to access this option. When selected, this option causes traffic containing viruses to be logged, but not blocked.

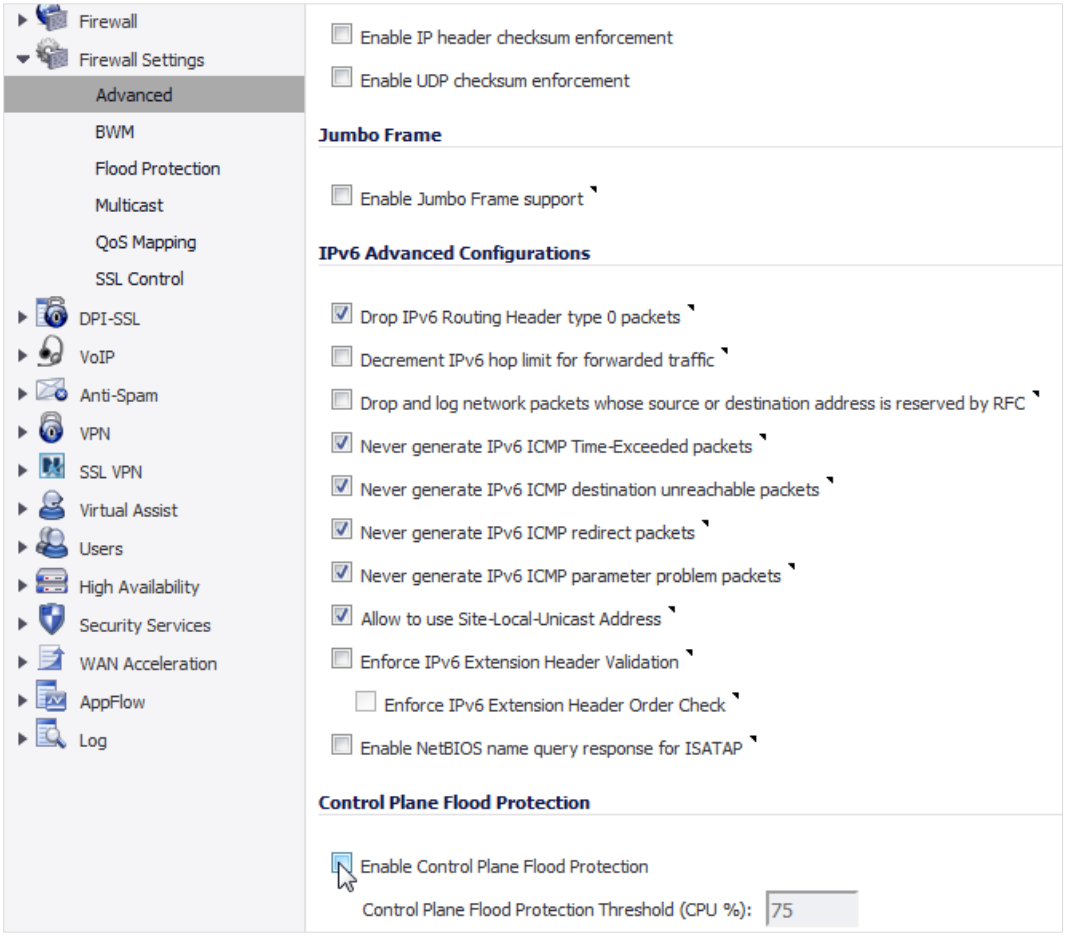
Enable detection-only mode option



Control Plane Flood Protection

The **Control Plane Flood Protection** section of the **Firewall Settings > Advanced** page provides a new **Enable Control Plane Flood Protection** checkbox together with **a Control Plane Flood Protection threshold (CPU %)** field in which you can enter a percentage of CPU capacity (default 75%).

Enable Control Plane Flood Protection option

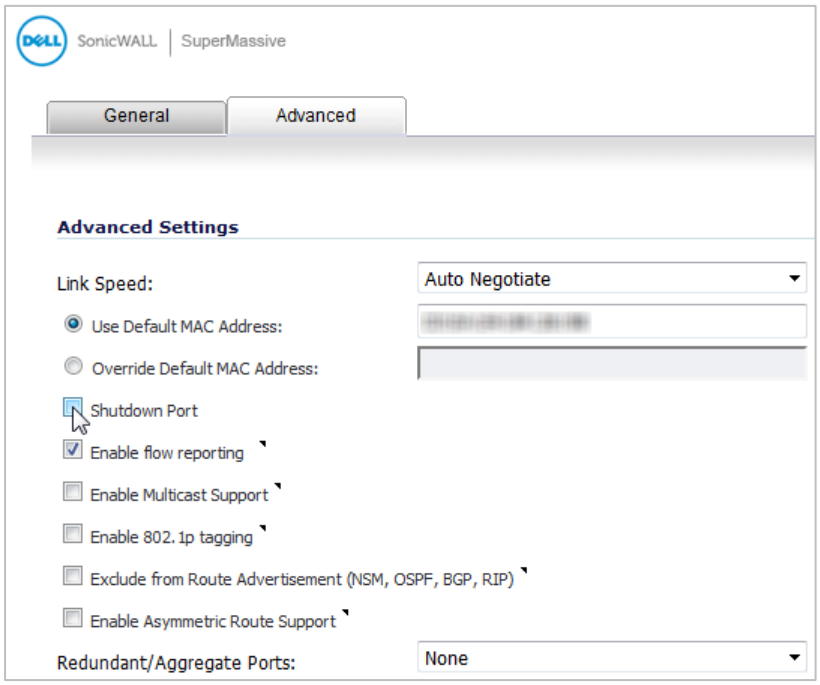


When the **Enable Control Plane Flood Protection** option is enabled, if traffic on the Control Plane (Core 0) exceeds the threshold specified in **Control Plane Flood Protection threshold (CPU %)**, the firewall forwards only control traffic destined to the firewall to the system Control Plane core. To give precedence to legitimate control traffic, excess data traffic is dropped. This restriction prevents too much data traffic from reaching the Control Plane core, which can cause slow system response and potential network connection drops. The percentage configured for control traffic is guaranteed.

Shutdown Port Option

On SuperMassive 9000 and NSA series appliances, a new **Shutdown Port** option is available in the **Advanced** tab when editing an interface on the **Network > Interfaces** page. You can select the **Shutdown Port** checkbox to temporarily take the interface offline for maintenance or other reasons. A confirmation displays; click **OK**. If connected, the link will go down. Clear the checkbox to activate the interface and allow the link to come back up.

Shutdown Port option



You cannot shut down the management interface or the interface you are currently using.

You can also shut down an interface by clicking the green checkmark icon in the **Enabled** column for the interface in the **Interface Settings** table. A confirmation message displays, such as "`Do you wish to administratively shut down port X4?`" If you click **OK**, the checkmark icon turns to a red 'x' icon (**Disabled** icon). To enable the interface, click the **Disabled** icon, and then click **OK** when the confirmation message displays.

Port based network monitoring

New checkboxes are available on the **Advanced** tab while editing a NAT policy:

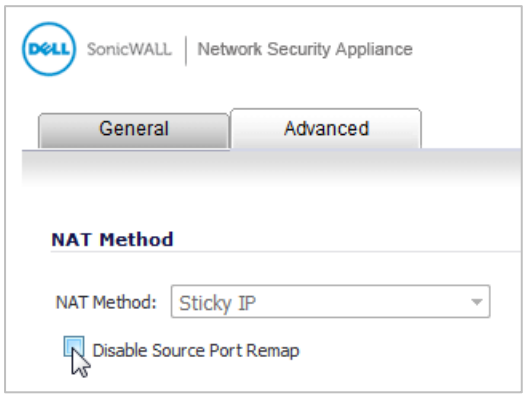
- Enable Port Probing
- RST Response Counts As Miss

This feature enhances network monitoring to provide port information in addition to IP addresses. NAT uses this information to mark eligibility for an IP address and port combination for translation. This feature also enhances NAT to consider the port while load balancing. This is disabled by default and is configurable.

Disable Source Port Remapping option for NAT

When editing a NAT policy from the **Network > NAT Policies** page, a new **Disable Source Port Remap** checkbox on the **Advanced** tab of the **Add/Edit** dialog provides a way to disable source port remapping on the policy.

Disable Source Port Remap option

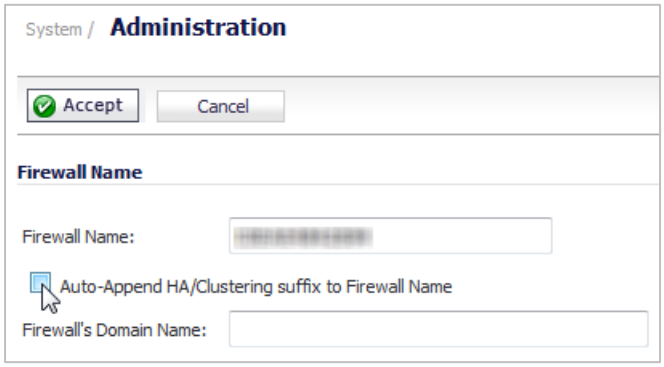


When this option is selected, SonicOS preserves the source port of the connection while executing other NAT mapping. This option is available when adding or editing a NAT policy if the source IP address is being translated. The checkbox cannot be selected if the **Translated Source** is set to **Original**.

Suffix Option for HA/Clustered Firewalls

A new **Auto-Append HA/Clustering suffix to Firewall Name** checkbox is provided on the **System > Administration** page under **Firewall Name**.

Auto-Append HA/Clustering suffix to Firewall Name option



When enabled, this option automatically appends an appropriate suffix to the firewall name in the **Dashboard > Log Monitor**:

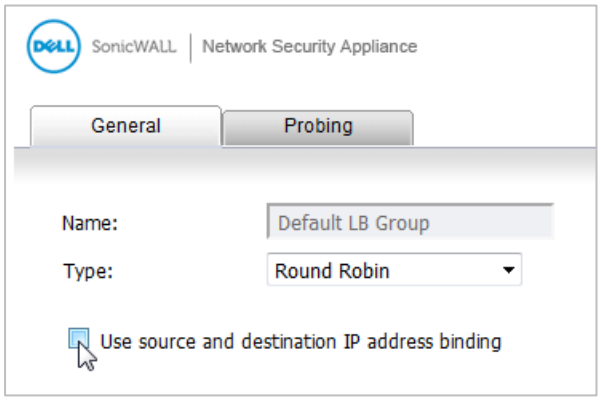
- - Primary
- - Secondary
- - Primary Node <*n*>
- - Secondary Node <*n*>

This option facilitates recognition of the primary/secondary firewalls in the log.

Source/Destination IP address binding for Round Robin/Spillover load balancing

When configuring a load balancing group from the **Network > Failover & LB** page, the **Use source and destination IP address binding** checkbox is now available for the Round **Robin** and **Spillover** load balancing types. In previous releases, this was only available when **Type** was set to **Ratio**.

Use source and destination IP address binding option



The option is especially useful when using HTTP/HTTPS redirection or in a similar situation. For example, Connection A and Connection B need to be on the same WAN interface, the source and destination IP addresses in Connection A are the same as those for Connection B, but a different service is being used. In this case, source and destination IP address binding is required to keep both the connections on the same WAN interface so that the transactions do not fail.

SonicPoint ACe/ACi/N2 FCC new rule certification for DFS channels

Beginning in SonicOS 6.2.5.1, FCC U-NII (Unlicensed –National Information Infrastructure) New Rule (Report and Order ET Docket No. 13-49) for DFS channels is supported on SonicPoint ACe/ACi/N2 running firmware version 9.0.1.0-2. FCC U-NII New Rule compliance helps to ensure that your Dell SonicWALL wireless appliance does not interfere with other types of users in U-NII bands.

SonicPoint ACe/ACi/N2 wireless access points manufactured with FCC New Rule compliant firmware are only supported with SonicOS 6.2.5.1 and higher. Older SonicPoint ACe/ACi/N2 access points are automatically updated to the FCC New Rule compliant firmware when connected to a firewall running SonicOS 6.2.5.1 or higher.

Feature support on TZ Series and SOHO Wireless appliances

Dell SonicWALL SOHO Wireless and TZ series appliances running SonicOS 6.2.5.1 support most of the features available for other platforms in earlier 6.2 releases, but not all.

The following features are not supported on the TZ series or SOHO Wireless appliances:

- Active/Active Clustering
- Advanced Switching
- Jumbo Frames
- Link Aggregation
- Port Redundancy
- Wire Mode

In addition, SOHO Wireless appliances do not support the following features:

- App Visualization (Real-Time Monitor and AppFlow)
- Geo-IP Filtering
- Botnet Filtering
- High Availability

Resolved issues

This section contains a list of issues that are fixed in this release.

3G/4G

Resolved issue	Issue ID
Some 3G/4G USB cards are not detected by SonicOS. Occurs when an ATT340U or Sprint 341U card is inserted into the U0 interface on the TZ and the firewall is rebooted one or more times.	159366

Application Control

Resolved issue	Issue ID
Using App Control to block Skype can also block access to `google.com`. Occurs when App Control Advanced is configured to block Skype in the IM category.	159478

GMS

Resolved issue	Issue ID
Incorrect SYSLOG close-connection message. Occurs when SENT/RCVD reports are larger than 4GB.	166750
Firewalls running SonicOS 6.2 cannot be managed via Dell SonicWALL GMS unless NAT is configured to translate the X0 IP address to the X1 IP address. Occurs when GMS is configured to manage the remote firewalls via a Management Tunnel and tries to manage the unit via the public address.	166455

High Availability

Resolved issue	Issue ID
The status of X-Series switches is not shown correctly on the standby firewall. Occurs when a series of failovers and failbacks happen with extended switches configured on the HA pair.	171030
Unable to log in to a secondary unit with changed administrator credentials. Occurs when the administrator username and password are changed on the primary unit; the change is not made on the secondary unit.	161560
With site-to-site VPN between a SonicWALL appliance and a Juniper NetScreen, ESP packets are dropped for inbound security associations with the message, `Octeon Decryption Failed Selector`. Occurs when the traffic is initiated from the computers behind the Juniper NetScreen; the initial ESP packets are dropped.	159438

Log

Resolved issue	Issue ID
Exported log messages show as random numbers in the CFS category. Occurs when a web site is added to a CFS block list and then that web site is accessed.	168542

Networking

Resolved issue	Issue ID
In a High Availability (HA) pair, deleting an extended switch on the Primary firewall is not synced to the Secondary firewall. Occurs when an X-series switch is deleted from the Primary firewall of an HA pair; the Secondary unit still shows the X-series switch as present.	170512
NAT priority is lost after disabling policies. Occurs when the priority of an already configured NAT policy is changed, and then the NAT policy is disabled.	165930
Some FQDN objects do not resolve. Occurs when a large number of both regular and wildcard FQDN objects are configured.	162862

SSL VPN

Resolved issue	Issue ID
An SSL VPN connection fails. Occurs when a Mobile Connect client using Apple AirPort tries to establish an SSL VPN connection to a firewall.	167361
Domain names are not recognized. Occurs when domain names with a period (.) and hyphen (-) combination are added under SSL VPN client settings.	160479
The message, `The page cannot be displayed`, is displayed instead of the CFS Block page for blocked HTTP websites. Occurs when a CFS App rule policy is configured and applied to an SSL VPN zone. The CFS policy is triggered when a user tries to access a web site in the blocked category, but displays the message instead of the CFS block page.	159438

Users

Resolved issue	Issue ID
SSO Bypass settings for Address Object/Group and/or Service Object/Group are lost. Occurs when the firmware is upgraded from 6.2.2.2 to 6.2.5.1.	169646
Some SSO Authentication/RADIUS accounting inactive users time out prematurely. Occurs when the inactivity time out is set to 24 hours.	168579
Guest Administrators cannot log in. Occurs when a Guest Administrator tries to log in from a zone that has Guest Services enabled even though regular guest users can log in from that zone.	166925
Guest users connecting to a SonicPoint SSID are redirected back to the page for accepting the user policy within a few minutes after they already clicked **Accept**. Sometimes a "`File not found`" error is displayed instead of the policy page. Occurs when **Enable Policy Page Without Authentication** is enabled and the user clicks **Accept** in the policy page, and then proceeds normally or is idle for a few minutes. The error is displayed when several guest clients connect at the same time.	164524
The firewall stops authenticating users over Single Sign On (SSO), and some users see the error message, `User Login Denied - LDAP communication or configuration error`. Multiple RADIUS Accounting Start/Stop message pairs are logged. Occurs when LDAP and RADIUS Accounting are configured for user authentication with SSO, and other non-SSO users/groups are authenticated via web login. The SSO Agent version is 4.0.18. The RADIUS Accounting Start/Stop message pairs occur when wireless users move between different access points.	163550
The Test LDAP User function returns "`LDAP communication error`". Occurs when Local User is configured for the User authentication method and an LDAP server is correctly configured.	162500

VPN

Resolved issue	Issue ID
VPN tunnel interface is not deleted. Occurs when a policy-based route (PBR) is added to a tunnel interface, changed to another interface, and then deleted before deleting the VPN tunnel interface.	170044
Policy Based Routing does not work. Occurs when an unnumbered tunnel interface (TI) is changed to a numbered TI that uses the same VPN policy as the unnumbered TI. The outgoing interface in the policy is changed to the numbered TI automatically, but the VPN traffic that matches the policy fails.	169786

Wireless

Resolved issue	Issue ID
Wireless VAP does not work on a 2.4GHz auto channel. Occurs when 2.4GHz with auto channel is selected and an internal VAP group is used to assign two VAPs to the group.	166580

Known issues

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

IMPORTANT: VPN Tunnel Interface

Known issue	Issue ID
Any unnumbered tunnel interface with dynamic routing is not retained during an upgrade. Occurs when SonicOS 6.x is upgraded to SonicOS 6.2.5.1.	169993

3G/4G

Known issue	Issue ID
A Sprint 341U card takes more than 10 minutes to connect. Occurs when the Sprint 341U is connected to U0, which is configured as the Final Backup with a 4G profile, and then failover from the Primary WAN (X1) is triggered by unplugging the cable from X1.	166381
A Huawei E182E 3G card is not properly detected by SonicOS and cannot connect. The console shows that the card is detected, but the SonicOS web management interface shows “No device”. The U0 interface is not shown as final backup, but appears in an alternate group. Occurs when the Huawei E182E 3G device is functioning properly at first, U0 is configured as final backup for the WAN in persistent mode, and the X1 interface is disconnected just before the appliance is restarted while the device remains inserted.	164232
It takes U0 between 4-6 minutes to reconnect after the data limit is reset. Occurs with AT&T Beam, Verizon 290, Sprint 760, and AirCard 340U when U0 is the final WAN backup in Persistent mode with 100K data limit, and after failover to U0 the data limit is reached and then the administrator resets the data limit on the **3G/4G > Data Usage** page.	160190
Huawei 3G cards do not connect to the Internet after the X1 WAN interface is disconnected. Occurs when one of several Huawei 3G cards is inserted in the TZ appliance and the U0 interface is configured as the **Final Backup** in the **Network > Failover & LB** page.	159273

Application Control

Known issue	Issue ID
App Control Advanced does not block the Psiphon client version 95 or 87. Occurs when the Proxy-access category is enabled in App Control Advanced along with signatures 5, 6, and 7, with or without DPI-SSL enabled, and with or without a rule to block UDP ports 500 and 4500.	162055
The Ultrasurf browser plugin is not blocked by an App Rule or App Control Advanced. Occurs when using the Chrome browser plugin for Ultrasurf.	161651
App Control does not block access to Google Play app store from a smartphone app, but play.google.com is blocked from a browser on a personal computer. Occurs when DPI-SSL is not enabled and an App Rule is configured on the firewall to block the Google Play application and signatures, then an Android smartphone connects to the firewall via a wireless access point and can download or update apps from the Google Play store.	157692

DPI-SSL

Known issue	Issue ID
NetExtender (SSL VPN Client) connection is disconnected. Occurs when HTTPS connections are initiated or files downloaded via SCP to a host on the other side of the SSL VPN connection.	169379
Client DPI-SSL does not inspect traffic on the WWAN interface. No messages, such as `connection is untrusted`, are displayed when connecting to a secure website using HTTPS. Occurs when the firewall is using a 3G or 4G card for the WAN connection and Client DPI-SSL is enabled, but the default Dell SonicWALL DPI-SSL CA certificate is not installed on the browser.	163672
Applications such as YouTube are slow to load or do not load properly. Occurs when the DPI-SSL service is enabled and policies are configured with Advanced Bandwidth Management; the policies might not work as configured.	158183

High Availability

Known issue	Issue ID
HA Primary and Secondary firewalls are unavailable to service for a brief period during a manual configuration change and a restart of the Primary Firewall in Active state. Occurs when a configuration change is made on the Primary firewall in the Active state, and then the restart link on the SonicOS management interface status bar is clicked.	171787
Synchronizing settings causes the **Network > Portshield Groups** page on the standby unit to be refreshed continuously. Occurs when there are X1052 and X1008 X-Series switches on a TZ series appliance. Without deleting either switch from the configuration, the X1008 switch is physically removed. The primary unit shows the correct status of both switches. On the **High Availability > Advanced** page, the **Synchronize Settings** button is clicked. The secondary unit reboots after synchronization, but **the Network > PortShield Groups** page refreshes continuously.	170876
A client using SSL VPN NetExtender fails to connect to the active unit of an HA Pair after a failover and failback. Occurs when the client is connected using SSL VPN NetExtender, then the Force Active/Standby Failover option is used to force a failover and the client is disconnected, but is able to reconnect, and then the same option is used to force a failback to the primary firewall. The client is disconnected and gets a “connection failed” error when attempting to reconnect.	167227

Log

Known issue	Issue ID
Cannot modify a syslog server port. Occurs when trying to modify the syslog port from a GMS server.	160355
The source and destination of the App Rules log messages are reversed. The source is the real destination, and the destination is the real source. Occurs when viewing the App Rules log messages.	149458

Networking

Known issue	Issue ID
An extended switch access VLAN configuration is not properly assigned. Occurs when a subinterface with a VLAN is created on a TZ appliance with an extended switch and either a common uplink or a switch uplink with a dedicated link. The extended switch is portshielded to the port with the VLAN configuration. When checking the extended switch, the VLAN configuration is assigned to some other VLAN supported in the dedicated uplink.	170434
The X-Series switch on a TZ series appliance is inaccessible and status is down after configuration of a dedicated link with just a MGMT uplink. Occurs when the X-Series switch is set up for **Dynamic IP**, thus receiving a new IP address when the DHCP server is enabled. **Workaround**: During the initial set up of the X-Series switch, be sure to choose **Static IP** instead of **Dynamic IP**.	170141
Portshielding X-Series switches on a TZ series appliance takes too long. Occurs when portshielding multiple ports in any combination to a PortShield group on any X-Series switch on a TZ series appliance. It takes 15 seconds to portshield each port. For example, to portshield 24 ports, it takes 15 seconds * 24 = 240 seconds = 6 minutes.	170026
Displaying the **Groups** tab on the **Network > PortShield** page is excessively slow. Occurs when two X-Series switches are provisioned on a TZ series appliance and then one switch is removed from the user interface of the appliance. The setting is exported and saved from the **System > Settings** page. When importing the saved settings, the display of the **Groups** tab is excessively slow.	169847
ICMPv6 service group shows inconsistent member objects. Occurs when editing the factory default ICMPv6 group (**Network > Services > Service Groups > Edit ICMPv6**). In the factory default state, about 30 service objects are shown as members of the ICMPv6 group. Any attempt to edit/add to this group results in errors (unable to find network object), deleted members, and an inability to add any subtype ICMPv6/ND members (ports 141 through 154).	168831
The firewall cannot form full adjacency with all neighboring routers using OSPF. Occurs when OSPF is enabled on one interface of the firewall with router priority 200, which is connected to a test system running OSPF with 20 simulated neighboring routers, all with priority 0. Only about half of the neighbors are able to reach FULL status.	166564
An IPv6 BGP neighbor cannot be established. Occurs when both IPv6 and IPv4 BGP are configured on the network at the same time, and the IPv4 BGP is configured with authentication, but the IPv6 BGP is not configured for authentication.	157525
The firewall cannot enable OSPF through the console. Occurs when trying to enable the OSPF through the firewall console. The network needs to first match the OSPF wildcard bits.	153350
The firewall cannot enable RIPv2 through the console. Occurs when trying to enable RIPv2 through the firewall console and the subnet is not set, or the subnet is 32-bit as with 10.8.109.0 where the IP address last byte is 0.	153267
The firewall learns OSPF routes from areas other than area0. Occurs when the network topology includes 3 firewalls with 3 areas, all with VLANs configured, and the OSPF routes are checked on the area1 firewall.	153096
There is no option to originate a default route for dynamic IPv6 routing via OSPFv3. Occurs when configuring OSPFv3 from the **Network > Routing** page. IPv6 default route origination via OSPFv3 is currently not supported.	150771

SSL VPN

Known issue	Issue ID
Configuring a VLAN ID causes the page to display "`Bad Request: The client issued a bad request.`" Occurs when **Enter** is pressed on the keyboard to configure a VLAN ID.	170036
Importing a certificate CRL file fails. Occurs when importing a certificate CRL file larger than 100KB.	169256

Switching

Known issue	Issue ID
The aggregated member interface of a Layer 2 Link Aggregation Group (LAG) fails to aggregate into the LAG after restarting the firewall. Occurs when the LAG aggregator interface and aggregated member interface are configured as trunk ports, each with a VLAN enabled, in the WAN zone using DHCP mode, and then the firewall is restarted.	167254

System

Known issue	Issue ID
The system time shows the wrong hour. Occurs when the year and hour are set manually and multiple times on the **System > Time** page.	168444
The 10 gigabit links on ports X16, X17, X18 and X19 can go down after a failover. The ports are fine again after administratively bringing them down and then up. Occurs when two SuperMassive 9000 series are connected as a High Availability pair with ports X16, X17, X18 and X19 configured in Wiremode and then a failover is forced during testing.	166758
Diagnostic reports cannot be sent from the firewall, and attempting to do so results in an incorrect log message, "`Failed to send file to remote backup server, Error: 1, File:TSR`". Occurs when using **Send Diagnostic to Support** from the **System > Settings** page.	163181
After importing the configuration settings file from an appliance running 5.9.0.x or 5.9.1.0 to a TZ600 running 6.2.5.1, the interface to which the site-to-site VPN policy is bound changes from X1 to X0. Occurs when the configuration settings file on the VPN-bound interface is incompatible with 6.2.x.	143210

User Interface

Known issue	Issue ID
Firmware upgrade fails when uploaded through the SonicOS management user interface (UI). Occurs when a firmware upgrade for an X-Series 4012 extended switch is attempted through the SonicOS management interface. **Workaround:** Upgrade the switch firmware directly from the extended switch.	171763
Options for PoE are displayed for non-PoE X-Series extended switches. Occurs when configuring a non-PoE extended switch. Options for PoE display on the **Advanced** tab of the **Add External Switch** dialog.	171573
Dynamic pages, such as **Dashboard > Log Monitor**, **Network > Address Objects**, or **Network > NAT Policies**, cannot be loaded with Microsoft Edge browser. Occurs when the Microsoft Edge browser is used. If the browser window is maximized, the page is blurred; if the browser window is not maximized, the page disappears.	169277

Known issue	Issue ID
The **Dashboard > Real-Time Monitor** does not appear to work properly on TZ series appliances with X-Series switches. Occurs when X-Series switches are provisioned on a TZ series appliance. For example, a link between the TZ appliance and the X-Series switch configured as 10Mbps is shown on the **Dashboard > Real-Time Monitor** as 100+MBps even though the link is working properly. As all the X-Series switch ports are portshielded, the data shown for these ports on the **Dashboard > Real-Time Monitor** is not applicable.	169000

VPN

Known issue	Issue ID
Unable to add a manual key. Occurs when attempting to add an IPv6 manual key on the **VPN > Settings > VPN Policy** dialog.	170547
VPN traffic does not go into a VPN tunnel. Occurs when an unnumbered tunnel interface policy with a static route is changed to an S2S VPN policy with **Apply NAT policy** option is enabled and then changed back to a tunnel interface policy with a static route.	170466
VPN tunnel interface cannot be deleted. Occurs when a VPN policy of type tunnel interface is configured and then a VPN tunnel interface with that name is configured. After upgrading to 6.2.5.1-20n, the VPN tunnel interface cannot be deleted as the name has been lost during the upgrade.	169627

Wireless

Known issue	Issue ID
Authentication for a SonicPoint ACe/ACi/N2 cannot be changed directly. Occurs when changing the authentication type from WPA2 - EAP to WEP – Shared Key by configuring the profile for a SonicPoint ACe/ACi/N2. **Workaround**: Change the authentication type from **WPA2-EAP** to **WEP-Both (OPEN System and Shared Key)**. And then, change the authentication type to **WEP-Shared Key**.	171722

System compatibility

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

Wireless 3G/4G broadband devices

SonicOS 6.2.5.1 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

Dell SonicWALL Global Management System (GMS) management of Dell SonicWALL security appliances running SonicOS 6.2.5.1 requires GMS 8.1 service pack 1, which will be released in April.

WXA support

The Dell SonicWALL WXA series appliances (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are supported for use with Dell SonicWALL security appliances running SonicOS 6.2.5.1. The recommended firmware version for the WXA series appliances is WXA 1.3.2.

Browser support

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

- Chrome 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 16.0 and higher
- Internet Explorer 9.0 and higher
- 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 Dell SonicWALL appliance system administration.

Product licensing

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

A number of security services are separately licensed features in SonicOS. When a service is licensed, full access to the functionality is available. SonicOS periodically checks the license status with the SonicWALL License Manager. The **System > Status** page displays the license status for each security service.

Upgrading information

For information about obtaining the latest firmware, upgrading the firmware image on your Dell SonicWALL appliance, and importing configuration settings from another appliance, see the *SonicOS 6.2 Upgrade Guide* available on MySonicWALL at https://mysonicwall.com/ or on the Support portal at https://support.software.dell.com/.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the portal provides direct access to product support engineers through an online Service Request system. To access the Support Portal, go to http://software.dell.com/support/.

The site enables you to:

- View Knowledge Base articles at:

  https://support.software.dell.com/kb-product-select
- View instructional videos at:

  https://support.software.dell.com/videos-product-select
- Engage in community discussions
- Chat with a support engineer
- Create, update, and manage Service Requests (cases)
- Obtain product notifications

SonicOS Administration Guides and related documents are available on the Dell Software Support site at https://support.software.dell.com/release-notes-product-select.

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit http://www.software.dell.com.

Contacting Dell

For sales or other inquiries, visit http://software.dell.com/company/contact-us.aspx or call 1-949-754-8000.

Legend

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

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

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

Last updated: 3/28/2016

232-003182-00 Rev A