Dell™ SonicWALL™ SonicOS 6.2.6.0

Release Notes

August 2016

These release notes provide information about the Dell™ SonicWALL™ SonicOS 6.2.6.0 release.

Topics:

About SonicOS 6.2.6.0

SonicOS 6.2.6.0 includes two important new features:

- Capture Advanced Threat Protection
- Content Filtering Service 4.0

See the New features section for more information.

This release provides all the features and contains all the resolved issues that were included in previous releases of SonicOS 6.2. For more information, see the previous release notes, available on MySonicWALL or on the Support Portal at: https://support.software.dell.com/release-notes-product-select.

TZ Series / SOHO Wireless feature support

Dell SonicWALL SOHO Wireless and TZ series appliances running SonicOS 6.2.6.0 support most of the features available for other platforms. Only the following features are *not* supported on the TZ series or SOHO Wireless appliances:

- Active/Active Clustering
- Advanced Switching
- Capture ATP (supported on TZ500/500W and TZ600)
- Jumbo Frames
- Link Aggregation

- Port Redundancy
- Wire Mode

Supported platforms

SonicOS 6.2.6.0 is supported on the following Dell SonicWALL network security appliances:

- SuperMassive 9400
- SuperMassive 9200

- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600

- TZ600
- TZ500 and TZ500 Wireless
- TZ400 and TZ400 Wireless
- TZ300 and TZ300 Wireless
- SOHO Wireless

New features

This section provides information about the new features in SonicOS 6.2.6.

Topics:

- About Capture ATP
- About CFS 4.0

About Capture ATP

Capture Advanced Threat Protection (ATP) is an add-on security service to the firewall, similar to Gateway Anti-Virus (GAV). Capture ATP helps a firewall identify whether a file contains a zero-day virus by transmitting a suspicious file to the Cloud where the Capture ATP service analyzes the file to determine if it contains a virus. Capture ATP then sends the results to the firewall. This is done in real time while the file is being processed by the firewall.

The **Capture ATP > Status** page displays a graph chart that shows the percentages of benign and malicious files discovered, as well as the total number of files analyzed. It also displays a log table that shows the results of individual files submitted for analysis.

Capture ATP must be configured on each firewall individually. Once the Capture ATP service license is activated, you can enable Capture ATP on the **Capture ATP > Settings** page.

Capture ATP can also analyze files that you upload for analysis from the **Capture ATP > Status** page. After the files are analyzed they are listed in the table on the **Status** page. You can click on any file in the log table on the **Status** page and see the results from the detailed analysis of that file.

Note that Capture ATP is only supported on the following appliances. The smaller TZ appliances and the SOHO wireless appliance do not support Capture ATP.

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200

- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600

- TZ600
- TZ500 and TZ500 Wireless

For more information about using Capture ATP, refer to the *SonicOS 6.2.6 Capture ATP Feature Guide*.

About CFS 4.0

Content Filtering Service (CFS) 4.0 has been redesigned to improve performance and ease of use. The workflow was redesigned and more accurate filtering options have been provided. Refer to *SonicOS 6.2.6 Content Filtering Service (CFS) 4.0 Feature Guide* for more details. For information about upgrading from an older version of CFS, see the *SonicOS 6.2.6 CFS 4.0 Upgrade Guide*.

Topics:

- CFS workflow
- CFS settings
- New CFS policy design
- CFS custom categories
- New objects in CFS 4.0
- CFS log entries
- Websense support in CFS 4.0
- Deprecated CFS 3.0 features
- Comparison of CFS 3.0 to CFS 4.0

CFS workflow

When processing packets, CFS follows this workflow:

1 A packet arrives and is examined by CFS.

2 CFS checks it against the configured exclusion addresses, and allows it through if a match if found.

3 CFS checks its policies and finds the first policy which matches the following conditions in the packet:

- Source Zone
- Destination Zone
- Address Object
- Users/Group
- Schedule
- Enabled state

4 CFS uses the CFS Profile defined in the matching policy to do the filtering, and returns the corresponding operation for this packet.

5 CFS performs the action defined in the CFS Action Object of the matching policy.

6 If no CFS Policy is matched, the packet is passed through without any action by CFS.

CFS settings

The following global settings are used in CFS 4.0:

- Global settings

    - **Max URI Caches (entries)** — Defines the maximum number of cached URI entries. Cached URI entries save the URI rating results, so that SonicOS does not need to ask the backend server for the rating of a known URI. In CFS 3.0, the cache size had a maximum; in CFS 4.0 the maximum is changed to the entry count.

    - **Enable Content Filtering Service** — This option can be cleared to bypass CFS for all packets. By default, it is selected.

    - **Enable HTTPS content filtering** — When enabled, CFS first attempts to get the ServerName from the client "hello". If that fails, CFS attempts to get the CommonName from the SSL certificate and then get the rating. If both attempts fail to get the ServerName/CommonName, CFS uses the IP address for the rating.

    - **Blocked if CFS Server is Unavailable** — If the CFS server cannot provide the rating request within the specified duration (5 seconds by default), this option defines whether to allow or deny the request.

- **CFS Exclusions**

    - **Exclude Administrator** — When enabled, content filtering is bypassed for all requests from an account with administrator privileges.

    - **Excluded address** — Content filtering is bypassed for all requests from address objects selected in the **Excluded address** list.

- **Custom Category**

    - **Enable CFS Custom Category** — Allows the administrator to customize the ratings for specific URIs. When CFS checks the ratings for a URI, it first checks the user ratings and then checks the CFS backend server for the ratings.

- **Advanced Settings**

    - **Enable Smart Filtering for Embedded URL** — When enabled, detects the embedded URL inside Google Translate (Https://translate.google.com) and filters the embedded URL too. Requires that client DPI-SSL be enabled also.

    - **Enable Safe Search Enforcement** — Enforces Safe Search when searching on any of the following web sites:

        - www.yahoo.com

        - www.ask.com

        - www.dogpile.com

        - www.lycos.com

      Requires that client DPI-SSL be enabled also.

    - **Enable Google Force Safe Search** — When enabled. overrides the Safe Search option for Google inside each CFS Policy and its corresponding CFS Action. Note that typically Safe Search happens automatically and is powered by Good, but when this option is enabled, SonicOS rewrites the Google domain in the DNS response to the Google Safe Search virtual IP address.

    - **Enable YouTube Restrict Mode** — When enabled, accesses YouTube in Safety mode. YouTube provides a new feature to screen videos that may contain inappropriate content flagged by users and other signals.

    - **Enable Bing Force Safe Search** — When enabled overrides the Safe Search option for Bing inside each CFS Policy and its corresponding CFS Action.

New CFS policy design

A CFS policy defines the filtering conditions that a packet is compared to, and CFS 4.0 provides a new policy design, different from the way policies were implemented in CFS 3.0. A default policy is provided, but you can define your own. When writing your own policies, following matching conditions can be defined:

- Name
- Source Zone
- Destination Zone
- Source Address
- Users/Group
- Schedule
- Profile
- Action

If a packet matches the conditions defined for Source Zone, Destination Zone, Address Object, Users/Groups, Schedule, and Enabled state, it is filtered according to the corresponding CFS Profile and then the CFS Action is applied. If authentication data is not available during matching for Users/Groups, no match is made for this condition. This strategy prevents performance issues, especially when Single Sign-On is in use.

Each CFS policy has a priority level and policies with higher priorities are checked first.

CFS custom categories

In CFS 4.0, CFS custom categories are handled consistently with the way ratings are handled in the CFS backend server. When adding or editing a custom category, you can select up to four categories for the URI.

Besides adding custom category entries one by one, export and import functions are also supported. One way to use this functionality is by exporting the custom category first, editing it, and then importing from that exported file.

Only the first 10,000 custom category entries in the file are imported. Invalid entries are skipped and do not count toward the maximum of 10,000 custom category entries that are supported.

New objects in CFS 4.0

Three new kinds of objects are supported in CFS 4.0:

- **URI List Objects** — Defines the URI list which can be marked as allowed or forbidden.
- **CFS Action Objects** — Defines what happens after a packet is filtered by CFS.
- **CFS Profile Objects** — Defines what kind of operation is triggered for each HTTP/HTTPS connection.

These objects are configured on the **Firewall** > **Content Filter Objects** page in the SonicOS management interface.

URI List Objects

In CFS 4.0, a *URI List Object* is used for URI/domain matching. Each URI List Object contains a custom list of URIs. You can add/edit/delete a CFS URI list object on the **Firewall** > **Content Filter Objects** page in SonicOS.

Use the following guidelines when configuring URI List Objects:

- A maximum of 128 URI list objects are allowed.
- In each object, up to 5,000 URIs are supported.
- A URI is a string containing host and path. Port and other content are currently not supported.

- An IPv4 or IPv6 address string is supported as the host portion of a URI.

- The maximum length of each URI is 255 characters.

- The maximum combined length of all URIs in one URI list object is 131,072 (1024*128) including one character for each new line (carriage return) between the URIs.

- Each URI can contain up to 16 tokens. A token in URI is a string composed of the characters:

  ```
  0-9
  a-z
  A-Z
  $ - _ + ! ' ( ) ,
  ```

- The maximum length of each token is 64 characters including one character for each separator (. or /) surrounding the token.

- An asterisk (*) can be used as a wildcard representing a sequence of one or more valid tokens.

When building a policy URI List Objects can be used as either the forbidden URI list or the allowed URI list. URI List Objects can also be used by the Web Excluded Domains of Websense.

Action Objects

The CFS Action Object defines what happens after a packet is filtered by CFS and specified by a CFS Policy. You can add/edit/delete a CFS Action Object on the **Firewall** > **Content Filter Objects** page in SonicOS. Within the Action Object you can define whether to block a web site, require a passphrase (password) for access, require a confirmation before proceeding to the web site, or use Bandwidth Management.

Passphrase and Confirm features only work for HTTP requests. HTTPS requests cannot be redirected to the Passphrase or Confirm page, respectively.

Profile Objects

The CFS Profile Object defines the action that is triggered for each HTTP/HTTPS connection. You can add/edit/delete a CFS Profile Object on the **Firewall** > **Content Filter Objects** page in SonicOS. When setting up a new Profile Object under the new design, a domain may now be resolved to one of four ratings. From highest to lowest, the ratings are:

- Block

- Passphrase

- Confirm

- BWM (Bandwidth Management)

If the URI is not categorized into any of these ratings, then the operation is allowed.

CFS log entries

In CFS 4.0, there are only three types of log entries:

- logstrSyslogWebSiteAccessed

- logstrWebSiteBlocked

- logstrCFSAlert — These log entries start with **CFS Alert:** and are followed by a descriptive message.

Websense support in CFS 4.0

The Websense configuration settings are shown in the Security Services > Content Filter page when the **Content Filter Type** selection is set to *Websense Enterprise*. Websense only works for IPv4 requests. It does not work with IPv6.

Websense can be used even when the firewall is not licensed for CFS 4.0 (Content Filtering Premium).

Deprecated CFS 3.0 features

CFS 4.0 includes the following changes to CFS 3.0 features:

- Merge "CFS via App Rules" and "CFS via Zones" into one.
- Remove the Global/Local custom lists, replaced by URI List objects.
- Users cannot use CFS without a license, but can still use Websense.
- Remove CFS configuration from Users/Groups CFS tab.
- Remove CFS configuration from Zone page if using SonicWALL CFS. The CFS configuration in Zone is available only if CFS type is Websense.
- Remove Restrict Web Features for Java/ActiveX. They can be replaced with entries in the Forbidden URI list using `*.java` and `*.ocx`.
- Remove Restrict Web Features for HTTP Proxy Server.
- In CFS 4.0, to block access to HTTP Proxy Server, go to the **Firewall** > **App Control Advanced** page, enable **App Control**, and then edit the 3648 signature ID to block HTTP proxy access.

Comparison of CFS 3.0 to CFS 4.0

The following table compares the user experience for various aspects of the old and new CFS.

CFS 3.0	CFS 4.0
Configure CFS on CFS page, Zone page, User page and App Rules page.	Centralized CFS configuration in one place.
Two modes (via Zones and via App Rules).	Merged functions into one mode.
Admin cannot predict the filtering results accurately after configuration.	Admin can exactly predict the filtering results.
Need to define duplicated filtering options.	Define CFS Category object, URI List object, Profile object and Action object, which can be reused in multiple policies.
Does not support wildcard matching.	Supports wildcard (*) matching for URI List.
Consent feature is global.	Consent feature is per policy.
BWM is only supported in App Rules mode.	BWM is fully supported.
Does not support Override – Confirm.	Supports Override – Confirm.
Only supports GET, POST and HEAD commands for HTTP.	Supports GET, HEAD, POST, PUT, CONNECT, OPTIONS, DELETE, REPORT, COPY and MOVE commands.
Cannot enable/disable CFS globally.	Can enable/disable CFS globally.
Custom category is based on category.	Custom category is based on domain, which is more intuitive.
Websense configuration is mixed with CFS configuration.	Separate Websense configuration from CFS configuration helps prevent errors.

Resolved issues

The following issues are resolved in this release.

App Rules

Resolved issue	Issue ID
An App Rule of SMTP Client type with File extension as Match Object does not block matching emails when used with SMTPS. Occurs when Client DPI-SSL and Application Firewall are enabled and the App Rules policy uses a Match Object Type: File extension, Content: exe,txt,jpg, and then email is sent from a client with txt or jpg files in the attachment. It works fine if Client DPI-SSL is not enabled.	175840

High Availability

Resolved issue	Issue ID
A High Availability pair of NSA 4600s experience frequent HA Failover/Failback events. Occurs when Physical Monitoring is enabled only on the X0 interface, and the active firewall detects a better link status on the idle firewall, in conjunction with the LDAP task waiting for too long for a lock to be released.	174010
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

Networking

Resolved issue	Issue ID
VLAN interfaces and subsequent VPN tunnel policies are not created. Occurs when importing a configuration file from an NSA 5600 firewall to an NSA 6600 firewall.	173505
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

System

Resolved issue	Issue ID
The active firewall in a High Availability pair goes down with memory errors on the data plane. Occurs when Single Sign-On users are authenticating over HTTP, and enterprise data center traffic is passing through the HA pair.	175380

User Interface

Resolved issue	Issue ID
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

Users

Resolved issue	Issue ID
The domain element of logged in users is not displayed on the Users > Status page if a very large number of users are authenticated using Single Sign-On, and a warning is displayed, "Attempt to free already freed entry 0x35d4f2d8 to UserIpDomain free list!". Occurs when the maximum allowed number of users (100,000 in this case) are authenticated using SSO on the appliance, with about two thirds of them (65,535) authenticated to the same domain, and then some of those users log out, causing the domain element to stop being displayed for the remaining users in that domain. After more users log out, the warning is displayed.	174654

VPN

Resolved issue	Issue ID
A VPN tunnel policy cannot be established. Occurs when the tunnel is bound to a DHCP WAN interface that is not in the WAN Load Balancing (WLB) group and the system is rebooted.	175975
The Allow Advanced Routing option should not be displayed on the Site-to-Site VPN policy configuration window. Occurs when configuring a Site-to-Site VPN policy and viewing the Advanced tab. This option should only be displayed for a Tunnel Interface policy.	175850
Unable to add a manual key. Occurs when attempting to add an IPv6 manual key on the **VPN** > **Settings** > **VPN Policy** dialog.	170547
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
A 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, the VPN tunnel interface cannot be deleted as the name has been lost during the upgrade.	169627

Resolved issue	Issue ID
The guest login status window with the Logout button is still displayed although the option to display it is disabled.	175286
Occurs when Wireless Guest Services is enabled and the "Show guest login status window with logout button" option is not selected on the Users > Guest Services page, and then a wireless client logs in.	
Authentication for a SonicPoint ACe/ACi/N2 cannot be changed directly.	171722
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**.	

Known issues

The following are known issues in this release.

3G/4G

Known issue	Issue ID
The Connect on Data mode is not working for 3G cards, causing traffic to stop passing and no Internet access due to an unsuccessful failover to WWAN after the WAN interface is disconnected.	175877
Occurs when a 3G card is connected to the U0 port, U0 is configured in Connect on Data mode as the final backup for the WAN (X1) interface, traffic is passing from a client system on the LAN side to the WAN and then the X1 interface is disconnected.	
Some China-Huawei 3G cards do not connect after the primary WAN interface goes down.	175146
Occurs when 3G is configured as final backup in DoD mode, while using a China-Huawei 3G card, including the Huawei E398 card with China Unicom SIM card and the Huawei EC169C card with China Telecom SIM card.	
Website access over AT&T Beam and AT&T Momentum 4G USB modem cards fails with a connection reset page. Other traffic types succeed, including ping, telnet, and nslookup.	168487
Occurs when accessing the Internet over the WWAN interface while either of these AT&T cards is connected to the U0 port. This issue occurs because the Maximum Transmission Unit (MTU) changed from 1500 to 40 in the AT&T network.	

AppFlow

Known issue	Issue ID
The GMS flow server continues to send flow data to Agent 1 after updating the configuration to use Agent 2.	175592
Occurs when Apply is not clicked after updating the configuration to use Agent 2.	

App Rules

Resolved issue	Issue ID
Policies with match objects are not enforced. Occurs when the match object size is greater than 150 bytes.	173739

Capture ATP

Known issue	Issue ID
The scanned files are truncated and the firewall log shows "File truncated due to highly delayed acks", but the scan history shows all 45 files scanned with result clean. Occurs when sending a PDF file with IMAP protocol as an attachment through a VPN tunnel interface.	176213
Some file uploads result in a "highly delayed acks" response and do not receive the expected receipt confirmation from the cloud servers. Occurs when the number of files uploaded for analysis exceeds the concurrent files limit for the platform. On a platform supporting 25 concurrent files, if 50 files are uploaded for analysis, a "highly delayed acks" response is received for two of them.	175967
The Gateway Anti-Virus status says, "Gateway Anti-Virus Status: File sent to Sandbox, but could not confirm receipt due to highly delayed acks". Occurs after sending a file to the Capture ATP cloud servers for analysis.	175415

DPI-SSL

Known issue	Issue ID
The HTTPS service object is not correctly excluded by Client DPI-SSL. Occurs when the firewall is deployed between an HTTPS proxy server and a client system, the proxy server is configured in the client browser, Client DPI-SSL is enabled along with the **Deployments wherein the Firewall sees a single server IP for different server domains, ex: Proxy setup** option, HTTPS is selected in the Client DPI-SSL Exclude drop-down for Service Object/Group, and then the user accesses some online banking websites which are not excluded as expected, but are decrypted by DPI-SSL and the certificates are re-issued by SonicWALL. If proxy is not set in the client browser, those sites are correctly excluded from DPI-SSL.	175696

Log

Known issue	Issue ID
The Web Site Hits table is always empty in the Log > Reports page. Occurs when clicking the Start Data Collection button on the Log > Reports page and then running LAN to WAN HTTP/HTTPS web browsing traffic.	176224

Networking

Known issue	Issue ID
SonicOS does not display the learned OSPF network in either the OSPF routing table or in the IP routing table. Occurs when the interface on the area border router (ABR) for the area including the firewall is configured as passive.	175469

Known issue	Issue ID
The tunnel interface name is not displayed in the connection monitor table after traffic passes through an unnumbered VPN tunnel interface. Occurs when a tunnel interface VPN policy is added and a static route going through this VPN tunnel interface is added, and then traffic is sent to the destination.	175449
Traffic fails on 10Gb interfaces that are changed from Wiremode in a High Availability pair. Occurs when X18 and X19 are configured as Wiremode pair interfaces in inspect mode and traffic is passing, and then X18 is unassigned, then assigned to the LAN zone as a static interface and a DHCP server is bound to it. After a client PC connected to X18 renews its DHCP lease, traffic to the WAN fails and pings from the client PC are not received.	175333
The link status between a TZ appliance and a Dell X-Series switch displays "no link". Occurs when changing the link settings to 100 Mbps Full-Duplex with one switch using an Isolated Link configuration or with two switches using a Common Link configuration.	175205
The FQDN resolved results are not synchronized on the firewalls in an HA pair. Occurs when a firewall in an HA pair is idle and Stateful Synchronization is enabled.	174716
Auto-added route entries for the WAN are disabled and dimmed in a firewall configured with a redundant WAN port. Occurs when WAN port goes down but its redundant port is still up, and then the firewall is restarted.	173703

Security Services

Known issue	Issue ID
Workstations cannot communicate with Windows Shared Folders. Files cannot be copied, and this GAV alert is generated, "SMB out of order read/write". Occurs when the CIFS/Netbios option is enabled on the Security Services > Gateway Anti-Virus page. Communication works after disabling CIFS/Netbios.	175366
Gateway Anti-Virus does not correctly block a malicious email attachment. Occurs when using Thunderbird as the email client to download email from an IMAP server on the WAN, and email with a malicious attachment is downloaded.	174499

Switching

Known issue	Issue ID
The L2 LAG members are not aggregated on the VLAN trunk ports, and traffic is blocked. Occurs when PortShield and L2 LAG are configured on the VLAN trunk, and the firewall is restarted.	175363
A VLAN interface bound to a Trunk interface cannot be deleted, and the Switching > VLAN Trunking page only shows the first 32 configured VLAN interfaces. Occurs when more than 32 VLAN interfaces are configured on the Trunk interface, and the one to be deleted is not displayed on the Switching > VLAN Trunking page.	175229
The L2 Link Aggregation Group (LAG) function does not respond. Occurs when creating a new LAG group, and the aggregator port link is down, and the primary WAN is in Round Robin mode.	175152

Syslog

Known issue	Issue ID
Syslog messages for both admin and user login sessions show "dur=0", instead of the actual duration of the login. This causes SonicWALL GMS to display zeros for the login session duration. Occurs when capturing and viewing the syslog messages that are sent to GMS, and when viewing the login durations in GMS.	175823

System

Known issue	Issue ID
Sending diagnostic reports to Support can cause the SonicOS management interface to become unresponsive for up to 15 minutes. Occurs when the **Send Diagnostic Reports to Support** button is clicked on the System > Diagnostics page.	175969
The **Enable FTP 'REST' requests with Gateway AV** option in the Gateway Anti-Virus settings is not turned on after enabling DPI and Stateful Firewall Security. Occurs when GAV is licensed but disabled with all options disabled, and then the **DPI and Stateful Firewall Security** button is clicked on the System > Settings page and the firewall restarts.	175100
The **Enable HTTP Byte-Range requests with Gateway AV** option in the Gateway Anti-Virus settings is not turned on after enabling DPI and Stateful Firewall Security. Occurs when GAV is licensed but disabled with all options disabled, and then the **DPI and Stateful Firewall Security** button is clicked on the System > Settings page and the firewall restarts.	175098
Connections do not update their configurations. Occurs when Enable Stealth Mode and Randomize IP ID are enabled, and Decrement IP TTL for forwarded traffic is disabled, and Maximum DPI Connections is set with DPI services enabled.	175006

Users

Known issue	Issue ID
Local users with Limited Administration rights and local users who are part of the Read-only Administrators group cannot access the SonicOS management page, but are redirected to an authentication page. Occurs when the local users also belong to the Guest Services group, and Guest Services is enabled in the LAN zone, and the user attempts to log into the appliance and clicks the Manage button.	175973
RADIUS or LDAP authenticated user sessions remain active after clicking the Logout button. Occurs when a user on the LAN side attempts to access the Internet through the firewall and logs in when the login redirect window is displayed and then clicks the Logout button. When the Users > Status page is checked, the Active User Sessions table still shows the user session as active, and the user can continue to access the Internet from the same computer without being required to log in again.	175765

VPN

Known issue	Issue ID
The **Apply NAT Policies** option cannot be enabled in a VPN policy of type Tunnel Interface, preventing NAT policies from being applied over the unnumbered tunnel interface. Occurs when the VPN policy is added with the Apply NAT Policies option enabled, but when verifying it, the checkbox for Apply NAT Policies is not selected and it cannot be enabled.	175882
Traffic over a numbered tunnel interface fails after upgrading the appliance firmware. Occurs when the firewall is upgraded from SonicOS 6.2.4.2 to 6.2.5.1 or 6.2.6.0. **Workaround**: After importing configuration settings from a firewall running 6.2.4.2 to a firewall running 6.2.5.1 or 6.2.6.0, manually recreate the VPN Tunnel Interface (numbered tunnel interface), the route entries, and the firewall access rules.	175845
Connecting via SSH to a firewall with a VPN tunnel set up results in the error message, "maximum number of ssh sessions are active, please try again later". Occurs when a site-to-site VPN tunnel is active between two firewalls and four SSH sessions are started on one of the firewalls, then the VPN tunnel is disabled followed by exiting all SSH sessions, and then the VPN tunnel is reconnected and the administrator attempts to connect via SSH again.	175610

Wireless

Known issue	Issue ID
The beacon interval for a SonicPoint Virtual Access Point (VAP) is affected by the beacon interval set for an internal wireless VAP. The error message "Error: Too small 802.11 Beacon Interval for Virtual Access Point" is displayed upon moving more than four VAP objects into a Virtual Access Point Group. Occurs when a SonicPoint is connected to a TZ Wireless appliance which has its wireless radio enabled with the Internal AP Group configured as the Virtual Access Point Group, and the beacon interval is set to a value such as 400 milliseconds on the Wireless > Advanced page. The SonicPoint is connected to a WLAN interface of the TZ and its beacon interval is set to a different value, such as 600 milliseconds, and then five VAP objects are added on the SonicPoint > Virtual Access Point page. Next, a Virtual Access Point Group is added and the five VAP objects are moved to it, resulting in the error message.	175891

Product licensing

The Capture ATP license requires that Gateway Anti-Virus (GAV) is also licensed. You must enable Gateway Anti-Virus (GAV) and Cloud Anti-Virus before you can use Capture ATP. See the *SonicOS 6.2.6 Capture ATP Feature Guide* for details on licensing Capture ATP.

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/.

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.