

Release Notes

Contents

<i>Platform Compatibility</i>	1
<i>Browser Support</i>	2
<i>Supported Features</i>	2
<i>Enhancements in SonicOS 5.8.1.8</i>	5
<i>Key Features in SonicOS 5.8</i>	9
<i>Known Issues</i>	24
<i>Resolved Issues</i>	25
<i>Upgrading SonicOS Image Procedures</i>	29
<i>Related Technical Documentation</i>	34

Platform Compatibility

The SonicOS 5.8.1.8 release is supported on the following SonicWALL Deep Packet Inspection (DPI) security appliances:

- SonicWALL NSA E8500
- SonicWALL NSA E7500
- SonicWALL NSA E6500
- SonicWALL NSA E5500
- SonicWALL NSA 5000
- SonicWALL NSA 4500
- SonicWALL NSA 3500
- SonicWALL NSA 2400
- SonicWALL NSA 240
- SonicWALL TZ 210 / 210 Wireless
- SonicWALL TZ 200 / 200 Wireless
- SonicWALL TZ 100 / 100 Wireless

The SonicWALL WXA series appliances (WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are also supported for use with SonicWALL NSA E-Class, NSA, and TZ products running 5.8.1.8. The minimum recommended firmware version for the WXA series appliances is 1.1.1.

Release Notes

Browser Support



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

This release supports the following Web browsers:

- Chrome 11.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 4.0 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 SonicWALL appliance system administration.

Supported Features

This section details the supported SonicOS 5.8 features by appliance model and how they are affected by the licensing status.

Supported Features by Appliance Model

The following table lists the key features in SonicOS 5.8 and which appliance models support them.

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 210 Series	TZ 200 Series	TZ 100 Series
Wireless Client Bridge Support			Supported	Supported	Supported
App Flow Monitor	Supported	Supported	Supported		
Real-Time Monitor	Supported	Supported	Supported		
Packet Monitor Enhancements	Supported	Supported	Supported	Supported	Supported
Log > Flow Reporting Enhancements	Supported	Supported	Supported		
App Control Advanced	Supported	Supported	Supported	Supported	Supported
App Rules	Supported	Supported	Supported		
DPI-SSL	Supported	Supported			
Cloud GAV	Supported	Supported	Supported	Supported	Supported
NTP Auth Type	Supported	Supported	Supported	Supported	Supported
Link Aggregation	Supported				
Port Redundancy	Supported				
CFS Enhancements	Supported	Supported	Supported	Supported	Supported
IPFIX & NetFlow Reporting	Supported	Supported	Supported		

Release Notes

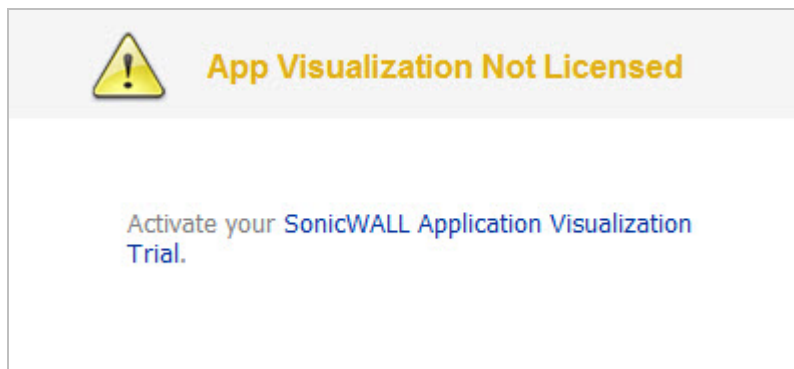
Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 210 Series	TZ 200 Series	TZ 100 Series
VLAN Subinterfaces	Supported	Supported	Supported	Supported	Supported
SonicPoint VAPs	Supported	Supported	Supported	Supported	Supported
CASS 2.0	Supported	Supported	Supported	Supported	Supported
Enhanced Connection Limit	Supported	Supported	Supported	Supported	Supported
Dynamic WAN Scheduling	Supported	Supported	Supported	Supported	Supported
Browser NTLM Auth	Supported	Supported	Supported	Supported	Supported
User Import from LDAP	Supported	Supported	Supported	Supported	Supported
SSL VPN NetExtender Client Update	Supported	Supported	Supported	Supported	Supported
DHCP Scalability Enhancements	Supported	Supported	Supported	Supported	Supported
SIP Application Layer Enhancements	Supported	Supported	Supported	Supported	Supported
SonicPoint-N DR	Supported	Supported	Supported	Supported	Supported
Accept Multiple VPN Client Proposals.	Supported	Supported	Supported	Supported	Supported
WAN Acceleration Support	Supported	Supported	Supported	Supported	Supported
App Control Policy Configuration via App Flow Monitor	Supported	Supported	Supported	Supported	Supported
Global BWM Ease of Use Enhancements	Supported	Supported	Supported	Supported	Supported
Application Usage and Risk Report	Supported	Supported	Supported		
Geo-IP Filtering and Botnet Command & Control Filtering	Supported	Supported	Supported		
Wire and Tap Mode	Supported	NSA 3500 and above			
Customizable Login Page	Supported	Supported	Supported	Supported	Supported
Preservation of Anti-Virus Exclusions After Upgrade	Supported	Supported	Supported	Supported	Supported
Management Traffic Only Option for Network Interfaces	Supported	Supported	Supported	Supported	Supported
Current Users and Detail of Users Options for TSR	Supported	Supported	Supported	Supported	Supported
User Monitor Tool	Supported	Supported	Supported		
Auto-Configuration of URLs to Bypass User Authentication	Supported	Supported	Supported	Supported	Supported

Release Notes

Supported Features and Licensing

Some pages in the SonicOS management interface do not display if the license is not activated for the feature on that page.

Here is an example of the Dashboard > Real-Time Monitor page with App Visualization not licensed:



The following table lists the key features in SonicOS 5.8 that depend on licenses and other settings for the related management interface pages to display and function properly:

SonicOS Feature	No license (SGSS)	With license Disabled in flow reporting	With license and enabled in flow reporting
Dashboard > Real-Time Monitor	Blocks the page with a license popup window.	All charts are independently enabled or disabled from the Log > Flow Reporting page. It is not dependent on Visualization being enabled.	All charts are enabled. The App charts content depends on whether Visualization or App Control Advanced is enabled with zone settings.
Dashboard > AppFlow Monitor	Blocks the page with a license popup window.	The AppFlow Monitor Page displays the message "flow reporting and visualization is disabled". Content is not shown.	All tabs are visible and fully operational.
Dashboard > BWM Monitor	Blocks the page with a license popup window.	Always on if Global BWM and Interface are enabled.	Always on if Global BWM and Interface are enabled.
Log > Flow Reporting	Blocks the page with a license popup window.	Available	Available
Security Services > GeolP Filter	Blocks the page with a license popup window.	Not available	Available
Security Services > Botnet Filter	Blocks the page with a license popup window. * This is a separate license and is not part of the SGSS.	Available	Available

Release Notes

Enhancements in SonicOS 5.8.1.8

This section details the enhancements in the SonicOS 5.8.1.8 release:

- **YouTube for School Content Filtering Support** — YouTube for Schools is a service that allows for customized YouTube access for students, teachers, and administrators. YouTube Education (YouTube EDU) provides schools access to hundreds of thousands of free educational videos. These videos come from a number of respected organizations. You can customize the content available in your school. All schools get access to all of the YouTube EDU content, but teachers and administrators can also create playlists of videos that are viewable only within their school's network. Before configuring your SonicWALL security appliance for YouTube for Schools, you must first sign up: www.youtube.com/schools

The configuration of YouTube for Schools depends on the method of Content Filtering you are using, which is configured on the **Security Services > Content Filter** page.

Membership in Multiple Groups

- If a user is a member of multiple groups where one policy allows access to any part of YouTube and the other policy has a YouTube for Schools restriction, the user will be filtered by the YouTube for Schools policy and not be allowed unrestricted access to YouTube.
- A user cannot be a member of multiple groups that have different YouTube for School IDs. While the firewall will accept the configuration, this is not supported.

Note: For more information on the general configuration of CFS, refer to the **Security Services > Content Filter** section in the *SonicOS Administrator's Guide*.

- When the **CFS Policy Assignment** pulldown menu is set to **Via Application Control**, YouTube for Schools is configured as an App Control Policy.

1. Navigate to **Firewall > Match Objects** and click **Add New Match Object**.

The screenshot shows the 'Match Object Settings' dialog box. The 'Object Name' field contains 'CFS Allow YT4S'. The 'Match Object Type' dropdown is set to 'CFS Allow/Forbidden List'. The 'Match Type' dropdown is set to 'Partial Match'. Under 'Input Representation', the 'Alphanumeric' radio button is selected. The 'Content' field contains 'youtube.com'. Below it, a list box contains 'youtube.com' and 'ytimg.com'. To the right of the list box are buttons for 'Add', 'Update', 'Remove', 'Remove All', and 'Load From File'. At the bottom of the dialog, there is a 'Ready' status bar and buttons for 'OK', 'Cancel', and 'Help'.

2. Type in a descriptive name, and then select **CFS Allow/Forbidden List** as the **Match Object Type**.
3. Select **Partial Match** for the **Match Type**.
4. In the **Content** field, type in "youtube.com" and then click **Add**.
5. Type in "ytimg.com" and then click **Add**.
6. Click **OK** to create the Match Object.

Release Notes

7. Navigate to the **Firewall > App Rules** page and click **Add New Policy**.

App Control Policy Settings

Policy Name: CFS YouTube

Policy Type: CFS

Address: Any

Exclusion Address: None

Match Object: CFS-Any

Action Object: CFS block page

Users/Groups: Included: All Excluded: None

Schedule: Always on

Enable flow reporting:

Enable Logging:

Log using CFS message format:

Log Redundancy Filter (seconds): Use Global Settings 1

Zone: Any

CFS Allow/Excluded List: CFS Allow YT4S

CFS Forbidden/Included List: None

Enable Safe Search Enforcement:

Enable YouTube for Schools:

School ID: uflGb16ejHSRqXnnnK2Jg

Note: BWM Type: Advanced; To change go to [Firewall Settings > BWM](#)

Ready

OK Cancel Help

8. Type in a descriptive **Policy Name**.
9. For the **Policy Type**, select **CFS**.
10. Select the appropriate settings for **Match Object** and **Action Object**, based on your environment.
11. For **CFS Allow/Excluded List**, select the Match Object you just created (our example uses “CFS Allow YT4S”).
12. Select the **Enable YouTube for Schools** checkbox.
13. Paste in your **School ID**, which is obtained from www.youtube.com/schools
14. Click **OK** to create the policy.

NOTE: Once the policy has been applied, any existing browser connections will be unaffected until the browser has been closed and reopened. Also, if you have a browser open as administrator on the firewall, you will be excluded from CFS policy enforcement unless you configure the firewall specifically not to exclude you (select the **Do not bypass CFS blocking for the Administrator** checkbox on the **Security Services > Content Filter** page).

Release Notes

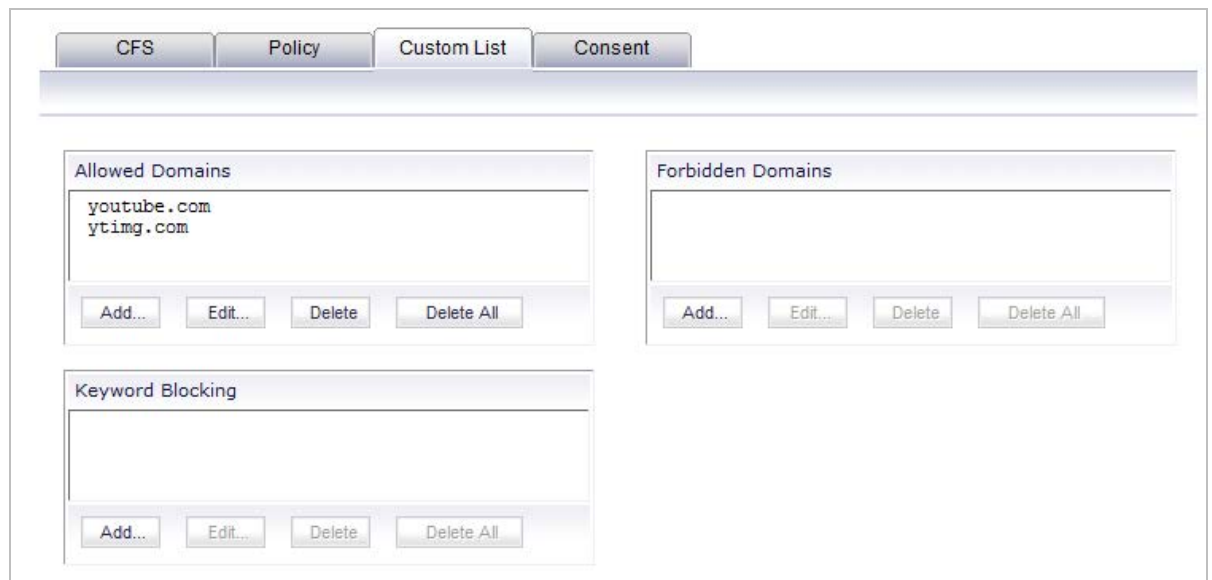
- When the **CFS Policy Assignment** pulldown menu is set to **Via User and Zone Screens**, YouTube for Schools is configured as part of the Content Filter policy.
 1. On the **Security Services > Content Filter** page, select **Content Filter Service** for the **Content Filter Type** pulldown menu.
 2. Click the **Configure** button.
 3. On the **Policy** tab, click the **Configure** icon for the CFS policy on which you want to enable YouTube for Schools.
 4. Click on the **Settings** tab, and select the **Enable YouTube for Schools** checkbox.
 5. Paste in your School ID, which is obtained from www.youtube.com/schools.

The screenshot shows the 'Settings' tab of the Content Filter configuration. Under 'Custom List Settings', three dropdown menus are set to 'Global'. Under 'Safe Search Enforcement Settings', the 'Enable Safe Search Enforcement' checkbox is unchecked. The 'YouTube for Schools' section is highlighted with a red box, showing the 'Enable YouTube for Schools' checkbox checked and the 'School ID' field containing 'Lj3Q2GVaHbr3k_yiY2lhkQ'. At the bottom, the 'Filter Forbidden URLs by time of day' dropdown is set to 'Always on'.

6. Click **OK**.
7. On the **Custom List** tab, click the **Add** button for **Allowed Domains**.
8. In the dialog box, type "youtube.com" into the **Domain Name** field and click **OK**.
9. Click **Add** again.

Release Notes

10. Type "yting.com" into the **Domain Name** field and click **OK**.



The screenshot shows the SonicWall configuration interface with the 'Custom List' tab selected. It features three main sections: 'Allowed Domains', 'Forbidden Domains', and 'Keyword Blocking'. The 'Allowed Domains' section contains a list with 'youtube.com' and 'yting.com'. Below this list are buttons for 'Add...', 'Edit...', 'Delete', and 'Delete All'. The 'Forbidden Domains' section is currently empty and also has 'Add...', 'Edit...', 'Delete', and 'Delete All' buttons. The 'Keyword Blocking' section is also empty with 'Add...', 'Edit...', 'Delete', and 'Delete All' buttons. At the top of the interface, there are tabs for 'CFS', 'Policy', 'Custom List', and 'Consent'.

11. Click **OK**.

These settings will override any CFS category that blocks YouTube.

NOTE: Once the policy has been applied, any existing browser connections will be unaffected until the browser has been closed and reopened. Also, if you have a browser open as administrator on the firewall, you will be excluded from CFS policy enforcement unless you configure the firewall specifically not to exclude you (select the **Do not bypass CFS blocking for the Administrator** checkbox on the **Security Services > Content Filter** page).

Release Notes

Key Features in SonicOS 5.8

The following are the key features introduced in SonicOS 5.8:

- **SonicOS Web-based Management Interface**— In SonicOS 5.8.1.8, HTTP access to the SonicOS web-based management interface is disabled by default. When running SonicOS 5.8.1.8 using factory defaults, the administrator can log into the management interface using HTTPS at <https://192.168.168.168>.

HTTP management is still allowed when upgrading from prior firmware versions, when already enabled in the previous configuration settings.

Note: HTTP management must be enabled when the firewall is being managed by SonicWALL GMS via a VPN tunnel. This applies when using either a GMS Management Tunnel or an existing VPN tunnel.

The System > Administration page has a new **Allow management via HTTP** checkbox to allow the administrator to enable/disable HTTP management globally.

Web Management Settings

Allow management via HTTP

HTTP Port: Delete cookies

HTTPS Port: End config. mode

Certificate Selection: ▾

Certificate Common Name:

Default Table Size: items per page ▾

Auto-updated Table Refresh Interval: in seconds ▾

Use System Dashboard View as starting page

Enable Tooltip

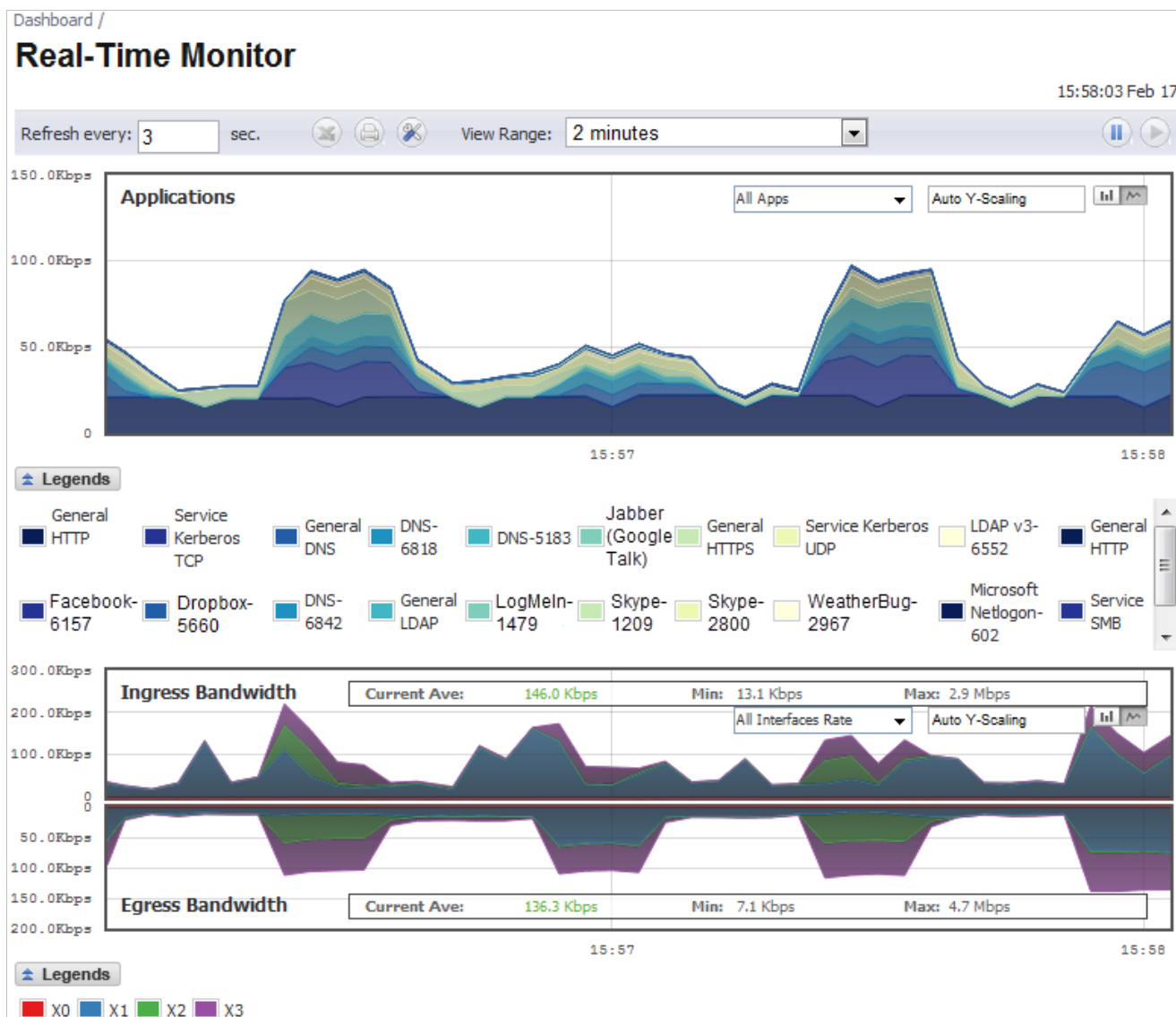
Form Tooltip Delay: in msec

Button Tooltip Delay: in msec

Text Tooltip Delay: in msec

Release Notes

- **Real-Time Monitor**— The real-time visualization dashboard monitoring feature allows administrators to respond quickly to network security vulnerabilities and network bandwidth issues. Administrators can see what websites their users are accessing, what applications and services are being used in their networks and to what extent, in order to police content transmitted in and out of their organizations.



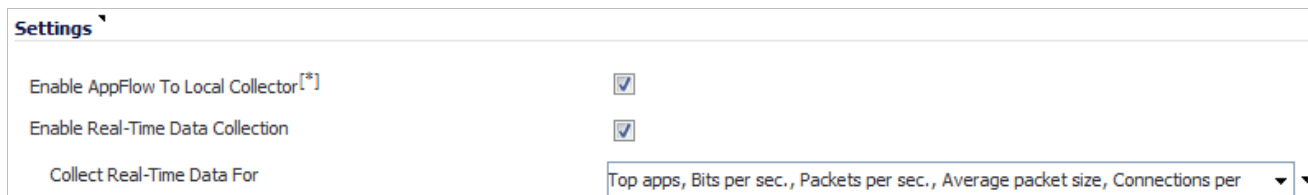
New appliances running SonicOS 5.8 receive an automatic 30-day free trial for App Visualization upon registration.

SonicWALL appliances upgrading to SonicOS 5.8 **and** already licensed for GAV/IPS/AS, Total Secure, or Comprehensive Gateway Security Suite (CGSS) automatically receive a complimentary App Visualization license for the Real-Time Visualization Dashboard.

Release Notes

To populate the Real-Time Monitor with data, navigate to the **Log > Flow Reporting** page, then click the **Enable Real-Time Data Collection** and **Enable AppFlow To Local Collector** checkboxes. In the **Collect Real-Time Data For** drop-down list, click the checkboxes for the types of data you wish to collect. You can then view real-time application traffic on the Dashboard > Real-Time Monitor page.

Note: Clicking the **Enable AppFlow to Local Collector** checkbox may require rebooting the device.

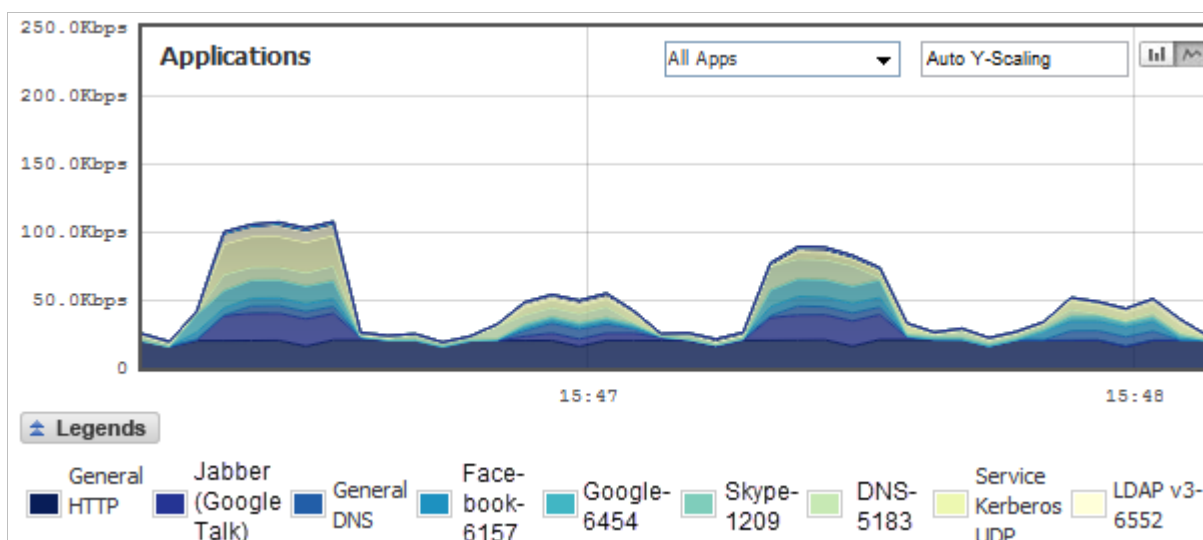


The screenshot shows the 'Settings' section of the Real-Time Monitor configuration. It includes three main settings:

- Enable AppFlow To Local Collector^[*]**:
- Enable Real-Time Data Collection**:
- Collect Real-Time Data For**: A dropdown menu with the selected option being "Top apps, Bits per sec., Packets per sec., Average packet size, Connections per".

All Real-Time Monitor application legends are hidden by default from the Application and Bandwidth charts.

To view the legends, click the **Legends** icon.



To relocate the legends into the Application or Bandwidth charts, click the  icon, then select the desired checkbox(s).



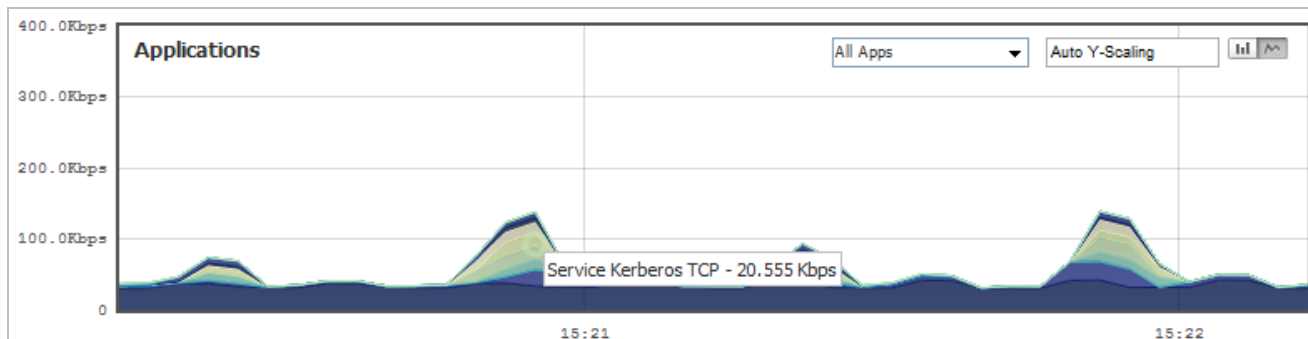
The screenshot shows a dialog box for configuring legend placement. It contains three checkboxes:

- Use Gradient
- Put legends inside Application Chart
- Put legends inside Bandwidth Chart

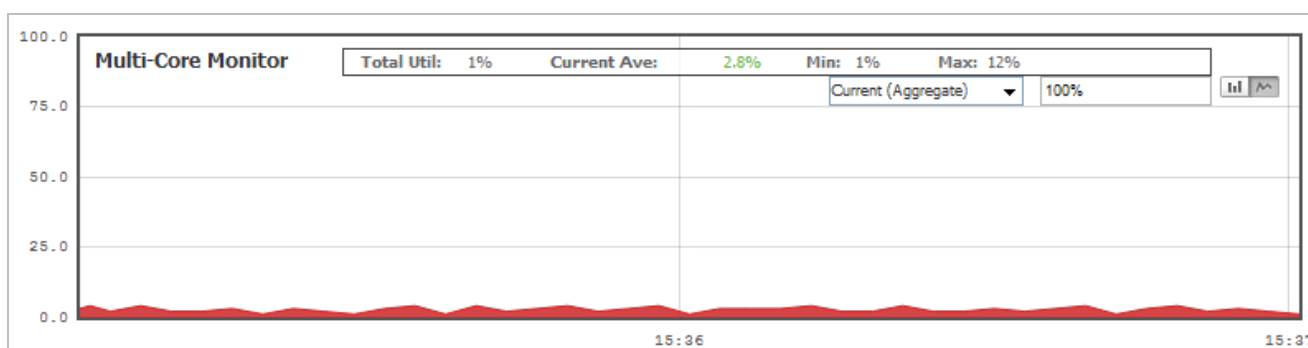
At the bottom of the dialog, there are four buttons: **Default**, **Generate**, **Cancel**, and **Save**.

Release Notes

To view individual application information, hover the mouse over the real-time visualization graph to display a tooltip.



By default, the Multi-Core Monitor displays as a stack chart, rather than as a bar graph, to easily show its relation to the other charts on this screen.



Note: In SonicOS 5.8.1.8, the Multi-Core Monitor only shows the processor load for the cores of the managing firewall. If operating in Active-Active DPI mode, the core load for the standby firewall does not display.

- **App Flow Monitor**—The toolbar categories display Total Packets, Total Bytes, and Average Rate, providing the user with a specific view of data being transferred.

Application	Sessions	Total Packets	Total Bytes	Ave Rate (KBps)	Threats
Dropbox	3	91	50,046	0.817	0
Service Kerberos TCP	7	76	21,168	2.953	0
BitTorrent/uTorrent	186	186	16,678	-	0
DNS	8	98	9,167	1.071	0
HTTP	4	142	7,482	0.970	0
LDAP v3	1	18	5,093	4.974	0

In the Flow Table, clicking on the number specified under the Sessions category of any Application, a Flow Table displays with Application-specific data, including the Rate in KBps.

Start Time	Last Update	Init MAC	Resp MAC	Init IP	Resp IP	Proto	Init Port	Resp Port	Init Iface	Resp Iface	Init Bytes	Resp Bytes	Rate (KBps)	Status
15:24:34 Jan 12	15:24:34 Jan 12	00:06:B1:10:4E:06	00:06:B1:10:4E:07	172.16.0.9	172.16.5.35	6	2854	80	X2	X3	23506	101000	-	Active
15:24:41 Jan 12	15:24:46 Jan 12	00:06:B1:10:4E:06	00:06:B1:10:4E:07	172.16.0.3	172.16.5.35	6	2854	80	X2	X3	46424	202048	425.906	Active

Release Notes

- **Log > Flow Reporting Page**— The Log > Flow Reporting page displays detailed external and internal flow reporting statistics.

External Flow Reporting Statistics		Internal AppFlow Reporting Statistics	
NetFlow/IPFIX Packets Sent:	0	Data Flows Enqueued:	559227
Connection Flows Enqueued:	0	Data Flows Dequeued:	559227
Connection Flows Dequeued:	0	Data Flows Dropped:	0
Connection Flows Dropped:	0	Data Flows Skipped Reporting:	0
Connection Flows Skipped Reporting:	0	General Flows Enqueued:	52647
Non-Connection data Enqueued:	0	General Flows Dequeued:	52647
Non-Connection data Dequeued:	0	General Flows Dropped:	30618
Non-connection data Dropped:	0	General Static Flows Dequeued:	192632
Netflow/IPFIX Templates sent:	0	AppFlow Collector Errors:	0
Non-connection related static data Reported:	0	Total Flows in DB:	8631

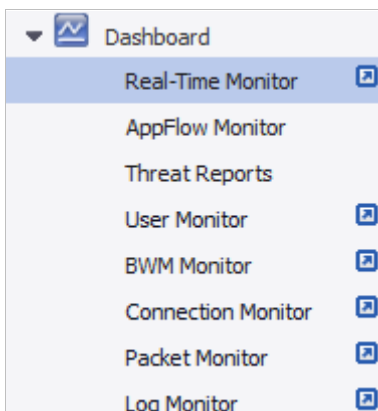
The **Settings** area provides options to enable AppFlow to Local Collector and Real-Time Data Collection, as well as to allow the selection of data type for real-time collection.

Report Settings are split into two sections, one for **Connection Report Settings** with options for reports about connections, and the other for **Other Report Settings** with additional options, including a way to specify URL types to include and an option to control the grouping of flows by domain or country.

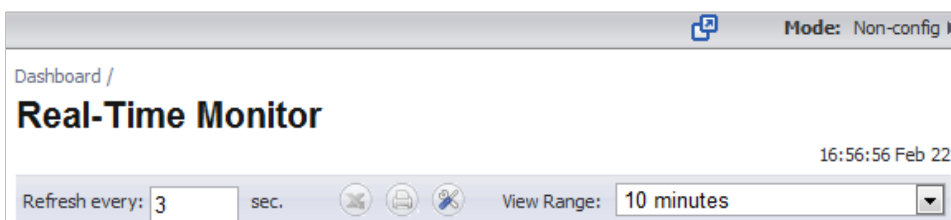
Settings	Connection Report Settings
Enable AppFlow To Local Collector ^[*]	Report Connections
Enable Real-Time Data Collection	Report On Connection OPEN
Collect Real-Time Data For	Report On Connection CLOSE
External Collector Settings	Report Connection On Active Timeout
Send AppFlow and Real-Time Data To EXTERNAL Collector ^[*]	Number Of Seconds
External Flow Reporting Format	Report Connection On Kilo BYTES Exchanged
External Collector's IP address	Kilobytes Exchanged
Source IP To Use Uor Collector On A VPN tunnel	Report ONCE
External Collector's UDP Port Number	Report Connections On Following Updates
Send IPFIX/Netflow Templates At Regular Interval	Other Report Settings
Send Static AppFlow At Regular Interval	Report DROPPED Connection
Send Static AppFlow For Following Tables	Skip Reporting STACK Connections
Send Dynamic AppFlow For Following Tables	Include Following URL Types
Include Following Additional Reports via IPFIX	Enable Geo-IP And Domain Resolution

Release Notes

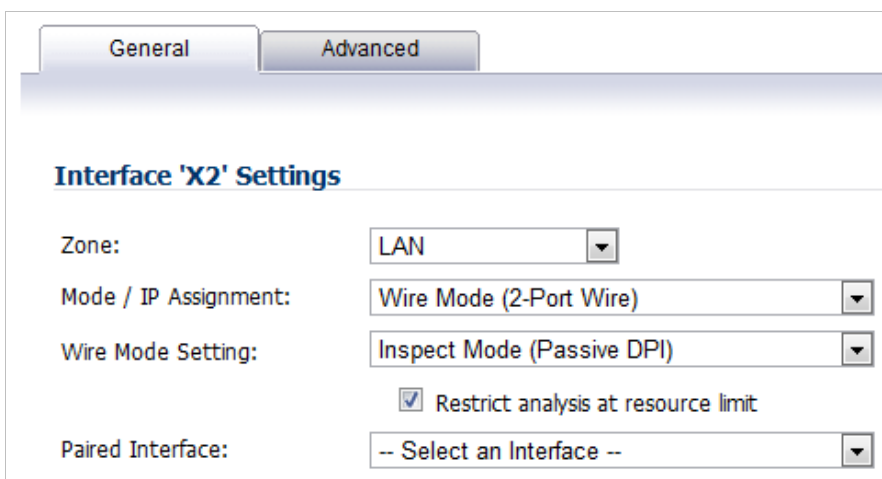
- **Pop-Up Visualization Dashboard Displays**—Several of the SonicWALL Visualization Dashboard pages contain a blue pop-up button that will display the dashboard in a standalone browser window that allows for a wider display. Click on the blue pop-up icon to the right of the page name in the left-hand navigating bar to display a dashboard page as a standalone page.



The pop-up button is also available at the top right of the individual dashboard pages, as shown below:



- **Wire Mode / Inspect Mode**—When **Inspect Mode (Passive DPI)** is selected as the **Wire Mode Setting**, a **Restrict analysis at resource limit** checkbox appears. This checkbox is selected by default. The behavior of this option is as follows:
 - Enabled – Scan only the amount of packets that the device can handle.
 - Disabled – Throttle the traffic to be able to scan all packets.



Release Notes

- **Application Intelligence + Control**—This feature has two components for more network security:

- (a) **Identification**: Identify applications and track user network behaviors in real-time.
- (b) **Control**: Allow/deny application and user traffic based on bandwidth limiting policies.

Administrators can easily create network policy object-based control rules to filter network traffic flows based on:

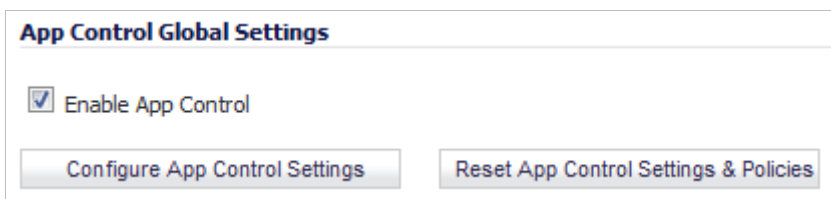
- Blocking signature-matching **Applications**, which are notoriously dangerous and difficult to enforce
- Viewing the real-time network activity of trusted **Users and User Groups** and guest services
- Matching **Content-rated categories**

Network security administrators now have application-level, user-level, and content-level real-time visibility into the traffic flowing through their networks. Administrators can take immediate action to re-traffic engineer their networks, quickly identify Web usage abuse, and protect their organizations from infiltration by malware. Administrators can limit access to bandwidth-hogging websites and applications, reserve higher priority to critical applications and services, and prevent sensitive data from escaping the SonicWALL secured networks.

New appliances running SonicOS 5.8 receive an automatic 30-day free trial for App Control upon registration.

SonicWALL appliances upgrading to SonicOS 5.8 **and** already licensed for GAV/IPS/AS, Total Secure, or Comprehensive Gateway Security Suite (CGSS) automatically receive a complimentary App Control license, required for creating Application Control policies.

Select the **Enable App Control** option on the Firewall > App Control Advanced page to begin using the App Control feature.

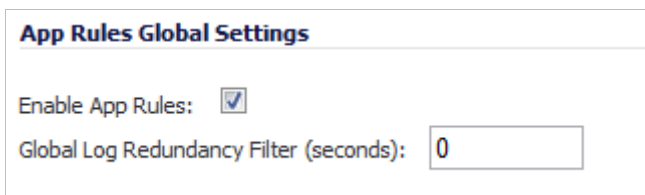


App Control Global Settings

Enable App Control

[Configure App Control Settings](#) [Reset App Control Settings & Policies](#)

To create policies using App Rules (included with the App Control license), select **Enable App Rules** on the Firewall > App Rules page.



App Rules Global Settings

Enable App Rules:

Global Log Redundancy Filter (seconds):

Release Notes

- **Global Bandwidth Management**—Global Bandwidth Management improves ease of use for bandwidth management (BWM) configuration, and increases throughput performance of managed packets for ingress and egress traffic on all interfaces, not just WAN. The new Firewall Settings > BWM page allows network administrators to specify guaranteed minimum bandwidth, maximum bandwidth, and control the number of different priority levels for traffic. These global settings are used in firewall access rules and application control policies. Global BWM provides:
 - Simple bandwidth management on all interfaces.
 - Bandwidth management of both ingress and egress traffic.
 - Support for specifying bandwidth management priority per firewall rules and application control rules.
 - Default bandwidth management queue for all traffic.
 - Support for applying bandwidth management directly from the Dashboard > App Flow Monitor page.

Global bandwidth management provides 8 priority queues, which can be applied to each physical interface.

The new **Firewall Settings > BWM** page is shown below:

Priority	Enable	Guaranteed	Maximum\Burst
0 Realtime	<input type="checkbox"/>	0 %	100 %
1 Highest	<input type="checkbox"/>	0 %	100 %
2 High	<input checked="" type="checkbox"/>	30 %	100 %
3 Medium High	<input type="checkbox"/>	0 %	100 %
4 Medium	<input checked="" type="checkbox"/>	50 %	100 %
5 Medium Low	<input type="checkbox"/>	0 %	100 %
6 Low	<input checked="" type="checkbox"/>	20 %	100 %
7 Lowest	<input type="checkbox"/>	0 %	100 %
Total:		100	

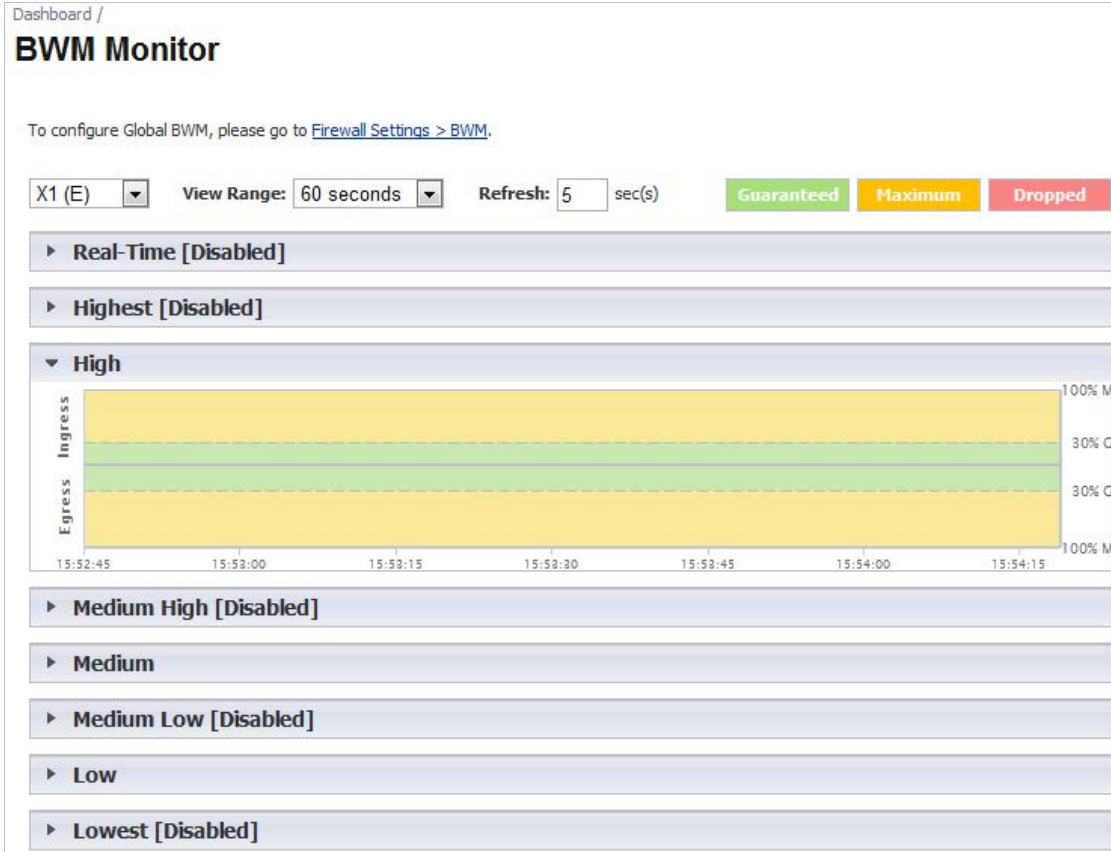
You can select either **WAN** or **Global** as the **Bandwidth Management Type**.

Note: When switching between bandwidth management modes, all bandwidth management settings in firewall access rules are set back to defaults and any custom settings must be reconfigured. Default BWM actions in Application Control policies are automatically converted to WAN BWM or Global BWM, using default priority levels.

In the global priority queue table, you can configure the **Guaranteed** and **Maximum\Burst** rates for each **Priority** queue. The rates are specified as a percentage. The actual rate is determined dynamically while applying BWM on an interface. The configured bandwidth on an interface is used in calculating the absolute value. The sum of all guaranteed bandwidth must not exceed 100%, and guaranteed bandwidth must not be greater than maximum bandwidth per queue.

Release Notes

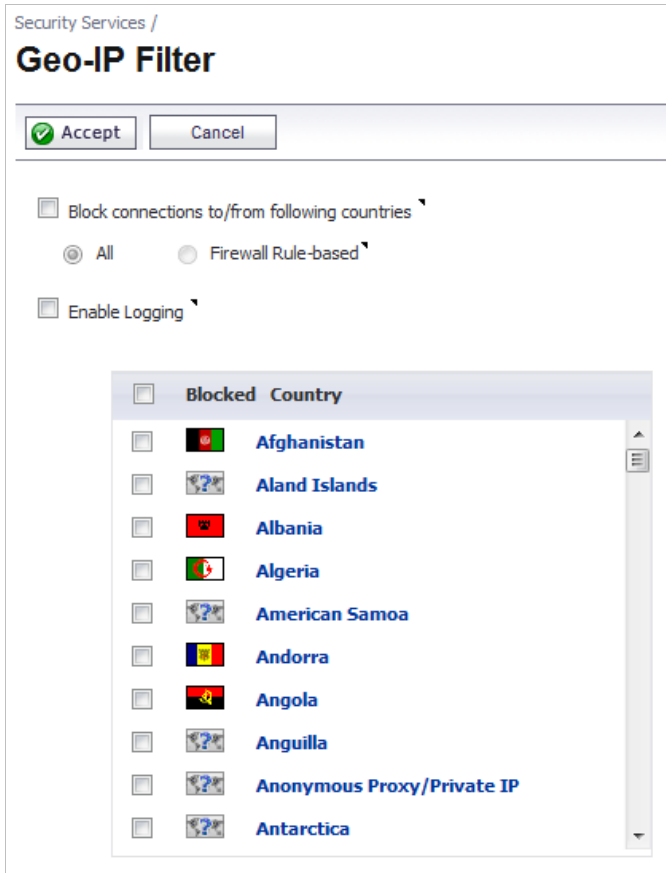
- **Bandwidth Management Monitor Page**—The new BWM Monitor page displays per-interface bandwidth management for ingress and egress network traffic. The BWM monitor graphs are available for real-time, highest, high, medium high, medium, medium low, low and lowest policy settings. The view range is configurable in 60 seconds, 2 minutes, 5 minutes, and 10 minutes (default). The refresh interval rate is configurable from 3 to 30 seconds. The bandwidth management priority is depicted by guaranteed, maximum, and dropped.



Release Notes

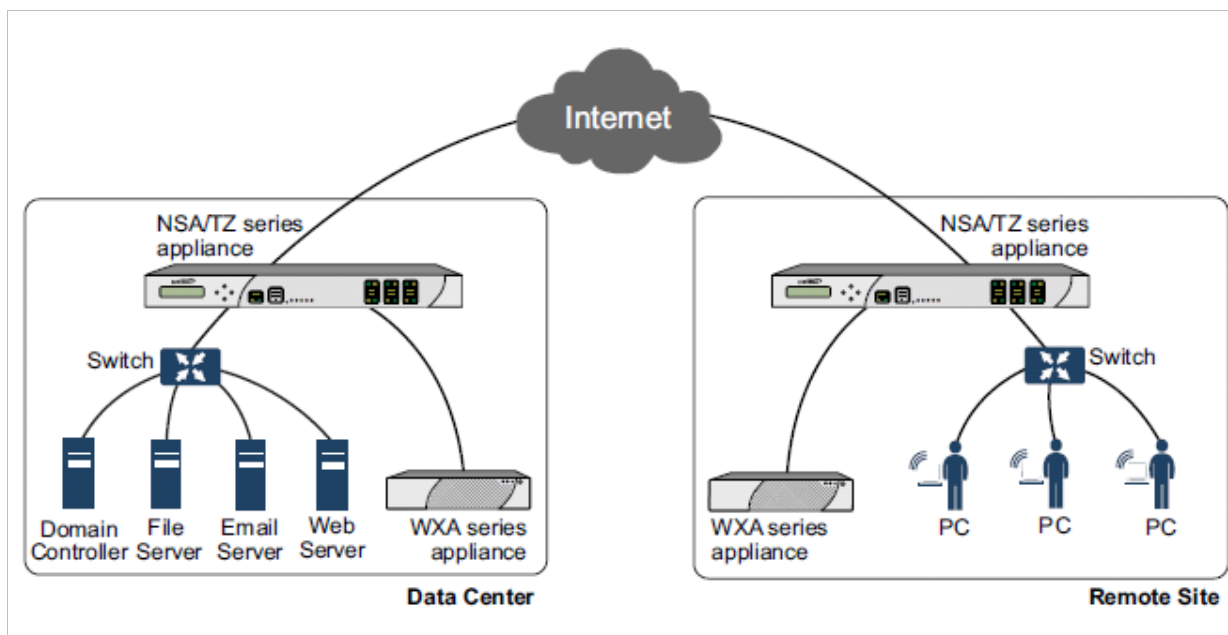
- **Geo-IP Filter**— The Geo-IP Filter includes several options, including the **Block Connections to/from Following Countries** checkbox and a checkbox for **Enable Logging**.

The **Block Connections to/from Following Countries** checkbox provides options to block **All** or block **Firewall Rule-Based**.



Release Notes

- **WAN Acceleration**—SonicOS 5.8.1.8 provides support for the SonicWALL WXA series appliances which are deployed in one-arm mode with SonicWALL firewalls. WAN Acceleration appliances employ techniques such as TCP acceleration and Windows File Sharing (WFS) acceleration to optimize WAN traffic between multiple locations connected by VPN or dedicated links. In this deployment, the SonicWALL appliance provides networking and security services, such as application control, intrusion prevention, anti-malware protection, VPN, routing, anti-spam, and content filtering while the WAN acceleration appliance eliminates redundant traffic and eliminates protocol latency. The following diagram illustrates the basic network topology for the SonicWALL WXA series appliances and the SonicWALL network security appliances.



WAN acceleration using a SonicWALL WXA series appliance can provide an increase in application performance response time without purchasing a higher quality service or larger provision of bandwidth. This is especially noticeable on WAN connections such with high latency, which causes some applications to perform poorly.

- **SonicPoint-N Dual Radio Support**—The SonicWALL **SonicPoint-N Dual Radio** appliance (SonicPoint-N DR) is supported by all SonicWALL NSA and TZ platforms when running SonicOS 5.8.0.3 or higher.

With support for two wireless radios at the same time, you can use **SonicPoint-N DR Clean Wireless** access points to create an enterprise-class secure wireless network. The SonicPoint-N DR uses six antennas to communicate with wireless clients on two frequency ranges: 2.4 GHz and 5 GHz. You can install and configure a SonicPoint-N DR access point in about an hour.

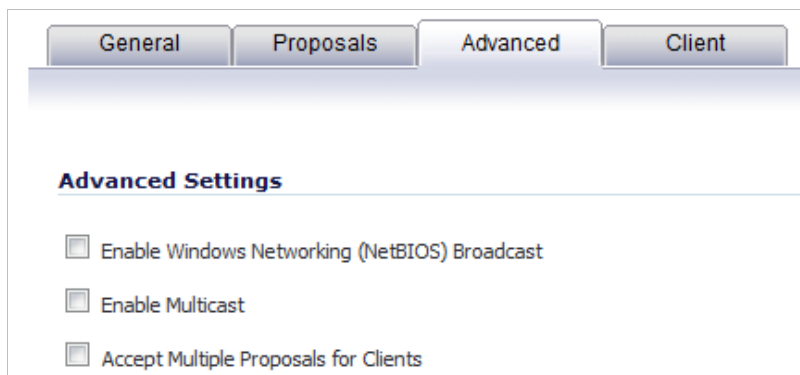
Note: The SonicPoint-N DR cannot broadcast the same Service Set Identifiers (SSID) when using Virtual Access Points (VAP) on 2.4 and 5 GHz frequency ranges.

For more information, see the *SonicWALL SonicPoint-N DR Getting Started Guide*, at: http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=PG&id=444



Release Notes

- **Accept Multiple Proposals for Clients Option**—The **Accept Multiple Proposals for Clients** checkbox allows multiple VPN or L2TP clients using different security policies to connect to a firewall running SonicOS 5.8.0.3 or higher
The option is on the **Advanced** tab when configuring a GroupVPN policy from the **VPN > Settings** page in SonicOS.



The client policy is still strictly checked against the configured proposal in the Proposals tab, as with clients connecting with SonicWALL GVC. This option has no effect on GVC.

If the **Accept Multiple Proposals for Clients** option is selected, SonicOS will allow connections from other L2TP clients, such as Apple OS, Windows, or Android clients whose offered proposal is different from what is configured on the Proposals tab. The proposal is accepted if it meets the following conditions:

- If the offered algorithm matches one of the possible algorithms available in SonicOS.
- If the offered algorithm is stronger and more secure than the configured algorithm in the SonicOS proposal.

If this option is not selected, SonicOS will require the client to strictly match the configured policy.

This option allows SonicWALL to support heterogeneous environments for Apple, Windows, and Android clients. Using this option, SonicOS can work with these clients if their proposal includes a combination of algorithms which are supported in SonicOS, but are not configured in the policy to prevent other clients like GVC from failing.

- **Deep Packet Inspection of SSL encrypted data (DPI-SSL)**—Provides the ability to transparently decrypt HTTPS and other SSL-based traffic, scan it for threats using SonicWALL's Deep Packet Inspection technology, then re-encrypt (or optionally SSL-offload) the traffic and send it to its destination if no threats or vulnerabilities are found. This feature works for both client and server deployments. It provides additional security, application control, and data leakage prevention functionality for analyzing encrypted HTTPS and other SSL-based traffic. The following security services and features are capable of utilizing DPI-SSL: Gateway Anti-Virus, Gateway Anti-Spyware, Intrusion Prevention, Content Filtering, Application Control, Packet Monitor and Packet Mirror. DPI-SSL is supported on SonicWALL NSA models 240 and higher.
- **Gateway Anti-Virus Enhancements (Cloud GAV)**—The Cloud Gateway Anti-Virus feature introduces an advanced malware scanning solution that compliments and extends the existing Gateway AV scanning mechanisms present on SonicWALL firewalls to counter the continued growth in the number of malware samples in the wild. Cloud Gateway Anti-Virus expands the Reassembly Free Deep Packet Inspection engine capabilities by consulting with the data center based malware analysis servers. This approach keeps the foundation of RFDPI-based malware detection by providing a low-latency, real-time solution that is capable of scanning unlimited numbers of files of unlimited size on all protocols that are presently supported without adding any significant incremental processing overhead to the appliances themselves. With this additional layer of security, SonicWALL's Next Generation Firewalls are able to extend their current protection to cover multiple millions of pieces of malware.

Release Notes

- **NTP Authentication Type**—When adding a Network Time Protocol server, the Add NTP Server dialog box provides a field to specify the NTP authentication type, such as MD5. Fields are also available to specify the trust key ID, the key number and the password.
- **Link Aggregation**—Link Aggregation provides the ability to group multiple Ethernet interfaces to form a trunk which looks and acts like a single physical interface. This feature is useful for high end deployments requiring more than 1 Gbps throughput for traffic flowing between two interfaces. This functionality is available on all NSA E-Class platforms.

Static Link Aggregation with the ability to aggregate up to 4 ports into a single link is supported on SonicOS 5.8. A round-robin algorithm is used for load balancing traffic across the interfaces in an aggregated link.
- **Port Redundancy**—Port Redundancy provides the ability to configure a redundant physical interface for any Ethernet interface in order to provide a failover path in case a link goes down. Port Redundancy is available on all NSA E-Class platforms.

When the primary interface is active, it handles all traffic from/to the interface. When the primary interface goes down, the backup interface takes over and handles all outgoing/incoming traffic. When the primary interface comes up again, it takes over all the traffic handling duties from the backup interface.

When Port Redundancy, High Availability and WAN Load Balancing are used together, Port Redundancy takes precedence followed by High Availability, then followed by WAN Load Balancing.
- **Content Filtering Enhancements**—The CFS enhancements provide policy management of network traffic based on Application usage, User activity, and Content type. Administrators can create multiple CFS policies per user group and set restrictive 'Bandwidth Management Policies' based on CFS categories.
- **IPFIX and NetFlow Reporting**—This feature enables administrators to gain visibility into traffic flows and volume through their networks, helping them with tracking, auditing and billing operations. This feature provides standards-based support for NetFlow Reporting, IPFIX, and IPFIX with extensions. The data exported through IPFIX with extensions contains information about network flows such as applications, users, and URLs extracted through Application Intelligence, along with standard attributes such as source/destination IP address (includes support for IPv6 networks), source/destination port, IP protocol, ingress/egress interface, sequence number, timestamp, number of bytes/packets, and more.
- **VLAN Support for TZ Series**—SonicOS 5.8 provides VLAN support for SonicWALL TZ 210/200/100 Series appliances, including wireless models. The TZ 210 and 200 Series support up to 10 VLANs, the TZ 100 Series supports up to 5 VLANs.
- **SonicPoint Virtual Access Point Support for TZ Series**—Virtual Access Points (VAPs) are supported when one or more SonicWALL SonicPoints are connected to a SonicWALL TZ 210/200/100 Series appliance. The TZ 210 and 200 Series support up to 8 VAPs, the TZ 100 Series supports up to 5 VAPs.
- **LDAP Primary Group Attribute**—To allow Domain Users to be used when configuring policies, membership of the Domain Users group can be looked up via an LDAP "Primary group" attribute. SonicOS 5.8.1.8 provides an attribute setting in the LDAP schema configuration for using this feature.
- **Preservation of Anti-Virus Exclusions After Upgrade**—SonicOS 5.8.1.8 includes the ability to detect if the starting IP address in an existing range configured for exclusion from anti-virus enforcement belongs to either LAN, WAN, DMZ or WLAN zones. After upgrading to a newer firmware version, SonicOS applies the IP range to a newly created address object. Detecting addresses for other zones not listed above, including custom zones, is not supported.

Anti-virus exclusions which existed before the upgrade and which apply to hosts residing in custom zones will not be detected. IP address ranges not falling into the supported zones will default to the LAN zone. Conversion to the LAN zone occurs during the restart process. There is no message in the SonicOS management interface at login time regarding the conversion.

Release Notes

- **Comprehensive Anti-Spam Service (CASS) 2.0**—The Comprehensive Anti-Spam Service (CASS) feature provides a quick, efficient, and effective way to add anti-spam, anti-phishing, and anti-virus capabilities to your SonicWALL security appliance. This feature increases the efficiency of your SonicWALL security appliance by providing you the ability to configure user view settings and filter junk messages before users see it in their inboxes. The following capabilities are available with CASS 2.0:
 - The Email Security Junk Store application can reside outside the Exchange Server system, such as on a remote server.
 - Dynamic discovery of Junk Store user interface pages feature allows the Junk Store to inform SonicOS of a list of pages to display under Anti-Spam in the SonicOS left hand navigation pane. For example, the pane might show Junk Box View, Junk Box Settings, Junk Summary, User View Setup, and/or Address Books.
 - User-defined Allow and Deny Lists can be configured with FQDN and Range address objects in addition to Host objects.
 - A GRID IP Check tool is available in the Anti-Spam > Status page. The SonicWALL administrator can specify (on-demand) an IP address to check against the SonicWALL GRID IP server. The result will either be LISTED or UNLISTED. Connections from a LISTED host will be blocked by the SonicWALL security appliance running CASS (unless overridden in the Allow List).
 - A parameter to specify the Probe Response Timeout is available in the Anti-Spam > Settings page Advanced Options section. This option supports deployment scenarios where a longer timeout is needed to prevent a target from frequently being marked as Unavailable. The default value is 30 seconds.
- **Enhanced Connection Limiting**—Connection Limiting enhancements expand the original Connection Limiting feature which provided global control of the number of connections for each IP address. This enhancement is designed to increase the granularity of this kind of control so that the SonicWALL administrator can configure connection limitation more flexibly. Connection Limiting uses Firewall Access Rules and Policies to allow the administrator to choose which IP address, which service, and which traffic direction when configuring connection limiting.
- **Dynamic WAN Scheduling**—SonicOS 5.8 supports scheduling to control when Dynamic WAN clients can connect. A Dynamic WAN client connects to the WAN interface and obtains an IP address with the PPPoE, L2TP, or PPTP. This enhancement allows the administrator to bind a schedule object to Dynamic WAN clients so that they can connect when the schedule allows it and they are disconnected at the end of the configured schedule. In the SonicOS management interface, a Schedule option is available on the WAN interface configuration screen when one of the above protocols is selected for IP Assignment. Once a schedule is applied, a log event is recorded upon start and stop of the schedule.
- **NTLM Authentication with Mozilla Browsers**—As an enhancement to Single Sign-On, SonicOS can now use NTLM authentication to identify users who are browsing using Mozilla-based browsers (including Internet Explorer, Firefox, Chrome and Safari). NTLM is part of a browser authentication suite known as “Integrated Windows Security” and should be supported by all Mozilla-based browsers. It allows a direct authentication request from the SonicWALL appliance to the browser with no SSO agent involvement. NTLM authentication works with browsers on Windows, Linux and Mac PCs, and provides a mechanism to achieve Single Sign-On with Linux and Mac PCs that are not able to interoperate with the SSO agent.
- **Single Sign-On Import Users from LDAP Option**—An **Import from LDAP** button on the Users > Local Users page allows you to configure local users on the SonicWALL by retrieving the user names from your LDAP server. This allows SonicWALL user privileges to be granted upon successful LDAP authentication. For ease of use, options are provided to reduce the list to a manageable size and then select the users to import.
- **SSL VPN NetExtender Update**—This enhancement supports password change capability for SSL VPN users, along with various fixes. When the password expires, the user is prompted to change it when logging in via the NetExtender client or SSL VPN portal. It is supported for both local users and remote users (RADIUS and LDAP).

Release Notes

- **DHCP Scalability Enhancements**—The DHCP server in SonicWALL appliances has been enhanced to provide between 2 to 4 times the number of leases previously supported. To enhance the security of the DHCP infrastructure, the SonicOS DHCP server now provides server side conflict detection to ensure that no other device on the network is using the assigned IP address. Conflict detection is performed asynchronously to avoid delays when obtaining an address.
- **SIP Application Layer Gateway Enhancements**—SIP operational and scalability enhancements are provided in SonicOS 5.8. The SIP feature-set remains equivalent to previous SonicOS releases, but provides drastically improved reliability and performance. The **SIP Settings** section under the **VoIP > Settings** page is unchanged. SIP ALG support has existed within SonicOS firmware since very early versions on legacy platforms. Changes to SIP ALG have been added over time to support optimized media between phones, SIP Back-to-Back User Agent (B2BUA), additional equipment vendors, and operation on a multi-core system. The SIP protocol is now in a position of business critical importance – protecting the voice infrastructure, including VoIP. To accommodate the demands of this modern voice infrastructure, SIP ALG enhancements include the following:
 - **SIP Endpoint Information Database** – The algorithm for maintaining the state information for known endpoints is redesigned to use a database for improved performance and scalability. Endpoint information is no longer tied to the user ID, allowing multiple user IDs to be associated with a single endpoint. Endpoint database access is flexible and efficient, with indexing by NAT policy as well as by endpoint IP address and port.
 - **Automatically Added SIP Endpoints** – User-configured endpoints are automatically added to the database based on user-configured NAT policies, providing improved performance and ensuring correct mappings, as these endpoints are pre-populated rather than “learnt.”
 - **SIP Call Database** – A call database for maintaining information about calls in progress is implemented, providing improved performance and scalability to allow SonicOS to handle a much greater number of simultaneous calls. Call database entries can be associated with multiple calls.
 - **B2BUA Support Enhancements** – SIP Back-to-Back User Agent support is more efficient with various algorithm improvements.
 - **Connection Cache Improvements** – Much of the data previously held in the connection cache is offloaded to either the endpoint database or the call database, resulting in more efficient data access and corollary performance increase.
 - **Graceful Shutdown** – Allows SIP Transformations to be disabled without requiring the firewall to be restarted or waiting for existing SIP endpoint and call state information to time out.
- **Management Traffic Only Option for Network Interfaces**—SonicOS 5.8.1.8 provides a **Management Traffic Only** option on the **Advanced** tab of the interface configuration window, when configuring an interface from the **Network > Interfaces** page. When selected, this option prioritizes all traffic arriving on that interface. The administrator should enable this option **ONLY** on interfaces intended to be used exclusively for management purposes. If this option is enabled on a regular interface, it will still prioritize the traffic, but that may not be the desired result. It is up to the administrator to limit the traffic to just management; the firmware does not have the ability to prevent pass-through traffic.

The purpose of this option is to provide the ability to access the SonicOS management interface even when the appliance is running at 100% utilization.
- **Auto-Configuration of URLs to Bypass User Authentication**—SonicOS 5.8.1.8 includes a new auto-configuration utility to temporarily allow traffic from a single, specified IP address to bypass authentication. The destinations that traffic accesses are then recorded and used to allow that traffic to bypass user authentication. Typically this is used to allow traffic such as anti-virus updates and Windows updates. To use this feature, navigate to **Users > Settings** and click the **Auto-configure** button in the Other Global User Settings section.

Release Notes

Known Issues

This section contains a list of known issues in the SonicOS 5.8.1.8 release.

Application Firewall

Symptom	Condition / Workaround	Issue
An App Firewall rule matching a source zone/network address object does not function properly.	Occurs when configuring an App Firewall rule to match a source zone/network address object.	120337

Content Filtering System

Symptom	Condition / Workaround	Issue
The YouTube for Schools feature is bypassed with iOS or Android wireless devices using the YouTube application.	Occurs when connecting an iOS or Android device to a wireless network that has YouTube for Schools filtering enabled. Use the YouTube application and see that all content is available for access.	121533

Security Services

Symptom	Condition / Workaround	Issue
Signature downloads fail for all three services (Gateway Anti-Virus, Intrusion Prevention, and Anti-Spyware), and the Signature Database status continually displays the message "download in progress".	Occurs when downloading signatures through a proxy server.	120386

Throughput

Symptom	Condition / Workaround	Issue
HTTP throughput performance may be reduced due to Deep Packet Inspection.	Occurs when the AppFlow Monitor is enabled.	119065

Wireless

Symptom	Condition / Workaround	Issue
The same SSID cannot be used on internal radio and VAP SonicPoints.	Occurs when setting the SSID on the internal radio, and then trying to create a VAP on the SonicPoint. A VAP is created when the SSID is set on the internal radio, therefore a VAP cannot be created on the SonicPoint with the same SSID because the SSID is used as the object name.	119621

Release Notes

Resolved Issues

The following issues were resolved in the SonicOS 5.8.1.8 release

Active-Active UTM

Symptom	Condition	Issue
The Active-Active UTM transaction for Application Firewall may not block the specified traffic after the first connection is established.	Occurs when deploying firewalls in an Active-Active UTM configuration with Application Firewall enabled.	112371

Application Firewall

Symptom	Condition	Issue
Signatures and categories may be randomly missing from the Application List Object field.	Occurs when navigating to Firewall > Match Objects > Add Application List Objects, and then adding signatures. After saving the changes, view the signatures and see that some are randomly missing.	118970
An App Rule is still active after it is disabled.	Occurs when creating an App Rule, and then disabling the "Enable App Rules" checkbox. Navigate to the Log > View page and see that App Rule is still blocking traffic.	100120

App Signatures

Symptom	Condition	Issue
Browsers using TLS v1.2 or TLS v1.1 are blocked from accessing HTTPS websites.	Occurs when navigating to a HTTPS website with App Control SID-6 prevention enabled.	117577
Some versions of UltraSurf are not blocked by the SonicOS Intrusion Prevention Service, although log messages state that the connection is blocked.	Occurs when UltraSurf 11.03 or 11.04 are being used to bypass the firewall policies	111716

Dashboard

Symptom	Condition	Issue
The Country list in the Geo-IP Filter page is blank after upgrading firmware.	Occurs when upgrading the firmware version, and then navigating to the Security Services > Geo-IP Filter page and viewing the Country list.	116258

DPI-SSL

Symptom	Condition	Issue
HTTPS websites in Internet Explorer may not be blocked by the CFS with DPI-SSL.	Occurs when using the CFS with DPI-SSL and accessing HTTPS websites that should be blocked by the CFS.	112288

Release Notes

Firmware

Symptom	Condition	Issue
WAN Failover may incorrectly trigger, causing an interrupted connection.	Occurs when the WAN Failover feature is enabled (this feature is enabled by default). The appliance triggers WAN Failover, then switches back to the primary WAN, even though the WAN interface never lost a physical connection.	113563

Gateway Anti-Virus

Symptom	Condition	Issue
A virus might not be detected by the Gateway Anti-Virus (GAV) feature.	Occurs when a firewall is configured in layer two bridge mode and GAV is activated.	114371
The Anti-Virus enforcement list is not correct after upgrading from SonicOS 5.6.0.x to 5.8.x.	Occurs when Kaspersky Anti-Virus is licensed on SonicOS 5.6.0.x, with AV enforcement enabled for the zone and an AV enforcement list configured on the Security Services page.	110845

GMS Firmware

Symptom	Condition	Issue
Cannot change the password for the Administrator account on a managed firewall.	Occurs when GMS is otherwise successfully managing the firewall running SonicOS 5.8.1.6 or 5.8.1.7.	117721

High Availability

Symptom	Condition	Issue
Traffic may not pass through the X1 interface.	Occurs when two appliances are configured as a High Availability Pair and the "Virtual MAC" checkbox is enabled. This issue only affects NSA 220, NSA 220W, NSA 250M, and NSA 250MW appliances with serial numbers beginning in "C0EAE4".	113169
WAN failover and failback can cause Internet connectivity problems.	Occurs when using WAN load balancing and probing fails on a NAT static IP address using ICMP or TCP for probing.	112783

IDP

Symptom	Condition	Issue
A user may be able to download TCP encrypted torrent files.	Occurs when using P2P Bittorrent signatures to block torrent file downloads.	115367

Release Notes

Log

Symptom	Condition	Issue
No user name is generated by the firewall in some syslog messages for connections from a terminal server. ViewPoint reporting therefore does not include the user names.	Occurs when syslog messages are sent for traffic from a terminal server after users connect to it, but before the user identification information for the connection is received from the TS agent.	89488

N2H2 and Websense CFS

Symptom	Condition	Issue
Web traffic throughput may decrease if Websense is enabled.	Occurs when web traffic passes through the firewall and the Websense feature is enabled.	113157

Networking

Symptom	Condition	Issue
The secondary WAN interface does not send a DHCP request after a loss of connectivity.	Occurs when configuring a secondary WAN interface and setting it to use DHCP.	119628
The Oracle control session succeeds and the server provides redirection information to the client machine, but the Oracle data packet may not be forwarded by the firewall.	Occurs when Network Address Translation (NAT) is enabled.	118920
The Open Shortest Path First (OSPF) feature is not sending the default route as part of the routing update.	Occurs when running two firewalls with one of them connected to a PPPoE WAN, and then selecting "Originate Default Route When WAN is UP" on the firewall connected to the PPPoE WAN.	117181
The connection to an Oracle server may become interrupted a few seconds after the initial connection is established.	Occurs when running an Oracle server behind the firewall and selecting the "Enable Support for Oracle (SQLNet)" checkbox.	115316
Large numbers of TCP connections are dropped, including inbound, outbound or between internal interfaces. Log entries claim the cache is full but the number of connections is not close to the actual maximum number of connections. The CPU Utilization stays at 100% for hours.	Occurs when the Local Collector is used on the Log > Flow Control page, in a small number of high-traffic customer networks.	113622
Sub-interfaces only display the interface IP and not the entire subnet.	Occurs when the sub-interface has Passive enabled and the main OSPF interface has Redistribute disabled.	112594
SonicPoint-ni may be detected as a spoofed device on the WLAN.	Occurs when connecting a SonicPoint-ni to the firewall's WLAN and then enabling all the checkboxes for MAC-IP Spoof settings. Check the Spoof Detection list and see that the SonicPoint-ni is sometimes listed.	101981
Some web pages may not load properly with Web Proxy Forwarding enabled.	Occurs when enabling the Web Proxy Forwarding feature, and then navigating to a web page.	89863

Release Notes

System

Symptom	Condition	Issue
After adding a VLAN interface, the firewall stops forwarding interesting, allowed traffic.	Occurs when a VLAN sub-interface is added; occurs on two different NSA 4500 appliances. Packets are dropped due to an enforced firewall rule.	114206
A Tech Support Report (TSR) does not download using HTTPS.	Occurs when logging in to the management interface using HTTPS, and then attempting to download a TSR.	113716

Users

Symptom	Condition	Issue
The User Configuration page does not display some of the tabs and lists correctly.	Occurs when creating a user or editing a user's properties.	115216
Custom login policies might not save correctly.	Occurs when navigating to the Users > Settings page, and then changing the custom login policy settings.	110562

User Interface

Symptom	Condition	Issue
A JavaScript error is sometimes displayed when editing DHCP settings.	Occurs when editing a DHCP option group or when editing interface settings and changing the DHCP scope.	110087

UTM – SSL VPN

Symptom	Condition / Workaround	Issue
Bookmarks and internal SonicPoint SSH management Java applets display warning messages about the certificate expiration date.	Occurs when accessing the Java Control Panel > Java Preferences page and checking the SonicWALL certificates.	120375

VPN

Symptom	Condition	Issue
The firewall shows an additional active VPN tunnel for the original local network, in addition to the expected ones for the translated local network.	Occurs when establishing a site-to-site VPN with Network Address Translation (NAT) to a remote device.	113571

Wireless

Symptom	Condition	Issue
A SonicPoint status may regularly display as "Non-Responsive", or appliances with internal wireless may exhibit reduced performance when wireless radio is enabled.	Occurs when managing a SonicPoint appliance with, or using the internal wireless radio on a SonicWALL network security appliance running SonicOS 5.8.1.7 or earlier.	115934

Release Notes

Upgrading SonicOS Image Procedures

The following procedures are for upgrading an existing SonicOS image to a newer version:

<i>Obtaining the Latest SonicOS Image Version</i>	29
<i>Saving a Backup Copy of Your Configuration Preferences</i>	29
<i>Upgrading a SonicOS Image with Current Preferences</i>	30
<i>Importing Preferences to SonicOS 5.8</i>	30
<i>Importing Preferences from SonicOS Standard to SonicOS 5.8 Enhanced</i>	31
<i>Support Matrix for Importing Preferences</i>	32
<i>Upgrading a SonicOS Image with Factory Defaults</i>	33
<i>Using SafeMode to Upgrade Firmware</i>	33

Obtaining the Latest SonicOS Image Version

To obtain a new SonicOS firmware image file for your SonicWALL security appliance:

1. Connect to your mysonicwall.com account at <http://www.mysonicwall.com>.
2. Copy the new SonicOS image file to a directory on your management station.

You can update the SonicOS image on a SonicWALL security appliance remotely if the LAN interface or the WAN interface is configured for management access.

Saving a Backup Copy of Your Configuration Preferences

Before beginning the update process, make a system backup of your SonicWALL security appliance configuration settings. The backup feature saves a copy of your current configuration settings on your SonicWALL security appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state.

In addition to using the backup feature to save your current configuration settings to the SonicWALL security appliance, you can export the configuration preferences file to a directory on your local management station. This file serves as an external backup of the configuration preferences, and can be imported back into the SonicWALL security appliance.

Perform the following steps to save a backup of your configuration settings and export them to a file on your local management station:

1. On the System > Settings page, click **Create Backup**. Your configuration preferences are saved. The System Backup entry is displayed in the Firmware Management table.
2. To export your settings to a local file, click **Export Settings**. A popup window displays the name of the saved file.
3. On the System > Diagnostics page, under Tech Support Report, select the following checkboxes and then click the **Download Report** button:
 - VPN Keys
 - ARP Cache
 - DHCP Bindings
 - IKE Info
 - SonicPointN Diagnostics
 - Current users
 - Detail of users

The information is saved to a "techSupport_" file on your management computer.

Release Notes

Upgrading a SonicOS Image with Current Preferences

Perform the following steps to upload new firmware to your SonicWALL appliance and use your current configuration settings upon startup:

1. Download the SonicOS firmware image file from mysonicwall.com and save it to a location on your local computer.
2. On the System > Settings page, click **Upload New Firmware**.
3. Browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**.
4. On the System > Settings page, click the **Boot** icon in the row for **Uploaded Firmware**.
5. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the login page.
6. Enter your user name and password. Your new SonicOS image version information is listed on the **System > Settings** page.

Importing Preferences to SonicOS 5.8

Preferences importing to the SonicWALL network security appliances is generally supported from the following SonicWALL appliances running SonicOS:

- NSA Series
- NSA E-Class Series
- TZ 210/200/100/190/180/170 Series
- PRO Series

There are certain exceptions to preferences importing on these appliances running the SonicOS 5.8 release. Preferences cannot be imported in the following cases:

- Settings files containing Portshield interfaces created prior to SonicOS 5.x
- Settings files containing VLAN interfaces are not accepted by the TZ 100/200 Series firewalls
- Settings files from a PRO 5060 with optical fiber interfaces where VLAN interfaces have been created

Full support for preferences importing from these appliances is targeted for a future release. At that time, you will need to upgrade your firmware to the latest SonicOS maintenance release available on MySonicWALL.

Release Notes

Importing Preferences from SonicOS Standard to SonicOS 5.8 Enhanced

The SonicOS Standard to Enhanced Settings Converter is designed to convert a source Standard Network Settings file to be compatible with a target SonicOS Enhanced appliance. Due to the more advanced nature of SonicOS Enhanced, its Network Settings file is more complex than the one SonicOS Standard uses. They are not compatible. The Settings Converter creates an entirely new target Enhanced Network Settings file based on the network settings found in the source Standard file. This allows for a rapid upgrade from a Standard deployment to an Enhanced one with no time wasted in re-creating network policies. **Note:** SonicWALL recommends deploying the converted target Network Settings file in a testing environment first and always keeping a backup copy of the original source Network Settings file.

The SonicOS Standard to Enhanced Settings Converter is available at:

<https://convert.global.sonicwall.com/>

If the preferences conversion fails, email your SonicOS Standard configuration file to settings_converter@sonicwall.com with a short description of the problem. In this case, you may also consider manually configuring your SonicWALL appliance.

To convert a Standard Network Settings file to an Enhanced one:

1. Log in to the management interface of your SonicOS Standard appliance, navigate to **System > Settings**, and save your network settings to a file on your management computer.
2. On the management computer, point your browser to <https://convert.global.sonicwall.com/>.
3. Click the **Settings Converter** button.
4. Log in using your MySonicWALL credentials and agree to the security statement.
The source Standard Network Setting file must be uploaded to MySonicWALL as part of the conversion process. The Setting Conversion tool uses MySonicWALL authentication to secure private network settings. Users should be aware that SonicWALL will retain a copy of their network settings after the conversion process is complete.
5. Upload the source Standard Network Settings file:
 - Click **Browse**.
 - Navigate to and select the source SonicOS Standard Settings file.
 - Click **Upload**.
 - Click the right arrow to proceed.
6. Review the source SonicOS Standard Settings Summary page.
This page displays useful network settings information contained in the uploaded source Network Settings file. For testing purposes, the LAN IP and subnet mask of the appliance can be changed on this page in order to deploy it in a testing environment.
 - (Optional) Change the LAN IP address and subnet mask of the source appliance to that of the target appliance.
 - Click the right arrow to proceed.
7. Select the target SonicWALL appliance for the Enhanced deployment from the available list.
SonicOS Enhanced is configured differently on various SonicWALL appliances, mostly to support different interface numbers. As such, the converted Enhanced Network Settings file must be customized to the appliance targeted for deployment.
8. Complete the conversion by clicking the right arrow to proceed.
9. Optionally click the **Warnings** link to view any differences in the settings created for the target appliance.
10. Click the **Download** button, select Save to Disk, and click OK to save the new target SonicOS Enhanced Network Settings file to your management computer.
11. Log in to the management interface for your SonicWALL appliance.
12. Navigate to **System > Settings**, and click the **Import Settings** button to import the converted settings to your appliance.

Release Notes

Support Matrix for Importing Preferences

		DESTINATION FIREWALLS																																						
		TZ100/	TZ100w/																	PRO	PRO	PRO	PRO	PRO	PRO	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA
		TZ200	TZ200w	TZ210	TZ210w	TZ170	TZ170w	TZ170SP	TZ170SPw	TZ180	TZ180w	TZ190	TZ190w	1260	2040	3060	4060	4100	5060	220	220W	240	250M	250MW	2400	3500	4500	5000	E5500	E6500	E7500	E8500	E8510							
S	TZ100/TZ200	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
O	TZ100w/TZ200w	C	✓	C	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
U	TZ 210	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
R	TZ 210W	✓	✓	C	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
C	TZ 170	B,D	B,D	B,D	B,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
E	TZ 170W	B,C,D	B,D	B,C,D	B,D	C	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
	TZ 170SP	B,C,D	B,C,D	B,C,D	B,D	C	C	✓	✓	C	C	C	C	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
F	TZ 170SPW	C,D	B,C,D	B,C,D	B,D	C	C	✓	✓	C	C	C	C	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
I	TZ 180	C,D	C,D	C,D	C,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
R	TZ 180W	C,D	C,D	C,D	C,D	C	✓	✓	✓	C	✓	C	✓	C	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
E	TZ 190	C,D	C,D	C,D	C,D	C	C	✓	✓	C	C	✓	✓	C	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
W	TZ 190W	C,D	C,D	C,D	C,D	C	C	✓	✓	C	✓	C	✓	C	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
A	PRO 1260	B,D	B,D	B,D	B,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				
L	PRO 2040	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				
L	PRO 3060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				
S	PRO 4060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				
	PRO 4100	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				
	PRO 5060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				
	NSA 220	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
	NSA 220W	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
	NSA 240	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
	NSA 250M	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
	NSA 250MW	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
	NSA 2400	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
	NSA 3500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
	NSA 4500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
	NSA 5000	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
	NSA E5500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
	NSA E6500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
	NSA E7500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
	NSA E8500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				
	NSA E8510	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗				

Notes:

- A - When VLANs are present, the settings file will not be accepted.
- B - Portshield interfaces prior to SonicOS 5.x are not supported.
- C - Configuration information from extra interfaces will be removed. NAT policies, Firewall access rules, and other interface-dependent configuration will also be removed.
- D - When importing from non-SonicOS 5.x devices, the X2 interface will be configured in the DMZ zone.
- E - VLANs created as sub-interfaces of the fiber interfaces will be renamed.

✓	Supported
✗	Unsupported. While importing the settings file may be successful, firewall limitations may result in the removal of items such as DHCP scopes, VPN settings, etc.

Release Notes

Upgrading a SonicOS Image with Factory Defaults

Perform the following steps to upload new firmware to your SonicWALL appliance and start it up using the default configuration:

1. Download the SonicOS firmware image file from mysonicwall.com and save it to a location on your local computer.
2. On the System > Settings page, click **Create Backup**.
3. Click **Upload New Firmware**.
4. Browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**.
5. On the System > Settings page, click the **Boot** icon in the row for **Uploaded Firmware with Factory Default Settings**.
6. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the Setup Wizard, with a link to the login page.
7. Enter the default user name and password (admin / password) to access the SonicWALL management interface.

Using SafeMode to Upgrade Firmware


The SafeMode procedure uses a reset button in a small pinhole, whose location varies: on the NSA models, the button is near the USB ports on the front; on the TZ models, the button is next to the power cord on the back. If you are unable to connect to the SonicWALL security appliance's management interface, you can restart the SonicWALL security appliance in SafeMode. The SafeMode feature allows you to quickly recover from uncertain configuration states with a simplified management interface that includes the same settings available on the System > Settings page.

To use SafeMode to upgrade firmware on the SonicWALL security appliance, perform the following steps:

1. Connect your computer to the X0 port on the SonicWALL appliance and configure your IP address with an address on the 192.168.168.0/24 subnet, such as 192.168.168.20.
2. Do one of the following to restart the appliance in SafeMode:
 - Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the front of the security appliance for more than 20 seconds.
 - Use the LCD control buttons on the front bezel to set the appliance to Safe Mode. Once selected, the LCD displays a confirmation prompt. Select **Y** and press the **Right** button to confirm. The SonicWALL security appliance changes to SafeMode.

The **Test** light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.

Note: *Holding the reset button for two seconds will send a diagnostic snapshot to the console. Holding the reset button for six to eight seconds will reboot the appliance in regular mode.*

3. Point the Web browser on your computer to **192.168.168.168**. The SafeMode management interface displays.
4. If you have made any configuration changes to the security appliance, select the **Create Backup On Next Boot** checkbox to make a backup copy of your current settings. Your settings will be saved when the appliance restarts.
5. Click **Upload New Firmware**, and then browse to the location where you saved the SonicOS firmware image, select the file, and click **Upload**.
6. Select the boot icon  in the row for one of the following:
 - **Uploaded Firmware – New!**
Use this option to restart the appliance with your current configuration settings.
 - **Uploaded Firmware with Factory Defaults – New!**
Use this option to restart the appliance with default configuration settings.
7. In the confirmation dialog box, click **OK** to proceed.
8. After successfully booting the firmware, the login screen is displayed. If you booted with factory default settings, enter the default user name and password (admin / password) to access the SonicWALL management interface.

Release Notes

Related Technical Documentation

SonicWALL user guides and reference documentation is available at the 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 SonicWALL Product Support website. The top navigation bar includes the Dell logo, SonicWALL logo, and links for Products, Solutions, How to Buy, Support, Sign In, and Register. A search bar is located on the right. The main content area is titled "Product Support" and features a banner for "E-Class NSA Series Appliances" with an image of the hardware. Below the banner are tabs for "Support Documents" and "Knowledge Base". The left sidebar contains a "Support" menu with various categories like Overview, Product Documentation, Network Security, and NSA E-Class Series. The main content area is divided into three sections: "List View Options" with filter checkboxes for Video Tutorials, Product Guides, Technical Notes, FAQs, Release Notes, and Support Data Sheets; "Product Guides" with a list of 6 items including "SonicOS Enhanced 5.5 Layer 2 Bridge Bypass Feature Module" and "SonicOS 5.8.1 Rev E Administrator's Guide"; and "Technical Notes" with a list of 6 items including "Using a Windows Enterprise Root CA with DPI-SSL" and "Integrating Agilink with SonicOS 5.8.1.5".

Last updated: 9/17/2012