

Release Notes

Contents

<i>Platform Compatibility</i>	1
<i>Browser Support</i>	2
<i>Supported Features</i>	2
<i>Enhancements in SonicOS 5.8.1.12</i>	6
<i>Key Features in SonicOS 5.8</i>	10
<i>Known Issues</i>	42
<i>Resolved Issues</i>	45
<i>Upgrading SonicOS Image Procedures</i>	47
<i>Related Technical Documentation</i>	53

Platform Compatibility

The SonicOS 5.8.1.12 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 5.8.1.12. 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 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 16.0 and higher
- Internet Explorer 8.0, 9.0, and 10.0 (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 shows SonicOS 5.8 feature support by model and lists features that are affected by 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
WAN Acceleration (WXA 1.2)	Supported	Supported	Supported	Supported	Supported
YouTube for Schools	Supported	Supported	Supported	Supported	Supported
IKEv2	Supported	Supported	Supported	Supported	Supported
Wireless Client Bridge Support			Supported	Supported	Supported
Real-Time Monitor	Supported	Supported	Supported		
AppFlow Monitor	Supported	Supported	Supported		
AppFlow Dash	Supported	Supported	Supported		
AppFlow Reports	Supported	Supported	Supported		
Packet Monitor Enhancements	Supported	Supported	Supported	Supported	Supported
AppFlow > Flow Reporting	Supported	Supported	Supported		

Release Notes

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 210 Series	TZ 200 Series	TZ 100 Series
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		
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
App Control Policy Configuration via App Flow	Supported	Supported	Supported	Supported	Supported

Release Notes

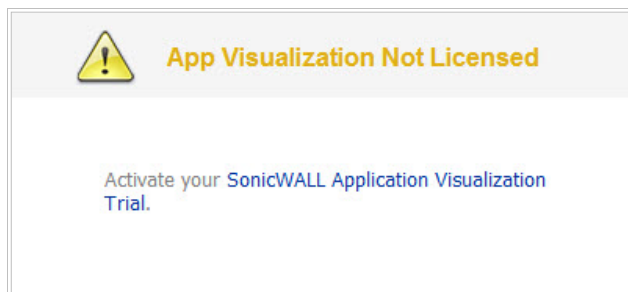
Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 210 Series	TZ 200 Series	TZ 100 Series
Monitor					
Global BWM Ease of Use Enhancements	Supported	Supported	Supported	Supported	Supported
Application Usage and Risk Report	Supported	Supported	Supported		
Geo-IP Filtering and Botnet Command & Control 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:

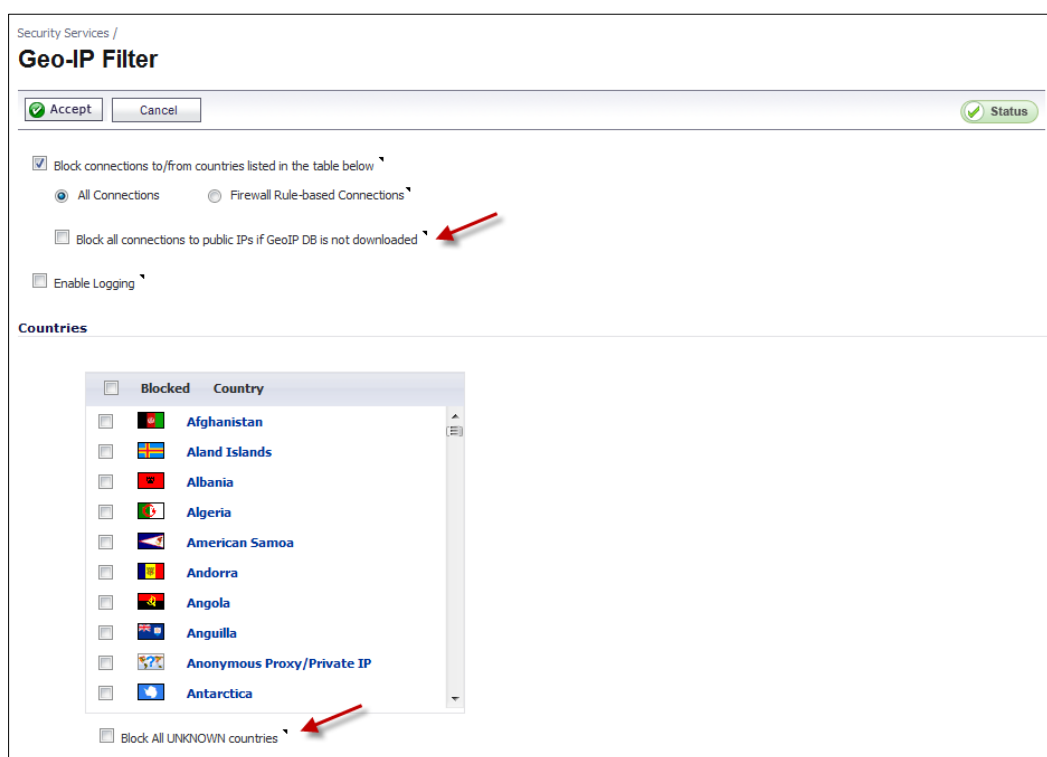
SonicOS Feature	No license (SGSS)	With license Disabled in flow reporting	With license and enabled in flow reporting
Dashboard > Real-Time Monitor	Blocks the page with a license popup window.	All charts are independently enabled or disabled from the AppFlow > Flow Reporting page. It is not dependent 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/Dash/Reports	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.
AppFlow > Flow Reporting	Available and displays a statement that App Visualization is not licensed.	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 Comprehensive Gateway Security Suite (CGSS).	Available	Available

Release Notes

Enhancements in SonicOS 5.8.1.12

This section describes the enhancements in the SonicOS 5.8.1.12 release:

- **Security Services > Geo-IP Filter** — The **Security Services > Geo-IP Filter** page has two new checkbox options:
 - **Block all connections to public IPs if GeoIP DB is not downloaded**
Select this option if you want all countries to be blocked whenever the firewall cannot download the Geo-IP database that contains the list of countries to be blocked. For selected countries to be blocked, the Geo-IP database must be downloaded from the internet. The firewall must be able to resolve the address "gbdata.global.sonicwall.com" to download the country database. If the Geo-IP database is not downloaded successfully, the firewall cannot block selected countries.
 - **Block ALL UNKNOWN countries**
Some countries may not be listed in the Geo-IP database. Select this option if you want all countries not listed in the Geo-IP database to be blocked.



Release Notes

- **Security Services > Botnet Filter** — The **Security Services > Botnet Filter** page has a new checkbox option:
 - **Block all connections to public IPs if BOTNET DB is not downloaded**
Select this option if you want all public IP addresses to be blocked whenever the firewall cannot download the Botnet database that contains the list of Botnet IP addresses to be blocked. For selected IP addresses to be blocked, the Botnet database must be downloaded from the internet. If the Botnet database is not downloaded successfully, the firewall cannot block Botnet IP addresses.

Security Services /
Botnet Filter

Accept Cancel Status

Block connections to/from Botnet Command and Control Servers [^]
 All Connections Firewall Rule-based Connections [^]

Block all connections to public IPs if BOTNET DB is not downloaded [^]

Enable Logging [^]

Botnet Exclusion Object:
Default Geo-IP and Botnet Exclusion Group [^]

Diagnostics

Botnet Cache Statistics	
Location Server IP:	173.240.214.190
Resolved Entries:	52
Unresolved Entries:	0
Current Entry Count:	52
Max. Entry Count:	50000
Location Map Count:	253

Release Notes

- **AppFlow > Flow Reporting** — The information on the **AppFlow > Flow Reporting** page has been divided into three new tabs:
 - Statistics
 - Settings
 - External Collector

The **Statistics** section is shown below.

AppFlow /
Flow Reporting

Accept Cancel Clear Default flow Download

Statistics Settings External Collector

External Flow Reporting Statistics	
Connection Flows Enqueued:	0
Connection Flows Dequeued:	0
Connection Flows Dropped:	0
Connection Flows Skipped Reporting:	0
Non-Connection data Enqueued:	5063
Non-Connection data Dequeued:	5063
Non-connection data Dropped:	0
Non-connection related static data Reported:	0

Internal AppFlow Reporting Statistics	
Data Flows Enqueued:	172260
Data Flows Dequeued:	172260
Data Flows Dropped:	0
Data Flows Skipped Reporting:	0
General Flows Enqueued:	5063
General Flows Dequeued:	5063
General Flows Dropped:	0
General Static Flows Dequeued:	333840
AppFlow Collector Errors:	0
Total Flows in DB:	8183

Total IPFIX Statistics	
Total NetFlow/IPFIX Packets Sent:	0
NetFlow/IPFIX Packets Sent to External Collector:	0
Netflow/IPFIX Templates sent:	0
Connection Flows Sent to External Collector:	0

Total IPFIX Statistics	
Non-Connection related Dynamic Flows Sent to External Collector:	0
Non-Connection related Static Flows Sent to External Collector:	0

Release Notes

The **Settings** section is shown below.

The screenshot shows the 'AppFlow / Flow Reporting' interface. At the top, there are buttons for 'Accept', 'Cancel', 'Clear', and 'Default'. Below these are three tabs: 'Statistics', 'Settings', and 'External Collector'. The 'Settings' tab is active, displaying a list of configuration options:

- Report Connections:** Radio buttons for 'All' (selected), 'Interface-based', and 'Firewall/App Rules-based'.
- Enable Real-Time Data Collection:** Checked checkbox.
- Collect Real-Time Data For:** Dropdown menu with 'Top apps, Bits per sec., Packets per sec., Average packet size, Connections per'.
- Enable Aggregate AppFlow Report Data Collection:** Checked checkbox.
- Collect Report Data For:** Dropdown menu with 'Apps Report, User Report, IP Report, Threat Report, Geo-IP Report, URL Report'.
- Local Server Settings:**
 - Enable AppFlow To Local Collector [*]:** Checked checkbox.
- Other Report Settings:**
 - Report DROPPED Connection:** Checked checkbox.
 - Skip Reporting STACK Connections:** Unchecked checkbox.
 - Include Following URL Types:** Dropdown menu with 'Gifs, Jpegs, Pngs, Htmis, Aspx'.
 - Enable Geo-IP Resolution:** Checked checkbox.
 - AppFlow Report Upload Timeout (sec):** Text input field with '30'.

The **Enable Domain Resolution** option and the **Enable Domain Resolution for Private IPs** option have been removed from the Settings section.

The **External Collector Settings** section is shown below.

The screenshot shows the 'AppFlow / Flow Reporting' interface with the 'External Collector' tab selected. The 'External Collector Settings' section is expanded, showing the following configuration options:

- Send Flows and Real-Time Data To External Collector [*]:** Unchecked checkbox.
- External Flow Reporting Format:** Dropdown menu with 'Netflow version-5'.
- External Collector's IP address:** Text input field with '0.0.0.0'.
- Source IP To Use For Collector On A VPN tunnel:** Text input field with '0.0.0.0'.
- External Collector's LDP Port Number:** Text input field with '2055'.
- Send IPFIX/Netflow Templates At Regular Interval:** Unchecked checkbox.
- Send Static AppFlow At Regular Interval:** Unchecked checkbox.
- Send Static AppFlow For Following Tables:** Dropdown menu with 'Applications, Viruses, Spyware, Intrusions, Services, Rating Map'.
- Send Dynamic AppFlow For Following Tables:** Dropdown menu with 'Connections, Users, URLs, URL ratings, VPNs, VCIPIs'.
- Include Following Additional Reports via IPFIX:** Empty dropdown menu.
- Report On Connection OPEN:** Checked checkbox.
- Report On Connection CLOSE:** Checked checkbox.
- Report Connection On Active Timeout:** Unchecked checkbox, with 'Number Of Seconds' set to '60'.
- Report Connection On Kilo BYTES Exchanged:** Unchecked checkbox, with 'Kilobytes Exchanged' set to '100' and a 'Report ONCE' checkbox.
- Report Connections On Following Updates:** Dropdown menu with 'threat detection, application detection, user detection, VPN tunnel detection'.

Release Notes

Key Features in SonicOS 5.8

The following are the key features in SonicOS 5.8:

- **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. It has the following fields and controls:

- Object Name:** CFS Allow YT4S
- Match Object Type:** CFS Allow/Forbidden List
- Match Type:** Partial Match
- Input Representation:** Alphanumeric (selected), Hexadecimal
- Content:** youtube.com
- List:** youtube.com, yting.com
- Buttons:** Add, Update, Remove, Remove All, Load From File
- Status:** Ready
- Footer Buttons:** OK, Cancel, 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 "yting.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: ufiGb16ejHSRXqXnnnK2Jg

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

Release Notes

not to exclude you (select the **Do not bypass CFS blocking for the Administrator** checkbox on the **Security Services > Content Filter** page).

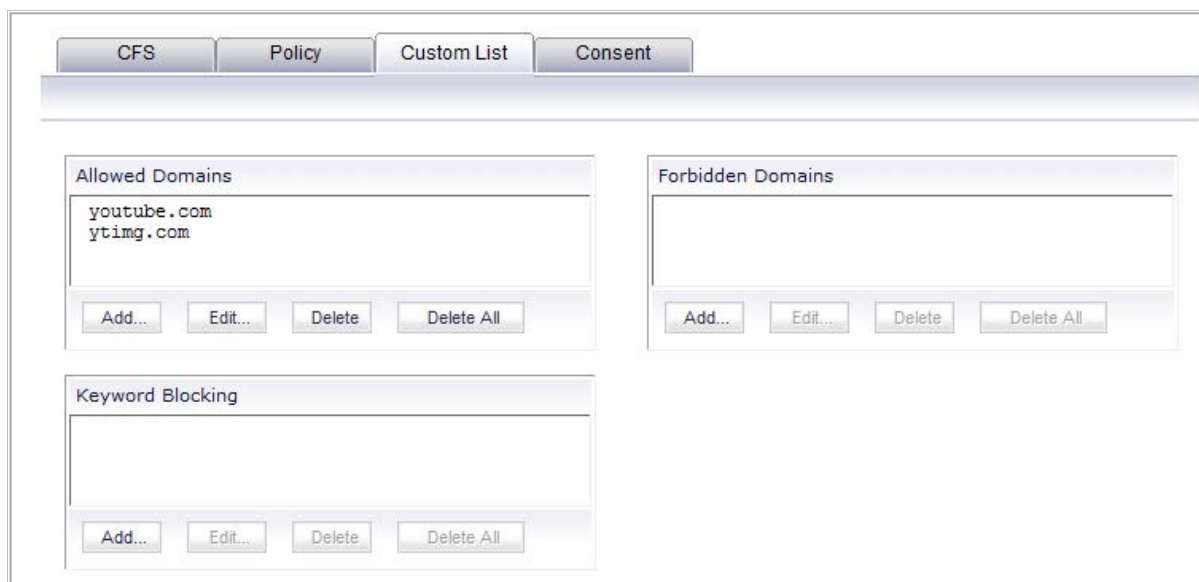
- When the **CFS Policy Assignment** pulldown menu is set to **Via User and Zone Screens**, YouTube for Schools is configured as part of the Content Filter policy.
 1. On the **Security Services > Content Filter** page, select **Content Filter Service** for the **Content Filter Type** pulldown menu.
 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 'Custom List' configuration page. It features three dropdown menus for 'Source of Allowed Domains', 'Source of Forbidden Domains', and 'Source of Keyword', all set to 'Global'. Below these is the 'Safe Search Enforcement Settings' section with an unchecked checkbox for 'Enable Safe Search Enforcement'. The 'YouTube for Schools' section is highlighted with a red box and contains a checked checkbox for 'Enable YouTube for Schools' and a text field for 'School ID' containing the value 'Lj3Q2GVaHbr3k_yiY2lhkQ'. At the bottom, the 'Filter Forbidden URLs by time of day' section has a dropdown menu 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**.



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).

- **IKEv2 Support** — Beginning in SonicOS 5.8.1.8, Internet Key Exchange version 2 (IKEv2) is the default proposal type for new Site-to-Site VPN policies when clicking the Add button from the VPN > Settings screen. IKEv2 is a protocol for negotiating and establishing a security association (SA). IKEv2 provides improved security and a simplified architecture. Compared to IKEv1 Main Mode, using IKEv2 greatly reduces the number of message exchanges needed to establish an SA, while IKEv2 is more secure and flexible than IKEv1 Aggressive Mode. This reduces the delays during re-keying. IPsec Secondary Gateway is supported with IKEv2. DHCP over VPN is not supported with IKEv2. IKEv2 is not compatible with IKEv1. When IKEv2 is used, all nodes in the VPN must use IKEv2 to establish the tunnels. IKEv2 has the following advantages over IKEv1:
 - More secure
 - More reliable
 - Simpler
 - Faster
 - Extensible
 - Fewer message exchanges to establish connections
 - EAP Authentication support
 - MOBIKE support
 - Built-in NAT traversal
 - Keep Alive is enabled as default

Release Notes

- **4G/3G Support** — SonicOS 5.8.1.11 and higher supports the following additional 4G and 3G devices:
 - AT&T Momentum U313 LTE USB (4G)
 - D-Link DWM 156 HSPA USB (3G)

Note: The user should update the 3G/4G device firmware on a PC prior to use, to ensure that it has the most current vendor firmware.
- **SNMP for VLAN Interfaces** — In SonicOS 5.8.1.11 and higher, SNMP MIB-II statistic counters are supported for VLAN interfaces.
- **SonicOS Web-based Management Interface**— HTTP access to the SonicOS web-based management interface is disabled by default. When running SonicOS with 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 **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

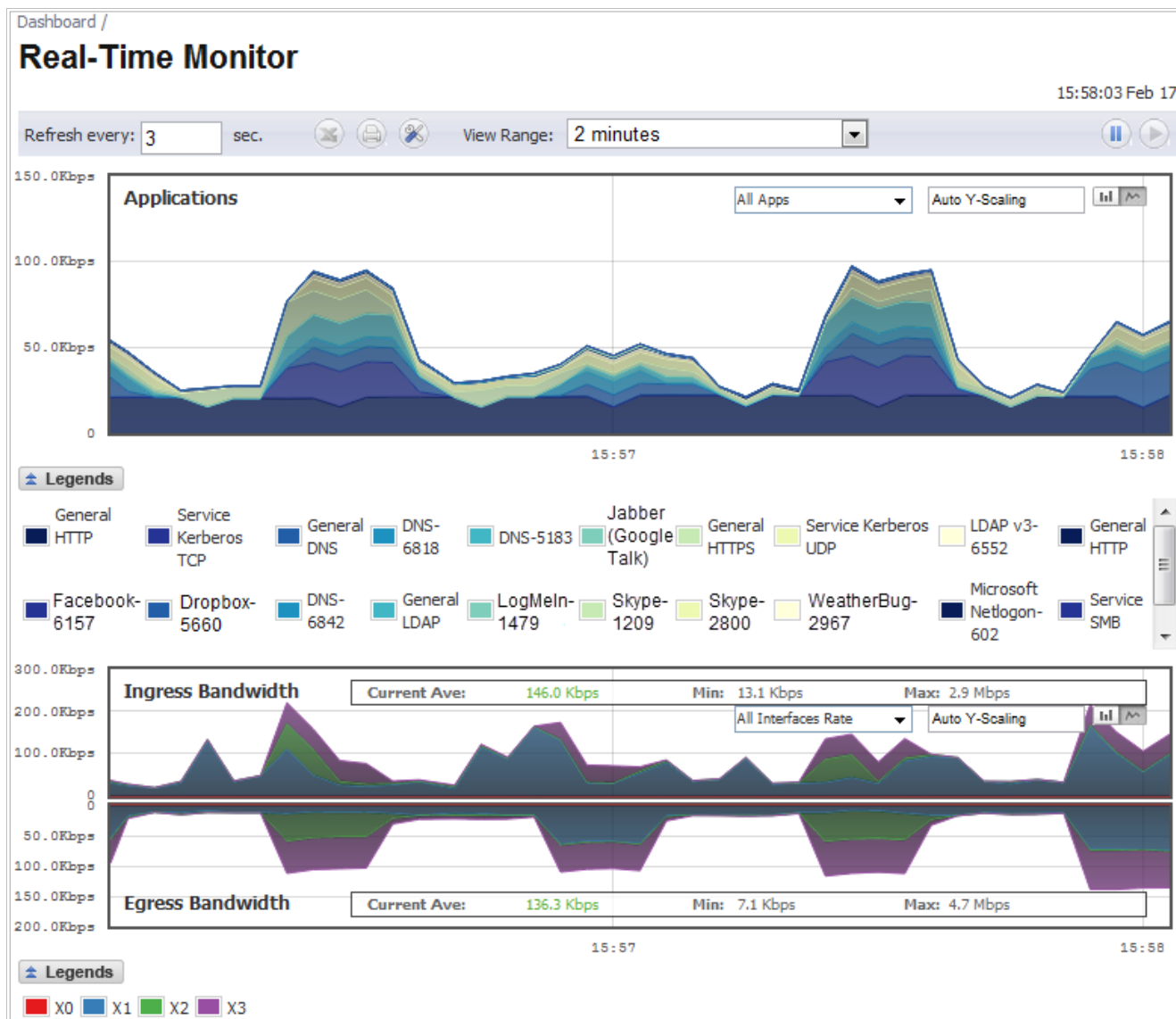
Form Tooltip Delay: in msec

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 5.8.1.12 receive an automatic 30-day free trial for App Visualization upon registration.

SonicWALL appliances upgrading from a pre-SonicOS 5.8 release **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.

To populate the Real-Time Monitor with data, navigate to the **AppFlow > 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.

Release Notes

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

Settings

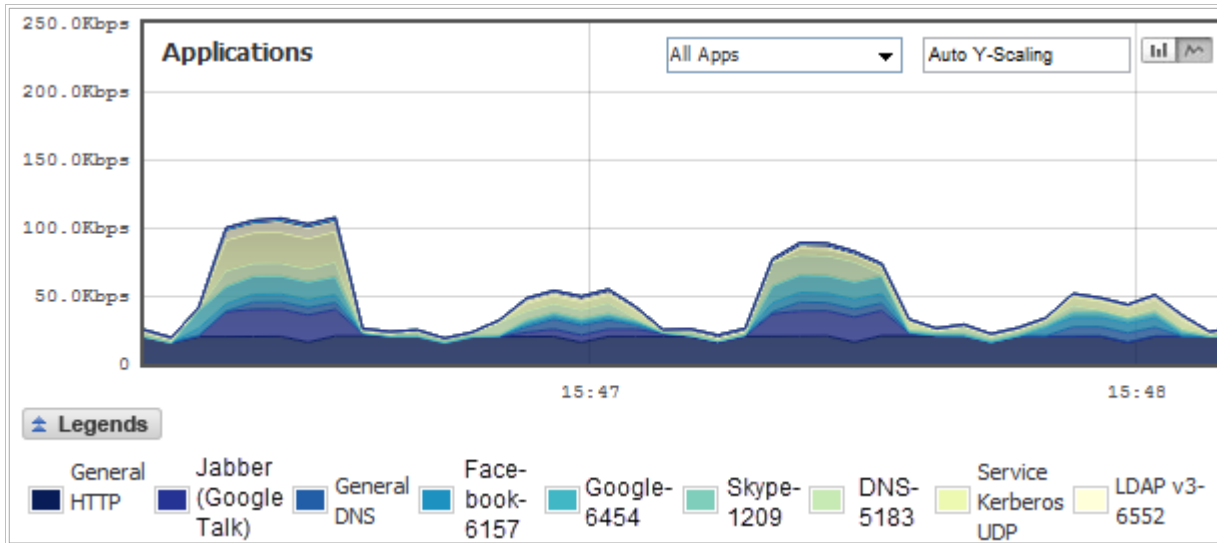
Enable AppFlow To Local Collector[*]


Enable Real-Time Data Collection

Collect Real-Time Data For 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).

Use Gradient

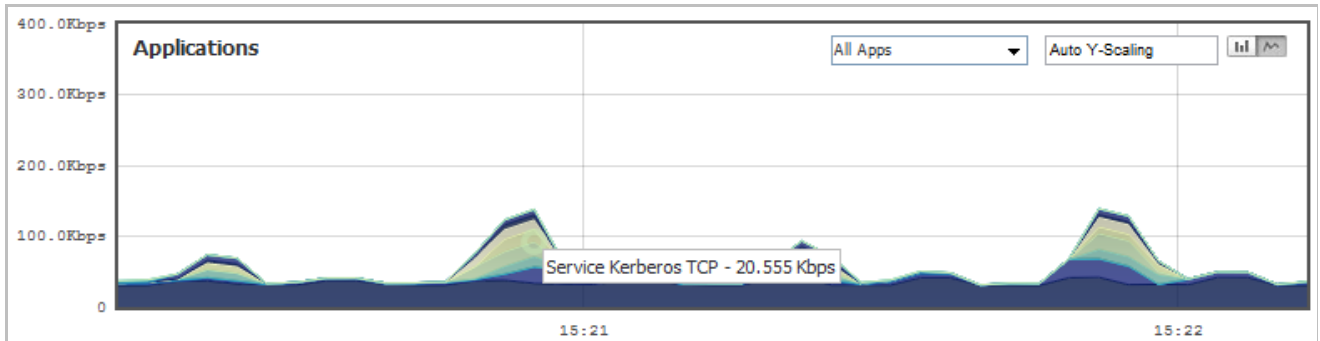
Put legends inside Application Chart

Put legends inside Bandwidth Chart

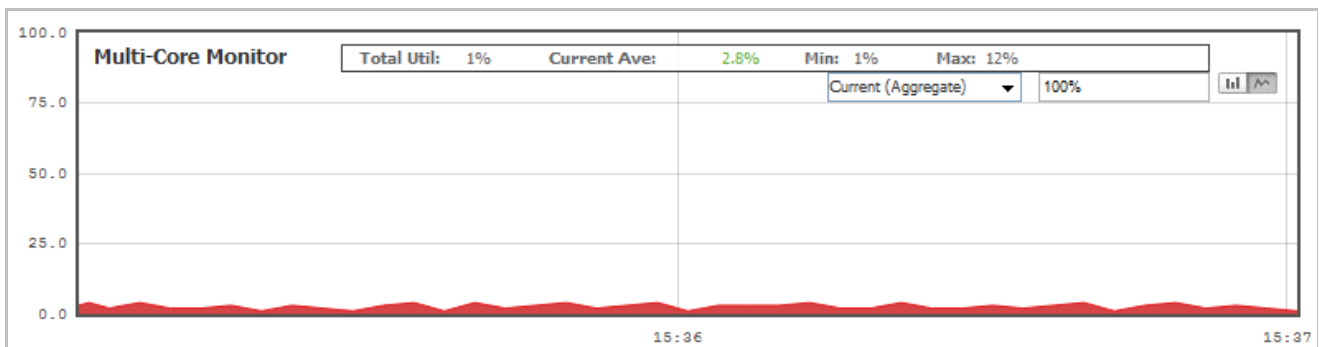
Default Generate Cancel Save

Release Notes

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

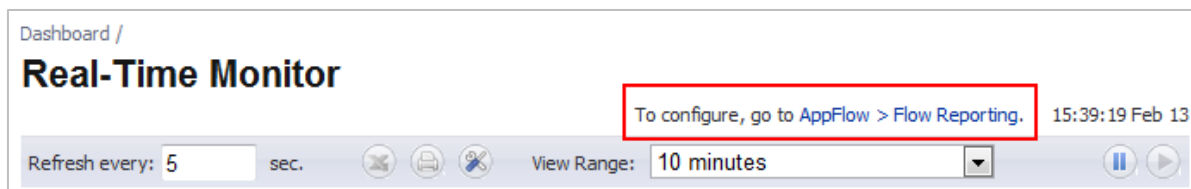


By default, the Multi-Core Monitor displays as a stack chart, rather than as a bar graph, to easily show its relation to the other charts on this screen.

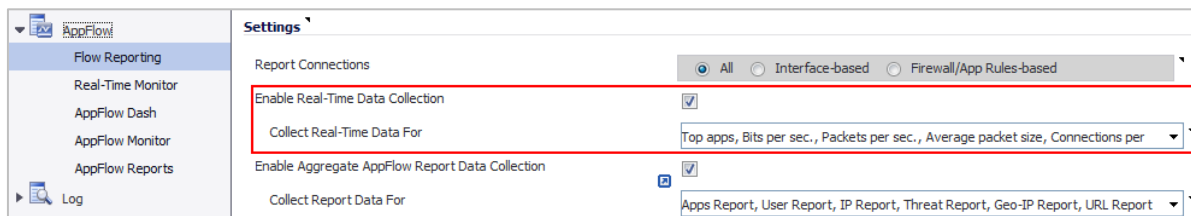


Note: The Multi-Core Monitor only shows the processor load for the cores of the managing firewall. If operating in Active-Active DPI mode, the core load for the standby firewall does not display.

Link to Flow Reporting — The **Dashboard > Real-Time Monitor** page provides a link to the **AppFlow > Flow Reporting** page, where you can enable/disable each chart in the Real-Time Monitor page.

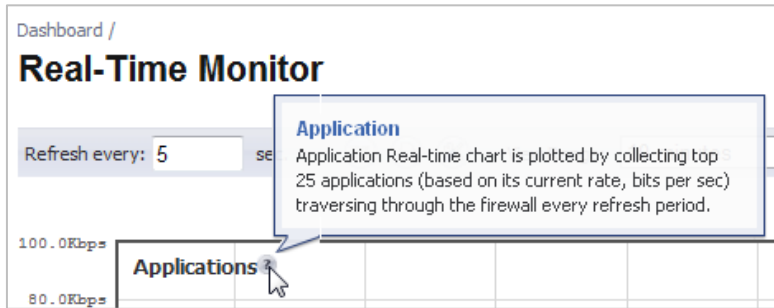


To enable/disable each chart in the Real-Time Monitor page, use the **Enable Real-Time Data Collection** option and associated drop-down list.

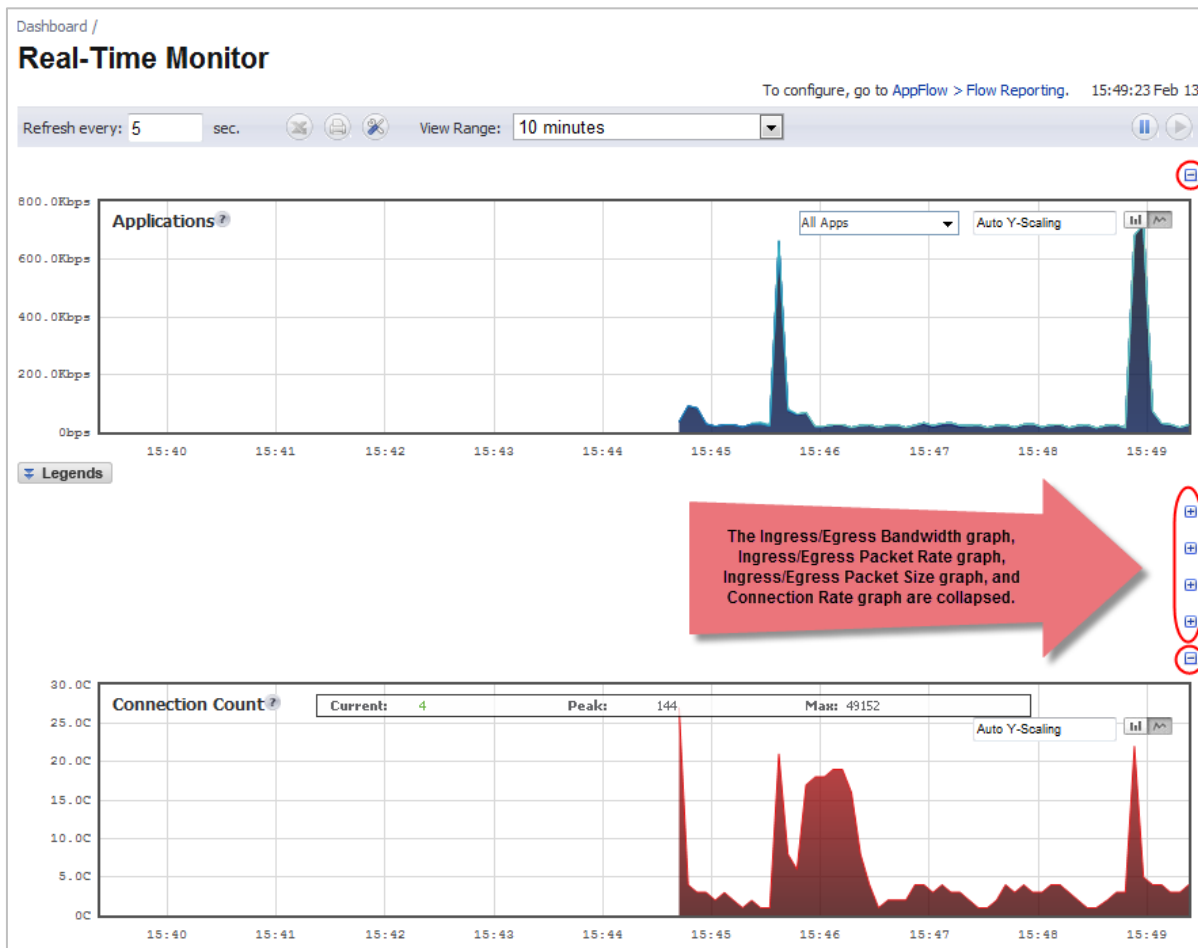


Release Notes

Real-Time Monitor Tooltips — The **Dashboard > Real-Time Monitor** page provides a tooltip with useful information next to each chart title.

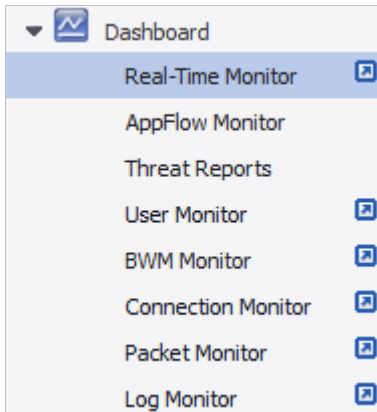


Real-Time Monitor Collapse/Expand Options — The **Dashboard > Real-Time Monitor** page provides a collapse/expand button for each chart. This allows the administrator to juxtapose two charts for comparison, even if they are normally far apart on the page.

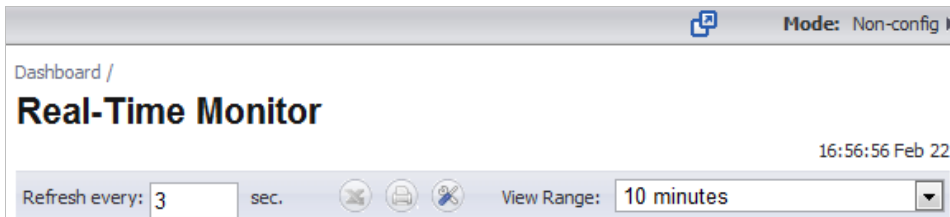


Release Notes

- **Standalone Dashboard Page** — 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:



Release Notes

- **AppFlow > Flow Reporting** — The **AppFlow > Flow Reporting** page provides the information previously displayed in the **Log > Flow Reporting** page, such as detailed external and internal flow statistics. In SonicOS 5.8.1.11 and higher, the **Log > Flow Reporting** page is removed, and its elements are now displayed in the **AppFlow > Flow Reporting** page.

More sections have been added to this page, and some elements have been rearranged and placed under one of the three tabs.

External Flow Reporting Statistics	
Connection Flows Enqueued:	0
Connection Flows Dequeued:	0
Connection Flows Skipped Reporting:	0
Non-Connection data Enqueued:	42
Non-Connection data Dequeued:	42
Non-connection data Dropped:	0
Non-connection related static data Reported:	0

Internal AppFlow Reporting Statistics	
Data Flows Enqueued:	64337
Data Flows Dequeued:	64337
Data Flows Dropped:	0
Data Flows Skipped Reporting:	0
General Flows Enqueued:	42
General Flows Dequeued:	42
General Flows Dropped:	0
General Static Flows Dequeued:	135723
AppFlow Collector Errors:	0
Total Flows in DB:	11519

Total IPFIX Statistics	
Total NetFlow/IPFIX Packets Sent:	0
NetFlow/IPFIX Packets Sent to External Collector:	0
Netflow/IPFIX Templates sent:	0
Connection Flows Sent to External Collector:	0

Total IPFIX Statistics	
Non-Connection related Dynamic Flows Sent to External Collector:	0
Non-Connection related Static Flows Sent to External Collector:	0

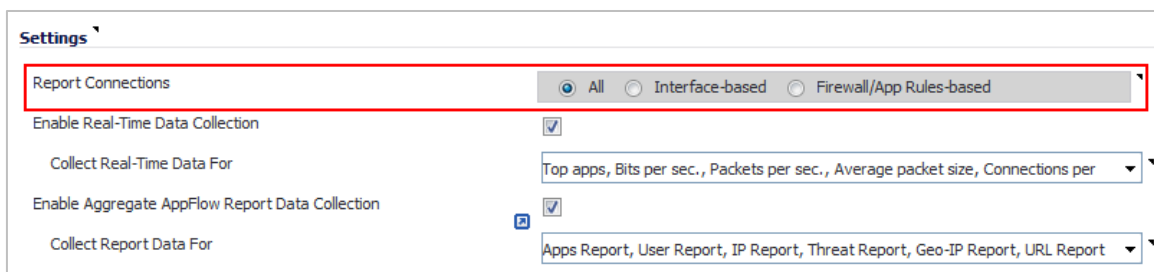
The **AppFlow** menu in the left navigation pane contains five pages. The lower four **AppFlow** pages display the corresponding **Dashboard** pages of the same names.

- AppFlow
 - Flow Reporting
 - Real-Time Monitor
 - AppFlow Dash
 - AppFlow Monitor
 - AppFlow Reports

A number of enhancements have been added to the **AppFlow** and **Dashboard** pages.

Release Notes

The options from the previous **Connection Report Settings** section are merged into the **External Collector Settings** section, except for the **Report Connections** option which is moved to the **Settings** section of the **AppFlow > Flow Reporting** page.



Settings

Report Connections: All Interface-based Firewall/App Rules-based

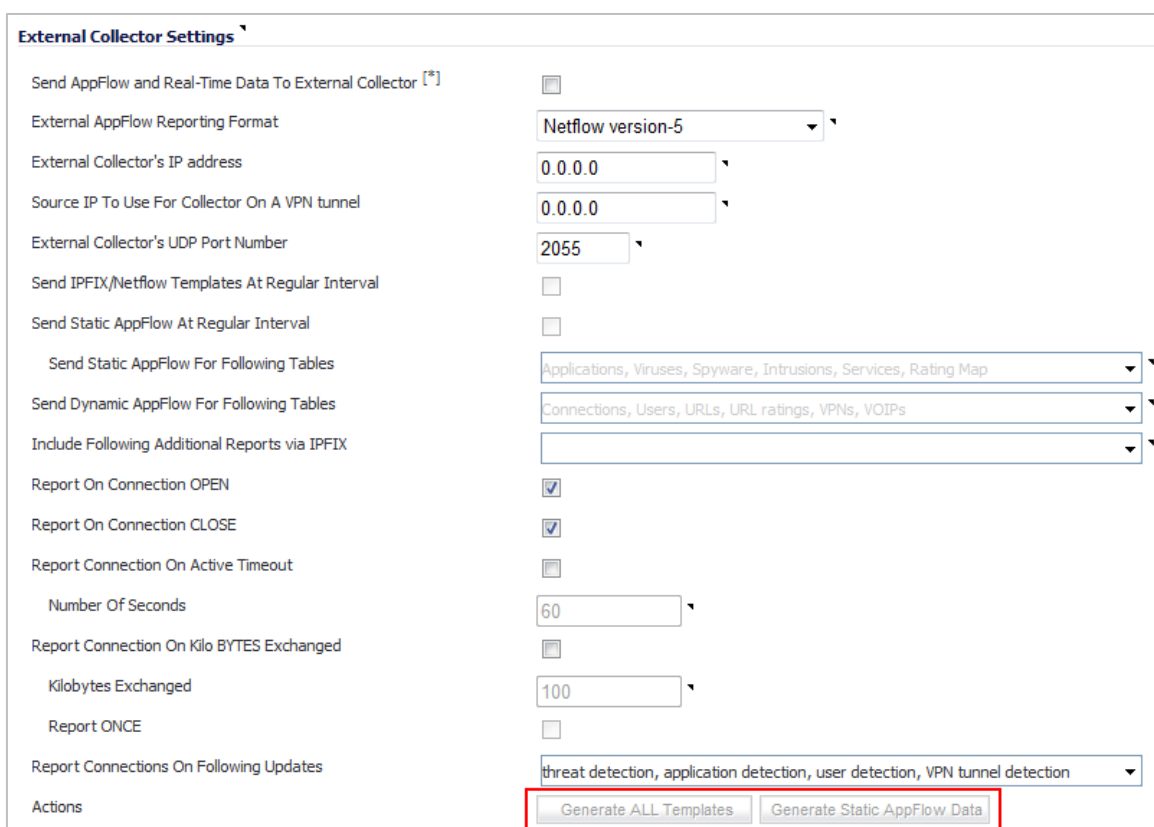
Enable Real-Time Data Collection:

Collect Real-Time Data For: Top apps, Bits per sec., Packets per sec., Average packet size, Connections per

Enable Aggregate AppFlow Report Data Collection:

Collect Report Data For: Apps Report, User Report, IP Report, Threat Report, Geo-IP Report, URL Report

The former **Generate All Templates** and **Generate Static AppFlow Data** buttons, which were at the top of the **Log > Flow Reporting** page, have been moved to the **Actions** option at the bottom of the **External Collector Settings** section of the page.



External Collector Settings

Send AppFlow and Real-Time Data To External Collector [*]:

External AppFlow Reporting Format: Netflow version-5

External Collector's IP address: 0.0.0.0

Source IP To Use For Collector On A VPN tunnel: 0.0.0.0

External Collector's UDP Port Number: 2055

Send IPFIX/Netflow Templates At Regular Interval:

Send Static AppFlow At Regular Interval:

Send Static AppFlow For Following Tables: Applications, Viruses, Spyware, Intrusions, Services, Rating Map

Send Dynamic AppFlow For Following Tables: Connections, Users, URLs, URL ratings, VPNs, VOIPs

Include Following Additional Reports via IPFIX:

Report On Connection OPEN:

Report On Connection CLOSE:

Report Connection On Active Timeout:

Number Of Seconds: 60

Report Connection On Kilo BYTES Exchanged:

Kilobytes Exchanged: 100

Report ONCE:

Report Connections On Following Updates: threat detection, application detection, user detection, VPN tunnel detection

Actions:

The **Settings** area provides options to control the reporting content by interface or rules, to control which graphs to display on the **Real-Time Monitor** page, and to control which graphs to display on the **AppFlow Monitor** page. The **Settings** area has an **Enable Aggregate AppFlow Report Data Collection** option and associated **Collect Report Data For** drop-down list. This allows the administrator to select the specific report types to be included in AppFlow reports. The functionality is very similar to the control over the Real-Time Monitor charts provided by the **Enable Real-Time Data Collection** option and drop-down list, also in the **Settings** section.

Release Notes

The **Local Server Settings** section provides the **Enable AppFlow to Local Collector** option. The **External Collector Settings** section provides a number of options for configuring an external collector.

The screenshot shows the 'Settings' page with several sections. The 'Local Server Settings' section includes the option 'Enable AppFlow To Local Collector' which is checked. The 'External Collector Settings' section includes 'Send AppFlow and Real-Time Data To External Collector' (checked), 'External AppFlow Reporting Format', and 'External Collector's IP address'. A red box highlights the 'Enable Aggregate AppFlow Report Data Collection' option in the 'Settings' section, which is checked. Below it, a dropdown menu is open, showing 'Collect Report Data For' with options: 'Apps Report, User Report, IP Report, Threat Report, Geo-IP Report, URL Report'. A second red box highlights this dropdown menu, which also shows a list of checked report types: 'Apps Report', 'User Report', 'IP Report', 'Threat Report', 'Geo-IP Report', and 'URL Report'.

The **Enable AppFlow to Local Collector** option, which was in the **Settings** section of the **Log > Flow Reporting** page, is moved to the **Local Server Settings** section.

The screenshot shows the 'Local Server Settings' section with the option 'Enable AppFlow To Local Collector' checked.

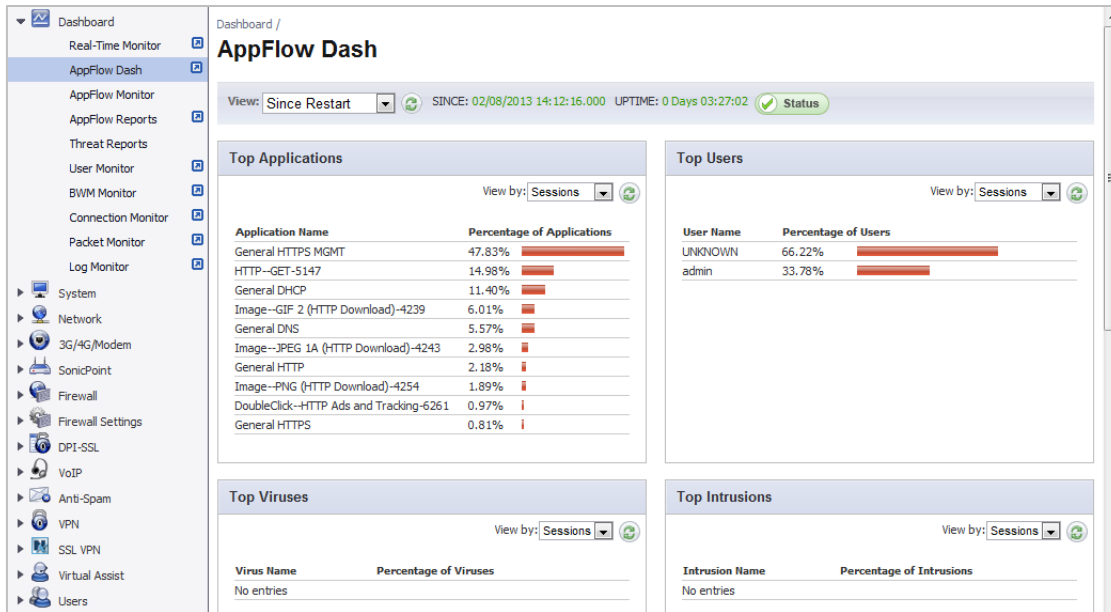
The **Other Report Settings** section near the bottom of the page provides additional settings for how connections are reported.

The screenshot shows the 'Other Report Settings' section. It includes options for 'Report DROPPED Connection' (checked), 'Skip Reporting STACK Connections' (checked), and 'Include Following URL Types' (Gifs, Jpegs, Pngs, Htmls, Aspx). A red box highlights the 'Enable Geo-IP Resolution' (unchecked), 'Enable Domain Resolution' (unchecked), 'Enable Domain Resolution for Private IPs' (unchecked), and 'AppFlow Report Upload Timeout (sec)' (30) options.

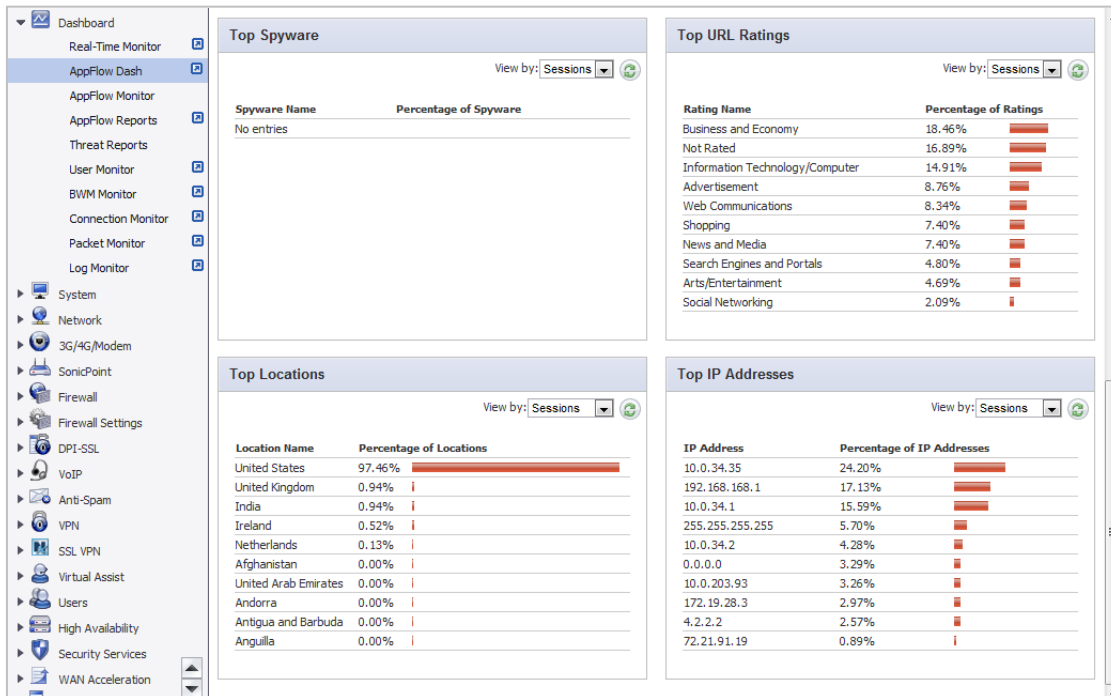
- **Enable Geo-IP Resolution**— AppFlow Monitor groups flows based on country under initiator and responder tabs.
- **Enable Domain Resolution**— AppFlow Monitor groups flows based on domain under initiator and responder tabs.
- **Enable Domain Resolution for Private IPs**—AppFlow Monitor groups flows based on the domain for private IPs in initiator and responder tabs. If the DNS server is public, this checkbox should be disabled. **Enable Domain Resolution** must be selected when this option is enabled. If Geo-IP blocking or Botnet blocking is enabled, then this checkbox is ignored.
- **AppFlow Report Upload Timeout (sec)**—Specifies the timeout in seconds when connecting to the AppFlow upload server. The minimum value is 5, the maximum is 120, and the default is 30.

Release Notes

- **Dashboard > AppFlow Dash** — The **Dashboard > AppFlow Dash** page provides graphs for Top Applications, Top Users, Top Viruses, Top Intrusions, Top Spyware, Top URL Ratings, Top Locations, and Top IP Addresses that are tracked with AppFlow. The top four graphs from the **AppFlow Dash** page are shown below:



The bottom four graphs from the **AppFlow Dash** page are shown below:



Release Notes

- **Dashboard > AppFlow 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
<input type="checkbox"/>	Dropbox	3	91	50,046	0.817	0
<input type="checkbox"/>	Service Kerberos TCP	7	76	21,168	2.953	0
<input type="checkbox"/>	BitTorrent/uTorrent	186	186	16,678	-	0
<input type="checkbox"/>	DNS	8	98	9,167	1.071	0
<input type="checkbox"/>	HTTP	4	142	7,482	0.970	0
<input type="checkbox"/>	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

The **Dashboard > AppFlow Monitor** page has several updates for enhanced usability.

- **AppFlow Monitor Filter**— A **Filter** text box provide a way to enter a text string to use for filtering the displayed information.

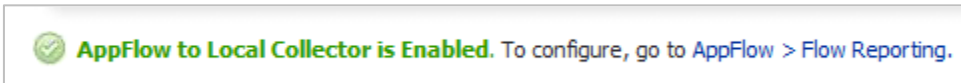
The screenshot shows the 'AppFlow Monitor' dashboard. At the top right, there is a 'Load Filter:' dropdown menu. Below it, a 'Filter View' button is visible. A text input field labeled 'Filter:' is highlighted with a red rectangular box. Below the filter field, there are several tabs: 'Applications', 'Users', 'URLs', 'Initiators', 'Responders', 'Threats', 'VoIP', 'VPN', 'Devices', and 'Contents'. The 'Applications' tab is currently selected. Below the tabs, there are controls for 'Create Rule', 'Filter View', 'Interval' (set to 'Last 60 seconds'), and 'Group' (set to 'Application'). At the bottom, a table displays application data with columns for '#', 'Application', 'Sessions', 'Total Packets', 'Total Bytes', and 'Ave Rate (KBps)'. The table contains three rows of data.

The **Filter** field is used to search for specific values in the main column, similar to this function on the **Dashboard > AppFlow Reports** page. The main column is the column to the right of the number (#) column, and its contents change depending on which tab is selected. For example, when the **Applications** tab is selected, you can filter on text strings that appear in the **Application** column.

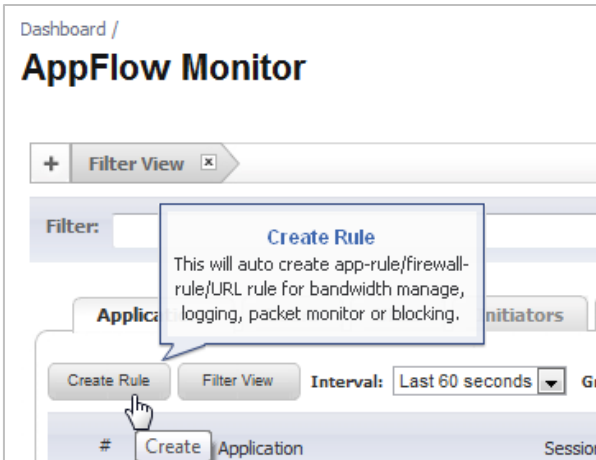
If another tab is selected, the main column changes accordingly and the search values would be different.

Release Notes

- **Link to AppFlow > Flow Reporting** — A link to the **AppFlow > Flow Reporting** page is provided at the bottom of the **Dashboard > AppFlow Monitor** page.



- **Local Collector Status** — A green or red status line at the bottom of the **Dashboard > AppFlow Monitor** page shows whether AppFlow to Local Collector is enabled (green) or disabled (red).
- **Tooltips** — Additional tooltips are available on the **Dashboard > AppFlow Monitor** page for the Create Rule button, Filter View button, and other elements.



- **Numbering and Auto-Scrolling** — Numbering is added in the left-most column of each table on the **Dashboard > AppFlow Monitor** page, along with an auto-scroll feature, which automatically loads more rows as you scroll down. This allows you to keep track of where you are in the list while scrolling down, and avoids delays from loading large amounts of data at once. The total number of items is always displayed.

#	Responder	Sessions	Total Packets	Total Bytes	Ave Rate (KBps)
76	223.165.26.46	2	105	82.44K	-
77	74.125.224.44	8	246	79.15K	-
78	69.171.224.42	5	197	78.82K	-
79	69.172.216.56	11	168	77.20K	-
80	23.21.208.110	6	168	76.21K	-
81	216.36.248.222	8	138	75.63K	-
82	67.195.146.230	1	86	75.07K	-
83	69.171.237.40	3	186	73.44K	-
84	69.171.234.34	4	188	71.14K	-
85	206.160.170.26	5	231	69.39K	-
86	65.54.87.125	1	95	69.09K	-
87	23.11.15.139	3	120	68.44K	-
Total:		372 item(s)	9.09K	129.13K	94.94M

Release Notes

- **Dashboard > AppFlow Reports** — The **Dashboard > AppFlow Reports** page provides aggregate AppFlow reports for the following cases:
 - Since the last firewall restart
 - Since the last reset of the counter; administrators can reset the counter manually
 - Scheduled reports; administrators can set a start and end time for data to be collected, and can configure the reports to be sent either via email or to an FTP server once the period ends. This is done via scheduled objects.

Dashboard / AppFlow Reports

Filter String:

Applications Users IP Viruses Intrusions Spyware Location Botnets URL Rating

Views: Since Restart (selected), Since Last Reset, On Schedule. Limit: 50. SINCE: 02/08/2013 14:12:16.000 UPTIME: 0 Days 03:33:49. Status: Enabled.

#	Name	Sessions	Inlet Bytes	Resp Bytes	Access Rules Block	App Rules Block	Location Block	BotNet Block	Viruses	Intrusions	Spyware
1	General HTTPS MGMT	4.71K	14.37M	17.82M	27%	0	0	0	0	0	0
2	HTTP--GET-5147	1.44K	2.72M	11.10M	17%	0	3	3	0	0	0
3	General DHCP	1.13K	358.84K	0	<1%	1,133	0	0	0	0	0
4	Image--GIF 2 (HTTP Download)-4239	579	2.75M	3.10M	4%	0	2	2	0	0	0
5	General DNS	539	57.82K	79.11K	<1%	0	0	0	0	0	0
6	Image--JPEG 1A (HTTP Download)-4243	287	961.32K	9.71M	14%	0	0	0	0	0	0
7	General HTTP	210	75.26K	450.60K	<1%	0	24	24	0	0	0
8	Image--PNG (HTTP Download)-4254	182	497.65K	5.60M	8%	0	0	0	0	0	0
9	DoubleClick--HTTP Ads and Tracks	93	217.42K	379.15K	<1%	0	0	0	0	0	0
Total: 50 item(s)		9.74K	23.55M	61.26M	1.13K	29	29	0	0	0	0

up time: 0 Days 03:34:57 last update: 17:46:01 Feb 08

Aggregate AppFlow reporting is enabled. Apps Reporting is enabled. To configure, go to AppFlow > Flow Reporting.

Release Notes

The **Filter String** field at the top of the page is used to search for specific values in the main column. The main column is the column to the right of the number (#) column, and its contents change depending on which tab is selected. For example, when the **Applications** tab is selected, you can filter on text strings that appear in the **Name** column:

Dashboard / AppFlow Reports

Filter String: google

Applications Users IP Viruses Intrusions Spyware Location Botnets URL Rating

View: Since Restart Limit: 50 SINCE: 02/08/2013 14:12:16.000 UPTIME: 0 Days 03:40:36 Status

#	Name	Sessions	Init Bytes	Resp Bytes	Access Rules Block	App Rules Block	Location Block	BotNet Block	Viruses	Intrusions	Spyware	
1	Google-SSL Any Google Domain 2-9379	14	<1%	29.51K	<1%	164.14K	<1%	0	0	0	0	0
2	Google Analytics-HTTP 2-2226	7	<1%	56.66K	<1%	1.17M	1%	0	0	0	0	0
3	Google Safe Browsing-Traffic 1-707	7	<1%	12.64K	<1%	7.14K	<1%	0	0	0	0	0
4	Google Safe Browsing-Traffic 2-708	7	<1%	17.20K	<1%	42.62K	<1%	0	0	0	0	0
5	Google Analytics-HTTP 4-7885	2	<1%	18.65K	<1%	372.66K	<1%	0	0	0	0	0

When the **IP** tab is selected, the contents in the **Filter String** box are cleared, and you can enter an appropriate value to search for in the **IP Address** column:

Dashboard / AppFlow Reports

Filter String: 206

Applications Users IP Viruses Intrusions Spyware Location Botnets URL Rating

View: Since Restart Limit: 50 SINCE: 02/08/2013 14:12:16.000 UPTIME: 0 Days 03:47:57 Status

#	IP Address	Sessions	Bytes Rcvd	Bytes Sent	Blocked	Virus	Spyware	Intrusion		
1	206.160.170.43	164	<1%	281.81K	<1%	997.03K	1%	0	0	0
2	206.160.170.35	45	<1%	252.74K	<1%	857.58K	<1%	0	0	0
3	206.160.170.11	44	<1%	235.43K	<1%	1.86M	2%	0	0	0
4	206.160.170.18	38	<1%	78.22K	<1%	522.68K	<1%	0	0	0
5	206.160.170.16	37	<1%	223.99K	<1%	3.82M	4%	0	0	0
6	206.191.168.170	35	<1%	120.67K	<1%	110.67K	<1%	0	0	0

Release Notes

- **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.

The screenshot shows the 'Advanced' tab of the configuration interface for 'Interface 'X2''. The settings are as follows:

Setting	Value
Zone:	LAN
Mode / IP Assignment:	Wire Mode (2-Port Wire)
Wire Mode Setting:	Inspect Mode (Passive DPI)
Restrict analysis at resource limit:	<input checked="" type="checkbox"/>
Paired Interface:	-- Select an Interface --

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:

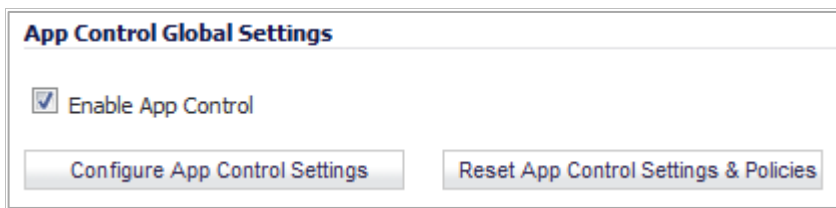
- Blocking signature-matching **Applications**, which are notoriously dangerous and difficult to enforce
- Viewing the real-time network activity of trusted **Users and User Groups** and guest services
- Matching **Content-rated categories**

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 5.8.1 and higher receive an automatic 30-day free trial for App Control upon registration.

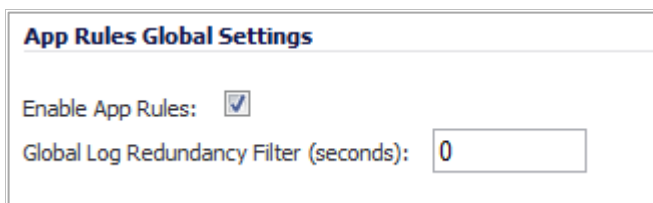
SonicWALL appliances upgrading from a pre-SonicOS 5.8 release **and** already licensed for GAV/IPS/AS, Total Secure, or Comprehensive Gateway Security Suite (CGSS) automatically receive a complimentary App Control license, required for creating Application Control policies.

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



The screenshot shows the 'App Control Global Settings' interface. It features a checkbox labeled 'Enable App Control' which is checked. Below the checkbox are two buttons: 'Configure App Control Settings' and '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.



The screenshot shows the 'App Rules Global Settings' interface. It features a checkbox labeled 'Enable App Rules' which is checked. Below it is a text input field labeled 'Global Log Redundancy Filter (seconds):' with the value '0' entered.

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

Firewall Settings /

BWM

Accept Cancel

Bandwidth Management Type: WAN Global None

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**.

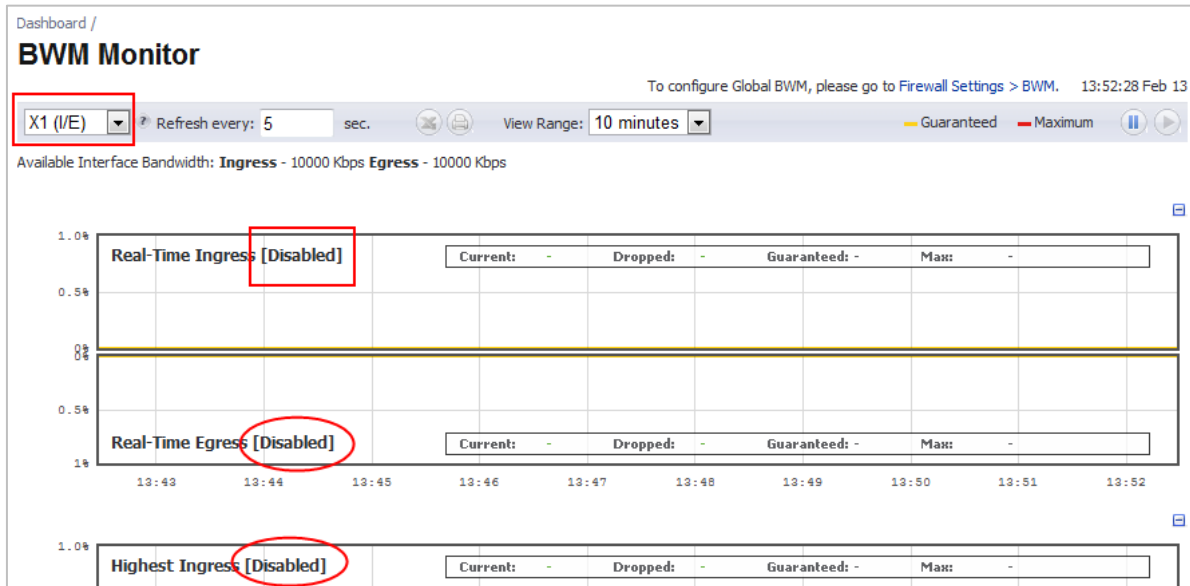
Note: When switching between bandwidth management modes, all bandwidth management settings in firewall access rules are set back to defaults and any custom settings must be reconfigured. Default BWM actions in Application Control policies are automatically converted to WAN BWM or Global BWM, using default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

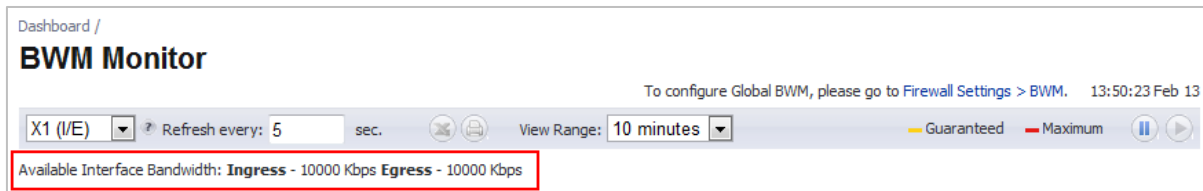
Release Notes

The **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.

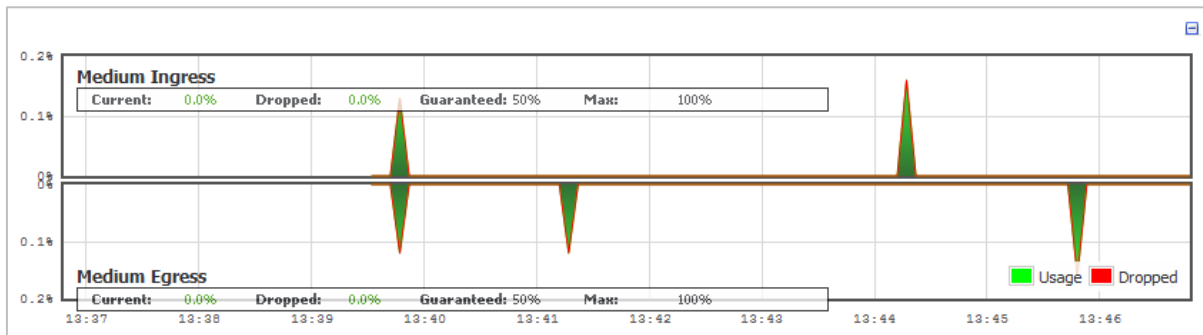
The **Dashboard > BWM Monitor** page displays a chart for each possible BWM setting for the selected interface, and displays **[Disabled]** unless BWM is enabled.



A text line is added near the top of the page showing the available bandwidth for the interface selected in the drop-down list at the top left.

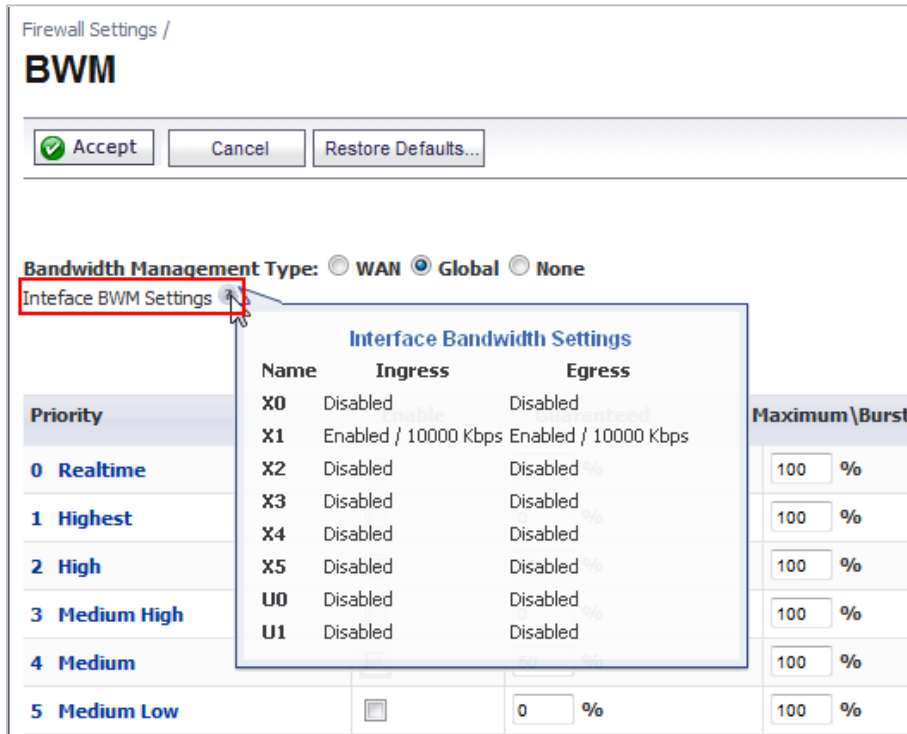


In each chart, an information box now shows the values for **Current** bandwidth, **Dropped** bandwidth, **Guaranteed** bandwidth, and **Max** bandwidth for the interface selected at the top of the page.



Release Notes

The **Firewall Settings > BWM** page has usability enhancements. An **Interface BWM Settings** tooltip displays all network interfaces and shows whether bandwidth management is enabled for them.

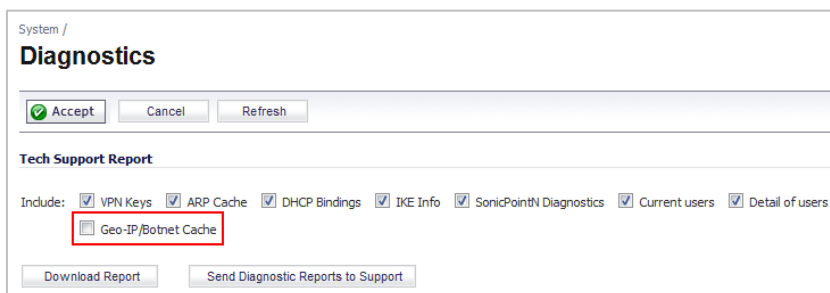


The following note is displayed at the bottom of the **Firewall Settings > BWM** page:

Note: This priority table is used only when global bandwidth management is selected. (When using legacy BWM, values can be set independently in Firewall Access Rules and Action Objects.)

In global BWM mode, all traffic (by default) is marked as "medium" priority unless configured via firewall rule/app firewall rule.

- **Geo-IP/Botnet** — The **System > Diagnostics** page has a **Geo-IP/Botnet Cache** checkbox. If selected, the Geo-IP and Botnet cached information is included when generating a Tech Support Report (TSR). If not selected, this lengthy data will not be included in the TSR.



Release Notes

- **Geo-IP Diagnostics** — The Geo-IP page has a **Diagnostics** section containing a **Show Resolved Locations** button and a table displaying cache statistics.

Geo-IP Cache Statistics	
Location Server IP:	204.212.170.189
Resolved Entries:	0
Unresolved Entries:	0
Current Entry Count:	0
Max. Entry Count:	50000
Location Map Count:	4198

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 Connections** or block **Firewall Rule-Based Connections**.

Security Services / **Geo-IP Filter**

Accept Cancel

Block connections to/from countries listed in the table below

All Connections Firewall Rule-based Connections

Enable Logging

Blocked	Country
<input type="checkbox"/>	Afghanistan
<input type="checkbox"/>	Aland Islands
<input type="checkbox"/>	Albania
<input type="checkbox"/>	Algeria
<input type="checkbox"/>	American Samoa
<input type="checkbox"/>	Andorra
<input type="checkbox"/>	Angola
<input type="checkbox"/>	Anguilla
<input type="checkbox"/>	Anonymous Proxy/Private IP
<input type="checkbox"/>	Antarctica

Geo-IP Exclusion Object:
Default Geo-IP and Botnet Exclusion Group

Release Notes

- **Botnet Filter**—The Botnet Filter feature is available as a free trial and can be activated by navigating to the **Security Services > Botnet Filter** page. The Botnet Filter page provides configuration options for blocking connections to/from Botnet Command and Control Services, enabling logging, defining Botnet exclusion objects, and checking Botnet server lookup.

Security Services /
Botnet Filter

Accept Cancel

Block connections to/from Botnet Command and Control Servers
 All Connections Firewall Rule-based Connections

Enable Logging

Botnet Exclusion Object:
Default Geo-IP and Botnet Exclusion Group

The Botnet page has a **Diagnostics** section containing a **Show Resolved Locations** button and a table displaying cache statistics.

Security Services

- Summary
- Content Filter
- Client AV Enforcement
- Gateway Anti-Virus
- Intrusion Prevention
- Anti-Spyware
- RBL Filter
- Geo-IP Filter
- Botnet Filter**
- WAN Acceleration

Diagnostics

Show Resolved Locations

Botnet Cache Statistics

Location Server IP:	204.212.170.189
Resolved Entries:	0
Unresolved Entries:	0
Current Entry Count:	0
Max. Entry Count:	50000
Location Map Count:	4198

Release Notes

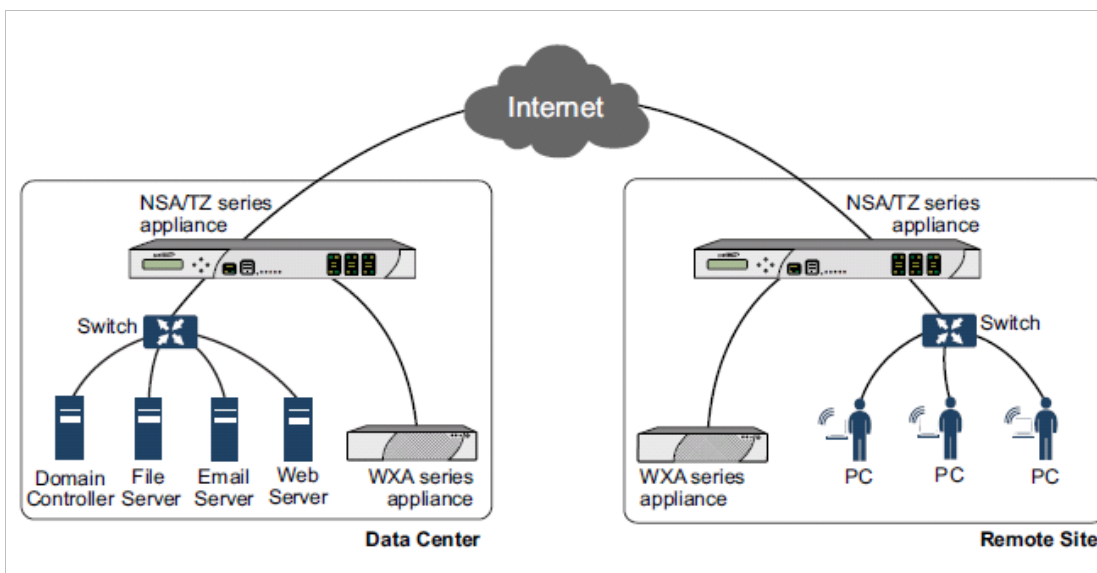
- **WXA 1.2 Support**—SonicOS 5.8.1.11 and higher supports SonicWALL WXA 1.2, which contains several enhancements over WXA 1.1.1:
 - **Unsigned SMB Acceleration**—In previous versions of WXA, SMB signing was the only supported method for shared access to files, which required joining the WXA series appliance to the domain and manually configuring shares. However, some networks do not need to use SMB signing. For these types of network environments, WXA 1.2 introduces support for Unsigned SMB, which allows the WXA series appliance to accelerate traffic without joining the domain. This greatly simplifies the configuration procedure for WFS Acceleration. Just click the **Unsigned SMB** checkbox, apply the changes, and shared files start accelerating between sites.

If your network uses unsigned and signed SMB traffic, the **Unsigned SMB** and **Support SMB Signing** checkboxes can be enabled to use both features simultaneously.

 - **Web Cache**—The Web Cache feature stores copies of frequently and recently requested Web content as it passes through the network. When a user requests this Web content, it is retrieved from the local web cache instead of the Internet, which can result in significant reductions in downloaded data and bandwidth usage.
 - **YouTube Web Caching**—The Web Cache feature also provides caching for YouTube content. This feature is only available when using Moderate (default) and Aggressive web caching strategies.

For more information about WAN Acceleration and these WXA 1.2 features, see the *WXA 1.2 User's Guide*.

WAN Acceleration—SonicOS 5.8.1.0 and higher, the WAN Acceleration service allows network administrators to accelerate WAN traffic between a central site and a branch site by using Transmission Control Protocol (TCP), Windows File Sharing (WFS), and a Web Cache. The Dell SonicWALL WXA series appliance is deployed in conjunction with a Dell SonicWALL NSA/TZ series appliance. In this type of deployment, the NSA/TZ series appliance provides dynamic security services, such as attack prevention, Virtual Private Network (VPN), routing, and Web Content Filtering. The WAN Acceleration service can increase application performance.



Release Notes

- **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.

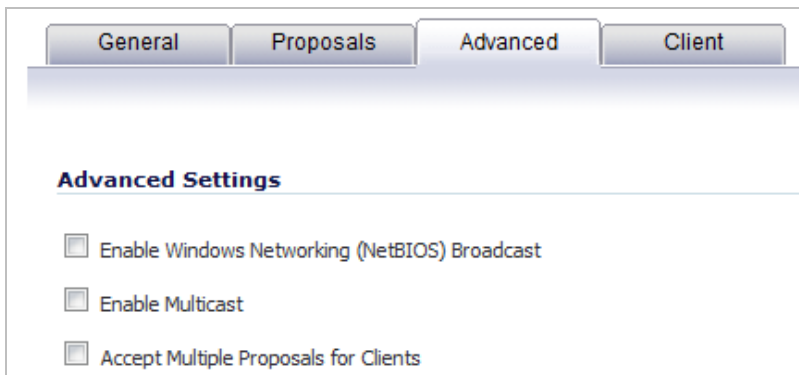
With support for two wireless radios at the same time, you can use **SonicPoint-N DR Clean Wireless** access points to create an enterprise-class secure wireless network. The SonicPoint-N DR uses six antennas to communicate with wireless clients on two frequency ranges: 2.4 GHz and 5 GHz. You can install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



- **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. This 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 allows connections from other L2TP clients, (such as Apple OS, Windows, or Android), whose proposals are different from the configured proposal in the Proposals tab. These proposals are accepted under the following conditions:

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

If this option is not selected, SonicOS requires 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.

Release Notes

- **ADTRAN Consolidation** — In SonicOS 5.8.1.11 and higher, ADTRAN NetVanta units run the same SonicOS firmware as SonicWALL units. Upon upgrading a NetVanta unit to SonicOS 5.8.1.11 or higher, the management interface will change from the previous NetVanta look and feel (color scheme, icons, logos) to the standard SonicWALL SonicOS look and feel. The Content Filter block page will look the same as that used by SonicWALL models.

In SonicOS 5.8.1.11 and higher, ADTRAN NetVanta units have the following capabilities:

- **Additional Features** — ADTRAN NetVanta units support the following additional features:
 - SonicPoint
 - Comprehensive Anti-Spam Service
 - WAN Acceleration
 - Enforced Client AV with Kaspersky Anti-Virus
 - Solera
 - Firmware Auto Update
 - **Feature Capabilities** — On ADTRAN NetVanta units, the following features provide the same capabilities as the equivalent SonicWALL units:
 - DHCP Server Leases
 - Maximum Schedule Object Group Depth
 - Maximum SonicPoints per Interface
 - SSLVPN Licenses
 - Virtual Assist Licenses
 - **Product Names** — On ADTRAN NetVanta units, the product name appears as the SonicWALL model name followed by “OEM” as follows:
 - NetVanta 2830 now appears as NSA 2400 OEM
 - NetVanta 2730 now appears as NSA 240 OEM
 - NetVanta 2730 EX now appears as NSA 240 OEM EX
 - NetVanta 2630 now appears as TZ 210 OEM
 - NetVanta 2630W now appears as TZ 210 wireless-N OEM
 - **URLs** — ADTRAN NetVanta units use the same URLs as SonicWALL units.
 - **WLAN SSID** — ADTRAN NetVanta units use “adtran” for the default Internal WLAN SSID.
 - **HTTPS Certificates** — ADTRAN NetVanta units use an ADTRAN-specific HTTPS management self-signed certificate.
- **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.

Release Notes

- **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.
- **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 in 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 5.8.1.11 and higher 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. Beginning in 5.8.1.0, SonicOS provides an attribute setting in the LDAP schema configuration for using this feature.

Release Notes

- **Preservation of Anti-Virus Exclusions After Upgrade**— SonicOS 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.

- **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.

Release Notes

- **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).
- **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.

Release Notes

- **Management Traffic Only Option for Network Interfaces**—Beginning in 5.8.1.0, SonicOS 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**—Beginning in 5.8.1.0, SonicOS includes an 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 5.8.1.12 release.

3G/4G

Symptom	Condition / Workaround	Issue
The Option AT&T Velocity does not connect.	Occurs on TZ 200 and TZ 200W platforms after rebooting.	128398
AT&T Momentum 4G Sierra Wireless U313 cannot always establish a connection.	Occurs when trying to connect wireless devices to the Internet.	128346
Customer cannot establish a connection using a Huawei E1750 3G modem (a supported device).	Occurs when trying to get an IP connection on port U0 or U1 using a Huawei E1750.	123501
A Sierra Wireless 308 card cannot establish a 4G connection. No IP address is obtained.	Occurs when trying to connect a Sierra Wireless 308 card to an NSA 240.	120689

Bandwidth Management

Symptom	Condition / Workaround	Issue
When the Bandwidth Management (BWM) Global option is enabled, undefined queues can be selected without any warning that they are undefined, and the selected queue is then replaced with the default Medium queue when used in an Access Rule.	Occurs when a user selects a priority queue other than the default High, Medium, and Low queues without first defining the selected queue.	125706

Content Filtering

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

DPI-SSL

Symptom	Condition / Workaround	Issue
Excluding a User Object or User Group for Server DPI-SSL causes Client DPI-SSL to not work properly.	Occurs when accessing HTTPS websites from a client computer without logging in as a user on the client computer. Client DPI-SSL does not change the site certificate to the SonicWALL certificate.	118962

Release Notes

Geo-IP Filtering

Symptom	Condition / Workaround	Issue
Geo-IP Filtering does not successfully block some IP addresses even though they are in the blocked countries list.	Occurs when a user tries to access a site with an IP address that is in a country that is blocked by Geo-IP Filtering. The user can intermittently access some sites that are in countries that are blocked by Geo-IP Filtering.	126610

Global VPN Client (GVC)

Symptom	Condition / Workaround	Issue
A GVC connection cannot be established when using OCSP. The connection fails and the user gets the error message: "OCSP send request failed: status update verification in progress failed ! initCookie 0x13f4b71e603".	Occurs when a user attempts to connect using a GVC connection with a certificate, and Online Certificate Status Protocol (OCSP) is enabled in the WAN VPN Group. Workaround: If OCSP is disabled, the GVC connects successfully with a certificate.	126441

Networking

Symptom	Condition / Workaround	Issue
A computer connected to one interface of a L2 Bridge pair cannot ping a computer connected to the other interface of the L2 Bridge pair.	Occurs when the "Never route traffic on this bridge-pair" option is enabled for the L2 Bridge pair (LAN/WAN). Workaround: Disable the "Never route traffic on this bridge-pair" option.	125837
Users cannot access the Internet when WXA web cache is enabled and RADIUS authentication is used.	Occurs when WXA is asked to authenticate a user using RADIUS. WXA requests are redirected to the login page. Workaround: Make policy changes that allow WXA traffic on the WAN and reboot the firewall.	124281
FTP or HTTP traffic cannot pass through a pair of interfaces configured in Wire Mode and set to Secure.	Occurs when using a Stateful High Availability pair and Active-Active DPI is enabled.	101359

Release Notes

SSL VPN

Symptom	Condition / Workaround	Issue
Java and ActiveX RDP Bookmarks do not work when connecting from a Windows 8 client.	Occurs when a user tries to connect to SSL VPN Virtual Office Bookmarks from a Windows 8 workstation. The user gets a bookmarks fail protocol error.	126736
Using the default SSL VPN NetExtender client, Windows 8 can connect to the SSL VPN server, but no route is configured on the client.	Occurs when the default NetExtender Windows Client (5.5.158) is installed on Windows 8. The client can connect to the SSL VPN server, but a NetExtender route cannot be configured.	123277
A client computer cannot connect to NetExtender.	Occurs when a user is using the Google Chrome browser to attempt to connect to NetExtender.	120973

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

VPN

Symptom	Condition / Workaround	Issue
The tunnel interface is bound to X0, but IKE traffic is allowed on X1 through the remote firewall that is reachable on X1.	Occurs when trying to establish a tunnel interface VPN between two firewalls discovered by the router. When trying to connect Firewall1 X0 to Firewall2 X0, when the IPsec Phase2 security association (SA) is accepted, but the VPN is down, the policy is bound to X0. Although the remote firewall is reachable through X1, no IKE packet should go through the X1 interface in this configuration.	121966

Release Notes

Resolved Issues

The following issues are resolved in the SonicOS 5.8.1.12 release:

Geo-IP Filtering

Symptom	Condition / Workaround	Issue
Geo-IP lookups are slow at times.	Occurs when Geo-IP lookups must access a DNS server for each address instead of finding them on an internal database.	127633

SonicPoint

Symptom	Condition / Workaround	Issue
SonicPoints become unresponsive and internal wireless performance becomes unstable.	Occurs when the firewall is using a hot fix.	119498

SSL VPN

Symptom	Condition / Workaround	Issue
Firewall has SSL/TLS 'Crime' vulnerability.	Occurs when the browser does TLS encryption of compressed data. Workaround: Make sure all browsers are updated to the latest browser versions.	123212
Computer screen displays message: "SSLv3.0/TLSv1.0 Protocol weak CBC mode vulnerability."	Occurs when an online vulnerability scan is performed. Workaround 1: Do not use the SSL VPN features in SonicOS. Use a dedicated SSL VPN appliance instead. Workaround 2: Limit the sources allowed to do HTTPS Management to all WAN interfaces of the firewall. Create WAN objects for all authorized remote locations from which management is allowed. Edit the WAN to WAN HTTPS Management rule, by changing the Source from Any to Source = Object or Object Group .	113097

System

Symptom	Condition / Workaround	Issue
NSA 4500 reboots due to semaphore deadlock.	Occurs when H.323 Transformations is enabled, and SonicOS incorrectly handles a large H.323 TCP segment that needs fragmentation.	125434

Release Notes

VPN

Symptom	Condition / Workaround	Issue
VPN is dropping packets incorrectly when firewall is upgraded to 5.8.1.11.	Occurs when firewall is upgraded to 5.8.1.11 and VPNs are established. Workaround: Downgrade to the previous firmware version.	127272

Wireless

Symptom	Condition / Workaround	Issue
Wireless SSIDs are not displayed.	Occurs when the SonicPoints have been running for 2 hours.	117816

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>	47
<i>Saving a Backup Copy of Your Configuration Preferences</i>	47
<i>Upgrading a SonicOS Image with Current Preferences</i>	48
<i>Importing Preferences to SonicOS 5.8.1.12</i>	48
<i>Importing Preferences from SonicOS Standard to SonicOS 5.8.1.12 Enhanced</i>	49
<i>Support Matrix for Importing Preferences</i>	50
<i>Upgrading a SonicOS Image with Factory Defaults</i>	51
<i>Using SafeMode to Upgrade Firmware</i>	51

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:
 - o VPN Keys
 - o ARP Cache
 - o DHCP Bindings
 - o IKE Info
 - o SonicPointN Diagnostics
 - o Current users
 - o 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 - New!**
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 5.8.1.12

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 5.8.1.12 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 5.8.1.12 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 retains a copy of their network settings after the conversion process is complete.
5. Upload the source Standard Network Settings file:
 - o Click **Browse**.
 - o Navigate to and select the source SonicOS Standard Settings file.
 - o Click **Upload**.
 - o 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.
 - o (Optional) Change the LAN IP address and subnet mask of the source appliance to that of the target appliance.
 - o 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

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 - New**.
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:
 - o 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.
 - o 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**.

Release Notes

6. Select the boot icon  in the row for one of the following:
 - o **Uploaded Firmware – New!**
Use this option to restart the appliance with your current configuration settings.
 - o **Uploaded Firmware with Factory Default Settings – 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 SonicWALL logo, menu items (Products, Solutions, How to Buy, Support), and a search bar. 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, there are tabs for "Support Documents" and "Knowledge Base". The "Support Documents" section is active, showing a list of product guides and technical notes. The "Product Guides" section lists six items, including user guides for SonicWALL Mobile Connect and administrator's guides for SonicOS 5.8.1. The "Technical Notes" section lists six items, including integration guides for CradlePoint and Agilink with SonicOS 5.9 and 5.8.1.5. A left-hand navigation menu lists various support categories, with "NSA E-Class Series" selected. A "List View Options" section allows users to filter the resource list by categories like Video Tutorials, Product Guides, Technical Notes, FAQs, Release Notes, and Support Data Sheets.

Last updated: 3/26/2013

SonicOS 5.8.1.12 Release Notes

P/N 232-001421-00 Rev A

