Release Notes

Contents

Platform Compatibility

The SonicOS 5.8.1.15 release is supported on the following SonicWALL Deep Packet Inspection (DPI) security appliances:

- SonicWALL NSA 250M Series
- SonicWALL NSA 220 Series
- SonicWALL TZ 215 Series

The SonicWALL WXA series appliances (WXA 6000 Software, 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 5.8.1.15. The minimum recommended firmware version for the WXA series appliances is 1.3. SonicOS 5.8.1.15 is only compatible with WXA 1.2.2 and newer. Earlier versions of WXA are not supported.

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 and higher (do not use compatibility mode)
- Safari 5.0 and higher

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

Known Issues

This section contains a list of known issues in the SonicOS 5.8.1.15 release.

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

Networking

Symptom	Condition / Workaround	Issue
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

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.	121966

Resolved Issues

The following issues are resolved in the SonicOS 5.8.1.15 release:

Appflow

Symptom	Condition / Workaround	Issue
Some devices and URLs are not shown on Flow Server.	Occurs when trying to view devices on the Flow Server.	139246

DPI-SSL

Symptom	Condition / Workaround	Issue
HTTPS Web sites cannot be accessed in Wire mode.	Occurs when Wire mode is in secure mode and Client DPI-SSL enabled.	134703

Security Services

Symptom	Condition / Workaround	Issue
No inbound emails are received.	Occurs when Anti-Spam is enabled.	134223

User Interface

Symptom	Condition / Workaround	Issue
The SonicOS management interface is slow to respond, or does not respond for a brief period of time.	Occurs when the WebListener task is in a loop waiting for more SSL data until it eventually times out. During this period, the tWebListen task may take 100% of the CPU time. **Note**: As a best practice, configure Access Control of the management interface on the WAN.	144909

VPN

Symptom	Condition / Workaround	Issue
NAT traffic is sent to WXA on the remote node.	Occurs when NAT traffic is sent over a VPN tunnel interface.	137694

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 220 Series	NSA 250M Series	TZ 215 Series
Accept Multiple Proposals for Clients	Supported	Supported	Supported
App Control Advanced	Supported	Supported	Supported
App Control Policy Configuration via AppFlow Monitor	Supported	Supported	Supported
App Rules	Supported	Supported	Supported
AppFlow > Flow Reporting	Supported	Supported	Supported
AppFlow Dash	Supported	Supported	Supported
AppFlow Monitor	Supported	Supported	Supported
AppFlow Reports	Supported	Supported	Supported
Application Usage and Risk Report	Supported	Supported	Supported
Auto-Configuration of URLs to Bypass User Authentication	Supported	Supported	Supported
Browser NTLM Authentication	Supported	Supported	Supported
CASS 2.0	Supported	Supported	Supported
CFS Enhancements	Supported	Supported	Supported
Cloud GAV	Supported	Supported	Supported
Connection Monitor	Supported	Supported	Supported
Current Users and Detail of Users Options for TSR	Supported	Supported	Supported
Customizable Login Page	Supported	Supported	Supported
DHCP Scalability Enhancements	Supported	Supported	Supported
DPI-SSL	Supported	Supported	
Dynamic WAN Scheduling	Supported	Supported	Supported
Enhanced Connection Limit	Supported	Supported	Supported
Geo-IP Filtering and Botnet Command & Control Filtering	Supported	Supported	Supported
Global BWM Ease of Use Enhancements	Supported	Supported	Supported

Feature / Enhancement	NSA 220 Series	NSA 250M Series	TZ 215 Series
IKEv2	Supported	Supported	Supported
IPFIX & NetFlow Reporting	Supported	Supported	Supported
LDAP Primary Group Attribute	Supported	Supported	Supported
Link Aggregation			
Log Monitor	Supported	Supported	Supported
Management Traffic Only Option for Network Interfaces	Supported	Supported	Supported
NSA Modules		Supported	
NTP Authentication Type	Supported	Supported	Supported
Packet Monitor Enhancements	Supported	Supported	Supported
Port Redundancy			
Preservation of Anti-Virus Exclusions After Upgrade	Supported	Supported	Supported
Real-Time Monitor	Supported	Supported	Supported
SIP Application Layer Enhancements	Supported	Supported	Supported
SonicPoint Ne/Ni	Supported	Supported	Supported
SonicPoint VAPs	Supported	Supported	Supported
SonicPoint-N DR	Supported	Supported	Supported
SSL VPN NetExtender Client Update	Supported	Supported	Supported
SSO User Import from LDAP	Supported	Supported	Supported
Top Global Malware	Supported	Supported	Supported
User Monitor Tool	Supported	Supported	Supported
VLAN Subinterfaces	Supported	Supported	Supported
WAN Acceleration Support	Supported	Supported	Supported
Wire and Tap Mode			
Wireless Client Bridge Support	Supported	Supported	Supported
YouTube for Schools	Supported	Supported	Supported

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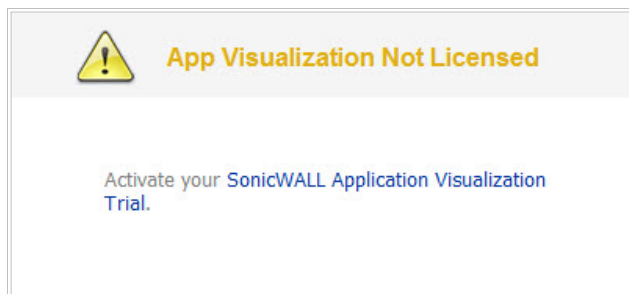
The following table lists the key features in SonicOS 5.8 that depend on licenses and other settings for the related management interface pages to display and function properly:

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 > GeoIP 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

Key Features in SonicOS 5.8

The following are the key features in SonicOS 5.8:

- **YouTube for Schools 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

  o 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.

  o 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*.

  Configuring YouTube for Schools as an App Control Policy

  o When the **CFS Policy Assignment** drop-down 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**.

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

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
	Included: Excluded:
Users/Groups:	All 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:	uflGb16ejHSRXqXnnnK2Jg

Note: BWM Type: Advanced; To change go to Firewall Settings > BWM

Ready

OK   Cancel   Help

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

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

SONICWALL®

Configuring YouTube for Schools as a Content Filter Policy

o   When the **CFS Policy Assignment** drop-down 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** drop-down 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.

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.

10. Type "ytimg.com" into the **Domain Name** field and click **OK**.
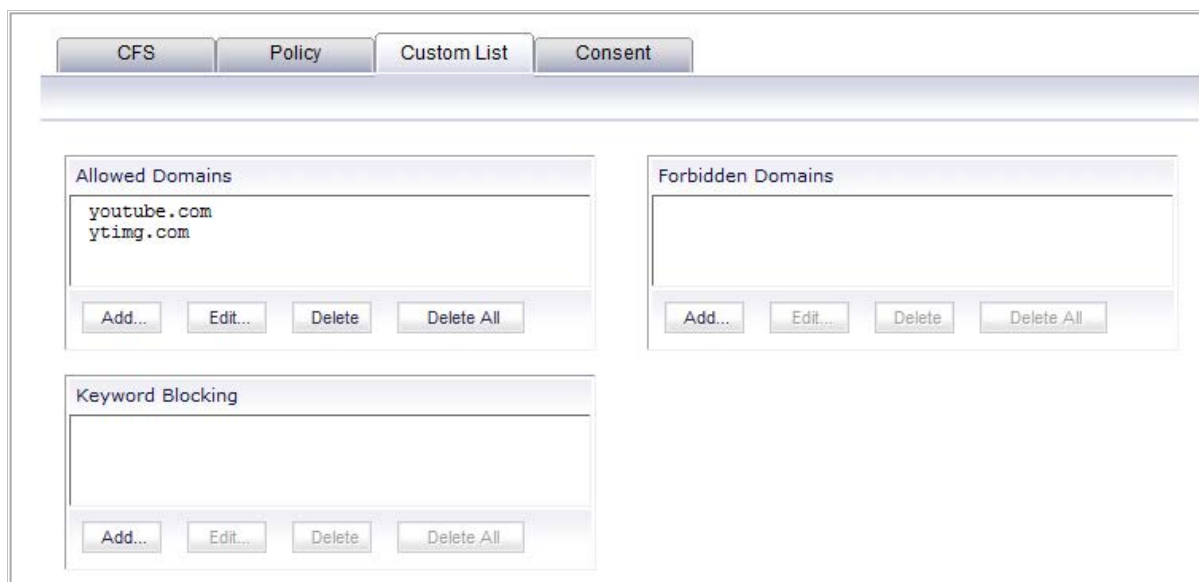
11. Click **OK**. These settings will override any CFS category that blocks YouTube.

   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:
   o More secure
   o More reliable
   o Simpler
   o Faster
   o Extensible
   o Fewer message exchanges to establish connections
   o EAP Authentication support
   o MOBIKE support
   o Built-in NAT traversal
   o Keep Alive is enabled as default

- **SNMP for VLAN Interfaces** — In SonicOS 5.8.1.12 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.

- **Module Support**—The following SonicWALL NSA modules are supported on the NSA 250M series appliance:

  WARNING: You **MUST** power down the appliance before installing or replacing the modules.

  - **1 Port ADSL (RJ-11) Annex A** – Provides Asymmetric Digital Subscriber Line (ADSL) over plain old telephone service (POTS) with a downstream rate of 12.0 Mbit/s and an upstream rate of 1.3 Mbit/s.

  - **1 Port ADSL (RJ-45) Annex B** – Provides Asymmetric Digital Subscriber Line (ADSL) over an Integrated Services Digital Network (ISDN) with a downstream rate of 12.0 Mbit/s and an upstream rate of 1.8 Mbit/s.

  - **1-port T1/E1 Module** – Provides the connection of a T1 or E1 (digitally multiplexed telecommunications carrier system) circuit to a SonicWALL firewall using a RJ-45 jack.

  - **2-port LAN Bypass Module** – Removes a single point of failure so that essential business communication can continue while a network failure is diagnosed and resolved.
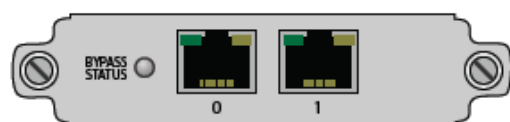
  - **2-Port SFP Module** – This small form-factor pluggable (SFP) network interface module offers a fiber alternative to the 4-Port GbE Module, enabling more flexible and scalable deployments in a wide range of environments. Note that port 0 (802.3at) is disabled by default and should be enabled manually from the SonicOS management interface.

  - **4-Port Gigabit Ethernet Module** – Expands port density of a SonicWALL NSA 250M Series firewall by adding four 1-Gbps Ethernet networking interfaces that negotiate the best Ethernet speeds available.
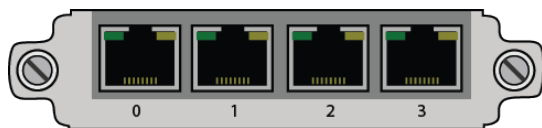
- **Real-Time Monitor** — The real-time visualization dashboard monitoring feature allows administrators to respond quickly to network security vulnerabilities and network bandwidth issues. Administrators can see what websites their users are accessing, what applications and services are being used in their networks and to what extent, in order to police content transmitted in and out of their organizations.
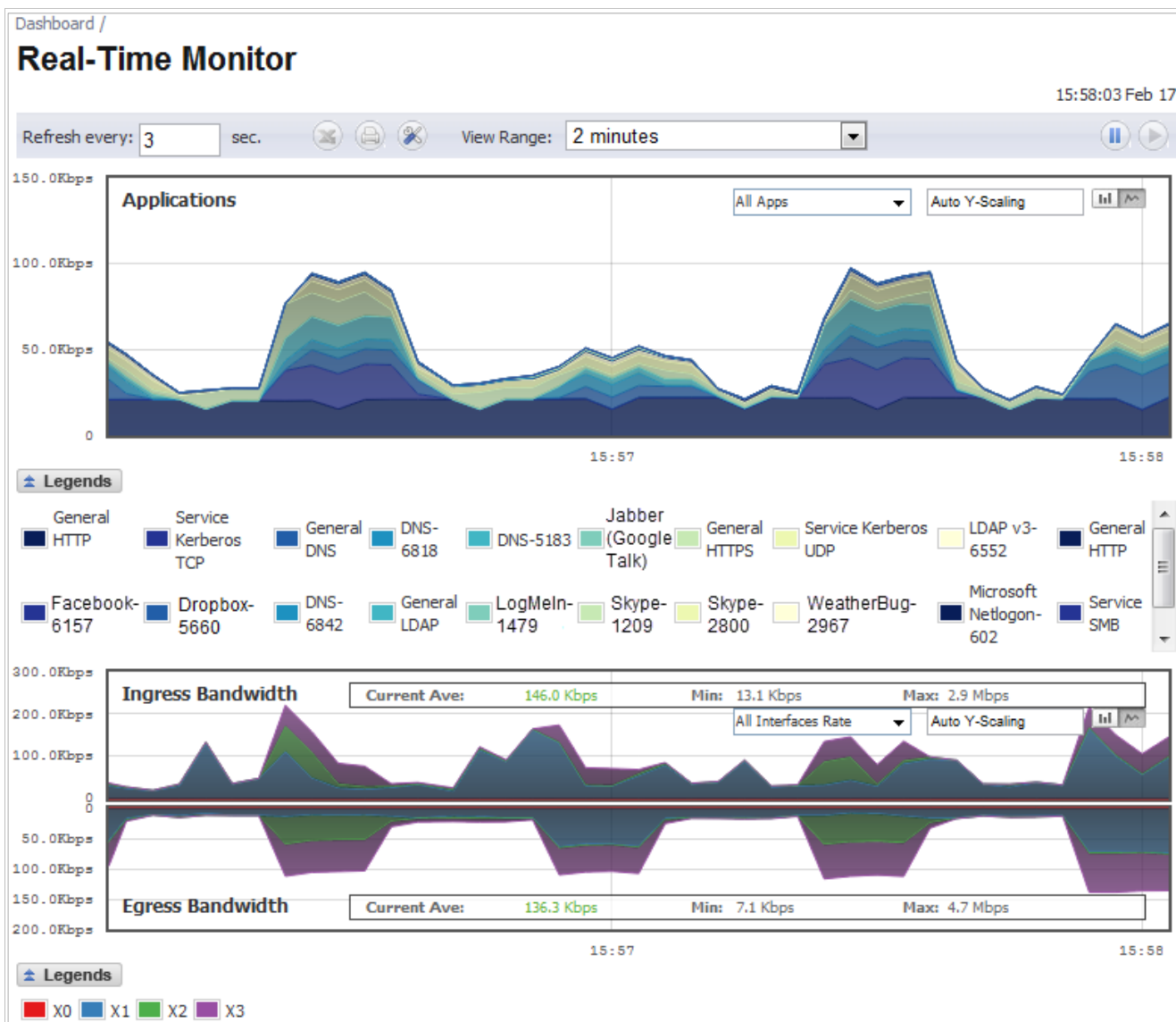
New appliances running SonicOS 5.8.1.15 receive an automatic 30-day free trial for App Visualization upon registration.

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.

SONICWALL®

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

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

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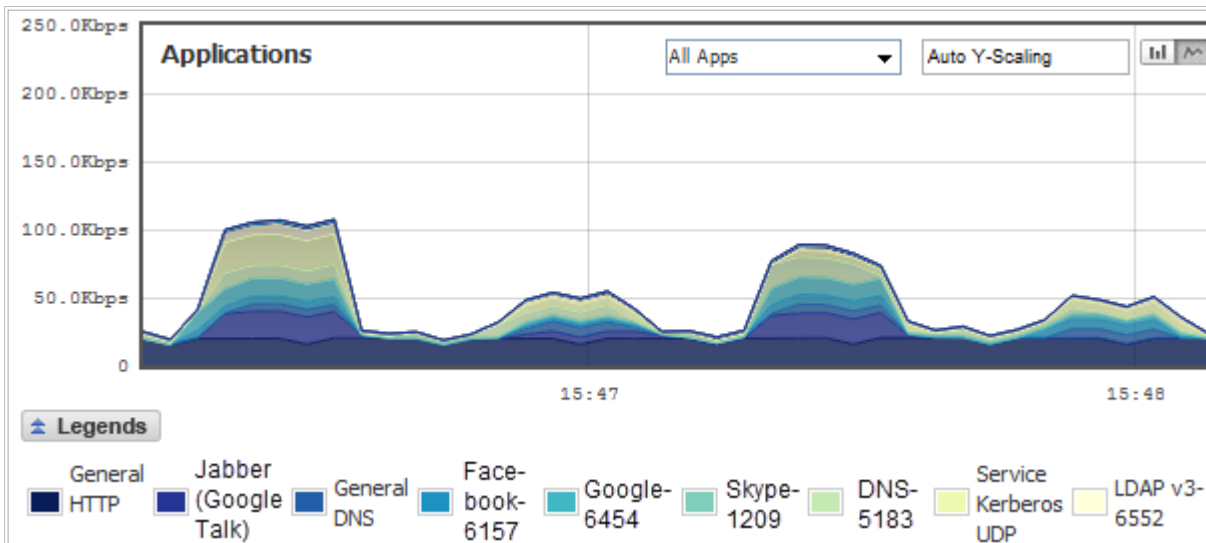
To relocate the legends into the Application or Bandwidth charts, click the ☒ icon, then select the desired checkbox(s).

To view individual application information, hover the mouse over the real-time visualization graph to display a tooltip.
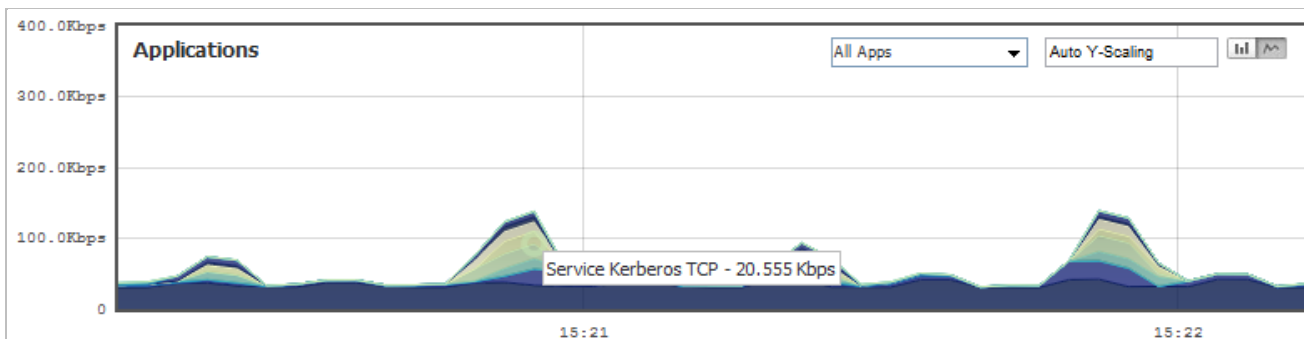
By default, the Multi-Core Monitor displays as a stack chart, rather than as a bar graph, to easily show its relation to the other charts on this screen.
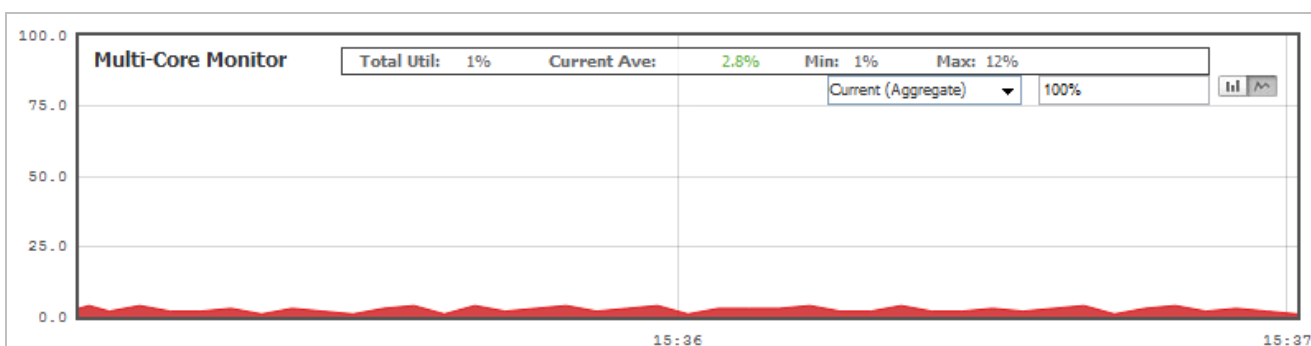
Note: The Multi-Core Monitor only shows the processor load for the cores of the managing firewall. If operating in Active-Active DPI mode, the core load for the standby firewall does not display.

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.
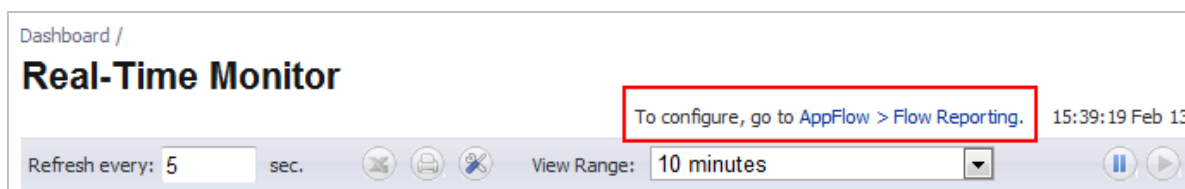
To enable/disable each chart in the Real-Time Monitor page, use the **Enable Real-Time Data Collection** option and associated drop-down list.
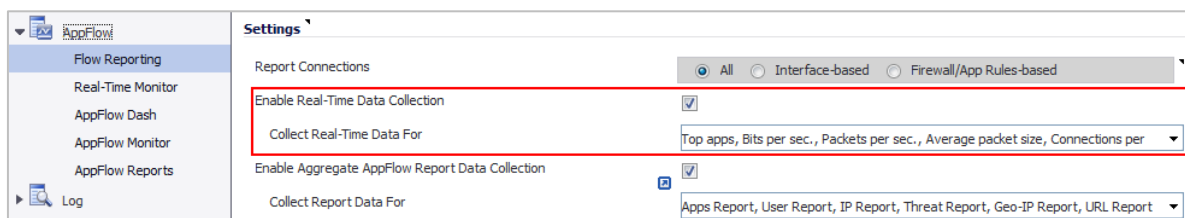
- **Real-Time Monitor Tooltips** — The **Dashboard > Real-Time Monitor** page provides a tooltip with useful information next to each chart title.
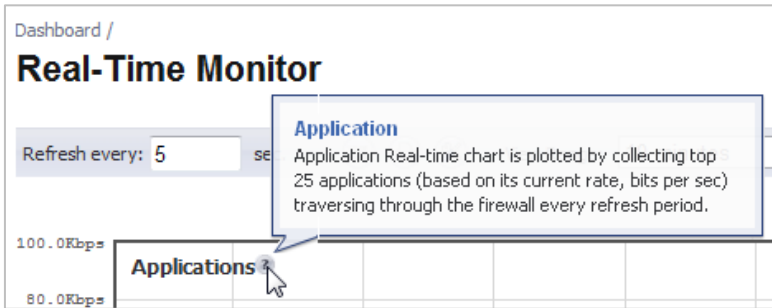
Real-Time Monitor Collapse/Expand Options — The **Dashboard > Real-Time Monitor** page provides a collapse/expand button for each chart. This allows the administrator to juxtapose two charts for comparison, even if they are normally far apart on the page.
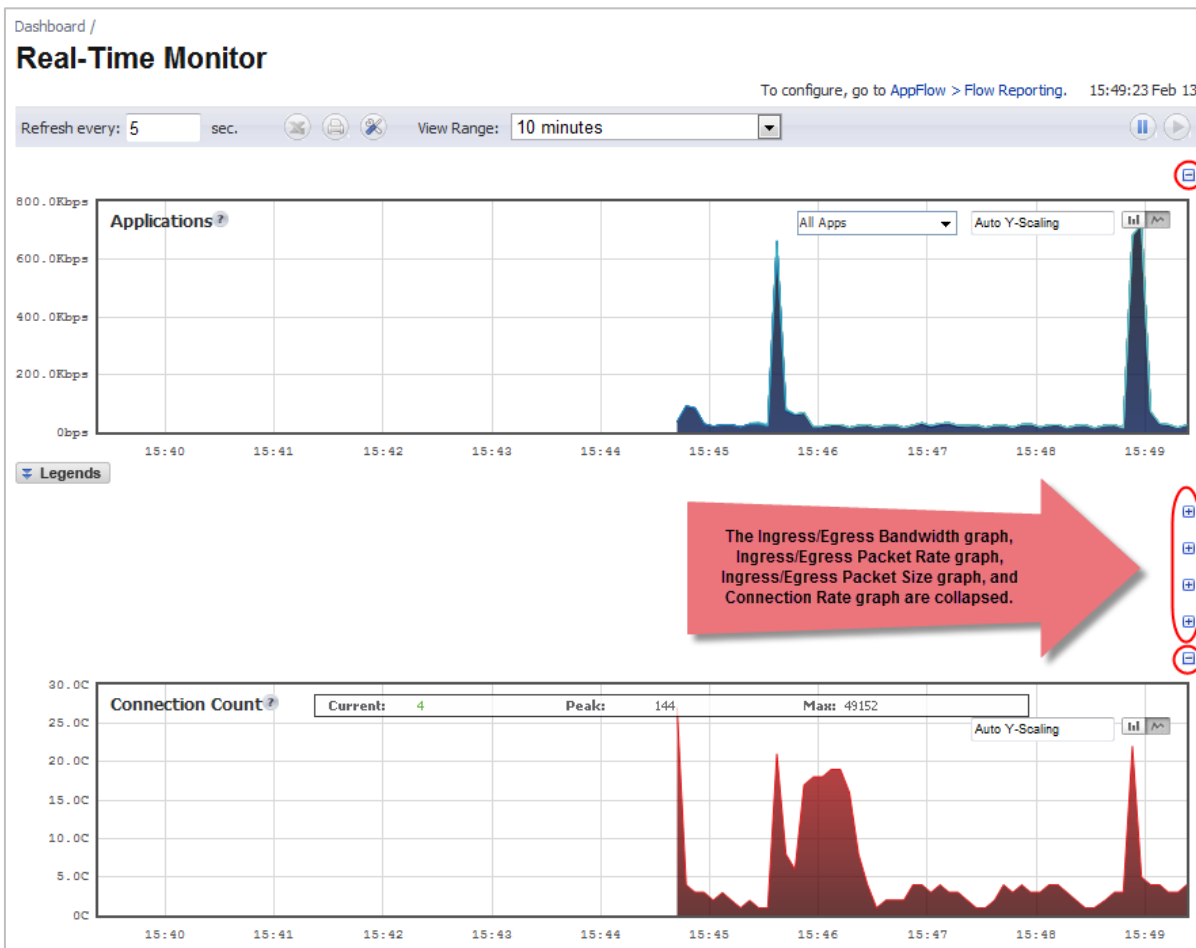
- **Standalone Dashboard Page** — Several of the SonicWALL Visualization Dashboard pages contain a blue pop-up button that will display the dashboard in a standalone browser window that allows for a wider display. Click on the blue pop-up icon to the right of the page name in the left-hand navigating bar to display a dashboard page as a standalone page.
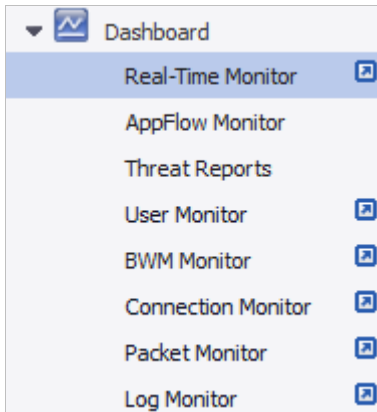
The pop-up button is also available at the top right of the individual dashboard pages, as shown below:
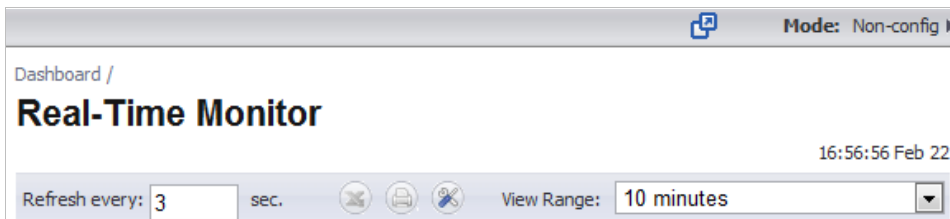
- **AppFlow** > **Flow Reporting** — The **AppFlow** > **Flow Reporting** page provides the information previously displayed in the **Log > Flow Reporting** page, such as detailed external and internal flow statistics. In SonicOS 5.8.1.11 and higher, the **Log** > **Flow Reporting** page is removed, and its elements are now displayed in the **AppFlow** > **Flow Reporting** page.

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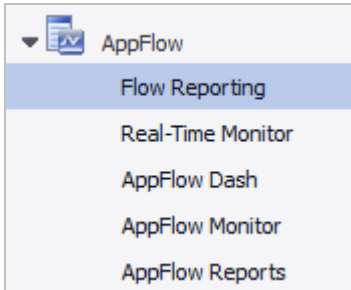
  A number of enhancements have been added to the **AppFlow** and **Dashboard** pages.

  More sections have been added to the **AppFlow** > **Flow Reporting** page, and some elements have been rearranged and placed under one of the three tabs:

  o   Statistics
  o   Settings
  o   External Collector

  The **Statistics** section is shown below.

The **Settings** section is shown below.

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.

The **Settings** section 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. Some other options under **Settings** are:

o   **Enable Geo-IP Resolution**— AppFlow Monitor groups flows based on country under initiator and responder tabs.

o   **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.

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

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.

- **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:
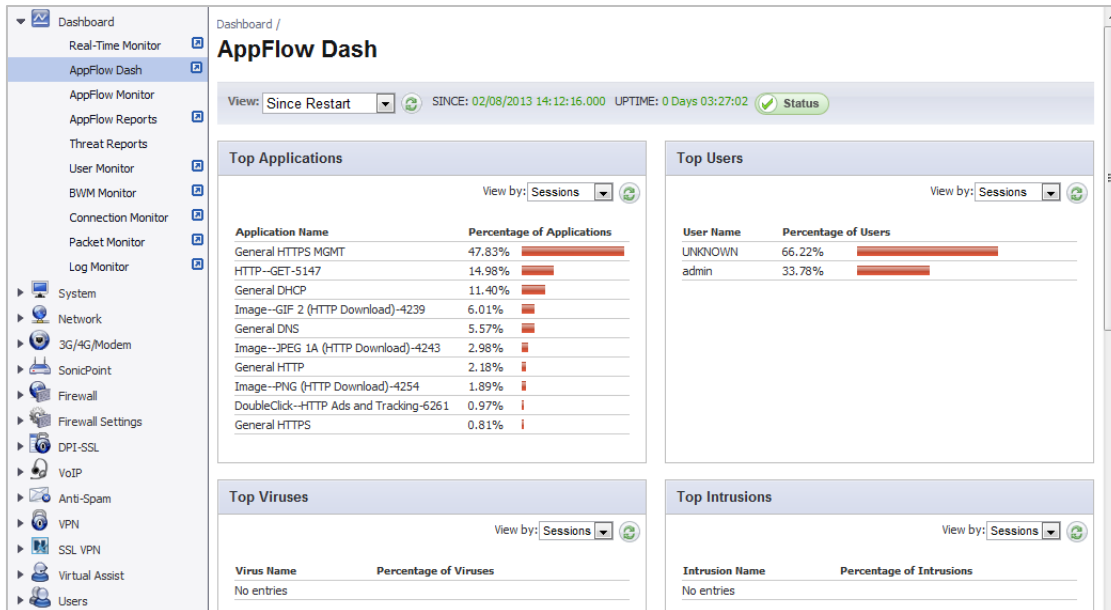
The bottom four graphs from the **AppFlow Dash** page are shown below:
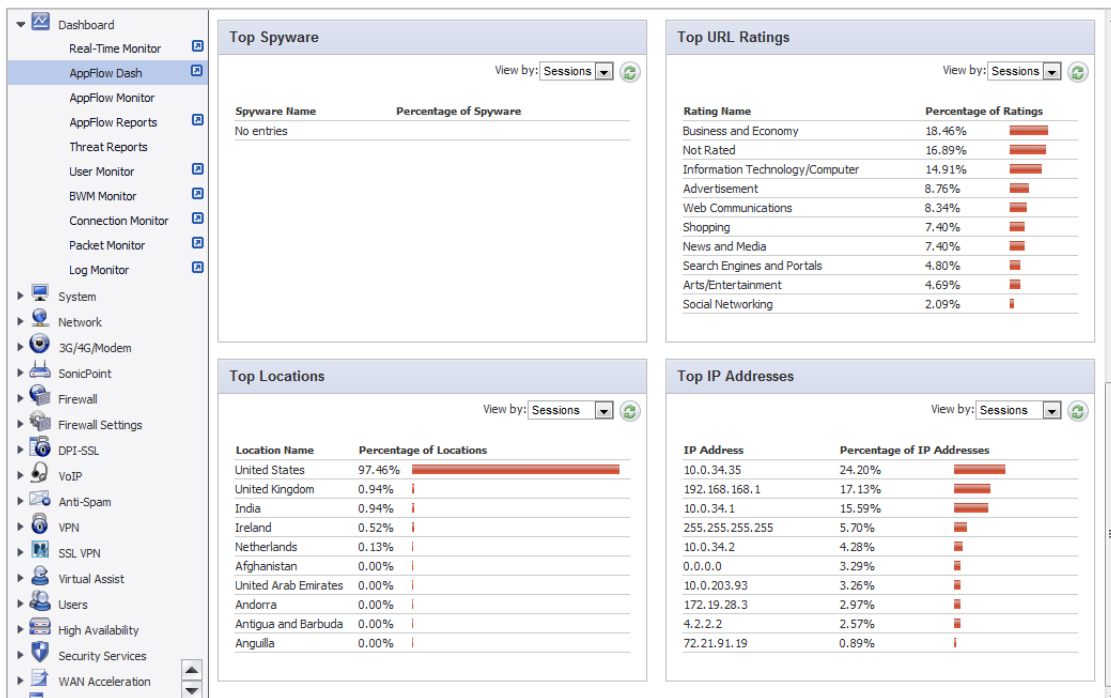
- **Dashboard > AppFlow Monitor** –– The toolbar categories display Total Packets, Total Bytes, and Average Rate, providing the user with a specific view of data being transferred.

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

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

Flow Table

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.

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

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.

o **Link to AppFlow > Flow Reporting** ⎯ A link to the **AppFlow > Flow Reporting** page is provided at the bottom of the **Dashboard > AppFlow Monitor** page.
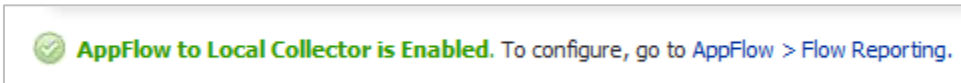
o **Local Collector Status** ⎯ A green or red status line at the bottom of the **Dashboard > AppFlow Monitor** page shows whether AppFlow to Local Collector is enabled (green) or disabled (red).

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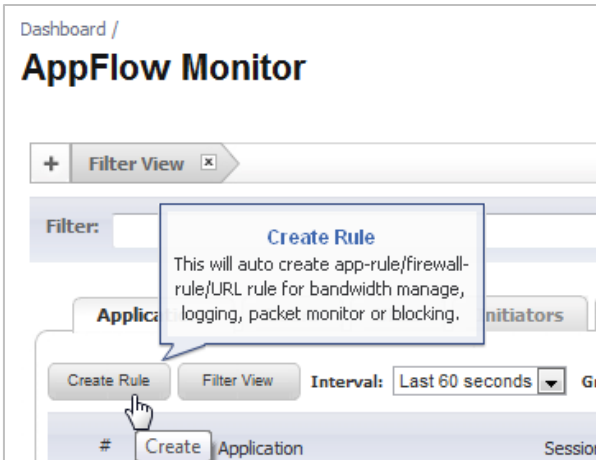
o **Numbering and Auto-Scrolling** ⎯ Numbering is added in the left-most column of each table on the **Dashboard** > **AppFlow Monitor** page, along with an auto-scroll feature, which automatically loads more rows as you scroll down. This allows you to keep track of where you are in the list while scrolling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

- **Dashboard** > **AppFlow Reports** — The **Dashboard > AppFlow Reports** page provides aggregate AppFlow reports for the following cases:

  o Since the last firewall restart

  o Since the last reset of the counter; administrators can reset the counter manually

  o 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.

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:


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:

- **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.

  App Control Global Settings

  ☑ Enable App Control

  | Configure App Control Settings | Reset App Control Settings & Policies |
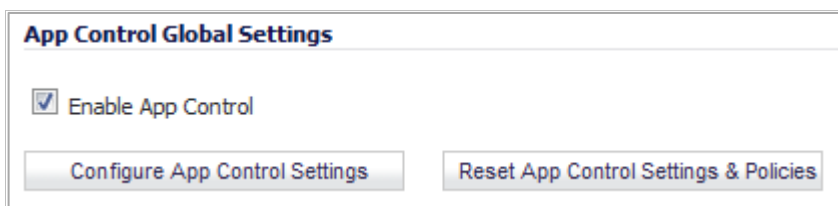
  To create policies using App Rules (included with the App Control license), select **Enable App Rules** on the Firewall > App Rules page.

  App Rules Global Settings

  Enable App Rules: ☑
  Global Log Redundancy Filter (seconds): 0
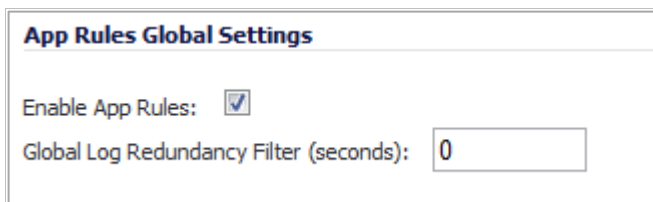
- **Global Bandwidth Management**—Global Bandwidth Management improves ease of use for bandwidth management (BWM) configuration, and increases throughput performance of managed packets for ingress and egress traffic on all interfaces, not just WAN. The Firewall Settings > BWM page allows network administrators 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.

SONICWALL®

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

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.

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

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.

- **Bandwidth Management Monitor Page**—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.
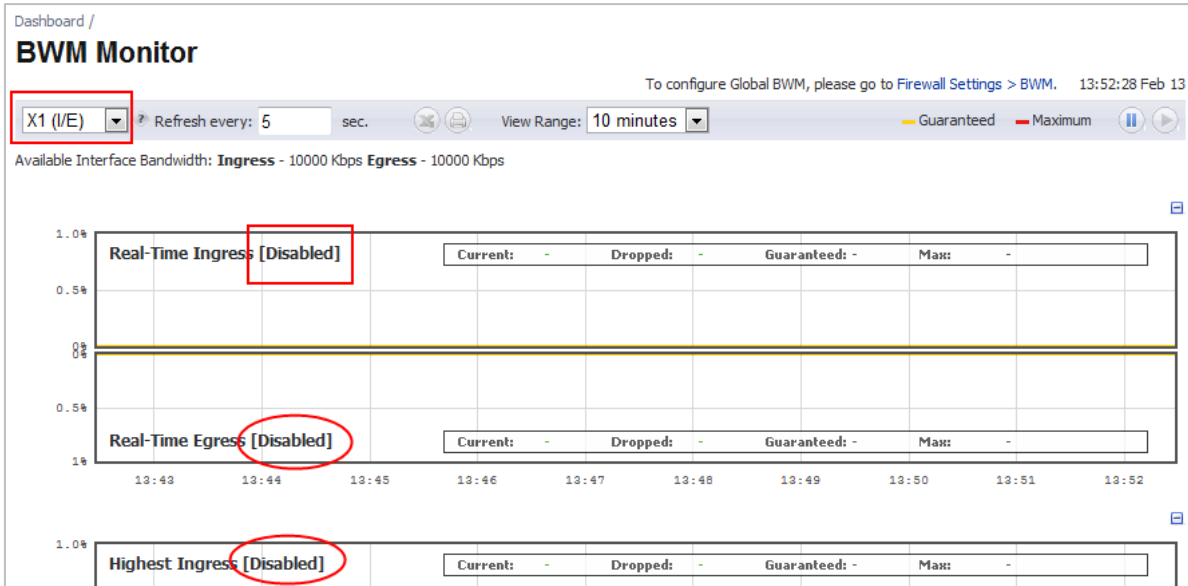
A text line is added near the top of the page showing the available bandwidth for the interface selected in the drop-down list at the top left.
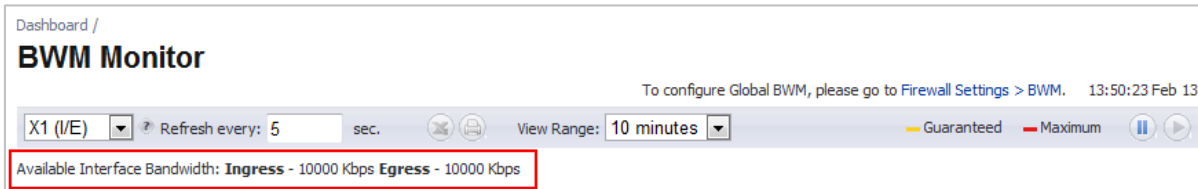
In each chart, an information box now shows the values for **Current** bandwidth, **Dropped** bandwidth, **Guaranteed** bandwidth, and **Max** bandwidth for the interface selected at the top of the page.
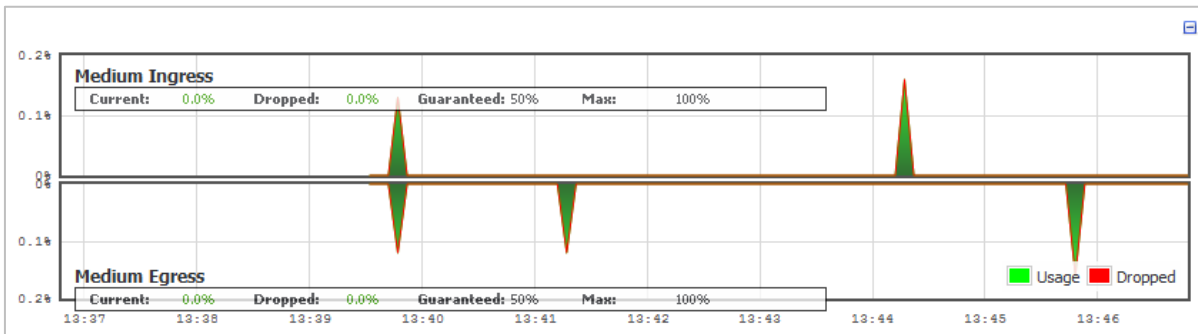
- **Geo-IP Filter** — The Geo-IP Filter page has a **Diagnostics** section containing a **Show Resolved Locations** button and a table displaying cache statistics.
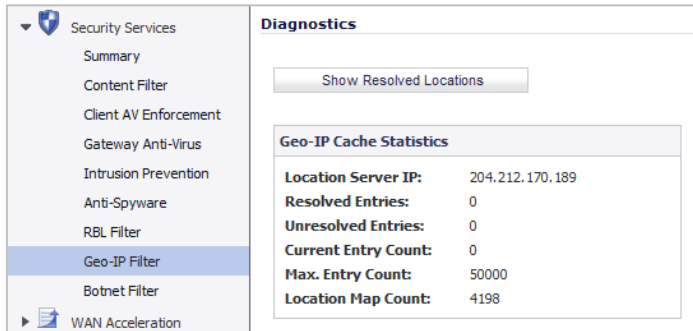
The **Geo-IP Filter** page includes several options, including **Block Connections to/from Following Countries**, **Block all connections to public IPs if GeoIP DB is not downloaded**, **Block ALL UNKNOWN countries**, and a checkbox for **Enable Logging**.

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

Select the **Block all connections to public IPs if GeoIP DB is not downloaded** 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.

Some countries may not be listed in the Geo-IP database. Select the **Block ALL UNKNOWN countries** option if you want all countries not listed in the Geo-IP database to be blocked.
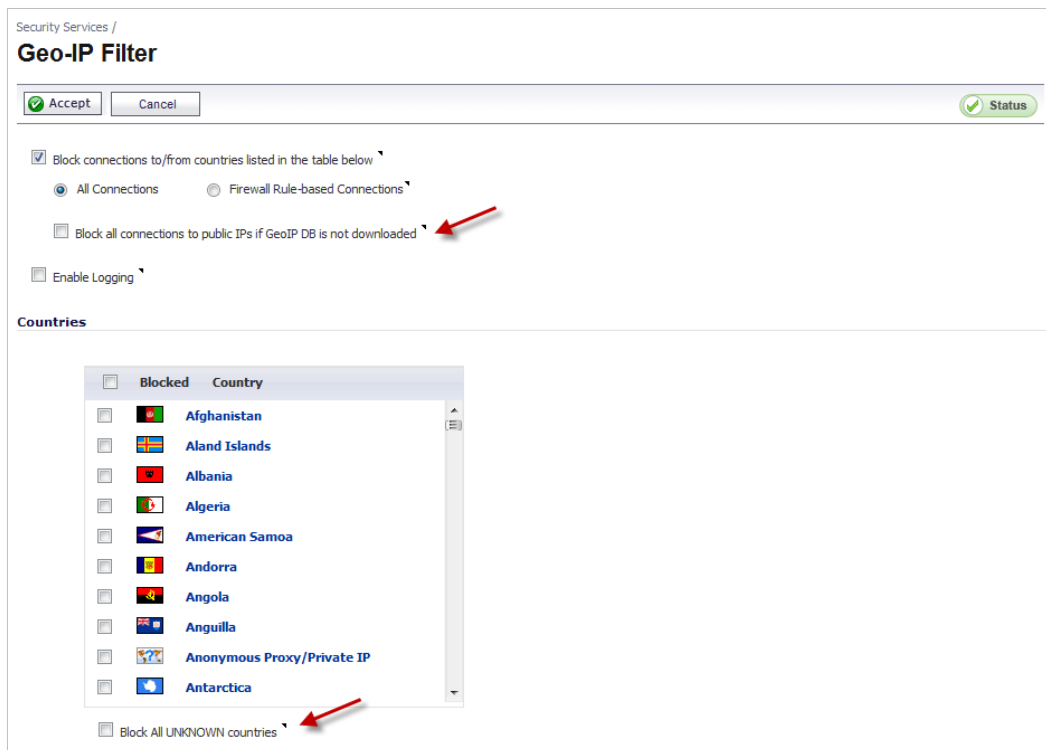
- **Botnet Filter**—The Botnet Filter feature is available as a free trial and can be activated by navigating to the **Security Services > Botnet Filter** page. The Botnet Filter page provides configuration options for **Block connections to/from Botnet Command and Control Services**, **Block all connections to public IPs if BOTNET DB is not downloaded**, **Enable Logging**, defining Botnet exclusion objects, and checking Botnet server lookup.

  Select the **Block all connections to public IPs if BOTNET DB is not downloaded** 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.

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

- **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.
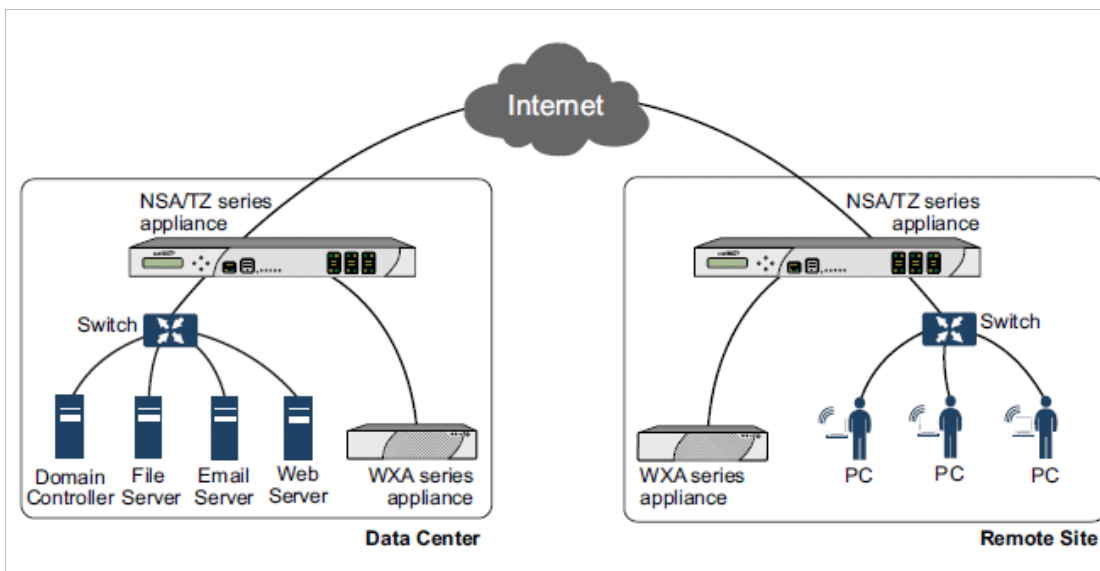
WXA 1.2 Support—SonicOS 5.8.1.12 and higher supports SonicWALL WXA 1.2, which contains several enhancements over WXA 1.1.1:

o **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.

o **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.

o **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*.

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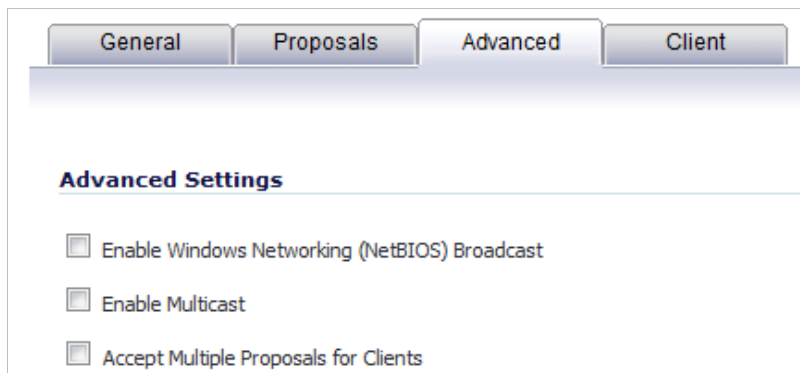
  The client policy is still strictly checked against the configured proposal in the Proposals tab, as with clients connecting with SonicWALL GVC. This option has no effect on GVC.

  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:

  o   If the offered algorithm matches one of the possible algorithms available in SonicOS.
  o   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.

- **Deep Packet Inspection of SSL encrypted data (DPI-SSL)**—Provides the ability to transparently decrypt HTTPS and other SSL-based traffic, scan it for threats using SonicWALL's Deep Packet Inspection technology, then re-encrypt (or optionally SSL-offload) the traffic and send it to its destination if no threats or vulnerabilities are found. This feature works for both client and server deployments. It provides additional security, application control, and data leakage prevention functionality for analyzing encrypted HTTPS and other SSL-based traffic. The following security services and features are capable of utilizing DPI-SSL: Gateway Anti-Virus, Gateway Anti-Spyware, Intrusion Prevention, Content Filtering, Application Control, Packet Monitor and Packet Mirror. DPI-SSL is supported on SonicWALL NSA models 240 and higher.

- **Gateway Anti-Virus Enhancements (Cloud GAV)**—The Cloud Gateway Anti-Virus feature introduces an advanced malware scanning solution that compliments and extends the existing Gateway AV scanning mechanisms present on SonicWALL firewalls to counter the continued growth in the number of malware samples in the wild. Cloud Gateway Anti-Virus expands the Reassembly Free Deep Packet Inspection engine capabilities by consulting with the data center based malware analysis servers. This approach keeps the foundation of RFDPI-based malware detection by providing a low-latency, real-time solution that is capable of scanning unlimited numbers of files of unlimited size on all protocols that are presently supported without adding any significant incremental processing overhead to the appliances themselves. With this additional layer of security, SonicWALL's Next Generation Firewalls are able to extend their current protection to cover multiple millions of pieces of malware.

- **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.

- **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**—SonicOS 5.8 provides VLAN support for SonicWALL NSA 220, NSA 250M, and TZ 215 series appliances, including wireless models.

- **SonicPoint Virtual Access Point Support**—Virtual Access Points (VAPs) are supported when one or more SonicWALL SonicPoints are connected to a SonicWALL NSA 220/250M/TZ 215 Series appliance.

- **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.

- **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.

SONICWALL®

- **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:

  o The Email Security Junk Store application can reside outside the Exchange Server system, such as on a remote server.

  o 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.

  o User-defined Allow and Deny Lists can be configured with FQDN and Range address objects in addition to Host objects.

  o 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).

  o A parameter to specify the Probe Response Timeout is available in the Anti-Spam > Settings page Advanced Options section. This option supports deployment scenarios where a longer timeout is needed to prevent a target from frequently being marked as Unavailable. The default value is 30 seconds.

- **Enhanced Connection Limiting**—Connection Limiting enhancements expand the original Connection Limiting feature which provided global control of the number of connections for each IP address. This enhancement is designed to increase the granularity of this kind of control so that the SonicWALL administrator can configure connection limitation more flexibly. Connection Limiting uses Firewall Access Rules and Policies to allow the administrator to choose which IP address, which service, and which traffic direction when configuring connection limiting.

- **Dynamic WAN Scheduling**—SonicOS 5.8 supports scheduling to control when Dynamic WAN clients can connect. A Dynamic WAN client connects to the WAN interface and obtains an IP address with the PPPoE, L2TP, or PPTP. This enhancement allows the administrator to bind a schedule object to Dynamic WAN clients so that they can connect when the schedule allows it and they are disconnected at the end of the configured schedule. In the SonicOS management interface, a Schedule option is available on the WAN interface configuration screen when one of the above protocols is selected for IP Assignment. Once a schedule is applied, a log event is recorded upon start and stop of the schedule.

- **NTLM Authentication with Mozilla Browsers**—As an enhancement to Single Sign-On, SonicOS can now use NTLM authentication to identify users who are browsing using Mozilla-based browsers (including Internet Explorer, Firefox, Chrome and Safari). NTLM is part of a browser authentication suite known as "Integrated Windows Security" and should be supported by all Mozilla-based browsers. It allows a direct authentication request from the SonicWALL appliance to the browser with no SSO agent involvement. NTLM authentication works with browsers on Windows, Linux and Mac PCs, and provides a mechanism to achieve Single Sign-On with Linux and Mac PCs that are not able to interoperate with the SSO agent.

- **Single Sign-On Import Users from LDAP Option**—An **Import from LDAP** button on the Users > Local Users page allows you to configure local users on the SonicWALL by retrieving the user names from your LDAP server. This allows SonicWALL user privileges to be granted upon successful LDAP authentication. For ease of use, options are provided to reduce the list to a manageable size and then select the users to import.

- **SSL VPN NetExtender Update**—This enhancement supports password change capability for SSL VPN users, along with various fixes. When the password expires, the user is prompted to change it when logging in via the NetExtender client or SSL VPN portal. It is supported for both local users and remote users (RADIUS and LDAP).

- **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:

    o **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.

    o **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."

    o **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.

    o **B2BUA Support Enhancements** – SIP Back-to-Back User Agent support is more efficient with various algorithm improvements.

    o **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.

    o **Graceful Shutdown** – Allows SIP Transformations to be disabled without requiring the firewall to be restarted or waiting for existing SIP endpoint and call state information to time out.

- **Management Traffic Only Option for Network Interfaces**—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.

Upgrading SonicOS Image Procedures

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

Obtaining the Latest SonicOS Image Version

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

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

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

Saving a Backup Copy of Your Configuration Preferences

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

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

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

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

    - VPN Keys

    - ARP Cache

    - DHCP Bindings

    - IKE Info

    - SonicPointN Diagnostics

    - Current users

    - Detail of users

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

Upgrading a SonicOS Image with Current Preferences

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

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

Upgrading a SonicOS Image with Factory Defaults

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

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

Importing Preferences to SonicOS 5.8

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

- NSA Series
- NSA E-Class Series
- TZ 215/210/205/200/105/100/190/180/170 Series
- PRO Series

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

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

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

Importing Preferences from SonicOS Standard to SonicOS 5.8 Enhanced

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

The SonicOS Standard to Enhanced Settings Converter is available at:
https://convert.global.sonicwall.com/

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

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

1. Log in to the management interface of your SonicOS Standard appliance, navigate to **System > Settings**, and save your network settings to a file on your management computer.
2. On the management computer, point your browser to https://convert.global.sonicwall.com/.
3. Click the **Settings Converter** button.
4. Log in using your MySonicWALL credentials and agree to the security statement.

   The source Standard Network Setting file must be uploaded to MySonicWALL as part of the conversion process. The Setting Conversion tool uses MySonicWALL authentication to secure private network settings. Users should be aware that SonicWALL will retain a copy of their network settings after the conversion process is complete.
5. Upload the source Standard Network Settings file:
   - Click **Browse**.
   - Navigate to and select the source SonicOS Standard Settings file.
   - Click **Upload**.
   - Click the right arrow to proceed.
6. Review the source SonicOS Standard Settings Summary page.

   This page displays useful network settings information contained in the uploaded source Network Settings file. For testing purposes, the LAN IP and subnet mask of the appliance can be changed on this page in order to deploy it in a testing environment.
   - (Optional) Change the LAN IP address and subnet mask of the source appliance to that of the target appliance.
   - Click the right arrow to proceed.
7. Select the target SonicWALL appliance for the Enhanced deployment from the available list.

   SonicOS Enhanced is configured differently on various SonicWALL appliances, mostly to support different interface numbers. As such, the converted Enhanced Network Settings file must be customized to the appliance targeted for deployment.
8. Complete the conversion by clicking the right arrow to proceed.
9. Optionally click the **Warnings** link to view any differences in the settings created for the target appliance.
10. Click the **Download** button, select Save to Disk, and click OK to save the new target SonicOS Enhanced Network Settings file to your management computer.
11. Log in to the management interface for your SonicWALL appliance.
12. Navigate to **System > Settings**, and click the **Import Settings** button to import the converted settings to your appliance.

Support Matrix for Importing Preferences

Legend:

- **Y** — Supported
- **N** — Unsupported. While importing the settings file may be successful, firewall limitations may result in the removal of items such as DHCP scopes, VPN settings, etc.
- **B** — Portshield interfaces prior to SonicOS 5.x are not supported.
- **C** — Configuration information from extra interfaces will be removed. NAT policies, Firewall access rules, and other interface-dependent configuration will also be removed.
- **D** — When importing from non-SonicOS 5.x devices, the X2 interface will be configured in the DMZ zone.
- **E** — VLANs created as sub-interfaces of the fiber interfaces will be renamed.

DESTINATION FIREWALLS (columns): PRO 1250, PRO 2040, PRO 3060, PRO 4060, PRO 4100, PRO 5060, TZ 170, TZ 170W, TZ 170SP, TZ 170SPW, TZ 180, TZ 180W, TZ 190, TZ 190W, TZ 100W/TZ 200W, TZ 105/TZ 205, TZ 105W/TZ 205W, TZ 210, TZ 210W, TZ 215, TZ 215W, NSA 220, NSA 220W, NSA 240, NSA 250M, NSA 250MW, NSA 2400, NSA 2400MX, NSA 3500, NSA 4500, NSA 5000, NSA E5500, NSA E6500, NSA E7500, NSA E8500, NSA E8510

Source firewalls (rows): PRO 1250, PRO 2040, PRO 3060, PRO 4060, PRO 4100, PRO 5060, TZ 170, TZ 170W, TZ 170SP, TZ 170SPW, TZ 180, TZ 180W, TZ 190, TZ 190W, TZ 100W/TZ 200, TZ 105/TZ 205, TZ 105W/TZ 205W, TZ 210, TZ 210W, TZ 215, TZ 215W, NSA 220, NSA 220W, NSA 240, NSA 250M, NSA 250MW, NSA 2400, NSA 2400MX, NSA 3500, NSA 4500, NSA 5000, NSA E5500, NSA E6500, NSA E7500, NSA E8500, NSA E8510

Using SafeMode to Upgrade Firmware

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

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

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

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

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

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.

_____

Last updated: 5/8/2014