

SONICWALL[®]

SonicOS 8

Monitor

Administration Guide

Contents

About SonicOS	7
Working with SonicOS	7
SonicOS Workflow	8
How to Use the SonicOS Administration Guides	9
Guide Conventions	11
Dashboard	12
System	13
Device	14
Summary	15
Traffic Distribution	16
Top Users	17
Insights	18
Observed Threats	19
Top Countries	20
Security Services	22
Network	23
Top Applications	24
Top Addresses	25
Top Users	26
Top Website Ratings	27
Threat	27
Top Intrusion	27
Top Virus	28
Top Spyware	28
Top Botnet	29
DNS Filtering	29
Access Points	31
Feature Limitations	32
Access Point Snapshot	32
Client Association	32
Real-Time Bandwidth	32
Client Report	33
OS Type	33
Radio	33

Top Client	33
Real-Time Client Monitor	34
Client Report and Client Monitor Filtering	34
Capture ATP	35
Topology	37
Managing the Topology View	37
Managing Access Points in the Topology View	38
Editing an Access Point	38
Showing Statistics	38
Monitoring Status on an Access Point	39
Deleting an Access Point	39
Real-Time Charts	40
System Monitor	41
Using the Toolbar	43
Common Features	43
Legends	44
Tooltips	44
Changing Chart Format	45
Selecting IPv6/IPv4	46
Current, Minimum, Maximum Display	46
Multicore Monitor	46
Options	47
Applications Bandwidth	47
Options	48
Interface Usage	48
Options	49
Packet Rate Monitor	49
Packet Size	51
Connection Usage	51
Active Connection Count	52
Protocol Monitor	54
Enabling the Protocol Monitor	56
Using the Toolbar	57
Using Per-Chart Viewing Options	58
Legends	58
Tooltips	58
User Monitor	60
Bandwidth Monitor	62

Enabling BWM Monitor	63
AppFlow	64
AppFlow Report	65
Applications	66
Users	67
IP Addresses	68
Viruses	68
Intrusions	69
Spyware	69
Locations	70
Botnets	70
Web Categories	71
AppFlow Monitor	72
Applications	73
Users	74
Web Activity	74
Initiator IPs	75
Responder IPs	75
Threats	76
VoIP	76
VPN	77
Devices	77
Contents	78
Policies	78
CTA Report	79
Generate & Download CTA Report	79
Advanced Options	80
Completed Reports	81
SD-WAN	82
Monitoring SD-WAN	83
Viewing SD-WAN Rules Connections	84
Logs	86
System Logs	87
Viewing System Logs	87
System Log Functions	88

Display Options	90
Filtering the View	92
Auditing Logs	94
What is Configuration Auditing	94
Benefits of Configuration Auditing	94
What Information is Recorded	95
What Information is Not Recorded	95
Audit Recording in High Availability Configurations	95
Modifying and Supplementing Configuration Auditing	96
SNMP Trap Control	96
E-CLI Commands	96
Auditing Record Storage and Persistence	96
Managing the Audit Logs Table	97
Viewing Auditing Logs	97
Manually Emailing Auditing Logs	98
Exporting Auditing Logs	98
Refreshing the Auditing Logs	98
Displaying the Auditing Logs on the console	99
Auditing All Parameters During Addition	99
Threat Logs	100
Viewing Threat Logs	100
Threat Log Functions	100
Display Options	101
Tools and Monitor	104
Using Packet Monitor	105
Benefits of Packet Monitor	106
How Does Packet Monitor Work?	106
Supported Packet Types	107
Configuring Packet Monitor	107
Configuring General Settings	108
Monitoring Captured Packets	118
Viewing Packet Monitoring Statistics	119
Viewing Connections	124
Searching the Connections	125
Filtering the Connection Log	125
Connections Log Functions	126
Monitoring Core 0 Processes	127

Using Packet Replay	128
Single Packets	128
Packet Crafting	128
Packet Buffer	130
Replay Pcap File	130
Replaying an IP Pcap File	130
Replaying a MAC Pcap File	131
Captured Packets	131
About Captured Packets	132
Packet Detail	133
Hex Dump	133
SonicWall Support	134
About This Document	135

About SonicOS

This guide is a part of the SonicOS collection of administrative guides that describe how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators with the management interface, API (Application Program Interface), and Command Line Interface (CLI) for firewall configuration. You can configure and manage your firewall by setting objects to secure and protect the network services, manage traffic, and provide the desired level of network service. This guide focuses on configuring the monitor settings on your SonicWall security appliance.

Topics:

- [Working with SonicOS](#)
- [SonicOS Workflow](#)
- [How to Use the SonicOS Administration Guides](#)
- [Guide Conventions](#)

Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and outside threats to your network. SonicOS functions in conjunction with SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices such as access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration, and diagnostics.

- *Classic Mode* is more consistent with earlier releases of SonicOS; in that you need to develop individual policies and actions for specific security services. Classic Mode has a redesigned interface.

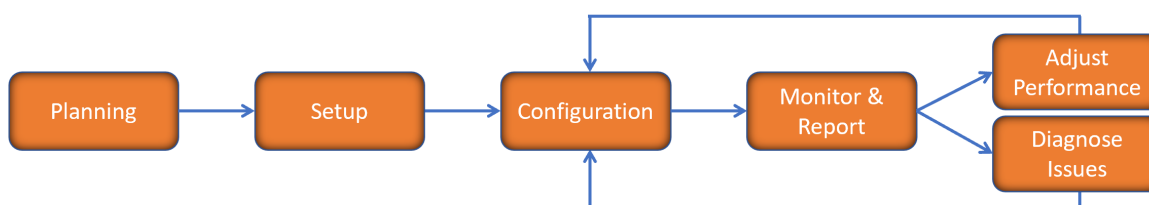
This following table identifies which of these modes can be used on various SonicWall firewalls:

Firewall Type	Classic Mode	Comments
TZ Series	yes	The entry level TZ Series, also known as desktop firewalls, delivers revamped features such as 5G readiness, better connectivity options, improved threat protection, SSL and decryption performance that addresses HTTPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support. It provides advanced networking and security features, like the multi-engine Capture Advanced Threat Protection (ATP) cloud-based sandbox service with patent-pending Real-Time Deep Memory Inspection (RTDMI™).

In addition to the management interface, SonicOS also has a full-featured API and a command-line interface (CLI) to manage the firewalls.

SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.



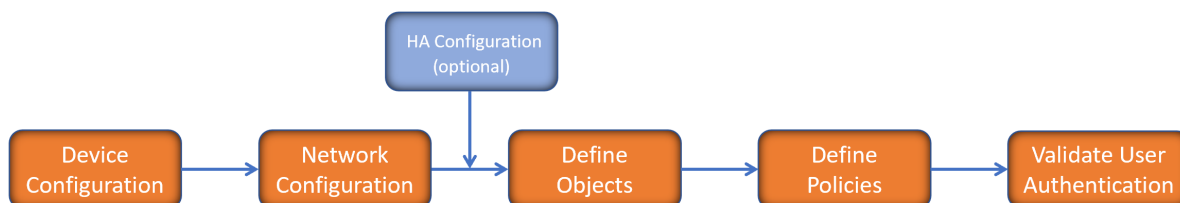
You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing [product information](#) and [solutions](#). After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The [Getting Started Guides](#) for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken

into the key command sets and features. Some documents may be used for all solutions, but others may be used only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the [specific Administration Guide for a SonicOS feature](#) for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

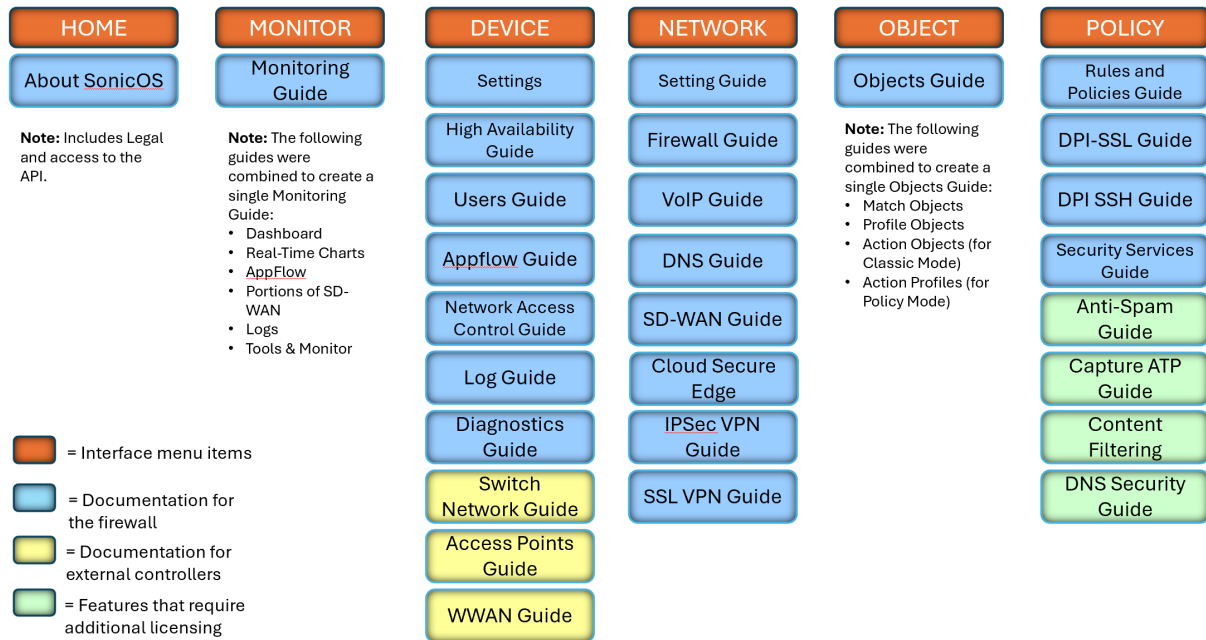


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the [SonicOS 8 Monitor Guide](#) and the [SonicOS 8 Objects Guide](#) which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicOS management interface.



The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the [Technical Documentation portal](#).

Guide Conventions

These text conventions are used in this guide:

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

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

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

Convention	Description
Bold text	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Function Menu group > Menu item	Indicates a multiple step menu choice on the user interface. For example, NETWORK System > Interfaces means to select the NETWORK functions at the top of the window, then click on System in the left navigation menu to open the menu group (if needed) and select Interfaces to display the page.
Code	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<Variable>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment serialnumber=<your serial number> , replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004 .
Italics	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

DASHBOARD

The Dashboard feature is a key function of SonicWall SonicOS, where you can quickly see if anything in your network is impacting performance. This part of the guide describes the elements of the different views and how they can be used to drill down to more detailed information. The Dashboard can be your starting place for monitoring performance. Symbols and colors are used to indicate whether things are operational, need attention, or if a problem needs to be resolved. Each view provides visibility into the health of the associated network elements.

Topics:

- [System](#)
- [Access Points](#)
- [Capture ATP](#)
- [Topology](#)

① **NOTE:** The images in this document may not be an exact match of what you see when you manage your firewall. The interface you see reflects the type of firewall you chose and the features you configured and licensed. Specific differences are noted when possible.


System

The **System** view of the SonicOS Dashboard provides a summary of the information that the firewall. The navigation path for the **System** view is **HOME > Dashboard > System**.

The screenshot shows the SonicOS Dashboard in the **System** view. The top navigation bar includes tabs for **Device**, **Summary**, **Security Services**, **Network**, **Threat**, and **DNS Filtering**. The main content area is divided into several panels:

- GENERAL:** Displays device information such as Name (00401039CD67), Friendly Name (SONICWALL NSv 470), Unified Policy (Yes), Product Code (27094), GUID (EC2AC9D8-23DE-1B0C-B995-80A916CE38D5), Serial Number (00401039CD67), Authentication Code (ZVDR-KJNL), Firmware Version (SonicOSX 7.1.0-6068), ROM Version (15.0.0.0), System Time (09/12/2022 09:45:10), Up Time (6 Days 13:08:51), Primary WAN (X1), and Connections (Peak: 635 Current: 592 Max: 1250000).
- SYSTEM STATUS:** Shows two line graphs for Management Plane and Data Plane, both ranging from 0% to 100% over a 60-second period.
- SYSTEM USAGE:** Displays 150.52 Kbps Bandwidth and 587 Active Connections.
- NETWORK INTERFACES:** Lists interfaces with their status and IP addresses: ZTNA Z0 (100.64.250.3), LAN X0 (20.0.163.237), WAN X1 (20.2.111.80), and WIREGUARD WG0 (192.168.2.1).
- SERVICES:** A grid of service status indicators:
 - SECURITY SERVICES:** Gateway Anti-Virus (Licensed, On), Anti-Spyware (On), Intrusion Prevention & Detection (On), Geo-IP Filter (On), Botnet Filter (On), Application Control (On), DPI SSL (Off), and DPI SSH (Off).
 - CONTENT FILTERING:** Content Filter (Licensed, On).
 - DNS SECURITY SERVICE:** DNS Security (License?, Off).
 - ENDPOINT SECURITY:** Capture Client (License?, Off).
 - ADVANCED PROTECTION:** Capture ATP (License?, Off).
- HIGH AVAILABILITY:** Shows Mode (None) and various states (Device State, Peer Device State, Stateful Sync, Settings Sync) as Not Configured.

The **System** view offers a high level view of the system performance. You can select different tabs for different types of summaries. They include **Device**, **Summary**, **Security Services**, **Network**, **Threat**, and **DNS Filtering**. Each pane on the tab represents a specific feature being tracked. If you see issues that need more investigation,

you can drill down on the options icon, , in the upper right corner. This takes you to other reports that can help you narrow the source of the issue.

Think of the **System** view as the starting point for most tasks. From the **System** page, you can select one of the tabs to see the data from a specific point of view

Topics:

- [Device](#)
- [Summary](#)
- [Security Services](#)
- [Network](#)
- [Threat](#)
- [DNS Filtering](#)

❗ | **IMPORTANT:** Zero Touch is not supported in SonicOS when implemented with on-premises Analytics.

For more information about the **System** option, refer to [SonicOS 8 System Administration Guide](#).

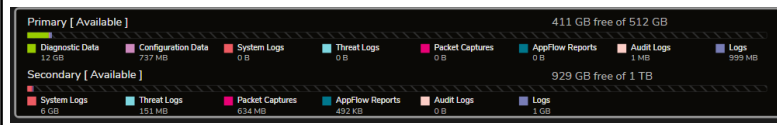
Device

HOME | Dashboard > System | Device displays the relevant information for the unit connected to your system. You have a physical view of the firewall at the top with window, followed by panes that summarize various information categories.


The screenshot displays the SonicOS 8 Device page for a SonicWall NSsp 10700. The top section shows a physical view of the firewall with various ports and storage options. Below this, the page is divided into several sections:

- GENERAL:** Displays device information such as Name (2CB8EDA31565), Product Code (Z3205), and Firmware Version (SonicOS 7.1.1-7037).
- SYSTEM STATUS:** Shows performance metrics for the Management Plane and Data Plane, along with a graph of bandwidth usage (539.47 Kbps) and active connections (30).
- SYSTEM USAGE:** Displays the current system usage, including bandwidth and active connections.
- NETWORK INTERFACES:** Lists network interfaces (LAN, WAN) and their status, including IP addresses and link status.
- SERVICES:** Lists various security services and their status, including Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention & Detection, Geo-IP Filter, Botnet Filter, Application Control, DPI SSL, DPI SSH, Content Filtering, DNS Security Service, Anti-Spam Service, Endpoint Security, and Advanced Protection.
- HIGH AVAILABILITY:** Shows the high availability configuration, including Mode (None), Device State (Not Configured), and Peer Device State (Not Configured).

❗ | **NOTE:** The image above illustrates and NSsp 10700 with the Storage feature. Your firewall view may vary slightly depending on the features you enabled and the type of firewall you have. For example, if you have extra storage, you can select **Storage** option, and see how the storage is distributed among the various logs as shown below.

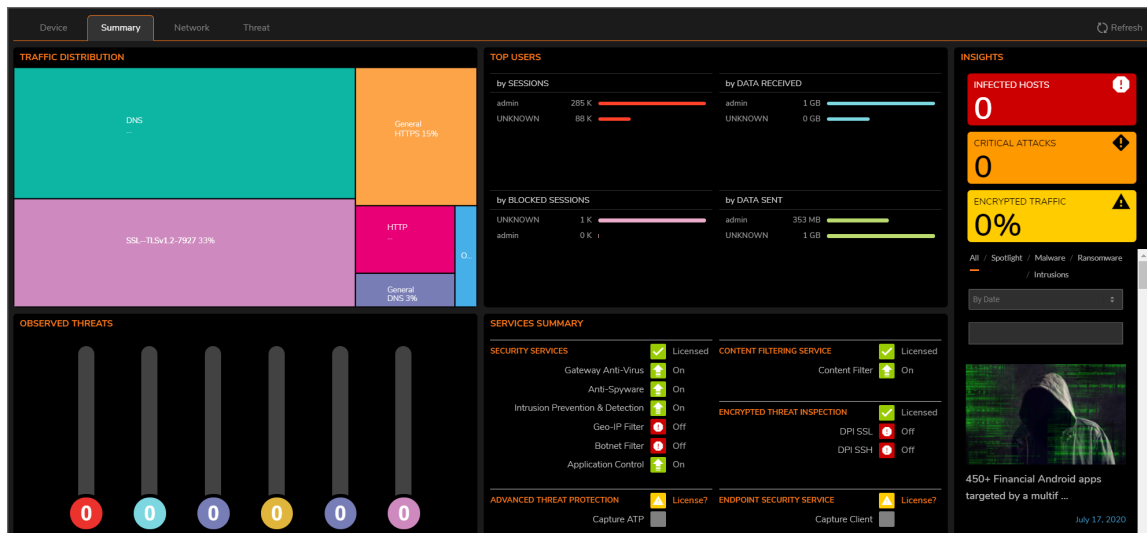




If you see issues on the dashboard that need more investigation, you can drill down on the options icon, , in the upper right corner. This takes you to other reports that can help you narrow the source of the issue.

Summary

The System Summary —located at **HOME | Dashboard > System > Summary**, provides a high-level view of the status of your security infrastructure. It summarizes the activity in easy-to-read, color-coded indicators. You can review the Summary and see at-a-glance when any issues might need investigating.



The **Summary** shows your devices and a representation of the traffic being generated. It allows you to view the devices in a geographical view using a map that you can zoom in and out of. The devices are marked on the map.

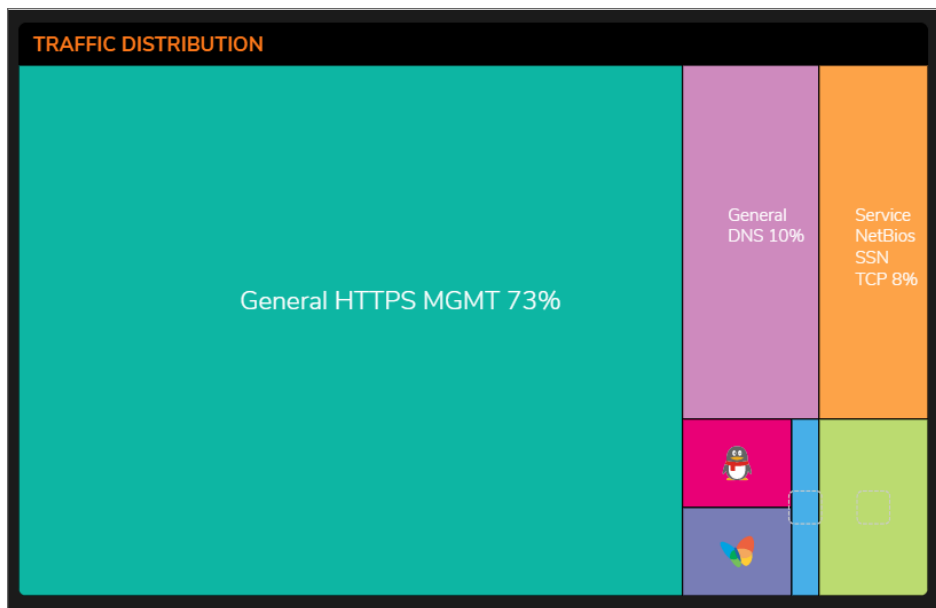
The following table describes the components that make up the **System Summary**.

SYSTEM SUMMARY

Feature	Description
Traffic Distribution	Displays all traffic within your infrastructure including threats and their locations.
Top Users	Provides data as it relates to the users connected to the system.
Insights	Provides a high-level view of the overall status of your security infrastructure.
Observed Threats	Tracks the number of system connections reporting triggered threats.
Top Countries	Show Top Countries sorted by Sessions

Traffic Distribution

The **TRAFFIC DISTRIBUTION** window displays all traffic within your infrastructure including threats and their locations. The threats are visually placed on the global map. You can use the roller on your mouse to zoom in or zoom out on a threat. This kind of data allows you to perform a deep dive on all the information available to you.



TRAFFIC DISTRIBUTION shows your devices and a representation of all traffic being generated. This window allows you to view the devices with a geographical view using a map that you can zoom in and out of. The devices are marked on the map.

This map provides PRIVATE IPs, FIREWALLS, THREATS, INCOMING TRAFFIC, and OUTGOING TRAFFIC information.

You can drill-down for more information on the TRAFFIC MAP segment as well. Use the mouse wheel to Zoom in and out on the global map or use the vertical + and - slider on the left side of the map. Click the flags and icons on the map to drill-down for additional details.

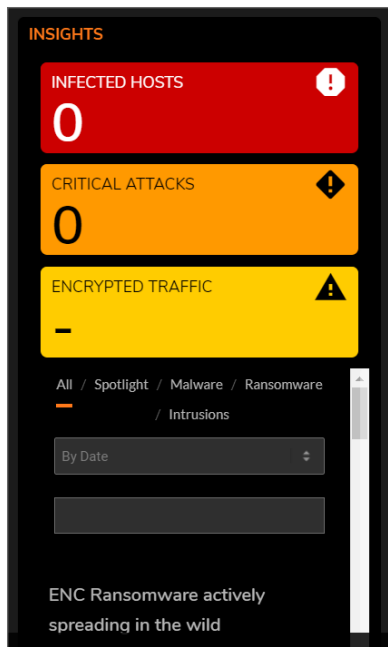
Top Users

The **Top Users** report window provides data as it relates to the users connected to the system. You can track user-level transactions and activities by filtering on several different options, including sessions, bytes received, bytes sent, and bytes blocked.



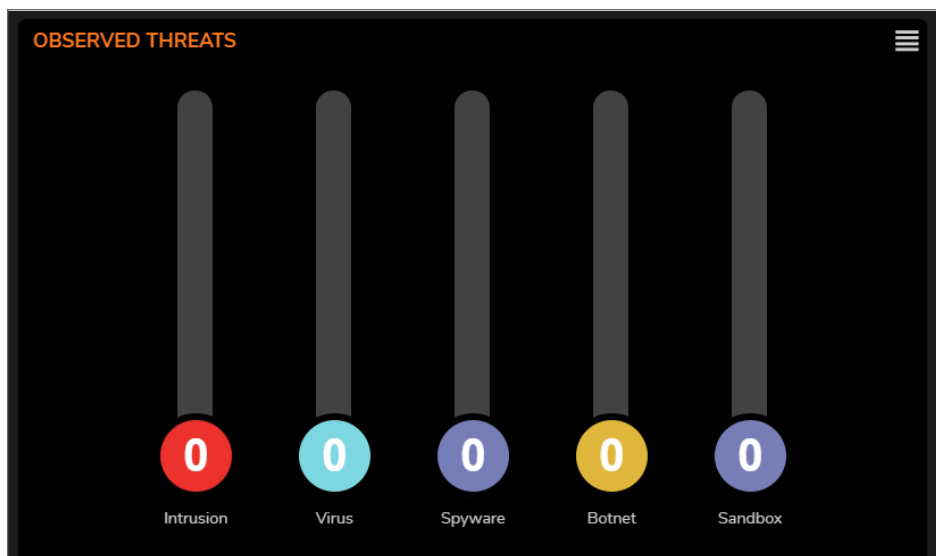
Insights

The Insights window provides a high-level view of the overall status of your security infrastructure. This window summarizes the activity in easy-to-read, color-coded indicators. You can review the Insights and see at-a-glance whether any issues need investigation, as well as additional filtering through spotlighting, malware, ransomware, intrusions, or all the above.



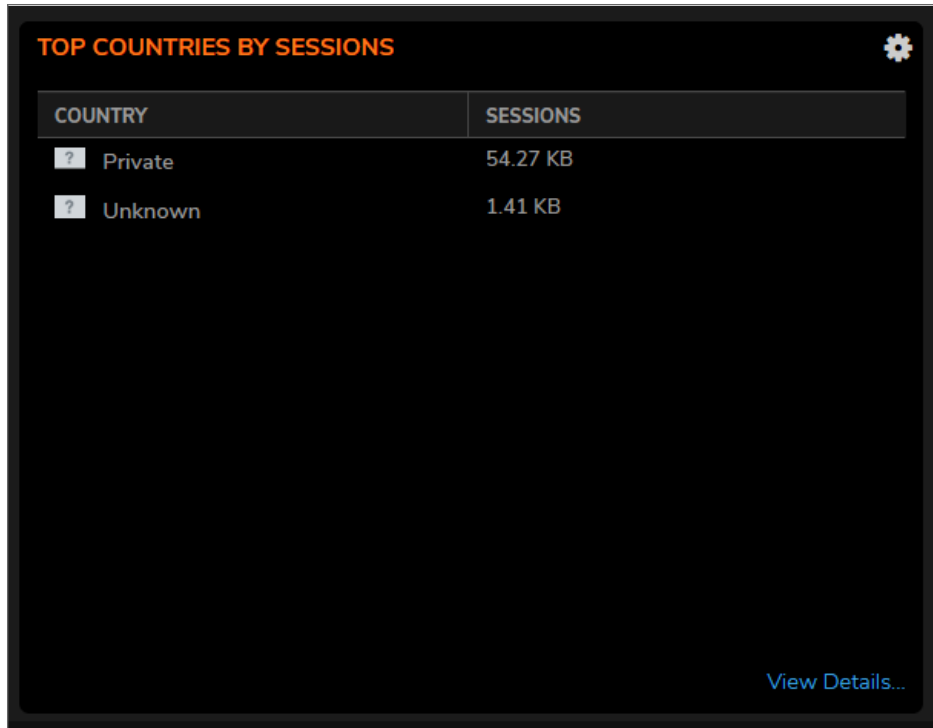
Observed Threats

Observed Threats tracks the number of system connections reporting triggered threats. The default view is Total connections, but you can filter with top intrusions, viruses, spyware, and botnets in the Threat drop-down lists. Navigate to **HOME | Dashboard > System > Threat** to see the various threat reports available. Click the **View Details** icon in each window to expand the available filtering options.



Top Countries

The **Top Countries by Sessions** report provides data as it relates to the country locations connected to the system.

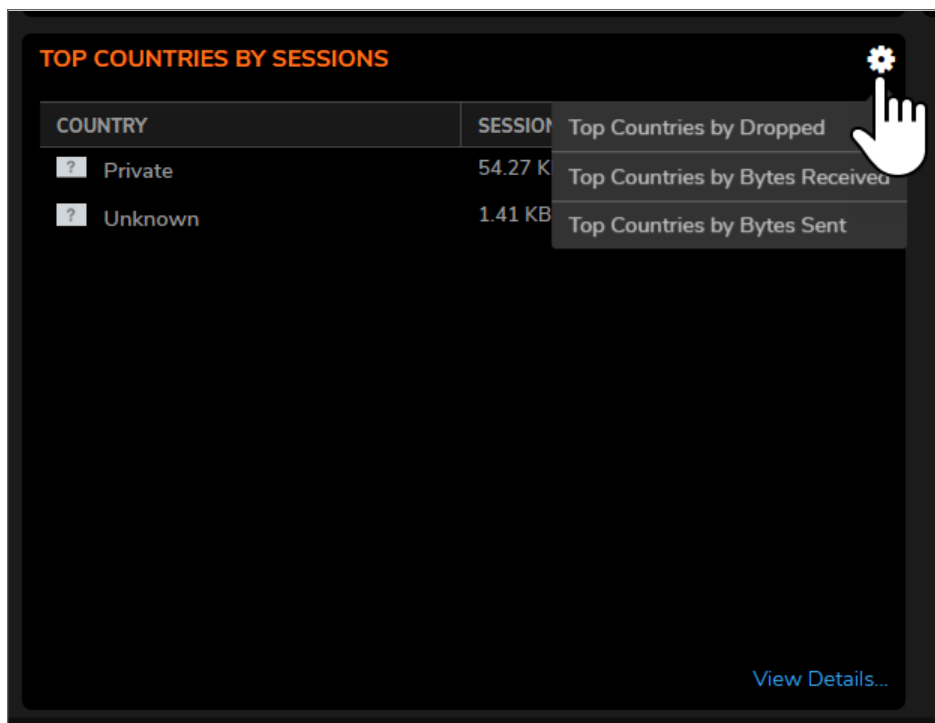


COUNTRY	SESSIONS
? Private	54.27 KB
? Unknown	1.41 KB

[View Details...](#)

You can track location-level transactions and activities by filtering on several different options including **Top Countries by:**

- **Dropped**
- **Bytes Received**
- **Bytes Sent**



Click **View Details** to see complete reporting on all Countries located in **MONITOR | AppFlow > AppFlow Report | Location**.

Dropped

The **Dropped** filter indicates the total number of packets or bytes sent (in the Transmit table) or received (in the Received table) on that interface that were dropped. If the interface is saturated, this number increments one time for every packet that has been dropped by the server mechanism.

Bytes Received

The Bytes Received filter reports the total bytes received from the host. The bytes received together with the bytes sent represent the total data transfer on the communications links between the server and the host computer.

Bytes Sent

The Bytes Sent filter reports the total bytes sent from the host. The bytes received together with the bytes sent represent the total data transfer on the communications links between the server and the host computer.

Security Services

Security Services allows the SonicWall firewall to access the Internet through a proxy server to download signatures to avoid compromising privacy. On the Dashboard, **HOME | Dashboard > System | Security Services** summarizes the status of the Security Services that you enabled on your firewall.

The screenshot displays the 'Security Services' dashboard with the following sections:

- LICENSES**: Shows Sync State as Successful, Last successful sync time (12/08/2023 15:45 hrs), Last LM contact (12/08/2023 16:19 hrs), and a License Summary link.
- GATEWAY ANTI-VIRUS**: Enabled. Signature Database Downloaded. On-box Database Timestamp: 12/07/2023 06:09 hrs. Back-end Database Timestamp: 12/07/2023 06:09 hrs. Last checked: 12/08/2023 15:45 hrs. License Expiration: 02/08/2026 12:00 hrs.
- CLOUD ANTI-VIRUS**: Enabled. Last checked: 12/08/2023 15:45 hrs. License Expiration: 02/08/2026 12:00 hrs.
- CAPTURE ATP**: Disabled. License Expiration: 02/08/2026 12:00 hrs.
- ANTI-SPYWARE**: Enabled. Signature Database Downloaded. On-box Database Timestamp: 12/06/2023 05:15 hrs. Back-end Database Timestamp: 12/06/2023 05:15 hrs. Last checked: 12/08/2023 15:45 hrs. License Expiration: 02/08/2026 12:00 hrs.
- INTRUSION PREVENTION AND DETECTION**: Enabled. Signature Database Downloaded. On-box Database Timestamp: 12/07/2023 06:54 hrs. Back-end Database Timestamp: 12/07/2023 06:54 hrs. Last checked: 12/08/2023 15:45 hrs. License Expiration: 02/08/2026 12:00 hrs.
- CONTENT FILTER**: Enabled. Server Status Connected. License Expiration: 02/08/2026 12:00 hrs.
- APPLICATION CONTROL**: Disabled. Signature Database Downloaded. On-box Database Timestamp: 12/07/2023 06:54 hrs. Back-end Database Timestamp: 12/07/2023 06:54 hrs. Last checked: 12/08/2023 15:45 hrs. License Expiration: 02/08/2026 12:00 hrs.
- BOTNET FILTER**: Disabled. Signature Database (0.0.0.0) Downloaded. On-box Database Timestamp: -. Back-end Database Timestamp: -. Last Successful Sync Time: -. License Expiration: 02/08/2026 12:00 hrs.
- GEO-IP FILTER**: Disabled. Signature Database (0.0.0.0) Downloaded. On-box Database Timestamp: -. Back-end Database Timestamp: -. Last Successful Sync Time: -. License Expiration: 01/01/2040 12:00 hrs.
- DNS SECURITY**: License Expiration: 02/08/2026 12:00 hrs.

Each of the panes represents a specific service and provides data on each. Review the table below for the specifics.

NOTE: You may not see all the options represented here; what you see depends on the options you enabled.

The **Licenses** pane show the **Sync State** of the Security Services license. Last successful sync time and last contact to License Manager provide additional information. Click the **License Summary** to see your license detail. You can also refresh your licenses from this pane.

These features offer a different set of information:

- **Gateway Anti-Virus**
- **Intrusion Prevention and Detection**
- **Botnet Filter**
- **Geo-IP Filter**
- **Anti-Spyware**
- **Application Control**

From these panes, you can enable and refresh the signatures. You can see the on-box and back-end database time stamps, along with when the signature was last checked and when the license expires. Note that when an option is not enabled, like with the Botnet Filter and Geo-IP Filter in the image above, the refresh option is not visible.

On the **Cloud Anti-Virus** pane, you can enable or disable the feature. You can also see when the license was last checked and when it expires.

Capture ATP lets you enable or disable the license and check the license expiration.

You can enable or disable the Content Filter signatures on the **Content Filter** pane. It shows Server Status and allows you to refresh the connection. you can also see the license expiration.

The **DNS Security** pane show when that signature expires.

Network

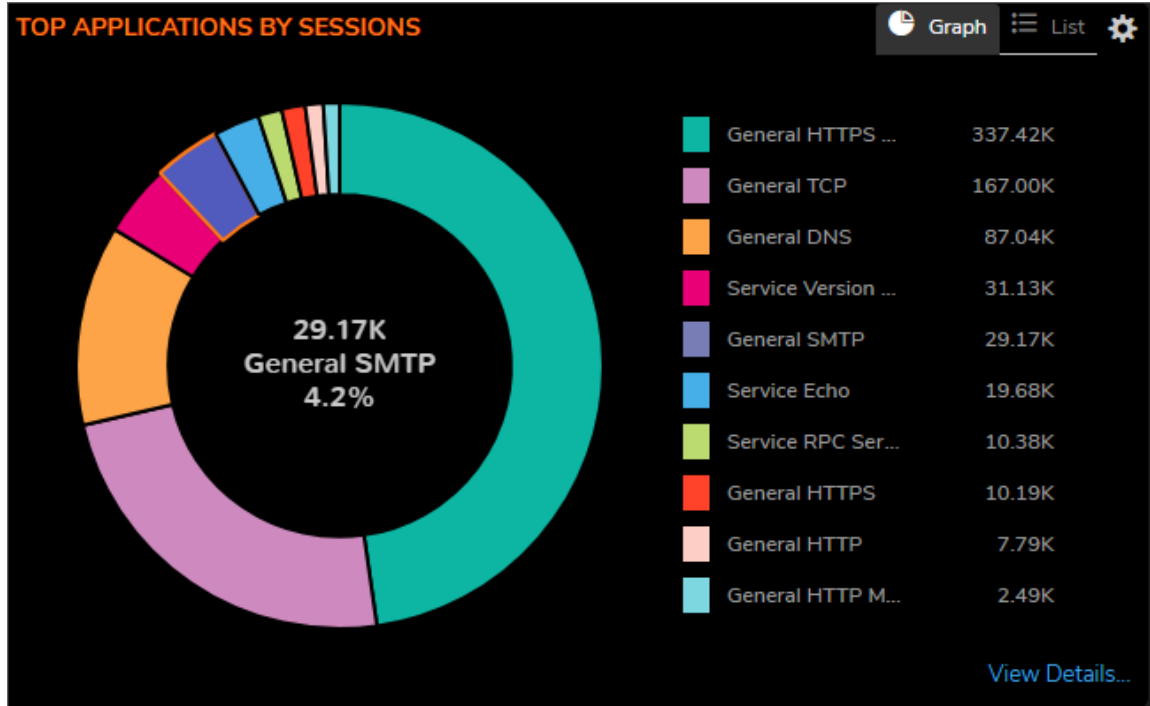
The **Network** view provides session reporting windows that display the top Applications, Addresses, Users, Website Ratings, Countries, and so on.

Topics:

- [Top Applications](#)
- [Top Addresses](#)
- [Top Users](#)
- [Top Website Ratings](#)

Top Applications

The **Top Applications** window summarizes all applications flowing through the firewall



You can view information in **Graph** form or you can select the **List** option.

You can track application-level transactions and activities by filtering on several different options. Click on the setting icon to see the filtering options, including **Top Applications by**:

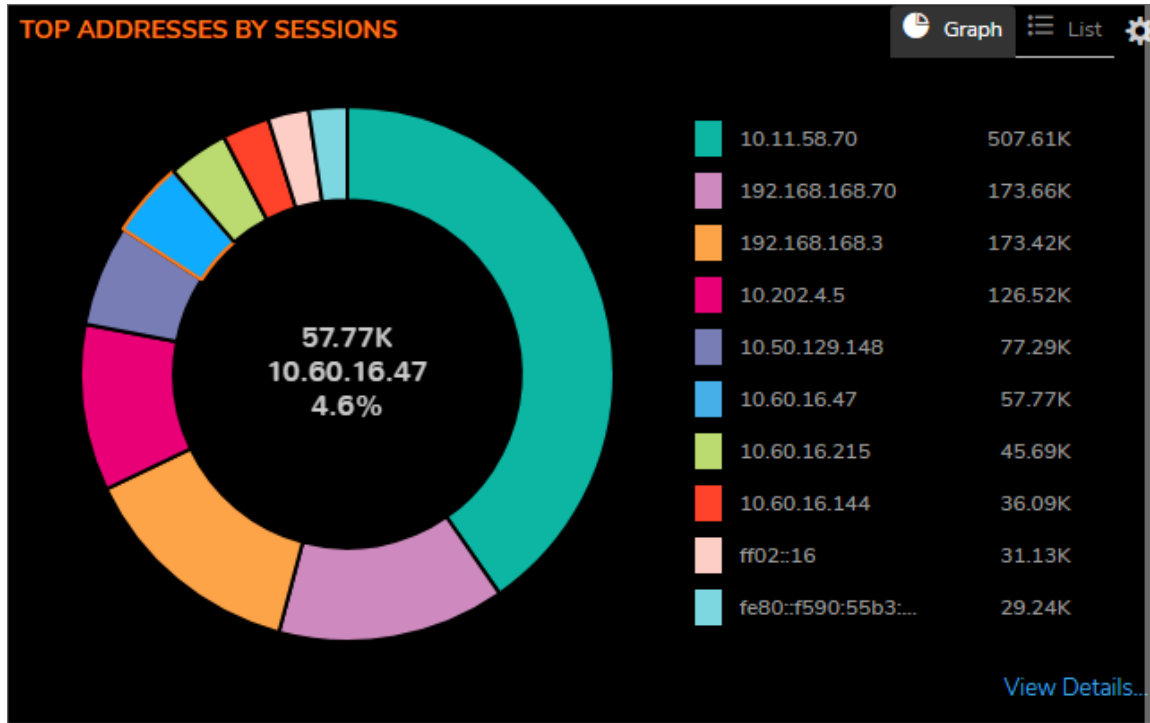
- By data received
- By data sent
- By access rules block
- By app rules block
- By location block
- By botnet block
- By virus
- By intrusion
- By spyware

For more information, you can click on **View Details...**:

- If operating in Classic Mode, it goes to **MONITOR | Logs > Threat Logs**.

Top Addresses

The **Top Addresses by Sessions** report provides data as it relates to the IP addresses connected to the system.



Click on the **List** option to see a list view of the data.

You can track IP address-level transactions and activities by filtering on several different options. Click on the setting icon to see the filtering options, including **Top Addresses by**:

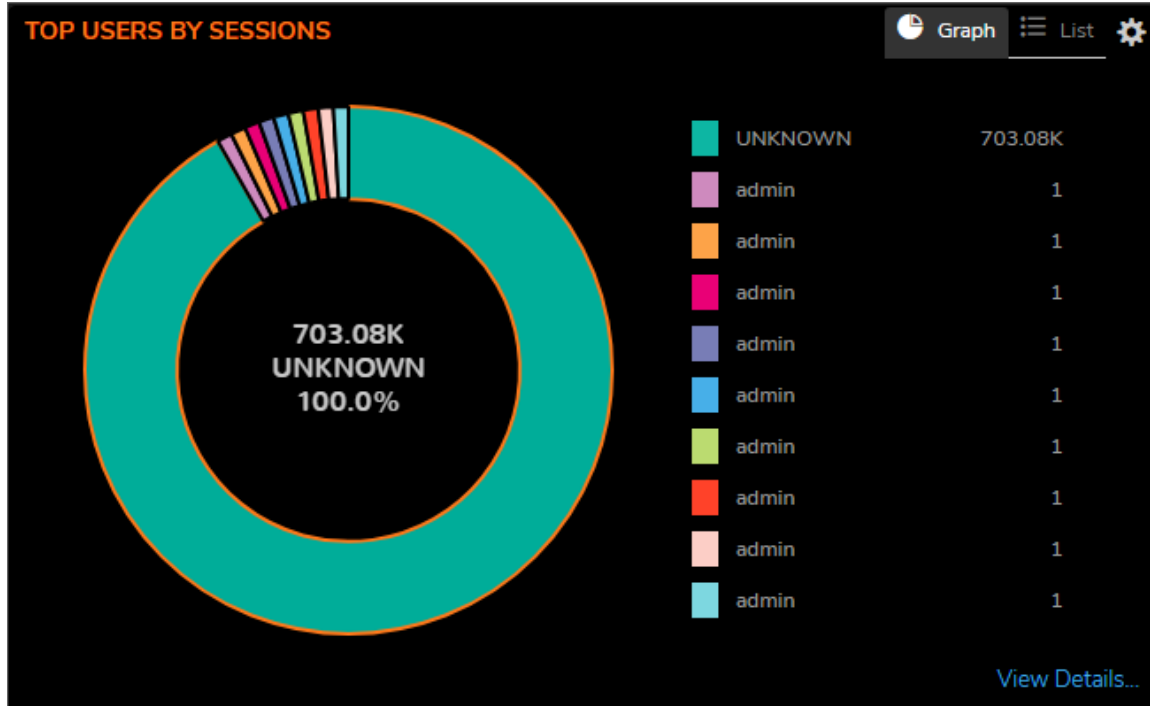
- Blocked
- Virus
- Spyware
- Intrusion
- Botnet block
- Data received
- Data sent

For more information, you can click on **View Details...**:

- If operating in Classic Mode, it goes to **MONITOR | Logs > Threat Logs**.

Top Users

The **Top Users by Sessions** report provides data as it relates to the top users connected to the system.



Click on the **List** option to see a list view of the data.

You can track top users and activities by filtering on several different options. Click on the setting icon to see the filtering options, including **Top Users**

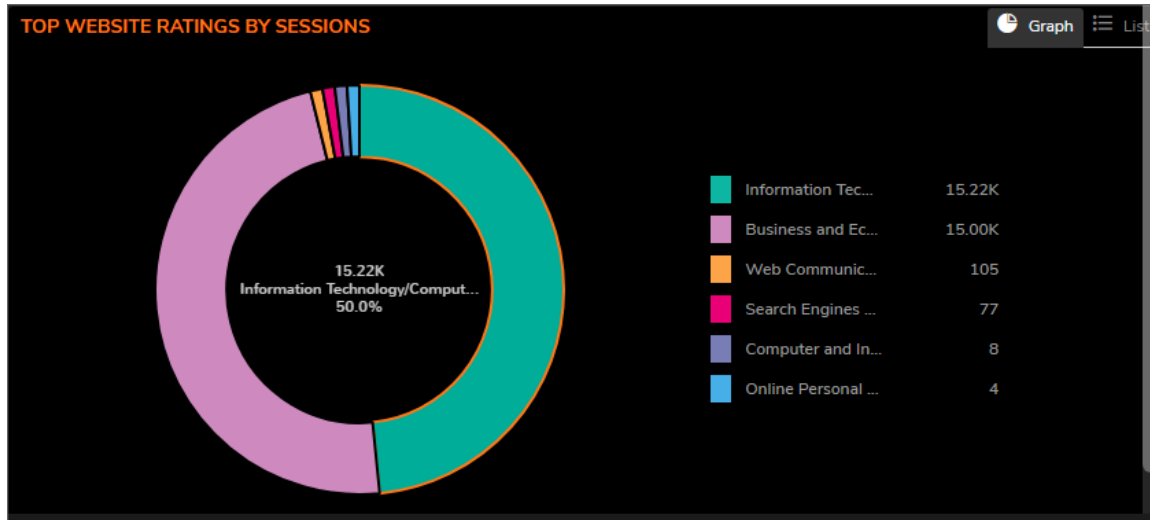
- Blocked
- Virus
- Spyware
- Intrusion
- Botnet block
- Data received
- Data sent

For more information, you can click on **View Details...**:

- If operating in Classic Mode, it goes to **MONITOR | Logs > Threat Logs**.

Top Website Ratings

The **Top Website Ratings by Sessions** report provides data as it relates to the URLs processed through the system.



You can view information in **Graph** form or you can select the **List** option.

For more information, you can click on **View Details...**:

- If operating in Classic Mode, it goes to **MONITOR | Logs > Threat Logs**.

Threat

These reports track the number of connections that have been impacted by threats. You can also filter on other options listed in the drop-down menus.

Topics:

- [Top Intrusion](#)
- [Top Virus](#)
- [Top Spyware](#)
- [Top Botnet](#)

Top Intrusion

The **Top Intrusion by Sessions** report provides data as it relates to intrusions processed through the system. You can select a **Graph** view or a **List** view by clicking the appropriate icon.

You can track intrusion-level transactions and activities by filtering on several different options including **Top Intrusion by**:

- Count
- Percentage

For more information, you can click on **View Details...**:

- If operating in Classic Mode, it goes to **MONITOR | Logs > Threat Logs**.

Top Virus

The **Top Virus by Sessions** report provides data as it relates to viral threats processed through the system. You can select a **Graph** view or a **List** view by clicking the appropriate icon.

You can track virus-level transactions and activities by filtering on several different options including **Top Virus by**:

- Count
- Percentage

For more information, you can click on **View Details...**:

- If operating in Classic Mode, it goes to **MONITOR | Logs > Threat Logs**.

Top Spyware

The **Top Spyware by Sessions** report provides data as it relates to spyware threats processed through the system. You can select a **Graph** view or a **List** view by clicking the appropriate icon.

You can track spyware-level transactions and activities by filtering on several different options including **Top Spyware by**:

- Count
- Percentage

For more information, you can click on **View Details...**:

- If operating in Classic Mode, it goes to **MONITOR | Logs > Threat Logs**.

Top Botnet

The **Top Botnet by Botnet Block** report provides data as it relates to botnet threats connected to the system. You can select a **Graph** view or a **List** view by clicking the appropriate icon.

You can track botnet-level transactions and activities by filtering on several different options including **Top Botnet by:**

- Blocked
- Virus
- Spyware
- Intrusion
- Bytes received
- Bytes sent

For more information, you can click on **View Details...**:

- If operating in Classic Mode, it goes to **MONITOR | Logs > Threat Logs**.

DNS Filtering

The DNS Filtering reports provide an summary and allows you to export the data.



The **DNS Filtering Data** pane shows the number of events by category:

- **Allow**
- **Block**
- **Negative Reply**
- **Forge IP**

The **Top Security** pane identifies the malware detected by type. You can select a **Graph** view or a **List** view by clicking the appropriate icon. The categories and counts are provided in either view.

The **Top Mature** pane identifies the how much adult, or mature, content traverses your network. The categories and number of events are listed. You can select either a **Graph** view or a **List** view of the data by clicking the appropriate icon.

The **Top Enterprise** pane identifies the how much content can be identified by Gaming, Social or Sports enterprises. The categories and number of events are listed. You can select either a **Graph** view or a **List** view of the data by clicking the appropriate icon.

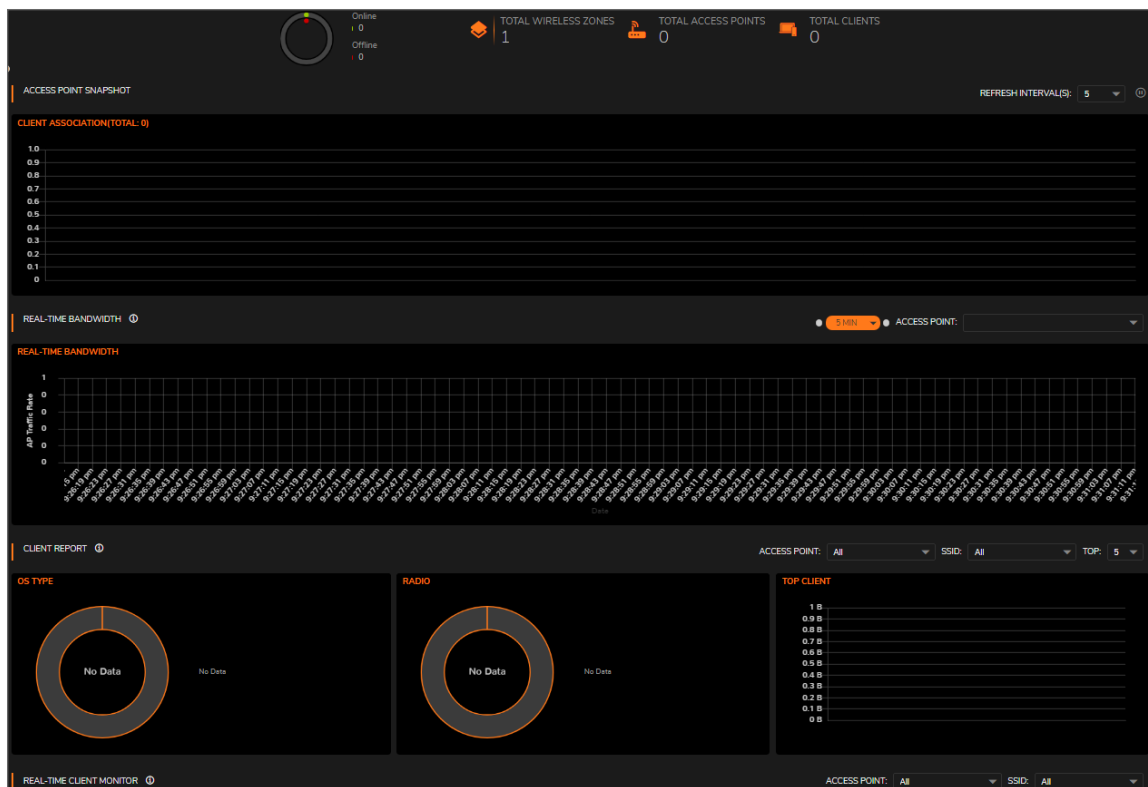
Access Points

The **Access Points** view of the SonicOS Dashboard summarizes the information about the access points in the network. The navigation path for the **Access Points** view is **HOME > Dashboard > Access Points**.

The **Access Points** view offers a high level view of the performance of the access points in the network. You can review the summaries across the top of the page and then scroll to see the different reports.

① | **NOTE:** If you have no access points configured, the reports will be blank.

For SonicWave, **HOME | Dashboard > Access Points** uses charts and graphs to help visualize the data related to the access points that are connected to your network. You can display both real-time status and historical status, as well as each client's rate, OS type, and host name. This Dashboard also displays the status of the SonicWave devices and provides information to help with monitoring problematic diagnosis.



A summary of the access points are shown at the top of the page. The data is presented as a doughnut chart; online is green and offline is red. The Online status includes operational, disabled, rebooting, and in IDS scanning mode. Offline status includes unresponsive and initializing states.

The count for the **Total Wireless Zones**, **Total Access Points** and **Total Clients** are also displayed.

For more information about the access point, refer to [SonicOS 8 Access Points Administration Guide](#).

Topics:

- [Feature Limitations](#)
- [Access Point Snapshot](#)
- [Client Association](#)
- [Real-Time Bandwidth](#)
- [Client Report](#)
- [Real-Time Client Monitor](#)
- [Client Report and Client Monitor Filtering](#)

Feature Limitations

SonicWave and SonicPoint AC device status is displayed on when the device is managed by a SonicWall firewall. Both the firewall and the access point needs to be functional or no valid data can be exchanged. SonicWave access points always retain a seven-day history of the dashboard data. However, because of memory limitations, SonicPoint AC devices lose all history data when they are rebooted.

Access Point Snapshot

One graph is shown in the **Access Point Snapshot** section. In the right corner, you can specify the refresh interval for these charts. Select the number of minutes from the drop-down menu; the options range from 5 to 10 minutes.

Client Association

The **Client Association** chart shows the number of clients associated with each access point in the configuration. The number of users is shown in bar chart form.

Real-Time Bandwidth

A graph showing the bandwidth being used by the selected access point is displayed in the **Real-Time Bandwidth** section of the **HOME | Dashboard > Access Points**.

① | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Real-Time Bandwidth** feature.

SonicOS shows a stacked chart of the real-time traffic on the selected access point(s). The Y value is the total traffic, both received and transmitted. By default, all access points are selected for the display.

To select the refresh interval, select the interval period from the drop-down menu by the chart title. Options are: 1 minute, 2 minutes, 5 minutes, 10 minutes, and 60 minutes.

To change the access point being displayed, go to the **Access Point** drop-down menu and select a different device. The chart updates with the data for that access point.

Client Report

Three graphs are shown in the **Client Report** section of the **HOME | Dashboard > Access Points: OS Type, Radio, and Top Client**.

① | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Client Report** feature.

Topics:

- [OS Type](#)
- [Radio](#)
- [Top Client](#)

OS Type

The **OS Type** pie chart displays the percentages of connected Windows clients, Macintosh clients, Linux clients, iPhones, Android, and so on. If the client has not generated any HTTP traffic, it might show as **Unknown**.

① | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **OS Type** feature.

Radio

The **Client Report** also provides a **Radio** chart. The **Radio** chart shows the percentage of clients connected to the 2.4GHz radio and the 5GHz radio.

① | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Radio** feature.

Top Client

The **Top Client** chart shows the clients who are using the most bandwidth. By going to the TOP field and selecting a number from the drop-down menu, you can show the top 5, top 10, top 15 or top 20 consumers for bandwidth. The values for both transmitting and receiving data are shown for the top users.

① | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Top Client** feature.

Real-Time Client Monitor

A graph showing the client connection details is displayed in the **Real-Time Client Monitor** section of the **HOME | Dashboard > Access Points**. This provides the detail for each user connected through the access points. You can see MAC addresses, host names, OS type, volume of traffic being received (Rx), and the volume of traffic being transmitted (Tx).

① | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Real-Time Client Monitor** feature.

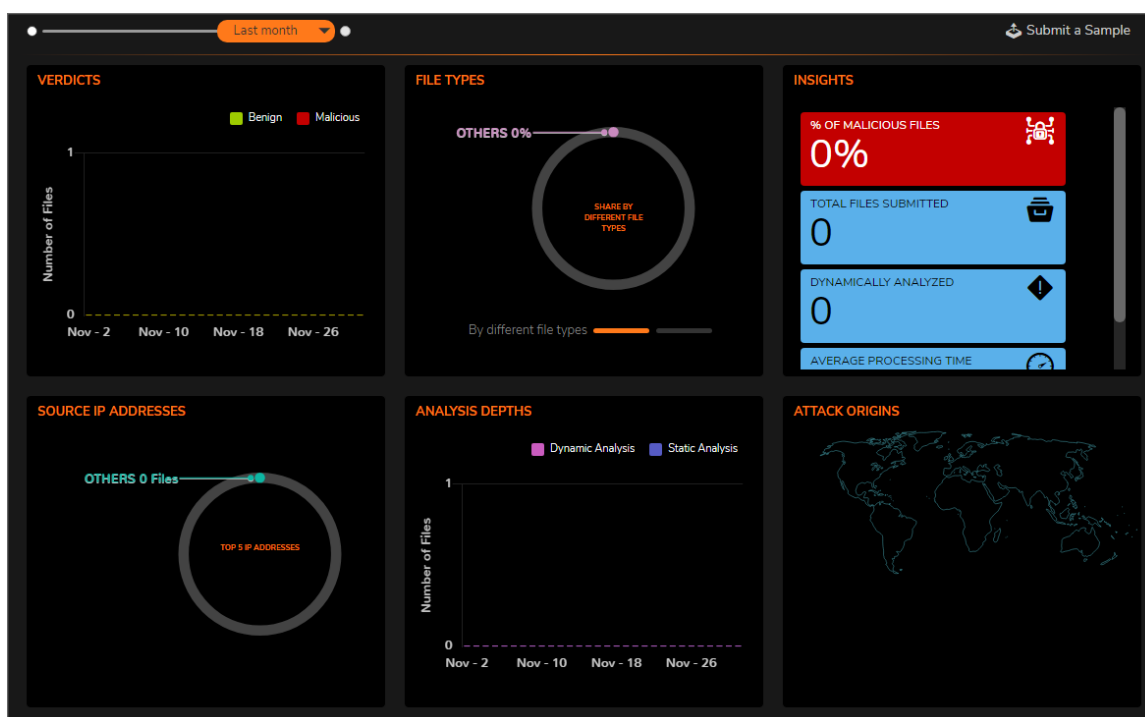
Client Report and Client Monitor Filtering

You can filter the output in both the **Client Report** section and the **Real-Time Client Monitor** section by selecting **All** or a specific access point in the **Access Point** drop-down menu, and/or by selecting **All** or a specific SSID in the **SSID** drop-down menu.

① | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support client detail filtering.

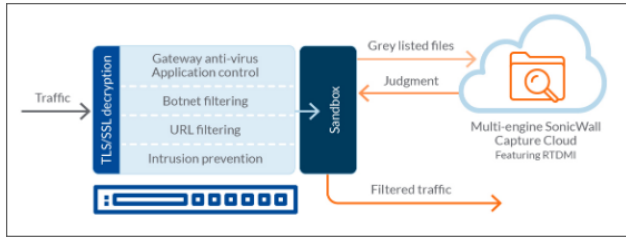
Capture ATP

The **Capture ATP** view of the SonicOS Dashboard, you can quickly see in one place which files are being sent to the backend for scanning and which ones are being blocked. The navigation path for the **Capture ATP** view is **.HOME > Dashboard > Capture ATP**.



The **SonicWall Capture Advanced Threat Protection (Capture ATP)** section of **DASHBOARD** view provides a cloud-based network sandbox that analyzes suspicious code. By doing so, it helps to discover and stop ransomware, advanced persistent threats (APTs), and zero-day attacks from entering the network at the gateway until a verdict is determined. It displays the status of the firmware being used to send files to the backend for protection.

Capture ATP offers multi-layer sandboxing; including SonicWall's Real-Time Deep Memory Inspection (RTDMI), full system emulation and virtualization techniques, to analyze suspicious code behavior. It scans traffic, suspicious code, and a broad range of file sizes and types.



For more information about the Capture ATP, refer to [SonicOS 8 Capture ATP Administration Guide](#).

Topics:

- Capture ATP Dashboard

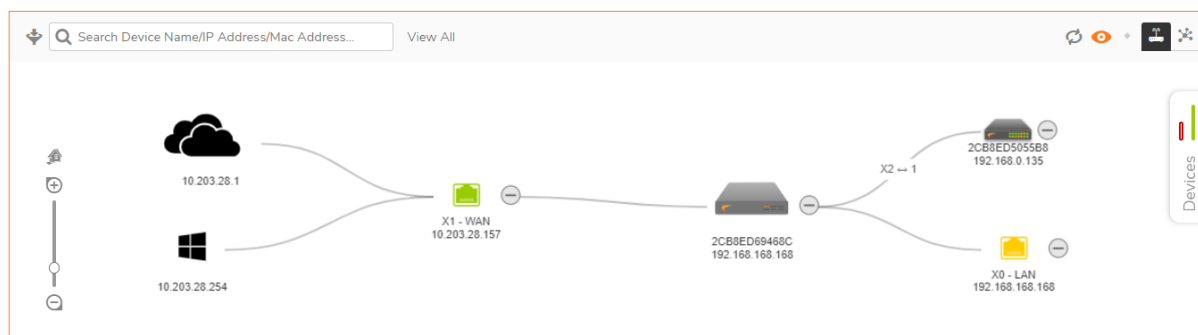
Topology

The **Topology** view of the SonicOS Dashboard provides a graphic view of the network. The navigation path for the **Topology** view is **Home > Dashboard > Topology**.

On the **HOME | Dashboard > Topology** page, devices can be managed with the **Topology** feature. **Topology** shows the network topology from the SonicWall firewall to the wireless access point. The access point real-time status can be monitored, and the context menu also provides configuration options.

This feature shows the logical relationship among all WAN, LAN, and WLAN zone devices, and provides a way to manage devices directly in the **Topology**.

The **HOME | Dashboard > Topology** page displays a tree-like or mesh diagram showing connected devices known to the firewall and their relationships, similar to the following figure:



Topics:

- [Managing the Topology View](#)
- [Managing Access Points in the Topology View](#)

Managing the Topology View

The Topology View is a simple interface. It provides the means to keep the view current and to modify the physical devices in the infrastructure.

You can also get detailed information on each of the devices in the Topology View. Just run your cursor over the device and a tool-tip bubble pops up. Depending on the type of device, it shows information like Name, IP address, Interface, and Model. For access points, you can also see additional information like status and number of clients.

Each access point also uses color to indicate status:

- Green = online
- Red = offline
- Yellow = busy

Managing Access Points in the Topology View

The Topology View has a context menu with commands that can be used to manage your access points.

① | **NOTE:** Only access points have context menus. None of the other devices in the topology map do.

Topics:

- [Editing an Access Point](#)
- [Showing Statistics](#)
- [Monitor Status on an Access Point](#)
- [Deleting an Access Point](#)

Editing an Access Point

To edit an access point in the Topology View::

1. Navigate to **HOME | Dashboard > Topology**.
2. Roll your mouse over the access point you want to edit.
3. Right-click on the access point.
4. Select **Edit this Access Point**.
5. Make changes to the object configuration as needed.
6. Click **OK** to save new settings.

Showing Statistics

To show statistics for an access point:

1. Navigate to **HOME | Dashboard > Topology**.
2. Roll your mouse over the access point you want to show.

3. Right-click on the access point.
4. Select **Show Access Point Statistics**.
5. Click **REFRESH** if you want to refresh the statistics.
6. Click **OK** when done.

Monitoring Status on an Access Point

To edit an access point in the Topology View:

1. Navigate to **HOME | Dashboard > Topology**.
2. Roll mouse over the access point you want to monitor.
3. Right-click on the access point.
4. Select **Monitor Access Point Status**.
The Access Point Monitor shows system status for the access point. It includes CPU usage, Memory Usage, Rx Rates and Tx Rates.
5. Click **REFRESH** if you want to refresh the data.
6. Click the **Details** icon if you want to see the details on the access point.
7. Click **OK** when done.

Deleting an Access Point

To delete an access point in the Topology View:

1. Navigate to **HOME | Dashboard > Topology**.
2. Roll your mouse over the access point you want to delete.
3. Right-click on the access point.
4. Select **Delete Access Point**.
5. Confirm that you want to delete the access point; cancel if you do not.

REAL-TIME CHARTS

- System Monitor
- Protocol Monitor
- User Monitor
- Bandwidth Monitor

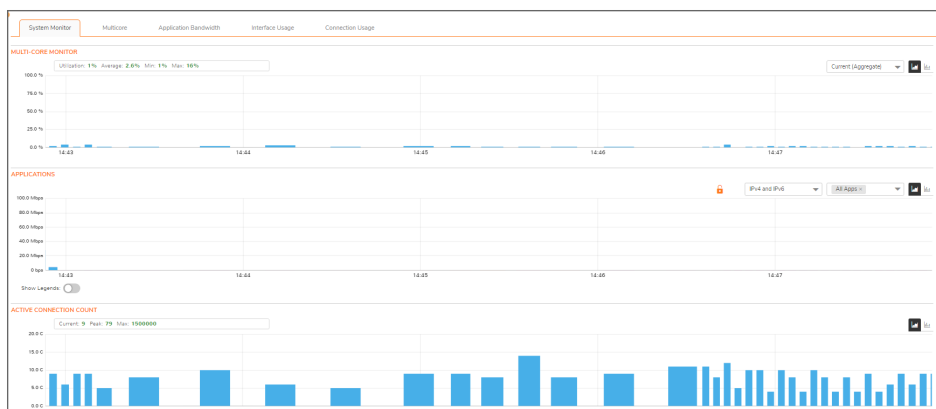
System Monitor

The **Monitor > Real Time Charts > System Monitor** page provides a real-time, multi-functional display with information about system monitoring, hardware multi-core utilization, application bandwidth usage, interface usage, and connection usage. rate.

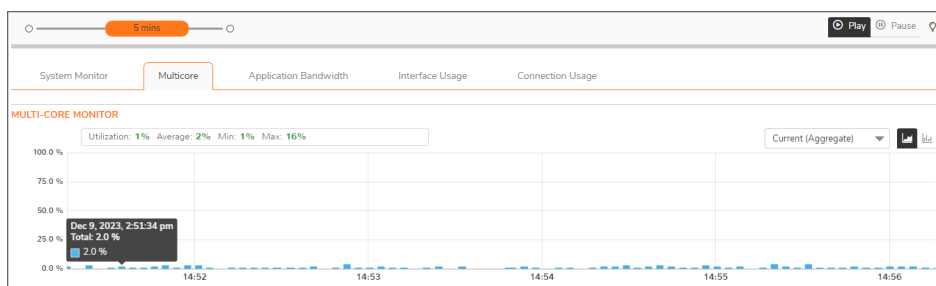
NOTE: A chart may be empty or blank if there are no recent data entries received within the viewing range. Also note that your charts will vary based on what firewalls and feature you implemented.

Five tabs display the options on the **System Monitor** page.

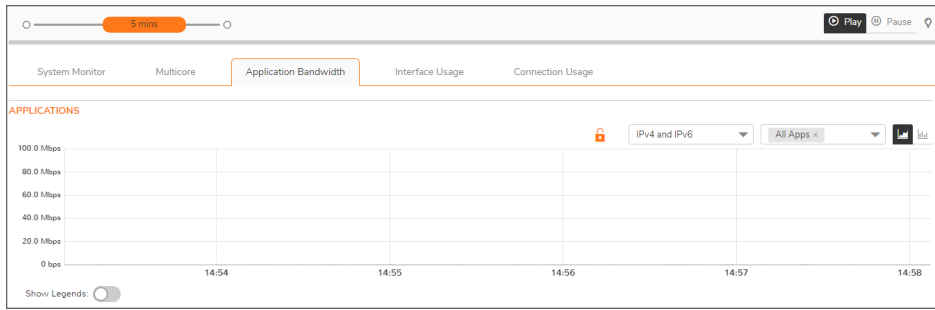
System Monitor



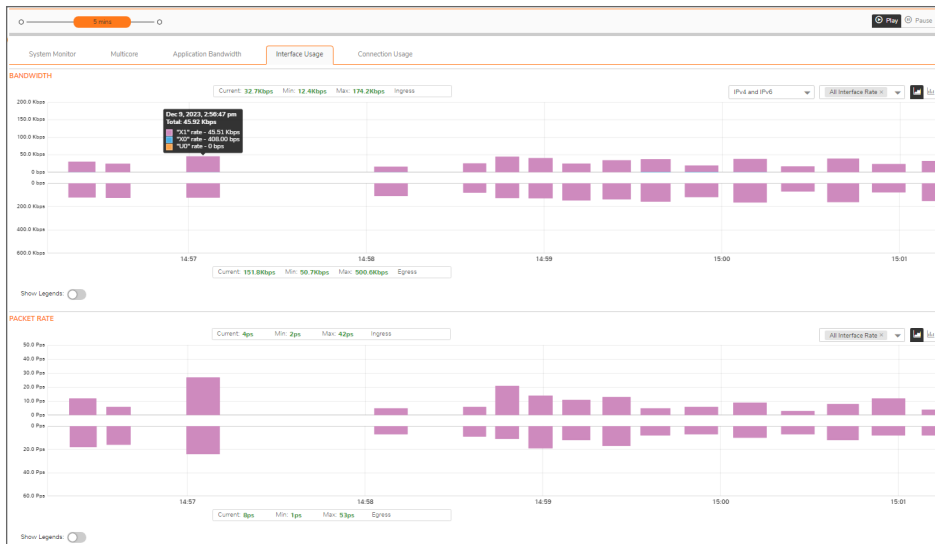
Multicore



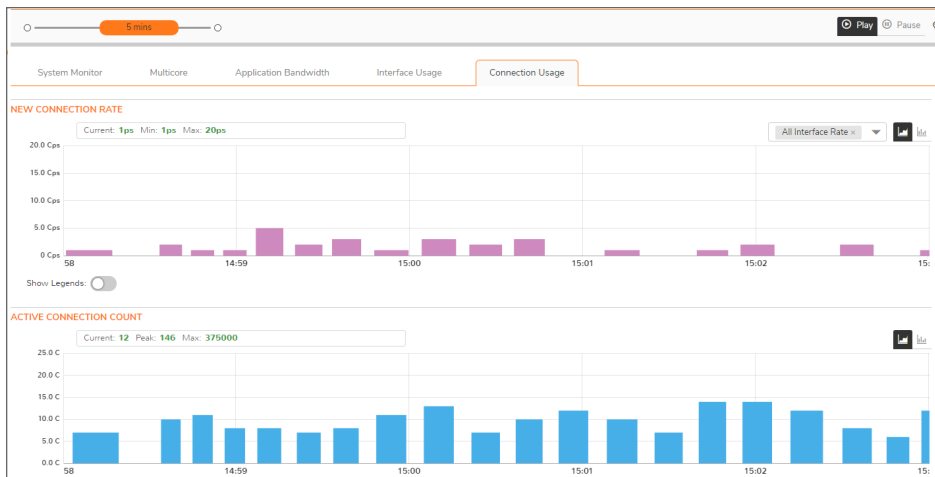
Application Bandwidth



Interface Usage

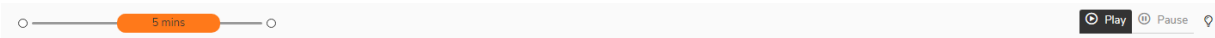


Connection Usage



Using the Toolbar

The **Policy Monitor** toolbar contains features to specify the refresh rate and pause or play the data flow. Changes made to the toolbar apply across all the data flows.



PROTOCOL MONITOR TOOLBAR OPTIONS

Option	Widget	Description
View Range		Displays data pertaining to a specific span of time. The View Range is configurable in 60 seconds, 2 minutes, 5 minutes, and 10 minutes. The default is 2 minutes.
Pause		Freezes the data flow. The Pause button appears black if the data flow has been frozen.
Play		Unfreezes the data flow. The time entries at the bottom of the tables will refresh as soon as the data flow is updated. The Play button appears black if the data flow is live.
Tips		Mouse over a data point to see values at that instant.

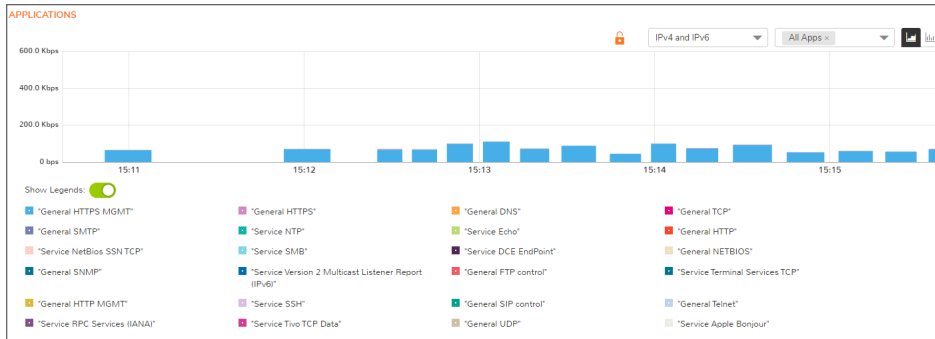
Common Features

Topics:

- [Legends](#)
- [Tooltips](#)
- [Changing Chart Format](#)
- [Selecting IPv6/IPv4](#)
- [Current, Minimum, Maximum Display](#)

Legends

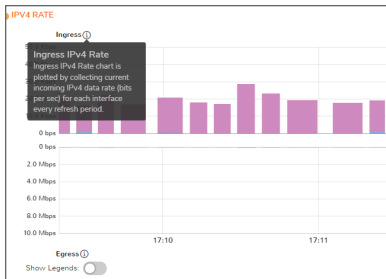
Some charts have the option to display a legend that shows the name and color used for the applications. Simply enable or disable the switch to **Show Legends**.



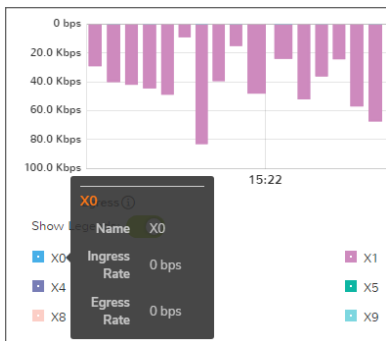
Tooltips

Various elements of the charts have associated tool-tips:

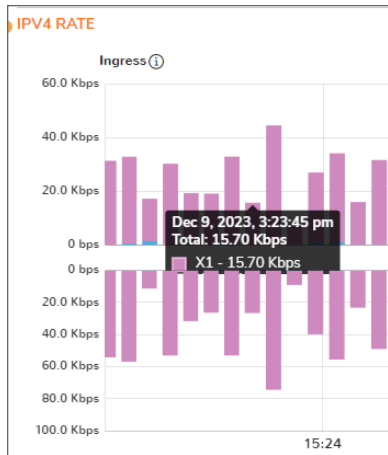
- The name of most charts have two tool-tip icons that briefly describe the ingress and egress information in the chart.



- Legend items display information about the item the legend represents.



- Hover over a bar on the chart to see more details on that instance.



To display a tool-tip, hover your mouse over the desired item or click on the chart. The information displayed varies by chart.

Changing Chart Format

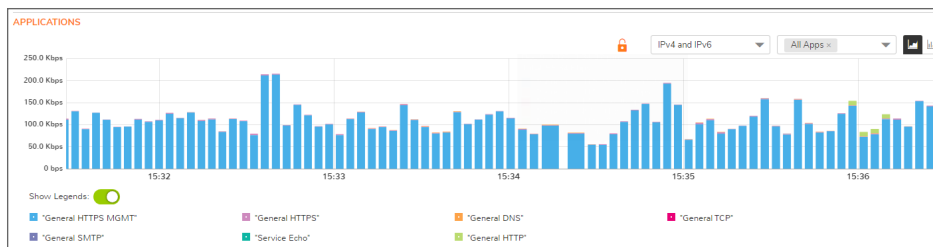
You are able to view individual charts in either stacked bar chart format or single bar chart format. Each chart has

Chart Format icons in the upper right corner of the chart  . The default is stack chart format.

Bar Chart

The bar chart format displays applications individually, thus allowing you to compare applications. In this chart, the applications, interfaces, or core monitors are arranged along the x-axis, for applications and interfaces according to the color code shown in the Legend. The y-axis displays information appropriate to the chart, such as the amount of traffic for each application or interface. To display the data in bar chart format, click on the **Stacked Bar** icon.

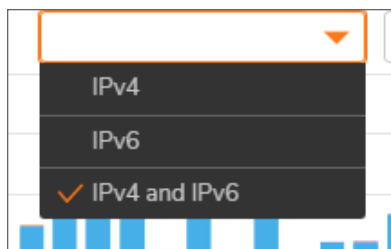
The following example is a Bar Chart view.



Selecting IPv6/IPv4

For complete information on the SonicOS implementation of IPv6, see the chapter on *Configuring Interfaces for Pv6* in the [SonicOS 8 System Administration Guide](#).

Real-Time Charts can be configured to see IPv4, IPv6 and both. Make the selection from the drop-down menu on the charts where this is an option.



Current, Minimum, Maximum Display

All charts, except **Applications**, display the current, minimum, and maximum values for the chart. The values vary by chart and can be in Mbps, Kbps, Pps (packets per second), Bytes, or Cps (connections per second).



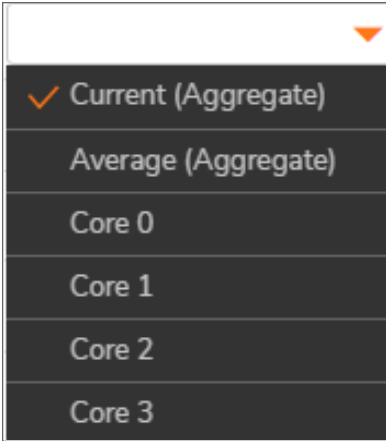
For the **Ingress/Egress** charts, the information is displayed for both halves, the Ingress on the top and the Egress on the bottom. For the other charts, the information is displayed on the top.

Multicore Monitor

The **Multicore Monitor** displays dynamically updated statistics on utilization of the individual cores of the firewall. The information is shown either for combined data in stacked bar chart format or for individual cores in bar chart format. Core 1 through core 8 handle the control plane. The remaining cores handle the data plane. To maximize processor flexibility, functions are not dedicated to specific cores; instead all cores can process all data plane tasks. Memory is shared across all cores. Each core can process a separate flow simultaneously, allowing for up to 88 flows to be processed in parallel.

Options

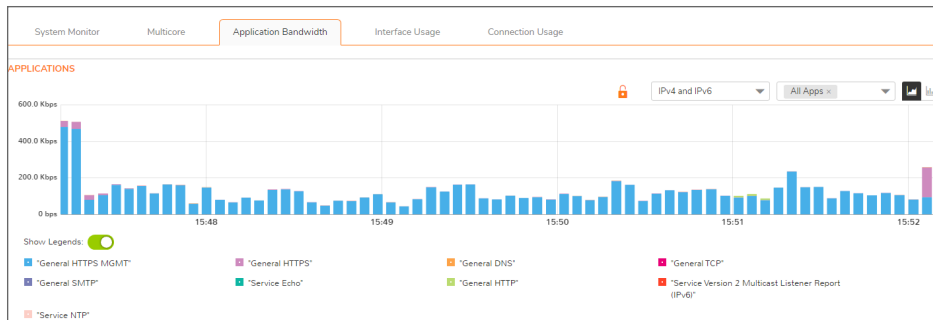
The following option is specific to the **Multicore** chart. For other options and display features, see [Common Features](#).

Option	Widget	Description
Aggregate Display		<p>Specifies which Cores are displayed in the Multi-Core Monitor Flow Chart.</p> <p>A drop-down menu allows you to specify Current (Aggregate), Average (Aggregate), and individual Cores. The individual Cores vary, depending on the number of Cores available. Multiple Cores can be selected.</p>

Applications Bandwidth



The Applications data flow provides a visual representation of the current applications accessing the network.

Bar Chart



Options

The following option is specific to the **Applications** chart. For other options and display features, see [Common Features](#).

Option	Widget	Description
Lock		Locks the Display for the Applications chart. The lock/unlock option is available when you select Most Frequent Apps . Most Frequent Apps displays the top 25 apps; you can use the lock or unlock option to keep the report from altering the top 25 apps.
Unlock		Unlocks the Display for the Applications chart.

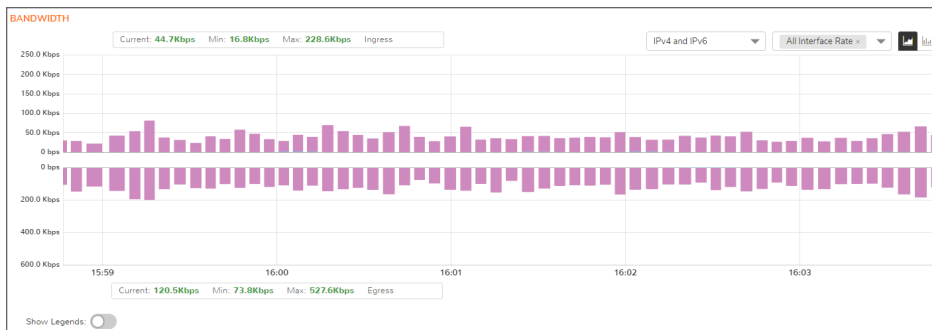
Interface Usage

The **Interface Usage** charts provide a visual representation of **Bandwidth**, **Packet Rate**, and **Packet Size**. The current value, plus the minimum and maximum amounts is available in the display. The ingress values are at the top of the chart and the egress is at the bottom of the chart.

NOTE: The Bandwidth charts have no direct correlation to the Application charts.

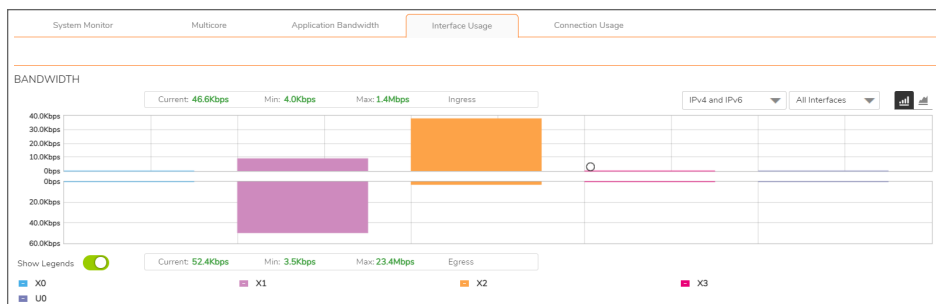
Stacked Bar Chart

The stacked chart format allows you to view all of traffic as it occurs. The x-axis displays the current time, and the y-axis displays the .



Bar Chart

The bar chart format displays data pertaining to individual interfaces in a bar chart; allowing comparisons of individual interfaces. In this chart, the x-axis denotes the interfaces whereas the y-axis denotes the traffic.



Options

The following option is specific to the **Interface Usage** chart. For other options and display features, see [Common Features](#).

Option	Widget	Description
Interface Rate Display		<p>Specifies which Interfaces are displayed in the Bandwidth Flow Chart.</p> <p>A drop-down menu provides options to specify All Interfaces Rate, All Interfaces (%), or rate or percentage (%) for individual interfaces.</p> <p>The individual interfaces vary depending on the number of interfaces on the network. Multiple interfaces can be selected if desired.</p>

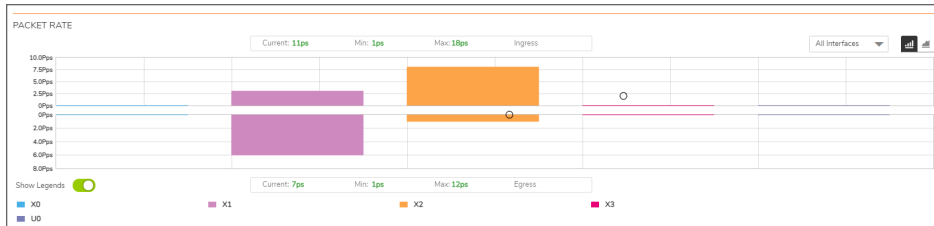
Packet Rate Monitor

The **Packet Rate** monitor provides information on the ingress and egress packet rate as packets per second (pps). This can be configured to show packet rate by network interface. The chart shows the current packet rate, minimum packet rate, and maximum packet rate for both ingress and egress network traffic.

Stacked Bar Chart



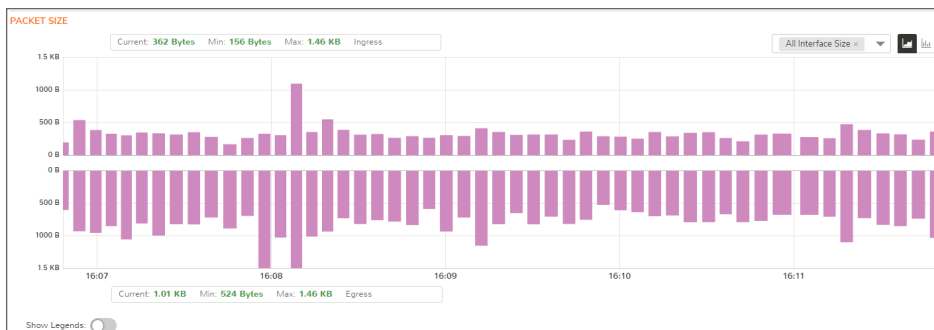
Bar Chart



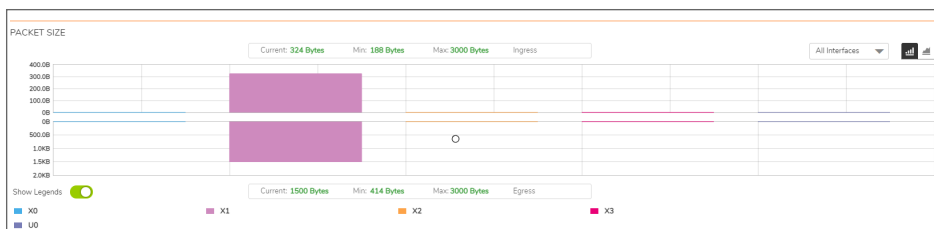
Packet Size

The **Packet Size** report provides information on the ingress and egress packet size in bytes (B). This can be configured to show packet size by network interface. The chart shows the current packet size, minimum packet size, and maximum packet size for both ingress and egress network traffic.

Stacked Chart



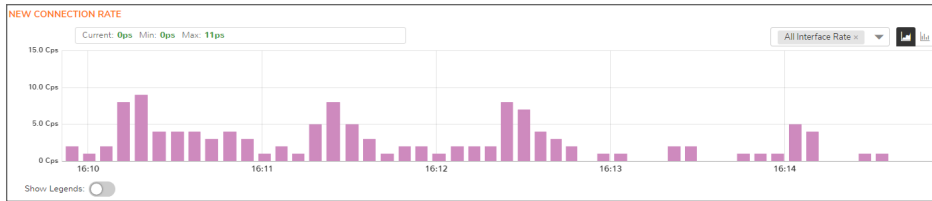
Bar Chart



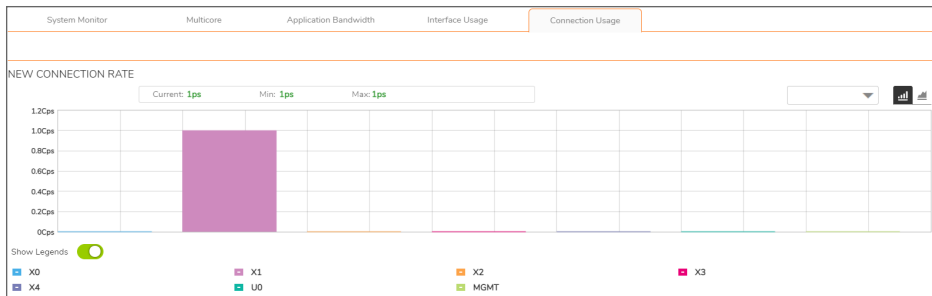
Connection Usage

The **Connection Usage** report is plotted by collecting the outgoing and incoming connection rates for each interface every refresh period. When looking at the combined connection rate of more than one interface at the same time, it may appear double than the actual connection rate. A single connection between a pair of interfaces is counted for both interfaces.

Stacked Bar Chart



Bar Chart



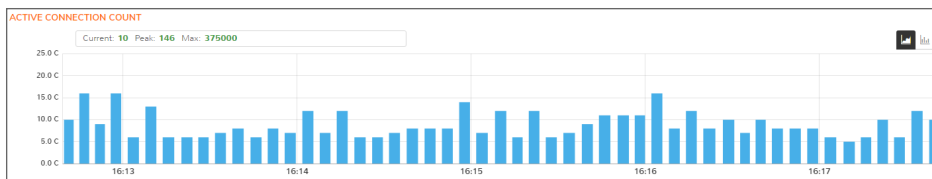
Topics:

Active Connection Count

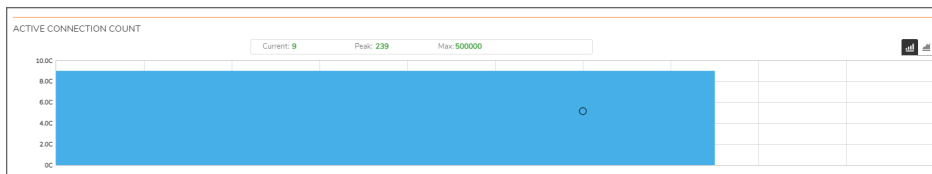
Active Connection Count

The **Active Connection Count** report provides a visual representation of the active total number of connections, peak number of connections, and maximum number of connections. The y-axis displays the total number of connections from 0C (zero connections) to 1KC (one kilo connections).

Stacked Chart



Bar Chart



① | **NOTE:** The **Connection Count** Monitor does not have legends.

Protocol Monitor

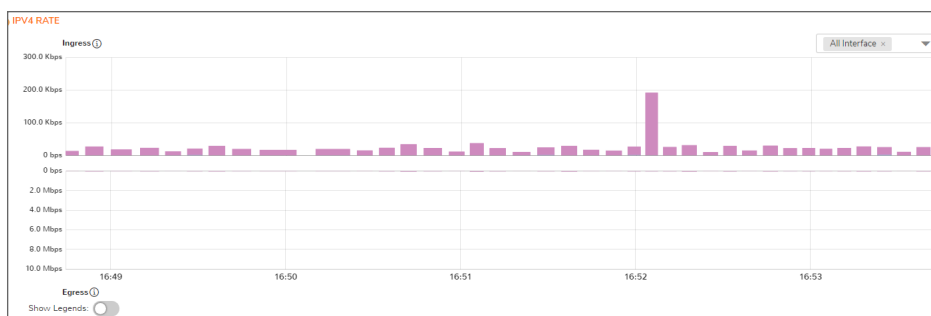
The **Monitor > Real Time Charts > Protocol Monitor** page displays real-time charts showing ingress and egress traffic rates for the following protocols:

IPv4 Rate	Internet Protocol version 4
ARP Rate	Address Resolution Protocol, used by IPv4 to map IP network addresses to link layer hardware addresses
IPv6 Rate	Internet Protocol version 6
UDP Rate	User Datagram Protocol, a connection-less protocol used for example by DNS, SNMP, RIP, DHCP
TCP Rate	Transmission Control Protocol, a connection oriented protocol allowing bidirectional traffic once the connection is established, used for example by FTP, SSH, Telnet, and also by DNS
ICMP Rate	Internet Control Message Protocol, used by network devices to send error messages and operational information; ping uses ICMP to send echo request packets to a host
IGMP Rate	Internet Group Management Protocol, used by hosts and routers to establish multicast group memberships

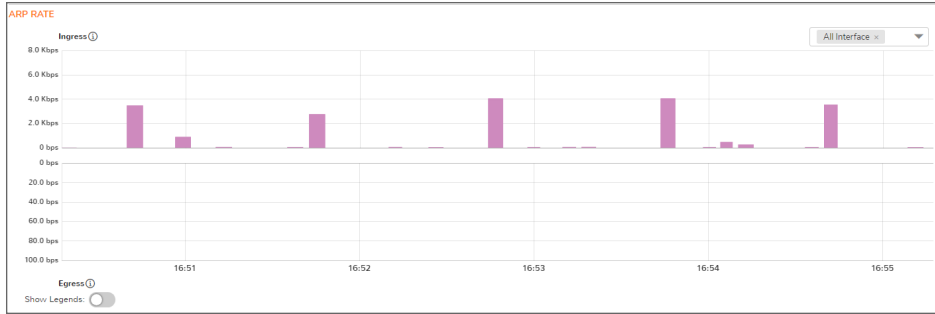
The seven real-time charts displayed on the **Protocol Monitor** page are shown in the images below. The **Ingress** rate is displayed on the top half of each chart, and the **Egress** rate is displayed on the bottom.

📘 | **NOTE:** A chart may be empty or blank if there are no recent data entries received within the viewing range.

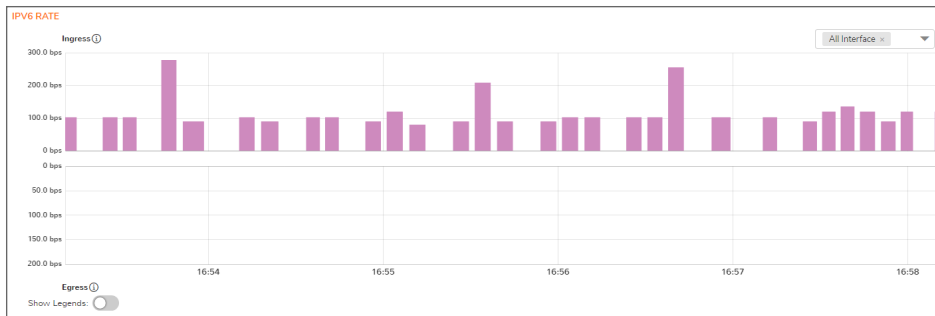
PROTOCOL MONITOR - IPV4 CHART



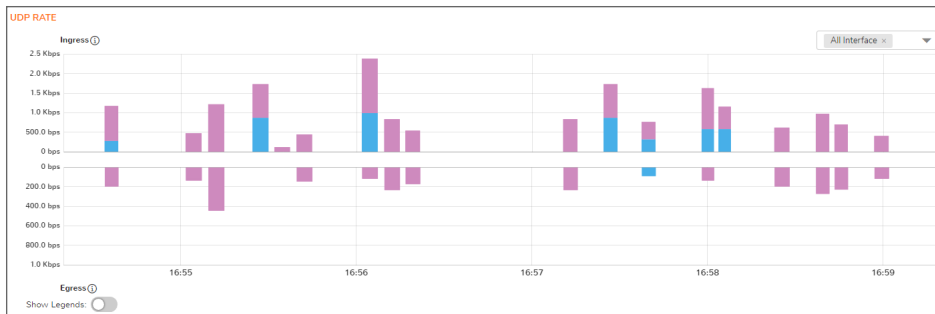
PROTOCOL MONITOR - ARP CHART



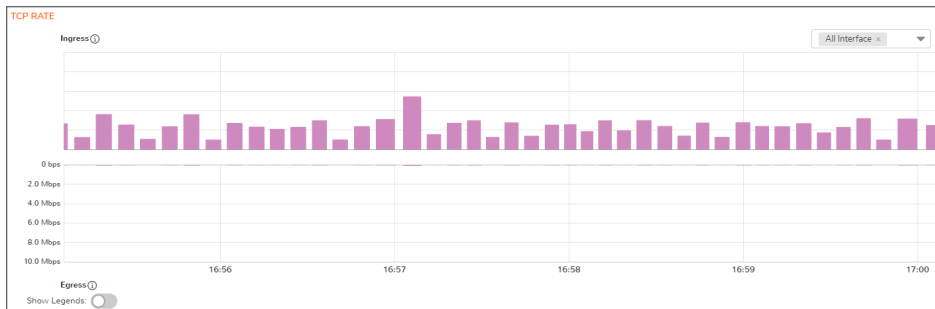
PROTOCOL MONITOR - IPV6 CHART



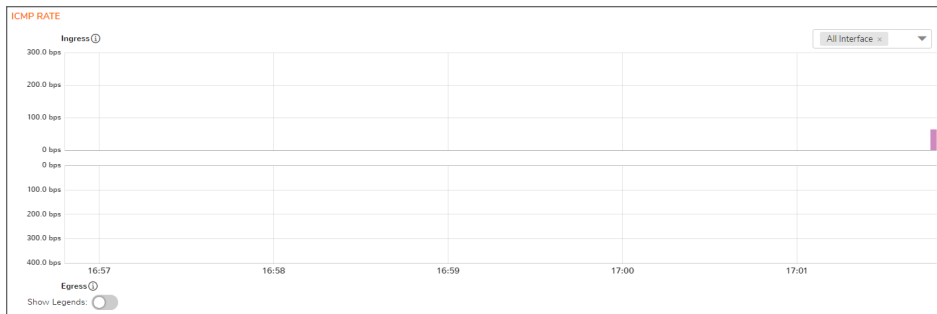
PROTOCOL MONITOR - UDP CHART



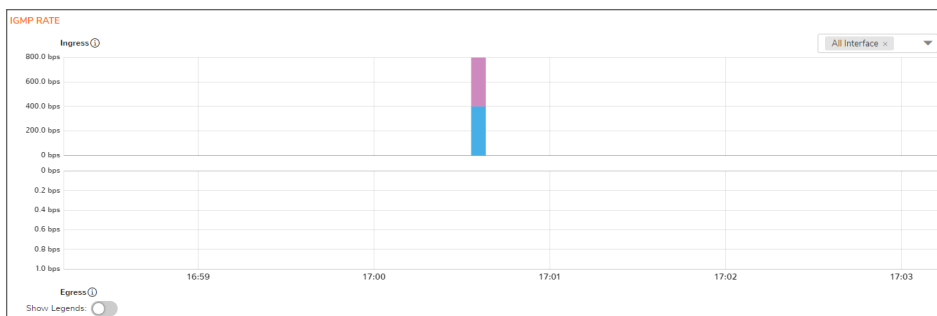
PROTOCOL MONITOR - TCP CHART



PROTOCOL MONITOR - ICMP CHART



PROTOCOL MONITOR - IGMP CHART

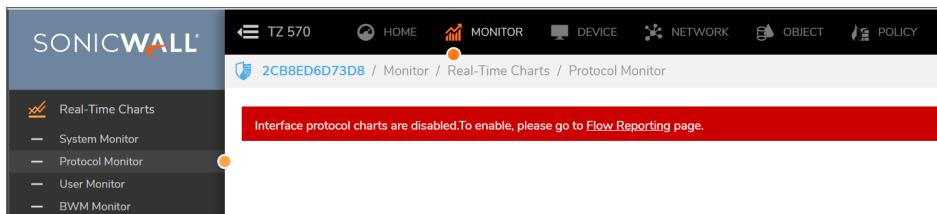


Topics:

- [Enabling the Protocol Monitor](#)
- [Using the Toolbar](#)
- [Using Per-Chart Viewing Options](#)

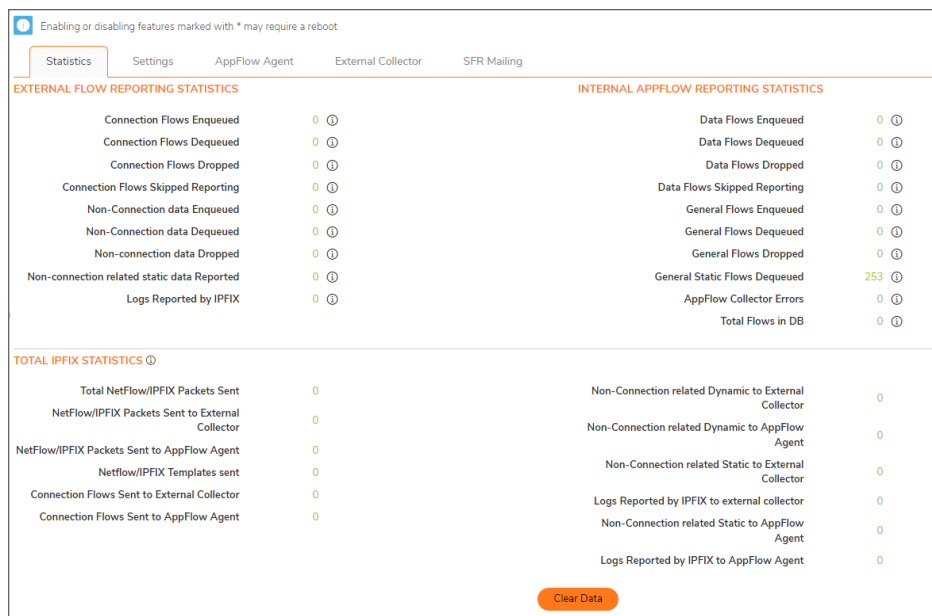
Enabling the Protocol Monitor

The first time you access the Protocol Monitor, it is disabled.



To enable the Protocol Monitor and start displaying statistics in the different charts:

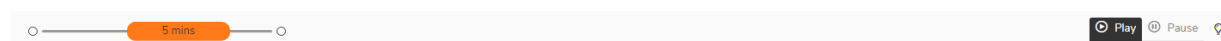
1. Click on the **Flow Reporting** page link.
You will be navigated to **Device > App Flow > Flow Reporting** page.
2. In the **Settings** tab, select **Interface protocols** option from the **Collect Real-Time Data For** drop-down and click **Accept**.



The settings are enabled, and statistics are displayed in the **Protocol Monitor** page.



Using the Toolbar

The Protocol Monitor toolbar contains features to specify the refresh rate and pause or play the data flow. Changes made to the toolbar apply across all the data flows.



PROTOCOL MONITOR TOOLBAR OPTIONS

Option	Widget	Description
View Range		Displays data pertaining to a specific span of time. The View Range is configurable in 60 seconds, 2 minutes, 5 minutes, and 10 minutes (default).
Pause		Freezes the data flow. The Pause button appears black if the data flow has been frozen.

Option Widget	Description
Play 	Unfreezes the data flow. The time entries at the bottom of the tables will refresh as soon as the data flow is updated. The Play button appears black if the data flow is live.
Tips 	Mouse over a data point to see values at that instant.

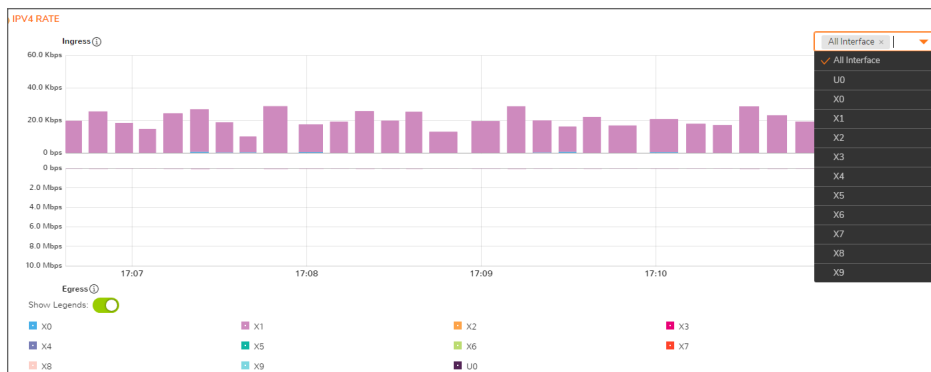
Using Per-Chart Viewing Options

Topics:

- [Legends](#)
- [Tooltips](#)


Legends

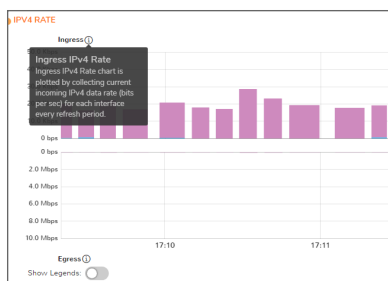
Each chart displays a legend that shows the name and color used for the interfaces selected in the chart's display options drop-down menu. To view the chart, select the interfaces from **All Interfaces** drop-down and toggle the **Show Legends** option.



Tooltips

Various elements of the charts have associated tool-tips:

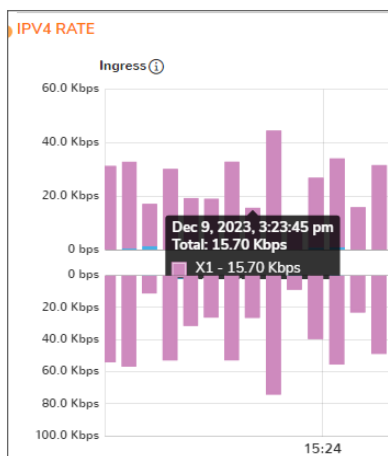
- The name of each chart has two tool-tip icons  that briefly describe the ingress and egress information in the chart.



- Legend items display information about the item the legend represents.



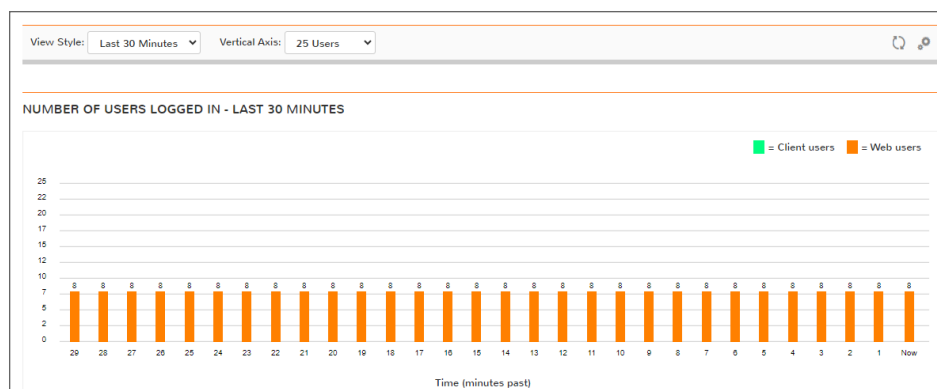
- Hover over a bar on the chart to see more details on that instance.



To display a tool-tip, hover your mouse over the desired item or click on the chart. The information displayed varies by chart.

User Monitor

The **Monitor > Real Time Charts > User Monitor** page provides a quick and easy method to monitor the number of active users on the SonicWall security appliance.




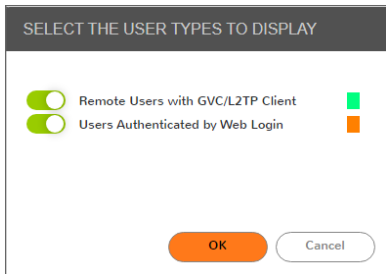
The **User Monitor** page provides these options to customize the display of recent user activity in the User Monitor table:

- **View Style:** Sets the scale of the X-axis, which displays the duration of time. The available options are:
 - Last 30 Minutes
 - Last 24 Hours
 - Last 30 Days
- **Vertical Axis:** Sets the scale of the Y-axis, which displays the number of users. The available options reflect the number of users. For example, two different systems would have different options.

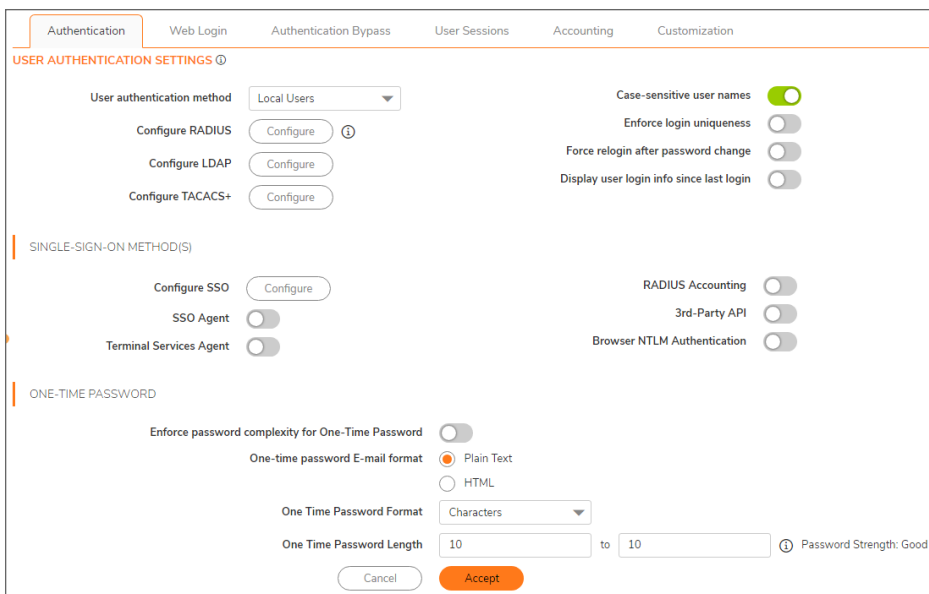
EXAMPLE OF OPTIONS FOR Y-AXIS BASED ON NUMBER OF USERS

Few Users	Many Users
10	800
100	8000
1000	80000

- **Select User Types icon**  : Displays a pop-up window, where you can select the types of users to be displayed, indicated by the associated color.



By default, the above two options are displayed. If you wish to display inactive users and users authenticated by Single-Sign-On method, navigate to **Device > Users > Settings** and enable **SSO Agent** option and click **Accept**.






When **SSO Agent** is enabled, the options **Inactive Users** and **Users Authenticated by Single-Sign-on** are displayed, indicated by the associated color.



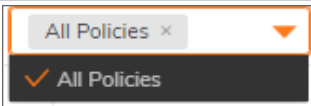
- **Refresh icon**  : Refreshes the User Monitor chart.

Bandwidth Monitor

The **Monitor > Real Time Charts > BWM Monitor** page displays policy-based bandwidth usage for ingress and egress network traffic, and a second chart with the top 10 for policy-based bandwidth usage.

The Bandwidth Monitor charts are available for All Policies or for selected policies in the drop-down policies list next to the chart. The refresh interval rate is configurable from 3 to 30 seconds. The bandwidth management priority is depicted by guaranteed, maximum, and dropped. The following display settings and configurable controls are available on this page:

Option	Widget	Description
View Range		Displays data pertaining to a specific span of time. The View Range is configurable in 60 seconds, 2 minutes, 5 minutes, and 10 minutes (default).
Refresh every	Refresh every: <input type="text" value="3"/> sec	Determines the frequency at which data is refreshed. A numerical integer between 1 to 10 seconds is required. The default is 3 seconds.
Play		Unfreezes the data flow. The time and date will refresh as soon as the data flow is updated. The Play button appears black if the data flow is live.
Pause		Freezes the data flow. The time and date will also freeze. The Pause button appears black if the data flow has been frozen.

Option	Widget	Description
Stacked Chart		Click the Stacked Bar Chart icon to display the chart in flow (area) chart format. The x-axis displays the current time and the y-axis displays the amount of ingress and egress traffic in Mbps.
Bar Chart		Click the Bar Chart icon to display the chart in bar chart format. The x-axis displays Rules in the Policy-Based Ingress/Egress chart and the names of the top 10 policies for bandwidth usage in the Policy-Based Top 10 chart. The y-axis displays the amount of ingress and egress traffic in Mbps. The Policy-Based Top 10 chart is always displayed as a bar chart with one bar for each policy.
Policies display		Specifies which Policies are displayed in the Policy-Based Ingress/Egress chart. A drop-down menu allows you to specify All Policies or select individual policies. The individual policies vary depending on the configured policies available. Multiple policies can be selected.

Enabling BWM Monitor

For Classic Mode, bandwidth management policies are configured from the **Policy > Rules and Policies > Access Rules** page. To view the BWM chart, edit the access rule for which you want to view the BWM chart and under **Traffic Shaping** tab, select the **Egress BWM**, **Ingress BWM**, and enable **Track Bandwidth Usage** options.

APPFLOW

- [AppFlow Report](#)
- [AppFlow Monitor](#)
- [CTA Report](#)

AppFlow Report

The **MONITOR | AppFlow > AppFlow Reports** page displays the following reports:

Applications								
Users								
IP Addresses								
Virus								
Intrusions								
Spyware								
Locations								
Botnets								
Web Categories								
Q Search...		IPv4 & IPv6	View: Since Restart		Limit: 50			+
#	APPLICATION NAME	SESSIONS		INITIATOR BYTES		RESPONDER BYTES		
		COUNT	PERCENTAGE	COUNT	PERCENTAGE	COUNT	PERCENTAGE	
1	General HTTPS MGMT	75.96K	69%	113.80 MB	62%	502.95 MB	47%	
2	General HTTPS	20.68K	18%	61.84 MB	34%	208.14 MB	19%	
3	General DNS	9.17K	8%	1.10 MB	0%	2.11 MB	0%	
4	Service NTP	1.51K	1%	156.68 KB	0%	155.12 KB	0%	
5	Service Version 2 Multicast Listener Report (IPv6)	1.05K	0%	89.24 KB	0%	0 B	0%	
6	General HTTP	347	0%	4.68 MB	2%	338.04 MB	32%	
7	Service RPC Services (IANA)	130	0%	33.01 KB	0%	0 B	0%	
8	General HTTP MGMT	129	0%	134.90 KB	0%	3.53 MB	0%	
9	Service Echo	8	0%	480 B	0%	0 B	0%	

The **MONITOR | AppFlow > AppFlow Report** page enables you to view top-level aggregate reports of what is going on in your network and, at a quick glance, answer such questions as the following:

- What are the top-most used applications running in my network?
- Which applications in terms of total number of sessions and bytes consume my network bandwidth?
- Which applications have viruses, intrusions, and spyware?
- What website categories are my users visiting?

The report data can be viewed from the point of the last system restart or since the data was last reset.

To enable and configure the reports, follow the procedures described in **Managing Flow Reporting Statistics** in the **SonicOS Logs** documentation. The green check mark icon at the top of the **MONITOR | AppFlow > AppFlow Report** page displays a link to the **DEVICE | AppFlow Settings > Flow Reporting** page, where you can configure the reports.

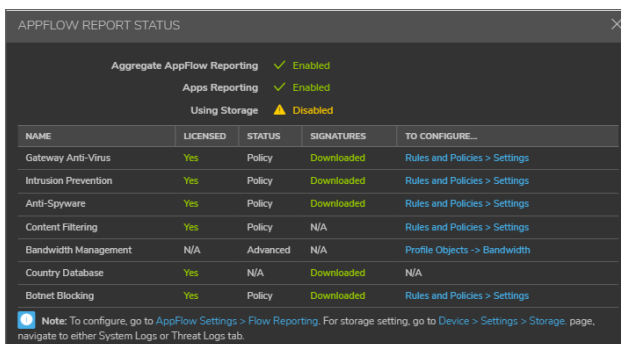
The top of the page displays the following settings and information:

Q Search...		IPv4 & IPv6	View: Since Restart		Limit: 50			+	Statistics	Send Report	Export	Refresh	Column Selection
-------------	--	-------------	---------------------	--	-----------	--	--	---	------------	-------------	--------	---------	------------------

- **IP Version** – Select IPv4, IPv6, or IPv4 and IPv6 to view the reports for that traffic.
- **View** – Choose View type to display reports based on the total activity **Since Restart** of firewall, activity **Since Last Restart** by user of activity based on the configured schedule. If **On Schedule** then you can configure to export report either by way of FTP/e-mail.

Choose one:

- **Since Restart** – Shows the aggregate statistics since the last appliance restart.
- **Since Last Reset** – Shows the aggregate statistics since the last time you cleared the statistics.
- **On Schedule** – You can configure to export your report either by FTP or e-mail.
- **Limit** – Limits the number of resulting entries.
- **Check mark** – Click or mouse over to expose a popup showing the Appflow Report Status. Links are provided to connect you to additional data.



- **Refresh** – Click to refresh the report data.

Topics:

- [Applications](#)
- [Users](#)
- [IP Addresses](#)
- [Viruses](#)
- [Intrusions](#)
- [Spyware](#)
- [Locations](#)
- [Botnets](#)
- [Web Categories](#)

Applications

Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based

on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

When viewing the Applications data, the key information is provided in the table:

- **Sessions** — Number of connections or flows
- **Initiator Bytes** — Number of bytes sent by the initiator
- **Responder Bytes** — Number of bytes sent by the responder

Additionally, the report provides the following information:

- **Application Name** — Name of the application - Signature ID
- **Count** — The frequency of this application in KBs of the total number of applications.
- **Percentage of Applications** — The frequency of this application as a percentage of the total number of applications
- **Access Rules** — Number of connections/flows blocked by the firewall rules
- **App Rules** — Number of connections/flows blocked by DPI engine
- **Location Block** — Number of connections/flows blocked by GEO enforcement
- **Botnet Block** — Number of connections/flows blocked by BOTNET enforcement
- **Virus** — Number of connections/flows with virus
- **Intrusion** — Number of connections/flows identified as intrusions
- **Spyware** — Number of connections/flows with spyware

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Users

Using the **View** drop-down list, select **Since Restart**, **Since Last Reset**, or **On Schedule**.

These selections are defined as:

- **Sessions** — Number of sessions/connections initiated/responded
- **Bytes Received** — Number of bytes received by the user
- **Bytes Sent** — Bytes of data sent by the user

The report provides the following information:

- **User Name** — Name of the user, or UNKNOWN
- **Count** — The activity of this user in KBs of the total activity of users
- **Percentage of Users** — The activity of this user as a percentage of the total activity of users
- **Blocked** — Connections/sessions blocked
- **Virus** — Number of connections/flows with virus

- **Spyware** — Sessions/connections detected with spyware
 - **Intrusion** — Number of Sessions/connections identified as intrusions
 - **Botnet** — Sessions/Connections detected as botnet
- The columns in the table can be customized so it displays only what you want to see.

Click the gear icon to select columns.

IP Addresses

Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

When viewing the IP Addresses data, the key information is provided in the table:

- **Sessions** — Number of sessions/connections initiated/responded
- **Bytes Received** — Number of bytes received by the user
- **Bytes Sent** — Bytes of data sent by the user

The report provides the following information:

- **IP Address** — The IP address
- **Count** — The frequency of connections/flows involving this IP address in KBs of the total number of connections/flows for all IP addresses
- **Percentage of IP Addresses** — The frequency of connections/flows involving this IP address as a percentage of the total number of connections/flows for all IP addresses
- **Blocked** — Connections/sessions blocked
- **Virus** — Number of connections/flows with virus
- **Spyware** — Sessions/connections detected with spyware
- **Intrusion** — Number of Sessions/connections identified as intrusions
- **Botnet** — Sessions/Connections detected as botnet

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Viruses

Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

The report provides the following information:

- **Sessions** — Number of sessions/connections with this virus

The report provides the following information:

- **Virus Name** — The name of the virus, or UNKNOWN
- **Count** — The frequency of this virus in KBs of the total number of viruses
- **Percentage of Viruses** — The frequency of this virus as a percentage of the total number of viruses

Intrusions

Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

The report provides the following information:

- **Sessions** — Number of sessions/connections with this virus

The report provides the following information:

- **Intrusion Name** — The name of the intrusion, or UNKNOWN
- **Count** — The frequency of this intrusion in KBs of the total number of intrusions
- **Percentage of Intrusions** — The frequency of this intrusion as a percentage of the total number of intrusions

Spyware

Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

The report provides the following information:

- **Sessions** — Number of sessions/connections with this virus

The report provides the following information:

- **Spyware Name** — The name of the spyware signature, or UNKNOWN
- **Count** — The frequency of this spyware in KBs of the total number of spyware
- **Percentage of Spyware** — The frequency of this spyware as a percentage of the total number of spyware

Locations

#	COUNTRY NAME	SESSIONS		BYTES RECEIVED		BYTES SENT	
		COUNT	PERCENTAGE	COUNT	PERCENTAGE	COUNT	PERCENTAGE
1	Private	1.61M	96%	2.54 GB	80%	3.37 GB	91%
2	Unknown	55.70K	3%	615.20 MB	19%	340.77 MB	8%

Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

These selections are defined as:

- **Sessions** — Number of sessions/connections initiated/responded
- **Bytes Received** — Number of bytes received by the user
- **Bytes Sent** — Bytes of data sent by the user

The report provides the following information:

- **Country Name** — Name of the location or country
- **Count** — The frequency of of connections/flows involving this location in KBs of the total number of connections/flows for all locations
- **Percentage of Locations** — The frequency of connections/flows involving this location as a percentage of the total number of connections/flows for all locations
- **Dropped** — Number of sessions/Connections dropped

Botnets

Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

The report provides the following information:

- **Botnet Name** — Name of the Botnet
- **Count** — Sessions or connections detected as a botnet

Web Categories

#	RATING NAME	COUNT	SESSIONS	
			COUNT	PERCENTAGE
1	Information Technology/Computer	15.54K		50%
2	Business and Economy	15.24K		49%
3	Web Communications	121		0%
4	Search Engines and Portals	90		0%
5	Computer and Internet Security	8		0%
6	Online Personal Storage	5		0%

Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

The report provides the following information:

- **Sessions** — Number of sessions/connections

The report provides the following information:

- **Rating Name** — The name of URL category
- **Count** — The frequency of access to URLs in this rating category in KBs of the total number of URL accesses
- **Percentage of Viruses** — The frequency of access to URLs in this rating category as a percentage of the total number of URL accesses

AppFlow Monitor

The **MONITOR | AppFlow > AppFlow Monitor** page displays a series of reports. Select the appropriate tab for one of the reports:

- [Applications](#)
- [Users](#)
- [Web Activity](#)
- [Initiator IPs](#)
- [Responder IPs](#)
- [Threats](#)
- [VoIP](#)
- [VPN](#)
- [Devices](#)
- [Contents](#)
- [Policies](#)

The **MONITOR | AppFlow > AppFlow Monitor** page enables you to monitor top-level aggregate reports of what is going on in your network and, at a quick glance, answer such questions as the following:

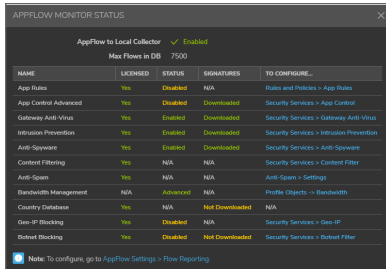
- What are the top-most used applications running in my network?
- Which applications in terms of total number of sessions and bytes consume my network bandwidth?
- Which applications have viruses, intrusions, and spyware?
- What website categories are my users visiting?

To enable and configure the reports, follow the procedures described in **Managing Flow Reporting Statistics** in the **SonicOS Logs** documentation. The green check mark icon at the top of the **MONITOR | AppFlow > AppFlow Monitor** page displays a link to the **DEVICE | AppFlow Settings > Flow Reporting** page, where you can configure the reports.

The top of the page displays the following settings and information:



- **+Create** – Click to create filtering on incidents
- **+Add to Filter** – Click to add filter criteria to selected applications
- **IP Version** – Select IPv4, IPv6, or IPv4 and IPv6 to view the reports on that traffic.
- **Slider** – Use the slider to filter flow results as of the Last 60 secs, 2 minutes, 10 minutes, 15 minutes, 30 minutes, 60 minutes, 3 hours, 6 hours, 12 hours, 24 hours, 7 days, 15 days, 30 days, or All Flows
- **Group By** – Filters results by grouping flows based on **Application**, **Category**, or **Signature**
- **Check mark** – Click or mouse over to expose a popup showing the Appflow Monitor Status. Links are provided to connect you to additional data.



- **Refresh** – Click to refresh the report data.

Applications

Applications							
#	APPLICATIONS	SESSIONS	TOTAL PACKETS	TOTAL BYTES	AVERAGE RATE (KBPS)	THREATS	
1	General HTTPS MGMT	31	180.26K	176.03 KB	1.494	0	
2	General TCP	4	720	720 B	-	0	
3	General DNS	1	1.56K	1.52 KB	0.224	0	

You can filter flows by **Application**. Applications can be grouped by **Application**, **Category**, or **Signature**.

These selections are defined as:

- **Application** — Name of the application - Signature ID
- **Sessions** — Number of connections or flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions or connections identified with intrusions, spyware, or a virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Users

#	USERS	SESSIONS	TOTAL PACKETS	TOTAL BYTES	AVERAGE RATE (KBPS)	THREATS
1	admin	47	183.02K	178.73 KB	0.208	0
2	unknown	5	1.72K	1.68 KB	0.121	0

The Users report allows filtering by **Users**. Users can be grouped the following:

- **User** — Name of the user- Signature ID
- **Sessions** — Number of connections/flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions/spyware/virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Web Activity

You can filter flows by **Web Activity**. Web URLs can be grouped by **Domain Name**, **URL**, or **Ratings**.

These selections are defined as:

- **Domain Name** — Name of the web domain
- **Add entry to filter** — Icon appears allowing you to add specific domain names into your filtering
- **Sessions** — Number of connections or flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions, spyware, or a virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Initiator IPs

#	INITIATOR IPS	SESSIONS	TOTAL PACKETS	TOTAL BYTES	AVERAGE RATE (KBPS)	THREATS
1		48	180.38K	176.15 KB	0.208	0
2		2	2.50K	2.44 KB	0.223	0
3		2	360	360 B	0.070	0

You can filter flows by **Initiator IP**. Initiator IPs can be grouped by **IP Address**, **Interface**, or **Country**.

These selections are defined as:

- **Initiator** — Name of the initiator IP address
- **Add entry to filter** — Icon appears allowing you to add specific initiator IP addresses into your filtering
- **Sessions** — Number of connections/flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions/spyware/virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Responder IPs

#	RESPONDER IPS	SESSIONS	TOTAL PACKETS	TOTAL BYTES	AVERAGE RATE (KBPS)	THREATS
1		55	205.04K	200.24 KB	0.541	0
2		4	720	720 B	0.070	0
3		2	2.01K	1.96 KB	0.246	0
4		1	503	503 B	0.240	0

You can filter flows by **Responder IPs**. Responder IPs can be grouped by **IP Address**, **Interface**, or **Country**.

These selections are defined as:

- **Responder** — Name of the responder IP address
- **Add entry to filter** — Icon appears allowing you to add specific responder IP addresses into your filtering
- **Sessions** — Number of connections or flows
- **Total Packets** — Number of packets

- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions, spyware, or a virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Threats

You can filter flows by **Threat**. Threats can be grouped as **All**, **Intrusion**, **Virus**, **Spyware**, **Anti-Spam**, or **Botnet**.

These selections are defined as:

- **Threat** — Name of the threat
- **Add entry to filter** — Icon appears allowing you to add specific threats into your filtering
- **Sessions** — Number of connections or flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions, spyware, or a virus

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

VoIP

You can filter flows by **VoIP**. VoIP can be grouped as **Media Type** or **Caller ID**.

These selections are defined as:

- **VoIP** — Name of the VoIP
- **Sessions** — Number of connections or flows.
- **Total Packets** — Number of packets.
- **Total Bytes** — Number of bytes sent by the initiator.
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections).
- **Out of Sequence/Lost Pkts** — Number of out of sequence or lost packets.
- **Average Jitter (msec)** — The average jitter or time delay between when a signal is transmitted and when it is received. It is measured in milliseconds.

- **Maximum Jitter (msec)** — The maximum amount of jitter between when a signal is transmitted and when it is received, measured in milliseconds.
- **Threats** — Number of sessions/connections identified with intrusions, spyware, or a virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

VPN

You can filter flows by **VPN**. VPN can be grouped by **Remote IP Address**, **Local IP Address**, or **Name**.

These selections are defined as:

- **VPN** — Name of the VPN
- **Sessions** — Number of connections/flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions/spyware/virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Devices

You can filter flows by **Device** IP address. Devices can be grouped by **IP Address**, **Interface**, **Name**, or **Vendor**.

These selections are defined as:

- **Device** — Name of the device
- **Sessions** — Number of connections/flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions/spyware/virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Contents

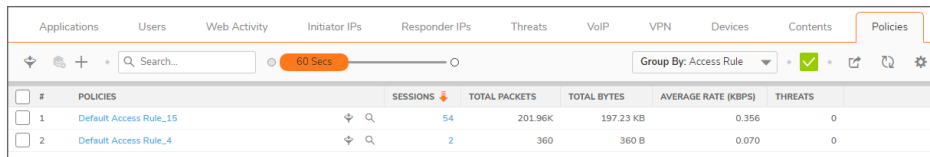
You can filter flows by **Contents**. Content can be grouped by **File Type** or **Email Address**.

These selections are defined as:

- **Content** — Name of the content
- **Sessions** — Number of connections/flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions/spyware/virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Policies



#	POLICIES	SESSIONS	TOTAL PACKETS	TOTAL BYTES	AVERAGE RATE (KBPS)	THREATS
1	Default Access Rule_15	54	201.96K	197.23 KB	0.356	0
2	Default Access Rule_4	2	360	360 B	0.070	0

You can filter flows by **Policies**. Security Policies can be grouped by **Access Rule**, **NAT Rule**, **Initiator Route Policy**, or **Responder Route Policy**.

These selections are defined as:

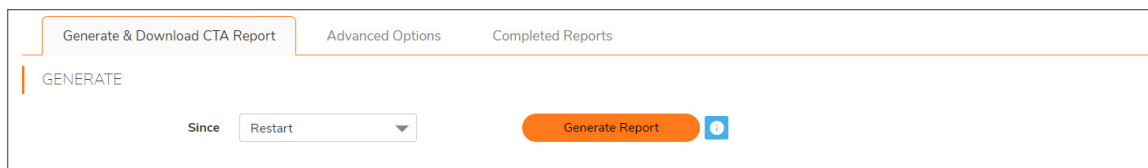
- **Policies** — Name of the security policy to be monitored
- **Sessions** — Number of connections or flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions, spyware, or a virus

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

CTA Report

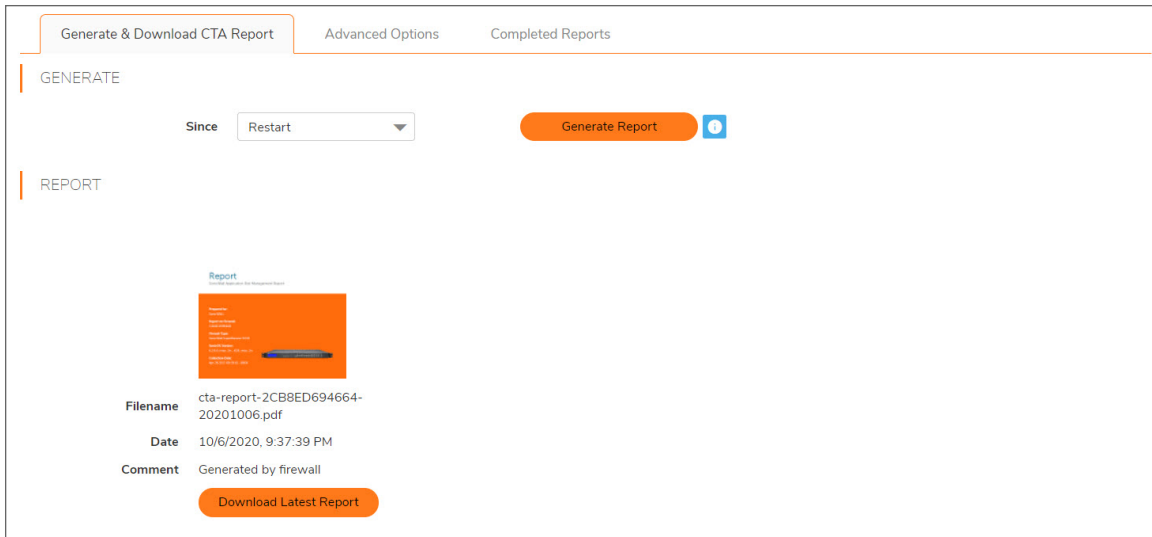
Use the Capture Threat Assessment (CTA) Report to generate a SonicFlow Report (SFR) that you can download and post to the Capture Threat Assessment service.

Generate & Download CTA Report



To generate and post the SonicFlow Report (SFR):

1. Navigate to the Capture Threat Assessment screen on the **MONITOR | AppFlow > CTA Report** page.
2. On the **Generate & Download CTA Report** tab, click **Generate Report**.
3. After the report is generated, you have the option to download the report or generate a new one.



4. Click **Download Report** to download the report.

Advanced Options

The values on the **Advance Options** tab are not saved to the firewall. Customized data is lost after you log out or clear your browser cache.

To configure Advanced CTA Report options:

1. Navigate to the **MONITOR | AppFlow > CTA Report** page.
2. Click the **Advanced Options** tab.

Generate & Download CTA Report | **Advanced Options** | Completed Reports

The values in this tab are not saved in the firewall. Customized data will be lost once you logout or clear your browser cache.

ADVANCED OPTIONS

Report Title About Text Top Chart Max Count

Company Name Contact Phone Preferred Industry

Preparer Name Contact Email

REPORT TYPE

Executive Summary Only ⓘ

SELECT SECTIONS

Application Highlights Glimpse Of Threats Botnet Analysis Top Users By Session

Risky Applications Malware Analysis Top Countries By Traffic Top Users By Traffic

Web Activity Exploits Used Top IPs By Session Report Configuration

File Transfer Investigation Known and Unknown Threats Top IPs By Traffic Shadow IT

CUSTOM LOGO

Provide custom logo image in base64 format ...

PNG in Base 64 Format ⓘ

3. Customize data for your CTA Reports using Advanced Options, Report Types, Desired Sections to appear, or include a customized Report logo.
4. After completing customized data entries, return to **Generate & Download CTA Report** and click **Generate Report**. The customized Report appears in the **Completed Reports** tab.

Completed Reports

Generate & Download CTA Report | Advanced Options | **Completed Reports**

Search...

#	FILENAME	DATE	LANGUAGE
1	cta-report-2CB8ED694664-20201006.pdf	2020/10/06 21:37:39	English

Total: 1 item(s)

Generated reports appear in the table and are available for download, viewing, and deleting.

SD-WAN

SD-WAN (Software-Defined Wide Area Network) provides software-based control over wide area network (WAN) connections.

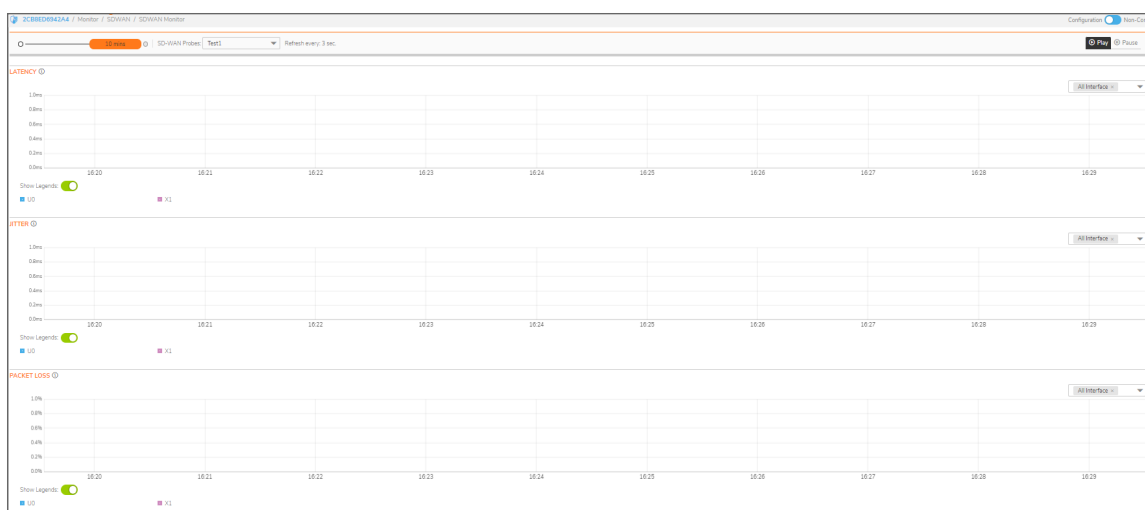
SD-WAN is best used for specific traffic types and/or applications requiring dynamically chosen optimal destination interfaces depending on how the network paths are behaving. To operate well, each application has a certain requirement from the network path. For example, the network quality for VoIP to operate well requires the optimal latency be 100 ms or less while a latency of 150 ms or higher results in choppy calls. SD-WAN helps in such scenarios by first dynamically measuring the various network SLA metrics, such as latency, jitter and packet loss on multiple network paths. SD-WAN then compares these metrics with the SLA threshold for a particular traffic flow and determines the optimal network that meets the flow's network quality accordingly.

From MONITOR | SDWAN, you can:

- [Monitoring SD-WAN](#)
- [Viewing SD-WAN Rules Connections](#)

Monitoring SD-WAN

① | **NOTE:** A chart may be empty or blank if there are no recent data entries received within the viewing range.



To monitor SD-WAN SLA:

1. Navigate to **Monitor | SD-WAN > SDWAN Monitor**.
2. From **SD-WAN Probes** drop-down box, select the SLA probe you would like to use to monitor.
3. Indicate the Refresh rate, in seconds, in the `Refresh Every` field.
4. Select a View Range:
 - **60 seconds** (default)
 - **2 minutes**
 - **5 minutes**
 - **10 minutes**
5. Choose an interface to track or select **All Interfaces** from the drop-down menu on the right side.

Viewing SD-WAN Rules Connections

You can view the connections that have been associated with SD-WAN Rules on the **Monitor | SDWAN > SD-WAN Connections** page.

- To view the activities associated with IPv4 SD-WAN Rules, click **IPv4** tab.
- To view the activities associated with IPv6 SD-WAN Rules, click **IPv6** tab.

SD-WAN CONNECTION DETAILS

SRC MAC	MAC address of the appliance that is the source of the connection.
SRC VENDOR	Name of the vendor of the appliance that is the source of the connection.
SRC IP	IP address of the appliance that is the source of the connection.
SRC PORT	Port on the appliance that is the source of the connection.
DST MAC	MAC address of the appliance that is the destination of the connection.
DST VENDOR	Name of the vendor of the appliance that is the destination of the connection.
DST IP	IP address of the appliance that is the destination of the connection.
DST PORT	Port on the appliance that is the destination of the connection.
PROTOCOL	Protocol used for the connection.
SRC IFACE	Interface on the appliance that is the source of the connection.
DST IFACE	Interface on the appliance that is the destination of the connection.
SRC ROUTE	Source route of the connection.
DST ROUTE	Destination route of the connection.
FLOW TYPE	Type of data flow control, such as FTP Control.
IPS CATEGORY	Internet Provider Security (IPS) category. If this information is not available or relevant, the column displays N/A.
ABR APP ID	App-Based Routing Application ID.
ABR CATEGORY ID	App-Based Routing Category ID.
EXPIRY (SEC)	Number of seconds until the connection expires.
TX BYTES	Number of bytes transmitted on the connection.
RX BYTES	Number of bytes received on the connection.
TX PKTS	Number of packets transmitted on the connection.

Rx PKTS	Number of packets received on the connection.
Flush	Displays the Flush icon. Clicking the icon flushes the connection.
Total	Total number of entries on the page. This is displayed at the bottom of the page.

You can perform the following actions on the SD-WAN Connections page:

- To search a log, enter a keyword related to an activity in the `Search` bar
- To filter the logs, click **Filter** icon, select the appropriate filter options, and then click **APPLY FILTERS**.
- To clear the filters applied, click **Clear Filter** icon
- To export the logs in CSV or TEXT files, click **Export** icon and select the required format
- To refresh the page, click **Refresh** icon

LOGS

- System Logs
- Auditing Logs
- Threat Logs

System Logs

The SonicWall network security appliance maintains an Event log for tracking potential security threats.

Topics:

- [Viewing System Logs](#)
- [System Log Functions](#)
- [Display Options](#)
- [Filtering the View](#)

Viewing System Logs

To view system events, navigate to **MONITOR | Logs > System Logs** page.

60 Secs											
Limit: 50											
Configure											
Filter Search...											
Clear Export Refresh Grid											
#	TIME	ID	CATEGORY	PRIORITY	MESSAGE	SOURCE	DESTINATION	INTERFACE	PROTOCOL	NOTES	OPERATION
1	02:27:08 Aug 8	84	Network	Notice	Failed to resolve name	-	-	-	-	Failed in DNS resolve nom-us-west-syslog.sonicwall.com	
2	02:27:06 Aug 8	972	VPN	Inform	IKEV2 Initiator: Remote party Timeout - Retransmitting IKEV2 Request.	10.5.95.139, 4500	52.42.109.76, 4500	udp	udp	VPN Policy: SGMSServer-VPN;	
3	02:26:55 Aug 8	972	VPN	Inform	IKEV2 Initiator: Remote party Timeout - Retransmitting IKEV2 Request.	10.5.95.139, 4500	52.42.109.76, 4500	udp	udp	VPN Policy: SGMSServer-VPN;	
4	02:26:50 Aug 8	973	VPN	Inform	IKEV2 Initiator: Received IKE_SA_INIT response	52.42.109.76, 500	10.5.95.139, 500	udp	udp	VPN Policy: SGMSServer-VPN;	
5	02:26:50 Aug 8	943	VPN	Inform	IKEV2 Accept IKE SA Proposal	52.42.109.76, 500	10.5.95.139, 500	udp	udp	VPN Policy: SGMSServer-VPN; 3DES; HMAC_SHA1_96; DH Group 2; IKEV2 InitiSP: 0a3b44ff1a7a77c97; IKEV2 RespSP: 0x64193c3be10d46e	
6	02:26:50 Aug 8	985	VPN	Inform	IKEV2 NAT device detected between negotiating peers	52.42.109.76, 500	10.5.95.139, 500	udp	udp	VPN Policy: SGMSServer-VPN; Local and Peer gateway are behind a NAT Device	
7	02:26:50 Aug 8	940	VPN	Inform	IKEV2 Initiator: Send IKE_AUTH Request	10.5.95.139, 4500	52.42.109.76, 4500	udp	udp	VPN Policy: SGMSServer-VPN;	
8	02:26:49 Aug 8	938	VPN	Inform	IKEV2 Initiator: Send IKE_SA_INIT Request	10.5.95.139, 500	52.42.109.76, 500	udp	udp	VPN Policy: SGMSServer-VPN;	
9	02:26:49 Aug 8	971	VPN	Warning	IKEV2 Peer is not responding. Negotiation aborted.	10.5.95.139, 4500	52.42.109.76, 4500	udp	udp	VPN Policy: SGMSServer-VPN; Failed 5 retries; IKEV2 InitiSP: 0a609992446850804; IKEV2 RespSP: 0x6c70a79975655007	
10	02:26:39 Aug 8	972	VPN	Inform	IKEV2 Initiator: Remote party Timeout - Retransmitting IKEV2 Request.	10.5.95.139, 4500	52.42.109.76, 4500	udp	udp	VPN Policy: SGMSServer-VPN;	
11	02:26:29 Aug 8	972	VPN	Inform	IKEV2 Initiator: Remote party Timeout - Retransmitting IKEV2 Request.	10.5.95.139, 4500	52.42.109.76, 4500	udp	udp	VPN Policy: SGMSServer-VPN;	
12	02:26:19 Aug 8	972	VPN	Inform	IKEV2 Initiator: Remote party Timeout - Retransmitting IKEV2 Request.	10.5.95.139, 4500	52.42.109.76, 4500	udp	udp	VPN Policy: SGMSServer-VPN;	

For a description of the:

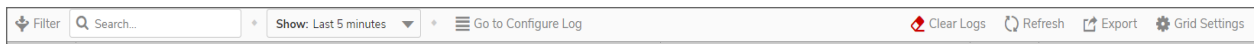
- Functions, see [System Log Functions](#)
- Columns, see [Display Options](#)

System Log Functions



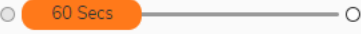
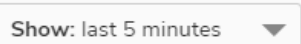
The System Log table provides numerous settings to allow you to navigate, view, and export results. Table columns can be customized, so that you can view full data on any event, or only the data you need. Table entries can be sorted to display in either ascending or descending order.





To sort the entries in the Event Log, click the column heading. The entries are sorted by ascending or descending order. The arrow to the right of the column name indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

The top row of the Event Log contains various functions. Functions pertaining only to Event Logs are described in the below table.



SYSTEM EVENT LOG FUNCTIONS

Option	Function	Action
	Filter	Set the filter for any specific log in the Event Log. You can set the filters based on GENERAL, SOURCE, and DESTINATION categories. For more information, refer to Filtering the View .
	Search	The Event Log displays the log entries that match the search string.
	Time Interval	Set the slider to filter the Event Log based on the time interval for the Event Log. You can set the slider anywhere between 60 Sec to 365 days.
	Show	Select the interval for the Event Log. The event logs from that period are displayed: <ul style="list-style-type: none"> • Last 60 seconds • Last 2 minutes • Last 5 minutes (default) • Last 10 minutes • Last 15 minutes • Last 30 minutes • Last 60 minutes • Last 3 hours • Last 6 hours • Last 12 hours • Last 24 hours • Last 7 days • Last 15 days • Last 30 days • All entries


 Refresh	Refresh	Click to refresh the system log data.
 Configure	Configure Log	Click this link and you are navigated to DEVICE Log > Settings to configure the items which needs to be tracked in the Event Log.
 Clear	Clear Logs	Click to clear the logs from the table.
 Export	Export	Click to export the logs in CSV, TXT files, and email

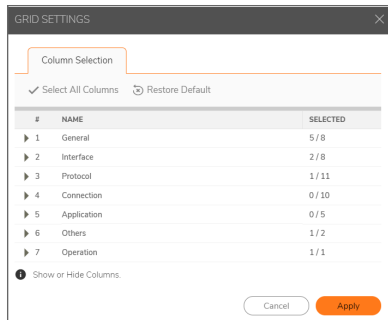
Display Options

Customize the Events log to display as many or few columns that meet your needs.

To select which columns to display:

1. Navigate to **MONITOR | Logs > System Logs**.

2. Click  **Grid Settings** icon . The **Grid Settings** dialog displays:



3. Select the items you want to appear as columns in the System Log.

General	General information about the log event.
Time	Local date and time the event occurred. i IMPORTANT: This option is selected by default. It is dimmed, and cannot be deselected.
ID	Identifying number for the event. i IMPORTANT: This option is selected by default. It is dimmed, and cannot be deselected.
Category	Category of the event. This option is selected by default.
Group	Group designation of the event.
Event	Name of the event.
Msg Type	Type of message; usually Standard Message String.
Priority	Priority level of the event, such as Inform (information) or Error. i IMPORTANT: This option is selected by default.
Message	Information about the event.

Interface	Information about the protocol of the packet triggering the event.	
	Source	Name of the source device, if applicable. This option is selected by default.
	Source IP	IP address of the source device.
	Source Port	Port number of the source.
	Source Interface	Source network and IP address, if applicable.
	Destination	Name of the destination device, if applicable. This option is selected by default.
	Destination IP	IP address of the destination device.
	Destination Port	Port number of the destination.
	Destination Interface	Destination network and IP address, if applicable.
Protocol	Information about the NAT policy in effect, if any.	
	Source Name	Protocol source name.
	Source NAT IP	Source address from the Source NAT IP address pool.
	Source NAT Port	Port number for the Source NAT.
	In SPI	Indicates whether the ingress packet is in Stateful Packet Inspection (SPI) mode, if applicable.
	Destination Name	Protocol destination name.
	Destination NAT IP	Destination address from the Source NAT IP address pool.
	Destination NAT Port	Port number for the Destination NAT.
	Out SPI	Indicates whether the egress packet is in Stateful Packet Inspection (SPI) mode, if applicable.
	IP Protocol	Protocol used to send error and control messages, if known. This option is selected by default.
	ICMP Type	ICMP packet's ICMP type, if known.
	ICMP Code	ICMP packet's ICMP code, if known.

Connection	Information about SPI, Access and IDP Rules, and policies, if any.	
	TX Bytes	Number of bytes transmitted.
	RX Bytes	Number of bytes received.
	Access Rule	Name of the Access Rule triggering the event, if any.
	NAT Policy	Name of the NAT policy.
	VPN Policy	Name of the VPN policy triggering the event, if any.
	User Name	Name of the user whose action triggered the event.
	Session Time	Duration of the session before the event.
	Session Type	Type of session triggering the event.
	IDP Rule	Name of the IDP Rule triggering the event, if any.
	IDP Priority	Priority of the IDP Rule.
Application	Information about the application being used.	
	HTTP OP	NPCS object op requestMethod HTTP OP code.
	URL	URL of the NPCS object op requestMethod HTTP OP code.
	HTTP Result	HTTP result code (such as, 200, 403) of Website hit rpkt cn1Label Packet received.
	Block Category	Block category that triggered the event.
	Application	The application being used.
Others	Information about the user, session, and application, if known.	
	FW Action	Configured firewall action. If no action has been specified, displays N/A.
	Notes	Includes notes. This option is selected by default.

4. When done, click **Apply** to preserve any changes or click **Restore Default** to revert back to the default settings.

You can perform the following actions on the System Logs page:

- To export the logs in CSV, TXT files, and email, click **Export** icon and select the required format
- To clear the logs from the table, click **Clear Logs** icon
- To refresh the page, click **Refresh** icon
- To view more details of the log, click the triangle icon of the log

Filtering the View

The Filter View input field at the top left corner of the System Log enables you to narrow your search using drop-down options and search strings.

To filter the System Event logs:

1. Navigate to **MONITOR | Logs > System Logs**.
2. Click **Filter** icon.

GENERAL	SOURCE	DESTINATION
Priority Any	Source Interface Any	Destination Interface Any
Category Any	Source IP Source IP Address ...	Destination IP Destination IP Address ...
IP Protocol IP Type name or code...	Source Port Source Port Number ...	Destination Port Destination Port Number ...

3. Select any filtering scheme you want. Filter on just one field or you can filter on all of them. In the General, Source and Destination fields, you can enter a partial string to filter on.
4. Click **Accept**.
OR
Click **Reset** to clear the filters applied.

Auditing Logs

This section describes in detail the recording feature that collects and records information on any changes in the security appliance configuration. To access this feature, navigate to **MONITOR | Logs > Auditing Logs** in the SonicOS web management interface.

What is Configuration Auditing

Configuration auditing is a feature that automatically records any configuration changes that an administrator attempts from one of the available user interfaces, web management (via HTTP and HTTPS), command line (via console or SSH), or SonicWall GMS. A configuration auditing records table is created to record all attempted configuration changes, both successful and failed. With configuration auditing, SonicOS archives the history of its configuration changes, so that the administrator or others can later revisit and analyze the records. This feature is enabled by default for the platforms where it is available.

Benefits of Configuration Auditing

Auditing of configuration change records can be useful as described below:

- Automatic documentation of any configuration changes performed by an administrator
- Assistance in troubleshooting unexpected changes in run-time system behavior
- Visibility, continuity, and consistency where there are several administrators, either simultaneously or consecutively. Each administrator has access to a record of changes performed or attempted by all other administrators.
- Third party integration with Firewall Manager, SEIM systems, logging and reporting solutions
- Compliance with regulations such as SOX, FISMA, NIST, DISA STIP

What Information is Recorded

Configuration auditing generates a record for every configuration change. The record includes:

- Which parameter was changed
- When the change was made
- Who made the change
- From where the change was made
- Details of the change, such as the previous and subsequent values

What Information is Not Recorded

The following are not included in the Configuration Auditing operation:

- Importing a Settings File - Configuration changes due to importing a settings file are currently not recorded by the configuration auditing feature. Since all current settings are cleared prior to applying imported configurations, the assumption is that all existing configurations are modified.
- WXA configuration settings — SonicOS does not audit any configuration changes in WAN Acceleration. Some settings are saved on the WXA instead of the firewall, although the settings can be configured from the SonicOS web management interface.
- ZEBOS settings for BGP/OSPF/RIP routing configurations — SonicOS stores these settings as one long string of ZEBOS CLI commands. Records of changes made by these commands are not duplicated in the configuration auditing operation.
- Anti-Spam Junk Store applications — Configuration settings changed through a proxy server running a junk store are excluded from configuration auditing.
- Licensing - All aspects of system licensing are authenticated through MySonicWall, and are not recorded through configuration auditing.
- Uploading a file from **Home > Capture ATP** does not audit uploading a file from the page, because the contents of this page do not reside on the firewall.

Audit Recording in High Availability Configurations

The Configuration Auditing operation records changes individually for each device. It does not synchronize the recorded information between appliances in an HA pair. When the active HA unit next synchronizes with the standby HA unit, it sends configuration changes to the standby unit. The synchronization operation information

updates the auditing record of the standby device in the pair. On the standby unit, the auditing record indicates that the configuration changes it recorded came from the active unit.

Modifying and Supplementing Configuration Auditing

Configuration Auditing operations can be modified and supplemented through the following:

SNMP Trap Control

SNMP (Simple Network Management Protocol) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks. SNMP traps allow the user to monitor security appliance status and configuration through a Management Information Database (MIB). Configuration auditing works in conjunction with SNMP by giving the user the option to enable a trap for each logged event collected during a network configuration change, whether successful or failed.

E-CLI Commands

E-CLI (Enterprise Command Line Interface) commands are available for configuration auditing record setting and display, for those administrators who like to work from the command line. You can use the following E-CLI commands to enable or disable configuration auditing and to view records:

to work with settings:

```
config(C0EAE49CE84C)# log audit settings
```

```
(config-audit)# enable
```

```
(config-audit)# debug
```

```
(config-audit)# auditall
```

```
(config-audit)# commit
```

to show audit records:

```
(config-audit)# show log audit view
```

Auditing Record Storage and Persistence

Configuration auditing records are saved to non-volatile storage (such as flash), so that records can be restored, if required, after a reboot. The number of records saved is directly proportional to the capability of the device, as

defined in the product matrix below. Higher-end platforms can store more records than lower-end devices. Devices with no flash or smaller flash capacity do not support configuration auditing.

All configuration auditing records, on any platform, are deleted when the appliance is rebooted with factory defaults.

Managing the Audit Logs Table

The administrator can manage the auditing records in many useful ways. The following activities are available:

Topics:

- [Viewing Auditing Logs](#)
- [Manually Emailing Auditing Logs](#)
- [Exporting Auditing Logs](#)
- [Refreshing the Auditing Logs](#)
- [Displaying the Auditing Logs on the console](#)
- [Auditing All Parameters During Addition](#)

Viewing Auditing Logs

The **MONITOR | Logs > Auditing Logs** page displays all the configuration auditing records. It allows a user to view, search, and sort the records.

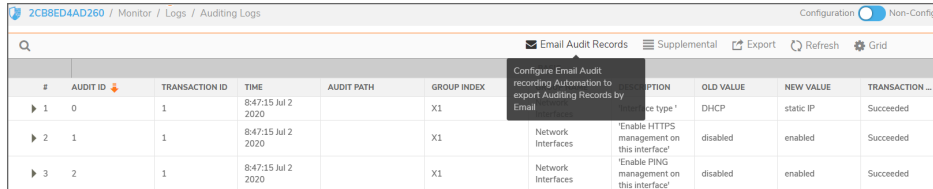
- The first column is expandable to display the summary of the log entry.
- There are also buttons for **Select all Columns** and **Restore Default** for ease of operation. Click **Grid Settings** icon to perform the desired action.
- The user can search for a specific string pattern and highlight the matched results, if any are found.
- Failed configuration changes are marked in red.
- All columns are sortable.

#	Audit ID	Transaction ID	Time	Audit Path	Group Index	Group Name	Description	Old Value	New Value	Transaction ...
▶ 1	0	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Interface type'	DHCP	static IP	Succeeded
▶ 2	1	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable HTTPS management on this interface'	disabled	enabled	Succeeded
▶ 3	2	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable PING management on this interface'	disabled	enabled	Succeeded
▶ 4	3	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Static IP Address'	0.0.0.0	10.5.193.110	Succeeded
▶ 5	4	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Static Subnet Mask'	255.255.255.0	255.255.254.0	Succeeded
▶ 6	5	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Static Gateway IP Address'	0.0.0.0	10.5.192.1	Succeeded

Manually Emailing Auditing Logs

When a valid mail server and email address are configured, the user can click the email button on the tool bar of the Auditing Records page to manually email auditing records at any time. The button is disabled if either the mail server or the email address is not configured under **DEVICE | Log > Automation**.

The **DEVICE | Log > Automation** page includes settings for configuring the SonicWall to send log files using Email and configuring mail server settings.

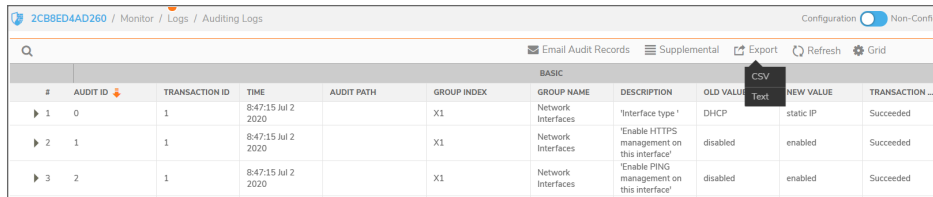


The screenshot shows the 'Auditing Logs' page with a toolbar containing 'Email Audit Records', 'Supplemental', 'Export', 'Refresh', and 'Grid'. A tooltip is visible over the 'Email Audit Records' button, indicating it is used to manually email auditing records.

#	AUDIT ID	TRANSACTION ID	TIME	AUDIT PATH	GROUP INDEX	DESCRIPTION	OLD VALUE	NEW VALUE	TRANSACTION ...
▶ 1	0	1	8:47:15 Jul 2 2020		X1	'Interface type'	DHCP	static IP	Succeeded
▶ 2	1	1	8:47:15 Jul 2 2020		X1	'Enable HTTPS management on this interface'	disabled	enabled	Succeeded
▶ 3	2	1	8:47:15 Jul 2 2020		X1	'Enable PING management on this interface'	disabled	enabled	Succeeded

Exporting Auditing Logs

There are two export options for auditing records. You can export the records as a text file or as a CSV file.

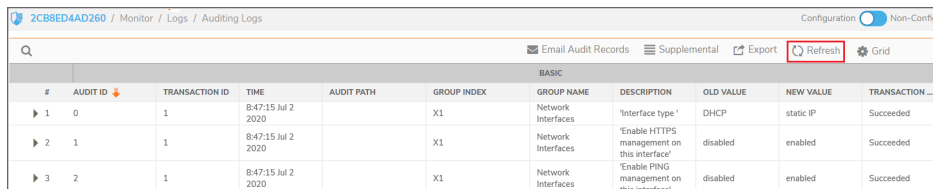


The screenshot shows the 'Auditing Logs' page with the 'Export' button highlighted. A tooltip indicates that the export options are 'CSV' and 'Text'.

#	AUDIT ID	TRANSACTION ID	TIME	AUDIT PATH	GROUP INDEX	GROUP NAME	DESCRIPTION	OLD VALUE	NEW VALUE	TRANSACTION ...
▶ 1	0	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Interface type'	DHCP	static IP	Succeeded
▶ 2	1	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable HTTPS management on this interface'	disabled	enabled	Succeeded
▶ 3	2	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable PING management on this interface'	disabled	enabled	Succeeded

Refreshing the Auditing Logs

The **Refresh** button provides a way to refresh the page and display the latest auditing records, as seen below:



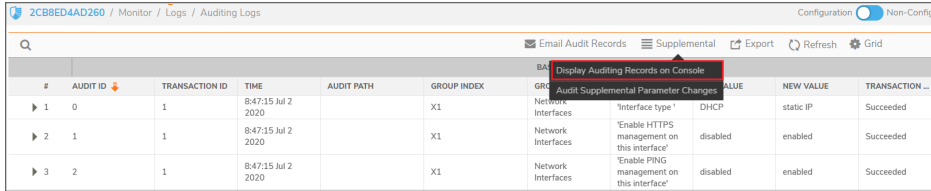
The screenshot shows the 'Auditing Logs' page with the 'Refresh' button highlighted in the toolbar.

#	AUDIT ID	TRANSACTION ID	TIME	AUDIT PATH	GROUP INDEX	GROUP NAME	DESCRIPTION	OLD VALUE	NEW VALUE	TRANSACTION ...
▶ 1	0	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Interface type'	DHCP	static IP	Succeeded
▶ 2	1	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable HTTPS management on this interface'	disabled	enabled	Succeeded
▶ 3	2	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable PING management on this interface'	disabled	enabled	Succeeded

Displaying the Auditing Logs on the console

To view the auditing records:

1. Navigate to **MONITOR | Logs > Auditing Logs**.
2. Click **Supplemental > Display Auditing Records on Console** option to display the auditing records on the console in a text format.



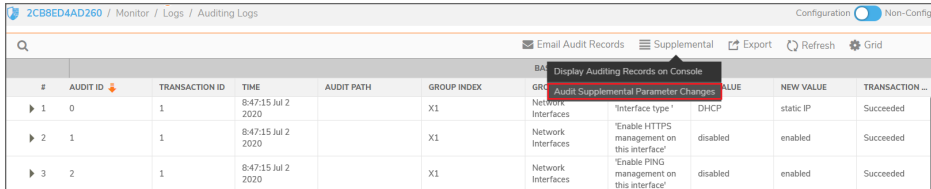
#	AUDIT ID	TRANSACTION ID	TIME	AUDIT PATH	GROUP INDEX	GRG	ALUE	NEW VALUE	TRANSACTION ...	
▶ 1	0	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Interface type'	DHCP	static IP	Succeeded
▶ 2	1	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable HTTPS management on this interface'	disabled	enabled	Succeeded
▶ 3	2	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable PING management on this interface'	disabled	enabled	Succeeded

Auditing All Parameters During Addition

By default, configuration auditing only logs significant changes, defined as changes where the new value of the parameter is different from the default value.

To view the updated parameter changes during addition activity:

1. Navigate to **MONITOR | Logs > Auditing Logs**.
2. Click **Supplemental > Audit Supplemental Parameter Changes** option to record all parameter changes during an addition activity, even when the new values are the same as the default values.



#	AUDIT ID	TRANSACTION ID	TIME	AUDIT PATH	GROUP INDEX	GRG	ALUE	NEW VALUE	TRANSACTION ...	
▶ 1	0	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Interface type'	DHCP	static IP	Succeeded
▶ 2	1	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable HTTPS management on this interface'	disabled	enabled	Succeeded
▶ 3	2	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable PING management on this interface'	disabled	enabled	Succeeded

Threat Logs

This section describes in detail the recording feature that collects and records information on any changes in the security appliance configuration. To access this feature, navigate to **MONITOR | Logs > Threat Logs** in the SonicOS web management interface.

#	TIME	USERNAME	VIRUS	INTRUSION	SPYWARE	BOTNET	START TIME	LAST UPDATED	INITIATOR IP	RESPONDER
No Data										

Topics:

- [Viewing Threat Logs](#)
- [Threat Log Functions](#)
- [Display Options](#)

Viewing Threat Logs

To view threat events, navigate to **MONITOR | Logs > Threat Logs** page.

For a description of the:

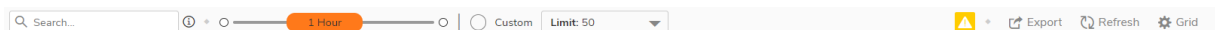
- Functions, see [Threat Log Functions](#)
- Columns, see [Display Options](#)

Threat Log Functions

The Threat Log table provides numerous settings to allow you to navigate, view, and export results. Table columns can be customized, so that you can view full data on any event, or only the data you need. Table entries can be sorted to display in either ascending or descending order.

To sort the entries in the Event Log, click the column heading. The entries are sorted by ascending or descending order. The arrow to the right of the column name indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

The top row of the Event Log contains various functions. Functions pertaining only to Event Logs are described in the below table.




SYSTEM EVENT LOG FUNCTIONS

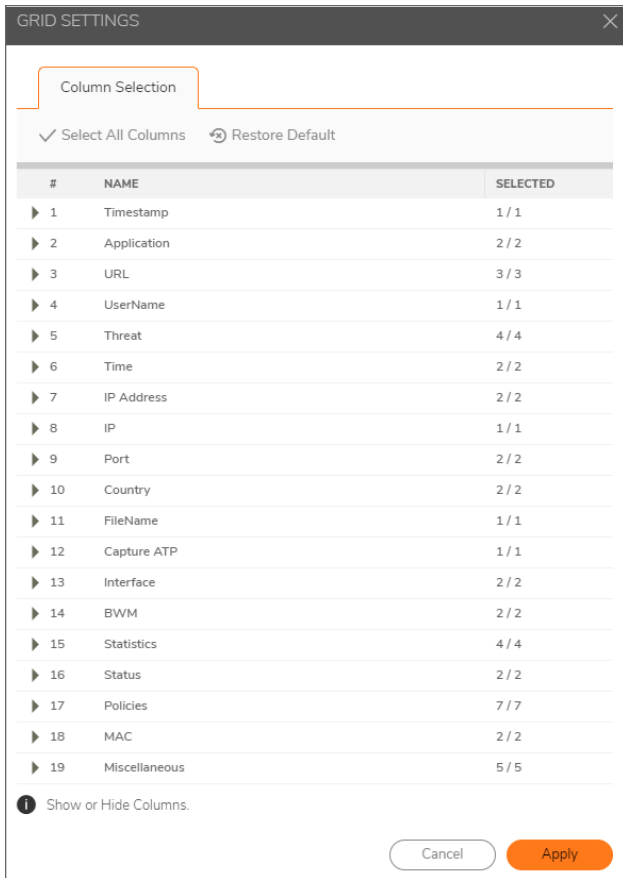
Option	Function	Action
<input type="text" value="Search..."/>	Search	The Event Log displays the log entries that match the search string.
<input type="range" value="60 Secs"/>	Time Interval	Set the slider to filter the Event Log based on the time interval for the Event Log. You can set the slider anywhere between 60 Sec to 365 days.
<input type="radio"/> Custom <input type="text" value="Limit: 50"/>	Custom	Select the interval for the Event Log. The event logs displays the maximum entries in the table based on selection. <ul style="list-style-type: none"> • 10 • 25 • 50 • 100 • 250 • 500 • 1000 • 8000 (Max)
<input type="button" value="Refresh"/>	Refresh	Click to refresh the log data.
<input type="button" value="Export"/>	Export	Click to export the logs.

Display Options

Customize the Events log to display as many or few columns that meet your needs.

To select which columns to display:

1. Navigate to **MONITOR | Logs > Threat Logs**.
2. Click  **Grid** icon . The **Grid Settings** dialog displays:



3. Select the items you want to appear as columns in the Threat Log.

Category Name	Column
Timestamp	Time
Application	Application
	Component
URL	URL
	URL Rating
	URL Severity
User Name	User Name
Threat	Virus
	Intrusion
	Spyware
	Botnet
Time	Start Time
	Last Updated

Category Name	Column
IP Address	Initiator IP
	Responder IP
IP	Protocol Name
Port	Initiator Port
	Responder Port
Country	Initiator
	Responder
FileName	FileName
Capture ATP	Action
Interface	Initiator Interface
	Initiator Interface
BWM	Inbound Priority
	Outbound Priority
Statistics	All Counters
	Initiator Bytes
	Responder Bytes
Status	Flow Status
	Blocked Reason
Policies	Security Rule
	NAT Rule
	Init Route Rule
	Resp Route Rule
	Decryption SSL Rule
	Decryption SSH Rule
	DoS Rule
MAC	Init MAC
	Responder MAC
Miscellaneous	Initiator Gateway
	Responder Gateway
	Initiator VPN Name
	Gateway VPN Name

- When done, click **Apply** to preserve any changes or click **Restore Default** to revert back to the default settings.

TOOLS AND MONITOR

- [Using Packet Monitor](#)
- [Viewing Connections](#)
- [Monitoring Core 0 Processes](#)
- [Using Packet Replay](#)

Using Packet Monitor

The Packet Monitor is a mechanism that allows you to monitor individual data packets that traverse your SonicWall network security appliance. Packets can be either monitored or mirrored. The monitored packets contain both data and addressing information. Addressing information from the packet header includes the following:

- Interface identification
- MAC addresses
- Ethernet type
- Internet Protocol (IP) type
- Source and destination IP addresses
- Port numbers
- L2TP payload details
- PPP negotiations details

You can configure the packet monitor feature in the enhanced management interface. The management interface provides a way to configure the monitor criteria, display settings, mirror settings, and file export settings, and displays the captured packets.

Current configurations are displayed on this page, hover over the information symbols to view the details.

Topics:

- [Benefits of Packet Monitor](#)
- [How Does Packet Monitor Work?](#)
- [Supported Packet Types](#)
- [Configuring Packet Monitor](#)
- [Monitoring Captured Packets](#)
- [Viewing Packet Monitoring Statistics](#)

Benefits of Packet Monitor

The packet monitor feature provides the functionality and flexibility that you need to examine network traffic without the use of external utilities, such as Wireshark (formerly known as Ethereal). Packet monitor includes the following features:

- Control mechanism with improved granularity for custom filtering (Monitor Filter)
- Display filter settings independent from monitor filter settings
- Packet status indicates if the packet was dropped, forwarded, generated, or consumed by the firewall
- Three output displays in the management interface:
 - List of packets
 - Decoded output of selected packet
 - Hexadecimal dump of selected packet
- Export capabilities include text or HTML format with hex dump of packets, plus CAP file formats, pcap and pcapNG
- Automatic export to FTP server when the buffer is full
- Bidirectional packet monitor based on IP address and port
- Configurable wrap-around of packet monitor buffer when full

How Does Packet Monitor Work?

As an administrator, you can configure the general settings, monitor filter, display filter, advanced filter settings, and FTP settings of the packet monitor tool. As network packets enter the packet monitor subsystem, the monitor filter settings are applied, and the resulting packets are written to the capture buffer. The display filter settings are applied as you view the buffer contents in the management interface. You can log the capture buffer to view in the management interface, or you can configure automatic transfer to the FTP server when the buffer is full.

Default settings are provided so that you can start using packet monitor without configuring it first. The basic functionality is:

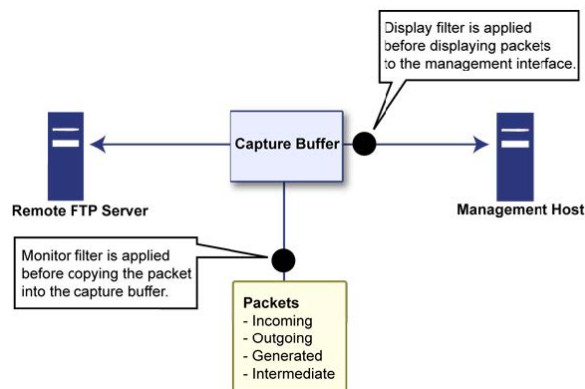
PACKETS: BASIC FUNCTIONALITY

Start: Click Start Capture to begin capturing all packets except those used for communication between the firewall and the management interface on your console system.

Stop: Click Stop Capture to stop the packet capture.

Refer to [Configuring Packet Monitor](#) for a high-level view of the packet monitor subsystem that shows the different filters and how they are applied.

PACKET MONITOR SUBSYSTEM SHOWING FILTERS



Supported Packet Types

When specifying the Ethernet or IP packet types that you want to monitor or display, you can use either the standard acronym for the type, if supported, or the corresponding hexadecimal representation. To determine the hex value for a protocol, refer to the RFC for the number assigned to it by IANA.

Supported Types	Protocol Acronyms	Notes
Supported Ethernet Types	<ul style="list-style-type: none">• ARP• IP• PPPoE-DIS• PPPoE-SES	To specify both PPPoE-DIS and PPPoE-SES, you can simply use PPPoE.
Supported IP Types	<ul style="list-style-type: none">• TCP• UDP• ICMP• IGMP• GRE• AH• ESP	

Configuring Packet Monitor

You can access the packet monitor tool on the **Monitor > Tools & Monitors > Packet Monitor** page of the management interface. There are six main areas of configuration for packet monitor, one of which is specifically

for packet mirror. The following sections describe the configuration options, and provide procedures for accessing and configuring the filter settings, log settings, and mirror settings:

Topics:

- [Configuring General Settings](#)
- [Monitoring Captured Packets](#)
- [Viewing Packet Monitoring Statistics](#)

Configuring General Settings

Topics:

- [Configuring General Settings](#)
- [Configuring the Monitor Filter](#)
- [Configuring Display Filter Settings](#)
- [Configuring Logging Settings](#)
- [Configuring Advanced Monitor Filter Settings](#)
- [Configuring Mirror Settings](#)

Configuring General Settings

This section describes how to configure packet monitor general settings, including the number of bytes to capture per packet and the buffer wrap option. You can specify the number of bytes using either decimal or hexadecimal, with a minimum value of 64. The buffer wrap option enables the packet capture to continue even when the buffer becomes full, by overwriting the buffer from the beginning.

To configure the general settings:

1. Navigate to the **Monitor > Tools & Monitors > Packet Monitor** page.
2. Select the **General** tab.
3. Select the **Settings** tab.

4. In the **Number of Bytes To Capture (per packet)** box, type the number of bytes to capture from each packet. The minimum value is 64 and the maximum value is 65535.
5. To continue capturing packets after the buffer fills up, select **Wrap Capture Buffer Once Full**. Selecting this option causes packet capture to start writing captured packets at the beginning of the buffer again after the buffer fills. This option has no effect if FTP server logging is enabled on the **Logging** tab, because the buffer is automatically wrapped when FTP is enabled.
6. Under Exclude Filter, select **Exclude encrypted GMS traffic** to prevent capturing or mirroring of encrypted management or syslog traffic to or from SonicWall GMS. This setting only affects encrypted traffic within a configured primary or secondary GMS tunnel. GMS management traffic is not excluded if it is sent through a separate tunnel.
7. Use the **Exclude Management Traffic** settings to prevent capturing or mirroring of management traffic to the appliance. Select the checkbox for each type of traffic (HTTP/HTTPS, SNMP, or SSH) to exclude. If management traffic is sent through a tunnel, the packets are not excluded.
8. Use the **Exclude Syslog Traffic** to settings to prevent capturing or mirroring of syslog traffic to the logging servers. Select the checkbox for each type of server (Syslog Servers or GMS Server) to exclude. If syslog traffic is sent through a tunnel, the packets are not excluded.
9. Use the **Exclude Internal Traffic** for settings to prevent capturing or mirroring of internal traffic between the SonicWall network security appliance and its High Availability partner or a connected SonicPoint. Select the checkbox for each type of traffic (HA, SonicPoint, BCP, Inter-Blade, or Back-Plane) to exclude.
10. To save your settings and exit the configuration window, click **Save**.

Configuring the Monitor Filter

All filters set on the Monitor Filter page are applied to both packet capture and packet mirroring.

To configure Monitor Filter settings:

1. Navigate to the **Tools & Monitors > Packet Monitor** page.
2. Select the **General** tab.
3. Select the **Monitor Filter** tab.

Captured Packets | **General** | Statistics

Settings | **Monitor Filter** | Display Filter | Logging | Advanced Monitor Filter | Mirror

MONITOR FILTER (USED FOR BOTH MIRRORING AND PACKET CAPTURE)

Enable filter based on the security policy /app rule ⓘ

Interface Name(s) ⓘ

Ether Type(s) ⓘ

IP Type(s) ⓘ

Source IP Address(es) ⓘ

Source Port(s) ⓘ

Destination IP Address(es) ⓘ

Destination Port(s) ⓘ

Enable Bidirectional Address and Port Matching ⓘ

Monitor (Leave all checkboxes unchecked for normal operation. Unchecked means capture all type of packets.)

Forwarded packets only

Consumed packets only

Dropped packets only

Default Cancel Save

4. Choose **Enable filter based on the firewall/app rule** if you are using firewall rules to capture specific traffic.
Before the **Enable filter based on the firewall rule** option is selected, be certain you have selected one or more access rules on which to monitor packet traffic. This configuration is done from the **POLICY > Rules and Policies > Access Rules** page.
5. Specify how Packet Monitor filters packets using these options:
 - **Interface Name(s)** - You can specify up to ten interfaces separated by commas. Refer to the **Network > Interfaces** page in the management interface for the available interface names. You can use a negative value to configure all interfaces except the one(s) specified; for example: !X0, or !LAN.
 - **Ether Type(s)** - You can specify up to ten Ethernet types separated by commas. Currently, the following Ethernet types are supported:
 - ARP
 - IP
 - PPPoE-SES
 - PPPoE-DIS

The latter two can be specified by PPPoE alone.

This option is not case-sensitive. For example, to capture all supported types, you could enter: `ARP, IP, PPPoE`. You can use one or more negative values to capture all Ethernet types except those specified; for example: `!ARP, !PPPoE`. You can also use hexadecimal values to represent the Ethernet types, or mix hex values with the standard representations; for example: `ARP, 0x800, IP`. Normally, you would only use hex values for Ethernet types that are not supported by acronym in SonicOS. (Refer to [Supported Packet Types](#) for more information.)

- **IP Type(s)** - You can specify up to ten IP types separated by commas. These IP types are supported:
 - TCP
 - UDP
 - ICMP
 - GRE
 - IGMP
 - AH
 - ESP

You can use one or more negative values to capture all IP types except those specified; for example: `!TCP, !UDP`. You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: `TCP, 0x1, 0x6`. (Refer to [Supported Packet Types](#) for more information.) This option is not case-sensitive.

- **Source IP Address(es)** - You can specify up to ten IP addresses separated by commas; for example: `10.1.1.1, 192.2.2.2`. You can use one or more negative values to capture packets from all but the specified addresses; for example: `!10.3.3.3, !10.4.4.4`.
- **Source Port(s)** - You can specify up to ten TCP or UDP port numbers separated by commas; for example: `20, 21, 22, 25`. You can use one or more negative values to capture packets from all but the specified ports; for example: `!80, !8080`.
- **Destination IP Address(es)** - You can specify up to ten IP addresses separated by commas; for example: `10.1.1.1, 192.2.2.2`. You can use one or more negative values to capture packets destined for all but the specified addresses; for example: `!10.3.3.3, !10.4.4.4`.
- **Destination Port(s)** - You can specify up to ten TCP or UDP port numbers separated by commas; for example: `20, 21, 22, 25`. You can use one or more negative values to capture packets destined for all but the specified ports; for example: `!80, !8080`.
- **Enable Bidirectional Address and Port Matching** - When this option is selected, IP addresses and ports specified in the **Source** or **Destination** fields on this page are matched against both the source and destination fields in each packet.
- **Forwarded packets only** - Select this option to monitor any packets that are forwarded by the firewall.
- **Consumed packets only** - Select this option to monitor all packets that are consumed by internal sources within the firewall.

- **Dropped packets only** - Select this option to monitor all packets that are dropped at the perimeter.
- ① **NOTE:** If a field is left blank, no filtering is done on that field. Packets are captured or mirrored without regard to the value contained in that field of their headers.

6. To save your settings and exit the configuration window, click **Save**.

Configuring Display Filter Settings

This section describes how to configure packet monitor display filter settings. The values that you provide here are compared to corresponding fields in the captured packets, and only those packets that match are displayed. These settings apply only to the display of captured packets on the management interface, and do not affect packet mirroring.

If a field is left blank, no filtering is done on that field. Packets are displayed without regard to the value contained in that field of their headers.

To configure Packet Monitor display filter settings:

1. Navigate to the **Monitor > Tools & Monitors > Packet Monitor** page.
2. Select the **General** tab.
3. Select the **Display Filter** tab.

4. In the **Interface Name(s)** box, type the SonicWall network security interfaces for which to display packets, or use the negative format (!X0) to display packets captured from all interfaces except those specified. You can specify up to ten interfaces separated by commas. Refer to the **Network > Interfaces** screen in the management interface for the available interface names.

5. In the **Ether Type(s)** box, enter the Ethernet types for which you want to display packets, or use the negative format (!ARP) to display packets of all Ethernet types except those specified. You can specify up to ten Ethernet types separated by commas. Currently, these Ethernet types are supported:

- ARP
- IP
- PPPoE-SES
- PPPoE-DIS

The latter two can be specified by PPPoE alone.

You can also use hexadecimal values to represent the Ethernet types, or mix hex values with the standard representations; for example: ARP, 0x800, IP. Normally, you would only use hex values for Ethernet types that are not supported by acronym in SonicOS. (Refer to [Supported Packet Types](#) for more information.)

6. In the **IP Type(s)** box, enter the IP packet types for which you want to display packets, or use the negative format (!UDP) to display packets of all IP types except those specified. You can specify up to ten IP types separated by commas. These IP types are supported:

- TCP
- UDP
- ICMP
- GRE
- IGMP
- AH
- ESP

You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: TCP, 0x1, 0x6. To display all IP types, leave blank. (Refer to [Supported Packet Types](#) for more information.)

7. In the **Source IP Address(es)** box, type the IP addresses from which you want to display packets, or use the negative format (!10.1.2.3) to display packets captured from all source addresses except those specified.
8. In the **Source Port(s)** box, type the port numbers from which you want to display packets, or use the negative format (!25) to display packets captured from all source ports except those specified.
9. In the **Destination IP Address(es)** box, type the IP addresses for which you want to display packets, or use the negative format (!10.1.2.3) to display packets with all destination addresses except those specified.
10. In the **Destination Port(s)** box, type the port numbers for which you want to display packets, or use the negative format (!80) to display packets with all destination ports except those specified.
11. Select **Enable Bidirectional Address and Port Matching** to match the values in the source and destination fields against either the source or destination information in each captured packet.
12. Select **Forwarded** to display captured packets that the SonicWall network security appliance forwarded, .
13. Select **Generated** to display captured packets that the SonicWall network security appliance generated.

14. Select **Consumed** to display captured packets that the SonicWall network security appliance consumed.
15. Select **Dropped** to display captured packets that the SonicWall network security appliance dropped, .
16. To save your settings and exit the configuration window, click **Save**.

Configuring Logging Settings

This section describes how to configure Packet Monitor logging settings. These settings provide a way to configure automatic logging of the capture buffer to an external FTP server. When the buffer fills up, the packets are transferred to the FTP server. The capture continues without interruption.

If you configure automatic FTP logging, this supersedes the setting for wrapping the buffer when full. With automatic FTP logging, the capture buffer is effectively wrapped when full, but you also retain all the data rather than overwriting it each time the buffer wraps.

To configure logging settings:

1. Navigate to the **Monitor > Tools & Monitors > Packet Monitor** page.
2. Select the **General** tab.
3. Select the **Logging** tab.

4. In the **FTP Server IP Address** box, type the IP address of the FTP server.
 - ① **NOTE:** Make sure that the FTP server IP address is reachable by the SonicWall network security appliance. An IP address that is reachable only through a VPN tunnel is not supported.
5. In the **Login ID** box, type the login name that the SonicWall network security appliance should use to connect to the FTP server.
6. In the **Password** box, type the password that the SonicWall network security appliance should use to connect to the FTP server.

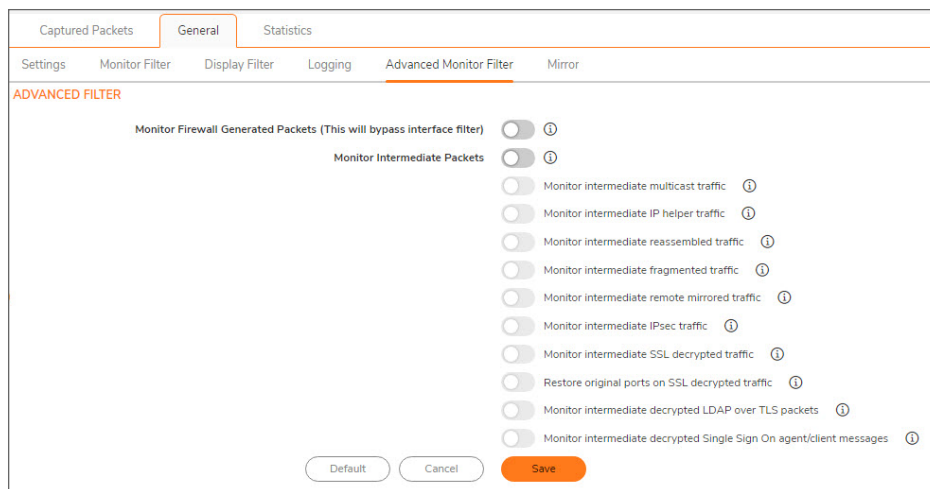
7. In the **Directory Path** box, type the directory location for the transferred files. The files are written to this location relative to the default FTP root directory.
For libcap format, files are named `packet-log--<>.cap`, where the `<>` contains a run number and date including hour, month, day, and year. For example, `packet-log--3-22-08292006.cap`.
8. For HTML format, file names are in the form `packet-log_h-<>.html`. For example, an HTML file name is: `packet-log_h-3-22-08292006.html`.
9. Select **Log To FTP Server Automatically** to enable automatic transfer of the capture file to the FTP server when the buffer is full. Files are transferred in both libcap and HTML format.
10. Select **Log HTML File Along With .cap File (FTP)** to enable transfer of the file in HTML format as well as libcap format.
11. Click **Log Now** to test the connection to the FTP server and transfer the capture buffer contents to it.
12. For example, `packet-log-F-3-22-08292006.cap` or `packet-log_h-F-3-22-08292006.html`.
13. To save your settings and exit the configuration window, click **Save**.

Configuring Advanced Monitor Filter Settings

This section describes how to configure monitoring for packets generated by the SonicWall network security appliance and for intermediate traffic.

To configure the Advanced Monitor Filter settings:

1. Navigate to **Tools & Monitors > Packet Monitor**.
2. Click the **General** tab.
3. Click the **Advanced Monitor Filter** tab.



4. To monitor packets generated by the SonicWall network security appliance, select **Monitor Firewall Generated Packets**.

5. Even when other monitor filters do not match, this option ensures that packets generated by the SonicWall network security appliance are captured. This includes packets generated by HTTP(S), L2TP, DHCP servers, PPP, PPPOE, and routing protocols. Captured packets are marked with 's' in the incoming interface area when they are from the system stack. Otherwise, the incoming interface is not specified.
 6. To monitor intermediate packets generated by the SonicWall network security appliance, select **Monitor Intermediate Packets**. Selecting this checkbox enables, but does not select, the subsequent checkboxes for monitoring specific types of intermediate traffic. Select the checkbox for any of the following options to monitor that type of intermediate traffic:
 - **Monitor intermediate multicast traffic** – Capture or mirror replicated multicast traffic.
 - **Monitor intermediate IP helper traffic** – Capture or mirror replicated IP Helper packets.
 - **Monitor intermediate reassembled traffic** – Capture or mirror reassembled IP packets.
 - **Monitor intermediate fragmented traffic** – Capture or mirror packets fragmented by the firewall.
 - **Monitor intermediate remote mirrored traffic** – Capture or mirror remote mirrored packets after de-encapsulation.
 - **Monitor intermediate IPsec traffic** – Capture or mirror IPSec packets after encryption and decryption.
 - **Monitor intermediate SSL decrypted traffic** – Capture or mirror decrypted SSL packets. Certain IP and TCP header fields might not be accurate in the monitored packets, including IP and TCP checksums and TCP port numbers (remapped to port 80). DPI-SSL must be enabled to decrypt the packets.
 7. **Restore original ports on SSL decrypted traffic** – Select to restore the original TCP ports from the encrypted connection in the SSL decrypted packets.
 - **Monitor intermediate decrypted LDAP over TLS packets** – Capture or mirror decrypted LDAPS packets. The packets are marked with "(ldp)" in the ingress/egress interface fields and has dummy Ethernet, IP, and TCP headers with some inaccurate fields. The LDAP server is set to 389. Passwords in captured LDAP bind requests are obfuscated.
 - **Monitor intermediate decrypted Single Sign On agent/client messages** – Capture or mirror decrypted messages to or from the SSO Agent. The packets are marked with "(sso)" in the ingress/egress interface fields and has dummy Ethernet, IP, and TCP headers with some inaccurate fields.
- ① | **NOTE:** Monitor filters are still applied to all selected intermediate traffic types.
8. To save your settings and exit the configuration window, click **Save**.

Configuring Mirror Settings

This section describes how to configure Packet Monitor mirror settings. Mirror settings provide a way to send packets to a different physical port of the same firewall or to send packets to, or receive them from, a remote SonicWall network security appliance.

To configure mirror settings:

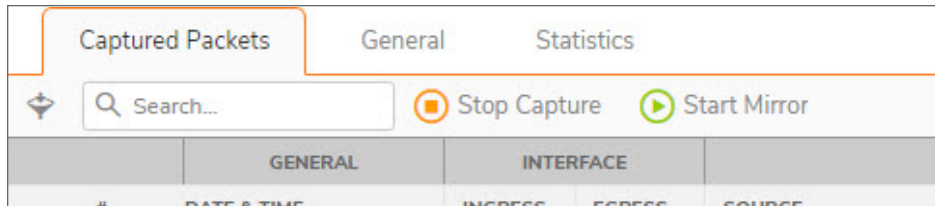
1. Navigate to the **Tools & Monitors > Packet Monitor** page.
2. Select the **General** tab.
3. Select the **Mirror** tab.
4. In the **Mirror Settings** section, type the desired maximum mirror rate into the Maximum mirror rate (in kilobits per second) field. If this rate is exceeded during mirroring, the excess packets are not mirrored and are counted as skipped packets. This rate applies to both local and remote mirroring. The default and minimum value is 100kbps, and the maximum is 1Gbps.
5. Select **Mirror only IP packets** to prevent mirroring of other Ether type packets, such as ARP or PPPoE. If selected, this option overrides any non-IP Ether types selected on the Monitor Filter view.
6. In the **Local Mirror Settings** section, select the destination interface for locally mirrored packets in the Mirror filtered packets to Interface (NSA platforms only) drop-down menu.
7. In the **Remote Mirror Settings (Sender)** section, in the **Mirror filtered packets to remote SonicWall firewall (IP Address)** field, type the IP address of the remote SonicWall to which mirrored packets are sent.
 - ① **NOTE:** The remote SonicWall network security appliance must be configured to receive the mirrored packets.
8. In the **Encrypt remote mirrored packets via IPSec (preshared key-IKE)** field, type the preshared key to be used to encrypt traffic when sending mirrored packets to the remote SonicWall network security appliance. Configuring this field enables an IPSec transport mode tunnel between this appliance and the remote SonicWall network security appliance. This pre-shared key is used by IKE to negotiate the IPSec keys.
9. In the **Remote Mirror Settings (Receiver)** section, in the **Receive mirrored packets from remote SonicWall firewall (IP Address)** field, type the IP address of the remote SonicWall network security appliance from which mirrored packets are received.
 - ① **NOTE:** The remote SonicWall network security appliance must be configured to send the mirrored packets.
10. In the **Decrypt remote mirrored packets via IPSec (preshared key-IKE)** field, type the pre-shared key to be used to decrypt traffic when receiving mirrored packets from the remote SonicWall network security appliance. Configuring this field enables an IPSec transport mode tunnel between this appliance and the remote SonicWall network security appliance. This pre-shared key is used by IKE to negotiate the IPSec keys.
11. Select the interface from the **Send received remote mirrored packets to Interface (NSA platforms only)** drop-down menu to mirror received packets to another interface on the local SonicWall network security appliance.
12. Select **Send received remote mirrored packets to capture buffer** to save received packets in the local capture buffer. This option is independent of sending received packets to another interface, and both can be enabled.
13. To save your settings and exit the configuration window, click **Save**.

Topics:

[Starting and Stopping Packet Mirror](#)

Starting and Stopping Packet Mirror

You can start a packet mirroring session that uses your configured mirror settings. On the **MONITOR | Tools & Monitors > Packet Monitor** page, click **Start Mirror**. It is not necessary to first configure specific criteria for display, logging, FTP export, and other settings. Packet mirroring stops when you click **Stop Capture**.



Monitoring Captured Packets

The **Captured Packets** page provides several buttons for general control of the packet monitor feature and display.

- **Monitor All** – Resets current monitor filter settings and advanced page settings so that traffic on all local interfaces is monitored. A confirmation dialog box displays when you click this button.
- **Monitor Default** – Resets current monitor filter settings and advanced page settings to factory default settings. A confirmation dialog box displays when you click this button.
- **Clear** – Clears the packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging. A confirmation dialog box displays when you click this button.

The other buttons and displays on this page are described in these sections:

- [Starting and Stopping Packet Capture](#)
- [Starting and Stopping Packet Mirror](#)

Starting and Stopping Packet Capture

You can start a packet capture that uses default settings without configuring specific criteria for packet capture, display, FTP export, and other settings. If you start a default packet capture, the SonicWall network security appliance captures all packets, except those for internal communication, and stops when the buffer is full or when you click **Stop Capture**.

To manage packet captures, navigate to **MONITOR | Tools & Monitor > Packet Monitor** and select the **Captured Packets** tab:

- To set the statistics back to zero, click **Clear**.
- To start the packet capture click **Start Capture**.
- To stop the packet capture, click **Stop Capture**.

Viewing Packet Monitoring Statistics

The **Statistics** page displays status indicators for packet capture (trace), mirroring, and FTP logging. Information pop-up tooltips display the configuration settings.

Topics:

- [Capture Statistics](#)
- [Local Mirror Statistics](#)
- [Remote Mirror TX Statistics](#)
- [Remote Mirror RX Statistics](#)
- [FTP Statistics](#)
- [Current Buffer Statistics](#)

Capture Statistics

Navigate to the **MONITOR | Tools & Monitor > Packet Monitor** page and select the **Statistics** tab.

The screenshot shows the 'Statistics' tab in the Packet Monitor interface. It is divided into several sections:

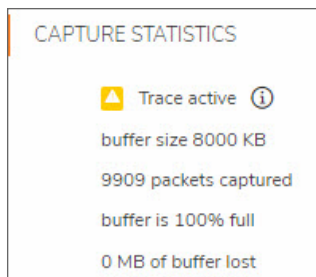
- CAPTURE STATISTICS:** Shows 'Trace active' with a yellow status icon. Details include 'buffer size 8000 KB', '9909 packets captured', 'buffer is 100% full', and '0 MB of buffer lost'.
- LOCAL MIRROR STATISTICS:** Shows 'Local mirroring off' with a red status icon. Details include 'mirroring to interface: NONE', '0 packets mirrored', '0 pkts skipped', and '0 pkts exceeded rate'.
- REMOTE MIRROR TX STATISTICS:** Shows 'Remote mirroring Tx off' with a red status icon. Details include 'mirroring to: 0.0.0.0', '0 packets mirrored', '0 pkts skipped', and '0 pkts exceeded rate'.
- REMOTE MIRROR RX STATISTICS:** Shows 'Remote mirroring Rx off' with a red status icon. Details include 'Receiving from: 0.0.0.0', '0 mirror packets rcvd', and '0 mirror packets rcvd but skipped'.
- FTP STATISTICS:** Shows 'FTP logging off' with a red status icon. Details include 'FTP server pass/failure count: 0/0', 'FTP Thread is idle', and 'Buffer is FULL'.
- CURRENT BUFFER STATISTICS:** Shows '2899 dropped', '151 forwarded', '3568 consumed', '3291 generated', and '0 unknown'.

At the bottom, there is a 'CURRENT CONFIGURATIONS' section with links for 'Filters', 'General', 'Logging', and 'Mirroring'.

In the **Capture Statistics** section, Trace shows one of the following three conditions:

- Red – Capture is stopped
- Green – Capture is running and the buffer is not full
- Yellow – Capture is on, but the buffer is full

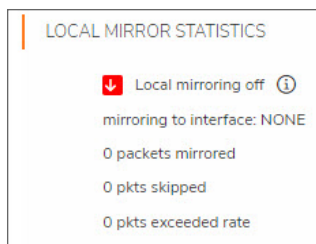
The **Capture Statistics** section also displays:



① **NOTE:** Although the buffer wrap option clears the buffer upon wrapping to the beginning, this is not considered lost data.

Local Mirror Statistics

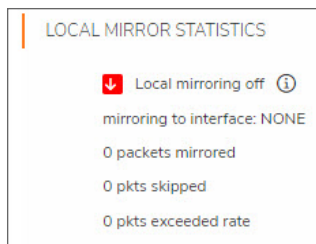
Navigate to the **MONITOR | Tools & Monitor > Packet Monitor** page and select the **Statistics** tab. The **Local Mirror Statistics** section displays this information about packets sent to another physical interface on the same SonicWall network security appliance:



- The status indicator shows one of the following three conditions:
 - Red – Mirroring is off
 - Green – Mirroring is on
 - Yellow – Mirroring is on but disabled because the local mirroring interface is not specified
- On/off indicator
- **Mirroring to interface** – The specified local mirroring interface
- **packets mirrored** – The total number of packets mirrored locally
- **pkts skipped** – The total number of packets that skipped mirroring because of packets that are incoming/outgoing on the interface on which monitoring is configured
- **pkts exceeded rate** – The total number of packets that skipped mirroring because of rate limiting

Remote Mirror TX Statistics

Navigate to the **MONITOR | Tools & Monitor > Packet Monitor** page and select the **Statistics** tab. The **Remote Mirror TX Statistics** status indicator shows the following:



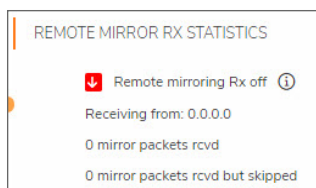
- Red – Mirroring is off
- Green – Mirroring is on and a remote SonicWall network security appliance IP address is configured
- Yellow – Mirroring is on but disabled because the remote device rejects mirrored packets and sends port unreachable ICMP messages

It also displays these statistics:

- On/off indicator
- **Mirroring to** – The specified remote SonicWall IP address
- **packets mirrored** – The total number of packets mirrored to a remote SonicWall network security appliance
- **pkts skipped** – The total number of packets that skipped mirroring because of packets that are incoming/outgoing on the interface on which monitoring is configured
- **pkts exceeded rate** – The total number of packets that failed to mirror to a remote SonicWall network security appliance, either because of an unreachable port or other network issues

Remote Mirror RX Statistics

Navigate to the **MONITOR | Tools & Monitor > Packet Monitor** page and select the **Statistics** tab. **Remote Mirror RX Statistics** track the packets received from a remote SonicWall network security appliance.



The status indicator shows one of these conditions:

- Red – Mirroring is off
- Green – Mirroring is on and a remote SonicWall IP address is configured

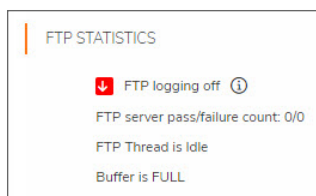
It also displays these statistics:

- On/off indicator
- **Receiving from** – The specified remote SonicWall IP address
- **mirror packets rcvd** – The total number of packets received from a remote SonicWall appliance

- **mirror packets rcvd but skipped** – The total number of packets received from a remote SonicWall appliance that failed to get mirrored locally because of errors in the packets

FTP Statistics

Navigate to the **MONITOR | Tools & Monitor > Packet Monitor** page and select the **Statistics** tab. FTP Statistics displays the following information:



- Red – Automatic FTP logging is off
- Green – Automatic FTP logging is on
- Yellow – The last attempt to contact the FTP server failed, and logging is now off

To restart automatic FTP logging, see [Restarting FTP Logging](#) on page 85.

It also displays these statistics:

- On/off indicator
- **FTP Server Pass/Failure count** – the number of successful and failed attempts to transfer the buffer contents to the FTP server
- **FTP Thread is Busy/Idle** – the current state of the FTP process thread
- **Buffer status** – the status of the capture buffer

If automatic FTP logging is off, either because of a failed connection or simply disabled, you can restart it in **Configure > Logging**.

To restart FTP logging:

1. Navigate to the **Tools & Monitors > Packet Monitor** page.
2. Select the **General** tab.
3. Select the **Logging** tab.
4. Verify that the settings are correct for each item on the page. (Refer to [Configuring Logging Settings](#) for more information.)
5. To change the FTP logging status page to active, select **Log To FTP Server Automatically**.
6. Optionally, test the connection by clicking **Log Now**.
7. To save your settings and exit the dialog, click **Save**.

Current Buffer Statistics

Navigate to the **MONITOR | Tools & Monitor > Packet Monitor** page and select the **Statistics** tab. The **Current Buffer Statistics** summarizes the number of each type of packet in the local capture buffer:

CURRENT BUFFER STATISTICS	
2899	dropped ⓘ
151	forwarded
3568	consumed
3291	generated
0	unknown

- **Dropped** – number of dropped packets
- **Forwarded** – number of dropped packets
- **Consumed** – number of dropped packets
- **Generated** – number of dropped packets
- **Unknown** - number of unidentified packets

Viewing Connections

Your SonicWall network security appliance maintains a connections log for tracking all active connections to the SonicWall network security appliance.

To view the Connections table:

1. Navigate to **MONITOR | Tools & Monitors > Connections**.
2. Click **IPv4** or **IPv6** to view the connections for that IP type.

The column names for the table are described in the following:

Src MAC	MAC address of the source device.
Src Vendor	Manufacturer of the source device.
Src IP	IP address of the source device.
Src Port	Port number of the source device.
Dst MAC	MAC address of the destination device.
Dst Vendor	Manufacturer of the destination device.
Dst IP	IP address of the destination device.
Dst Port	Port number of the destination device.
Protocol	Protocol used for the connection, such as TCP or ICMPv6.
Src Iface	Interface on the source device.
Dst Iface	Interface on the destination device.
Flow Type	Flow type of the connection, such as generic or HTTP Management.
IPS Category	Type of Intrusion Prevention System (IPS) used; N/A = Not Available.
Expiry (sec)	Number of seconds remaining before the connection expires.
Tx Bytes	Number of bytes transferred.
Rx Bytes	Number of bytes received.
Tx Pkts	Number of packets transferred.
Rx Pkts	Number of packets received.
Flush	Contains the Flush icon for each entry.

Topics:

- [Filtering the Connection Log](#)
- [Connections Log Functions](#)

Searching the Connections

Use **Filter** to find connections that meet specific search criteria.

1. Click the **Filter** icon.

2. Enable the filter options you want.
3. Click **Apply Filters**. You are asked to confirm your choice. Once the filter is applied, the table updates.

Filtering the Connection Log

Filter the **Connections** table so it displays only those connections matching the criteria specified in the **Filter** option.

Filter by

- Source IP
- Destination IP
- Destination Port
- Protocol
- Flow Type
- Source Interface
- Destination Interface

Filter Logic displays how the filter is applied.

The fields you enter values into are combined into a search string with a logical AND. For example, if you enter values for **Source IP** and **Destination IP**, the search string looks for connections matching:

```
Source IP AND Destination IP
```

Check the **Group** box next to any two or more criteria to combine them with a logical OR. For example, if you enter values for **Source IP**, **Destination IP**, and **Protocol**, and check **Group** next to **Source IP** and **Destination IP**, the search string looks for connections matching:

(Source IP OR Destination IP) AND Protocol

- Click **Apply Filters** to apply the filter immediately to the **Active Connections** table.
- Click **Reset Filters** to clear the filter and display the unfiltered results again.
- Click **Export**, and select if you want the results exported to a plain text file, or a Comma Separated Value (CSV) file for importing to a spreadsheet, reporting tool, or database. If you are prompted to Open or Save the file:
 1. Select **Save**.
 2. Enter a filename and path.
 3. Click **OK**.

Connections Log Functions

EVENT LOG FUNCTIONS

Function	Action
IPv4/IPv6	The Connection Log is configured the same for IPv6 and IPv4. To change the view, select the IP version from the drop-down menu. IPv4 is the default.
Refresh	Click to immediately refresh the Event Log.
Export to file	Exports the data to an external file. From the drop-down menu, select the file format: CSV, Text, or Email.
Clear	Deletes all logs displayed in the Event Log. You are asked to confirm your decision before the events are deleted.
Flush	Click this icon to flush that connection from the table. This option is found in the far right column of the table.

Monitoring Core 0 Processes

The **Core 0 Processes** page shows the individual system processes on core 0, their CPU utilization, and their system time.

#	NAME	PRIORITY	TOTAL %	TOTAL (SECS)	CURRENT %	CURRENT (SECS)
1	sonicosv	20	0.08	415.55	0.00	0.00
2	sonicosv	20	0.00	12.45	0.00	0.00
3	sonicosv	20	0.04	208.03	0.00	0.00
4	tGblcMon	20	0.02	80.35	0.00	0.00
5	tGblcPrese_ect	20	0.02	80.47	0.00	0.00
6	tpsuProbeTask	20	0.00	4.90	0.00	0.00
7	tASFlbWr	20	0.00	0.00	0.00	0.00
8	t3rdAppHandler	20	0.00	0.00	0.00	0.00
9	dhcpc6lnotify	20	0.00	0.10	0.00	0.00
10	tSarc	20	0.02	77.45	0.00	0.00
11	tWbDnsLkp	20	0.02	82.50	0.00	0.00
12	tSchedObjTimer	20	0.02	82.05	0.00	0.00
13	tNetMon	20	0.00	3.18	0.00	0.00
14	tNetMonXmit	20	0.02	78.20	0.00	0.00
15	tTimerTask	20	0.00	15.10	0.00	0.00
16	tMsTimerTask	20	0.03	174.23	0.00	0.00
17	tN5SecsTimerTask	20	0.00	4.35	0.00	0.00
18	v6Control	20	0.02	78.87	0.00	0.00
19	tHandleNetlink	20	0.00	0.06	0.00	0.00
20	tSpoolTask	20	0.02	81.60	0.00	0.00
21	tSpoolArpTask	20	0.02	76.72	0.00	0.00
22	cloudSyncTask	20	0.02	76.72	0.00	0.00
23	tsrGenTask	20	0.01	75.98	0.00	0.00
Task Total			2.53	12924.28	2.04	0.03
Idle			94.44	482575.66	94.90	1.55
System			3.04	15511.03	3.06	0.05

Using Packet Replay

Packet replay is an integrated tool to firewall for testing and debugging purposes. You can replay packets in these ways:

Craft a packet	Specify packet header fields and payload, one by one, through the management interface.
Use packet buffer	Input packet data (both header and payload) or just copy from other places and paste it.
Replay Pcap file	Replay a sequence of packets stored in a Pcap file.

Replayed packets are restrained from traveling outside this firewall; they are dropped before transmitting through interfaces.

Topics:

- [Single Packets](#)
- [Replay Pcap File](#)
- [Captured Packets](#)

Single Packets

These procedures describe how to craft a packet for analysis. Some fields may change when the **IP Type** is changed.

Topics:

- [Packet Crafting](#)
- [Packet Buffer](#)

Packet Crafting

The following procedure uses **IP Type = UDP**.

To craft a packet:

1. Navigate to **MONITOR > Tools & Monitor > Packet Replay**.
2. Click **Single Packet**.
3. Choose **Packet Crafting**.
4. Enter the following information; options change depending on your selection for **IP Type**:

IP TYPE = UDP

Field	Definition
Receiving Interface	Select the interface from which the packet is received.
Destination MAC	Enter the destination MAC address.
Source MAC	Enter the source MAC address.
Ether Type	Select the protocol type. The default is IPv4.
IP Type	Select UDP.
Source IP	Enter the source IP address.
Destination IP	Enter the destination IP address.
TTL	Enter the IP header.
Source Port	Enter the UDP source port number.
Destination Port	Enter the UDP destination port number.

5. If you select **IP Type = ICMP**, these fields are different from UDP:

IP TYPE = ICMP

Field	Definition
ICMP Type	Select Echo Request or Echo Response from the drop-down menu.
ID	Type in the ICMP identifier.
Sequence	Type in the ICMP sequence number.

6. If you select **IP Type = IGMP**, these fields are different from UDP:

IP TYPE = IGMP

Field	Definition
IGMP Type	Select IGMP Type from the drop-down menu. The default is Membership Query.
Max Response	Type in the IGMP maximum response timeout. Enter the value in seconds.
Group IP Address	Type in the group IP address for the query.

7. In the **Payload** field, enter or copy the payload hex data.
8. Click **Send**.

The crafted packet is sent to the firewall engine.

Packet Buffer

To build a packet buffer:

1. Navigate to **MONITOR > Tools & Monitor > Packet Replay**.
2. Click **Single Packet**.
3. Choose **Packet Buffer**.
4. From **Receiving Interface**, select the interface to receive the data.
5. Enter the **Packet Buffer** data, in hex.
6. Click **Send**.

The crafted packet is sent to the firewall engine.

Replay Pcap File

The Pcap filter can be defined by IP address or MAC address.

Topics:

- [Replaying an IP Pcap File](#)
- [Replaying a MAC Pcap File](#)

Replaying an IP Pcap File

To define by IP:

1. Navigate to **MONITOR > Tools & Monitor > Packet Replay**.
2. Click **Packets from File**.
3. Click **IP**. Two IP filters are provided.
4. For each IP filter, complete the following:

Field	Definition
IP Address	Enter the destination address to be looked up.
Receiving Interface	Select the receiving interface. The IP packets that have the destination address listed in IP Address are assumed to arrive from the interface selected in this option.
New IP Address	If enabled (the option is selected), the new IP address listed in this field replaces the filtered destination IP address when replaying the packets.

5. To search for and select a Pcap file to be replayed. click **Choose File**.
 - To upload the selected file, click **Upload**.
 - To replay the packets in the uploaded Pcap file, click **Replay**.
 - When done, to delete the uploaded file, click **Delete**.

Replaying a MAC Pcap File

To define by Mac address:

1. Navigate to **MONITOR > Tools & Monitor > Packet Replay**.
2. Click **Packets from File**.
3. Click **MAC**. Two IP filters are provided.
4. For each IP filter, complete the following:

Field	Definition
MAC Address	Enter the destination address to be looked up.
Receiving Interface	Select the receiving interface. The IP packets that have the destination address listed in MAC Address are assumed to arrive from the interface selected in this option.
New IP Address	If enabled (the option is selected), the new IP address listed in this field replaces the filtered destination IP address when replaying the packets.

5. To search for and select a Pcap file to be replayed. click **Choose File**.
 - To upload the selected file, click **Upload**.
 - To replay the packets in the uploaded Pcap file, click **Replay**.
 - When done, to delete the uploaded file, click **Delete**.

Captured Packets

Captured and replayed packets are displayed on the **Captured Packets** page. It provides three sections to display different views of captured packets:

- [About Captured Packets](#)
- [Packet Detail](#)
- [Hex Dump](#)

To view the list of captured packets:

1. Navigate to **MONITOR > Tools & Monitor > Packet Replay**.
2. Click **Captured Packets**.

Use these options to manage the Captured Packets:

Clear	Clears the packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging.
Export	Exports the file in the format you select from the drop-down menu. Saved files are placed on your local management system.
Reload	Refreshes the packet display windows on this page to show new buffer data.
Grid Settings	Allows you to customize which columns are displayed.

About Captured Packets

The **Captured Packets** page displays these statistics about each packet:

- **#** - The packet number relative to the start of the capture.
- **Date & Time** - The date and time that the packet was captured.
- **Ingress** - The firewall interface on which the packet arrived is marked with an asterisk (*). The subsystem type abbreviation is shown in parentheses. Subsystem type abbreviations are defined as:

Abbreviation	Definition
i	Interface
hc	Hardware-based encryption or decryption
sc	Software-based encryption or decryption
m	Multicast
r	Packet reassembly
s	System stack
ip	IP helper
f	Fragmentation

- **Egress** - The firewall interface on which the packet was captured when sent out. The subsystem type abbreviation is shown in parentheses.

Abbreviation	Definition
i	Interface
hc	Hardware-based encryption or decryption
sc	Software-based encryption or decryption
m	Multicast
r	Packet reassembly
s	System stack
ip	IP helper

Abbreviation	Definition
f	Fragmentation

- **Source IP** - The source IP address of the packet.
- **Destination IP** - The destination IP address of the packet.
- **Ether Type** - The Ethernet type of the packet from its Ethernet header.
- **Packet Type** - The type of the packet depending on the Ethernet type; for example:

Ethernet type	Packet type
IP packets	TCP, UDP, or another protocol that runs over IP
PPPoE packets	PPPoE Discovery or PPPoE Session
ARP packets	Request or Reply

- **Ports [Src, Dst]** - The source and destination TCP or UDP ports of the packet.
- **Length [Actual]** - Length value is the number of bytes captured in the buffer for this packet. Actual value, in brackets, is the number of bytes transmitted in the packet.
- **Status** - The status field for the packet.

The **Status** field shows the state of the packet with respect to the firewall. A packet can be dropped, generated, consumed, or forwarded by the firewall. Position the mouse pointer over dropped or consumed packets to show this information:

Packet Status	Displayed Value	Definition of Displayed Value
Dropped	Module-ID = <integer>	Value for the protocol subsystem ID
	Drop-code = <integer>	Reason for dropping the packet
	Reference-ID: <code>	SonicWall-specific data
Consumed	Module-ID = <integer>	Value for the protocol subsystem ID

Packet Detail

When you click a packet on the **Captured Packets** page, the packet header fields are displayed on the **Packet Detail** page. The display varies depending on the type of packet that you select.

Hex Dump

When you click a packet in the **Captured Packets** page, the packet data is displayed in hexadecimal and ASCII format on the **Hex Dump** page.

- The hex format is shown on the left side of the window, with the corresponding ASCII characters displayed to the right for each line.
- When the hex value is zero, the ASCII value is displayed as a dot.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The [Support Portal](#) provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The [Support Portal](#) enables you to:

- View [Knowledge Base articles](#) and [Technical Documentation](#)
- View and participate in the [Community Forum](#) discussions
- View [Video Tutorials](#)
- Access [MySonicWall](#)
- Learn about [SonicWall Professional Services](#)
- Review [SonicWall Support services and warranty information](#)
- Register at [SonicWall University](#) for training and certification

About This Document

SonicOS Monitor Administration Guide

Updated - November 2024

Software Version - 8

232-006178-00 Rev A

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035