



SonicOS 7.1

Monitor Appflow

Administration Guide

SONICWALL<sup>®</sup>

# Contents

<b>About SonicOS</b>	<b>4</b>
Working with SonicOS	4
SonicOS Workflow	6
How to Use the SonicOS Administration Guides	7
Guide Conventions	8
<b>AppFlow Report</b>	<b>9</b>
Applications	10
Users	11
IP Addresses	12
Viruses	12
Intrusions	13
Spyware	13
Locations	13
Botnets	14
Web Categories	14
<b>AppFlow Monitor</b>	<b>16</b>
Applications	17
Users	18
Web Activity	18
Initiator IPs	19
Responder IPs	19
Threats	20
VoIP	20
VPN	21
Devices	21
Contents	22
Policies	22
<b>AppFlow Sessions</b>	<b>23</b>
All	24
Threats	24
Web Access	24
<b>CTA Report</b>	<b>25</b>

Generate & Download CTA Report .....25

Advanced Options ..... 26

Completed Reports .....27

**SonicWall Support .....28**

About This Document ..... 29

# About SonicOS

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

## 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 threats to your network. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices like 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 two different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration and diagnostics.

- *Policy Mode* provides a unified policy configuration work flow. It combines Layer 3 to Layer 7 policy enforcement for security policies and optimizes the work flow for other policy types. This unified policy work flow gathers many security settings into one place, which were previously configured on different pages of the management interface.
- *Classic Mode* is more consistent with earlier releases of SonicOS; you need to develop individual policies and actions for specific security services. The Classic Mode has a redesigned interface.

This table identifies which modes can be used on the different SonicWall firewalls:

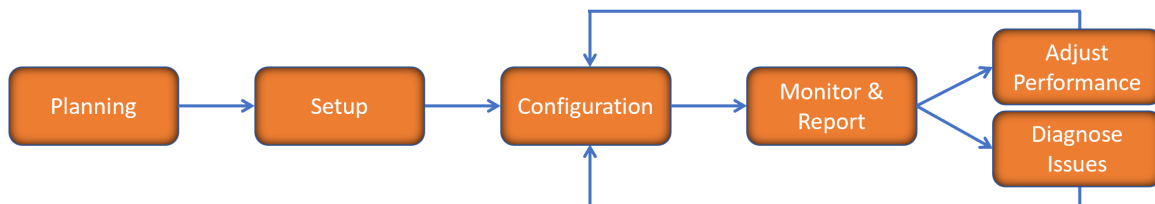
Firewall Type	Classic Mode	Policy Mode	Comments
TZ Series	yes	no	The entry level TZ Series, also known as desktop firewalls, deliver revamped features such as 5G readiness, better connectivity options, improved threat, SSL and decryption performance that address HTTPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support.
NSa Series	yes	no	NSa firewalls provide your mid sized network with enhanced security . They are designed specifically for businesses with 250 and up. it can provide cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, SD-WAN, real-time visualization, and WLAN management.
NSsp 10700, NSsp 11700, NSsp 13700	yes	no	The NSsp platforms high-end firewalls that deliver the advanced threat protection and fast speeds that large enterprises, data centers, and service providers need.
NSsp 15700	no	yes	The NSsp 15700 is designed for large distributed enterprises, data centers, government agencies and services providers. It provides advanced threat protection like Real-Time Deep Memory Inspection, multi-instance firewall configuration, and unified policy creation and modification, with scalability and availability.
NSv Series	yes	yes	The NSv series firewalls offers all the security advantages of a physical firewall with the operational and economic benefits of virtualization. The NSv firewalls can operate in either Policy Mode or Classic Mode. You can switch between modes, but some configuration information from extra interfaces is removed.

In addition to the management interface, SonicOS also has a full-featured API and a CLI to manage the firewalls. For more information, refer to:

- [SonicOS Command Line Interface Reference Guide](#)

# SonicOS Workflow

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

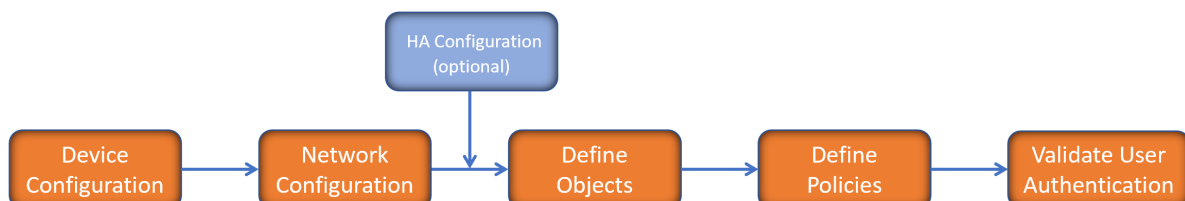


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing [product information](#) and [solutions](#).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

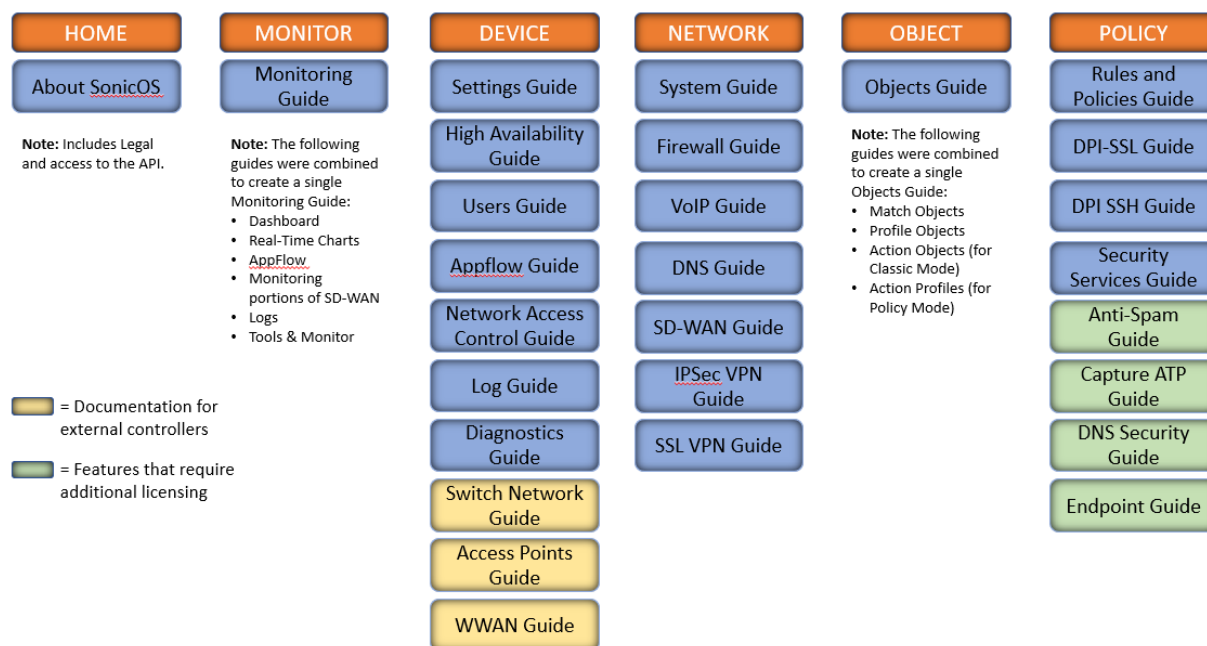


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement 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 7.1 Monitor Guide](#) and the [SonicOS 7.1 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 SonicWall management interface.



The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the <https://www.sonicwall.com/support/technical-documentation/>.

# 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
<b>Bold text</b>	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.
<b>Function   Menu group &gt; Menu item</b>	Indicates a multiple step menu choice on the user interface. For example, <b>NETWORK   System &gt; Interfaces</b> means to select the <b>NETWORK</b> functions at the top of the window, then click on <b>System</b> in the left navigation menu to open the menu group (if needed) and select <b>Interfaces</b> to display the page.
<b>Code</b>	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<b>&lt;Variable&gt;</b>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment <b>serialnumber=&lt;your serial number&gt;</b> , replace the variable and brackets with the serial number from your device, such as <b>serialnumber=2CB8ED000004</b> .
<b>Italics</b>	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.



# 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.

APPFLOW REPORT STATUS

Aggregate AppFlow Reporting ✓ Enabled  
 Apps Reporting ✓ Enabled  
 Using Storage ⚠ Disabled

NAME	LICENSED	STATUS	SIGNATURES	TO CONFIGURE...
Gateway Anti-Virus	Yes	Policy	Downloaded	Rules and Policies > Settings
Intrusion Prevention	Yes	Policy	Downloaded	Rules and Policies > Settings
Anti-Spyware	Yes	Policy	Downloaded	Rules and Policies > Settings
Content Filtering	Yes	Policy	N/A	Rules and Policies > Settings
Bandwidth Management	N/A	Advanced	N/A	Profile Objects -> Bandwidth
Country Database	Yes	N/A	Downloaded	N/A
Botnet Blocking	Yes	Policy	Downloaded	Rules and Policies > Settings

Note: To configure, go to AppFlow Settings > Flow Reporting. For storage setting, go to Device > Settings > Storage page, navigate to either System Logs or Threat Logs tab.

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

## Topics:

- [Top Applications](#)
- [Top Users](#)
- [Top IP Addresses](#)
- [Top Viruses](#)
- [Top Intrusions](#)
- [Top Spyware](#)
- [Top Locations](#)
- [Top Botnets](#)
- [Top 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
- **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
- **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 botnetThe 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
- **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
- **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
- **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
- **Percentage of Spyware** — The frequency of this spyware as a percentage of the total number of spyware

## Locations

Applications Users IP Addresses Virus Intrusions Spyware Locations Botnets Web Categories									
✚ Q Search...		IPv4 & IPv6		View: Since Restart		✓ + ≡ ⌂ ↻ ⌂ ⚙			
#	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
- **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

Applications Users IP Addresses Virus Intrusions Spyware Locations Botnets Web Categories			
<div> <div> <div>+</div> <div>Search...</div> </div> <div> <div>IPv4 &amp; IPv6</div> <div>▼</div> </div> <div> <div>View: Since Restart</div> <div>▼</div> </div> </div> <div> <div>✓</div> <div>+</div> <div>≡</div> <div>🔍</div> <div>🔄</div> <div>📄</div> <div>⚙️</div> </div>			
#	RATING NAME	COUNT	SESSIONS 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
- **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:

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

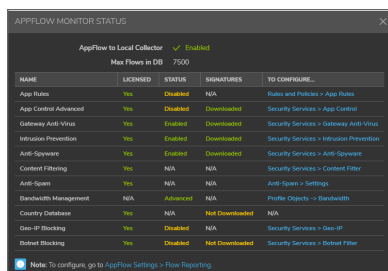
To enable and configure the reports, follow the procedures described in **Managing Flow Reporting Statistics** in the **SonicOS Logs** documentation. The green check mark icon at the top of the **MONITOR | AppFlow > AppFlow Monitor** page displays a link to the **DEVICE | AppFlow Settings > Flow Reporting**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

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

The screenshot shows the top navigation bar of the AppFlow Monitor page. It includes a '+ Create' button, a '+ Add to Filter' button, a search bar with 'Search...' text, a dropdown menu for 'IPv4 & IPv6', a radio button for 'All Flows', a dropdown for 'Group By: Application', a green checkmark icon, an 'Export' button, a 'Refresh' button, and a 'Column Selection' button.



- **+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									
<div> <div> <div>+</div> <div>Q Search...</div> </div> <div> <div>IPv4 &amp; IPv6</div> <div>60 Secs</div> </div> <div> <div>Group By: Application</div> <div>+</div> <div>✓</div> <div>+</div> <div>+</div> <div>+</div> <div>+</div> <div>+</div> <div>+</div> <div>+</div> </div> </div>									
#	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

Applications

Users

Web Activity

Initiator IPs

Responder IPs

Threats

VoIP

VPN

Devices

Contents

Policies

+

Q Search...

IPv4 & IPv6

60 Secs

Group By: User Name

#	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

Applications Users Web Activity Initiator IPs Responder IPs Threats VoIP VPN Devices Contents Policies									
+ - Search...		IPv4 & IPv6	60 Secs	Group By: IP Address + [check] + [copy] [refresh] [gear]					
#	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

Applications Users Web Activity Initiator IPs Responder IPs Threats VoIP VPN Devices Contents Policies									
+ - Search...		IPv4 & IPv6	60 Secs	Group By: IP Address + [check] + [copy] [refresh] [gear]					
#	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.

# AppFlow Sessions

① | **NOTE:** Appflow Session are a feature of SonicOS running Policy Mode. It is not available in Classic Mode.

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

- All
- Threats
- Web Access

The **MONITOR | AppFlow > AppFlow Sessions** page enables you to monitor the status of 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 viruses, intrusions, and spyware have threatened my network?
- 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 top of the page displays the following settings and information:

The screenshot shows the top navigation bar of the AppFlow Sessions page. It includes a search bar on the left, a filter slider set to 'Last 60 secs', a dropdown menu for 'Limit: 100 Entries', a green checkmark icon, and buttons for 'Export', 'Refresh', and 'Grid Settings'.

- **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
- **Limit** – Limits results by filtering flows based on the number of entries
- **Check mark** – The green check mark icon at the top of the **MONITOR | AppFlow > AppFlow Sessions** page displays a popup showing the Appflow Monitor Status for Policy Mode. Links are provided to connect you to additional data and procedures.

APPFLOW MONITOR STATUS				
AppFlow to Local Collector		⚠ Disabled		
Max Flows in DB		25000		
NAME	LICENSED	STATUS	SIGNATURES	TO CONFIGURE...
Gateway Anti-Virus	Yes	Policy	Downloaded	<a href="#">Rules and Policies &gt; Settings</a>
Intrusion Prevention	Yes	Policy	Downloaded	<a href="#">Rules and Policies &gt; Settings</a>
Anti-Spyware	Yes	Policy	Downloaded	<a href="#">Rules and Policies &gt; Settings</a>
Content Filtering	Yes	Policy	N/A	<a href="#">Rules and Policies &gt; Settings</a>
Bandwidth Management	N/A	Advanced	N/A	<a href="#">Profile Objects -&gt; Bandwidth</a>
Country Database	Yes	N/A	Downloaded	N/A
Botnet Blocking	Yes	Policy	Downloaded	<a href="#">Rules and Policies &gt; Settings</a>
 Note: To configure, go to <a href="#">AppFlow Settings &gt; Flow Reporting</a> .				

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

## All

Choose the **All** tab to see all the AppFlow sessions. Application entries can be displayed as either limited or unlimited. Column **Grid Settings** can be added or removed, or expanded and rearranged. Click **Grid Settings**, and use the arrows next to the column **Name** to expand column options. A checkbox next to a name adds the selection to the grid.

## Threats

Select the **Threats** tab to show the monitoring status of AppFlow sessions that contain threats. Entries can be displayed as either limited or unlimited. Column **Grid Settings** can be added or removed or expanded and rearranged. Click **Grid Settings**, and use the arrows next to the column **Name** to expand column options. A checkbox next to a name adds the selection to the grid.

## Web Access

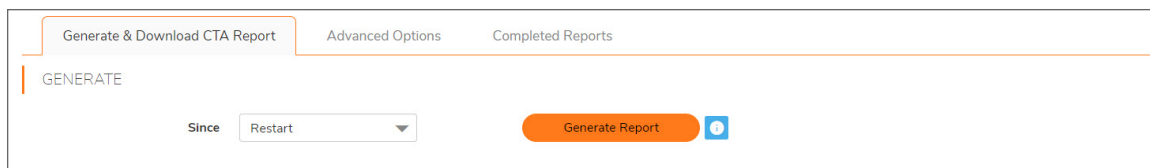
Select the **Web Access** tab to monitor status of AppFlow sessions that have **Web Access**. Application entries can be displayed as either limited or unlimited. Column **Grid Settings** can be added or removed, or expanded and rearranged. Click **Grid Settings**, and use the arrows next to the column **Name** to expand column options. A checkbox next to a name adds the selection to the grid.



# 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



Generate & Download CTA Report   Advanced Options   Completed Reports

GENERATE

Since

### *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.

Generate & Download CTA Report   Advanced Options   Completed Reports

GENERATE

Since: Restart   Generate Report

REPORT

Report  
10/6/2020, 9:37:39 PM

Filename: cta-report-2CB8ED694664-20201006.pdf  
Date: 10/6/2020, 9:37:39 PM  
Comment: Generated by firewall

Download Latest Report

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...			Refresh
#	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.

# 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. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

# About This Document

SonicOS Monitor Appflow Administration Guide

Updated - December 2023

Software Version - 7.1

232-006094-00 Rev A

Copyright © 2023 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