SonicOS 7.0

Monitor AppFlow

Administration Guide

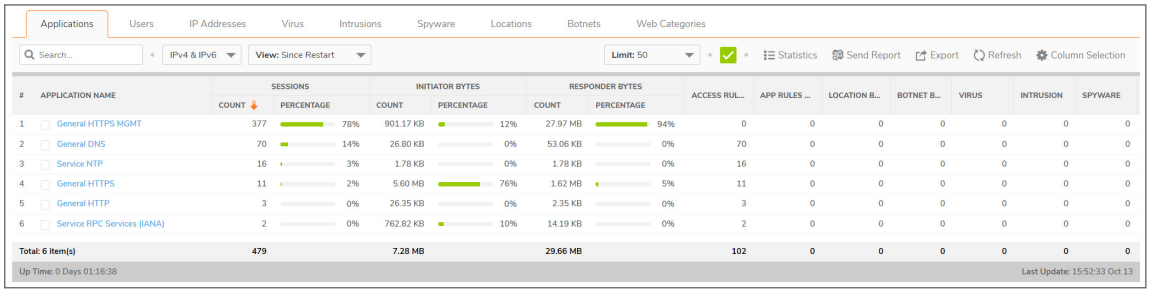
SONICWALL®

Contents

1

AppFlow Report

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



NOTE: The **MONITOR | AppFlow > AppFlow Report** page is supported on SonicWall TZ, NSv, and NSsp series appliances.

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/X 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:

- **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. This can be configured by clicking **Configure**.

Choose one of:

- **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 link to **DEVICE | AppFlow Settings > Flow Reporting**.
- **Refresh** – Click to refresh the report data.

Topics:

Top Applications

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

These selections are defined as:

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

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

Top 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 botnet

Top IP Addresses

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:

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

Top Viruses

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

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

Top Intrusions

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

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

Top Spyware

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

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

Top Locations

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:

- **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

Top Botnet

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

The report provides the following information:

- **Botnet Name** — Name of the Botnet
- **Count** — Sessions/Connections detected as botnet

Top Web Categories

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

The report provides the following information:

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

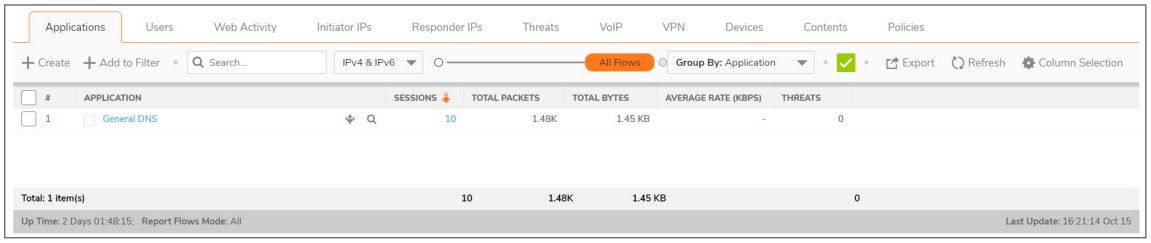
The report provides the following information:

- **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

2

AppFlow Monitor

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



NOTE: The **MONITOR | AppFlow > AppFlow Monitor** page is supported on SonicWall TZ, NSv, and NSsp series appliances.

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/X 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 to expose monitor status and a link to **DEVICE | AppFlow Settings > Flow Reporting**.
- **Refresh** – Click to refresh the report data.

Topics:

Top Applications

Allows flow filtering 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/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.

Top Users

Allows flow filtering by **Users**. Users can be grouped by **User Name**, **IP Address**, **Domain Name**, or **Auth type**.

These selections are defined as:

- **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.

Top Web Activities

Allows flow filtering 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/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.

Top Initiator IPs

Allows flow filtering 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.

Top Responder IPs

Allows flow filtering 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/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.

Top Threats

Allows flow filtering 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/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.

Top VoIP

Allows flow filtering by **VoIP**. VoIP can be grouped as **Media Type** or **Caller ID**.

These selections are defined as:

- **VoIP** — Name of the VoIP
- **Add entry to filter** — Icon appears allowing you to add specific VoIP data 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.

Top VPN

Allows flow filtering 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
- **Add entry to filter** — Icon appears allowing you to add specific VPN data 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.

Top Devices

Allows flow filtering 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
- **Add entry to filter** — Icon appears allowing you to add specific device data 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.

Top Contents

Allows flow filtering by **Contents**. Content can be grouped by **File Type** or **Email Address**.

These selections are defined as:

- **Content** — Name of the content
- **Add entry to filter** — Icon appears allowing you to add specific content data 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.

Top Policies

Allows flow filtering by Security **Policies**. Security Policies can be grouped by **Access Rule**, **NAT Rule**, **Initiator Route Policy**, or **Responder Route Policy**.

These selections are defined as:

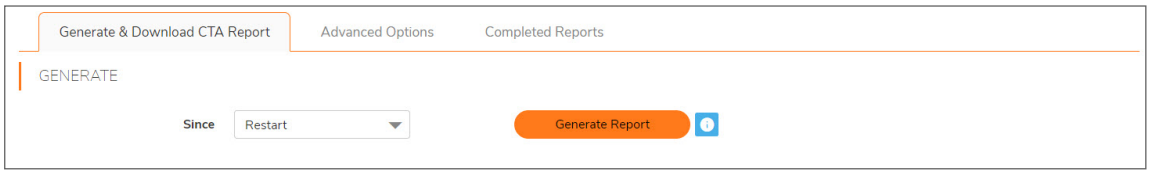
- **Policies** — Name of the security policy to be monitored
- **Add entry to filter** — Icon appears allowing you to add specific policy data into your filtering
- **Sessions** — Number of connections/flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator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

3

CTA Report

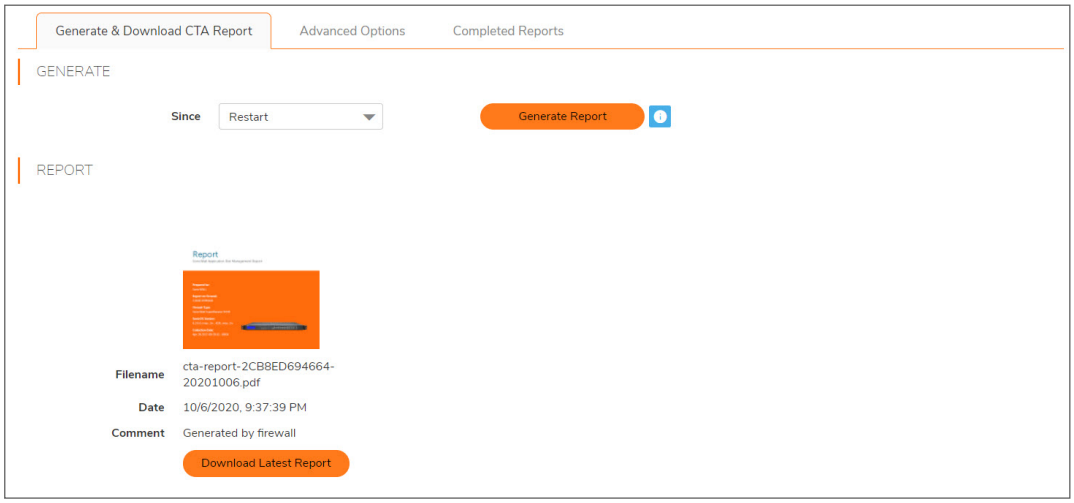
Use Capture Threat Assessment (CTA) Report to generate a SonicFlow Report (SFR) that you can download and post to the Capture Threat Assessment service.

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.



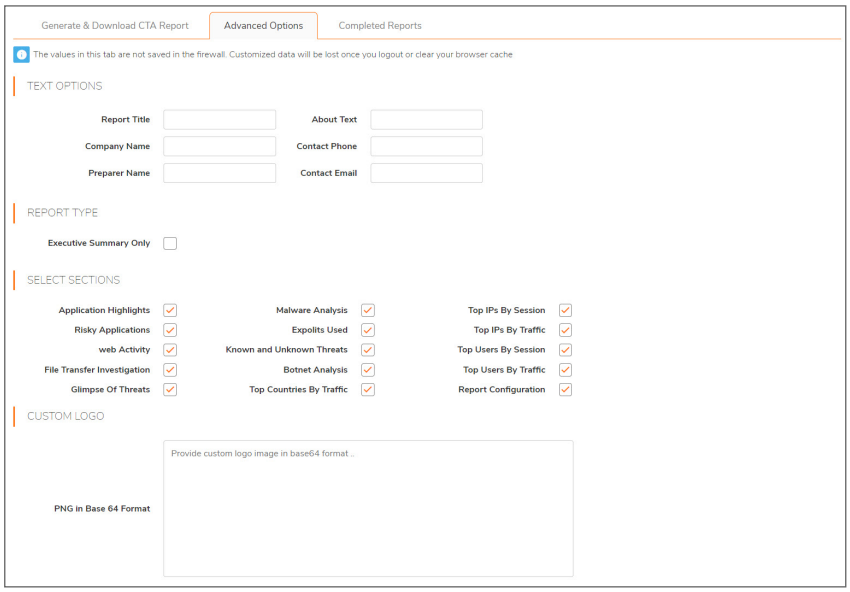
4. Click **Download Report** to download the report.

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.

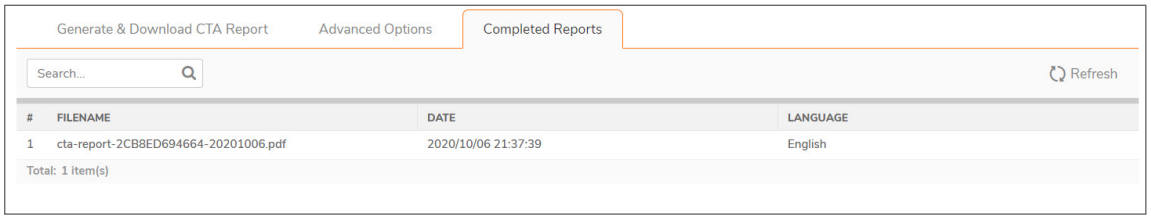
To configure Advanced CTA Report options:

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



3. Customize data for your CTA Reports using Text 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**. Customized Report data appears in the PDFs available in the **Completed Reports** tab.

Completed Reports



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

4

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

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information.

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.

SonicOS Monitor AppFlow Administration Guide
Updated - January 2021
Software Version - 7.0
232-005326-10 Rev B

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