SonicOS 7

Dashboard

Administration Guide

SONICWALL®

Contents

1

Dashboard

The **Dashboard** includes monitoring views for your System, Access Points, Capture ATP, WWAN, and Topology.

- In System, the **Summary** tab provides a synopsis of the **Network**, **Threats**, and **Device** details. The **Summary** modules provide data reports for each of the parameters featured.
- The **Access Points** option provides an Access Point Snapshot of all connected access points online and offline, the clients associated with them, the bandwidth consumption, a client report, and a real-time client monitor.
- **Capture ATP** provides a cloud-based network sandbox that analyzes suspicious code.

  WWAN represents your view into the 3G/4G/LTE devices connected to your environment.

  Topology provides network mapping and connected devices to give you an overview of associated systems.

2

System

The **HOME | Dashboard > System | Device** view is the default view you see when you log in to SonicOS for the first time. This is where you can get a quick overview of status and reports setup on the **Network** and **Threat** views for the devices contained within your infrastructure. Think of the **HOME** view as the starting point for most tasks, which include:

Topics:

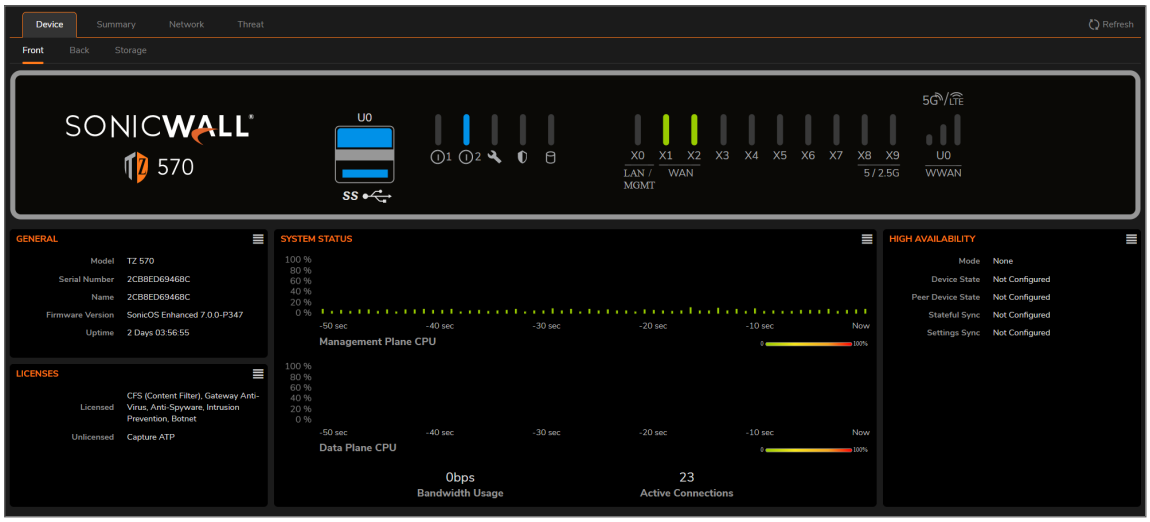
- Summary
- Network
- Threat
- Device

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

NOTE: The information available in the **Overview** section vary according to the type of view you selected in the other views.

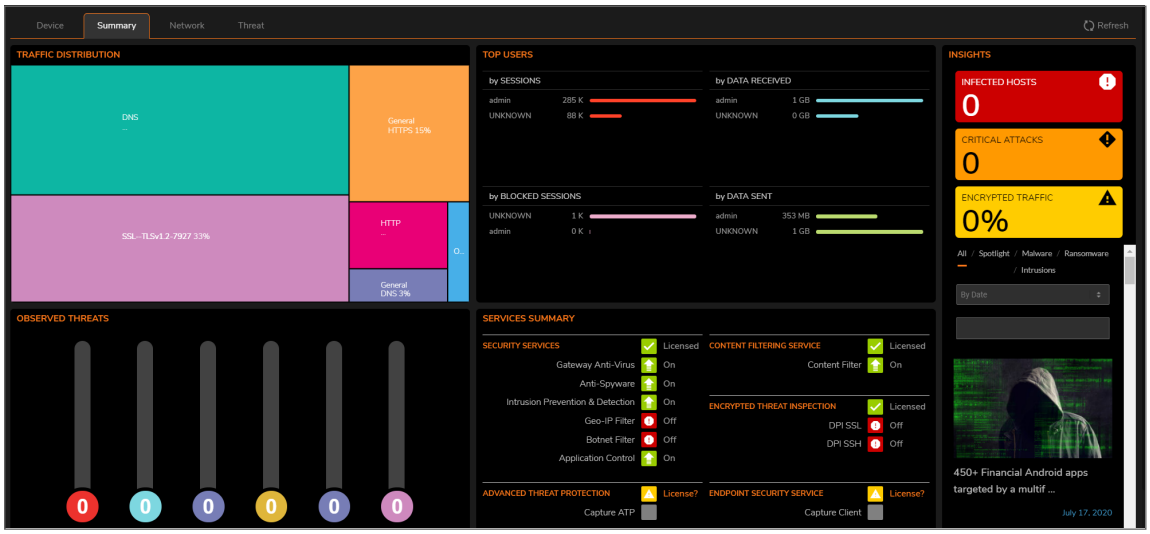
Device

The **HOME | Dashboard > System | Device** view displays the relevant information for the unit connected to your system. Window summaries showing the general details about the device are shown as a group of tables. In those views, you can also review licenses, high availability data, system status, and so on, as well as the Front, Back, and Storage views of your device.



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 System Summary and see at-a-glance when any issues might need investigating.



The **System 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.

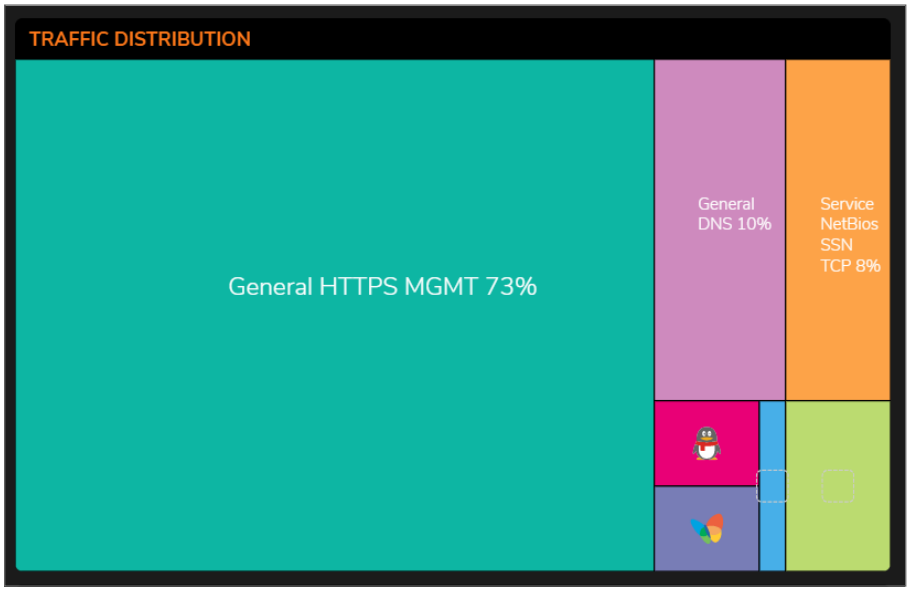
The following table describes the components that make up the **System Summary**.

SUMMARY OVERVIEW

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.
Observed Threats	Tracks the number of system connections reporting triggered threats.
Services Summary	Provides a bird's eye view of all active and inactive, licensed and not licensed services available (or not) within your network.

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.

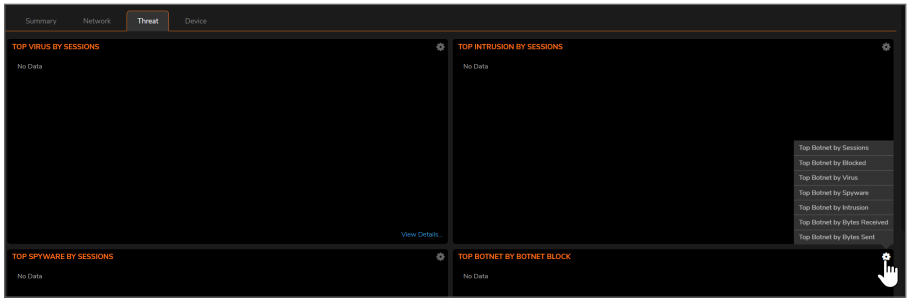
You can drill-down for more information on the TRAFFIC MAP segment as well. Use the mouse wheel to Zoom in and out on the global mag or use the vertical + and - slider on the left side of the map. Click the flags and icons on the map to drill-down for additional details.

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.

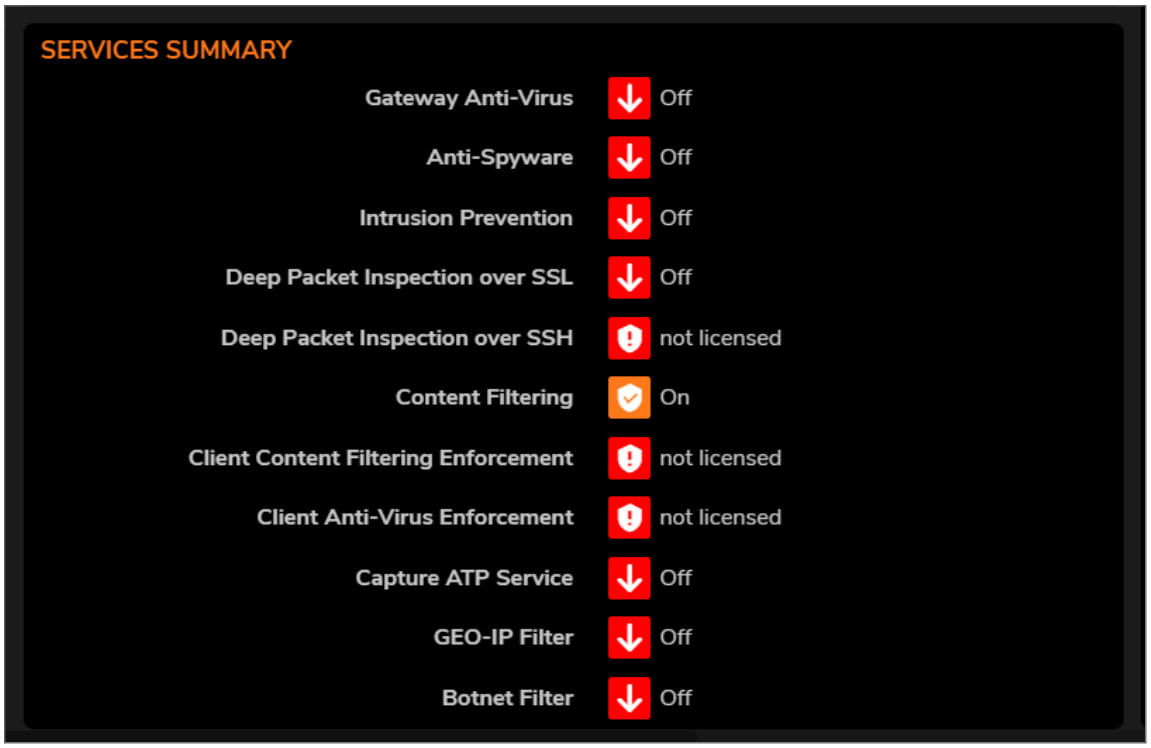
Observed Threats

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 **Options** icon in each window to expand the available filtering options.



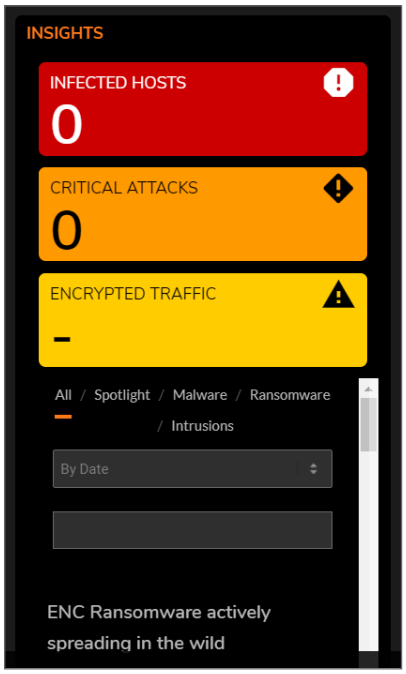
Services Summary

The **Services Summary** window provides a bird's eye view of all active and inactive, licensed and not licensed services available (or not) within your network.



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.



Network

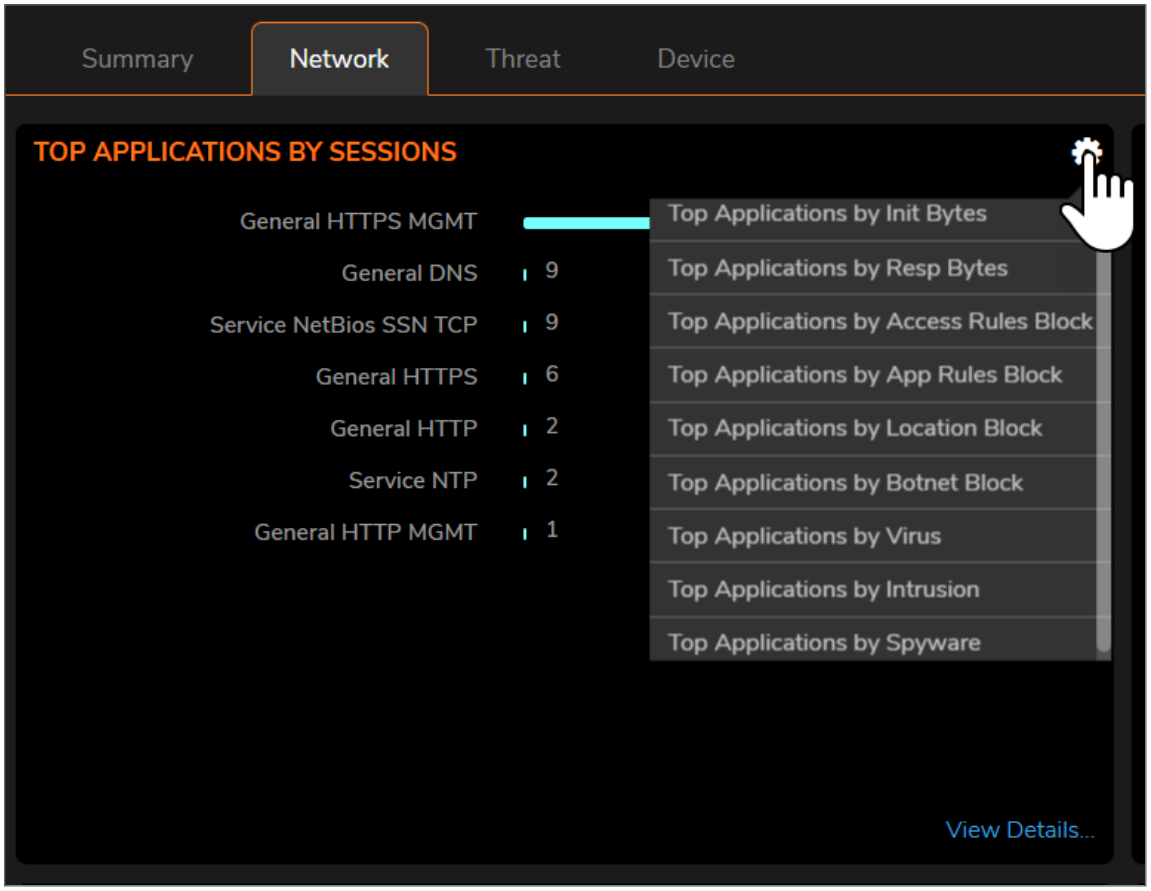
The **Network** view provides session reporting windows that display the top Applications, Addresses, Users, Website Ratings, Countries, and so on.

Topics:

- Top Applications
- Top Addresses
- Top Users
- Top Website Ratings
- Top Countries

Top Applications

The **Top Applications** window indicates all applications flowing through the firewall by bits per second.



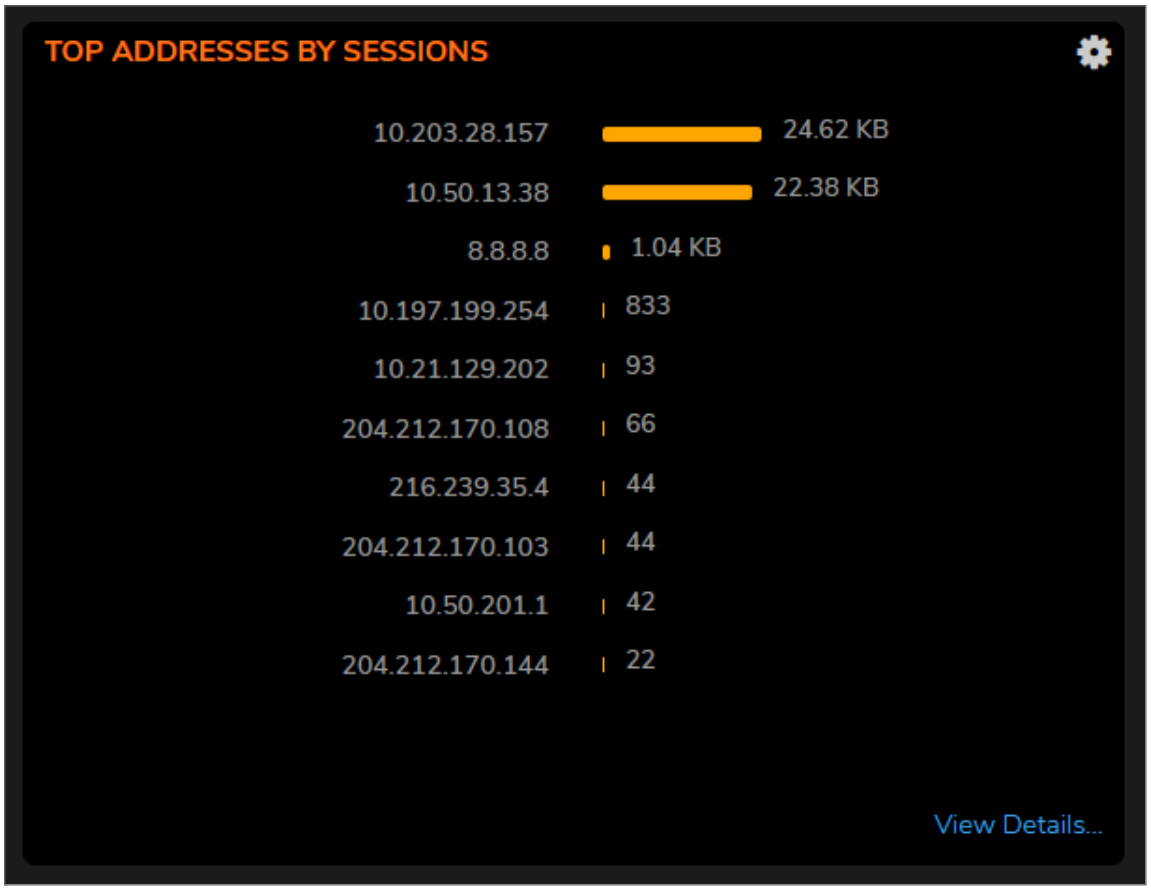
You can also track other user-level transactions and activities by filtering on several different options including **Top Users by**:

- Init Bytes
- Resp Bytes
- Access Rules Block
- App Rules Block
- Location
- Botnet Block
- Virus
- Intrusion
- Spyware

Click **View Details** to see complete reporting on all application filtering located in **MONITOR | AppFlow > AppFlow Report | Applications**.

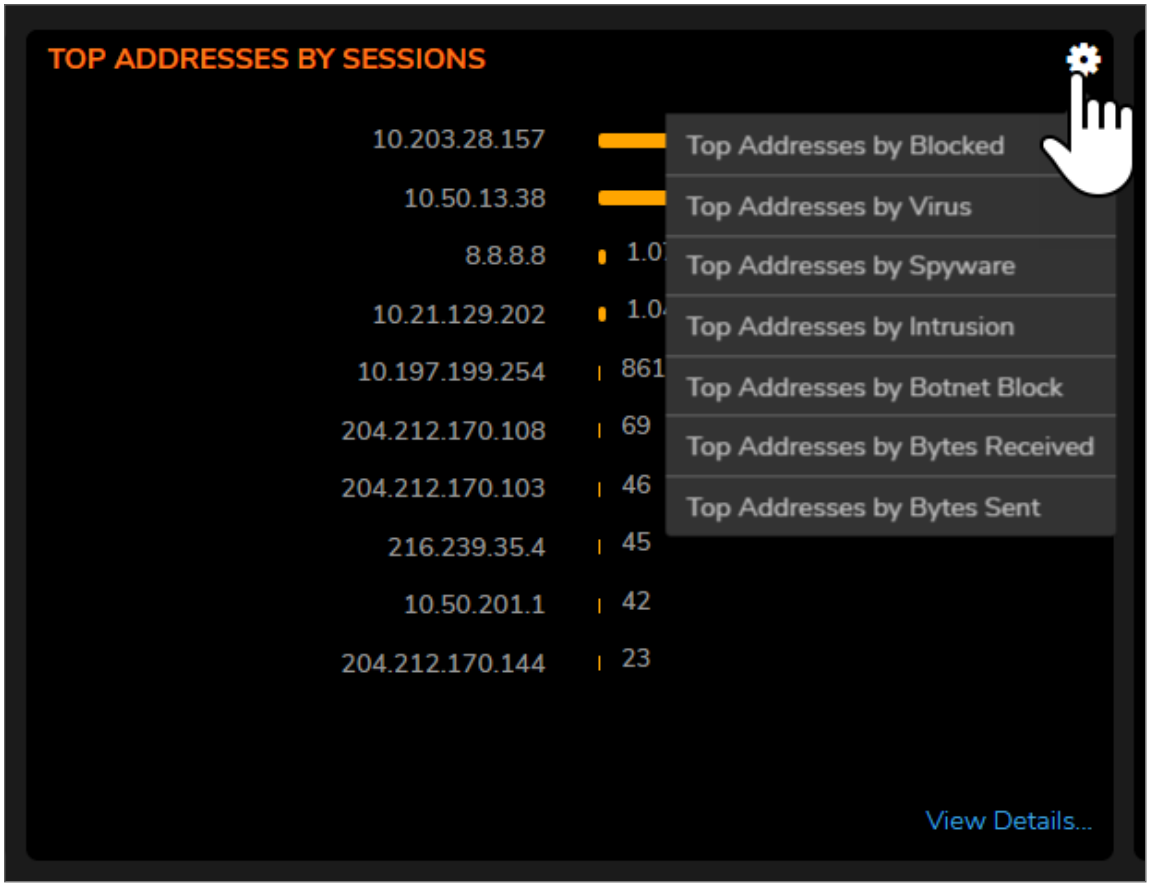
Top Addresses

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



You can track IP address-level transactions and activities by filtering on several different options including **Top Addresses by**:

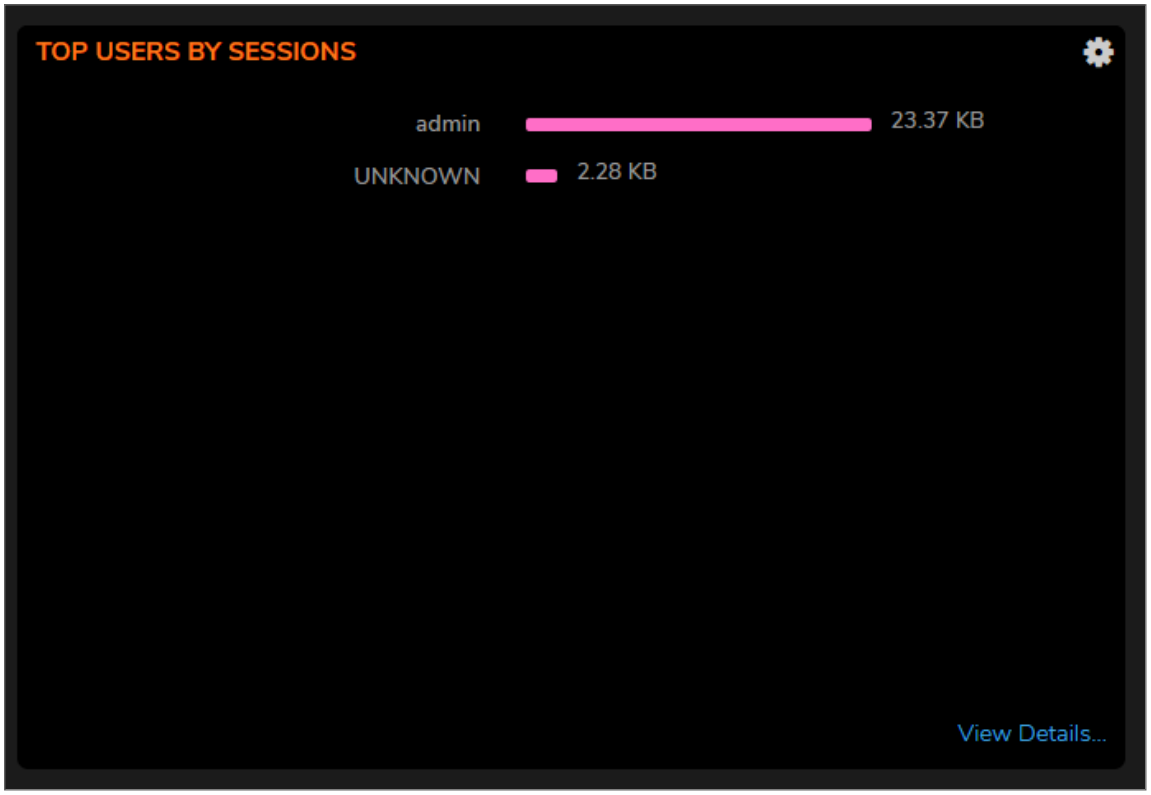
- Blocked
- Virus
- Spyware
- Intrusion
- Botnet Block
- Bytes Received
- Bytes Sent



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

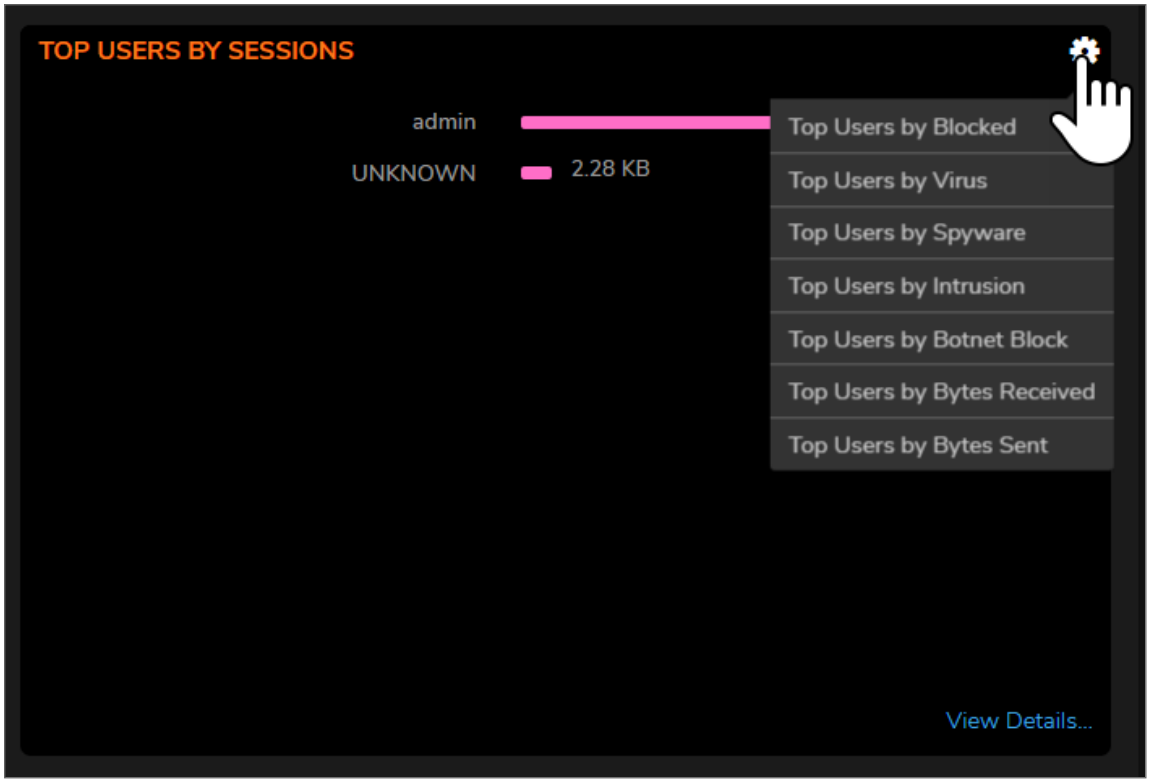
Top Users

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



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

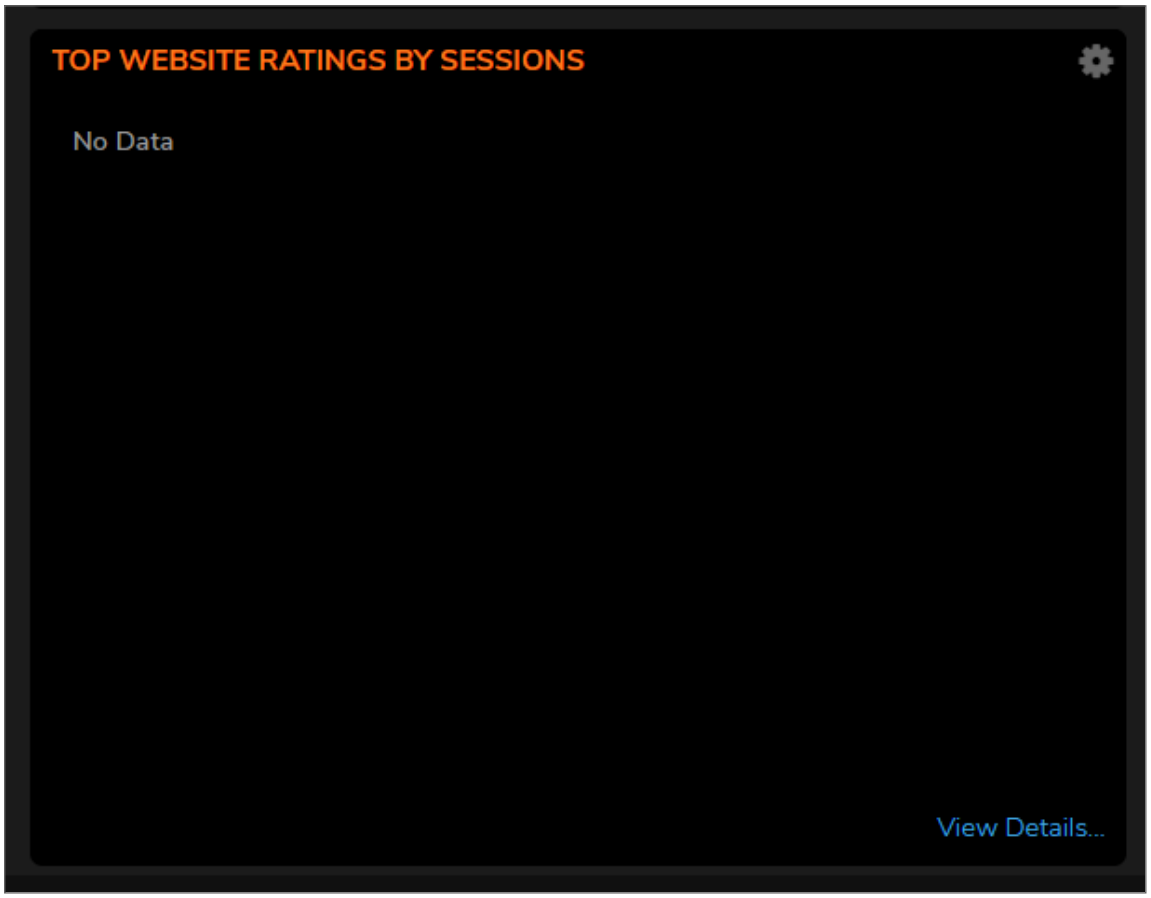
- Blocked
- Virus
- Spyware
- Intrusion
- Botnet Block
- Bytes Received
- Bytes Sent



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

Top Website Ratings

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



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

- Count
- Percentage

Click **View Details** to see complete reporting on all Website Ratings located in **MONITOR | AppFlow > AppFlow Report | URL Ratings**.

Top Countries

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

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**.

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 Virus
- Top Intrusion
- Top Spyware
- Top Botnet

Top Virus

The **Top Virus by Sessions** report provides data as it relates to viral threats processed through the system. You can track virus-level transactions and activities by filtering on several different options including **Top Virus by**:

- Count
- Percentage

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

Top Intrusion

The **Top Intrusion by Sessions** report provides data as it relates to intrusions processed through the system.

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

- Count
- Percentage

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

Top Spyware

The **Top Spyware by Sessions** report provides data as it relates to spyware threats processed through the system.

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

- Count
- Percentage

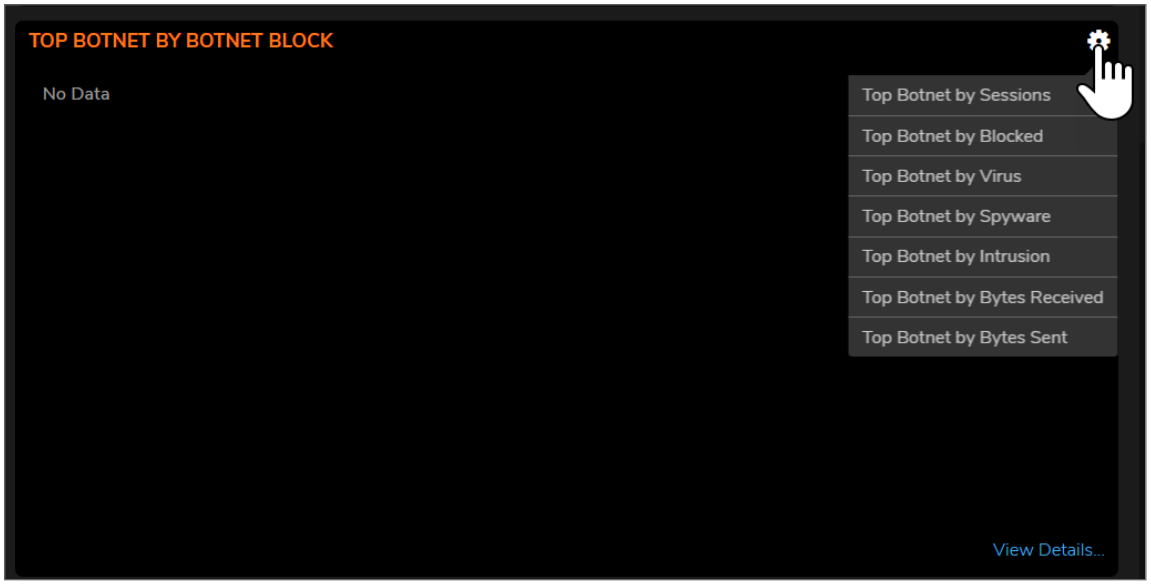
Click **View Details** to see complete reporting on all viruses located in **MONITOR | AppFlow > AppFlow Report | Spyware**.

Top Botnet

The **Top Botnet by Botnet Block** report provides data as it relates to botnet threats connected to the system.

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



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

Packet Filtering

Packet Filtering is a firewall technique used to control network access to your system. You can monitor incoming and outgoing packets and allow them to pass or halt based on their sources and destination Internet Protocol (IP) addresses, protocols and ports. Packet filtering can be enforced through any of the following filters:

Access Rules Block

The **Access Rules Block** reports track the number of blocked connections made with Access Rules in place.

Application Rules Block

The App Rules Block report tracks the number of Application Rules blocked connections. You can select options from the drop-down menu.

Blocked

This report tracks the number of blocked connections.

Botnet

This report tracks the Botnet addresses that are detected within your system.

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.

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.

Initiator Bytes

The **Init Bytes** report displays the number of connections based on location of the source. You can by the connection types listed in the drop-down menu. Additional source IP reports can be selected from the drop-down menu by the title.

Intrusions

The Intrusions summaries include two type of reports (represented by the different tabs): Number of sessions/connections/initiated/responded to intrusions and the statistical percentages.

Locations

This report displays the number of connections based on country of the destination. Additional destination IP reports can be selected from the drop-down menus by the title.

Responder Bytes

The **Resp Bytes** report displays the number of connections based on the IP address of the source. You can filter the source types, listed in the drop-down menu. Additional destination IP reports can be selected from the drop-down menu by title.

Spyware

This report tracks the spyware that has been detected in your system. You can filter on which connections it occurred or on which spyware (name) was blocked.

Viruses

This report tracks all viruses that have been detected within your system. You can filter based on the connections they occurred on or by which viruses were blocked. Details are provided in the table.

3

Access Points

For SonicWave and SonicPoint AC devices, **HOME | Dashboard > Access Points** uses charts and graphs to help visualize the data related to the access points that are connected to your infrastructure. 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 and SonicPoint devices and provides information to help with monitoring problematic diagnosis.

Topics:

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

Two graphs are shown in the **Access Point Snapshot** section of the **HOME | Dashboard > Access Points| Access Point Online/Offline and Client Association**. 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.

Access Point Online/Offline

The **Access Point Online/Offline** graph shows a quick status of the access points in the infrastructure. The data is presented as a doughnut chart; online is green and offline is red. To the right of the chart, the number of access points and the status is also listed.

The Online status includes operational, disabled, rebooting, and in IDS scanning mode.

Offline status includes unresponsive and initializing states.

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**.

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**.

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

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**.

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.

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.

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).

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.

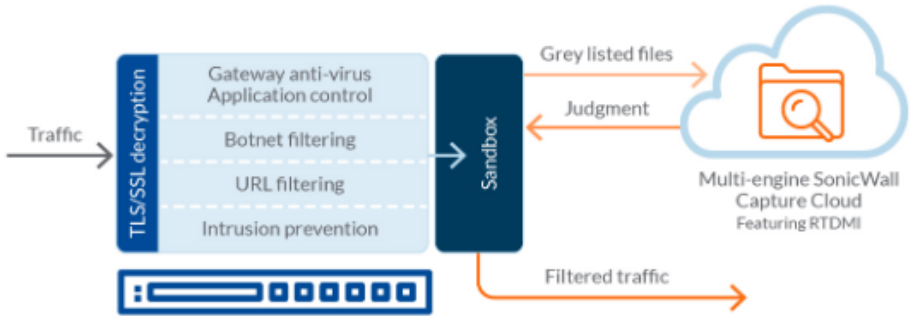
NOTE: Only SonicPoint ACe/ACi/N2 and SonicWave devices support client detail filtering.

4

Capture ATP

The **SonicWall Capture Advanced Threat Protection (ATP)** section of the **HOME** 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.



Capture ATP Dashboard

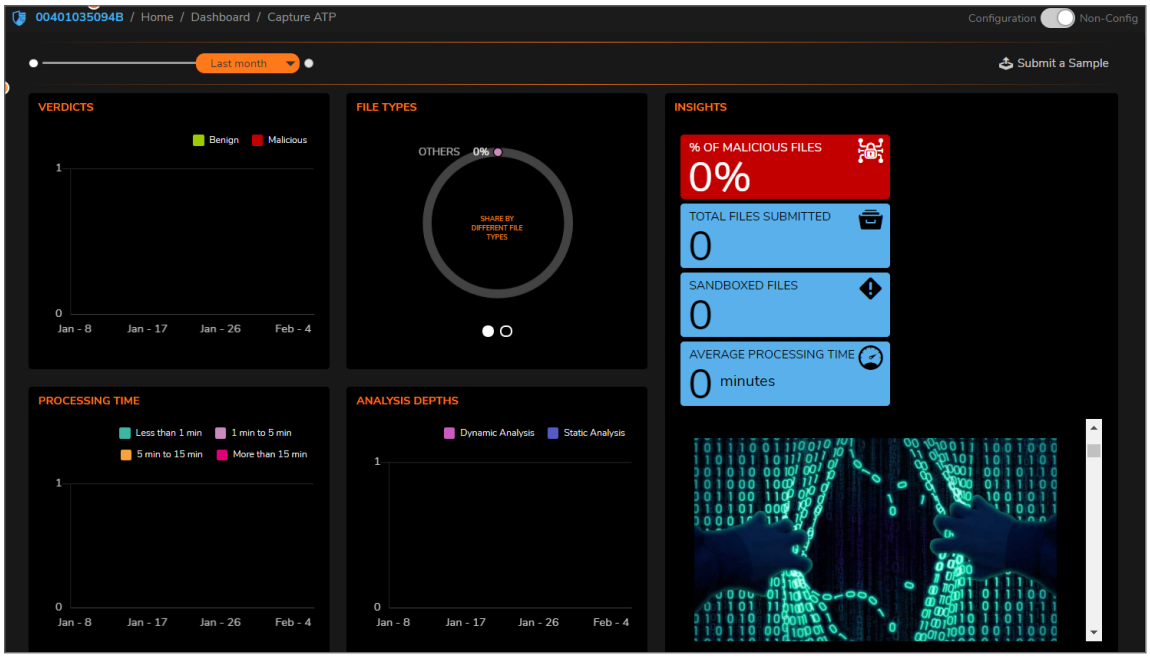
The **Capture ATP Dashboard** (**HOME | Dashboard > Capture ATP**) allows you see in one place which files are being sent to the backend for scanning and which ones are being blocked. The blue boxes show the total files scanned and the red box shows the total malicious files found. Files can be scanned for the last month, week, or 24 hour period.

The Capture ATP Dashboard also informs you about the date of the work being done by the firewall and how many files have been scanned. Colored bars give you the percentage and number of days malicious files have been found.

Other reports are available in this section, and you can create customized report windows with the **Custom** drop-down menu. You can also add filters to the files being scanned in the **Column Selection** drop-down menu, and see the files listed by their Disposition, File Name, File Hash, Type, Submitter, and the Date and Time. Capture ATP can also be configured at **POLICY | Capture ATP > Settings**.

For more information, refer to the *SonicWall Management Services Capture ATP Administration Guide*.

Capture ATP is an add-on security service to the firewall, similar to Gateway Anti-Virus (GAV) that helps your system identify malicious files. To enable the service you need a license, GAV, and Cloud Anti-Virus Database services.



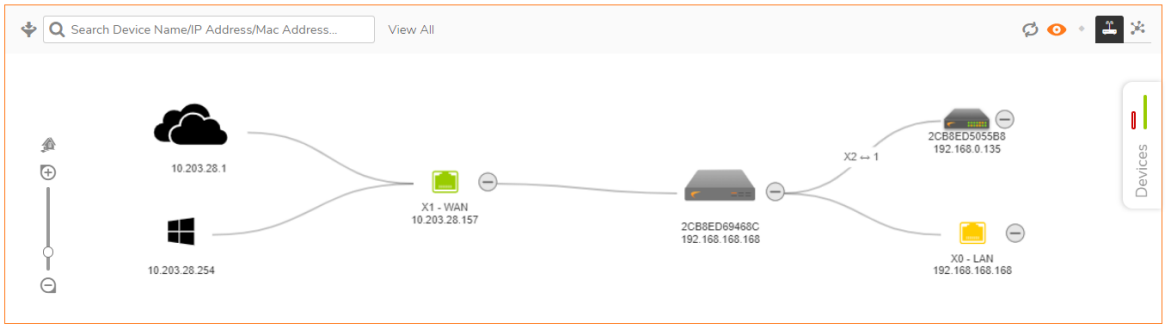
5

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, like 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.

ⓘ | **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.

6

Legal Information

Legal Information for SonicOS is stated at **HOME | Legal Information**.

The terms and conditions applicable to your download and use of this product are located at https://www.sonicwall.com/legal/#tab-id-3 (“Agreement”). Please read this Agreement carefully as it contains provisions such as how you may use the product and associated restrictions, warranties and warranty disclaimers, limitation on damages and remedies that may be claimed, audit rights. BY DOWNLOADING, INSTALLING OR USING THIS PRODUCT, YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL, ACCESS OR USE THE PRODUCT BECAUSE YOU DO NOT HAVE A LICENSE TO THE PRODUCT.

7

API

The SonicWall API use agreement can be reviewed at **HOME | API**.

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING SonicOS API. BY DOWNLOADING, INSTALLING OR USING THIS API, YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. PLEASE GO TO HTTPS://SONICOS-API.SONICWALL.COM TO VIEW THE APPLICABLE VERSION OF API FOR YOUR PRODUCT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL OR USE THIS API.

8

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 Dashboard Administration Guide
Updated - February 2021
Software Version - 7
232-005330-10 Rev C

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