SonicOSX 7 Dashboard

Administration Guide

SONICWALL®

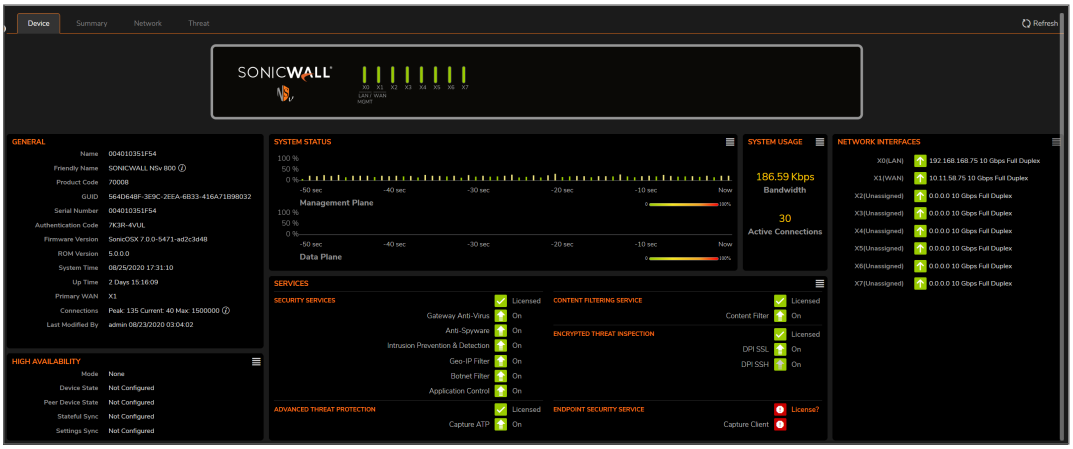
Contents

1

System

The **HOME | Dashboard > System** view is the default view you see when you log in to SonicOSX 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 system infrastructure. Think of the **System** view as the starting point for most tasks, which include:

- The Dashboard **System**, which provides a **Summary** synopsis of the **Device, Network**, and **Threat** details.
- The **Summary** modules provide data reports for each of the parameters featured.
- **Capture ATP** provides a cloud-based network sandbox that analyzes suspicious code.
- The **Policy Overview** provides a one-stop overview of all policy activity.



Topics:

- Device
- Summary
- Network
- Threat

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

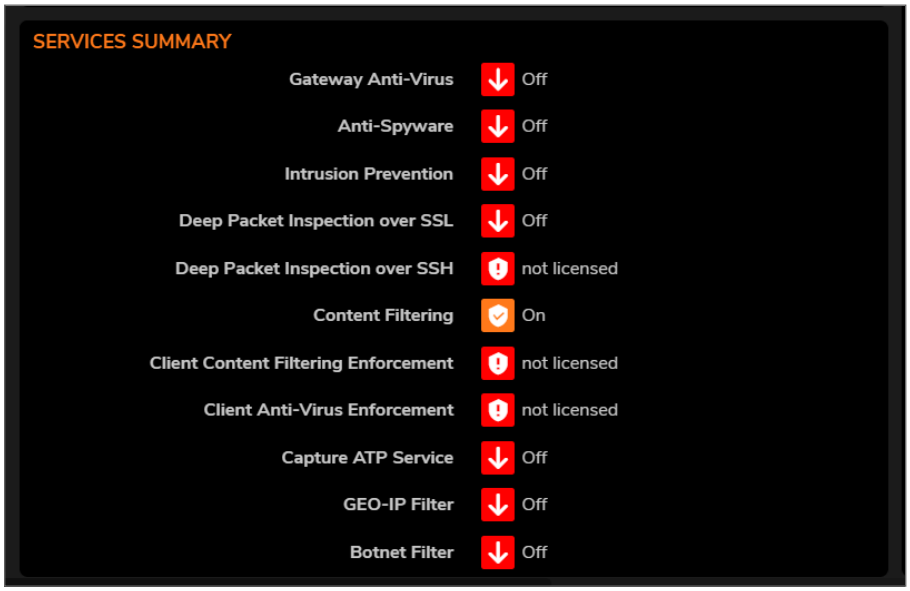
NOTE: The information available in the **System** section could vary according to the type of view you selected in the other views.

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.

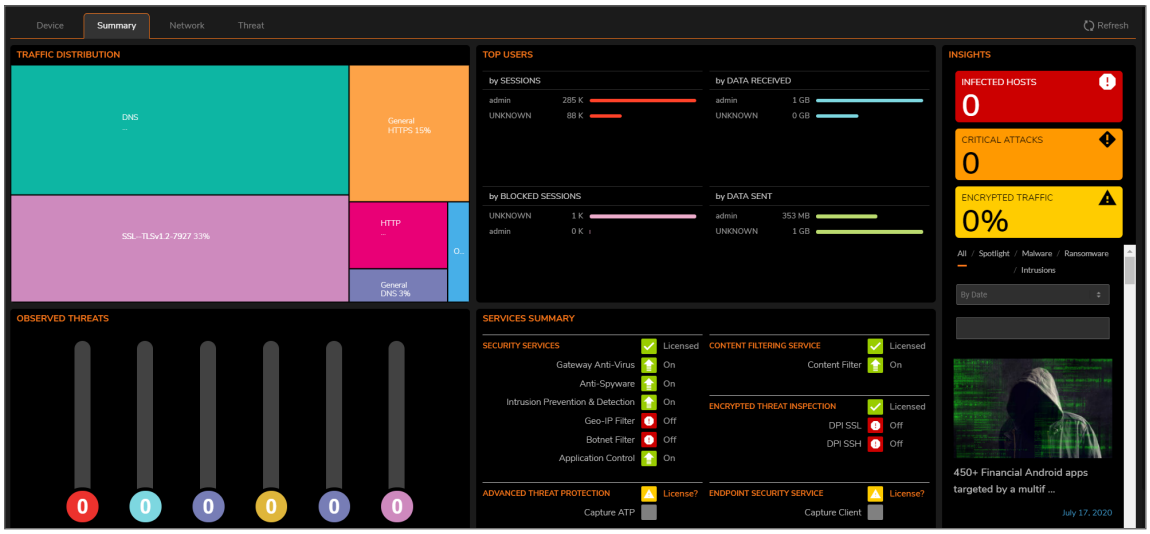
Services

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



Summary

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



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

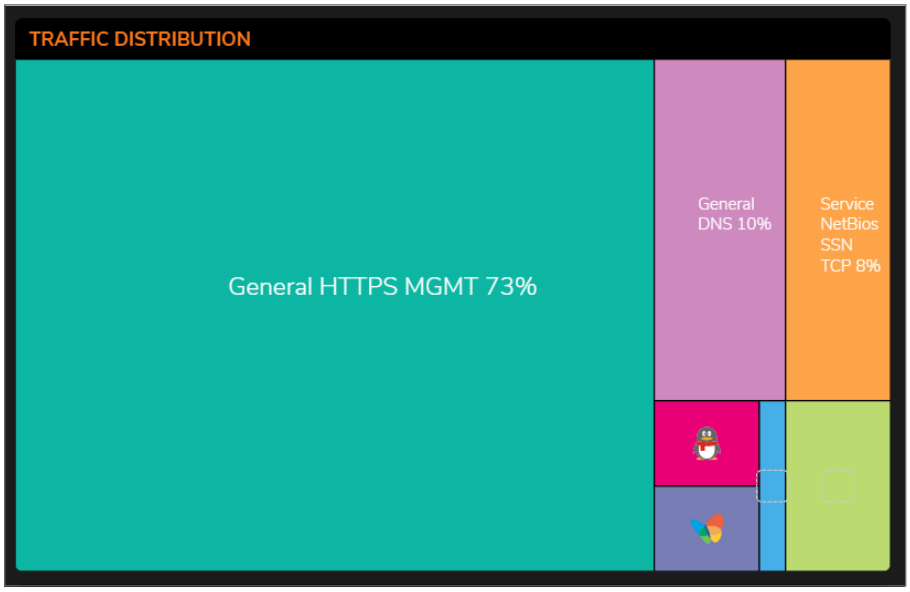
The following table describes the components that make up the **System Summary**.

SYSTEM SUMMARY

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

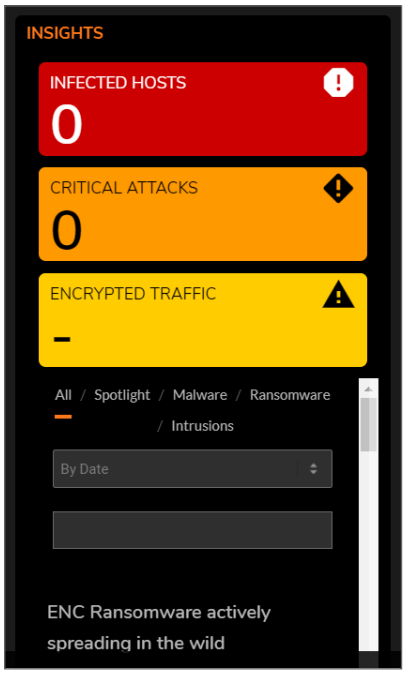
You can drill-down for more information on the TRAFFIC MAP segment as well. Use the mouse wheel to Zoom in and out on the global mag or use the vertical + and - slider on the left side of the map. Click the flags and icons on the map to drill-down for additional details.

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.

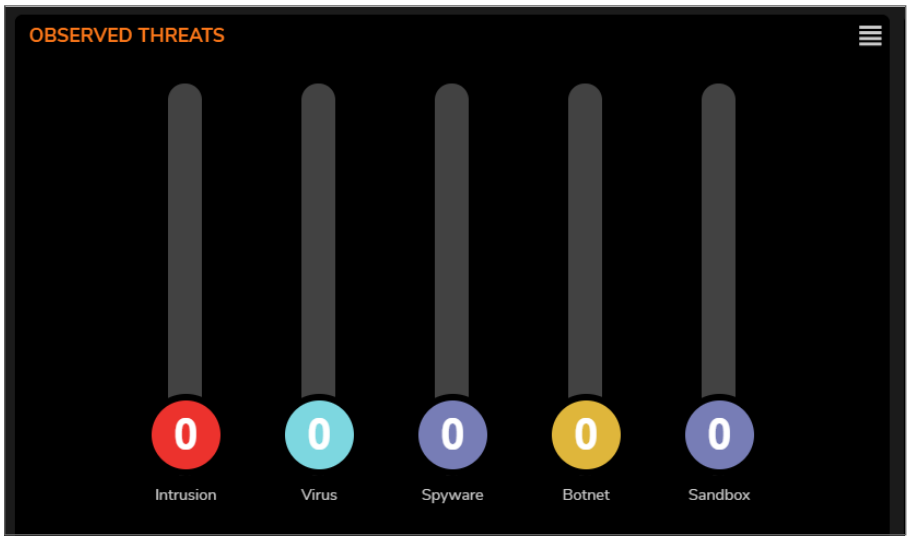
Insights

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



Observed Threats

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



Top Countries

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

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**.

Network

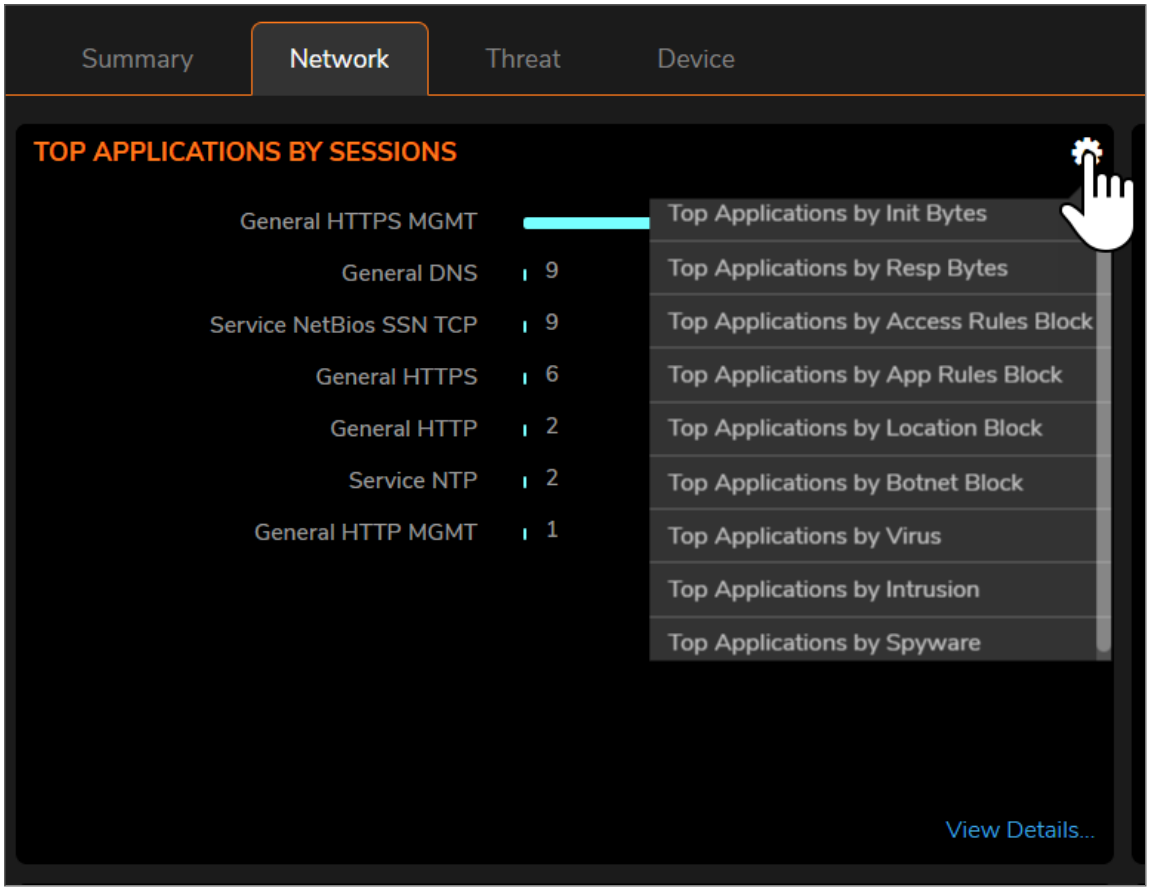
The **Network** view provides session reporting windows that display the top Applications, Addresses, Users, Website Ratings, Countries, and so on.

Topics:

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

Top Applications

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



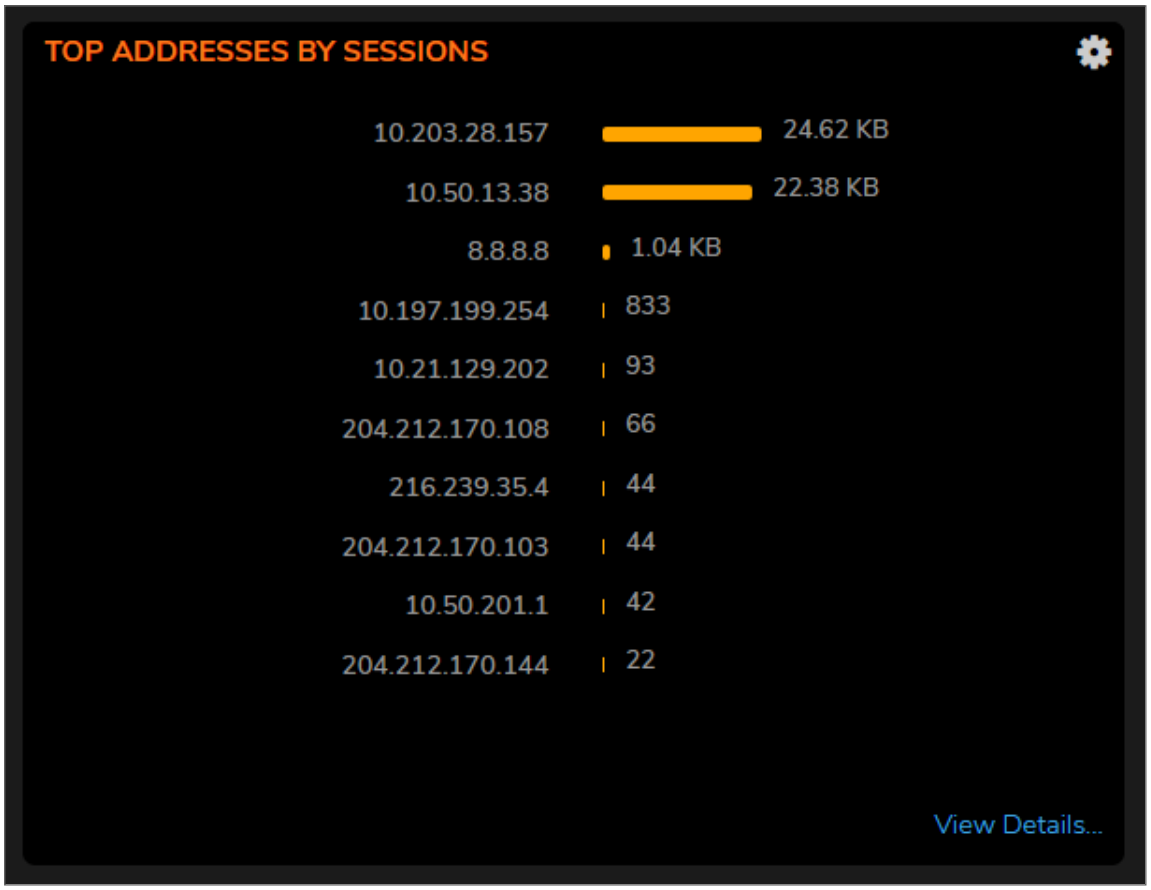
You can also track other user-level transactions and activities by filtering on several different options including **Top Users by**:

- 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**.

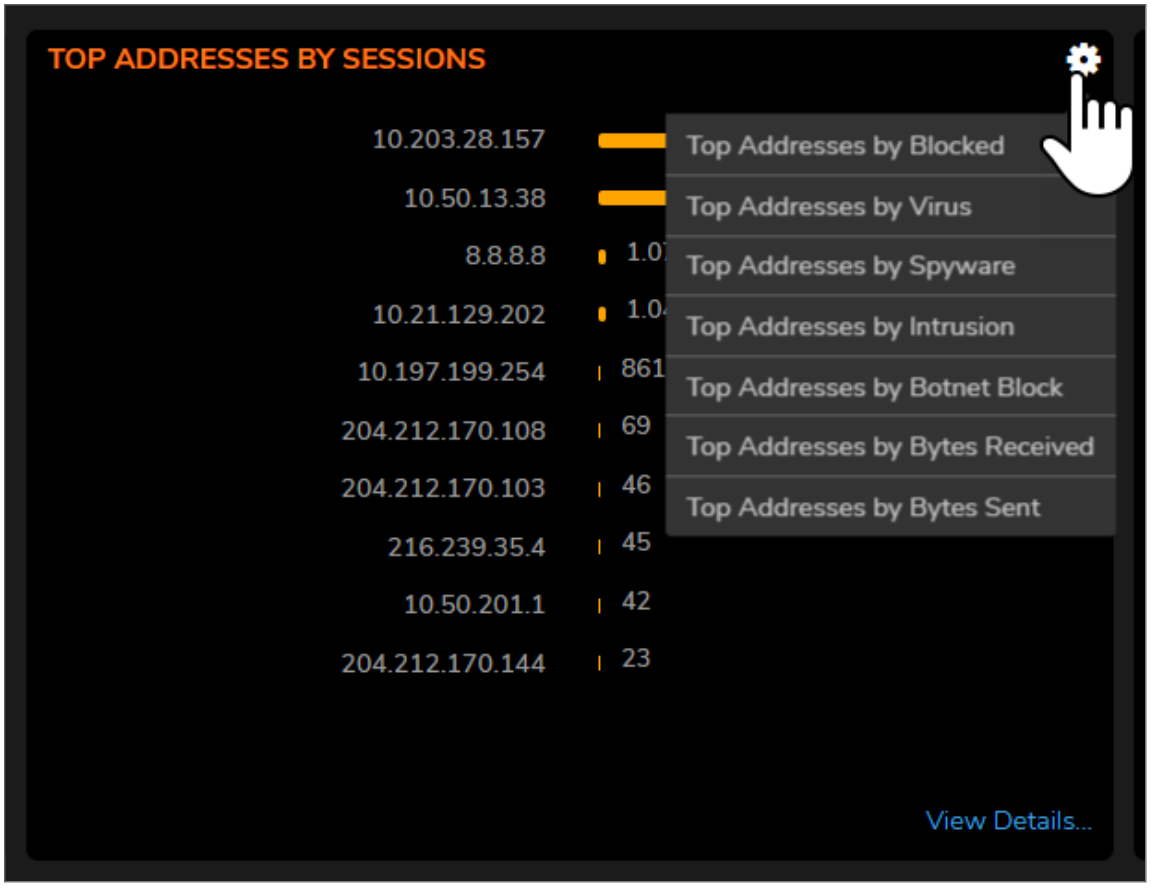
Top Addresses

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**:

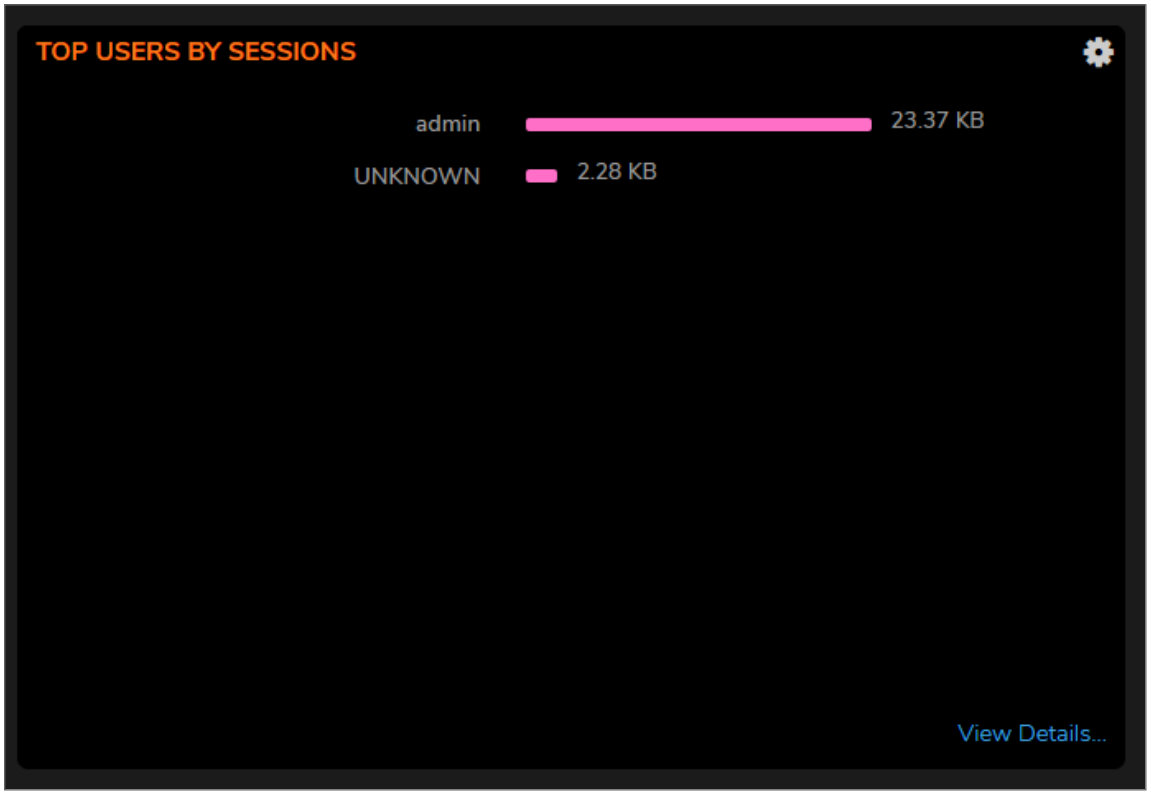
- Blocked
- Virus
- Spyware
- Intrusion
- Botnet Block
- Bytes Received
- Bytes Sent



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

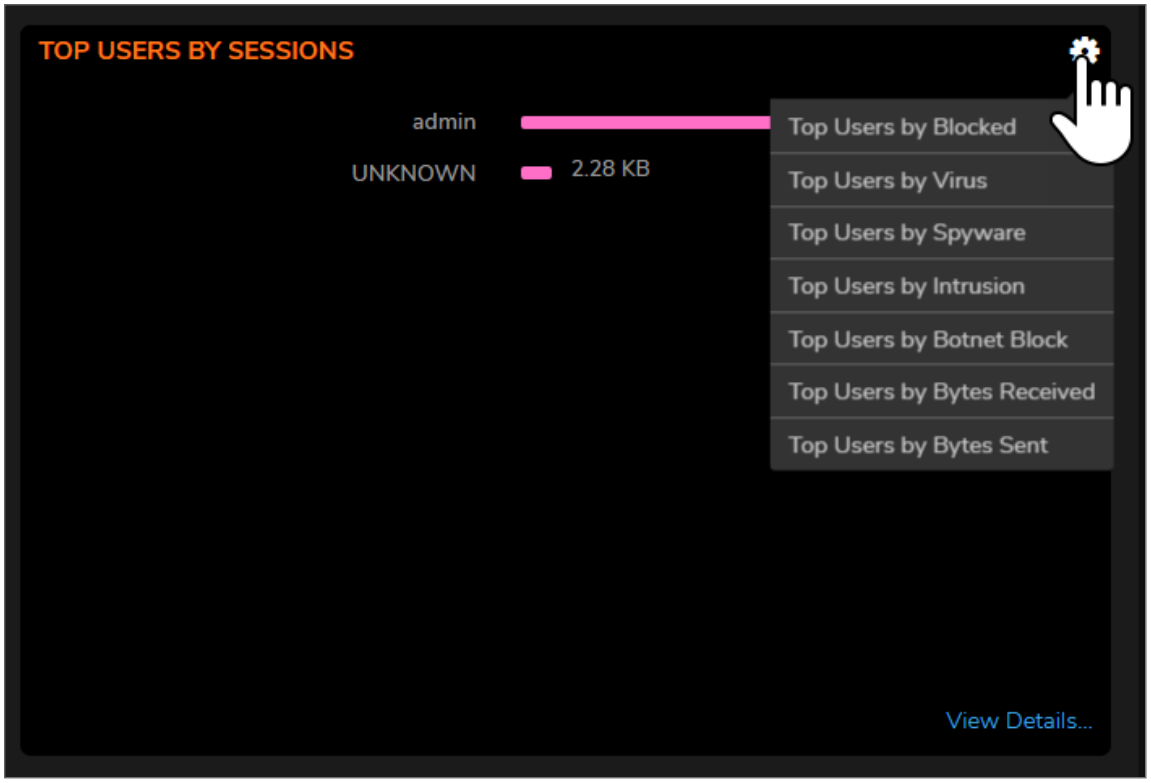
Top Users

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**:

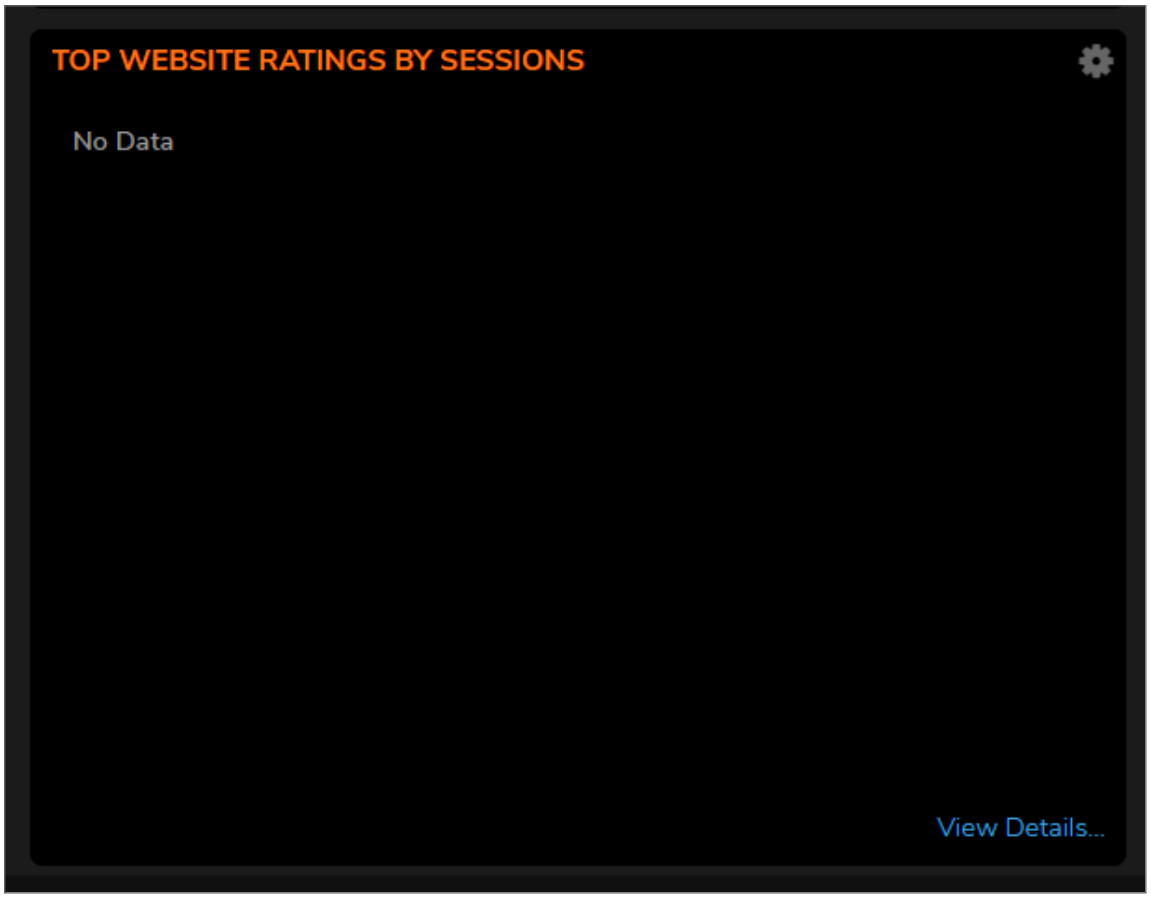
- Blocked
- Virus
- Spyware
- Intrusion
- Botnet Block
- Bytes Received
- Bytes Sent



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**.

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 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 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 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

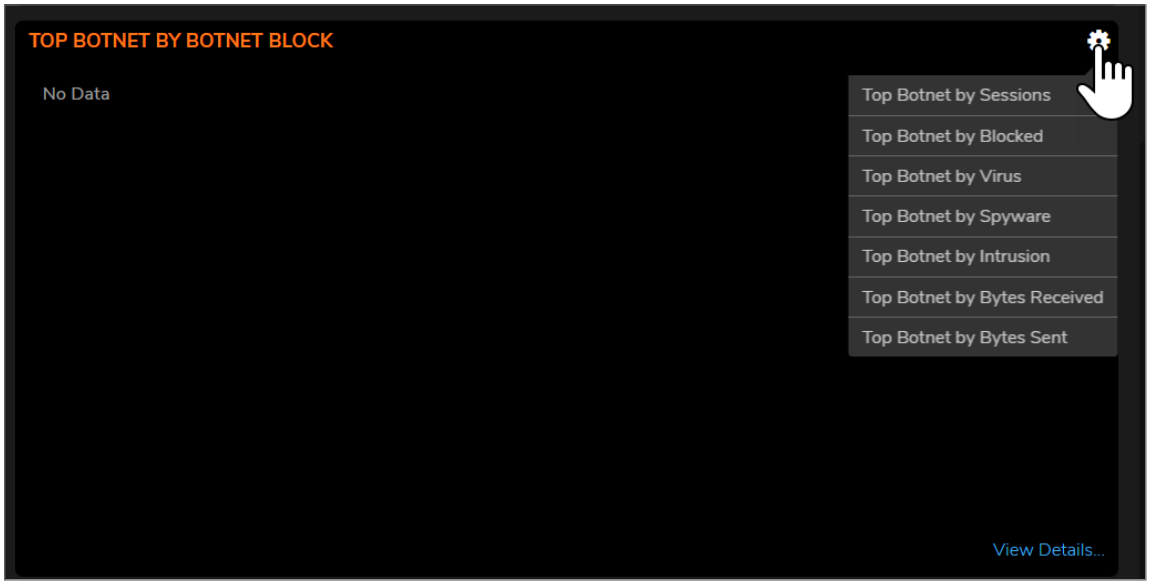
Click **View Details** to see complete reporting on all viruses located in **MONITOR | AppFlow > AppFlow Report | Spyware**.

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



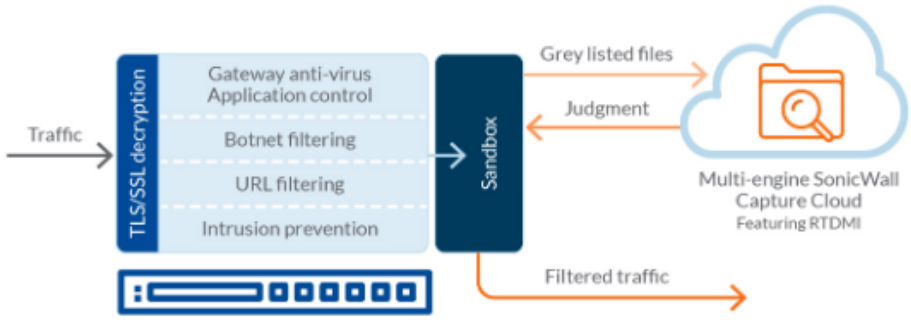
Click **View Details** to see complete reporting on all botnets located in **MONITOR | AppFlow > AppFlow Report | IP**.

2

Capture ATP

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

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



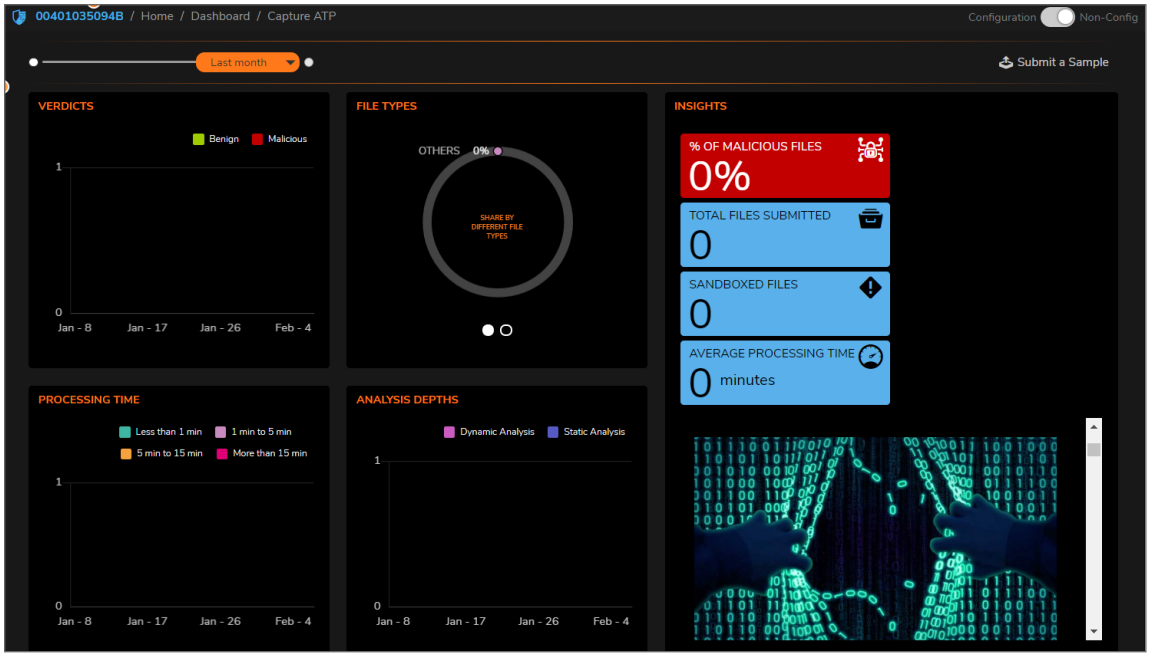
Capture ATP Dashboard

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.

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 Gateway Anti-Virus Database services.


00401035094B / Home / Dashboard / Capture ATP
Configuration
Non-Config
Last month
Submit a Sample
VERDICTS
Benign
Malicious
1
0
Jan - 8
Jan - 17
Jan - 26
Feb - 4
FILE TYPES
OTHERS 0%
SHARE BY DIFFERENT FILE TYPES
INSIGHTS
% OF MALICIOUS FILES
0%
TOTAL FILES SUBMITTED
0
SANDBOXED FILES
0
AVERAGE PROCESSING TIME
0 minutes
PROCESSING TIME
Less than 1 min
1 min to 5 min
5 min to 15 min
More than 15 min
ANALYSIS DEPTHS
Dynamic Analysis
Static Analysis

3

Policy Overview

You can look up security policy effectiveness by manually providing filtering fields for the match attributes. This service shows the rules that would be affected based on the match attributes you provide. You can also select “show all matched rules” to see all the rules that would potentially be hit for the provided match attributes.

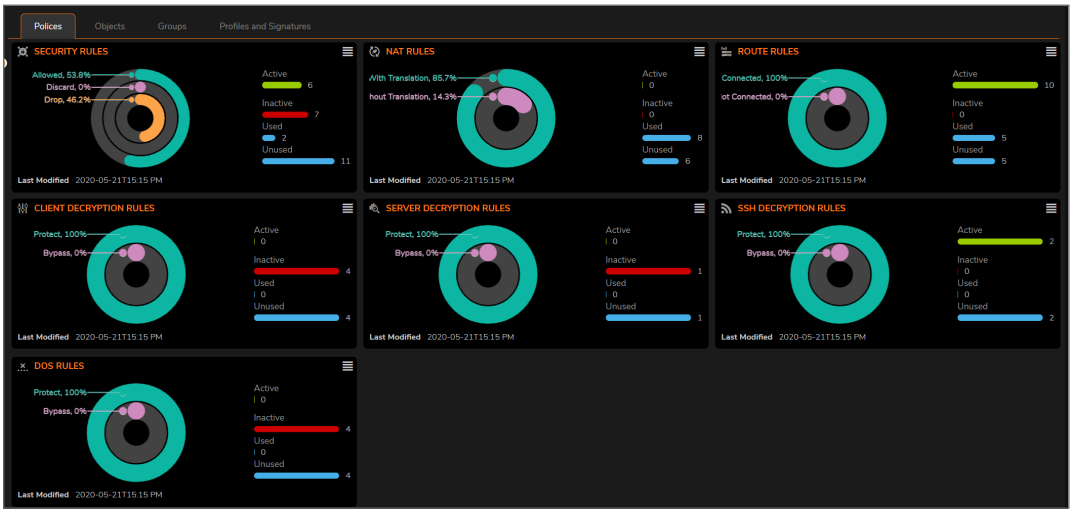
Policies

On the **Policies** tab, you can view a real-time policy overview for all established policy rules, or for an individual rule, which you would like to monitor. Real-time multi-level charts are displayed in the following ways:

- Connections Allowed/Discarded/Dropped
- Active/Inactive components
- Used/Unused components
- Bandwidth Usage
- Total connection usage

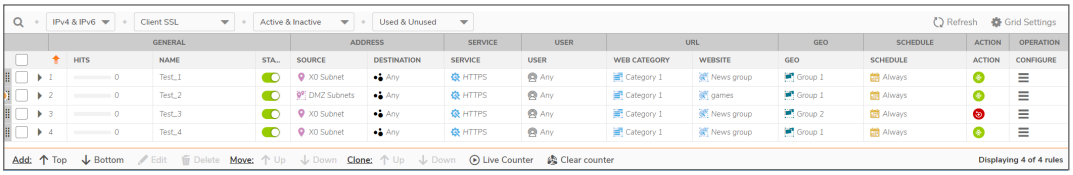
To view the policy overview:

1. Navigate to **HOME | Dashboard > Policy Overview > Policies**.



2. You can click the **Redirect** icon on the top right of each display to manage or change configuration of the chart.

3. In this instance, click the Redirect icon on the Client Decryption Rules overview, takes you to the Decryption Policy page at **POLICY | Rules and Policies > Decryption Policy**. Using the filters at the top of the table, you can narrow your display requirements for the associated Policy chart.



Objects

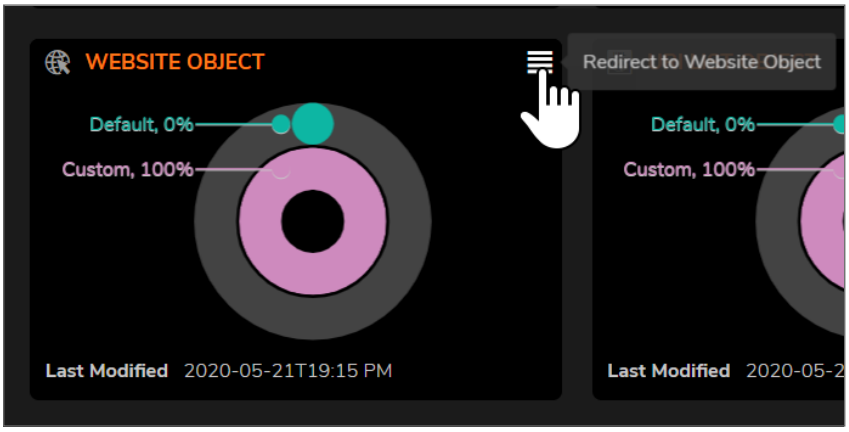
On the **Objects** tab, you can view a real-time match object overview for all established match objects, or for an individual object rules, which you would like to monitor. Real-time multi-level charts are displayed in the following ways:

- Default object usage
- Custom object usage

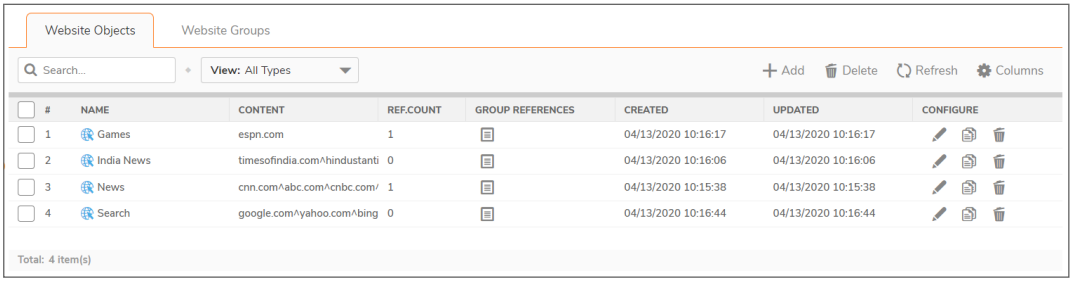
To view the Objects overview:

1. Navigate to **HOME | Dashboard > Policy Overview > Objects**.

2. You can click the **Redirect** icon on the top right of each display to manage or change configuration of the chart.



3. In this instance, click the Redirect icon on the Website Object overview, takes you to the **Website Objects** page at **OBJECT | Match Objects > Websites | Match Objects**. Using the filters at the top of the table, you can narrow your display requirements for the associated Website Objects chart.



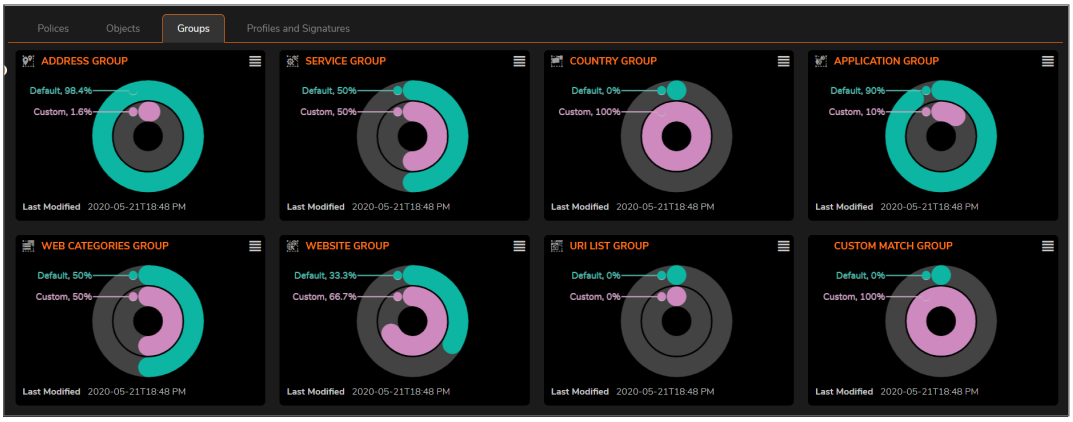
Groups

On the **Groups** tab, you can view a real-time match object groups overview for all established match group objects, or for an individual group object rules, which you would like to monitor. Real-time multi-level charts are displayed in the following ways:

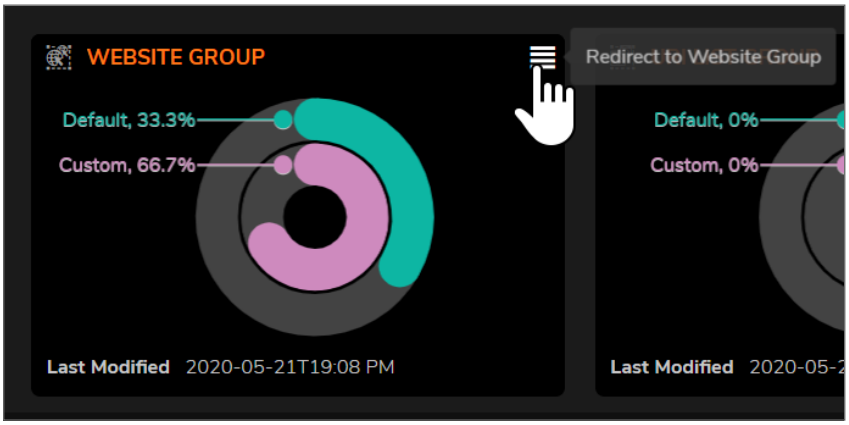
- Default group object usage
- Custom group object usage

To view the Groups overview:

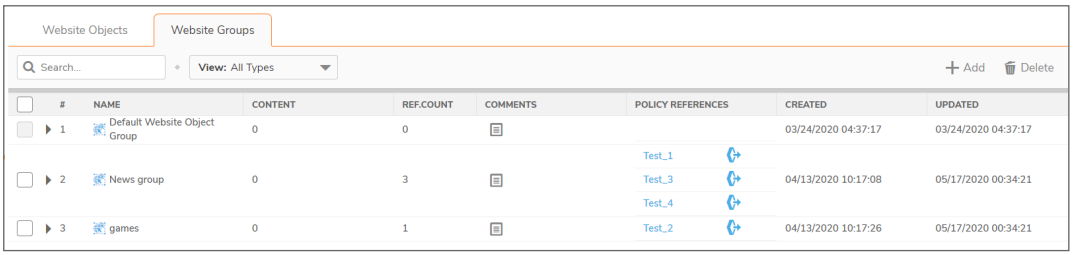
1. Navigate to **HOME | Dashboard > Policy Overview > Groups**.



2. You can click the **Redirect** icon on the top right of each display to manage or change configuration of the chart.



3. In this instance, click the Redirect icon on the Website Group overview, takes you to the Websites page at **OBJECT | Match Objects > Websites | Website Groups**. Using the filters at the top of the table, you can narrow your display requirements for the associated Service Groups chart.



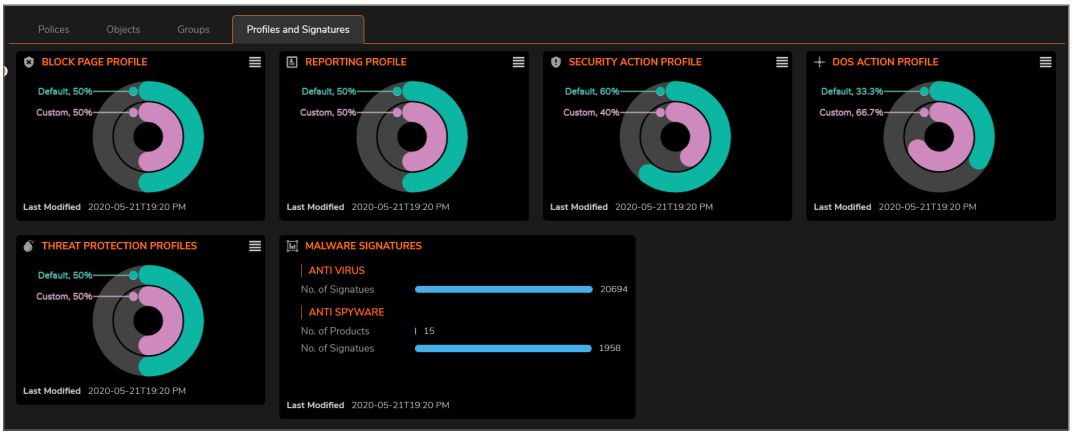
Profiles and Signatures

On the **Profiles and Signatures** tab, you can view a real-time match object groups overview for all profiles and malware signatures that you would like to monitor. Real-time multi-level charts are displayed in the following ways:

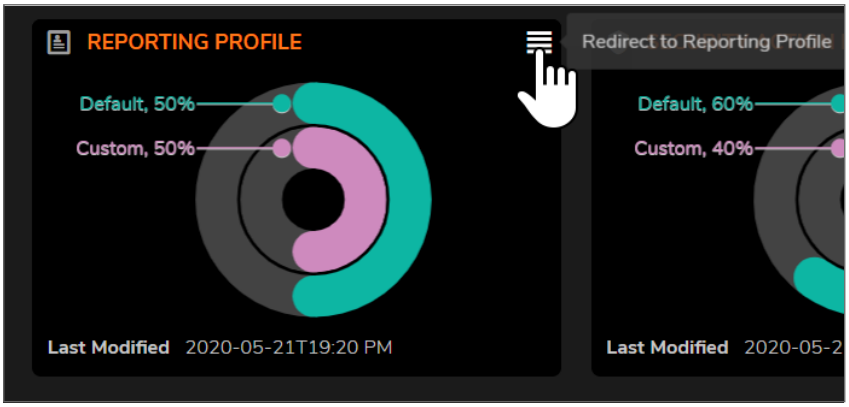
- Default profile usage
- Custom profile usage
- Number of Signatures discovered
- Number of affected units

To view the Profiles and Signatures overview:

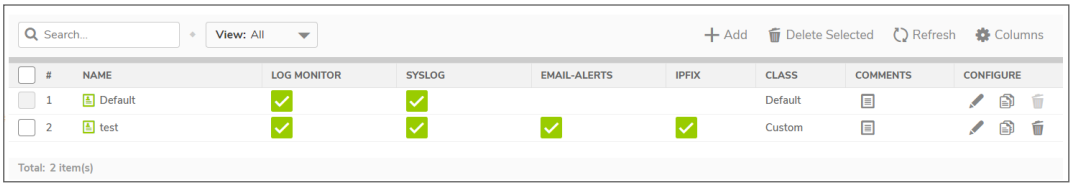
1. Navigate to **HOME | Dashboard > Policy Overview > Profiles and Signatures**.



2. You can click the **Redirect** icon on the top right of each display to manage or change configuration of the chart.



3. In this instance, click the Redirect icon on the Reporting Profile overview, takes you to the Reporting page at **OBJECT | Profiles > Reporting**. Using the filters at the top of the table, you can narrow your display requirements for the associated Reporting Profile chart.



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.

SonicOSX Dashboard Administration Guide
Updated - August 2020
Software Version - 7
232-005330-00 Rev A

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/en-us/legal/license-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