



SonicOS 7.0

Dashboard

Administration Guide

SONICWALL[®]

Contents

About Dashboard	4
System View	4
Access Point View	5
Topology View	6
Capture ATP View	7
Policy Overview	7
System	9
Device	9
Summary	10
Traffic Distribution	10
Top Users	12
Insights	13
Observed Threats	14
Top Countries	15
Network	16
Top Applications	17
Top Addresses	18
Top Users	20
Top Website Ratings	21
Threat	21
Top Intrusion	22
Top Virus	22
Top Spyware	22
Top Botnet	23
Access Points	24
Feature Limitations	25
Access Point Snapshot	25
Client Association	25
Real-Time Bandwidth	25
Client Report	25
OS Type	26
Radio	26
Top Client	26
Real-Time Client Monitor	26
Client Report and Client Monitor Filtering	26

Capture ATP	27
WWAN	28
Policy Overview	29
Policies	29
Objects	31
Groups	32
Profiles and Signatures	34
Topology	36
Managing the Topology View	36
Managing Access Points in the Topology View	37
Editing an Access Point	37
Showing Statistics	37
Monitoring Status on an Access Point	38
Deleting an Access Point	38
Legal Information	39
API	40
SonicWall Support	41
About This Document	42

About Dashboard

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

Topics:

- [System View](#)
- [Access Point View](#)
- [Capture ATP View](#)
- [Topology View](#)
- [Policy Overview](#)


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

System View

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

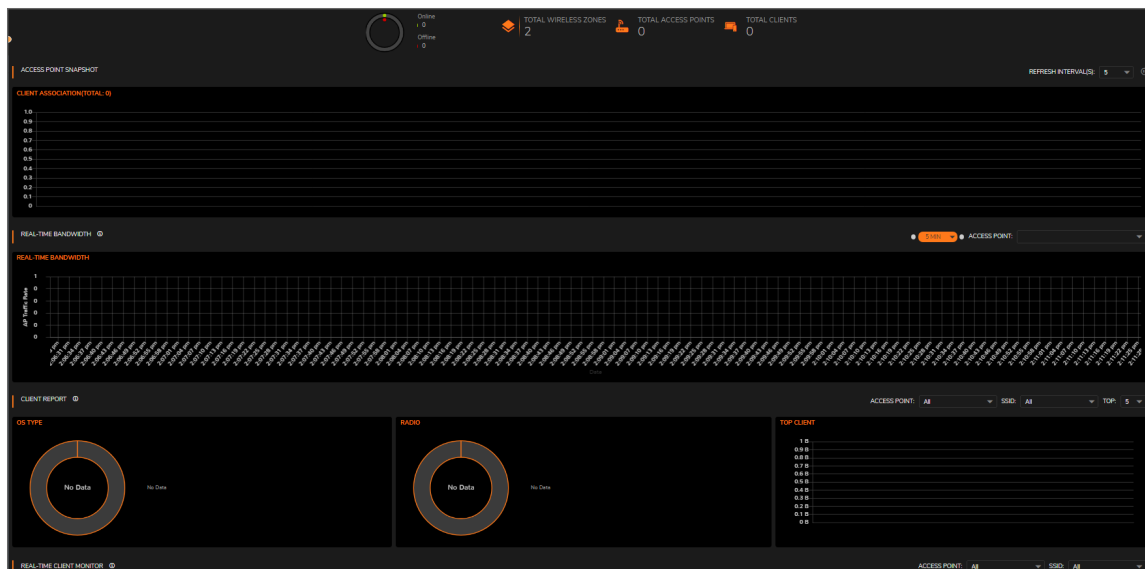


The **System** view offers a high level view of the system performance. You can select different tabs for different types of summaries. They include **Device**, **Summary**, **Network**, and **Threat**. Each pane on the tab represents a specific feature being tracked. If you see issues that need more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

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

Access Point View

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

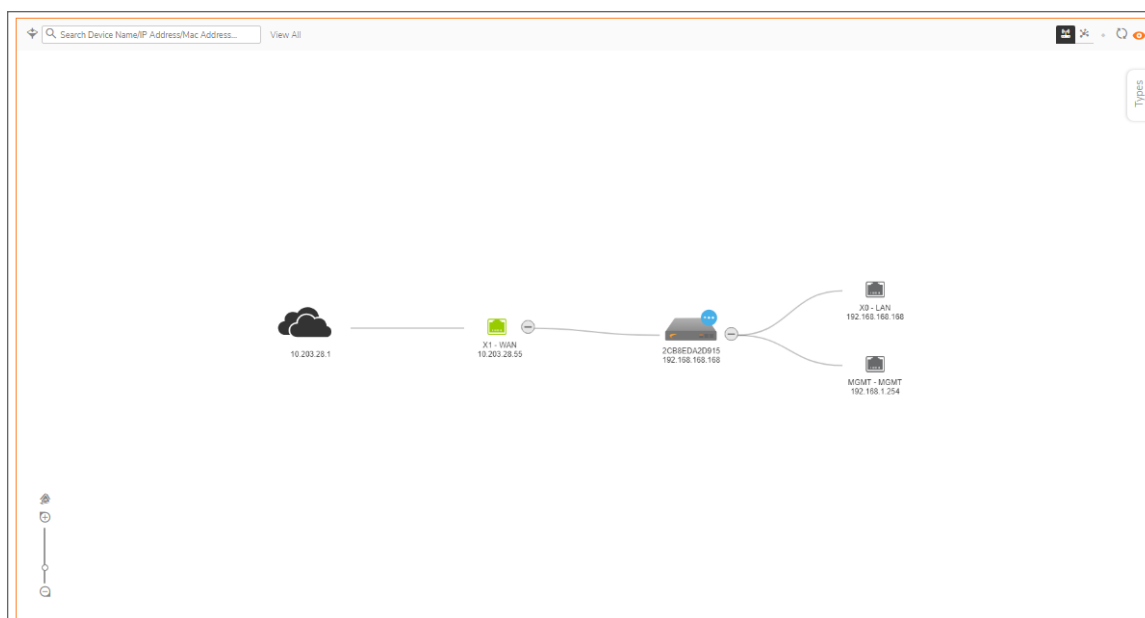


The **Access Points** view offers a high level view of the performance of the access points in the network. You can review the summaries across the top of the page and then scroll to see the different reports.

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

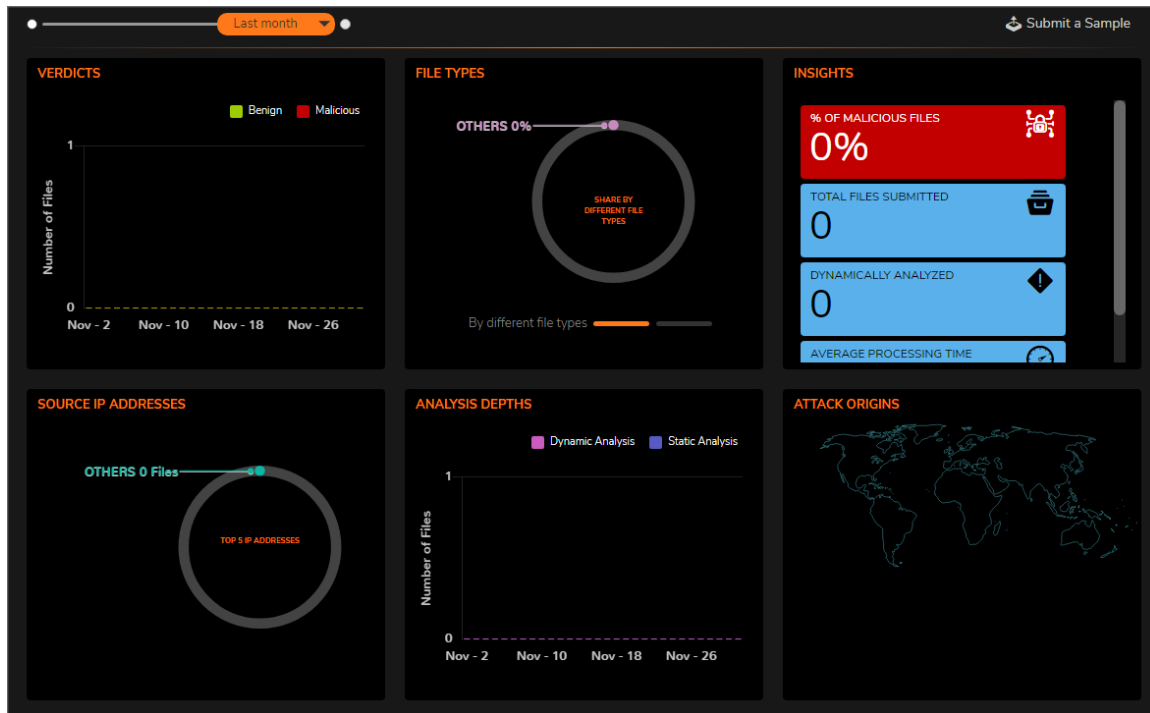
Topology View

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



Capture ATP View

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



Policy Overview

When operating in Policy Mode, the **Policy Overview** option displays on the dashboard. The SonicOS Dashboard summarizes policy effectiveness for different match attributes. The navigation path for the **Policy Overview** is **HOME > Dashboard > Policy Overview**



You can review the different types of summaries by selecting the different tabs: **Policies**, **Objects**, **Groups**, and **Profiles and Signatures**. If you see issues that need more investigation, you can drill down on the options icon,



in the upper right corner. This takes you to other reports that can help you narrow the source of the issue.

System

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


Topics:

- [Device](#)
- [Summary](#)
- [Network](#)
- [Threat](#)

① | **IMPORTANT:** Zero Touch is not supported in SonicOS when implemented with on-premises Analytics.

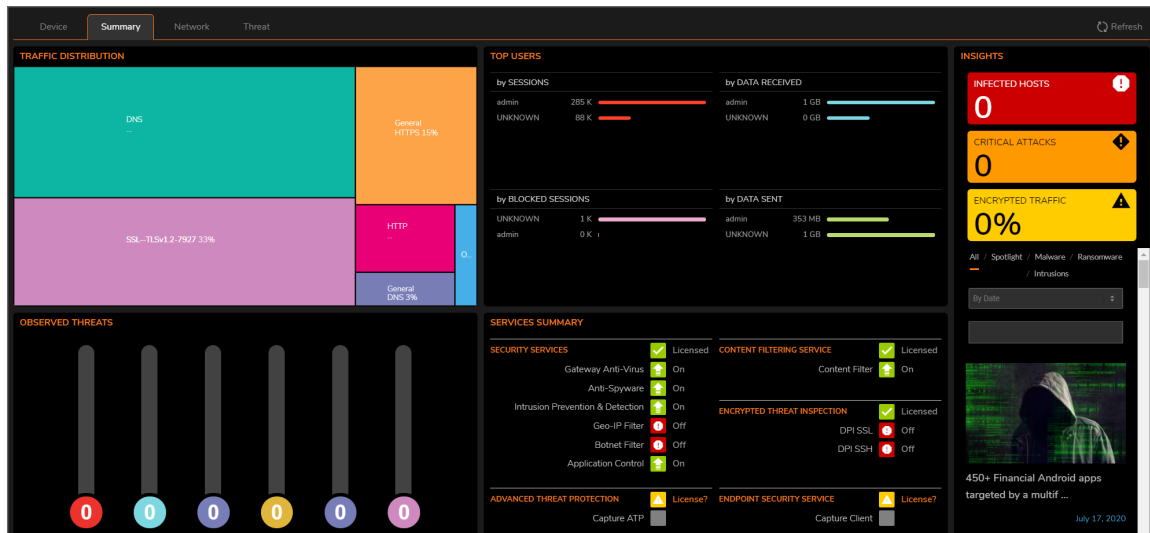
Device

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

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

Summary

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



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

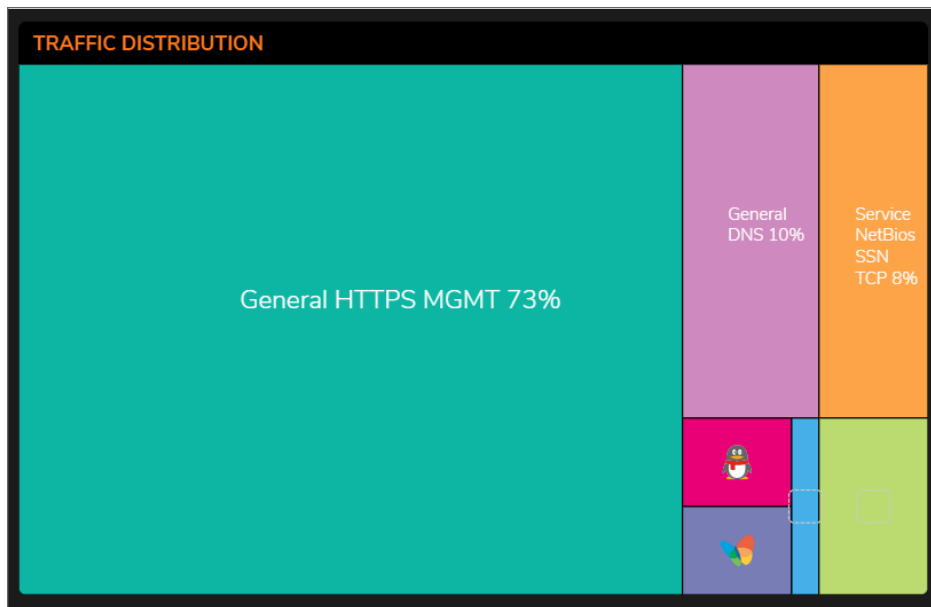
The following table describes the components that make up the **System Summary**.

SYSTEM SUMMARY

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

Traffic Distribution

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



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

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

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

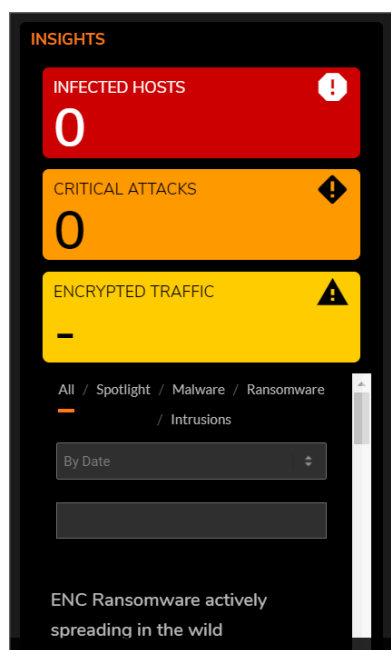
Top Users

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



Insights

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



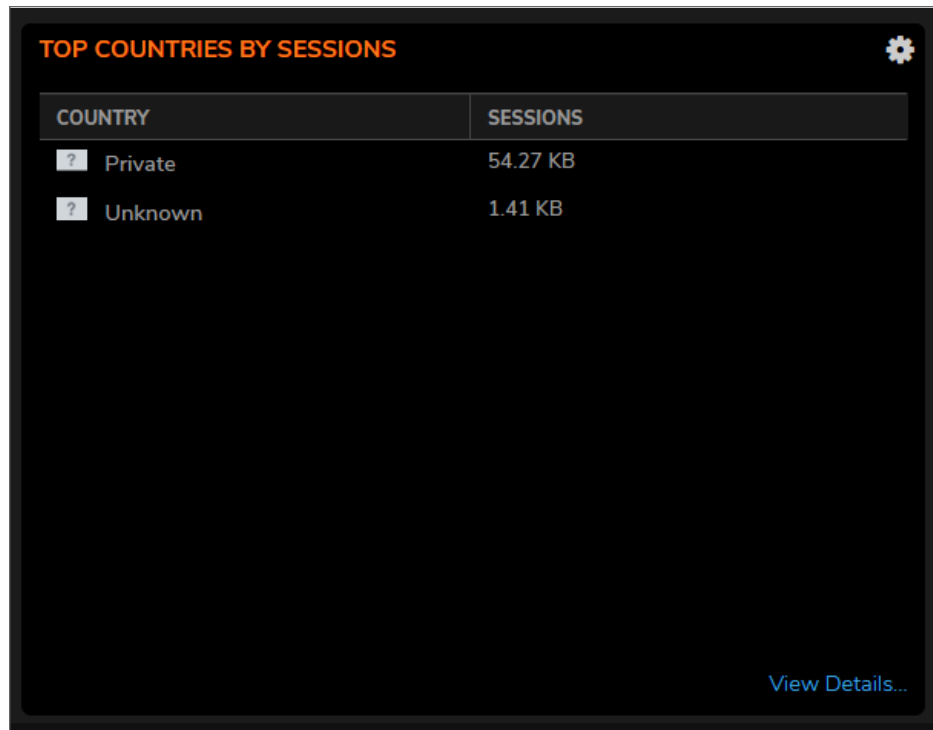
Observed Threats

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



Top Countries

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



COUNTRY	SESSIONS
? Private	54.27 KB
? Unknown	1.41 KB

[View Details...](#)

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

- Dropped
- Bytes Received
- Bytes Sent



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

Network

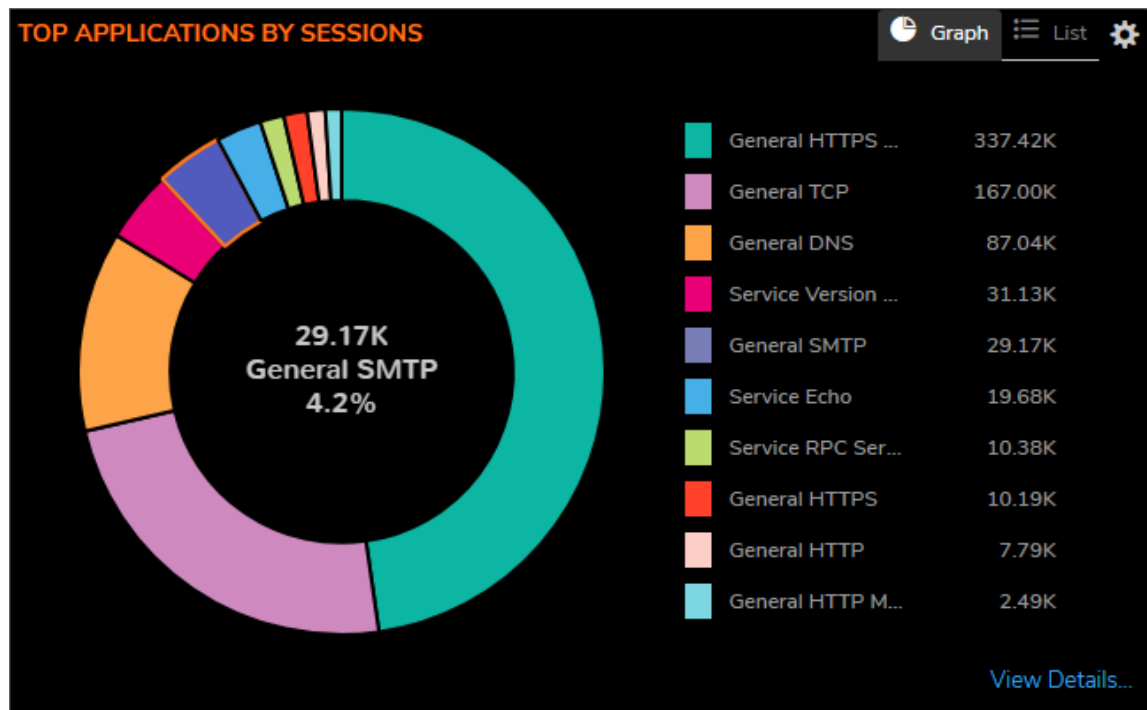
The **Network** view provides session reporting windows that display the top Applications, Addresses, Users, Website Ratings, Countries, and so on.

Topics:

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

Top Applications

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



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

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

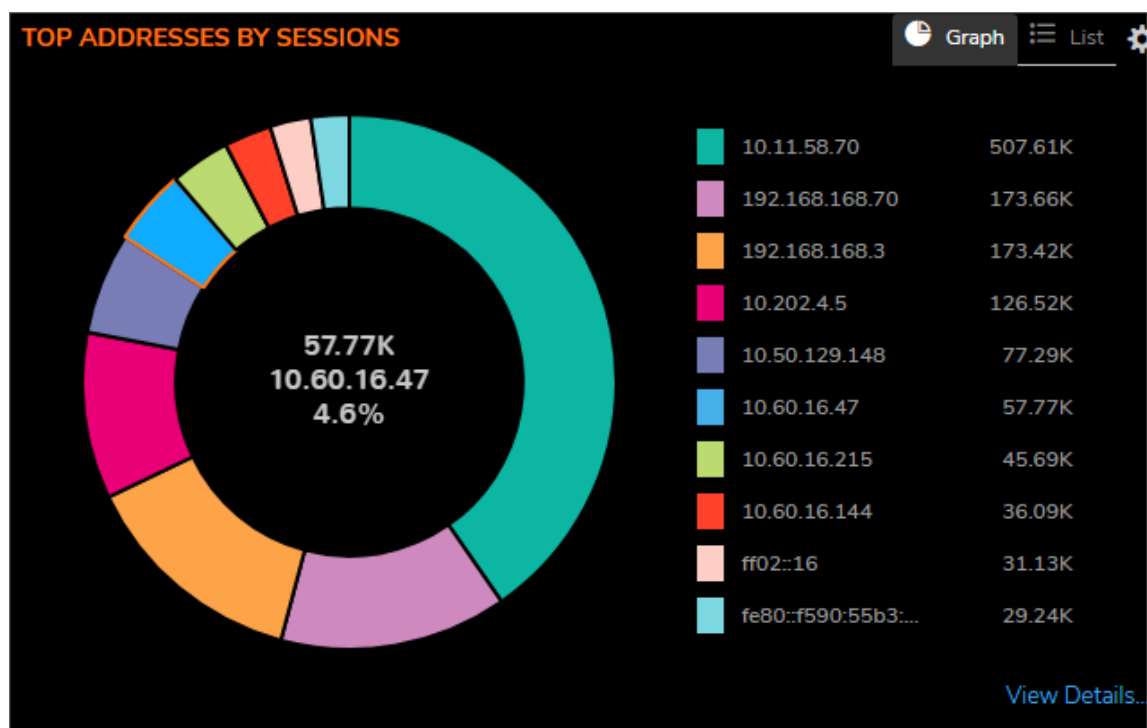
- By data received
- By data sent
- By access rules block
- By app rules block
- By location block
- By botnet block
- By virus
- By intrusion
- By spyware

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

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



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

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

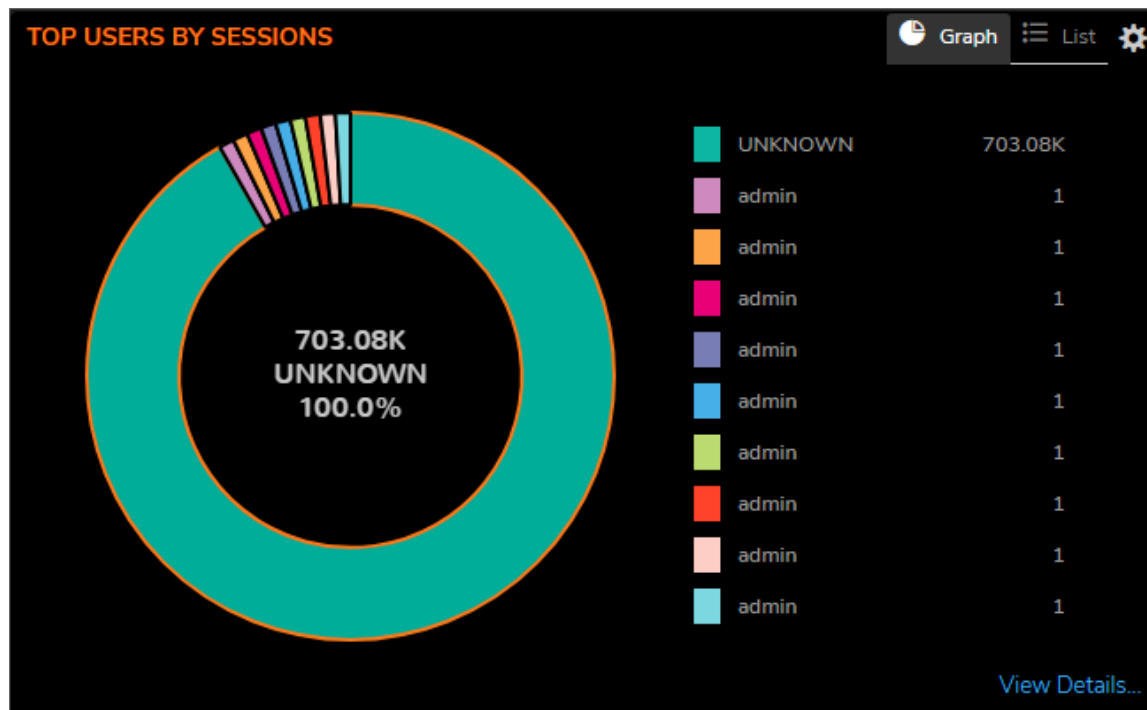
- Blocked
- Virus
- Spyware
- Intrusion
- Botnet block
- Data received
- Data sent

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

- If operating in Classic Mode, it goes to **MONITOR | Logs > Threat Logs**.
- If operating in Policy Mode, it goes to **MONITOR | AppFlow > AppFlow Report | IP Addresses**.

Top Users

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



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

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

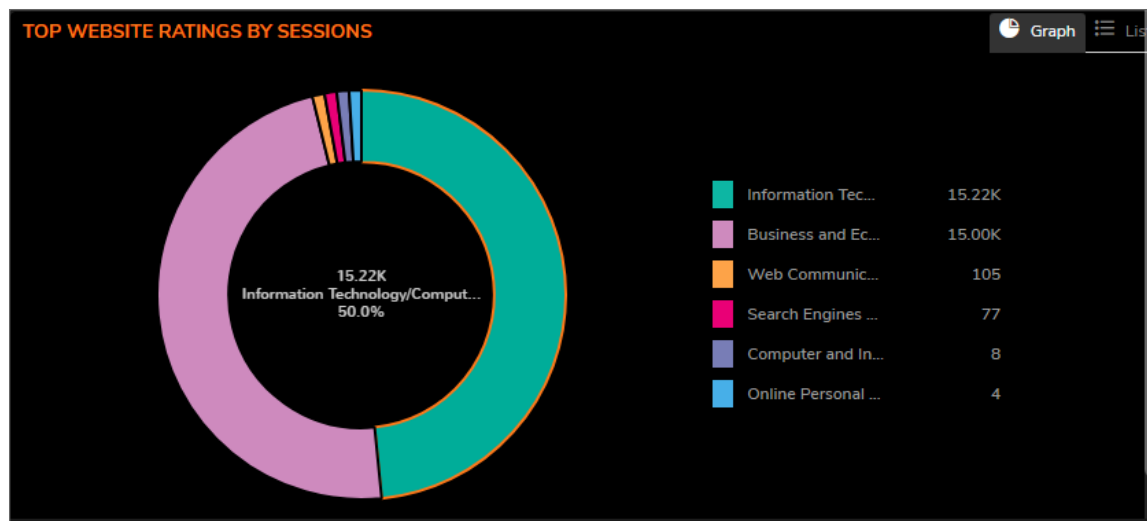
- Blocked
- Virus
- Spyware
- Intrusion
- Botnet block
- Data received
- Data sent

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

- If operating in Classic Mode, it goes to **MONITOR | Logs > Threat Logs**.
- If operating in Policy Mode, it goes to **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 view information in **Graph** form or you can select the **List** option.

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

- If operating in Classic Mode, it goes to **MONITOR | Logs > Threat Logs**.
- If operating in Policy Mode, it goes to **MONITOR | AppFlow > AppFlow Report | Web Categories**.

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 select a **Graph** view or a **List** view by clicking the appropriate icon.

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

- Count
- Percentage

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

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

Top Virus

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

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

- Count
- Percentage

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

- If operating in Classic Mode, it goes to **MONITOR | Logs > Threat Logs**.
- If operating in Policy Mode, it goes to **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 select a **Graph** view or a **List** view by clicking the appropriate icon.

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

- Count
- Percentage

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

- If operating in Classic Mode, it goes to **MONITOR | Logs > Threat Logs**.
- If operating in Policy Mode, it goes to **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 select a **Graph** view or a **List** view by clicking the appropriate icon.

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

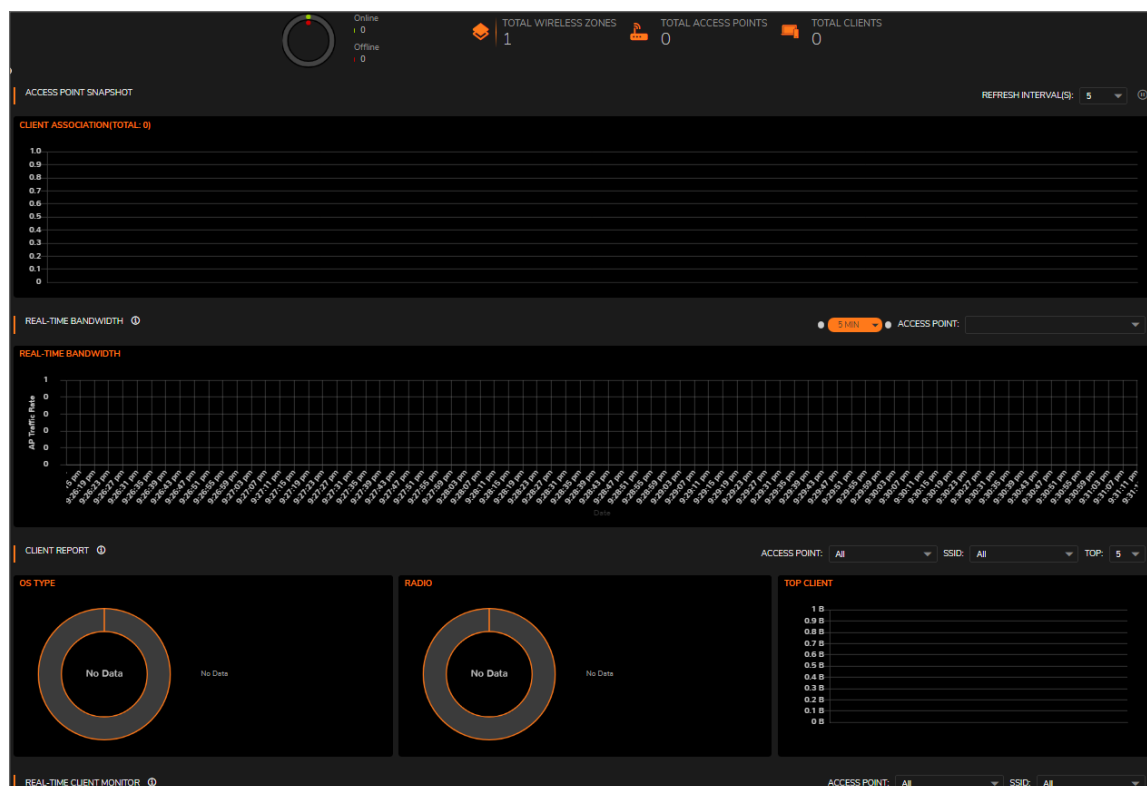
- Blocked
- Virus
- Spyware
- Intrusion
- Bytes received
- Bytes sent

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

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

Access Points

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



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

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

Feature Limitations

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

Access Point Snapshot

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

Client Association

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

Real-Time Bandwidth

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

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

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

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

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

Client Report

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

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

OS Type

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

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

Radio

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

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

Top Client

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

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

Real-Time Client Monitor

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

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

Client Report and Client Monitor Filtering

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

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

Capture ATP

The **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.

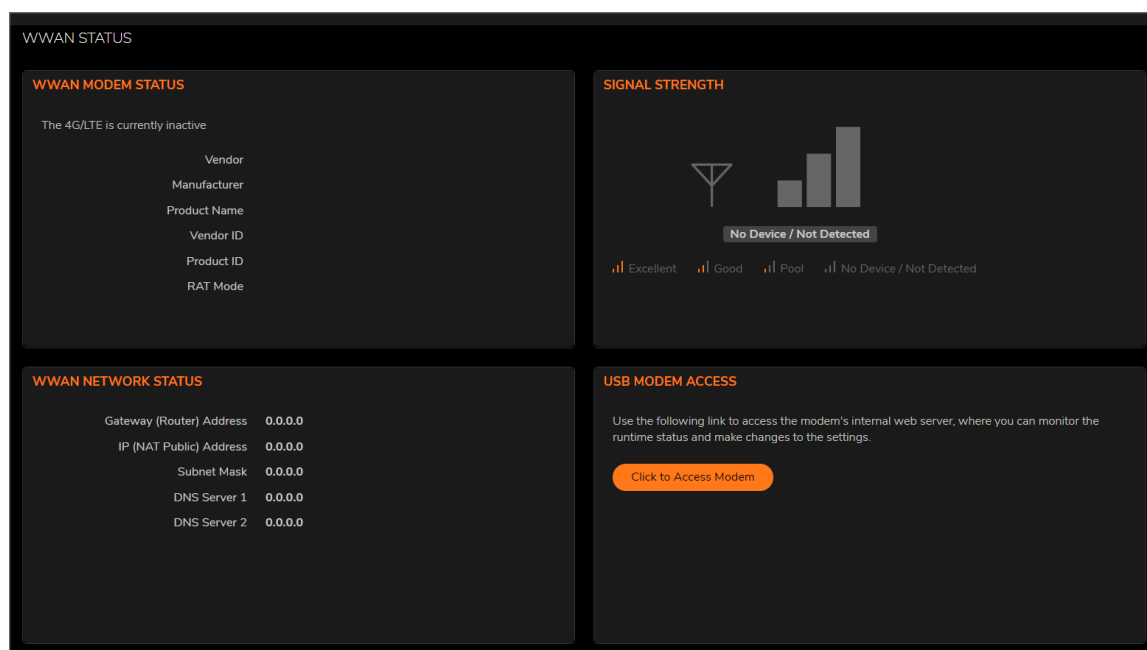
Capture ATP is available in Policy Mode. It is not available in Classic Mode.

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.



WWAN

If you have a 3G/4G/LTE device connected to one of your access points, the **HOME | Dashboard > WWAN** page offers monitoring information on that device.



The first panel provides connectivity data and modem status, and the second panel shows a graphical representation of the device's signal strength.

If no 3G/4G/LTE device is detected on one of your access points, you get the following message on the **HOME | Dashboard > WWAN | Signal Strength** page:

No Device / Not Detected.

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.

Policy Overview feature of SonicOS running Policy Mode. It is not available in Classic Mode.

Policies

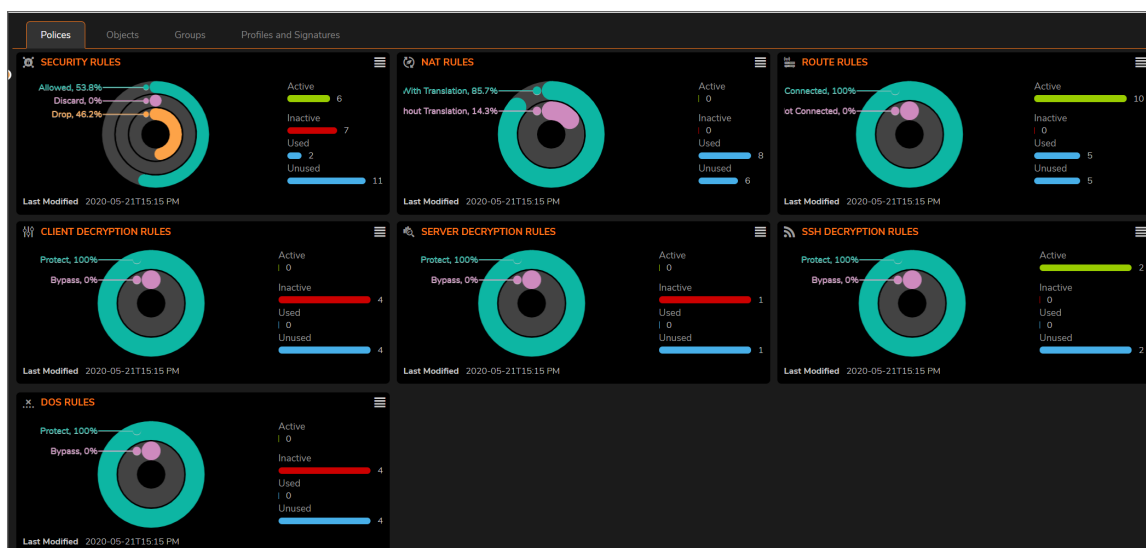
On the **Policies** tab, you can view a real-time policy overview for all established policy rules, or for an individual rule, which you would like to monitor. Real-time multi-level charts are displayed in the following ways:

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

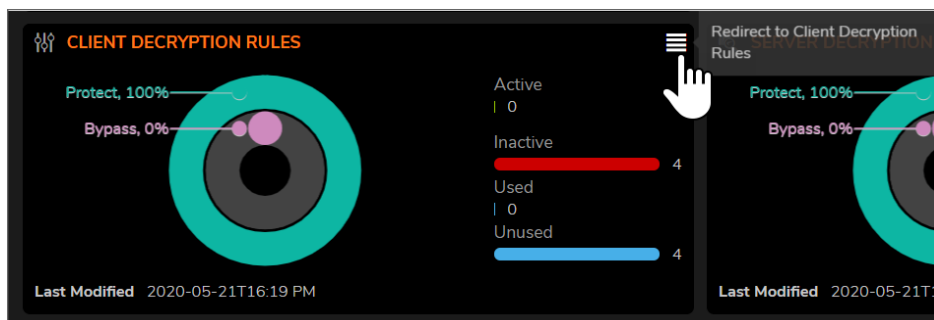
Policies tab is available in Policy Mode. It is not available in Classic Mode.

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.

<div> <input type="text" value="Q"/> <input type="text" value="IPv4 & IPv6"/> <input type="text" value="Client SSL"/> <input type="text" value="Active & Inactive"/> <input type="text" value="Used & Unused"/> <input type="button" value="Refresh"/> <input type="button" value="Grid Settings"/> </div>													
	HITS	NAME	STATUS	SOURCE	DESTINATION	SERVICE	USER	WEB CATEGORY	WEBSITE	GEO	SCHEDULE	ACTION	OPERATION
1	0	Test_1	ON	X0 Subnet	Any	HTTPS	Any	Category 1	News group	Group 1	Always	ON	CONFIGURE
2	0	Test_2	ON	DMZ Subnets	Any	HTTPS	Any	Category 1	games	Group 1	Always	ON	CONFIGURE
3	0	Test_3	ON	X0 Subnet	Any	HTTPS	Any	Category 1	News group	Group 2	Always	OFF	CONFIGURE
4	0	Test_4	ON	X0 Subnet	Any	HTTPS	Any	Category 1	News group	Group 1	Always	ON	CONFIGURE

Objects

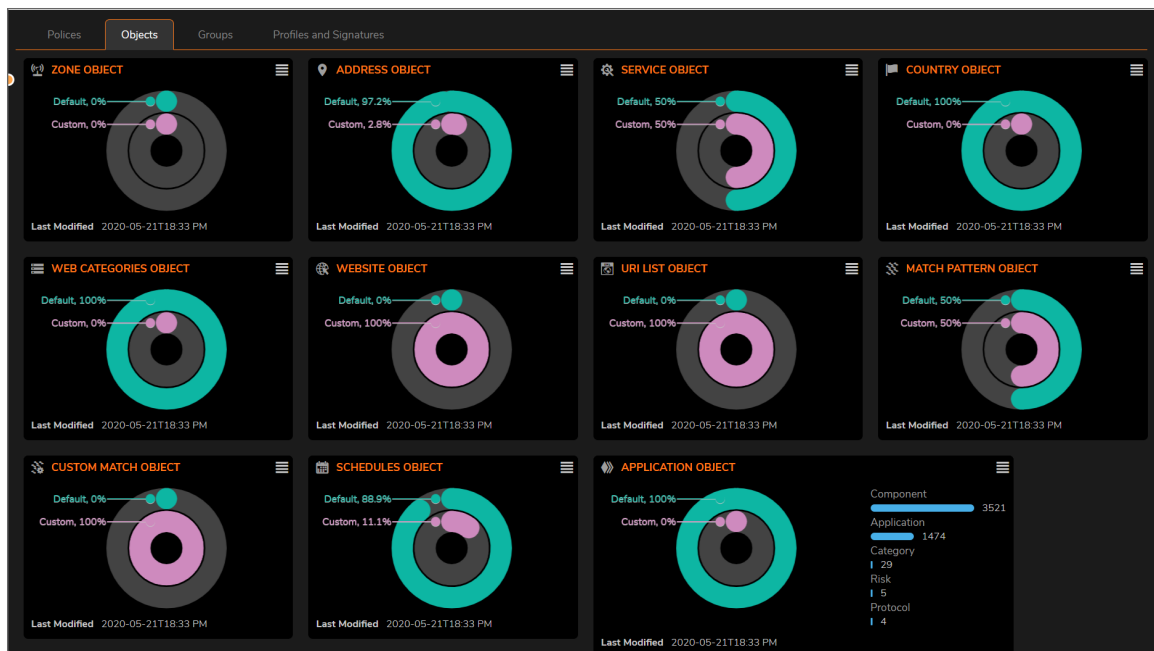
On the **Objects** tab, you can view a real-time match object overview for all established match objects, or for an individual object rules, which you would like to monitor. Real-time multi-level charts are displayed in the following ways:

- Default object usage
- Custom object usage

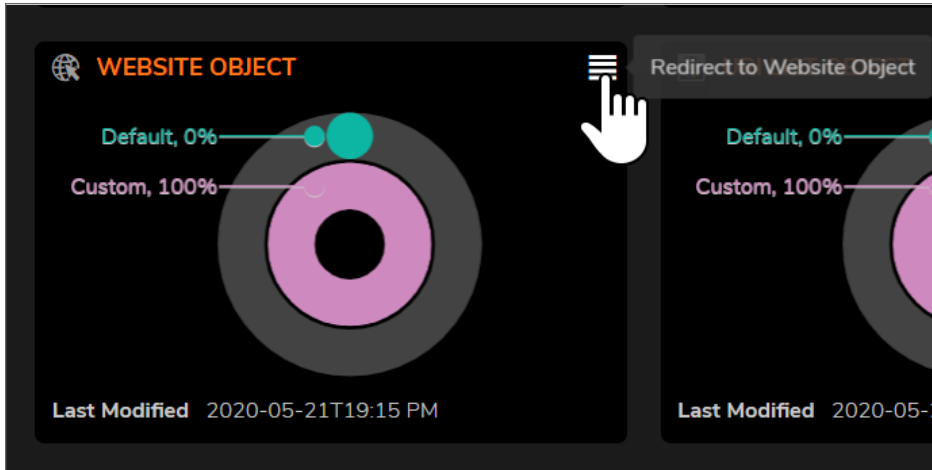
Policy Overview > Object tab is available in Policy Mode. It is not available in Classic Mode.

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.

Website Objects							
Website Groups							
Q Search...		View: All Types		+ Add Delete Refresh Columns			
#	NAME	CONTENT	REF.COUNT	GROUP REFERENCES	CREATED	UPDATED	CONFIGURE
1	Games	espn.com	1		04/13/2020 10:16:17	04/13/2020 10:16:17	
2	India News	timesofindia.com^hindustanti	0		04/13/2020 10:16:06	04/13/2020 10:16:06	
3	News	cnr.com^abc.com^cnbc.com/	1		04/13/2020 10:15:38	04/13/2020 10:15:38	
4	Search	google.com^yahoo.com^bing	0		04/13/2020 10:16:44	04/13/2020 10:16:44	
Total: 4 item(s)							

Groups

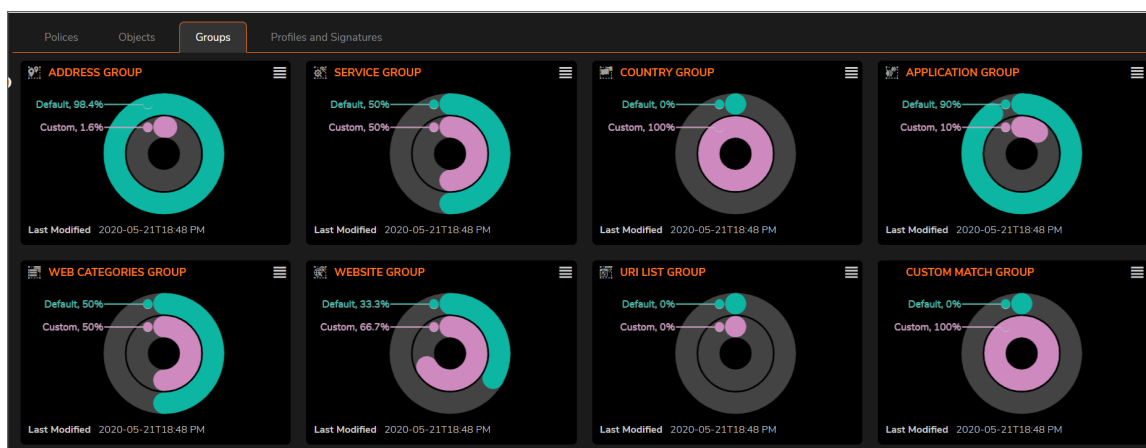
On the **Groups** tab, you can view a real-time match object groups overview for all established match group objects, or for an individual group object rules, which you would like to monitor. Real-time multi-level charts are displayed in the following ways:

- Default group object usage
- Custom group object usage

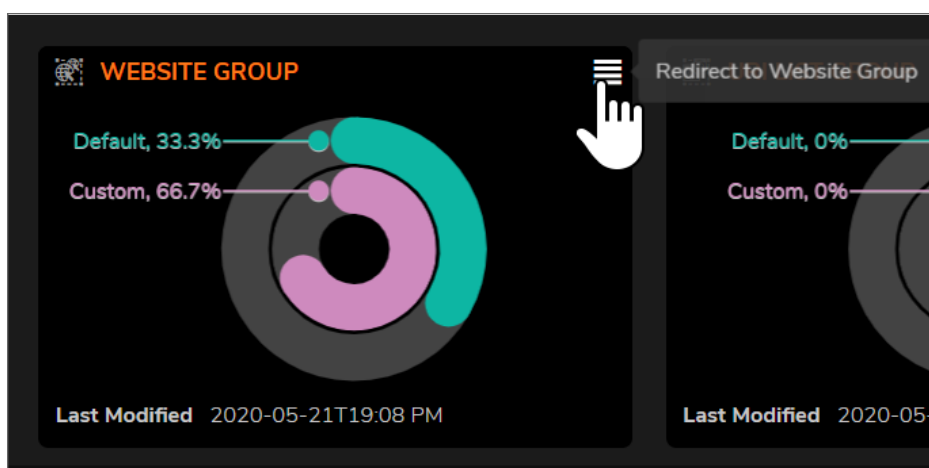
Groups tab is available in Policy Mode. It is not available in Classic Mode.

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.

Website Objects		Website Groups						
Q Search...		View: All Types		+ Add - Delete				
<input type="checkbox"/>	#	NAME	CONTENT	REF.COUNT	COMMENTS	POLICY REFERENCES	CREATED	UPDATED
<input type="checkbox"/>	1	Default Website Object Group	0	0		Test_1	03/24/2020 04:37:17	03/24/2020 04:37:17
<input type="checkbox"/>	2	News group	0	3		Test_3 Test_4	04/13/2020 10:17:08	05/17/2020 00:34:21
<input type="checkbox"/>	3	games	0	1		Test_2	04/13/2020 10:17:26	05/17/2020 00:34:21

Profiles and Signatures

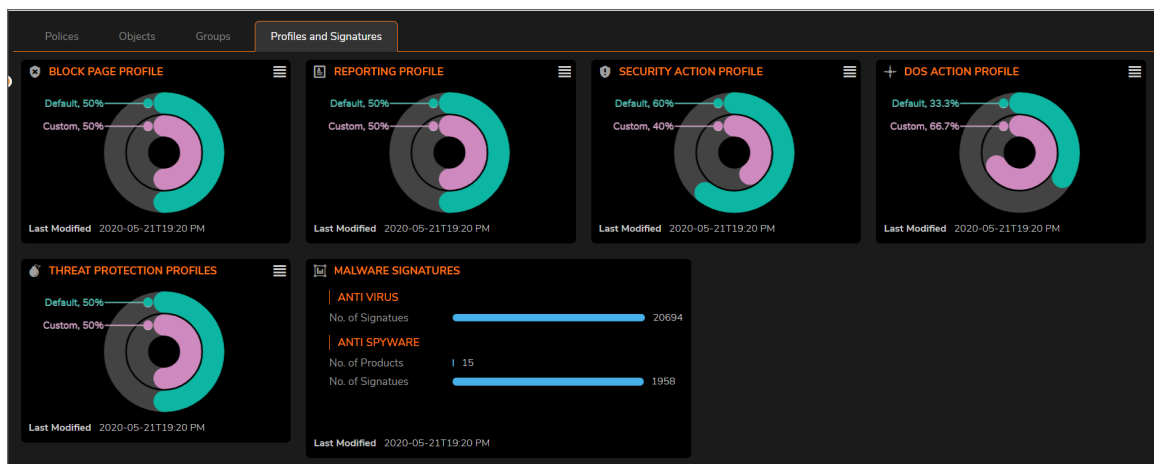
On the **Profiles and Signatures** tab, you can view a real-time match object groups overview for all profiles and malware signatures that you would like to monitor. Real-time multi-level charts are displayed in the following ways:

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

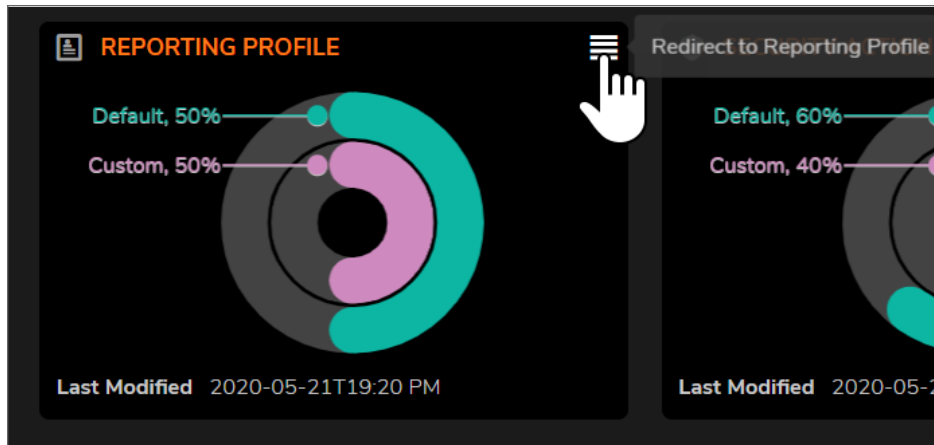
Profiles and Signatures tab is available in Policy Mode. It is not available in Classic Mode.

To view the Profiles and Signatures overview:

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



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



- 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.

Q Search...

+ View: All

+ Add

Delete Selected

Refresh

Columns

<input type="checkbox"/>	#	NAME	LOG MONITOR	SYSLOG	EMAIL-ALERTS	IPFIX	CLASS	COMMENTS	CONFIGURE
<input type="checkbox"/>	1	Default					Default		
<input type="checkbox"/>	2	test					Custom		

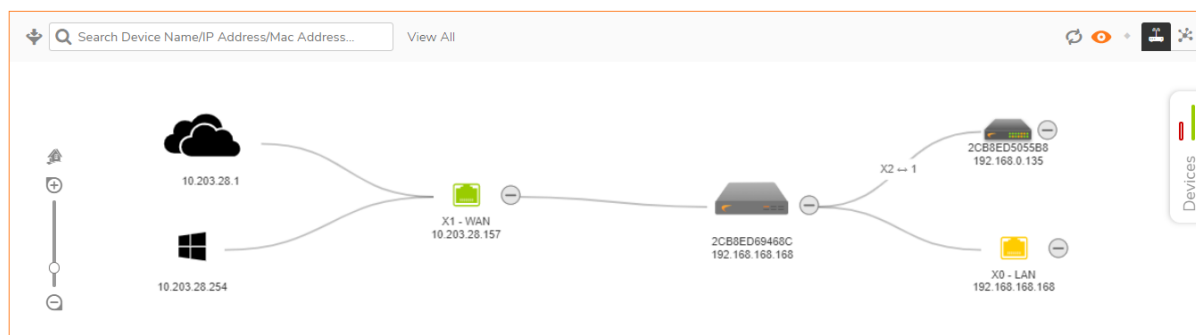
Total: 2 item(s)

Topology

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

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

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



Topics:

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

Managing the Topology View

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

You can also get detailed information on each of the devices in the Topology View. Just run your cursor over the device and a tool-tip bubble pops up. Depending on the type of device, it shows information like Name, IP

address, Interface, and Model. For access points, you can also see additional information like status and number of clients.

Each access point also uses color to indicate status:

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

Managing Access Points in the Topology View

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

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

Topics:

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

Editing an Access Point

To edit an access point in the Topology View::

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

Showing Statistics

To show statistics for an access point:

1. Navigate to **HOME | Dashboard > Topology**.
2. Roll your mouse over the access point you want to show.
3. Right-click on the access point.
4. Select **Show Access Point Statistics**.

5. Click **REFRESH** if you want to refresh the statistics.
6. Click **OK** when done.

Monitoring Status on an Access Point

To edit an access point in the Topology View:

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

Deleting an Access Point

To delete an access point in the Topology View:

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

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.

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](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.

SonicWall Support

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

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

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

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

About This Document

SonicOS Dashboard Administration Guide

Updated - May 2024

Software Version - 7.0

232-005330-00 Rev C

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products.

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

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

End User Product Agreement

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

Open Source Code

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

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