SonicOS 7.1

Real-Time Charts

Administration Guide

SONICWALL®

Contents

1

About SonicOS

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

Topics:

Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and threats to your network. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices like access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers two different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration and diagnostics.

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

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

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

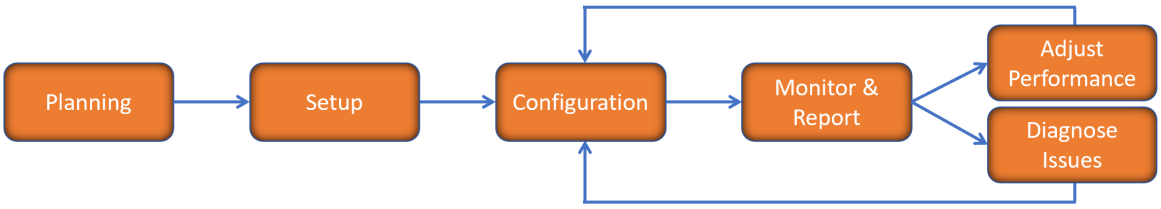
In addition to the management interface, SonicOS also has a full-featured API and a CLI to manage the firewalls. For more information, refer to:

- SonicOS 7.1 API Reference Guide

- *SonicOS Command Line Interface Reference Guide*

SonicOS Workflow

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

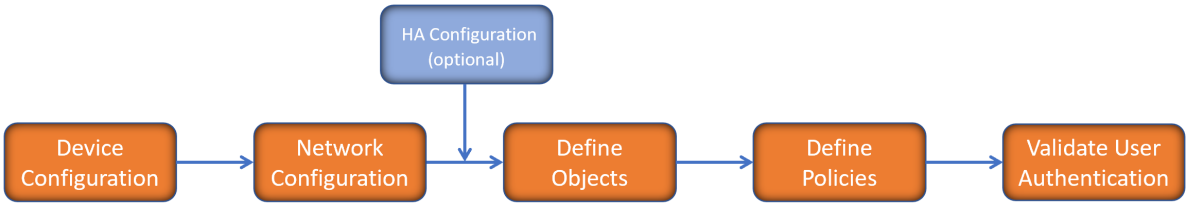


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing product information and solutions. After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The Getting Started Guides for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used use only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the specific Administration Guide for a SonicOS feature for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

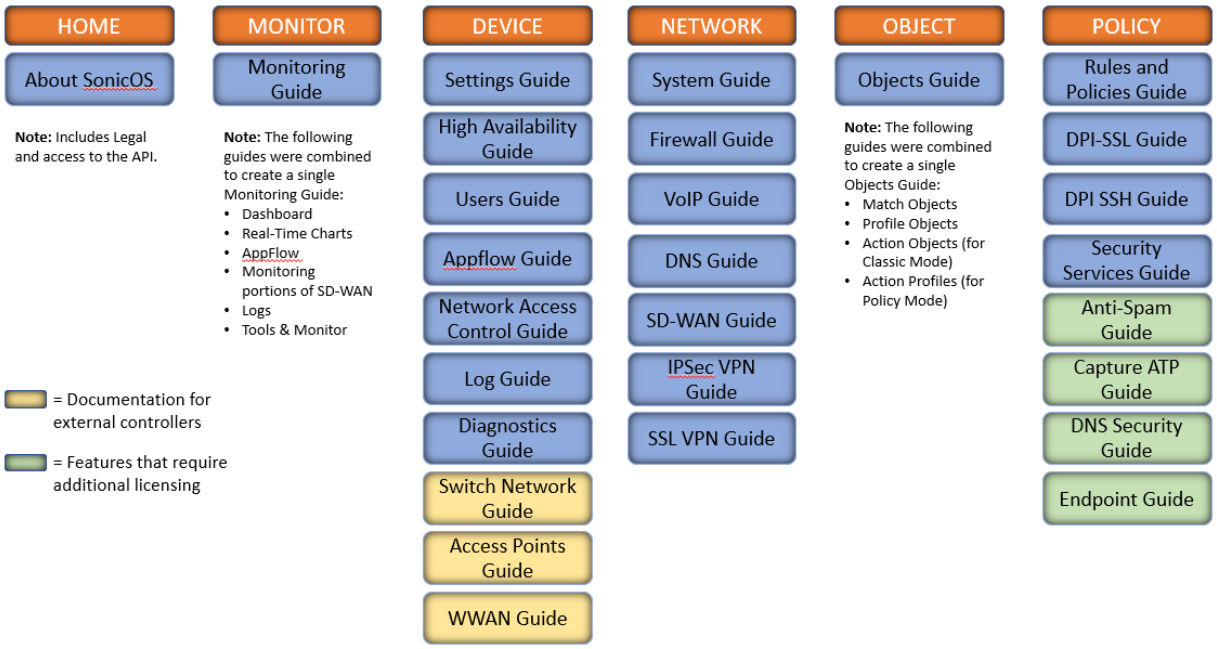


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the SonicOS 7.1 Monitor Guide and the SonicOS 7.1 Objects Guide which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicWall management interface.



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

Guide Conventions

These text conventions are used in this guide:

ⓘ | **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.**

Convention	Description
Bold text	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Function | Menu group > Menu item	Indicates a multiple step menu choice on the user interface. For example, **NETWORK | System > Interfaces** means to select the **NETWORK** functions at the top of the window, then click on **System** in the left navigation menu to open the menu group (if needed) and select **Interfaces** to display the page.
`Code`	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<Variable>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment **serialnumber=***<your serial number>*, replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004.
Italics	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

2

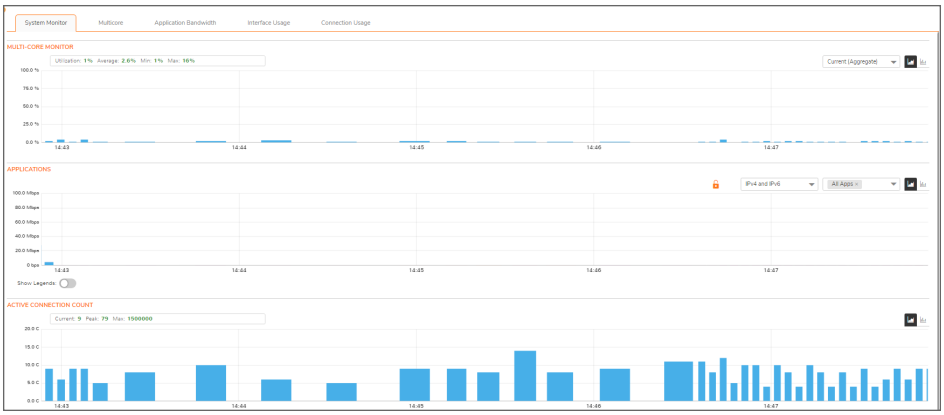
System Monitor

The **Real Time Charts > System Monitor** page provides a real-time, multi-functional display with information about system monitoring, hardware multi-core utilization, application bandwidth usage, interface usage, and connection usage. rate.

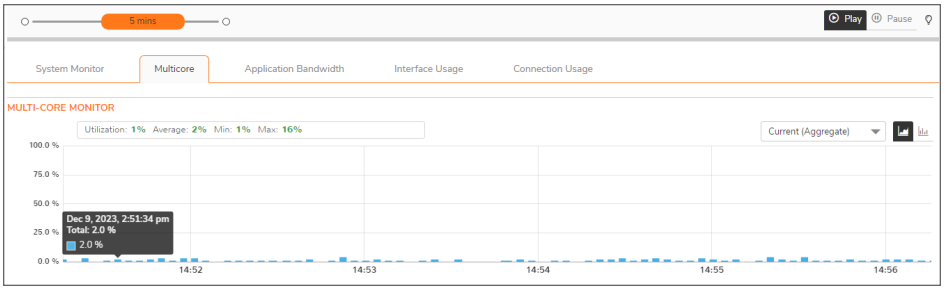
NOTE: A chart may be empty or blank if there are no recent data entries received within the viewing range. Also note that your charts will vary based on what firewalls and feature you implemented.

Five tabs display the options on the **System Monitor** page.

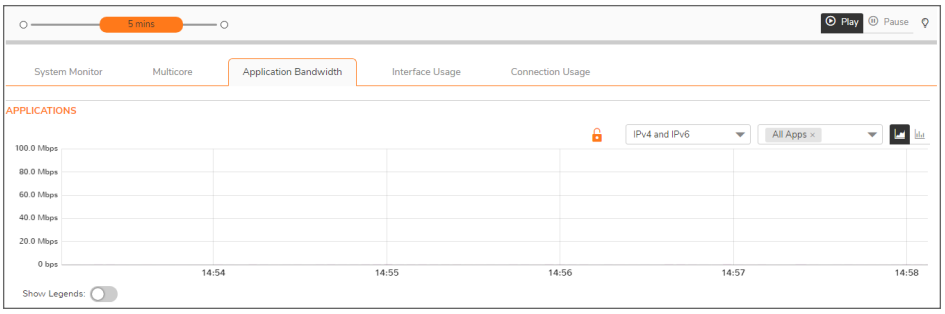
System Monitor



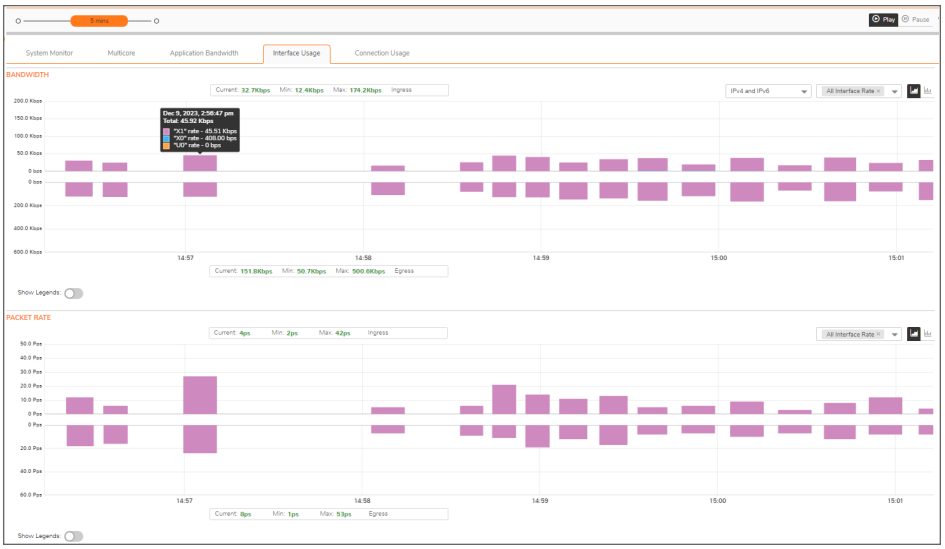
Multicore



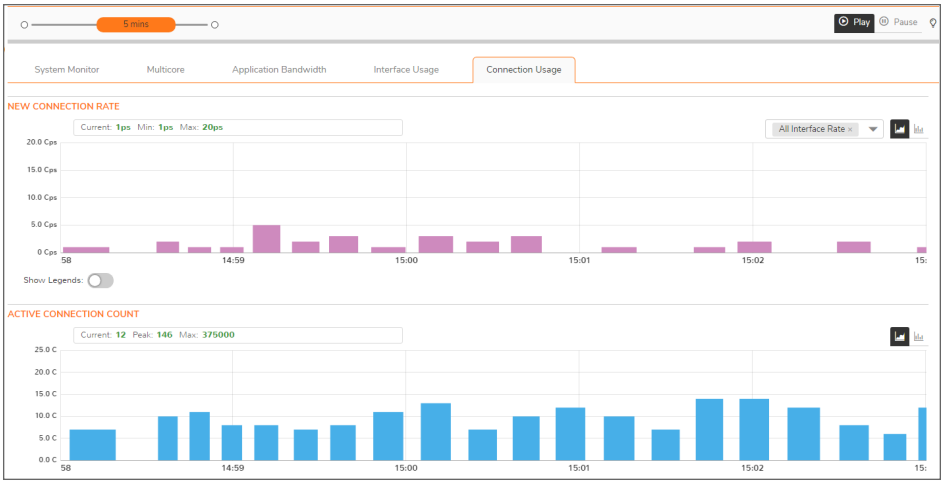
Application Bandwidth



Interface Usage

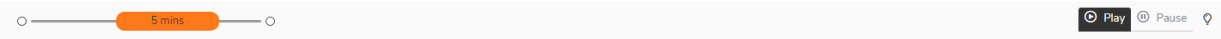


Connection Usage



Using the Toolbar

The **Policy Monitor** toolbar contains features to specify the refresh rate and pause or play the data flow. Changes made to the toolbar apply across all the data flows.



PROTOCOL MONITOR TOOLBAR OPTIONS

Option	Widget	Description
View Range		Displays data pertaining to a specific span of time. The **View Range** is configurable in 60 seconds, 2 minutes, 5 minutes, and 10 minutes. The default is **2** minutes.
Pause		Freezes the data flow. The **Pause** button appears black if the data flow has been frozen.
Play		Unfreezes the data flow. The time entries at the bottom of the tables will refresh as soon as the data flow is updated. The **Play** button appears black if the data flow is live.
Tips		Mouse over a data point to see values at that instant.

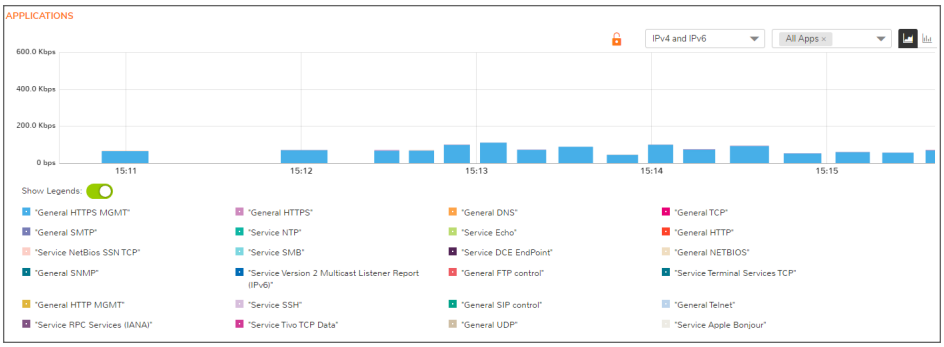
Common Features

Topics:

- Legends
- Tooltips
- Changing Chart Format
- Selecting IPv6/IPv4
- Current, Minimum, Maximum Display

Legends

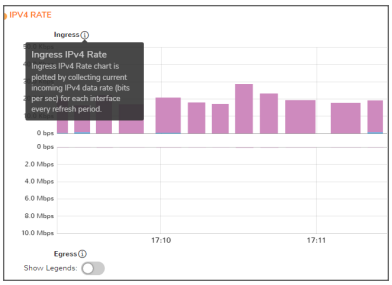
Some charts have the option to display a legend that shows the name and color used for the applications. Simply enable or disable the switch to **Show Legends**.



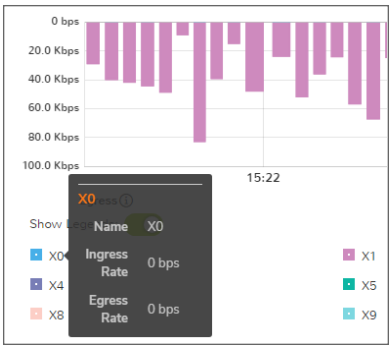
Tooltips

Various elements of the charts have associated tool-tips:

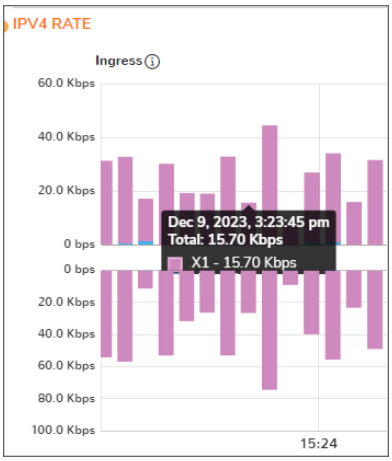
- The name of most charts hve two tool-tip icons that briefly describe the ingress and egress information in the chart.



- Legend items display information about the item the legend represents.



- Hover over a bar on the chart to see more details on that instance.



To display a tool-tip, hover your mouse over the desired item or click on the chart. The information displayed varies by chart.

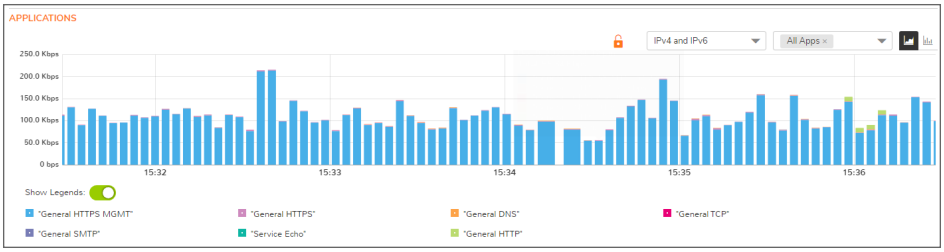
Changing Chart Format

You are able to view individual charts in either stacked bar chart format or single bar chart format. Each chart has Chart Format icons in the upper right corner of the chart  . The default is stack chart format.

Bar Chart

The bar chart format displays applications individually, thus allowing you to compare applications. In this chart, the applications, interfaces, or core monitors are arranged along the x-axis, for applications and interfaces according to the color code shown in the Legend. The y-axis displays information appropriate to the chart, such as the amount of traffic for each application or interface. To display the data in bar chart format, click on the **Stacked Bar** icon.

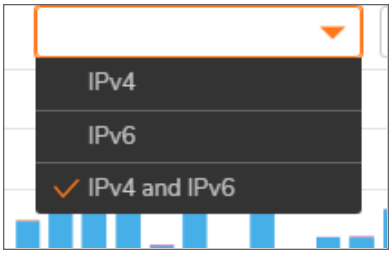
The following example is a Bar Chart view.



Selecting IPv6/IPv4

For complete information on the SonicOS implementation of IPv6, see the chapter on *Configuring Interfaces for Pv6* in the SonicOS 7.1 System Administration Guide.

Real-Time Charts can be configured to see IPv4, IPv6 and both. Make the selection from the drop-down menu on the charts where this is an option.



Current, Minimum, Maximum Display

All charts, except **Applications**, display the current, minimum, and maximum values for the chart. The values vary by chart and can be in Mbps, Kbps, Pps (packets per second), Bytes, or Cps (connections per second).

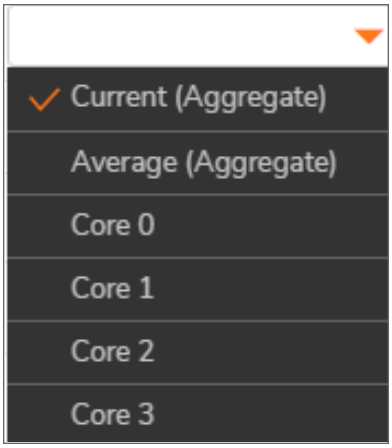
For the **Ingress/Egress** charts, the information is displayed for both halves, the Ingress on the top and the Egress on the bottom. For the other charts, the information is displayed on the top.

Multicore Monitor

The **Multicore Monitor** displays dynamically updated statistics on utilization of the individual cores of the firewall. The information is shown either for combined data in stacked bar chart format or for individual cores in bar chart format. Core 1 through core 8 handle the control plane. The remaining cores handle the data plane. To maximize processor flexibility, functions are not dedicated to specific cores; instead all cores can process all data plane tasks. Memory is shared across all cores. Each core can process a separate flow simultaneously, allowing for up to 88 flows to be processed in parallel.

Options

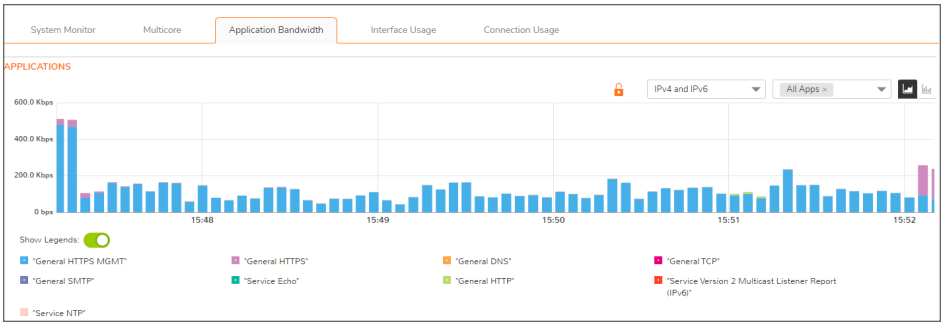
The following option is specific to the **Multicore** chart. For other options and display features, see Common Features.

Option	Widget	Description
Aggregate Display		Specifies which Cores are displayed in the Multi-Core Monitor Flow Chart. A drop-down menu allows you to specify **Current (Aggregate)**, **Average (Aggregate)**, and individual Cores. The individual Cores vary, depending on the number of Cores available. Multiple Cores can be selected.

Applications Bandwidth

The Applications data flow provides a visual representation of the current applications accessing the network.

Bar Chart



Options

The following option is specific to the **Applications** chart. For other options and display features, see Common Features.

Option	Widget	Description
Lock		Locks the Display for the Applications chart. The lock/unlock option is available when you select **Most Frequent Apps**. Most Frequent Apps displays the top 25 apps; you can use the lock or unlock option to keep the report from altering the top 25 apps.
Unlock		Unlocks the Display for the Applications chart.

Interface Usage

The **Interface Usage** charts provide a visual representation of **Bandwidth**, **Packet Rate**, and **Packet Size**. The current value, plus the minimum and maximum amounts is available in the display. The ingress values are at the top of the chart and the egress is at the bottom of the chart.

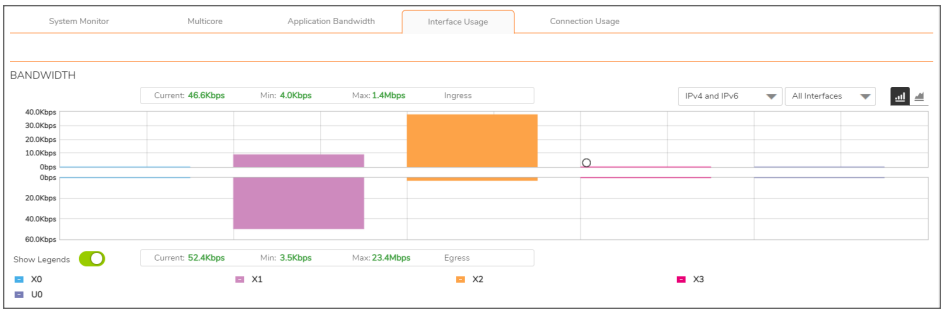
ⓘ | **NOTE:** The Bandwidth charts have no direct correlation to the Application charts.

Stacked Bar Chart

The stacked chart format allows you to view all of traffic as it occurs. The x-axis displays the current time, and the y-axis displays the .

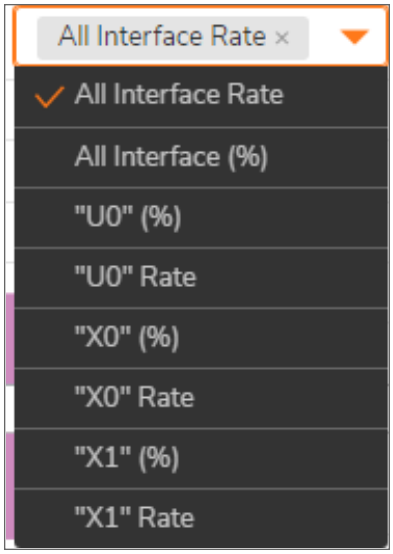
Bar Chart

The bar chart format displays data pertaining to individual interfaces in a bar chart; allowing comparisons of individual interfaces. In this chart, the x-axis denotes the interfaces whereas the y-axis denotes the traffic.



Options

The following option is specific to the **Interface Usage** chart. For other options and display features, see Common Features.

Option	Widget	Description
Interface Rate Display		Specifies which Interfaces are displayed in the Bandwidth Flow Chart. A drop-down menu provides options to specify **All Interfaces Rate**, **All Interfaces (%)**, or rate or percentage (%) for individual interfaces. The individual interfaces vary depending on the number of interfaces on the network. Multiple interfaces can be selected if desired.

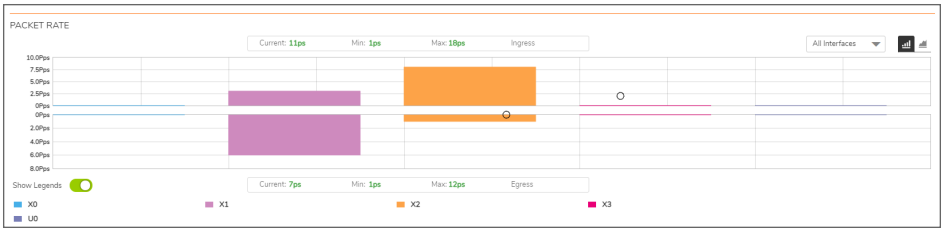
Packet Rate Monitor

The **Packet Rate** monitor provides information on the ingress and egress packet rate as packets per second (pps). This can be configured to show packet rate by network interface. The chart shows the current packet rate, minimum packet rate, and maximum packet rate for both ingress and egress network traffic.

Stacked Bar Chart


PACKET RATE
Current: 16ps Min: 1ps Max: 45ps Ingress
All Interface Rate
50.0 Pps
40.0 Pps
30.0 Pps
20.0 Pps
10.0 Pps
0 Pps
0 Pps
20.0 Pps
40.0 Pps
60.0 Pps
16:06
16:07
16:08
16:09
16:10
Current: 18ps Min: 2ps Max: 54ps Egress
Show Legends:

Bar Chart

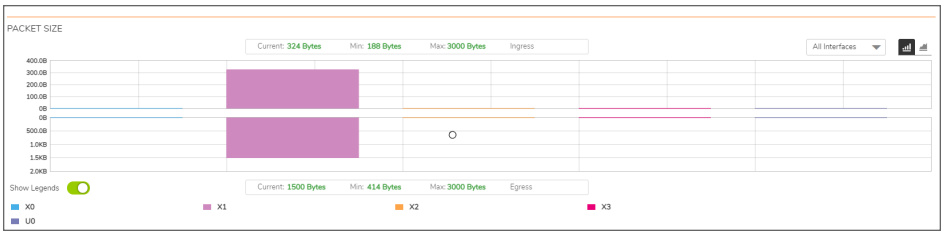


Packet Size

The **Packet Size** report provides information on the ingress and egress packet size in bytes (B). This can be configured to show packet size by network interface. The chart shows the current packet size, minimum packet size, and maximum packet size for both ingress and egress network traffic.

Stacked Chart

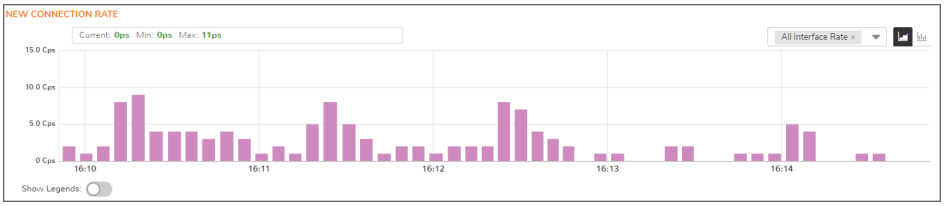
Bar Chart



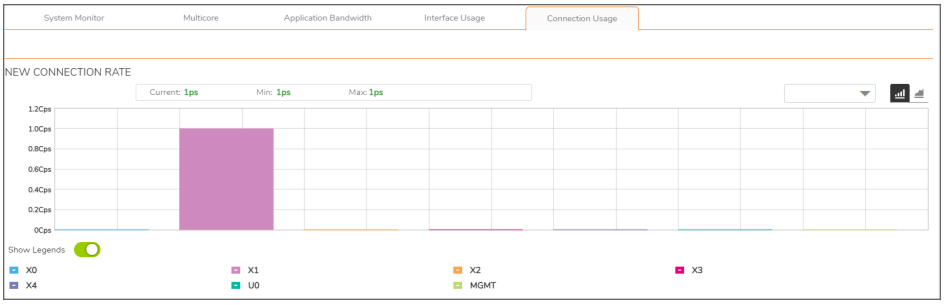
Connection Usage

The **Connection Usage** report is plotted by collecting the outgoing and incoming connection rates for each interface every refresh period. When looking at the combined connection rate of more than one interface at the same time, it may appear double than the actual connection rate. A single connection between a pair of interfaces is counted for both interfaces.

Stacked Bar Chart



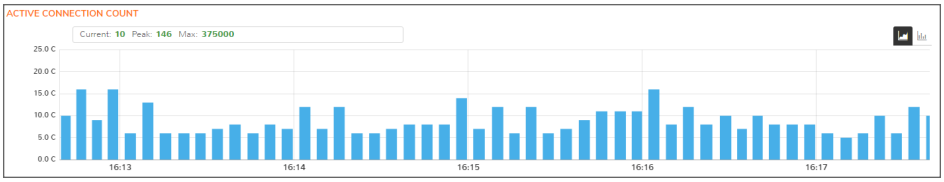
Bar Chart



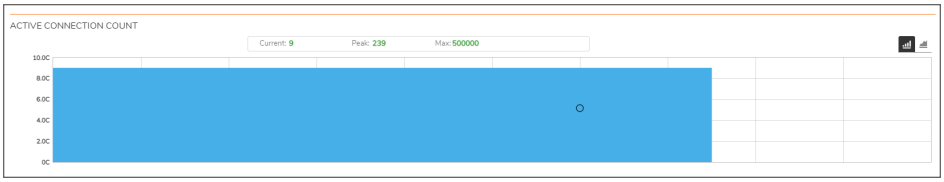
Active Connection Count

The **Active Connection Count** report provides a visual representation of the active total number of connections, peak number of connections, and maximum number of connections. The y-axis displays the total number of connections from 0C (zero connections) to 1KC (one kilo connections).

Stacked Chart



Bar Chart



ⓘ | **NOTE:** The **Connection Count** Monitor does not have legends.

3

Protocol Monitor

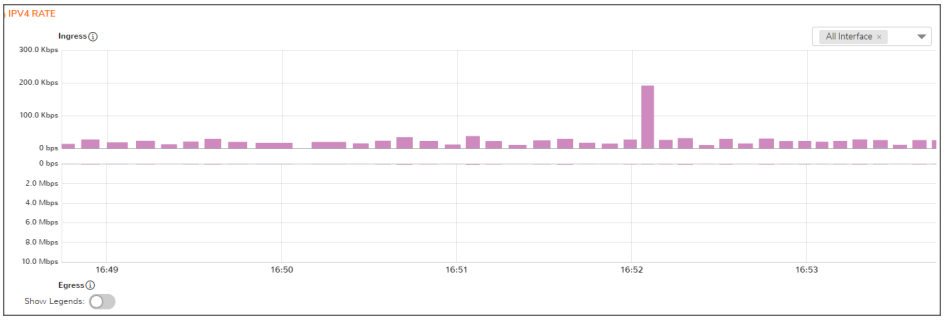
The **Real Time Charts > Protocol Monitor** page displays real-time charts showing ingress and egress traffic rates for the following protocols:

IPv4 Rate	Internet Protocol version 4
ARP Rate	Address Resolution Protocol, used by IPv4 to map IP network addresses to link layer hardware addresses
IPv6 Rate	Internet Protocol version 6
UDP Rate	User Datagram Protocol, a connection-less protocol used for example by DNS, SNMP, RIP, DHCP
TCP Rate	Transmission Control Protocol, a connection oriented protocol allowing bidirectional traffic once the connection is established, used for example by FTP, SSH, Telnet, and also by DNS
ICMP Rate	Internet Control Message Protocol, used by network devices to send error messages and operational information; ping uses ICMP to send echo request packets to a host
IGMP Rate	Internet Group Management Protocol, used by hosts and routers to establish multicast group memberships

The seven real-time charts displayed on the **Protocol Monitor** page are shown in the images below. The **Ingres** rate is displayed on the top half of each chart, and the **Egress** rate is displayed on the bottom.

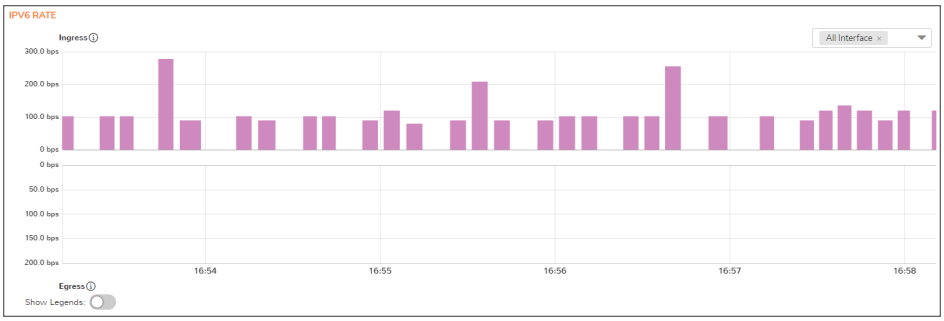
ⓘ | **NOTE:** A chart may be empty or blank if there are no recent data entries received within the viewing range.

PROTOCOL MONITOR - IPV4 CHART

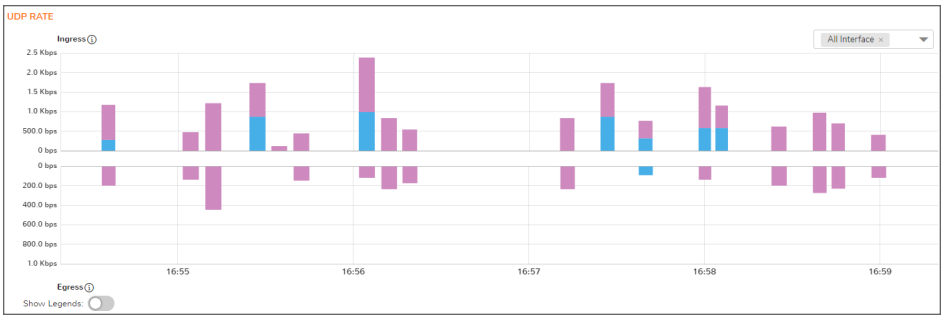


PROTOCOL MONITOR - ARP CHART

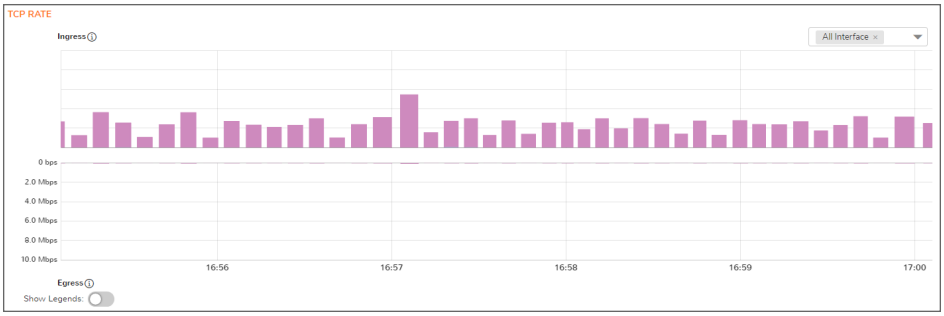
PROTOCOL MONITOR - IPV6 CHART



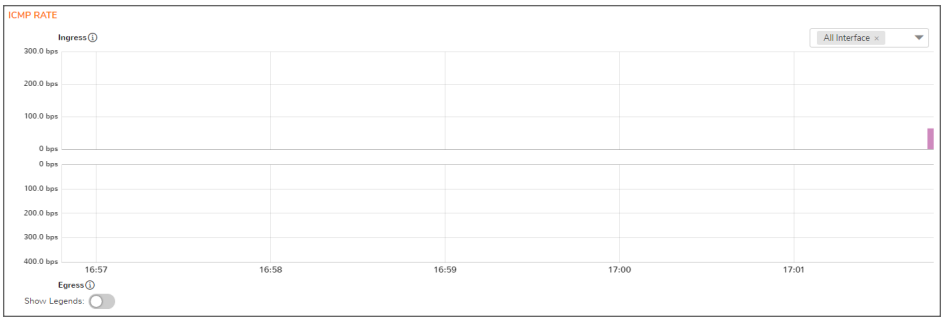
PROTOCOL MONITOR - UDP CHART



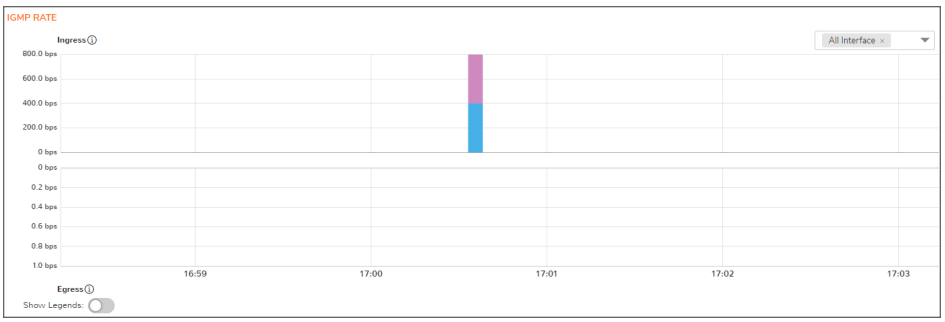
PROTOCOL MONITOR - TCP CHART



PROTOCOL MONITOR - ICMP CHART

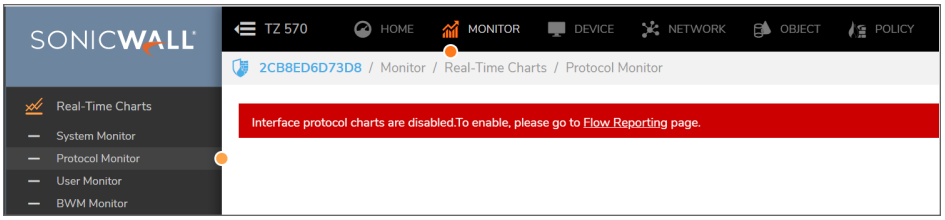


PROTOCOL MONITOR - IGMP CHART



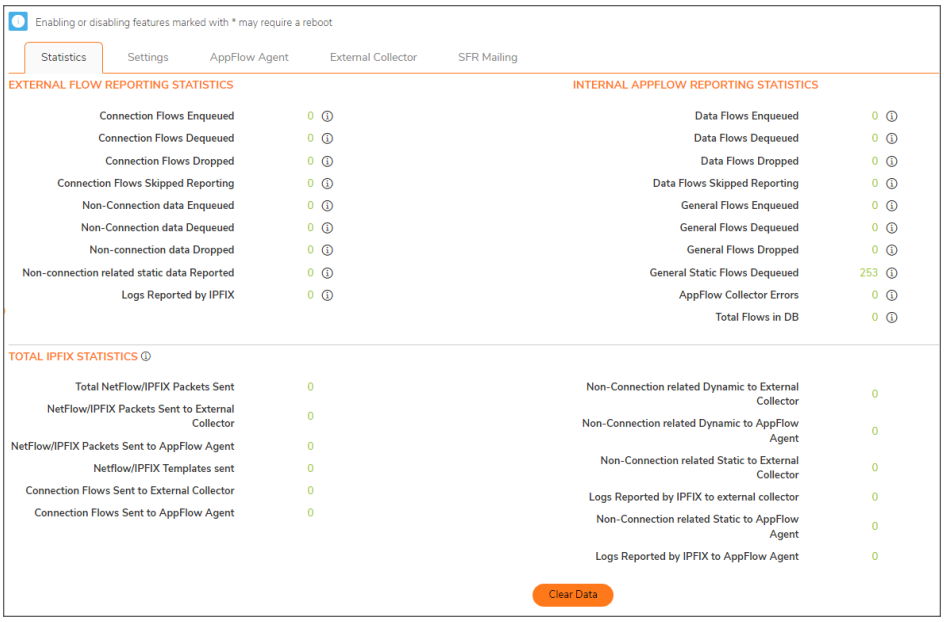
Enabling the Protocol Monitor

The first time you access the Protocol Monitor, it is disabled.



To enable the Protocol Monitor and start displaying statistics in the different charts:

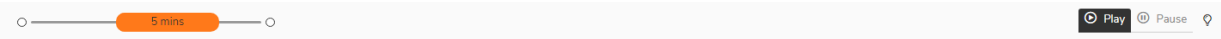
1. Click on the **Flow Reporting** page link.
   You will be navigated to **Device > App Flow > Flow Reporting** page.
2. In the **Settings** tab, select **Interface protocols** option from the **Collect Real-Time Data For** drop-down and click **Accept**.



The settings are enabled, and statistics are displayed in the **Protocol Monitor** page.

Using the Toolbar

The Protocol Monitor toolbar contains features to specify the refresh rate and pause or play the data flow. Changes made to the toolbar apply across all the data flows.



PROTOCOL MONITOR TOOLBAR OPTIONS

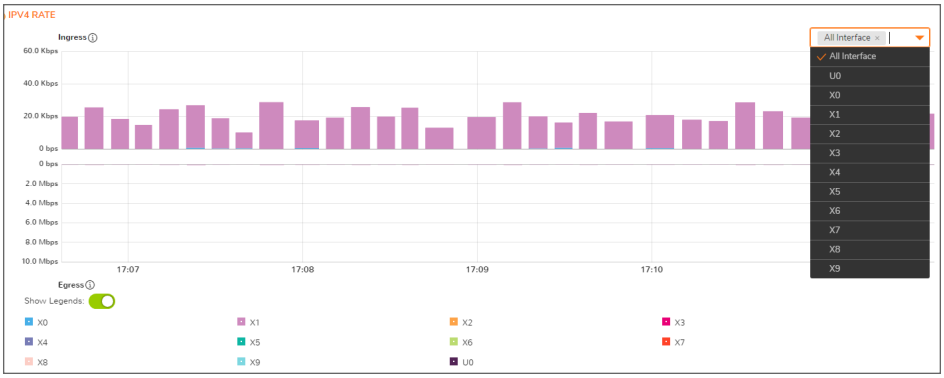
Option	Widget	Description
View Range		Displays data pertaining to a specific span of time. The **View Range** is configurable in 60 seconds, 2 minutes, 5 minutes, and 10 minutes (default).
Pause		Freezes the data flow. The **Pause** button appears black if the data flow has been frozen.
Play		Unfreezes the data flow. The time entries at the bottom of the tables will refresh as soon as the data flow is updated. The **Play** button appears black if the data flow is live.
Tips		Mouse over a data point to see values at that instant.

Using Per-Chart Viewing Options

Topics:

Legends

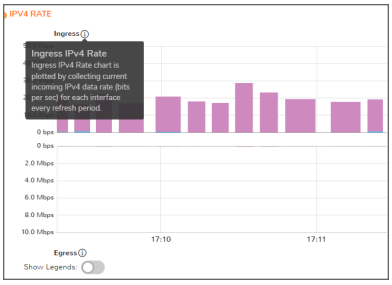
Each chart displays a legend that shows the name and color used for the interfaces selected in the chart's display options drop-down menu. To view the chart, select the interfaces from **All Interfaces** drop-down and toggle the **Show Legend**s option.



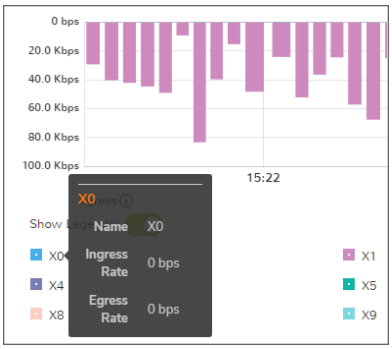
Tooltips

Various elements of the charts have associated tool-tips:

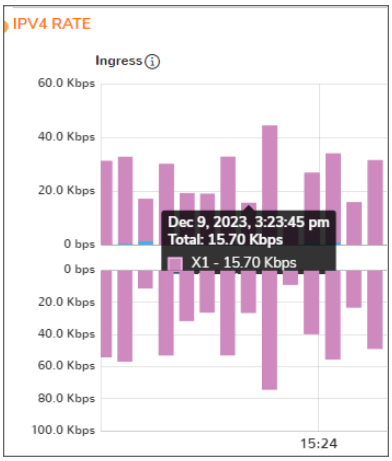
- The name of each chart has two tool-tip icons that briefly describe the ingress and egress information in the chart.



- Legend items display information about the item the legend represents.



- Hover over a bar on the chart to see more details on that instance.



To display a tool-tip, hover your mouse over the desired item or click on the chart. The information displayed varies by chart.

4

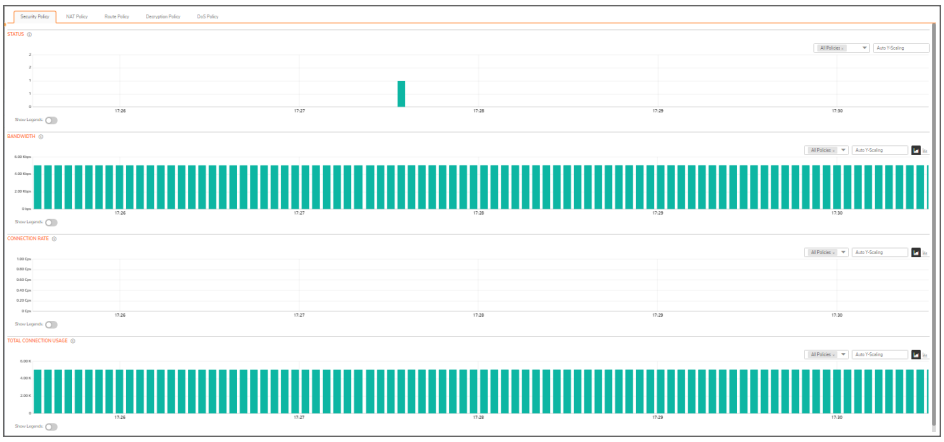
Policy Monitor

The **Real Time Charts > Policy Monitor** page provides a real-time, multi-functional display with information about security, NAT, Route, Decryption, and DoS policies.

ⓘ | **NOTE:** A chart may be empty or blank if there are no recent data entries received within the viewing range.

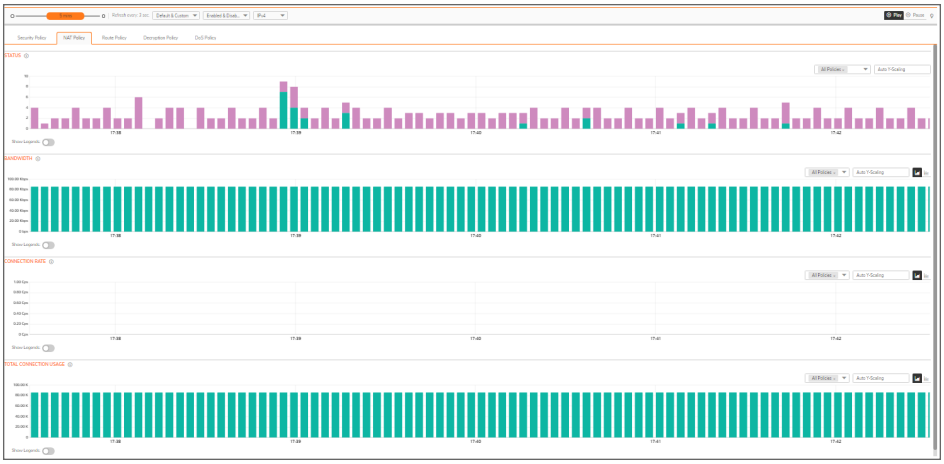
Security Policy

To view the Security Policy chart, you must configure and enable a policy under **Policy > Rules and Policies > Security Policy**.



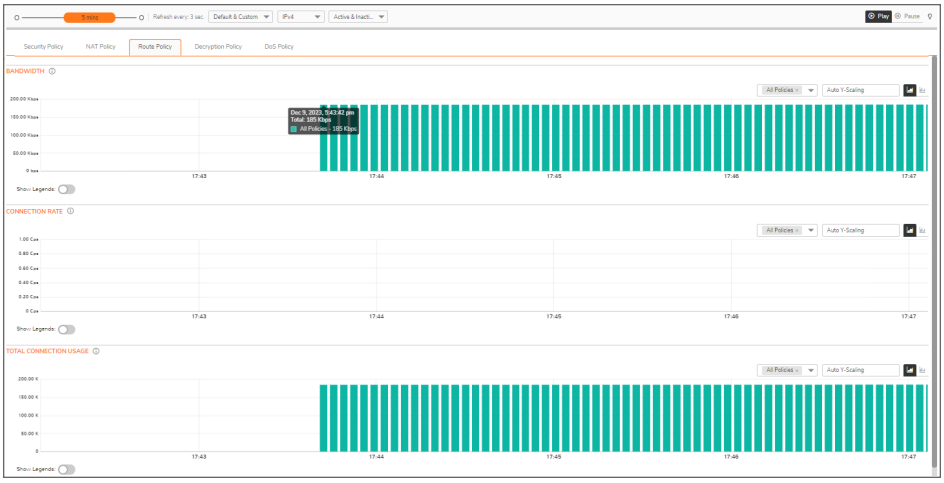
NAT Policy

To view the NAT Policy chart, you must configure and enable a policy under **Policy > Rules and Policies > NAT Policy**.



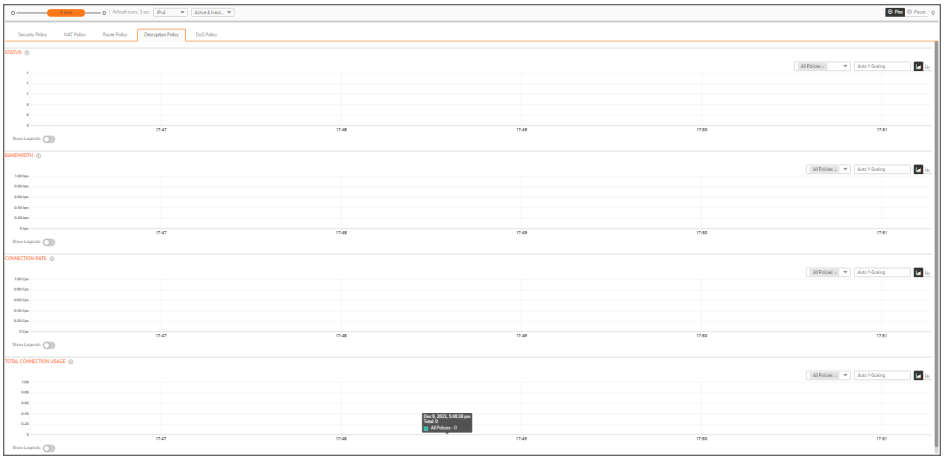
Route Policy

To view the Route Policy chart, you must configure and enable a policy under **Policy > Rules and Policies > Route Policy**.



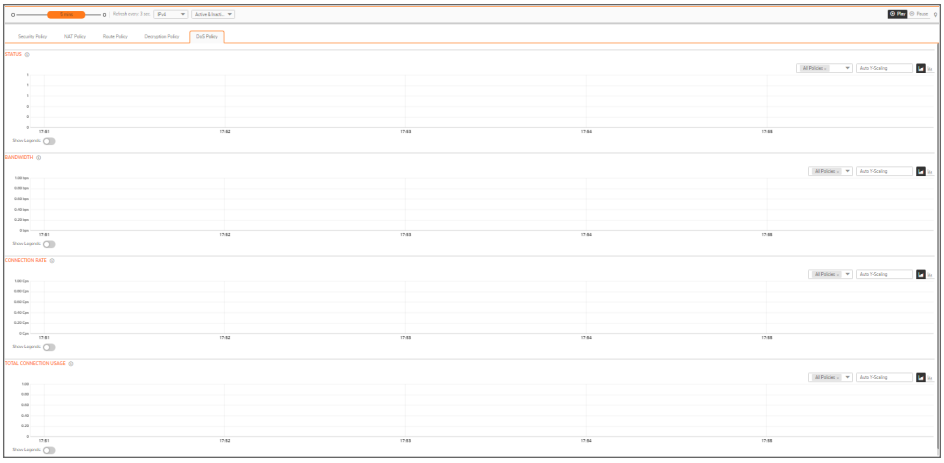
Decryption Policy

To view the Decryption Policy chart, you must configure and enable a policy under **Policy > Rules and Policies > Decryption Policy**.



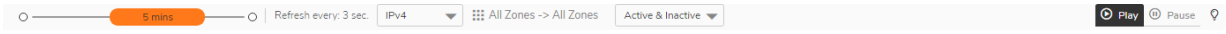
DoS Policy

To view the DoS Policy chart, you must configure and enable a policy under **Policy > Rules and Policies > DoS Policy**.

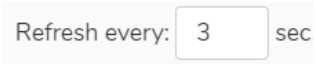


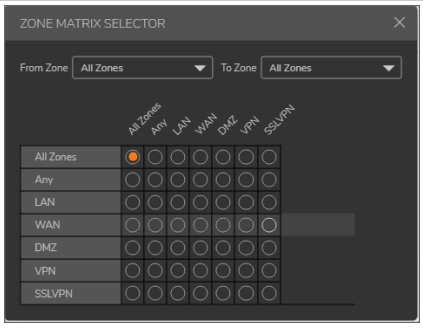
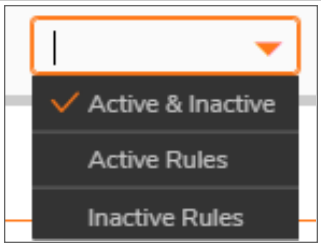
Using the Toolbar

The **Policy Monitor** toolbar contains features to specify the refresh rate, change the amount of data displayed, and pause or play the data flow. Changes made to the toolbar apply across all the data flows.



PROTOCOL MONITOR TOOLBAR OPTIONS

Option	Widget	Description
View Range		Displays data pertaining to a specific span of time. The **View Range** is configurable in 60 seconds, 2 minutes, 5 minutes, and 10 minutes. The default is **2** minutes.
Refresh Rate		Determines the frequency at which data is refreshed. A numerical integer between 1 to 10 seconds is required. The default is **3** seconds.
IPv4/IPv6		Select either **IPv4**, **IPv6** or **Both** to include in the monitoring.

Zones		Select which zone to include in the policy monitoring. You can select from the drop-down menus or you can chose option in the matrix.
Active & Inactive		Select whether to monitor active or inactive policies or both.
Pause		Freezes the data flow. The **Pause** button appears black if the data flow has been frozen.
Play		Unfreezes the data flow. The time entries at the bottom of the tables will refresh as soon as the data flow is updated. The **Play** button appears black if the data flow is live.
Tips		Mouse over a data point to see values at that instant.

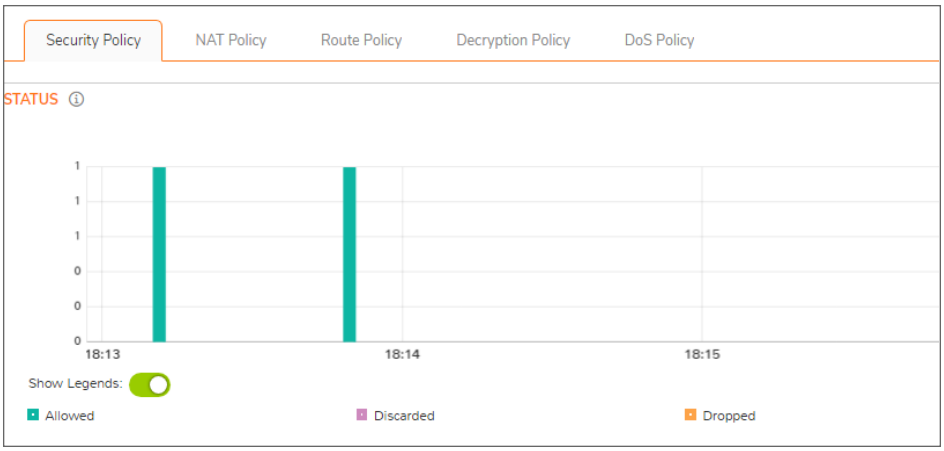
Common Features

Topics:

- Legends
- Tooltips
- Changing Chart Format
- Scaling a Chart

Legends

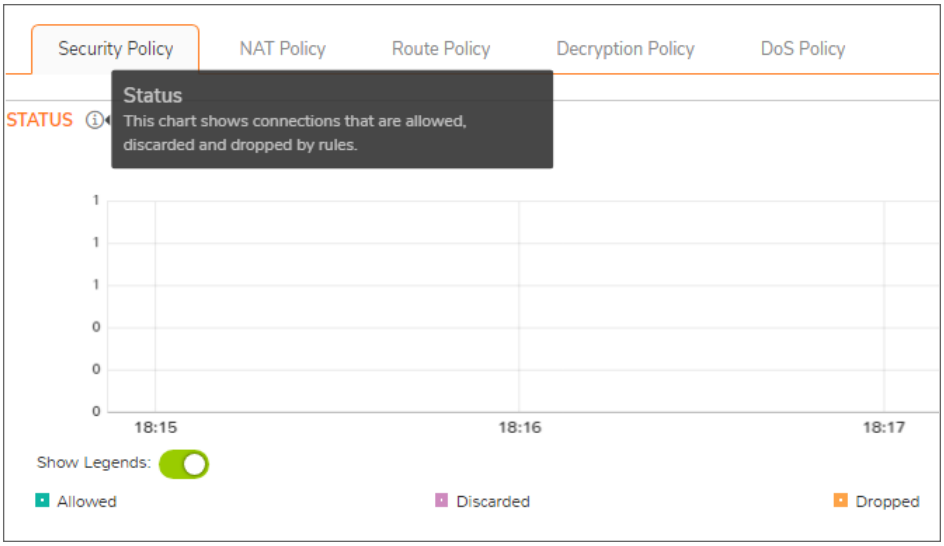
Most charts display a legend that shows the name and color used for the policies.



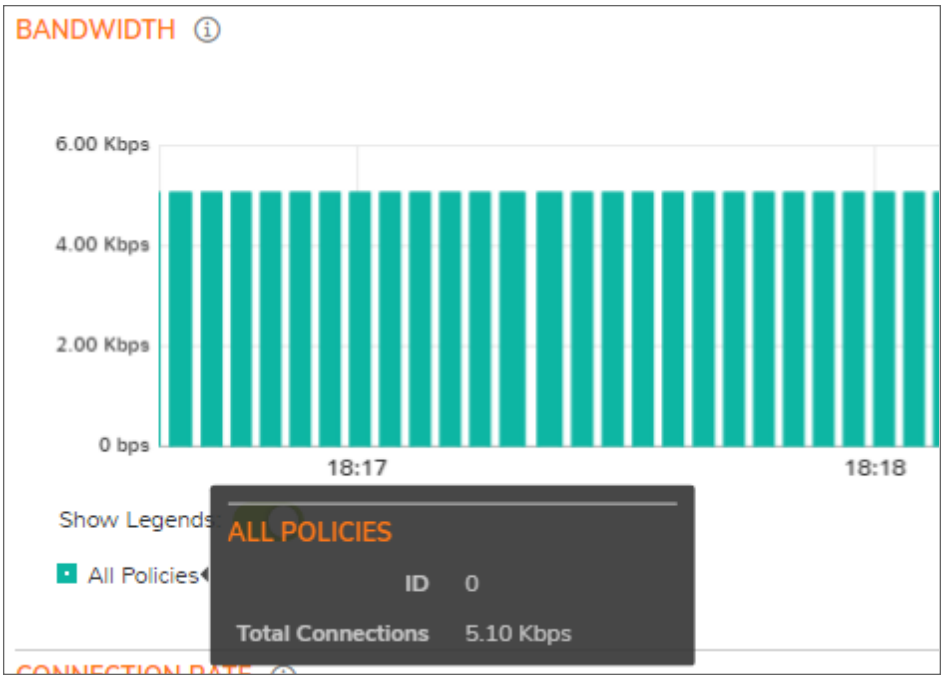
Tooltips

Various elements of the charts have associated tool-tips:

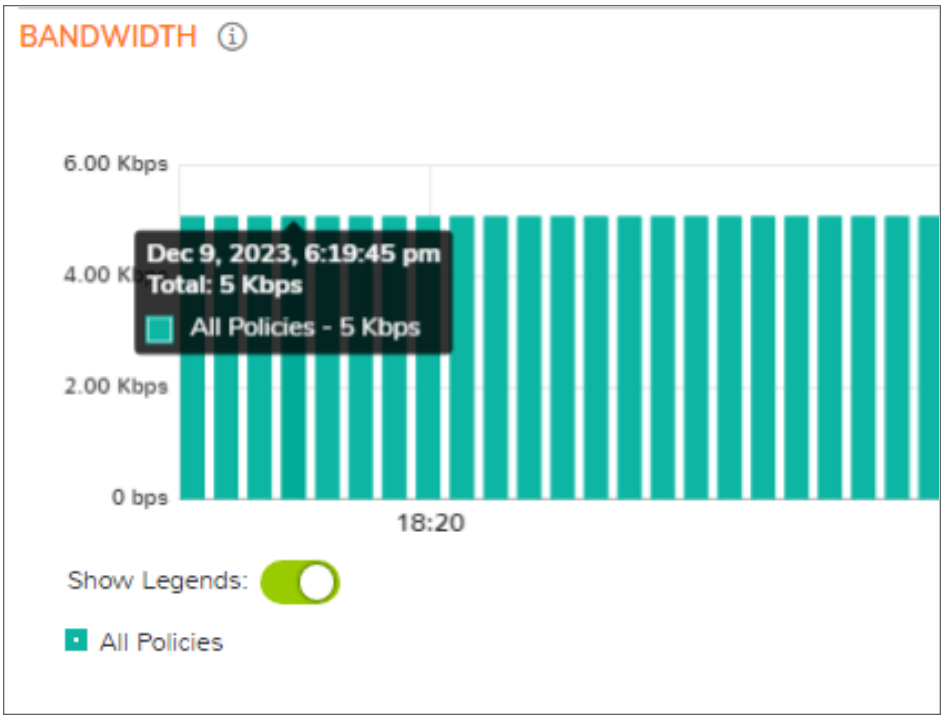
- The name of the chart has a tool-tip icon that briefly describe the chart.



- Legend items display information about the item the legend represents.



- Hover over a bar on the chart to see more details on that instance.



To display a tool-tip, hover your mouse over the desired item or click on the chart. The information displayed varies by chart.

Changing Chart Format

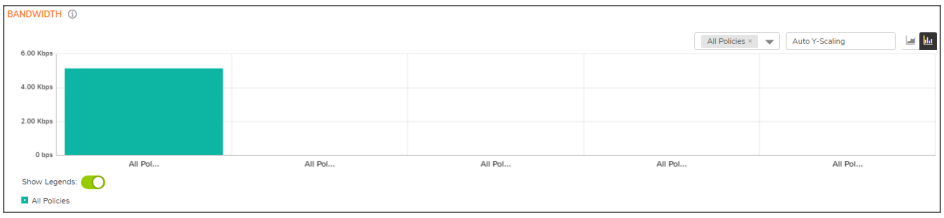
You are able to view individual charts in either stacked bar chart format or regular bar chart format. Each chart has Chart Format icons in the upper right corner of the chart  . The default is stacked bar chart format.

Bar Chart

The bar chart format displays applications individually, thus allowing you to compare policies. In this chart, the policies or rules arranged along the x-axis according to the color code shown in the Legend. The y-axis displays information appropriate to the chart, such as the amount of traffic for each policy.

To display the data in bar chart format, click on the **Bar Chart** icon  .

The following example is a Bar Chart view.



Stacked Bar Chart

The stack chart format displays over-lapping data in a stacked format as it occurs. In this chart, the x-axis displays the current time and the y-axis displays information appropriate to the chart, such as the amount of traffic for each policy. To display data in the stack chart format, click the **Stacked Bar Chart** icon  . The following example is a Stacked BAr Chart view.

Scaling a Chart

The Scale box, , to the upper right of each chart, allows for automatic y-axis scaling or custom scaling of a chart.

- Auto (default) – Auto Y-Scaling, where the y-axis is scaled so it is just large enough to show the maximum data in the chart.
- <num>[<unit>] – The values for customized scaling must be a numeric integer. Specifying a unit is optional. If a unit is desired, four options are available:
    - K for Kilo
    - M for Mega
    - G for Giga
    - % for Percentage

  For example, if a custom scale of 100Kbps is desired, then 100K should be entered: The numeric integer 100 followed by the unit K.

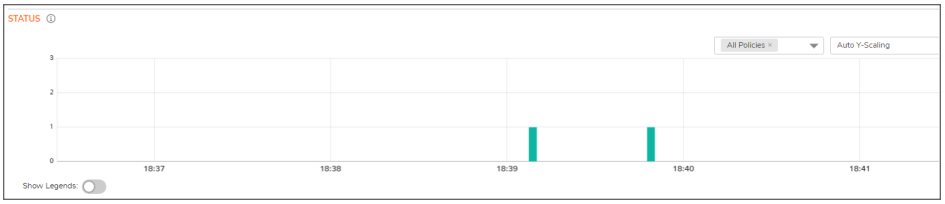
  ⓘ | **NOTE:** An invalid entry results in the default, Auto Y-Scaling, being used.

Security Policy

To view the Security Policy chart, you must configure and enable a policy under **Policy > Rules and Policies > Security Policy**.

Status

The Status chart displays connections that are allowed, discarded, and dropped by the rules configured. The x-axis displays the current time and the y-axis displays the number of policies that are allowed, discarded, and dropped.



Bandwidth

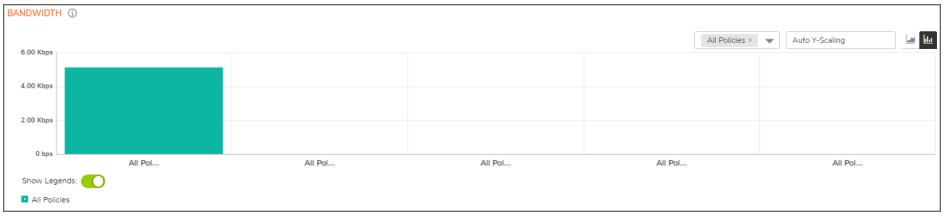
Bandwidth chart is plotted by collecting number of bytes per rule traversing through the firewall every refresh period.

Stacked Bar Chart

In the stacked chart, the x-axis displays the current time and the y-axis displays the amount of traffic for each policy in Kbps or bps (kilobits or bits per second).

Bar Chart

The bar chart format displays policies individually along the x-axis according to the color code shown in the legend. The y-axis displays information appropriate to the chart, such as the amount of traffic for each policy in Kbps or bps (kilobits or bits per second).

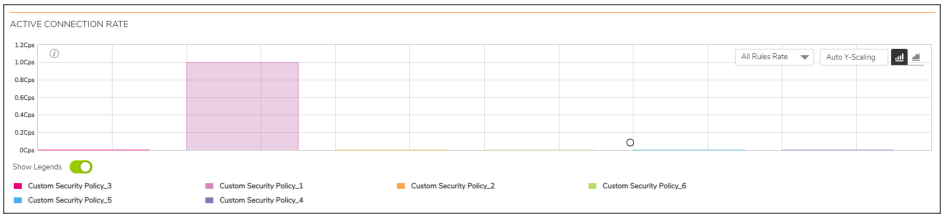


Connection Rate

The Connection Rate chart provides a visual representation of the current total number of outgoing and incoming connection rate for each rule in Cps (Connections per second).

Stacked Bar Chart

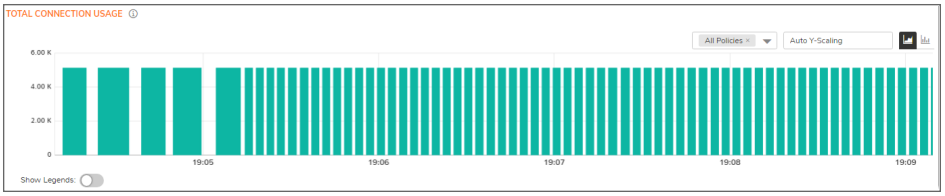
Bar Chart



Total Connection Usage

The Total Connection Usage chart provides a visual representation of the total number of connections per rule.

Stacked Bar Chart



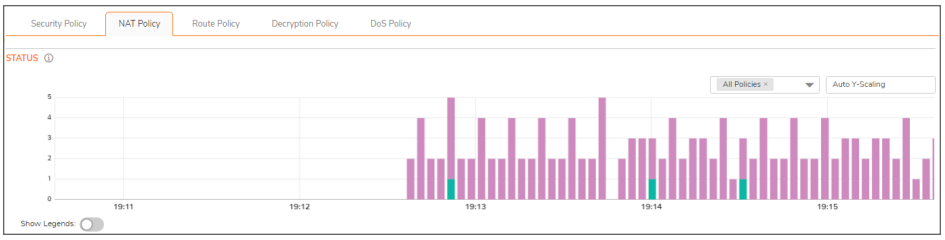
Bar Chart

NAT Policy

To view the NAT Policy chart, you must configure and enable a policy under **Policy > Rules and Policies > NAT Policy**.

Status

The Status chart displays connections that are translated and untranslated by NAT rules. The x-axis displays the current time and the y-axis displays the number of policies that are translated and untranslated by NAT rules.

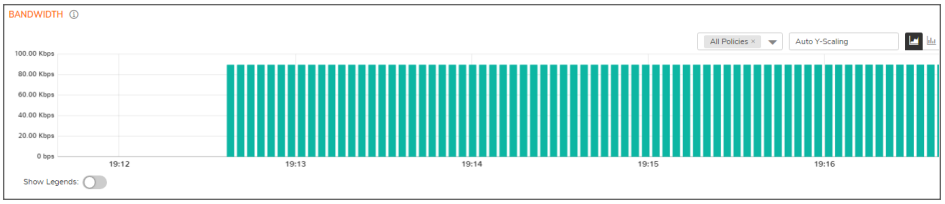


Bandwidth

Bandwidth chart is plotted by collecting number of bytes per rule traversing through the firewall every refresh period.

Stacked Bar Chart

In the stacked chart, the x-axis displays the current time and the y-axis displays the amount of traffic for each policy in Kbps or bps (kilobits or bits per second).



Bar Chart

The bar chart format displays policies individually along the x-axis according to the color code shown in the legend. The y-axis displays information appropriate to the chart, such as the amount of traffic for each policy in Kbps or bps (kilobits or bits per second).

Connection Rate

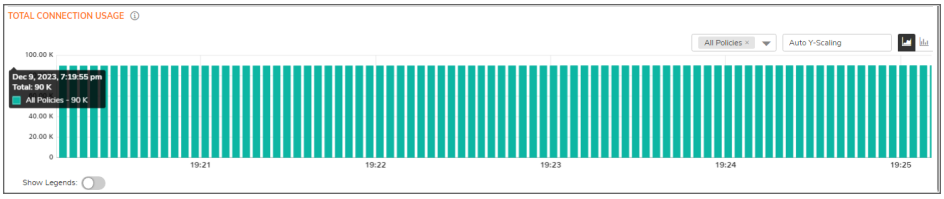
The Connection Rate chart provides a visual representation of the current total number of outgoing and incoming connection rate for each rule in Cps (Connections per second).

Stacked Bar Chart

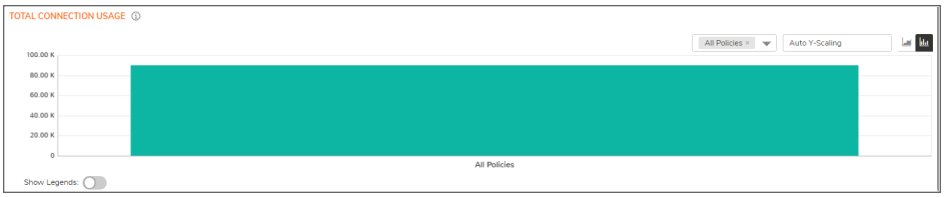
Total Connection Usage

The Connection Usage chart provides a visual representation of the total number of connections per rule.

Stacked Chart



Bar Chart



Route Policy

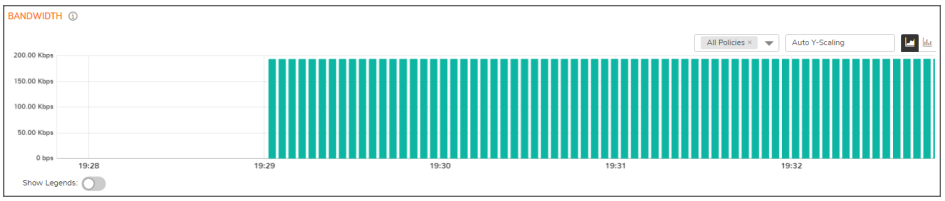
To view the Route Policy chart, you must configure and enable a policy under **Policy > Rules and Policies > Route Policy**.

Bandwidth

Bandwidth chart is plotted by collecting number of bytes per rule traversing through the firewall every refresh period.

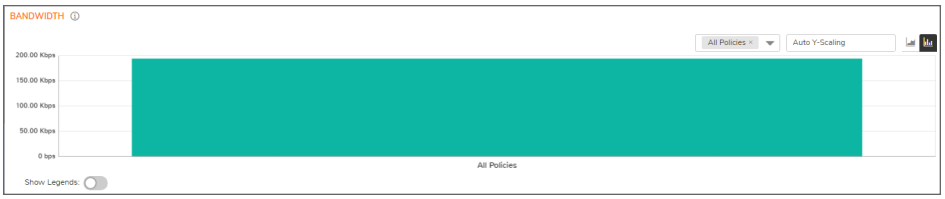
Stacked Bar Chart

In the stacked chart, the x-axis displays the current time and the y-axis displays the amount of traffic for each policy in Kbps or bps (kilobits or bits per second).



Bar Chart

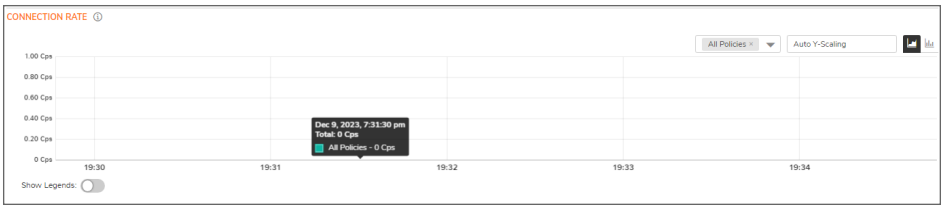
The bar chart format displays policies individually along the x-axis according to the color code shown in the legend. The y-axis displays information appropriate to the chart, such as the amount of traffic for each policy in Kbps or bps (kilobits or bits per second).



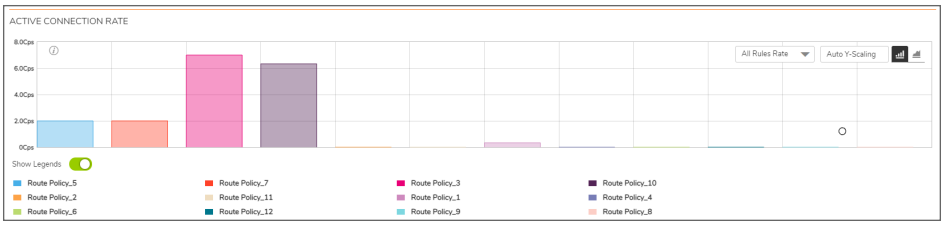
Connection Rate

The Connection Rate chart provides a visual representation of the current total number of outgoing and incoming connection rate for each rule in Cps (Connections per second).

Stacked Bar Chart



Bar Chart

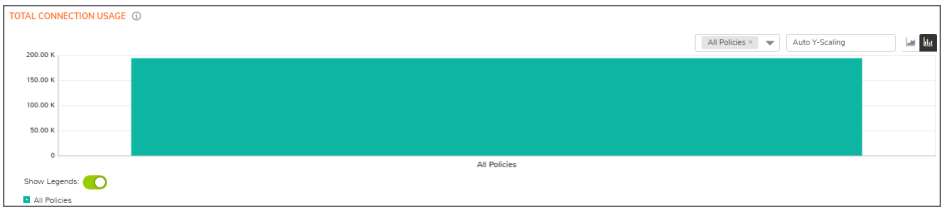


Total Connection Usage

The Connection Usage chart provides a visual representation of the total number of connections per rule.

Stacked Bar Chart

Bar Chart



Decryption Policy

To view the Decryption Policy chart, you must configure and enable a policy under **Policy > Rules and Policies > Decryption Policy**.

Status

The Status chart displays connections that are bypassed and decrypted by decryption rules. The x-axis displays the current time and the y-axis displays the number of policies that are bypassed and decrypted by decryption rules.

Bandwidth

Bandwidth chart is plotted by collecting number of bytes per rule traversing through the firewall every refresh period.

In the stacked bar chart, the x-axis displays the current time and the y-axis displays the amount of traffic for each policy in Kbps or bps (kilobits or bits per second). The regular bar chart format displays policies individually along the x-axis according to the color code shown in the legend. The y-axis displays information appropriate to the chart, such as the amount of traffic for each policy in Kbps or bps (kilobits or bits per second).

Connection Rate

The Active Connection Rate chart provides a visual representation of the current total number of outgoing and incoming connection rate for each rule in Cps (Connections per second).

Total Connection Usage

The Total Connection Usage chart provides a visual representation of the total number of connections per rule.

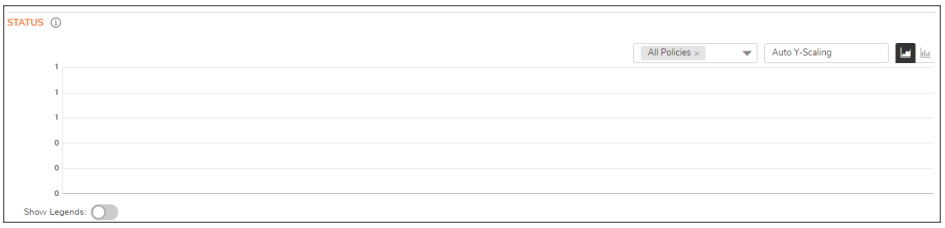
DoS Policy

To view the DoS Policy chart, you must configure and enable a policy under **Policy > Rules and Policies > DoS Policy**.

NOTE: Some of these images show no data, but the chart is provided so you can see the options and values of the axis.

Status

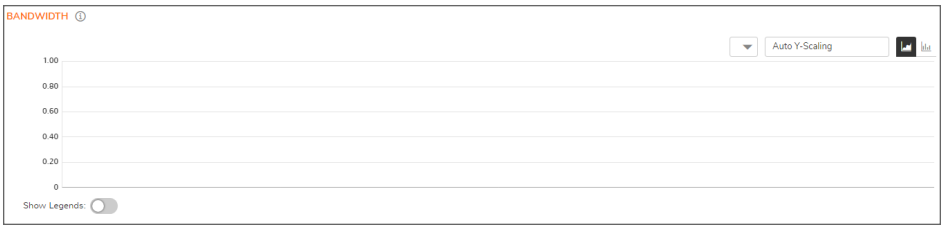
The Status chart displays connections that are protected and bypassed by DoS rules. The x-axis displays the current time and the y-axis displays the number of policies that are protected and bypassed by DoS rules.



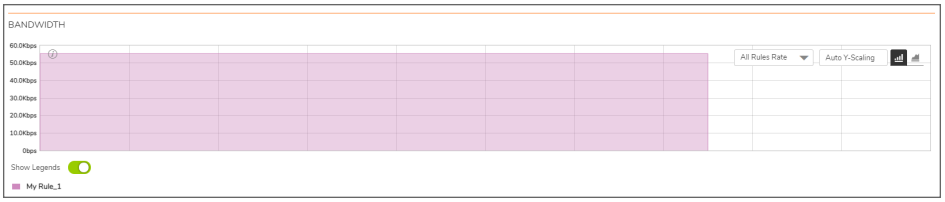
Bandwidth

Bandwidth chart is plotted by collecting number of bytes per rule traversing through the firewall every refresh period. In the stacked bar chart, the x-axis displays the current time and the y-axis displays the amount of traffic for each policy in Kbps or bps (kilobits or bits per second). The regular bar chart format displays policies individually along the x-axis according to the color code shown in the legend. The y-axis displays information appropriate to the chart, such as the amount of traffic for each policy in Kbps or bps (kilobits or bits per second).

Stacked Bar Chart

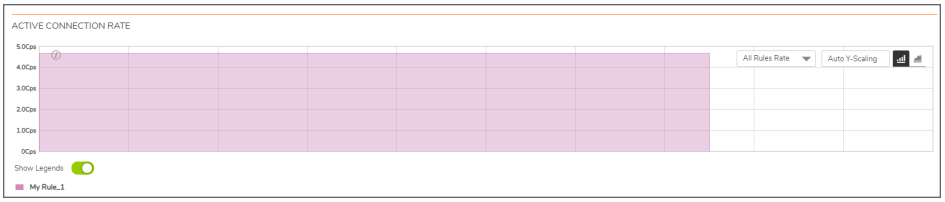


Bar Chart



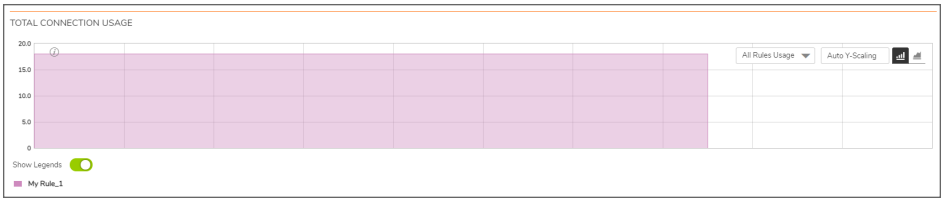
Connection Rate

The Connection Rate chart provides a visual representation of the current total number of outgoing and incoming connection rate for each rule in Cps (Connections per second). The following is an example of a summary bar chart.



Total Connection Usage

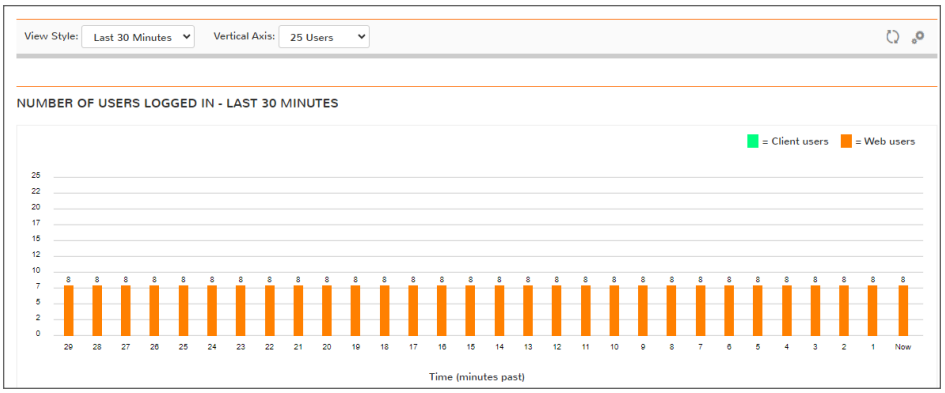
The Connection Usage chart provides a visual representation of the total number of connections per rule. The stacked bar chart stacks all the rules in a single bar differentiated by color. A standard bar chart summarizes all the connections into a single bar. The following shows a regular bar chart.



5

User Monitor

The **Real Time Charts > User Monitor** page provides a quick and easy method to monitor the number of active users on the SonicWall security appliance.



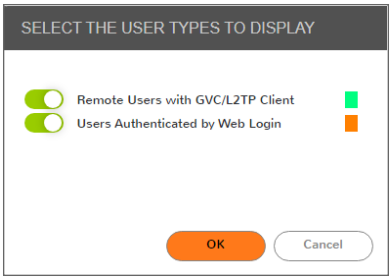
The **User Monitor** page provides these options to customize the display of recent user activity in the User Monitor table:

- **View Style**: Sets the scale of the X-axis, which displays the duration of time. The available options are:
  - Last 30 Minutes
  - Last 24 Hours
  - Last 30 Days
- **Vertical Axis**: Sets the scale of the Y-axis, which displays the number of users. The available options reflect the number of users. For example, two different systems would have different options.

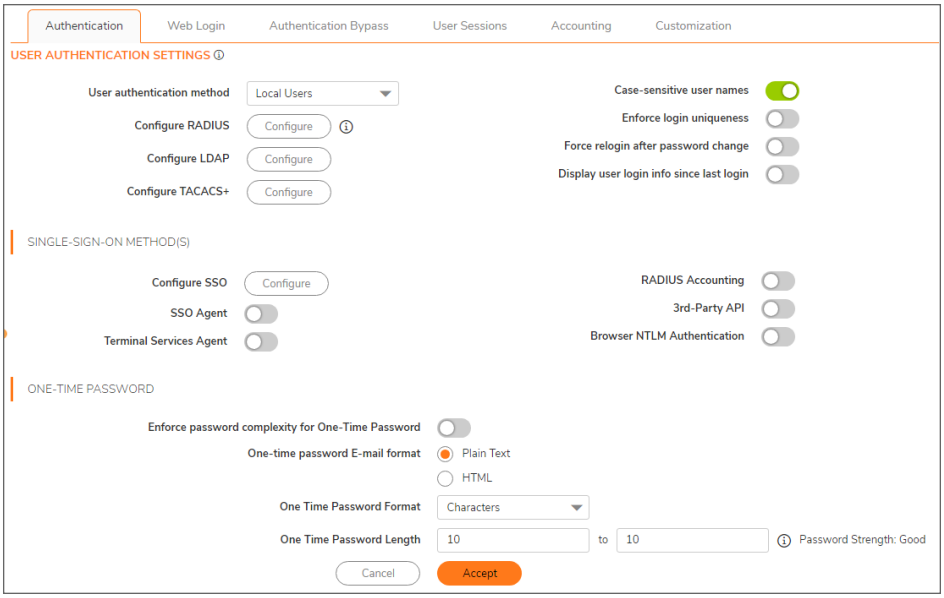
EXAMPLE OF OPTIONS FOR Y-AXIS BASED ON NUMBER OF USERS

Few Users	Many Users
10	800
100	8000
1000	80000

- **Select User Types** icon : Displays a pop-up window, where you can select the types of users to be displayed, indicated by the associated color.



By default, the above two options are displayed. If you wish to display inactive users and users authenticated by Single-Sign-On method, navigate to **Device > Users > Settings** and enable **SSO Agent** option and click **Accept**.



When **SSO Agent** is enabled, the options **Inactive Users** and **Users Authenticated by Single-Sign-on** are displayed, indicated by the associated color.

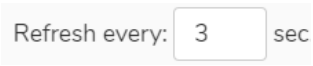
- **Refresh** icon : Refreshes the User Monitor chart.

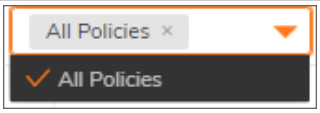
6

Bandwidth Monitor

The **Real Time Charts > BWM Monitor** page displays policy-based bandwidth usage for ingress and egress network traffic, and a second chart with the top 10 for policy-based bandwidth usage.

The Bandwidth Monitor charts are available for All Policies or for selected policies in the drop-down policies list next to the chart. The refresh interval rate is configurable from 3 to 30 seconds. The bandwidth management priority is depicted by guaranteed, maximum, and dropped. The following display settings and configurable controls are available on this page:

Option	Widget	Description
View Range		Displays data pertaining to a specific span of time. The **View Range** is configurable in 60 seconds, 2 minutes, 5 minutes, and 10 minutes (default).
Refresh every		Determines the frequency at which data is refreshed. A numerical integer between 1 to 10 seconds is required. The default is **3** seconds.
Play		Unfreezes the data flow. The time and date will refresh as soon as the data flow is updated. The **Play** button appears black if the data flow is live.
Pause		Freezes the data flow. The time and date will also freeze. The **Pause** button appears black if the data flow has been frozen.

Stacked Chart		Click the **Stacked Bar Chart** icon to display the chart in flow (area) chart format. The x-axis displays the current time and the y-axis displays the amount of ingress and egress traffic in Mbps.
Bar Chart		Click the **Bar Chart** icon to display the chart in bar chart format. The x-axis displays Rules in the Policy-Based Ingress/Egress chart and the names of the top 10 policies for bandwidth usage in the Policy-Based Top 10 chart. The y-axis displays the amount of ingress and egress traffic in Mbps. The Policy-Based Top 10 chart is always displayed as a bar chart with one bar for each policy.
Policies display		Specifies which Policies are displayed in the Policy-Based Ingress/Egress chart. A drop-down menu allows you to specify All Policies or select individual policies. The individual policies vary depending on the configured policies available. Multiple policies can be selected.

Enabling BWM Monitor

For Classic Mode, bandwidth management policies are configured from the **Policy > Rules and Policies > Access Rules** page. To view the BWM chart, edit the access rule for which you want to view the BWM chart and under **Traffic Shaping** tab, select the **Egress BWM**, **Ingress BWM**, and enable **Track Bandwidth Usage** options.

7

SonicWall Support

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

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

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

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

About This Document

SonicOS Real-Time Charts Administration Guide
Updated - December 2023
Software Version - 7.1
232-005652-10 Rev A

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