



Contents

About SonicOS	. 4
Working with SonicOS	. 4
SonicOS Workflow	. 6
How to Use the SonicOS Administration Guides	. 7
Guide Conventions	. 8
System Monitor	. 9
Using the Toolbar	11
Common Features	. 11
Legends	.12
Tooltips	.12
Changing Chart Format	.13
Selecting IPv6/IPv4	
Current, Minimum, Maximum Display	.14
Multicore Monitor	
Options	. 15
Applications Bandwidth	.15
Options	. 16
Interface Usage	.16
Options	
Packet Rate Monitor	
Packet Size	.19
Connection Usage	
Active Connection Count	.20
Protocol Monitor	.21
Enabling the Protocol Monitor	23
Using the Toolbar	24
Using Per-Chart Viewing Options	.25
Legends	
Tooltips	.25
Policy Monitor	27
Using the Toolbar	30
Common Features	
Legends	
Tooltips	

Changing Chart Format	
Scaling a Chart	
Security Policy	
Status	
Bandwidth	
Connection Rate	
Total Connection Usage	
NAT Policy	
Status	
Bandwidth	
Connection Rate	
Total Connection Usage	
Route Policy	
Bandwidth	
Connection Rate	41
Total Connection Usage	
Decryption Policy	
Status	
Bandwidth	
Connection Rate	
Total Connection Usage	43
DoS Policy	
Status	
Bandwidth	
Connection Rate	
Total Connection Usage	
User Monitor	
Bandwidth Monitor	47
Enabling BWM Monitor	
SonicWall Support	
About This Document	

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 Workflow
- How to Use the SonicOS Administration Guides
- Guide Conventions

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.

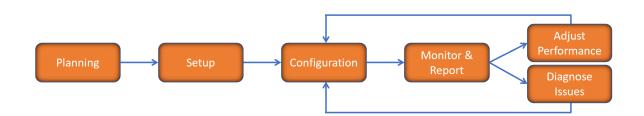
In addition to the management interface, SonicOS also has a full-featured API and a CLI to manage the firewalls. For more information, refer to:

• 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.

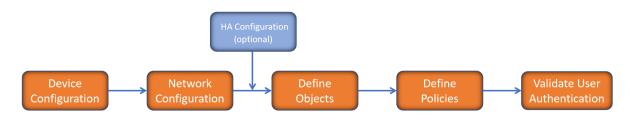


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing product information and solutions. After selecting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

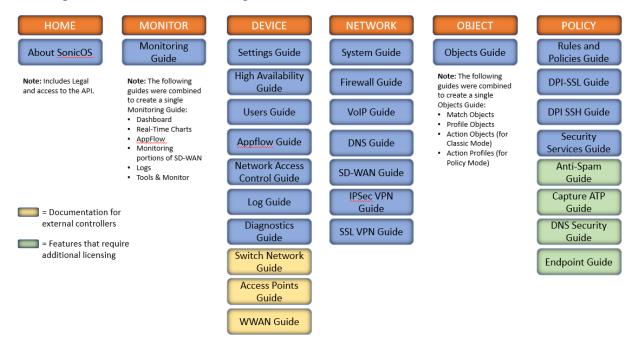


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement 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:

- (i) **NOTE:** A NOTE icon indicates supporting information.
- (i) | 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.
- M 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></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= < <i>your serial number</i> >, 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.

System Monitor

2

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.

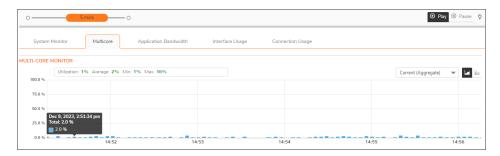
(i) **NOTE:** A chart may be empty or blank if there are no recent data entries received within the viewing range. Also note that your charts will vary based on what firewalls and feature you implemented.

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

System Monitor



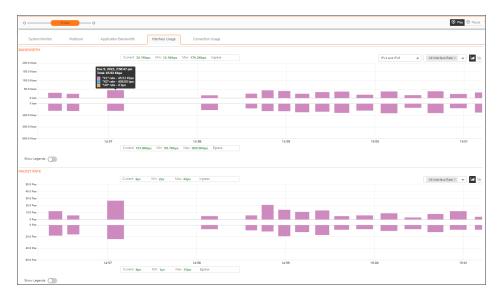
Multicore



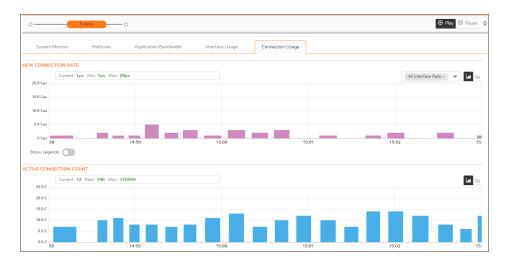
Application Bandwidth

°	5 mins O					⊚	Play Pause
System Monitor	Multicore App	olication Bandwidth	Interface Usage	Connection Usage			
PPLICATIONS							
100.0 Mbps				6	IPv4 and IPv6	▼ All Apps ×	
80.0 Mbps							
60.0 Mbps							
40.0 Mbps							
20.0 Mbps							
0 bps	14:54		14:55	14:56		14:57	14:58

Interface Usage

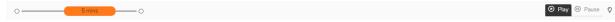


Connection Usage



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	5 mins O 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 Q	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**.

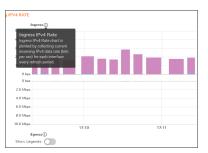
PPLICATIONS					
600.0 Kbps			IPv4 and IPv6	All Apps ×	▼ 🖬
400.0 Kbps					
200.0 Kbps					
0 bps 15:11	15:12	15:13	15:14	15:15	
Show Legends:					
"General HTTPS MGMT"	"General HTTPS"	"General DNS"	General TCP*		
"General SMTP"	"Service NTP"	"Service Echo"	General HTTP		
"Service NetBios SSN TCP"	"Service SMB"	"Service DCE EndPoint"	General NETB	IOS"	
"General SNMP"	 "Service Version 2 Multicast Listener Report (IPv6)" 	General FTP control"	 "Service Termin 	al Services TCP*	
General HTTP MGMT*	Service SSH"	"General SIP control"	"General Telnet		
"Service RPC Services (IANA)"	"Service Tivo TCP Data"	General UDP*	Service Apple	Bonjour"	

Tooltips

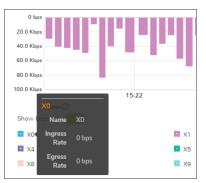
Various elements of the charts have associated tool-tips:

• The name of most charts hve two tool-tip icons (i) information in the chart.

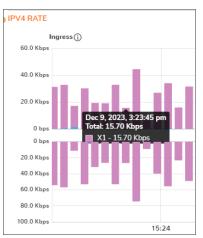
that briefly describe the ingress and egress



• 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.

 APPLICATIONS

 250 0 Maps

 200 0 Maps

 150 0 Maps

 0 bas

 15.32

 15.33

 15.34

 15.35

 15.35

 15.36

 15.37

 15.38

 15.39

 15.30

 15.31

 15.32

 15.33

 15.34

 15.35

 15.35

 15.36

 15.37

 15.38

 15.39

 15.30

 15.30

 15.31

 15.32

 15.32

 15.33

 15.35

 15.36

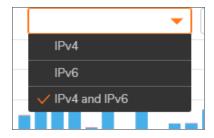
 15.3

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).



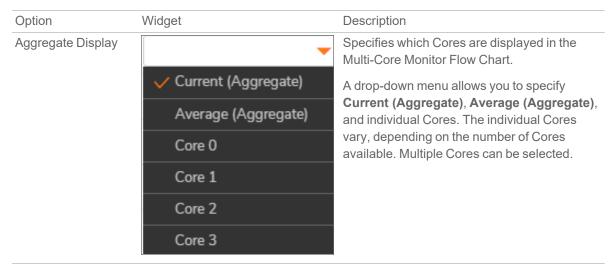
For the **Ingress/Egress** charts, the information is displayed for both halves, the Ingress on the top and the Egress on the bottom. For the other charts, the information is displayed on the top.

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.



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	G	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.

(i) **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.

System Monitor	Multicore	Application	Bandwidth	Interface Usage	Connection Usage			
ANDWIDTH								
	Current: 46.6Kbps	Min: 4.0Kbps	Max: 1.4Mbps	Ingress		IPv4 and IPv6	▼ All Interface	<u>س</u> 🔻
40.0Kbps								
30.0Kbps 20.0Kbps								
10.0Kbps					0			
Obps Obps					0			
20.0Kbps								
40.0Kbps								
60.0Kbps								
ihow Legends	Current: 52.4Kbps	Min: 3.5Kbps	Max: 23.4Mbp	Egress				
x0		X1		🗖 X2		🗖 X3		
 X0 U0 		X1		🗖 X2		X 3		

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	All Interface Rate × 🛛 🔫	Specifies which Interfaces are displayed in the Bandwidth Flow Chart.
	✓ All Interface Rate	A drop-down menu provides options to
	All Interface (%)	specify All Interfaces Rate , All Interfaces (%), or rate or percentage (%) for individual
	"U0" (%)	interfaces.
	"U0" Rate	The individual interfaces vary depending on the number of interfaces on the network.
	"X0" (%)	Multiple interfaces can be selected if desired.
	"X0" Rate	
	"X1" (%)	
	"X1" Rate	

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



Bar Chart

×0	🔳 X1			X2		X3		
how Legends – –		Current: 7ps	Min: 1ps	Max: 12ps	Egress			
8.0Pps								
6.0Pps								
4.0Pps								
2.0Pps								
OPps					0			
0Pps						0		
2.5Pps			_			0		
5.0Pps								
10.0Pps 7.5Pps								
		Current: 11ps	Min: 1ps	Max: 18ps	Ingress		All Inter	faces 🔻 📶
ACKET RATE		Current: 11ps	Min: 1ps	Max: 18ps	Ingress		All Inter	faces 🔻

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



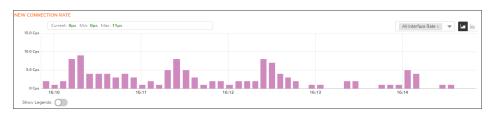
Bar Chart



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



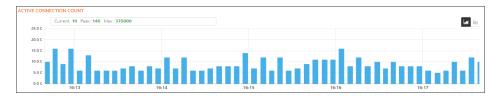
Bar Chart



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



(i) NOTE: The Connection Count Monitor does not have legends.

Protocol Monitor

3

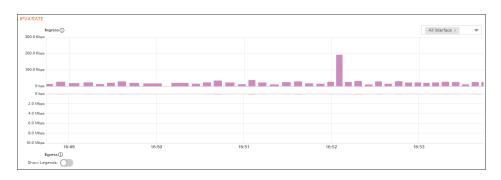
The **Real Time Charts > Protocol Monitor** page displays real-time charts showing ingress and egress traffic rates for the following protocols:

Iayer 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		
Iayer hardware addressesIPv6 RateInternet Protocol version 6UDP RateUser Datagram Protocol, a connection-less protocol used for example by DNS, SNMP, RIP, DHCPTCP RateTransmission Control Protocol, a connection oriented protocol allowing bidirectional traffic once the connection is established, used for example by FTF SSH, Telnet, and also by DNSICMP RateInternet Control Message Protocol, used by network devices to send error messages and operational information; ping uses ICMP to send echo request packets to a hostIGMP RateInternet Group Management Protocol, used by hosts and routers to establish	IPv4 Rate	Internet Protocol version 4
UDP RateUser Datagram Protocol, a connection-less protocol used for example by DNS, SNMP, RIP, DHCPTCP RateTransmission Control Protocol, a connection oriented protocol allowing bidirectional traffic once the connection is established, used for example by FTF SSH, Telnet, and also by DNSICMP RateInternet Control Message Protocol, used by network devices to send error messages and operational information; ping uses ICMP to send echo request packets to a hostIGMP RateInternet Group Management Protocol, used by hosts and routers to establish	ARP Rate	Address Resolution Protocol, used by IPv4 to map IP network addresses to link layer hardware addresses
SNMP, RIP, DHCP TCP Rate Transmission Control Protocol, a connection oriented protocol allowing bidirectional traffic once the connection is established, used for example by FTF 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	IPv6 Rate	Internet Protocol version 6
bidirectional traffic once the connection is established, used for example by FTF SSH, Telnet, and also by DNSICMP RateInternet Control Message Protocol, used by network devices to send error messages and operational information; ping uses ICMP to send echo request packets to a hostIGMP RateInternet Group Management Protocol, used by hosts and routers to establish	UDP Rate	User Datagram Protocol, a connection-less protocol used for example by DNS, SNMP, RIP, DHCP
messages and operational information; ping uses ICMP to send echo request packets to a hostIGMP RateInternet Group Management Protocol, used by hosts and routers to establish	TCP Rate	bidirectional traffic once the connection is established, used for example by FTP,
	ICMP Rate	messages and operational information; ping uses ICMP to send echo request
	IGMP Rate	

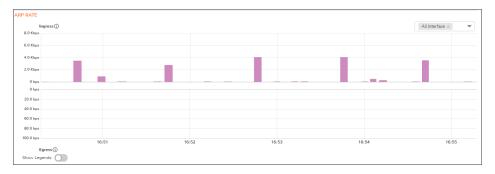
The seven real-time charts displayed on the **Protocol Monitor** page are shown in the images below. The **Ingres** rate is displayed on the top half of each chart, and the **Egress** rate is displayed on the bottom.

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

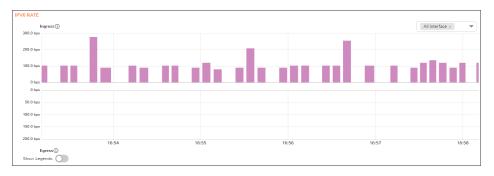
PROTOCOL MONITOR - IPV4 CHART



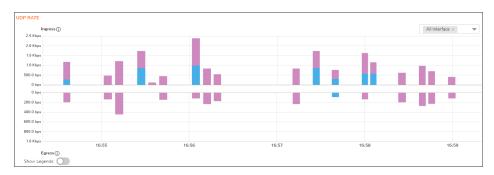
PROTOCOL MONITOR - ARP CHART



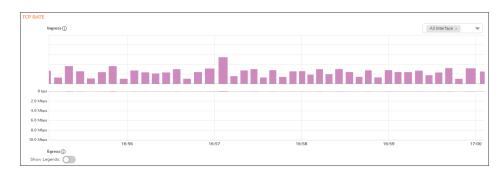
PROTOCOL MONITOR - IPV6 CHART



PROTOCOL MONITOR - UDP CHART



PROTOCOL MONITOR - TCP CHART



PROTOCOL MONITOR - ICMP CHART

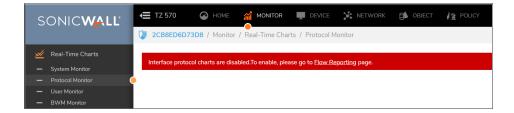
ICMP RATE					
300.0 bps	Ingress				All Interface ×
200.0 bps					
100.0 bps					
0 bps					
0 bps					
100.0 bps					
200.0 bps					
300.0 bps					
400.0 bps	16:57 16	:58 16	:59 17	:00 1	7:01
	Egress ()	100	100	100	
Show Leg	gends:				

PROTOCOL MONITOR - IGMP CHART

GMP RATE					
Ingress (j)					All Interface ×
800.0 bps					
600.0 bps					
400.0 bps					
200.0 bps					
200.0 bps					
0 bps					
0 bps					
0.2 bps					
0.4 bps					
0.6 bps					
0.8 bps					
1.0 bps	16:59	17:00	17:01	17:02	17:03
Egress					
Show Legends:					

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:

- 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**.

Statistics Settings AppFlow	Agent External Collector	SFR Mailing	
TERNAL FLOW REPORTING STATISTICS		INTERNAL APPFLOW REPORTING STATISTICS	
Connection Flows Enqueued	0 (j)	Data Flows Enqueued	0 (j)
Connection Flows Dequeued	0 (j)	Data Flows Dequeued	0 (j)
Connection Flows Dropped	0 (j)	Data Flows Dropped	0 (j)
Connection Flows Skipped Reporting	0 (j)	Data Flows Skipped Reporting	0 (j)
Non-Connection data Enqueued	0 (j)	General Flows Enqueued	0 (j
Non-Connection data Dequeued	0 (j)	General Flows Dequeued	0 (j)
Non-connection data Dropped	0 (j)	General Flows Dropped	0 (j)
Non-connection related static data Reported	0 (j)	General Static Flows Dequeued	253 🛈
Logs Reported by IPFIX	0 (j)	AppFlow Collector Errors	0 (j)
		Total Flows in DB	0 (j)
OTAL IPFIX STATISTICS (1)			
Total NetFlow/IPFIX Packets Sent	0	Non-Connection related Dynamic to External	0
NetFlow/IPFIX Packets Sent to External	0	Collector	
Collector		Non-Connection related Dynamic to AppFlow Agent	0
letFlow/IPFIX Packets Sent to AppFlow Agent	0	Non-Connection related Static to External	
Netflow/IPFIX Templates sent	0	Collector	0
Connection Flows Sent to External Collector	0	Logs Reported by IPFIX to external collector	0
Connection Flows Sent to AppFlow Agent	0	Non-Connection related Static to AppFlow Agent	0
		Logs Reported by IPFIX to AppFlow Agent	0

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 O	5 mins O 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 Q	Mouse over a data point to see values at that instant.

🕑 Play 🕕 Pause 💡

Using Per-Chart Viewing Options

Topics:

- Legends
- Tooltips

Legends

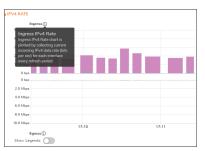
Each chart displays a legend that shows the name and color used for the interfaces selected in the chart's display options drop-down menu. To view the chart, select the interfaces from **All Interfaces** drop-down and toggle the **Show Legends** option.



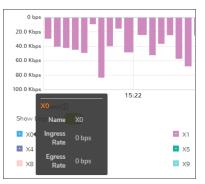
Tooltips

Various elements of the charts have associated tool-tips:

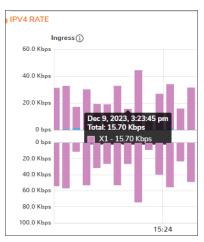
The name of each chart has two tool-tip icons that briefly describe the ingress and egress information in the chart.



• 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.

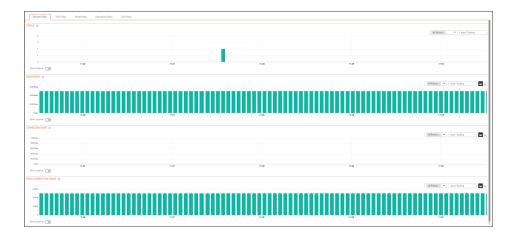
Policy Monitor

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

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

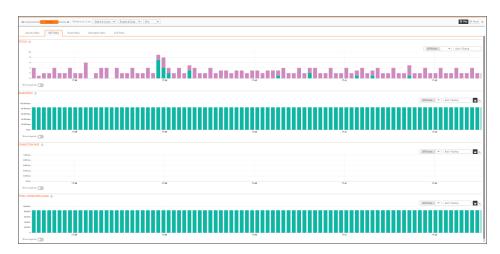
Security Policy

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**.

5 mins O Re	hish every: 3 sec. Default & Custom 💌	Pvi v Active&Inacti. v			O Play 🛞 P
ecurity Policy NAT Policy Route P	nicy Decryption Policy DoS P	sicy			
мотн ()					
				All Policies - 💌 🖌	uto Y-Scaling
Chos					
(has		Dec 9, 2023, 5(43:42 pm Total: 185 K2ps All Policies - 185 K2ps			
(har					
Gan					
2 hpm	17:43	17:44	17.45	17:48	17
v Legends:					
CTION RATE (1)					
Can				All Policies × 🐨 🖌	uto Y-Scaling
1 Car					
) Car					
) C _{2**}					
2 Cpa					
) Cax	17:43	17:44	17)45	17,46	17
v Legenda: 🔘					
CONNECTION USAGE					
				All Policies × 💗 🕹	uto Y-Scaling
00 X					
00 K					
00 K					
00 K					
	17:43	17.44	17.45	17:46	
					17:

Decryption Policy

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

	p Ritchney, Jac. Put V Anieškani, V				S Rev S
Security Policy NAT Policy R	Route Policy Descyption Policy DaS Policy				
7.5 ()					
					All Polces • • Auto Y-Scaleg
	2.0	17-48	17-48	17.60	15.01
hon Lagandic 🕥	017	1758	1748	1786	1.181
DWIDTH ()					
and the fill					AllPoloist - V Auto Y-Scaling
00 type					AllPolces - 💌 AntrYdcalog
10 hpn					
2 hpm					
2 kpm					
2 kpm					
0 Japa	1947	17.48	17-49	17.60	12.61
ton Lagendi:	1.147	1748	1748	1784	12.01
ECTION RATE (0)					
					All Policies . 💌 Auto Y-Scaling
00 (ps					
N-Can					
0 Gym					
15m					
10ps					
0 Gyr	1947	12.48	1749	17.60	17.61
on Lagendi:	1047	0.48	174	1/104	1.081
CONNECTION USAGE ()					
					All Palcies - 💌 Auto Y-Scaling
100					alforder + Augustaling
0.00					
6.60					
0.0		0	1 3070 F.48-78		
		Data Total	0 DPMcies-0		
9.29					
6.20 g	247	17.48	1749	17:60	17.61

DoS Policy

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

Strive 0 Refe	nhom: Im Pid • Iddu Llazi. •			Ø Rør ⊗
Security Policy NAT Policy Route Pol	licy Decryption Policy DaS Policy			
5 0				
				All Policies - V
4				
0 17.61	15.62	1748	17.64	12.66
w Lagandic 🔘				
() HTOM				
0 typ				All Palcies - * Auto Y Scaling
i tys				
lian				
-				
i iya				
17.61	17.62	17-63	17.64	12.00
w Lagandic 🔘				
CTION RATE ()				
				M Palcies . 🖤 Auto V-Scaling
(p				
rije Kan				
Gen				
inge				
15a 1741				
n Lagandia C	12.62	17.63	17.64	12.08
ONNECTION USAGE ()				
				Mi Palaini - 💌 Arra Y Caling
100				All Packet + Auto Hocking
0.00				
0.10				
0.20				
17.61	17/82	1243	17.64	17.68

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.

Option	Widget	Description
View Range	0 5 mins	 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	Refresh every: 3 sec	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	IPv4	Select either IPv4 , IPv6 or Both to include in the monitoring.

Zones	ZONE MATRIX SELECTOR X From Zone All Zones To Zone Any To Zone To Zone All Zones To	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	Active & Inactive Active Rules Inactive Rules	Select whether to monitor active or inactive policies or both.
Pause	(1)	Freezes the data flow. The Pause button appears black if the data flow has been frozen.
Play	\odot	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	Q	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.

Security Policy	NAT Policy	Route Policy	Decryption Policy	DoS Policy	
STATUS (1)					
1					
0					
0 0 18:13		18:14		18:1	5
Show Legends:)	Discarded		D C	Propped

Tooltips

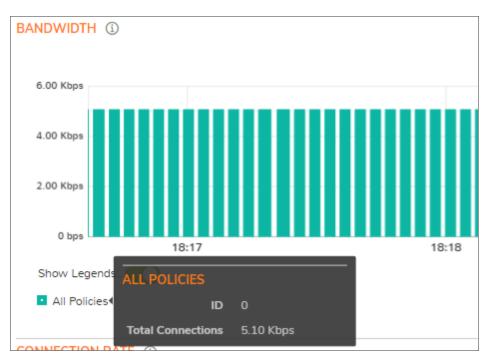
•

Various elements of the charts have associated tool-tips:

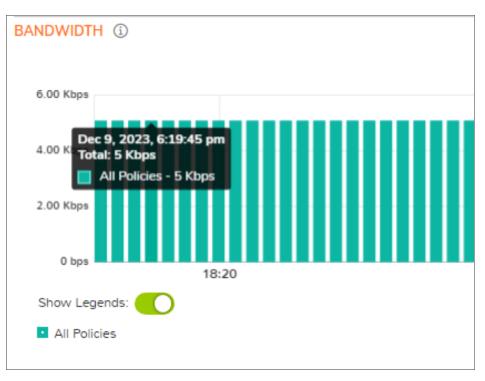
The name of the chart has a tool-tip icon (i) that briefly describe the chart.

	tatus	····	- 1 1 1		
_		ows connections th d dropped by rules.			
1				-	
1					
1					
0					
0					
0	18:15		18:	16	18:17
Show Legend	ls:				

• 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.

DANDWIDTH ()						
6.00 Kbps				All Policies ×	▼ Auto Y-Scaling	- <u>H</u>
4.00 Kbps						
2.00 Kbps						
0 bps						
	All Pol	All Pol	All Pol	All Pol	All Pol	
Show Legends:						
All Policies						

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 **I**. The following example is a Stacked BAr Chart view.

Security Policy NAT Poli	icy Route Policy Decryption F	Policy DoS Policy		
STATUS (1)				
2				All Policies ×
2				
1				
1				
8:23	18:24	18:25	18:26	18:27
Show Legends:	16:24	18:25	rc:26	10:27

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 xaxis displays the current time and the y-axis displays the number of policies that are allowed, discarded, and dropped.

STATUS (1)					
2				All Policies	× • Auto Y-Scaling
2					
1				_	
0	18:37	18:38	18:39	18:40	18:41
Show Legends:					

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).

Security Policy NAT Polic	y Route Policy Decryption Po	licy DoS Policy		
STATUS (1)				
				All Policies ×
2				
1				
1				
8:23	18:24	18:25	18:26	18:27
Show Legends:				

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).

BANDWIDTH (1)				
6.00 Kbps ,			All Policies ×	▼ Auto Y-Scaling
4.00 Kbps				
2.00 Kbps				
0 bps All Pol	All Pol	All Pol	All Pol	All Pol
Show Legends:				
All Policies				

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

CONNECTION RATE (1)					
1.00 Cps				All Policies × 🖤 Auto Y-Scaling	🖬 🖬
0.80 Cps					
0.60 Cps					
0.40 Cps					
0.20 Cps					
0 Cps	19:16	19:17	19:18	19:19	19:2
Show Legends:					
TOTAL CONNECTION USAGE	D				

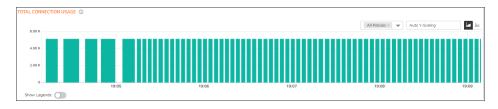
Bar Chart

Custom Security Policy_3 Custom Security Policy_5	Custom Security Policy_1 Custom Security Policy_4	Custom Security Policy_2	Custom Security Policy_6	
Show Legends – –				
0Cps			0	
0.2Cps				
0.4Cps				
0.6Cps				
0.8Cps				
1.0Cps				All Rules Rate 🔻 Auto Y-Scaling 📶 🛋
CTIVE CONNECTION RATE				All Rules Rate 📼 Anto Y.Scalino 🚮

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

			All Policies ×	💌 Auto Y-Scaling
4.00 K	3			
All Pol	All Pol	All Pol	All Pol	All Pol
Show Legends:				

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.

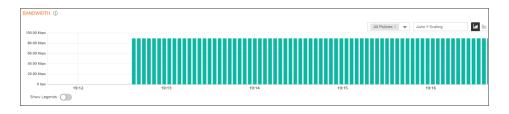
Security Policy	NAT Policy	Route Policy	Decryption Policy	DoS Policy									
STATUS ①													
5										All Policies	-	Auto Y-Sc	aling
4													
3									h.,			t ne	
2				du		nhui	la la i	hilli	htt	t hi		de He	the st
0													
Show Legends:	19:11		19:12		19:13			19:14				19:15	

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).

BANDWIDTH ①		
100.00 Kbps	All Policies × 👿 Auto Y-Scaling	La La
100.00 Kops		
80.00 Kbps		
60.00 Kbps		
40.00 Kbps		
20.00 Kbps		
0 bps	All Policies	
Show Legends:		

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).

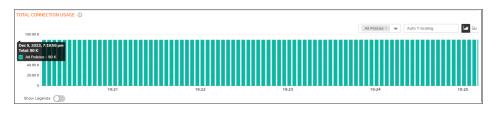
Stacked Bar Chart

CONNECTION	RATE (1)				
1.00 Cps				All Policies >	👻 Auto Y-Scaling
0.80 Cps					
0.60 Cps					
0.40 Cps					
0.20 Cps					
0 Cps		9:16 1!	9:17 19	118 11	9:19 19:2
Show Leger	nds:				
TOTAL CONNE	CTION USAGE (1)				

Total Connection Usage

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

Stacked Chart



Bar Chart

TOTAL CO	NNECTION USAGE	ie ()	
100.00	ĸ	All Policies × 💌 Auto 1	Y-Scaling
80.00			
60.00			
20.00			
	0	All Policies	
Show L	egends:		

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).

BANDWIDTH	0					
200.00 Kbps					All Policies × 💌 Auto Y-Scaling	
150.00 Kbps						
100.00 Kbps						
50.00 Kbps						
0 bps	19:28	19:29	19:30	19:31	19:32	
Show Leger	nds:					

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).

BANDWIDTH ()				
200.00 Kbps		All Policies ×	Auto Y-Scaling	Let M
150.00 Kbps				
100.00 Kbps				
50.00 Kbps				
0 bps	All Policies			
Show Legends:				

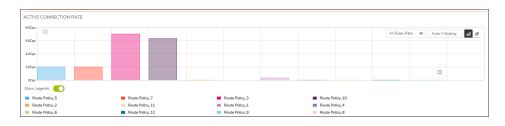
Connection Rate

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

CONNECTION	RATE (1)					
1.00 Cps				AJ	Policies × 🛛 Auto Y-Scaling	
0.80 Cps						
0.60 Cps						
0.40 Cps		Dec 9, 2023, 1	7:31:30 pm			
0.20 Cps		Total: 0 Cps All Policies	- 0 Cps			
0 Cps	19:30	19:31	19:32	19:33	19:34	
Show Leger	ends:					

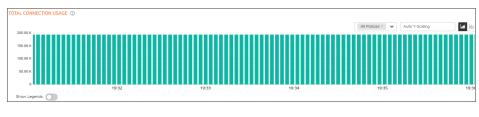
Bar Chart



Total Connection Usage

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

Stacked Bar Chart



Bar Chart

Y-Scaling	la la

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**.

(i) **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.

STATUS ()	
	All Policies × Auto Y-Scaling
1	
1	
0	
0	
0	

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

BANDWIDTH	0			
1.00 -		•	Auto Y-Scaling	Let his
1.00				
0.80				
0.60				
0.40				
0.20				
0				
Show Leg	nds: 💽			

Bar Chart

BANDV	VIDTH										
60.0Kbps 50.0Kbps	0								All Rules Rate	 Auto Y-Scal 	ng 📶 🏄
40.0Kbps											
30.0Kbps											
20.0Kbps 10.0Kbps											
Obps											
Show Le	now Legends:										

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.

ACTIV	E CONNECTION RATE	E									
5.0Cps	0								All Rules Rate	 Auto Y-Scaling 	
4.0Cps											
3.0Cps 2.0Cps											
1.0Cps											
OCps											
Show L	Show Legenda 💽										
My	■ My Rule_1										

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.

TC	TAL CONNECTION US	AGE						_
	0.0	MOL						
	() 15.0					All Rules Usage 🔻 🛛 Aut	o Y-Scaling	#
	10.0							
	5.0							
9	o Logends							
	My Rule_1							

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.

ew Style:	Las	t 30 N	linute	5 🗸	Ve	ertical /	Axis:	25 U	Isers	~																		(Q
MBER C	DF U	SERS	LOG	GED	IN -	LAST	5 30	MINU	JTES																				
																								=	Client	users	=	Web	us
5																													
5																													
2	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	
5 2		ł	ł	ł	ł			ł		ł		ł	ł		ł	ł	ł	ł				ł	ł	ł				l	
29	28	27	28	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	N

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**.

A	uthentication	Web Login	Authentication Bypass	User Sessions	Accounting	Customization	
USER A	UTHENTICATIO	N SETTINGS (1)					
	User auth	entication method	Local Users 💌		Ca	se-sensitive user names	
		Configure RADIUS	Configure 3		E	nforce login uniqueness	0
		Configure LDAP	Configure		Force relogin	after password change	0
	Co	onfigure TACACS+	Configure		Display user lo	ogin info since last login	
SING	LE-SIGN-ON M	ETHOD(S)					
		Configure SSO	Configure			RADIUS Accounting	0
		SSO Agent				3rd-Party API	
	Termin	al Services Agent			Browse	r NTLM Authentication	
ONE-	TIME PASSWO	RD					
		Enforce password	I complexity for One-Time Password	0			
			One-time password E-mail format	Plain Text			
			One Time Password Format	Characters	•		
			One Time Password Length	10	to 1	10	Password Strength: Good
			Cancel	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	0 5 mins	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	Refresh every: 3 sec	Determines the frequency at which data is refreshed. A numerical integer between 1 to 10 seconds is required. The default is 3 seconds.
Play	\odot	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	(1)	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	<u>.11</u>	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	All Policies × All Policies	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.

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

Copyright © 2023 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