SonicWall® SonicOS 6.5 Investigate

Administration

Contents

Part 1. Investigate | Logs

Part 2. Investigate | Reports

Part 3. Investigate | Tools

Part 4. Investigate | Appendix

Part 1

INVESTIGATE | Logs

- Event Logs
- Connection Logs
- Appflow Logs
- WAN Acceleration Logs
- Anti-Spam Junkbox

1

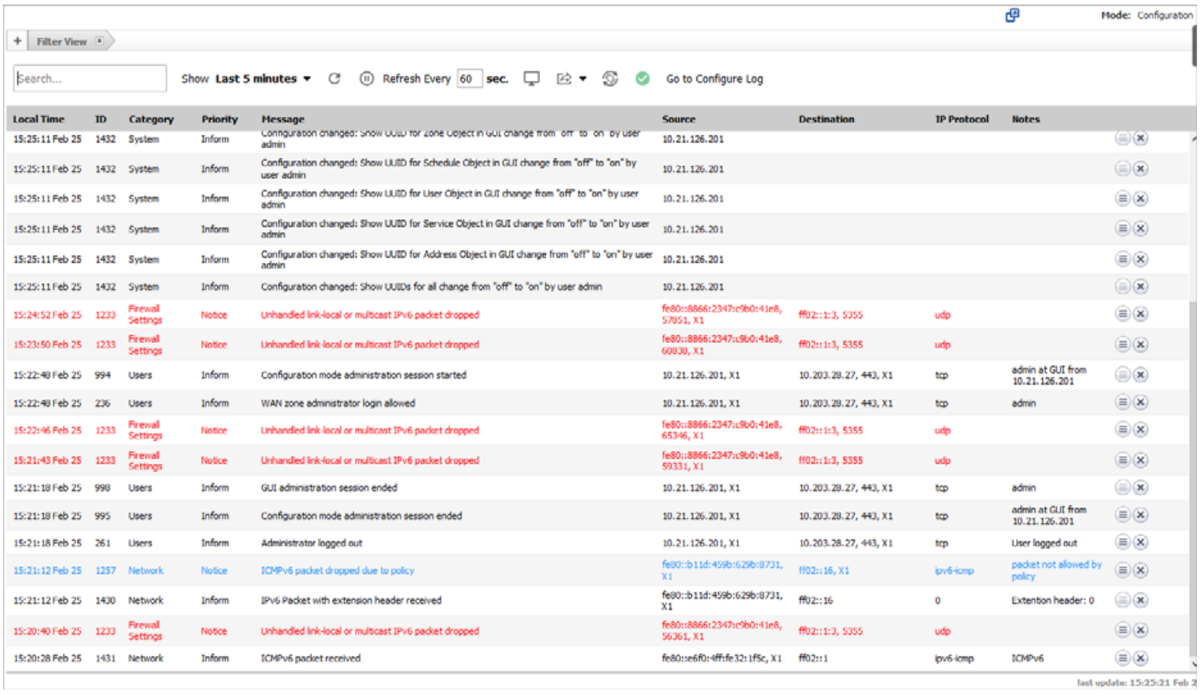
Event Logs

Topics:

- Viewing Events on page 7
- Filtering the View on page 11

Viewing Events

The SonicWall network security appliance maintains an Event log for tracking potential security threats.



Mode: Configuration

Show Last 5 minutes

Refresh Every 60 sec.

Local Time	ID	Category	Priority	Message	Source	Destination	IP Protocol	Notes
15:25:11 Feb 25	1432	System	Inform	Configuration changed: Show UUID for Zone Object in GUI change from "off" to "on" by user admin	10.21.126.201			
15:25:11 Feb 25	1432	System	Inform	Configuration changed: Show UUID for Schedule Object in GUI change from "off" to "on" by user admin	10.21.126.201			
15:25:11 Feb 25	1432	System	Inform	Configuration changed: Show UUID for User Object in GUI change from "off" to "on" by user admin	10.21.126.201			
15:25:11 Feb 25	1432	System	Inform	Configuration changed: Show UUID for Service Object in GUI change from "off" to "on" by user admin	10.21.126.201			
15:25:11 Feb 25	1432	System	Inform	Configuration changed: Show UUID for Address Object in GUI change from "off" to "on" by user admin	10.21.126.201			
15:25:11 Feb 25	1432	System	Inform	Configuration changed: Show UUIDs for all change from "off" to "on" by user admin	10.21.126.201			
15:24:52 Feb 25	1233	Firewall Settings	Notice	Unhandled link-local or multicast IPv6 packet dropped	fe80::8866:2347:c9b0:41e8, 57851, X1	ff02::1:3, 5355	udp	
15:23:50 Feb 25	1233	Firewall Settings	Notice	Unhandled link-local or multicast IPv6 packet dropped	fe80::8866:2347:c9b0:41e8, 60838, X1	ff02::1:3, 5355	udp	
15:22:48 Feb 25	994	Users	Inform	Configuration mode administration session started	10.21.126.201, X1	10.203.28.27, 443, X1	tcp	admin at GUI from 10.21.126.201
15:22:48 Feb 25	236	Users	Inform	WAN zone administrator login allowed	10.21.126.201, X1	10.203.28.27, 443, X1	tcp	admin
15:22:46 Feb 25	1233	Firewall Settings	Notice	Unhandled link-local or multicast IPv6 packet dropped	fe80::8866:2347:c9b0:41e8, 65346, X1	ff02::1:3, 5355	udp	
15:21:43 Feb 25	1233	Firewall Settings	Notice	Unhandled link-local or multicast IPv6 packet dropped	fe80::8866:2347:c9b0:41e8, 59331, X1	ff02::1:3, 5355	udp	
15:21:18 Feb 25	998	Users	Inform	GUI administration session ended	10.21.126.201, X1	10.203.28.27, 443, X1	tcp	admin
15:21:18 Feb 25	995	Users	Inform	Configuration mode administration session ended	10.21.126.201, X1	10.203.28.27, 443, X1	tcp	admin at GUI from 10.21.126.201
15:21:18 Feb 25	261	Users	Inform	Administrator logged out	10.21.126.201, X1	10.203.28.27, 443, X1	tcp	User logged out
15:21:12 Feb 25	1257	Network	Notice	ICMPv6 packet dropped due to policy	fe80::b11d:459b:629b:8731, X1	ff02::16, X1	ipv6-icmp	packet not allowed by policy
15:21:12 Feb 25	1430	Network	Inform	IPv6 Packet with extension header received	fe80::b11d:459b:629b:8731, X1	ff02::16	0	Extention header: 0
15:20:40 Feb 25	1233	Firewall Settings	Notice	Unhandled link-local or multicast IPv6 packet dropped	fe80::8866:2347:c9b0:41e8, 56361, X1	ff02::1:3, 5355	udp	
15:20:28 Feb 25	1431	Network	Inform	ICMPv6 packet received	fe80::e6f0:4ff:fe32:1f5c, X1	ff02::1	ipv6-icmp	ICMPv6

last update: 15:25:21 Feb 2

For a description of the:

- Functions, see Event Log Functions on page 7.
- Columns, see Display Options on page 8.

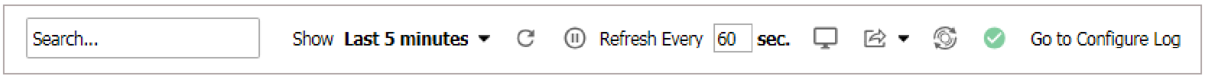
The date and time of the last update are displayed in the bottom right corner of the page.

Event Log Functions

The **Event Log** table provides numerous settings to allow you to navigate, view, and export results. Table columns can be customized, so that you can view full data on any event, or only the data you need. Table entries can be sorted to display in either ascending or descending order.

To sort the entries in the **Event Log**, click the column heading. The entries are sorted by ascending or descending order. The arrow to the right of the column name indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

The top row of the **Event Log** contains various functions. Functions pertaining only to Event Logs are described in Event Log Functions; common functions are described in *SonicWall SonicOS 6.5 About SonicOS*.

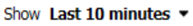
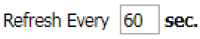

Search...

Show **Last 5 minutes**

Refresh Every 60 **sec.**

Go to Configure Log

Event Log Functions

Option	Function	Action
Search...	Search	The Event Log displays the log entries that match the search string. Click the **X** in the **Search** field to delete the search string.
 Show **Last 10 minutes**	Show	Select the interval for the Event Log. The event logs from that period are displayed: **Last 60 seconds** (default) **Last 2 minutes** **Last 5 minutes** **Last 10 minutes** **Last 15 minutes** **Last 30 minutes** **Last 60 minutes** **Last 3 hours** **Last 6 hours** **Last 12 hours** **Last 24 hours** **Last 7 days** **Last 15 days** **Last 30 days** **All Entries**
 Refresh Every 60 **sec.**	Refresh Interval	In the field, type the number of seconds between data refreshes.
Go to Configure Log	Go to Configure Log	Click this link and you are taken to **MANAGE | Logs & Reporting > Log Settings > Base Setup** to configure the items tracked in the Event Log.

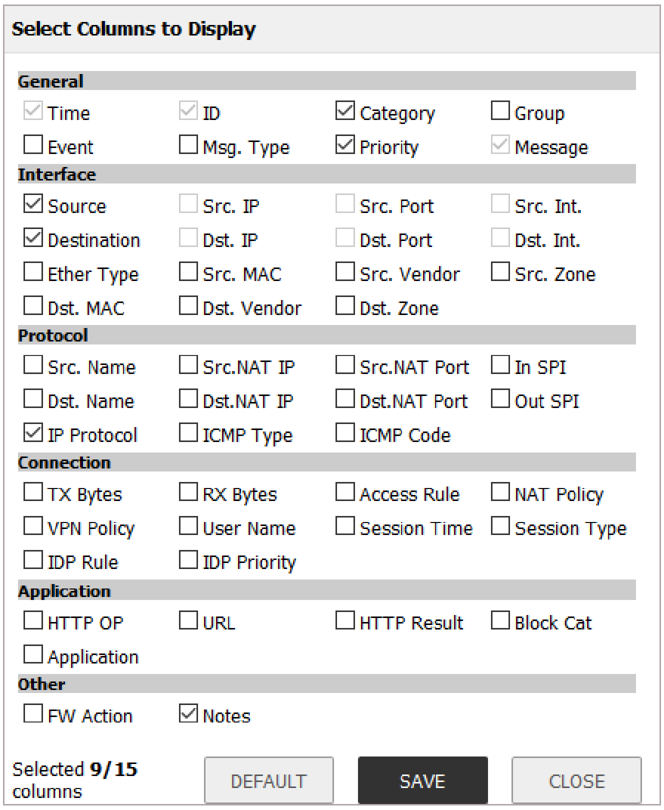
Display Options

Customize the Events log to display as many or few columns that meet your needs.

To select which columns to display:

1 Navigate to **INVESTIGATE | Logs > Event Logs**.

2 Click the **Display Options** icon. The **Select Columns to Display** dialog displays:



Select Columns to Display

General

☑ Time	☑ ID	☑ Category	□ Group
□ Event	□ Msg. Type	☑ Priority	☑ Message

Interface

☑ Source	□ Src. IP	□ Src. Port	□ Src. Int.
☑ Destination	□ Dst. IP	□ Dst. Port	□ Dst. Int.
□ Ether Type	□ Src. MAC	□ Src. Vendor	□ Src. Zone
□ Dst. MAC	□ Dst. Vendor	□ Dst. Zone	

Protocol

□ Src. Name	□ Src.NAT IP	□ Src.NAT Port	□ In SPI
□ Dst. Name	□ Dst.NAT IP	□ Dst.NAT Port	□ Out SPI
☑ IP Protocol	□ ICMP Type	□ ICMP Code	

Connection

□ TX Bytes	□ RX Bytes	□ Access Rule	□ NAT Policy
□ VPN Policy	□ User Name	□ Session Time	□ Session Type
□ IDP Rule	□ IDP Priority		

Application

□ HTTP OP	□ URL	□ HTTP Result	□ Block Cat
□ Application			

Other

□ FW Action	☑ Notes		

Selected **9/15** columns

3 Select the items you want to appear as columns in the Event Log.

General General information about the log event.

Time Local date and time the event occurred.

IMPORTANT: This option is selected by default. It is dimmed, and cannot be deselected.

ID Identifying number for the event.

IMPORTANT: This option is selected by default. It is dimmed, and cannot be deselected.

Category Category of the event. This option is selected by default.

Group Group designation of the event.

Event Name of the event.

Msg Type Type of message; usually Standard Message String.

Priority Priority level of the event, such as Inform (information) or Error This option is selected by default.

Message Information about the event.

Interface Information about the protocol of the packet triggering the event.

Source Name of the source device, if applicable. This option is selected by default.

TIP: If this option is selected, the **Src. IP**, **Src. Port**, and **Src. Int.** options are dimmed and cannot be selected.

Src. IP IP address of the source device.

NOTE: This option is dimmed if **Source** is selected.

	Src. Port	Port number of the source. **NOTE:** This option is dimmed if **Source** is selected.
	Src. Int.	Source network and IP address, if applicable. **NOTE:** This option is dimmed if **Source** is selected.
	Destination	Name of the destination device, if applicable. This option is selected by default. **TIP:** If this option is selected, the **Dst. IP**, **Dst. Port**, and **Dst. Int.** options are dimmed and cannot be selected.
	Dst. IP	IP address of the destination device. **NOTE:** This option is dimmed if **Destination** is selected.
	Dst. Port	Port number of the destination. **NOTE:** This option is dimmed if **Destination** is selected.
	Dst. Int.	Destination network and IP address, if applicable. **NOTE:** This option is dimmed if **Destination** is selected.
	Ether Type	Ethernet type of the packets, if known.
	Src. MAC	MAC address of the source device, if known.
	Src. Vendor	Name of the source device's manufacturer, if known.[a]
	Src. Zone	Source zone, if known.
	Dst. MAC	MAC address of the destination device, if known.
	Dst. Vendor	Name of the destination device's manufacturer, if known.[a]
	Dst. Zone	Destination zone, if known.
Protocol	Information about the NAT policy in effect, if any.	
	Src. Name	Protocol source name.
	Src. NAT IP	Source address from the Source NAT IP address pool.
	Src. NAT Port	Port number for the Source NAT.
	In SPI	Indicates whether the ingress packet is in Stateful Packet Inspection (SPI) mode, if applicable.
	Dst. Name	Protocol destination name.
	Dst. NAT IP	Destination address from the Source NAT IP address pool.
	Dst. NAT Port	Port number for the Destination NAT.
	Out SPI	Indicates whether the egress packet is in Stateful Packet Inspection (SPI) mode, if applicable.
	IP Protocol	Protocol used to send error and control messages, if known. This option is selected by default.
	ICMP Type	ICMP packet's ICMP type, if known.
	ICMP Code	ICMP packet's ICMP code, if known.
Connection	Information about SPI, Access and IDP Rules, and policies, if any.	
	TX Bytes	Number of bytes transmitted.
	RX Bytes	Number of bytes received.
	Access Rule	Name of the Access Rule triggering the event, if any.
	NAT Policy	Name of the NAT policy.
	VPN Policy	Name of the VPN policy triggering the event, if any.
	User Name	Name of the user whose action triggered the event.

	Session Time	Duration of the session before the event.
	Session Type	Type of session triggering the event.
	IDP Rule	Name of the IDP Rule triggering the event, if any.
	IDP Priority	Priority of the IDP Rule.
Application	Information about the application being used.	
	HTTP OP	NPCS object op requestMethod HTTP OP code.
	URL	URL of the NPCS object op requestMethod HTTP OP code.
	HTTP Result	HTTP result code (such as, 200, 403) of Website hit rpkt cn1Label Packet received.
	Block Cat	Block category that triggered the event.
	Application	The application being used.
Others	Information about the user, session, and application, if known.	
	FW Action	Configured firewall action. If no action has been specified, displays N/A.
	Notes	**NOTE:** Includes notes. This option is selected by default.

a. Every wired or wireless networking device has a 48-bit MAC address assigned by its hardware manufacturers. An organizationally unique identifier (OUI) is a 24-bit number that uniquely identifies a vendor, manufacturer, or other organization globally or worldwide. The first three octets of the MAC address are the OUI.

4 When done, click **SAVE** to preserve any changes; click **DEFAULT** to revert back to the default settings.

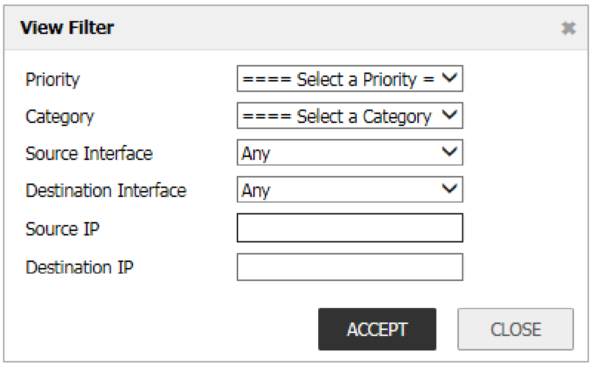
Filtering the View

The **Filter View** input field at the top left corner of the Event Log enables you to narrow your search using drop-down options and search strings.

To filter the Event Log:

1 Navigate to **INVESTIGATE | Logs > Event Logs**.

2 Click the **+** sign by **Filter View**. The **View Filter** pop-up dialog displays.



View Filter

Priority	==== Select a Priority =
Category	==== Select a Category
Source Interface	Any
Destination Interface	Any
Source IP	
Destination IP	

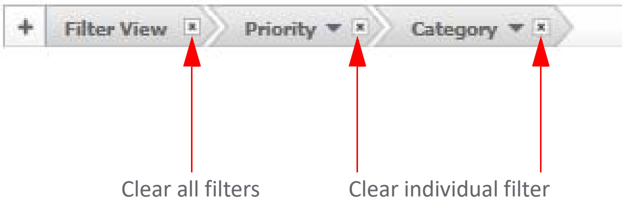
3 Select any filtering scheme you want. Filter on just one field or you can filter on all of them. In the **Source IP** and **Destination IP** fields, you can enter a partial string to filter on.

4 Click **ACCEPT**.

To clear the filter(s):

1 Do one:

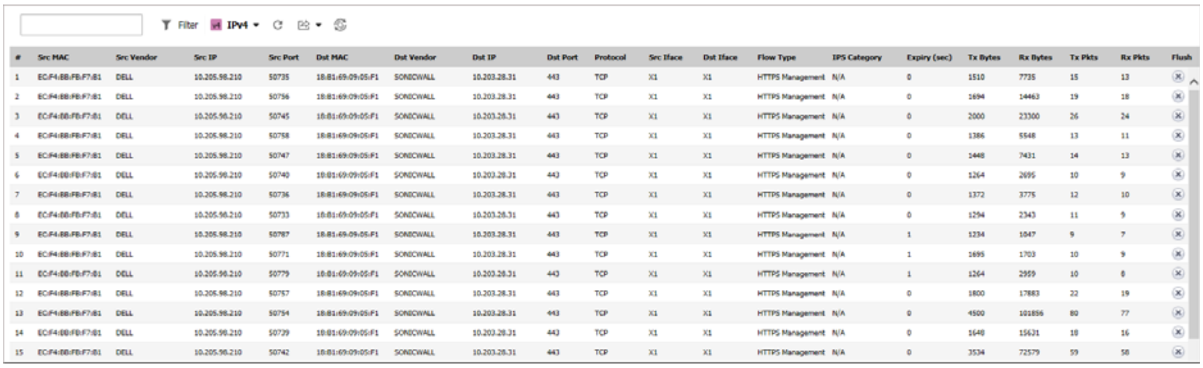
- To clear just one filter criterion, click the **X** by its name.
- To clear all filters click the **X** by **Filter View**.



2

Connection Logs

The SonicWall network security appliance maintains a Connection Log for tracking all active connections to the SonicWall security appliance. To view the Connection Log table, navigate to **Logs > Connection Logs** on the **INVESTIGATE** view.



#	Src MAC	Src Vendor	Src IP	Src Port	Dst MAC	Dst Vendor	Dst IP	Dst Port	Protocol	Src Iface	Dst Iface	Flow Type	IPS Category	Expiry (sec)	Tx Bytes	Rx Bytes	Tx Pkts	Rx Pkts	Flush
1	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50735	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	0	1510	7735	15	13	⊗
2	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50756	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	0	1694	14463	19	18	⊗
3	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50745	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	0	2000	23300	26	24	⊗
4	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50758	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	0	1386	5548	13	11	⊗
5	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50747	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	0	1448	7431	14	13	⊗
6	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50740	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	0	1264	2695	10	9	⊗
7	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50736	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	0	1372	3775	12	10	⊗
8	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50733	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	0	1294	2343	11	9	⊗
9	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50787	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	1	1234	1047	9	7	⊗
10	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50771	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	1	1695	1703	10	9	⊗
11	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50779	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	1	1264	2959	10	8	⊗
12	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50757	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	0	1800	17883	22	19	⊗
13	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50754	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	0	4500	101856	80	77	⊗
14	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50739	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	0	1648	15631	18	16	⊗
15	EC:F4:BB:FB:F7:81	DELL	10.205.98.210	50742	18:B1:69:09:05:F1	SONICWALL	10.203.28.31	443	TCP	X1	X1	HTTPS Management	N/A	0	3534	72579	59	58	⊗

Topics:

- Viewing Connections
- Searching the Connection Log
- Filtering the Connection Log
- Connection Log Functions

Viewing Connections

The connections for a SonicWall appliance are listed in the **Connections Log**. The column names for the table are described in the following:

Src MAC	MAC address of the source device.
Src Vendor	Manufacturer of the source device.
Src IP	IP address of the source device.
Src Port	Port number of the source device.
Dst MAC	MAC address of the destination device.
Dst Vendor	Manufacturer of the destination device.
Dst IP	IP address of the destination device.
Dst Port	Port number of the destination device.
Protocol	Protocol used for the connection, such as TCP or ICMPv6.
Src Iface	Interface on the source device.
Dst Iface	Interface on the destination device.

Flow Type Flow type of the connection, such as generic or HTTP Management.

IPS Category Type of Intrusion Prevention System (IPS) used; N/A = Not Available.

Expiry (sec) Number of seconds remaining before the connection expires.

Tx Bytes Number of bytes transferred.

Rx Bytes Number of bytes received.

Tx Pkts Number of packets transferred.

Rx Pkts Number of packets received.

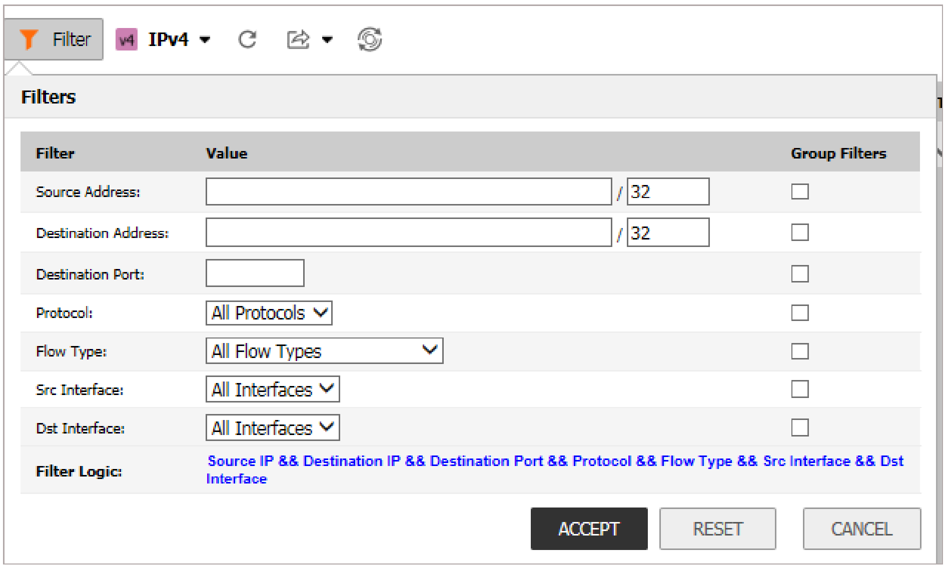
Flush Contains the **Flush** icon for each entry.

Searching the Connection Log

Use **Search** to find connections that meet a specific search criteria. Type a search string into the **Search** field and the Connection Log displays the entries that match the string. Click the **X** in the **Search** field to delete the search string.

Filtering the Connection Log

Filter the Connection Log table so it displays only those connections matching the criteria specified in the **Filter** option.



Filter	Value	Group Filters
Source Address:	/ 32	□
Destination Address:	/ 32	□
Destination Port:		□
Protocol:	All Protocols	□
Flow Type:	All Flow Types	□
Src Interface:	All Interfaces	□
Dst Interface:	All Interfaces	□
Filter Logic:	Source IP && Destination IP && Destination Port && Protocol && Flow Type && Src Interface && Dst Interface	

Filter by:

- **Source Address**
- **Destination Address**
- **Destination Port**
- **Protocol**
- **Flow Type**
- **Src Interface**
- **Dst Interface**

Filter Logic displays how the filter is applied.

The fields you enter values into are combined into a search string with a logical AND. For example, if you enter values for **Source IP** and **Destination IP**, the search string looks for connections matching:

```
Source IP AND Destination IP
```

Check the **Group** box next to any two or more criteria to combine them with a logical **OR**. For example, if you enter values for **Source IP, Destination IP**, and **Protocol**, and check Group next to Source IP and Destination IP, the search string looks for connections matching:

```
    (Source IP OR Destination IP) AND Protocol
```

Click **Apply Filters** to apply the filter immediately to the **Active Connections** table. Click **Reset Filters** to clear the filter and display the unfiltered results again.

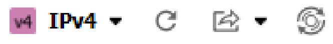
Export the list of active connections to a file. Click **Export Results**, and select if you want the results exported to a plain text file, or a Comma Separated Value (CSV) file for importing to a spreadsheet, reporting tool, or database. If you are prompted to Open or Save the file, select **Save**. Then enter a filename and path, and click **OK**.

Connection Log Functions

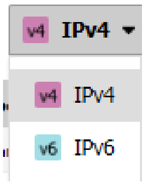
The **Connection Logs** table provides several settings to allow you to navigate, view, and export results. Table entries can be sorted to display in either ascending or descending order.

To sort the entries in the **Event Log**, click the column heading. The entries are sorted by ascending or descending order. The arrow to the right of the column name indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

The top row of the **Event Log** contains several functions:



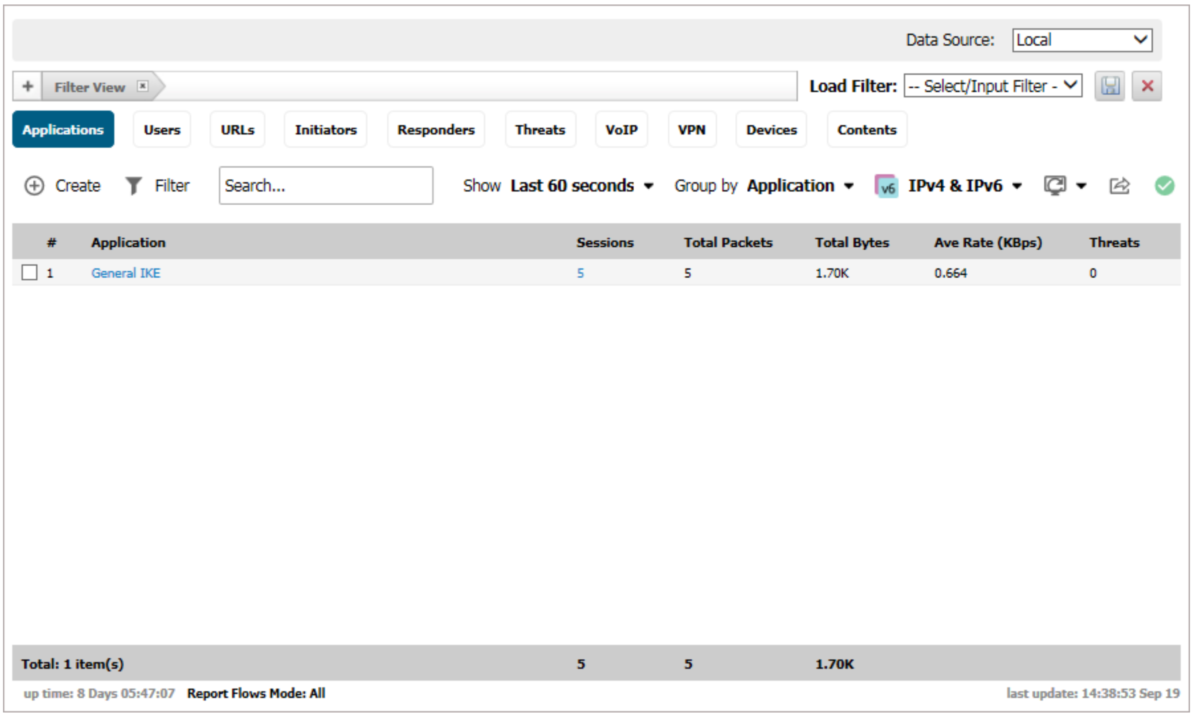
Event Log Functions

Option	Function	Action
	IPv4/IPv6	The **Connection Log** is configured the same for IPv6 and IPv4. To change the view, select the IP version from the drop-down menu. **IPv4** is the default.
⟳	Refresh	Click to immediately refresh the Event Log.
↗ ▾	Export to file	Exports the data to an external file. From the drop-down menu, select the file format: **CSV**, **Text**, or **Email**.
⟲	Clear	Deletes all logs displayed in the **Event Log**. You are asked to confirm your decision before the events are deleted.
⊗	Flush	Click this icon to flush that connection from the table. This option is found in the far right column of the table.

3

Appflow Logs

The **Appflow Logs** provides real-time, incoming and outgoing network data. Various views and customizable options in the Appflow Monitor Interface assist in visualizing the traffic data by applications, users, URLs, initiators, responders, threats, VoIP, VPN, devices, or contents.



Data Source: Local

Load Filter: -- Select/Input Filter -

Search...

Show Last 60 seconds · Group by Application · IPv4 & IPv6

	#	Application	Sessions	Total Packets	Total Bytes	Ave Rate (KBps)	Threats
☐	1	General IKE	5	5	1.70K	0.664	0
Total: 1 item(s)			5	5	1.70K		

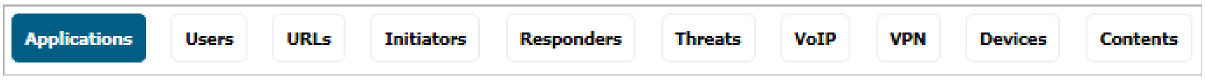
up time: 8 Days 05:47:07 **Report Flows Mode: All** last update: 14:38:53 Sep 19

Topics:

- Appflow Table Options
- Appflow Log Functions
- Group Options
- Appflow Status
- Appflow Display Options

Appflow Table Options

The **Appflow Table options** contain details about incoming and outgoing network traffic. Each option, or button, provides a particular view of the network flow.

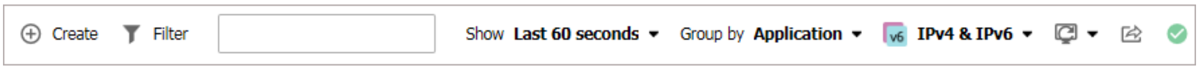


Appflow Table Options

This tab	Displays
Applications	A list of Applications currently accessing the network.
Users	A list of Users currently connected to the network.
URLs	A list of URLs currently accessed by Users. ***To enable this report:*** 1 Navigate to **MANAGE | Policies > Objects > Content Filter Objects**. 2 Select **CFS Action Objects**. 3 Click the **Edit** icon for **CFS Default Action**. 4 Select **Enable Flow Reporting**. 5 Click **OK**. 6 Navigate to **MANAGE | System Setup > Network > Zones**. 7 Click the **Edit** icon for the zone to be monitored. The **Edit Zone** dialog displays. 8 Select **Enable Client CF Service**. 9 Click **OK**.
Initiators	Details about current connection initiators.
Responders	Details about current connection responders.
Threats	A list of threats encountered by the network.
VoIP	Current VoIP and media traffic.
VPN	A list of VPN sessions connected to the network.
Devices	A list of devices currently connected to the network.
Contents	Information about the type of traffic flowing through the network. ***To enable this report:*** 1 Navigate to **MANAGE | Security Configuration > Security Services > Intrusion Prevention**. 2 In the **IPS Global Settings** section, select **Enable IPS**. 3 Click **ACCEPT**. 4 Navigate to **MANAGE | Policies > Rules > App Control**. 5 In the **App Control Global Settings** section, select **Enable App Control**. 6 Click **ACCEPT**. 7 Navigate to **MANAGE | System Setup > Network > Zones**. 8 Click the **Edit** icon for the zone to be monitored. 9 Select **Enable IPS**. 10 Click **OK**.

Appflow Log Functions

The Appflow log functions allow customization of the Appflow Logs table. The ability to create rules and add items to filters allows more application and user control. Different views, pause and play abilities, customizable data intervals and refresh rates are also available to aid in visualizing incoming, real-time data. Selecting data by group and configuring the columns displayed on a tab enable refining of the display.



Appflow Logs Functions

Option	Widget	Description
Create	⊕ Create	Starts the App Control Wizard. For more information on using this wizard, refer to **Policies | Rules > App Rules** and App Control in *SonicWall SonicOS 6.5 Policies*. **NOTE:** General- and service-type applications cannot be included in a rule.
Filter	Filter	Correlates data among the tabs. For more information about creating a filter, see Filter Options.
Search	Search...	Type a search string into the **Search** field and the Appflow Log displays the log entries that match the string. Click the **X** in the search field to delete the search string.
Show *interval* (Where *interval* is the time between monitoring operations)	Show **Last 10 minutes** ▾	From the drop-down menu, select the interval for the Event Log. The event logs from that period are displayed. The options are **Last 60 seconds** (default), **Last 2 minutes**, **Last 5 minutes**, **Last 10 minutes**, **Last 15 minutes**, and **Last 30 minutes**.
Group by *option* (where *option* is one of the options from the drop-down menu)	Group by **Application** ▾	Categorizes selections according to the options in the drop-down menu. The options vary depending on the tab that is selected. See Group Options.
IP Version		Allows selection of Internet protocol: **IPv4**, **IPv6**, or both **IPv4 & IPv6** (default).
Display options	🖵	Click to open the Display Options window, and select an option from the drop-down menu: **Table View**, **Chart View**, **Monitor View**, or **Column Display**. **Column Display** allows you to customize which columns are displayed.
Export to file	⇗	Exports the data flow in comma separated variable (.CSV) format.
Status	✓	Click to open the status window.

Group Options

The **Group** option sorts data based on the specified group, and each group contains different grouping options.

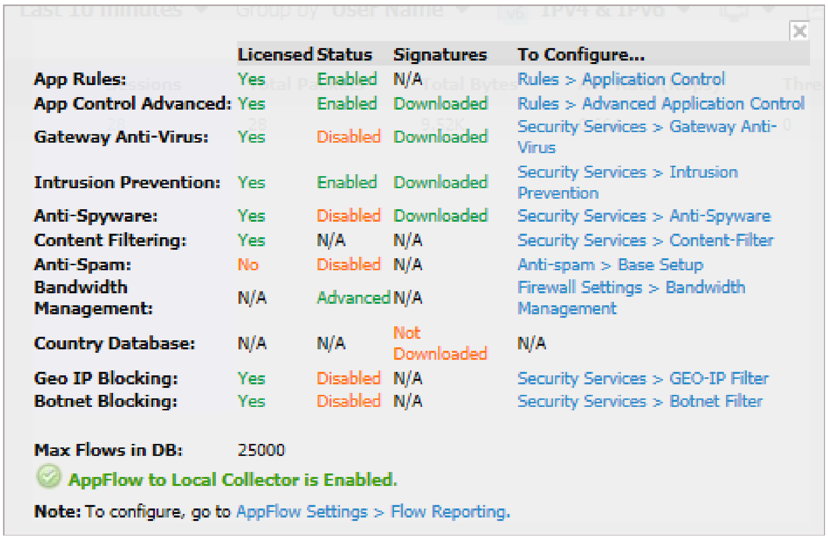
Group Options by Button

Appflow Table Option	Grouped by Option	Description
Applications	Application (default)	Displays all traffic generated by individual applications.
	Category	Groups all traffic generated by an application category.
	Signatures	Groups all traffic generated by an application signature
Users	User Name (default)	Groups all traffic generated by a specific user.
	IP Address	Groups all traffic generated by a specific IP address.
	Domain Name	Groups all traffic generated by a specific domain name.
	Auth Type	Groups all traffic generated by a specific authorizing method.
URLs	URL (default)	Displays all traffic generated by each URL.
	Domain Name	Groups all traffic generated by a domain name.
	Rating	Groups all traffic generated based on CFS rating.
Initiators	IP Address (default)	Groups all traffic generated by a specific IP address.
	Interface	Groups all traffic according to the firewall interface.
	Country	Groups all traffic generated by each country, based on country IP database.
Responders	IP Address (default)	Groups all traffic by IP address.
	Interface	Groups responders by interface.
	Country	Groups responders by each country, based on country IP database.
Threats	Intrusions	Displays flows in which intrusions have been identified.
	Viruses	Displays flows in which viruses have been identified.
	Spyware	Displays flows in which spyware has been identified.
	Spam	Shows all flows that fall under the category of spam.
	Botnet	Displays all flows blocked connecting to/from Botnet servers.
	All (default)	Displays all flows in which a threat has been identified or that fall under the category of spam.
VoIP	Media Type (default)	Groups VoIP flows according to media type.
	Caller ID	Groups VoIP flows according to caller ID.
VPN	Remote IP Address (default)	Groups VPN flows access according to the remote IP address.
	Local IP Address	Groups VPN flows access according to the local IP address.
	Name	Groups VPN flows access according to the tunnel name.
Devices	IP Address (default)	Groups flows by IP addresses inside the network.
	Interface	Groups flows by interfaces on the firewall.
	Name	Groups flows by device name or MAC address.
Contents	Email Address (default)	Groups contents by email address.
	File Type	Groups flows by file type detected.

Appflow Status

The **Appflow Status** appears when the **Status** icon in the toolbar is selected. The **Appflow Status** provides licensing information, status, and signature updates about App Rules, App Control Advanced, GAV, IPS, Anti-Spyware, CFS, Anti-Spam, BWM, country databases, Geo-IP blocking, and Botnet blocking. The tooltip also displays the maximum flows in the database and how Appflow is enabled. For easy configuration of the Appflow Monitor display, the tooltip provides links to the appropriate user interface pages for each item as well as a link to **Appflow > Flow Reporting** for configuring Appflow.

Click the **X** in the upper-right corner to close the **Appflow Status**.



	Licensed	Status	Signatures	To Configure...
App Rules:	Yes	Enabled	N/A	Rules > Application Control
App Control Advanced:	Yes	Enabled	Downloaded	Rules > Advanced Application Control
Gateway Anti-Virus:	Yes	Disabled	Downloaded	Security Services > Gateway Anti-Virus
Intrusion Prevention:	Yes	Enabled	Downloaded	Security Services > Intrusion Prevention
Anti-Spyware:	Yes	Disabled	Downloaded	Security Services > Anti-Spyware
Content Filtering:	Yes	N/A	N/A	Security Services > Content-Filter
Anti-Spam:	No	Disabled	N/A	Anti-spam > Base Setup
Bandwidth Management:	N/A	Advanced	N/A	Firewall Settings > Bandwidth Management
Country Database:	N/A	N/A	Not Downloaded	N/A
Geo IP Blocking:	Yes	Disabled	N/A	Security Services > GEO-IP Filter
Botnet Blocking:	Yes	Disabled	N/A	Security Services > Botnet Filter

Max Flows in DB: 25000

✓ AppFlow to Local Collector is Enabled.

Note: To configure, go to AppFlow Settings > Flow Reporting.

Appflow Display Options

Three views are available for the Appflow display: **Table View**, **Chart View**, and **Monitor View**. Each view provides a unique display of incoming, real-time data.

Table View

In the **Table View,** and depending on which Appflow button across the top is selected, the table is comprised of columns displaying real-time data. These columns are organized into sortable categories. Some columns are common to all buttons. The VoIP tab, however, also has columns specific to it. Tooltips are associated with most column headings, providing definitions.

Chart View

The **Chart View** displays the number of top items and the percentage of bandwidth used by each. The percentage of bandwidth used is determined by taking the total amount of bandwidth used by the top items and then dividing that total by the number of items. The data is then displayed in a pie chart.

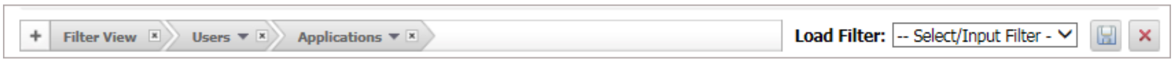
Monitor View

The **Monitor View** displays the network usage according to the Kbps used over the specified period. For each Appflow button at the top, you can select additional options in the drop-down menu below the chart. In the **Scaling** field, **Auto Y-Scaling** is the default. Add specific numbers and units for different scalings.

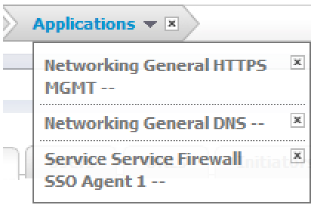
Filter Options

ⓘ **NOTE:** Filter options are available only in the List view although they affect the other views.

The Appflow Filter options allow you to filter incoming, real-time data. Apply, create, and delete filters to customize the information displayed. The filter options apply across all the Appflow buttons.



Appflow Monitor Filter Options

Option	Widget	Description
Add to Filter	+	Adds the current selection to filter. At least 1 item must be selected to use the filter options. After selecting the option, all other tabs update with information pertaining to the items in the filter.
Remove from Filter	Filter View ☒	Removes all the current selections from the filter view by clicking the **X**.
Filter Element	 Applications ▾ ☒ Networking General HTTPS MGMT -- ☒ Networking General DNS -- ☒ Service Service Firewall SSO Agent 1 -- ☒	Indicates a filter element.
Load Filter	Load Filter: -- Select/Input Filter -	Provides a drop-down menu listing the existing filter settings, or you can enter a new name to creates a new filter.
Save	💾	Saves the current filter settings.
Delete	☒	Deletes the current filter settings.
Filter View	▼ Filter	Correlates data among the tabs.

Creating filters reduces the amount of data seen in the Appflow Logs. Create simple or complex filters, depending on the criteria you specify. By doing so, you can focus on points of interest without distraction from other applications.

Topics:

- Creating a Filter with Filter View
- Viewing Entries in Filter View
- Saving Filter Views
- Deleting Filter Views

Creating a Filter with Filter View

To create a filter using Filter View:

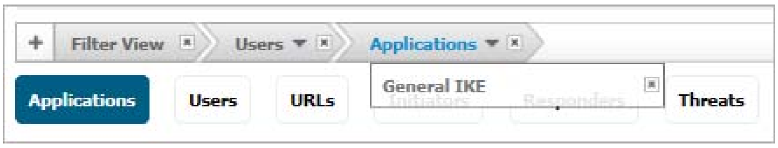
1. Navigate to the **INVESTIGATE** view.
2. Select **Logs | Appflow Logs**.
3. Select a button: for example, **Applications** or **Users**.
4. Check the box(es) of the item(s) on the tab you wish to add to the filter.
5. Click either **Filter View** or **Add to Filter**.

   After entries have been added to the filter, only those entries are visible in the log. In the other Appflow log views, only information about those items associated with the filtered entries are visible.

   Views with a filter are indicated by a button in the Filter View.
6. To further refine the filter, select another tab and repeat Step 4 and Step 5. Each tab is added to the Filter View.

Viewing Entries in Filter View

For a quick look at the items in a filtered view, click the options shown in the Filter View banner. A drop-down menu appears listing all items selected for that option.



To close the drop-down menu, click the option name.

Saving Filter Views

Save a filter view for future use after you created it.

To save a filter view:

1. Click the **Load Filter** drop-down menu.
2. Select the blank line at the top of the list.
3. Enter a friendly, easy-to-remember name for the filter.

4 Click **Save Filter** next to the **Load Filter** drop-down menu.

Deleting Filter Views

Delete all the filter views, the filter view of a tab, or just a few of the items in a particular filter view.

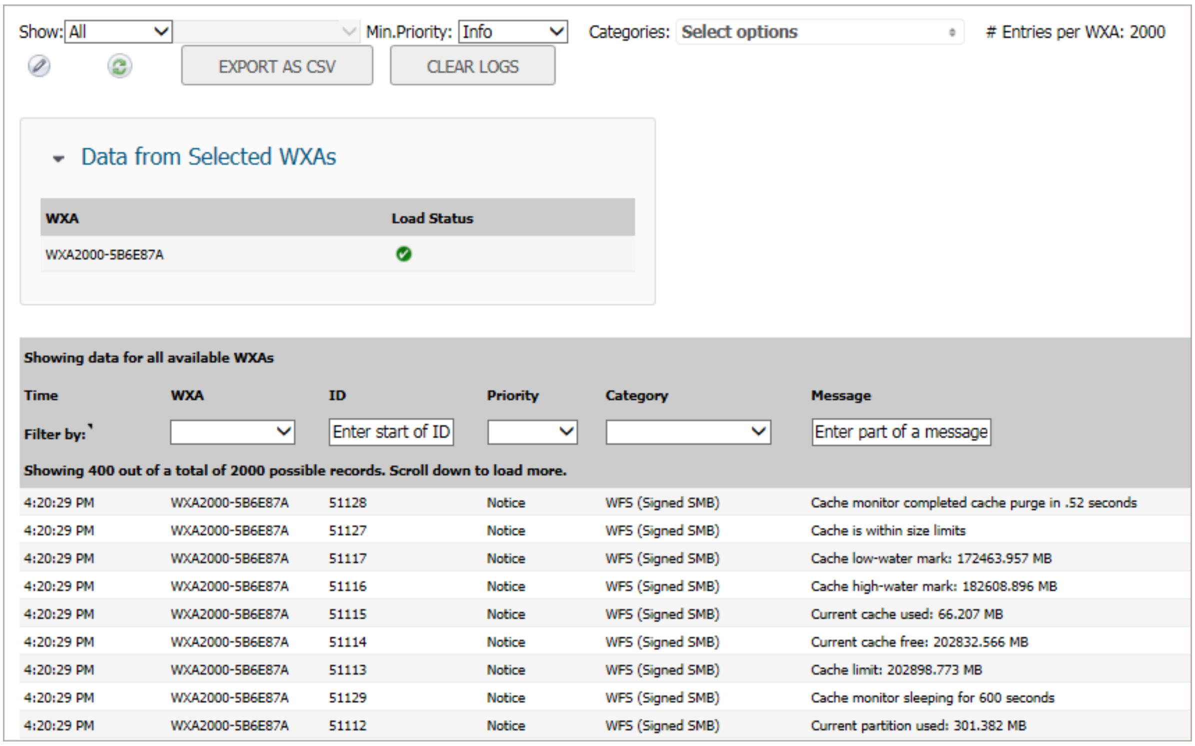
How to Delete Filter Views

To Delete	Do This
All the filter views	Click the **X** in **Remove from Filter**.
A particular filter view	Click the **X** in **Filter View** for that tab.
One or more items in a filter view	Click the name of the tab to display the drop-down menu, and then click the **X** next to the item(s) to delete.
A saved filter	Select the filter in the **Load Filter** drop-down menu and then click **Delete** to the right of the **Load Filter** drop-down menu.

4

WAN Acceleration Logs

The **WAN Acceleration > Log** page on the **INVESTIGATE** view provides a detailed list of log event messages and provides multiple options to change how the log messages display. The Minimum Priority and Categories drop-down menus can be used to determine which logs are retrieved from the WXA. The filters above the data determine which of those entries are actually shown on the screen. Use the scroll function to see more log entries as you scroll down the page.



WXA	Load Status
WXA2000-5B6E87A	✓

Showing data for all available WXAs

Filter by: WXA, ID: Enter start of ID, Priority, Category, Message: Enter part of a message

Showing 400 out of a total of 2000 possible records. Scroll down to load more.

Time	WXA	ID	Priority	Category	Message
4:20:29 PM	WXA2000-5B6E87A	51128	Notice	WFS (Signed SMB)	Cache monitor completed cache purge in .52 seconds
4:20:29 PM	WXA2000-5B6E87A	51127	Notice	WFS (Signed SMB)	Cache is within size limits
4:20:29 PM	WXA2000-5B6E87A	51117	Notice	WFS (Signed SMB)	Cache low-water mark: 172463.957 MB
4:20:29 PM	WXA2000-5B6E87A	51116	Notice	WFS (Signed SMB)	Cache high-water mark: 182608.896 MB
4:20:29 PM	WXA2000-5B6E87A	51115	Notice	WFS (Signed SMB)	Current cache used: 66.207 MB
4:20:29 PM	WXA2000-5B6E87A	51114	Notice	WFS (Signed SMB)	Current cache free: 202832.566 MB
4:20:29 PM	WXA2000-5B6E87A	51113	Notice	WFS (Signed SMB)	Cache limit: 202898.773 MB
4:20:29 PM	WXA2000-5B6E87A	51129	Notice	WFS (Signed SMB)	Cache monitor sleeping for 600 seconds
4:20:29 PM	WXA2000-5B6E87A	51112	Notice	WFS (Signed SMB)	Current partition used: 301.382 MB

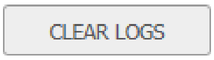
The menus and buttons in the tool bar determine which records are retrieved from the WXA. The records are not all loaded into the table immediately. More records are appended as you scroll down.

Topics:

- Managing the WAN Acceleration Logs
- Data from Selected WXAs
- Filtering WAN Acceleration Logs

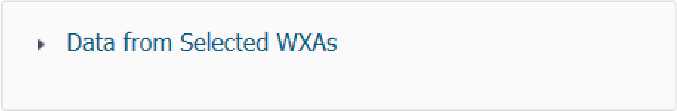
Managing the WAN Acceleration Logs

The **WAN Acceleration > Logs** page displays log messages from the connected WXA. Use the following options to manage the data in the WAN acceleration logs; for common options, see *SonicWall SonicOS 6.5 About SonicOS*.

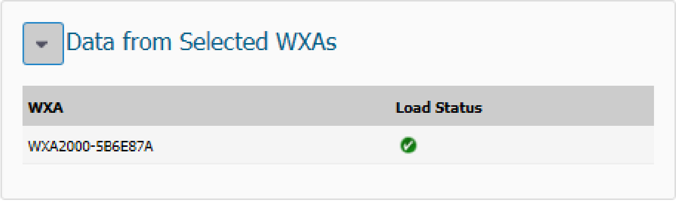
Name	Option	Description
Show	Show: All	Menu from which to select whether to show **All**, **For Group**, or **For WXA**.
Min. Priority	Min.Priority: Info	Displays the log entries of the selected priority or higher.
Categories	Categories: Select options	Displays the log entries of the selected categories. Check the options that you want displayed. Uncheck those you do not want displayed.
# Entries	# Entries per WXA: 2000	Shows the number of entries retrieved and displayed in the logs list. Depending on the number, you might need to scroll through the table to view all the log entries.
Edit	✎	Displays the **Logs: Reporting Period** dialog. Configure the period over which you want to view the reported log entries and set the limit for number of entries from each WAN Accelerator.
EXPORT AS CSV	EXPORT AS CSV	Exports the currently logged messages to a Comma Separated Values (CSV) file that can be saved and viewed as a spreadsheet. The time, priority, category, message, and ID fields are exported.
Clear Logs	 CLEAR LOGS	Clears all of the logged messages from the WXA appliance. **NOTE:** This action cannot be reversed.
Filter by		Filter the results by selecting from the drop-down lists and entering text in text fields: **ID, Priority, Category,** and **Message.** The filters you select determine which of the log entries retrieved from the WXA series appliance are displayed on the **Log** screen.

Data from Selected WXAs

Toward the tops of the WAN Acceleration Logs, at **Logs > WAN Acceleration Logs**, there is a pane labeled **Data from Selected WXAs**.



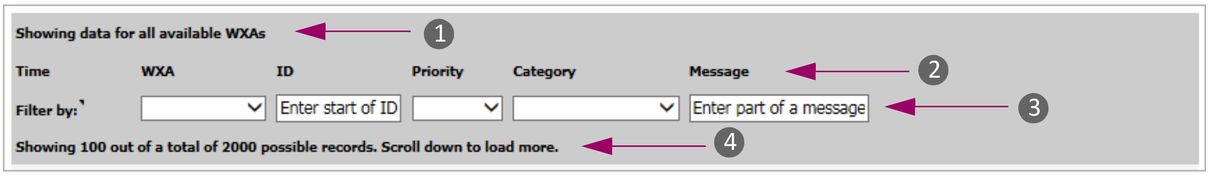
When you click the expansion arrow, the pane expands to reveal information about the selected WXAs in the infrastructure. It also shows the load status of the WXA.



WXA	Load Status
WXA2000-5B6E87A	✓

Filtering WAN Acceleration Logs

The header for the log table is designed to provide basic information about the logs and to let you filter the logs.


Showing data for all available WXAs

Time WXA ID Priority Category Message

Filter by: Enter start of ID Enter part of a message

Showing 100 out of a total of 2000 possible records. Scroll down to load more.

1 The top line of the header section tells what WXAs are included in the WAN Acceleration Logs. In this example all the WXAs are being displayed.

2 These are the headings for the table.

3 These are the **Filter by** fields you can use to customize the views of the WAN Acceleration Logs.

Field	Definition	
WXA	Allows you to select an WXA to filter on.	
ID	Enter the first few numbers of the ID and the log data is immediately filtered on those values. Click the **X** on the right side of the field to clear it. You might need to refresh your screen to clear the filtering. The ID number ranges for the WXA components are:	
	10000-19999	WXA System
	20000-29999	WXA System Network
	30000-39999	TCP Acceleration
	40000-49999	Unsigned WFS
	50000-59999	Signed WFS
	60000-69999	Web Cache
	70000-79999	Management
Priority	Allows you to select a priority level to filter on. Options include: **Error**, **Info**, **Notice**, and **Warning**. To clear the filter, select the blank option.	
Category	Allows you to select a log category to filter on. To clear the filter, select the blank option.	
Message	Enter letters or words from any part of the message to filter on. For example, if you enter *monitor*, the log is filtered to so all messages with the term *monitor* in it. Click the **X** on the right side of the field to clear it. You might need to refresh your screen to clear the filtering.	

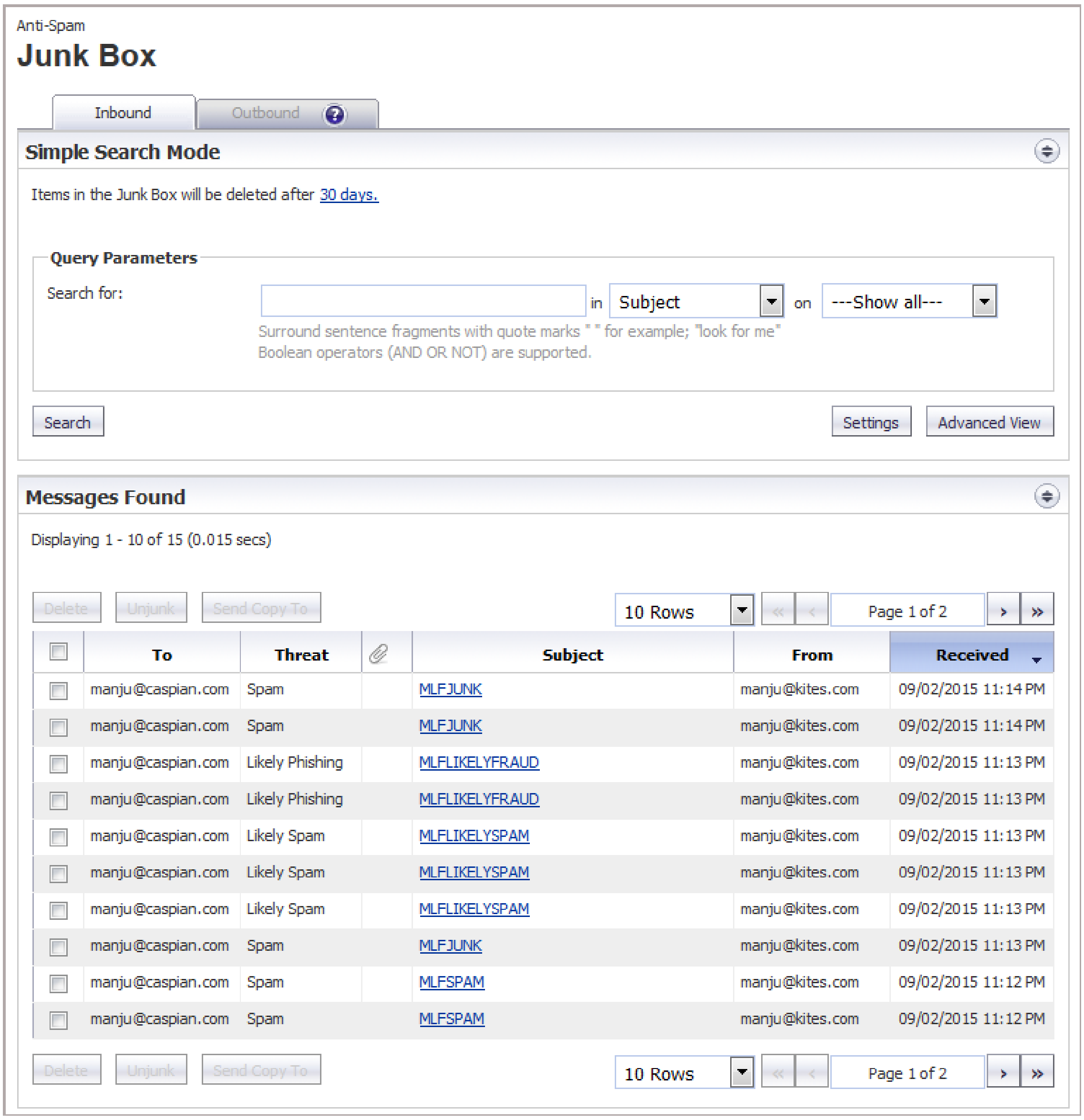
4 The bottom line of the header section tells how many records are being displayed. It tells you to scroll down if you have more logs than your screen can currently display. It also changes as you filter the logs so you can see how many logs there are each time you change filter parameters.

Anti-Spam Junkbox

The Anti-Spam feature provides a quick, efficient, and effective way to add anti-spam, anti-phishing, and anti-virus capabilities to your existing firewall. In a typical Anti-Spam configuration, you choose to add Anti-Spam capabilities by selecting it in the SonicOS interface and licensing it. The firewall then uses advanced spam-filtering technology to reduce the amount of junk email delivered to users.

View the Anti-Spam Junkbox to view, search and manage that are currently in the Junk Store on the Exchange or SMTP server. Navigate to **Logs > Anti-Spam Junkbox** on the **INVESTIGATE** view.

ⓘ **NOTE:** This functionality is only available if the Junk Store is installed.



Anti-Spam

Junk Box

Inbound | Outbound

Simple Search Mode

Items in the Junk Box will be deleted after 30 days.

Query Parameters

Search for: [ ] in Subject on ---Show all---

Surround sentence fragments with quote marks " " for example; "look for me"
Boolean operators (AND OR NOT) are supported.

Messages Found

Displaying 1 - 10 of 15 (0.015 secs)

□	To	Threat		Subject	From	Received
□	manju@caspian.com	Spam		MLFJUNK	manju@kites.com	09/02/2015 11:14 PM
□	manju@caspian.com	Spam		MLFJUNK	manju@kites.com	09/02/2015 11:14 PM
□	manju@caspian.com	Likely Phishing		MLFLIKELYFRAUD	manju@kites.com	09/02/2015 11:13 PM
□	manju@caspian.com	Likely Phishing		MLFLIKELYFRAUD	manju@kites.com	09/02/2015 11:13 PM
□	manju@caspian.com	Likely Spam		MLFLIKELYSPAM	manju@kites.com	09/02/2015 11:13 PM
□	manju@caspian.com	Likely Spam		MLFLIKELYSPAM	manju@kites.com	09/02/2015 11:13 PM
□	manju@caspian.com	Likely Spam		MLFLIKELYSPAM	manju@kites.com	09/02/2015 11:13 PM
□	manju@caspian.com	Spam		MLFJUNK	manju@kites.com	09/02/2015 11:13 PM
□	manju@caspian.com	Spam		MLFSPAM	manju@kites.com	09/02/2015 11:12 PM
□	manju@caspian.com	Spam		MLFSPAM	manju@kites.com	09/02/2015 11:12 PM

Topics:

- Navigating the Junk Box
- Managing Messages
- Performing a Simple Search
- Performing an Advanced Search

Navigating the Junk Box

The Anti-Spam Junk Box has several tabs, buttons and icons you can use to manage and view the data.

- **Inbound** tab lists only the inbound messages.
- **Outbound** tab lists only the outbound messages.

> ⓘ **NOTE:** If you cannot see the **Outbound** view, you must upgrade your Junk Store license. Click the **Question Mark** icon for more information.

The function and display of the two views are the same. Each tab contains two sections:

- **Simple/Advanced Search Mode**
- **Messages Found**

Collapse or expand either section by clicking its **Expand/Collapse** icon.

In the **Simple Search Mode** section are two links to other pages:

- Click the link at the end of **Items in the Junk Box will be deleted after 30 days** to change how long junk mail is kept before being deleted. You are taken to the **Security Configuration > Anti-spam > Junkbox Settings** page on the **MANAGE** view where you can make the change.
- Click **Settings** at the bottom of the section to display the **Anti-Spam > Settings** page. You are taken to the **Security Configuration > Anti-spam > Junkbox Settings** page on the **MANAGE** view where you can make the change.

Managing Messages

The **Messages Found** table displays information about the messages quarantined in the Junk Box.

This column	Contains or indicates
Checkbox	Checkbox for each item in the table. Checking the box next a message selects it for action. If you check the box in the heading selects all items in the table.
To	Recipient’s email address.
Threat	Type of threat the email poses.
Paper clip icon	Email has attachments.
Subject	Subject line of the email.
From	Sender’s email address.
Received	Date the email was sent.

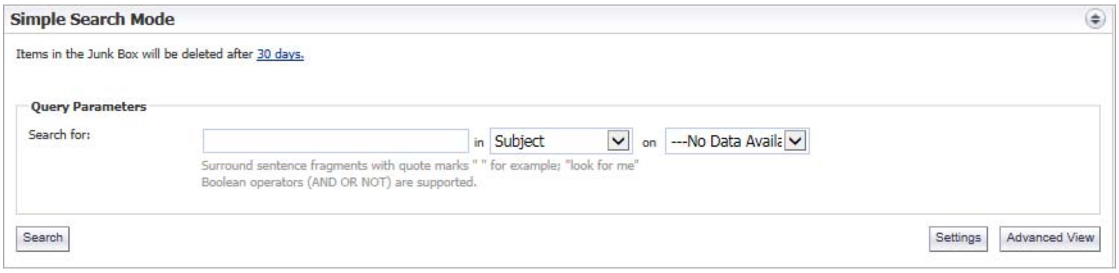
Use the buttons at the top of the **Messages Found** table to complete the following Junk Box management tasks:

Button	Function
Delete	Permanently delete the selected message(s) from the Junk Box; to delete all messages click the checkbox in the table heading.
Unjunk	Remove the selected message(s) from the Junk Box and deliver them to the user(s) to whom they are addressed. The delivery time and date are set by the Exchange server when each message is delivered to the user mailbox.
Send Copy To	Keep the selected message(s) in the Junk Box and send a copy of it (them) to a user.

Performing a Simple Search

To perform a Simple Search of the Junk Box data:

1. Navigate to **Logs > Anti-Spam Junkbox** on the **INVESTIGATE** view.
2. Select either the **Inbound** tab or the **Outbound** tab.



Simple Search Mode

Items in the Junk Box will be deleted after 30 days.

Query Parameters

Search for: in Subject on ---No Data Avail

Surround sentence fragments with quote marks " " for example; "look for me"
Boolean operators (AND OR NOT) are supported.

3. Type a search string in the **Search for** field. Surround sentence fragments with quotation marks (“). Boolean operators (AND, OR, NOT) can be used.
4. Select the desired email field in which to search from **in**:
   - **Subject** (default)
   - **From**
   - **To**
   - **Unique Message ID**
5. From **on**, select a date to search:
   - **---Show all---** (default)
   - **Today**
   - A particular date; the number of dates vary, depending on the length of time junk messages are held
6. Click **Search** to complete the search.

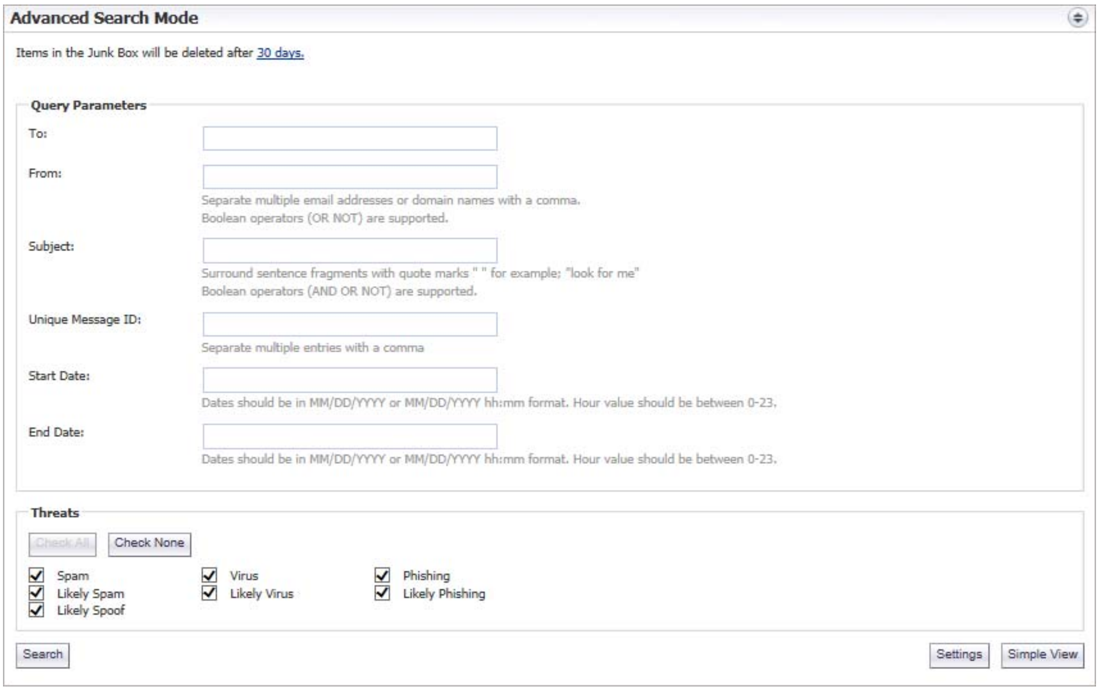
   The results are displayed in the **Messages Found** section of the page, and a message is displayed at the top. If the search is successful, the message contains the word, **Success!**, and the entire message is highlighted in green. If a search is not successful, it contains the word, **Warning!**, and the entire message is highlighted in yellow.
7. To return the **Messages Found** table to its original state:
   a. Delete the data from the **Search for** field.
   b. Click **Search**.

Performing an Advanced Search

1 Navigate to **Logs > Anti-Spam Junkbox** on the **INVESTIGATE** view.

2 Select either the **Inbound** tab or the **Outbound** tab.

3 Click **Advanced View**.



Advanced Search Mode

Items in the Junk Box will be deleted after 30 days.

Query Parameters

To:

From:

Separate multiple email addresses or domain names with a comma.
Boolean operators (OR NOT) are supported.

Subject:

Surround sentence fragments with quote marks " " for example: "look for me"
Boolean operators (AND OR NOT) are supported.

Unique Message ID:

Separate multiple entries with a comma

Start Date:

Dates should be in MM/DD/YYYY or MM/DD/YYYY hh:mm format. Hour value should be between 0-23.

End Date:

Dates should be in MM/DD/YYYY or MM/DD/YYYY hh:mm format. Hour value should be between 0-23.

Threats

☑ Spam
☑ Likely Spam
☑ Likely Spoof
☑ Virus
☑ Likely Virus
☑ Phishing
☑ Likely Phishing

4 In the **Query Parameters** section, enter your search criteria in one or more of the **Query Parameter** fields:

Parameter	Query criteria
To	Recipient's email address.
From	Sender's email address. Separate multiple email addresses or domain names with commas. Boolean operators OR and NOT are both supported.
Subject	Subject of the email. Enclose sentence fragments with quotation marks ("). Boolean operators AND, OR, and NOT are all supported.
Unique Message ID	Unique message ID. Separate multiple entries with commas.
Start Date	First date to search. Enter dates in either format: • `MM/DD/YYYY` • `MM/DD/YYYY hh:mm` (Hour values should be between 0 and 23 [24-hour clock])

Parameter	Query criteria
End Date	Last date to search. Enter dates in either format: • `MM/DD/YYYY` • `MM/DD/YYYY hh:mm` (Hour values should be between 0 and 23 [24-hour clock])

5 In the **Threats** section, specify the threat categories for which to search. By default, all categories are selected.

Deselect any category you do not want to include in the search by clearing the checkbox. To deselect all categories, click **Check None**. All the categories become unchecked, **Check All** becomes active, and **Check None** becomes dimmed.

6 Click **Search** to complete the search.

The results are displayed in the **Messages Found** section of the page, and a message is displayed at the top. If the search is successful, the message contains the word, **Success!**, and the entire message is highlighted in green. If a search is not successful, it contains the word, **Warning!**, and the entire message is highlighted in yellow.

7 To return to the **Simple View**, click **Simple View**.

8 To return the **Messages Found** table to its original state:

a Delete the data from the **Search for** field.

b Click **Search**.

Part 2

INVESTIGATE | Reports

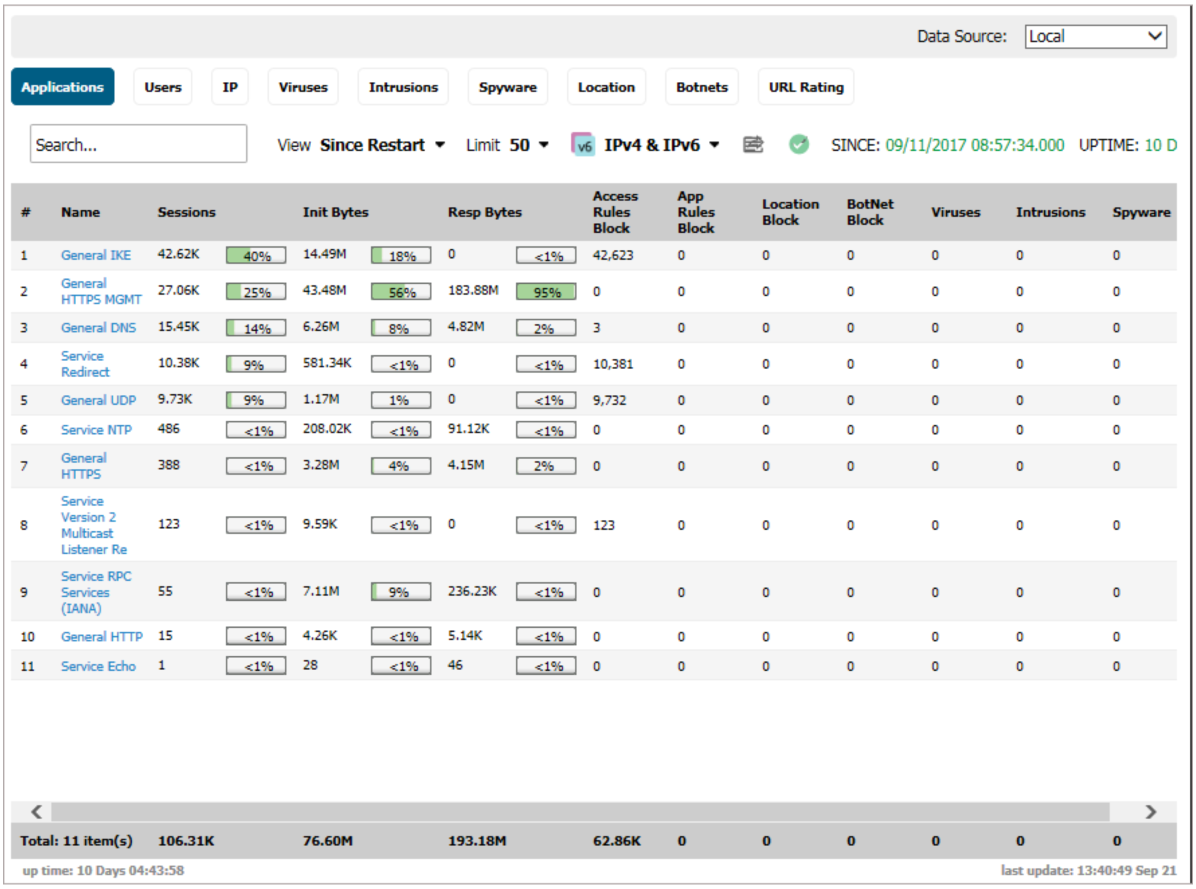
- Appflow Reports
- Log Reports
- RF Analysis
- TCP Acceleration Reports
- WFS Acceleration Reports
- WXA Web Cache Reports
- Capture Threat Assessment

6

Appflow Reports

The **Appflow Reports** page provides configurable scheduled reports by applications, users, IP addresses, viruses, intrusions, spyware, locations, botnets, and URL rating. Appflow Reports statistics enable you to view a top-level aggregate report of what is going on in your network and, at a quick glance, answer such questions as the following:

- What are the top-most used applications running in my network?
- Which applications in terms of total number of sessions and bytes consume my network bandwidth?
- Which applications have viruses, intrusions, and spyware?
- What website categories are my users visiting?



View **Since Restart** Limit **50** **IPv4 & IPv6** SINCE: 09/11/2017 08:57:34.000 UPTIME: 10 D

#	Name	Sessions		Init Bytes		Resp Bytes		Access Rules Block	App Rules Block	Location Block	BotNet Block	Viruses	Intrusions	Spyware
1	General IKE	42.62K	40%	14.49M	18%	0	<1%	42,623	0	0	0	0	0	0
2	General HTTPS MGMT	27.06K	25%	43.48M	56%	183.88M	95%	0	0	0	0	0	0	0
3	General DNS	15.45K	14%	6.26M	8%	4.82M	2%	3	0	0	0	0	0	0
4	Service Redirect	10.38K	9%	581.34K	<1%	0	<1%	10,381	0	0	0	0	0	0
5	General UDP	9.73K	9%	1.17M	1%	0	<1%	9,732	0	0	0	0	0	0
6	Service NTP	486	<1%	208.02K	<1%	91.12K	<1%	0	0	0	0	0	0	0
7	General HTTPS	388	<1%	3.28M	4%	4.15M	2%	0	0	0	0	0	0	0
8	Service Version 2 Multicast Listener Re	123	<1%	9.59K	<1%	0	<1%	123	0	0	0	0	0	0
9	Service RPC Services (IANA)	55	<1%	7.11M	9%	236.23K	<1%	0	0	0	0	0	0	0
10	General HTTP	15	<1%	4.26K	<1%	5.14K	<1%	0	0	0	0	0	0	0
11	Service Echo	1	<1%	28	<1%	46	<1%	0	0	0	0	0	0	0
Total: 11 item(s)		106.31K		76.60M		193.18M		62.86K	0	0	0	0	0	0

up time: 10 Days 04:43:58 last update: 13:40:49 Sep 21

The report data can be viewed from the point of the last system restart, since the system reset, or by defining a schedule range. Reports also can be sent by FTP or by email.

ⓘ **TIP:** The **Dashboard > Appflow Dash** page displays the top ten items in each category (except IP addresses) in graph format.

To configure your Appflow Reports, follow the procedures described in *SonicWall SonicOS 6.5 Log and Reports* for **Logs & Reporting > Appflow Settings > Flow Reporting**.

The bottom of the page displays the:

- Totals for each column, such as number of entries, number of bytes sent by the initiator and responder, locations blocked
- Total up time of the appliance in days, hours, minutes, and seconds
- Time of the last update/reset: hour, minute, second, month, and day

Topics:

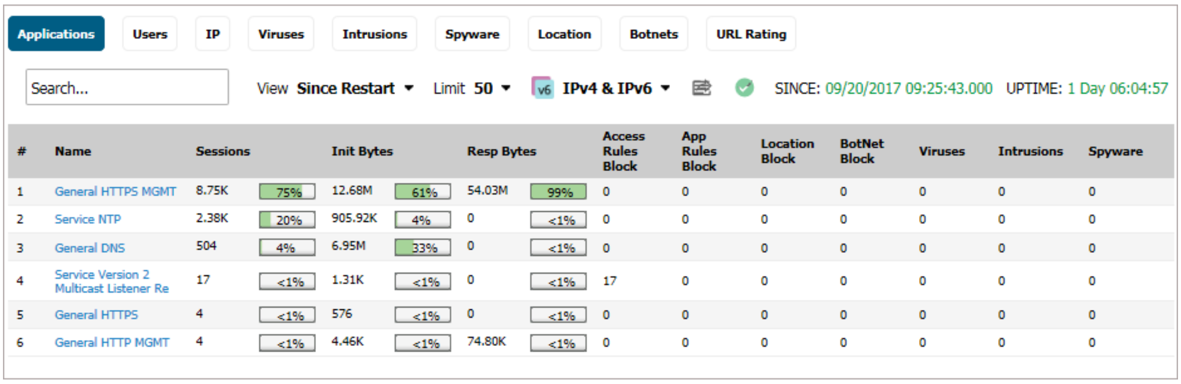
- Appflow Reports on page 34
- Common Functions on page 38
- Viewing Appflow Data on page 39
- Downloading Appflow Reports on page 42

Appflow Reports

The **Reports > Appflow Reports** page displays these reports on separate views. Click the view name to see the view you want.

- Applications on page 34
- Users on page 35
- IP on page 35
- Viruses on page 36
- Intrusions on page 36
- Spyware on page 36
- Location on page 37
- Botnets on page 37
- URL Rating on page 38

Applications



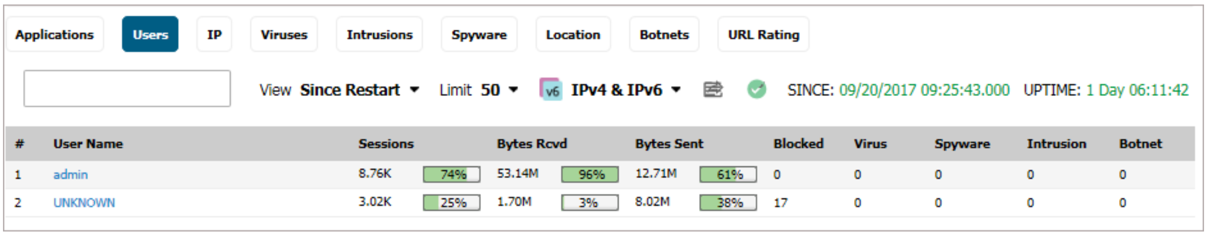
View Since Restart ▾ Limit 50 ▾ IPv4 & IPv6 ▾ SINCE: 09/20/2017 09:25:43.000 UPTIME: 1 Day 06:04:57

#	Name	Sessions		Init Bytes		Resp Bytes		Access Rules Block	App Rules Block	Location Block	BotNet Block	Viruses	Intrusions	Spyware
1	General HTTPS MGMT	8.75K	75%	12.68M	61%	54.03M	99%	0	0	0	0	0	0	0
2	Service NTP	2.38K	20%	905.92K	4%	0	<1%	0	0	0	0	0	0	0
3	General DNS	504	4%	6.95M	33%	0	<1%	0	0	0	0	0	0	0
4	Service Version 2 Multicast Listener Re	17	<1%	1.31K	<1%	0	<1%	17	0	0	0	0	0	0
5	General HTTPS	4	<1%	576	<1%	0	<1%	0	0	0	0	0	0	0
6	General HTTP MGMT	4	<1%	4.46K	<1%	74.80K	<1%	0	0	0	0	0	0	0

- **Name**—Name of the application, the signature ID
- **Sessions**—Number of connections/flows both as a number and as a percentage

- **Init Bytes**—Number of bytes sent by the initiator both as a number and as a percentage
- **Resp Bytes**—Number of bytes sent by the responder both as a number and as a percentage
- **Access Rules Block**—Number of connections/flows blocked by firewall rules
- **App Rules Block**—Number of connections/flows blocked by the DPI engine
- **Location Block**—Number of connections/flows blocked by GEO enforcement
- **Botnet Block**—Number of connections/flows blocked by Botnet enforcement
- **Viruses**—Number of connections/flows with viruses
- **Intrusions**—Number of connections/flows identified as intrusions
- **Spyware**—Number of connections/flows with spyware

Users

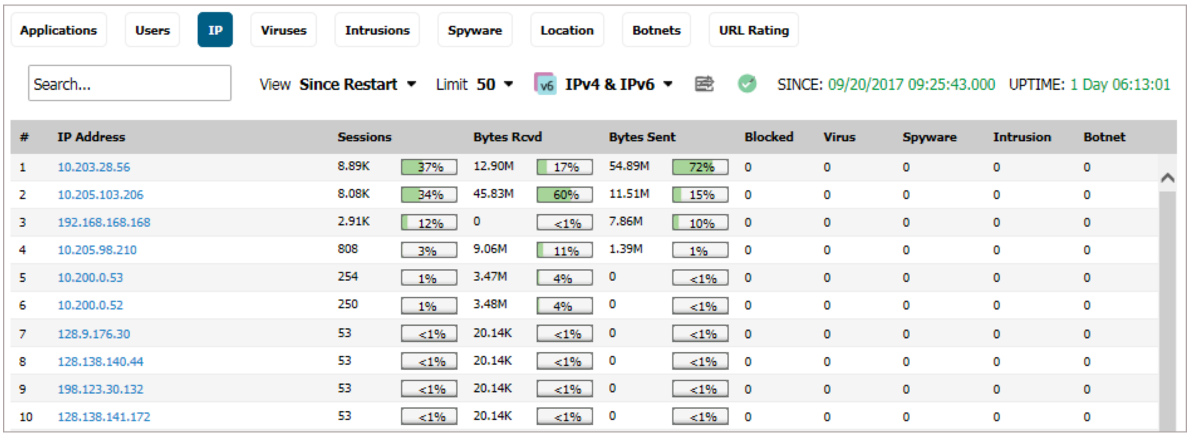


View Since Restart ▾ Limit 50 ▾ v6 IPv4 & IPv6 ▾ SINCE: 09/20/2017 09:25:43.000 UPTIME: 1 Day 06:11:42

#	User Name	Sessions		Bytes Rcvd		Bytes Sent		Blocked	Virus	Spyware	Intrusion	Botnet
1	admin	8.76K	74%	53.14M	96%	12.71M	61%	0	0	0	0	0
2	UNKNOWN	3.02K	25%	1.70M	3%	8.02M	38%	17	0	0	0	0

- **User Name**—Name of the user
- **Sessions**—Number of sessions/connections initiated/responded both as a number and as a percentage
- **Bytes Rcvd**—Number of bytes received by the user both as a number and as a percentage
- **Bytes Sent**—Number of bytes sent by the user both as a number and as a percentage
- **Blocked**—Number of sessions/connections blocked
- **Virus**—Number of sessions/connections detected with a virus
- **Spyware**—Number of sessions/connections detected with spyware
- **Intrusion**—Number of sessions/connections detected as intrusions

IP

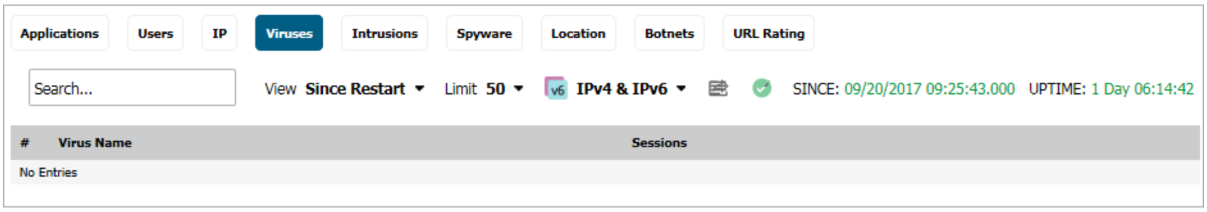


Search... View Since Restart ▾ Limit 50 ▾ v6 IPv4 & IPv6 ▾ SINCE: 09/20/2017 09:25:43.000 UPTIME: 1 Day 06:13:01

#	IP Address	Sessions		Bytes Rcvd		Bytes Sent		Blocked	Virus	Spyware	Intrusion	Botnet
1	10.203.28.56	8.89K	37%	12.90M	17%	54.89M	72%	0	0	0	0	0
2	10.205.103.206	8.08K	34%	45.83M	60%	11.51M	15%	0	0	0	0	0
3	192.168.168.168	2.91K	12%	0	<1%	7.86M	10%	0	0	0	0	0
4	10.205.98.210	808	3%	9.06M	11%	1.39M	1%	0	0	0	0	0
5	10.200.0.53	254	1%	3.47M	4%	0	<1%	0	0	0	0	0
6	10.200.0.52	250	1%	3.48M	4%	0	<1%	0	0	0	0	0
7	128.9.176.30	53	<1%	20.14K	<1%	0	<1%	0	0	0	0	0
8	128.138.140.44	53	<1%	20.14K	<1%	0	<1%	0	0	0	0	0
9	198.123.30.132	53	<1%	20.14K	<1%	0	<1%	0	0	0	0	0
10	128.138.141.172	53	<1%	20.14K	<1%	0	<1%	0	0	0	0	0

- **IP Address**—
- **Sessions**—Number of sessions/connections initiated/responded both as a number and as a percentage
- **Bytes Rcvd**—Number of bytes received by this IP address both as a number and as a percentage
- **Bytes Sent**—Number of bytes sent by this IP address both as a number and as a percentage
- **Blocked**—Number of sessions/connections blocked
- **Virus**—Number of sessions/connections detected with a virus
- **Spyware**—Number of sessions/connections detected with spyware
- **Intrusion**—Number of sessions/connections detected as intrusion

Viruses

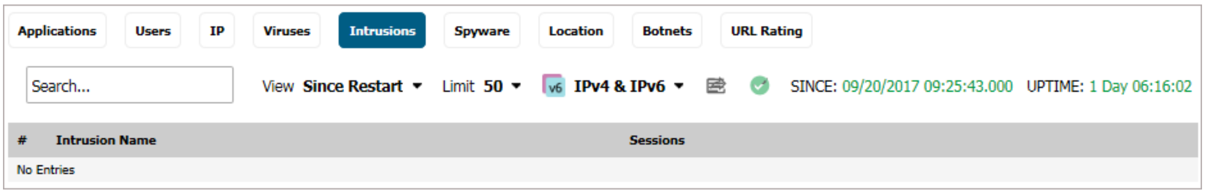


View **Since Restart** Limit **50** **IPv4 & IPv6** SINCE: 09/20/2017 09:25:43.000 UPTIME: 1 Day 06:14:42

#	Virus Name	Sessions
No Entries		

- **Virus Name**—
- **Sessions**—Number of sessions/connections with this virus

Intrusions

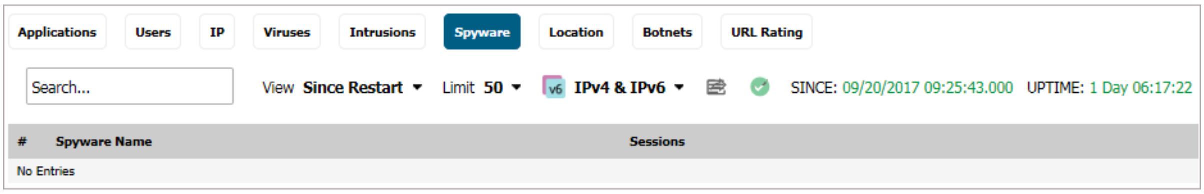


View **Since Restart** Limit **50** **IPv4 & IPv6** SINCE: 09/20/2017 09:25:43.000 UPTIME: 1 Day 06:16:02

#	Intrusion Name	Sessions
No Entries		

- **Intrusion Name**—
- **Sessions**—Number of sessions/connections detected as an intrusion

Spyware

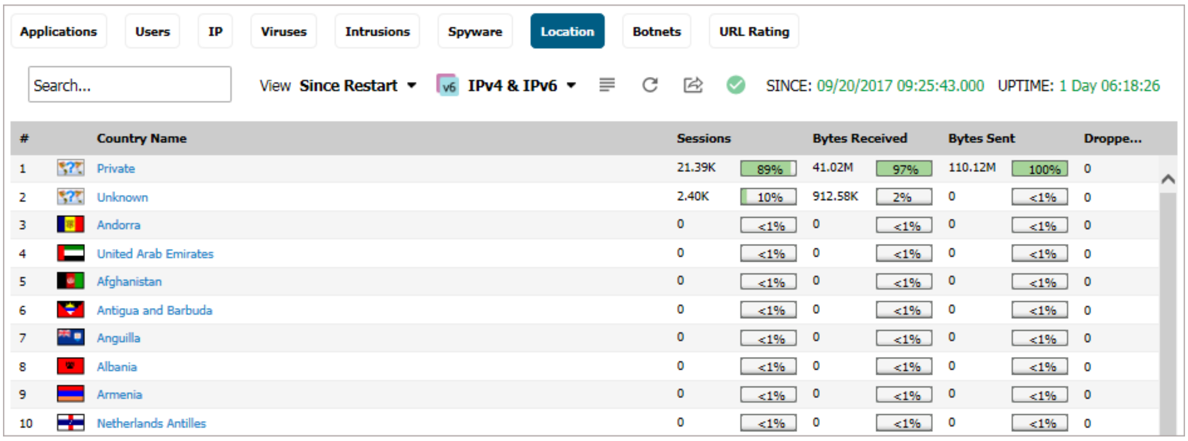


View **Since Restart** Limit **50** **IPv4 & IPv6** SINCE: 09/20/2017 09:25:43.000 UPTIME: 1 Day 06:17:22

#	Spyware Name	Sessions
No Entries		

- **Spyware Name**—Name of the spyware signature
- **Sessions**—Number of sessions/connections with this spyware

Location

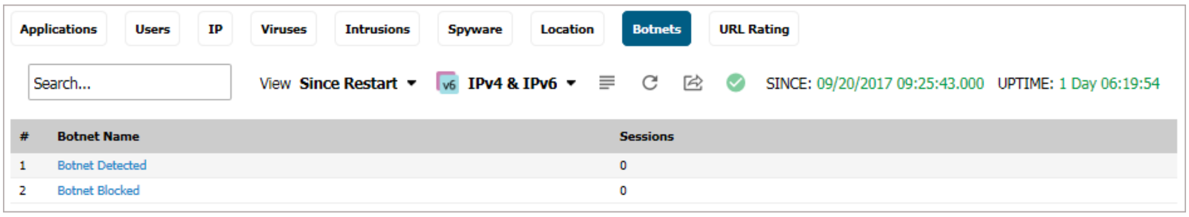


View Since Restart ▾ IPv4 & IPv6 ▾ SINCE: 09/20/2017 09:25:43.000 UPTIME: 1 Day 06:18:26

#	Country Name	Sessions		Bytes Received		Bytes Sent		Droppe...
1	Private	21.39K	89%	41.02M	97%	110.12M	100%	0
2	Unknown	2.40K	10%	912.58K	2%	0	<1%	0
3	Andorra	0	<1%	0	<1%	0	<1%	0
4	United Arab Emirates	0	<1%	0	<1%	0	<1%	0
5	Afghanistan	0	<1%	0	<1%	0	<1%	0
6	Antigua and Barbuda	0	<1%	0	<1%	0	<1%	0
7	Anguilla	0	<1%	0	<1%	0	<1%	0
8	Albania	0	<1%	0	<1%	0	<1%	0
9	Armenia	0	<1%	0	<1%	0	<1%	0
10	Netherlands Antilles	0	<1%	0	<1%	0	<1%	0

- **Country Name**—Name and flag of the country initiating/responding to a session/connection
- **Sessions**—Number of sessions/connections initiated/responded by this country both as a number and as a percentage
- **Bytes Rcvd**—Number of data bytes received by this country both as a number and as a percentage
- **Bytes Sent**—Number of data bytes sent by this country both as a number and as a percentage
- **Dropped**—Number of sessions/connections dropped

Botnets

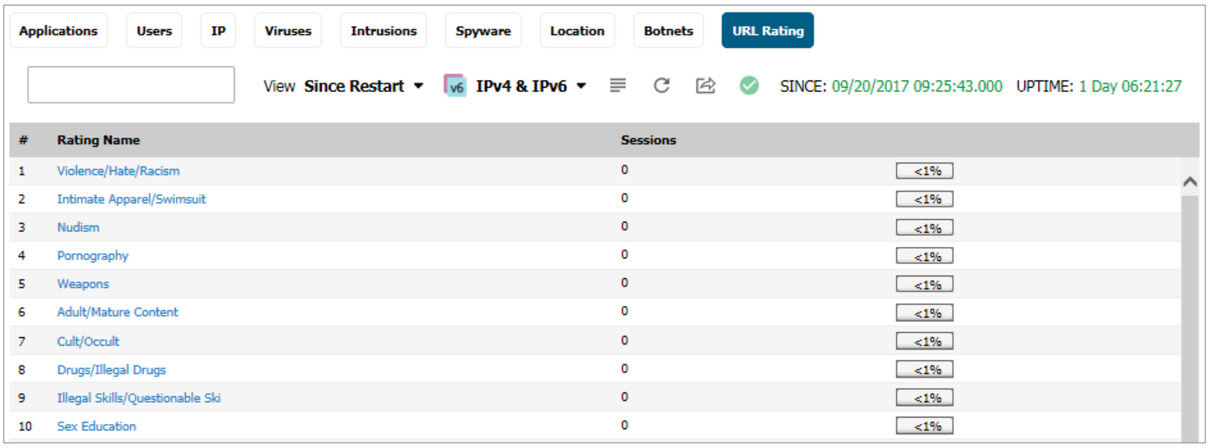


View Since Restart ▾ IPv4 & IPv6 ▾ SINCE: 09/20/2017 09:25:43.000 UPTIME: 1 Day 06:19:54

#	Botnet Name	Sessions
1	Botnet Detected	0
2	Botnet Blocked	0

- **Botnet Name**:
  - **Botnet Detected**—
  - **Botnet Blocked**—
- **Sessions**—Number of sessions/connections where a botnet was detected/blocked

URL Rating



View Since Restart ▾ IPv4 & IPv6 ▾ SINCE: 09/20/2017 09:25:43.000 UPTIME: 1 Day 06:21:27

#	Rating Name	Sessions	
1	Violence/Hate/Racism	0	<1%
2	Intimate Apparel/Swimsuit	0	<1%
3	Nudism	0	<1%
4	Pornography	0	<1%
5	Weapons	0	<1%
6	Adult/Mature Content	0	<1%
7	Cult/Occult	0	<1%
8	Drugs/Illegal Drugs	0	<1%
9	Illegal Skills/Questionable Ski	0	<1%
10	Sex Education	0	<1%

- **Rating Name**—Name of the URL category
- **Sessions**—Number of sessions/connections both as a number and as a percentage

Common Functions

Topics:

- Specifying the Data Source on page 38
- Downloading SonicWall Security Services Signatures on page 38
- Limiting the Number of Entries Displayed on page 39
- Creating a CSV File on page 39

Specifying the Data Source

Select the source of the report data in the **Data Source** drop-down menu:

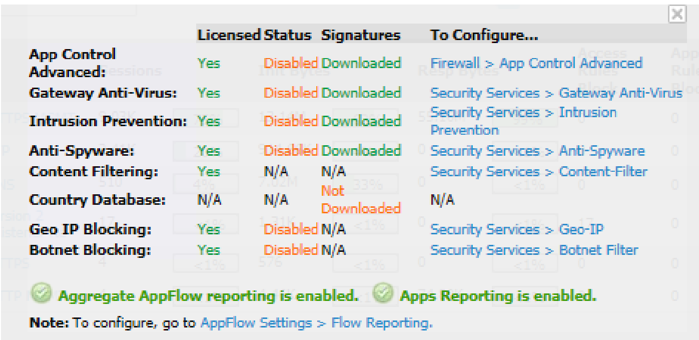
Data Source: Local

- **Local** (default)
- **Appflow Server**, if available
- **GMSFlow Server**, if available

Downloading SonicWall Security Services Signatures

The **Appflow Reports** feature requires that you enable the latest SonicWall Security Services signature downloads. That way you have the latest dynamic protection updates.

Click the **Status** icon on any tab to view the list of enabled SonicWall Security Services:



	Licensed	Status	Signatures	To Configure...
App Control Advanced:	Yes	Disabled	Downloaded	Firewall > App Control Advanced
Gateway Anti-Virus:	Yes	Disabled	Downloaded	Security Services > Gateway Anti-Virus
Intrusion Prevention:	Yes	Disabled	Downloaded	Security Services > Intrusion Prevention
Anti-Spyware:	Yes	Disabled	Downloaded	Security Services > Anti-Spyware
Content Filtering:	Yes	N/A	N/A	Security Services > Content-Filter
Country Database:	N/A	N/A	Not Downloaded	N/A
Geo IP Blocking:	Yes	Disabled	N/A	Security Services > Geo-IP
Botnet Blocking:	Yes	Disabled	N/A	Security Services > Botnet Filter

✓ **Aggregate AppFlow reporting is enabled.** ✓ **Apps Reporting is enabled.**

Note: To configure, go to AppFlow Settings > Flow Reporting.

The pop-up displays the following for each service generating an Appflow Report:

- Whether the service is licensed, not licensed, or a license is N/A (not applicable)
- Whether the service is enabled, disabled, or N/A
- Whether the relevant database has been downloaded for the service or NA
- A link to the relevant SonicWall page for configuring the service

Limiting the Number of Entries Displayed

Limit the number of entries displayed in a report by selecting one of these numbers from **Limit**:

- **10**
- **25**
- **50** (default)
- **100**
- **150**
- **Unlimited**

ⓘ **NOTE:** The number of entries for the **Location, Botnets**, and **URL Rating** reports cannot be limited.

Creating a CSV File

Create a CVS file of a particular view by clicking the **Export** icon.

Viewing Appflow Data

From **View**, you can select a view for the Appflow data:

- **Since Restart** shows Appflow data since the last reboot or restart of the firewall. The date and time of the reboot are given in green as well as the total up time, in days, hours, minutes, and seconds, since the reboot. For example, `SINCE: 08/14/2014 15:40:06.000 UPTIME: 32 Days 01:25:10`.

  ⓘ **TIP:** The up time is also displayed at the bottom of the page along with the date and time of the last update.

- **Since Last Reset** shows you the Appflow data since the last reset of the firewall. This report shows the aggregate statistics since the last time you cleared the statistics by pressing **Reset**. The date and time of the reset are given in green as well as the total up time, in days, hours, minutes, and seconds, since the reset.

  The reset option allows you to quickly view Appflow Report statistics from a fresh reset of network flows. The reset clears the counters seen at the bottom of the page that displays counter totals for the number of sessions, initiator and responder bytes, to the number of intrusions and threats.

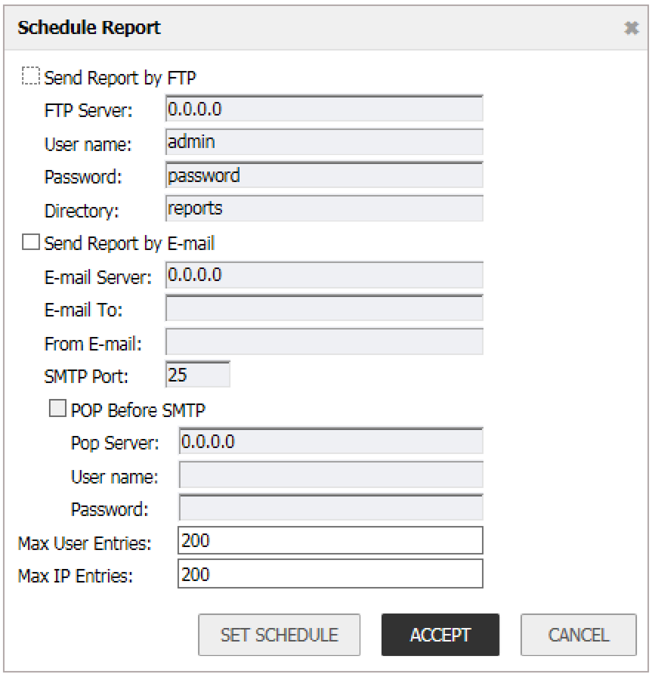
- **On Schedule** shows Appflow data by a defined schedule start and end time. This report shows Appflow statistics collected during the time range specified in the configure settings options. After the end time of the schedule is reached, scheduled Appflow statistics are exported automatically to an FTP server or an email server. Appflow statistical data is exported in CSV file format. After the Appflow statistics are exported, the data is refreshed and cleared.

To configure an On Schedule Appflow report:

1 Navigate to **Reports > Appflow Reports** on the **INVESTIGATE** view.

2 From **View**, choose **On Schedule**.

3 Click the **Configure** icon. The **Schedule Report** dialog displays.



Schedule Report

□ Send Report by FTP

FTP Server: 0.0.0.0

User name: admin

Password: password

Directory: reports

□ Send Report by E-mail

E-mail Server: 0.0.0.0

E-mail To:

From E-mail:

SMTP Port: 25

□ POP Before SMTP

Pop Server: 0.0.0.0

User name:

Password:

Max User Entries: 200

Max IP Entries: 200

4 To send your Appflow Reports automatically, select one or both of these options:

- **Send Report by FTP**
- **Send Report by E-mail**

5 For reports sent by FTP, configure these options:

a Type the FTP server address in the **FTP Server** field.

b Input the user name in the **User name** field; the default is **admin**.

c Input a password in the **Password** field.

d Type the directory name in the **Directory** field, where the reports are sent. The default is **reports**.

6 For reports sent by email, enter these options:

a Type the email server in the **E-Mail Server** field.

b Type recipient's email address in the **E-mail To** field.

c Type the email address used for the sender in the **From E-mail** field.

d Add the SMTP port number to the **SMTP Port** field.

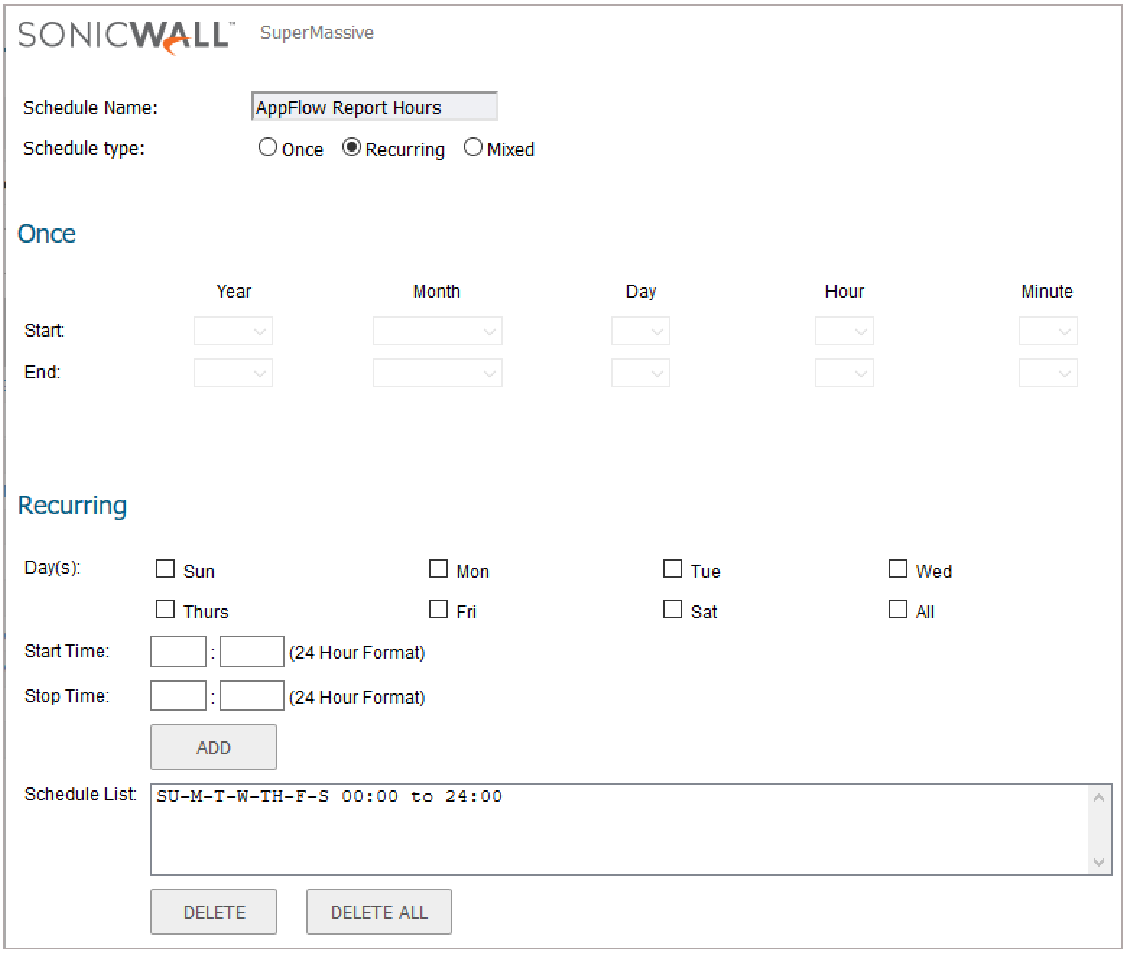
7 If your email server requires SMTP authentication, select **POP Before SMTP** and enter these options.

- Address of the POP server in the **Pop Server** field.
- User name in the **User name** field.
- Password in the **Password** field.

8 Enter the maximum number of user entries in the **Max User Entries** field; the default is **200**.

9 Enter the maximum number of IP entries in the **Max IP Entries** field; the default is **200**.

10 Click **SET SCHEDULE** to define a start and end schedule.



Schedule Name: AppFlow Report Hours

Schedule type: ○ Once ● Recurring ○ Mixed

Once

	Year	Month	Day	Hour	Minute
Start:					
End:					

Recurring

Day(s): □ Sun □ Mon □ Tue □ Wed □ Thurs □ Fri □ Sat □ All

Start Time: : (24 Hour Format)

Stop Time: : (24 Hour Format)

Schedule List: SU-M-T-W-TH-F-S 00:00 to 24:00

11 Type a name in the **Schedule Name** field.

12 From **Schedule type**, choose:

- **Once** – Creates a one-time schedule. The **Once** schedule options allow you to set reporting schedules based on a calendar start and end date with time in hours and minutes.
- **Recurring** – Creates an ongoing scheduled. The **Recurring** schedule options allow to select ongoing schedules based on days of the week and start and end hour and minute time targets. This option is selected by default.

- **Mixed** – Creates both a one-time schedule and an ongoing schedule.

  The **Recurring** and **Mixed** schedules display your selections in the **Schedule List**.

13 If you selected **Recurring** or **Mixed** for the schedule type, complete the schedule times:

- Specify the **day(s)**, **Start Time** and **Stop Time** of the schedule.
- For **Mixed**, in the **Once** section, specify the **Year**, **Month**, **Day**, **Hour**, and **Minute** for the **Start** and **End** of the report.

14 Click **OK** to save your Appflow Reports schedule.

15 On the **Schedule Reports** options page, click **APPLY** to start using your Appflow Reports schedule object settings.

Downloading Appflow Reports

Download the Appflow Reports to one of these formats:

- **CSV** (Microsoft Excel Comma Separated Values File)—opens in Excel as a swarm.csv file

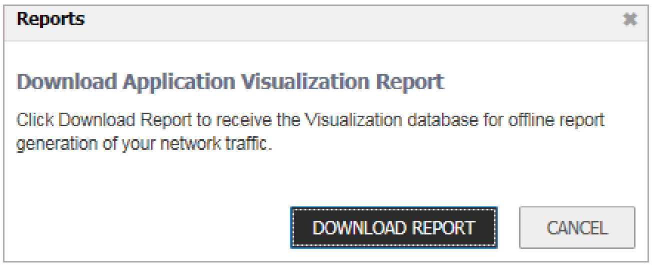
  ⓘ **NOTE:** This is not the same CSV file that is generated by clicking **Create CSV File**.

- **DOC** (Microsoft Word Document)—opens in Word as a swarm.docx file
- **PDF**—opens as an HTML file in the browser window

To download a report:

1 Navigate to **Reports > Appflow Reports** on the **INVESTIGATE** view.

2 Click **Send Report**.



Reports

Download Application Visualization Report

Click Download Report to receive the Visualization database for offline report generation of your network traffic.

3 Click **DOWNLOAD REPORT**. An **Opening *file*.wri.sfr** window displays.

4 Click **Save** to save the file. The file is downloaded to your Downloads folder.

5 Open a browser window.

6 Log on to **MySonicWall.com**.

7 Navigate to **SW Tools > App Reports**. The **Upload Report** page displays.

8 Click **Browse**. A **File Upload** dialog displays.

9 Locate the file.

10 Click **Open**. The file name appears on the **Upload Report** page.

11 Click **Upload**. It might take several minutes to upload the report.

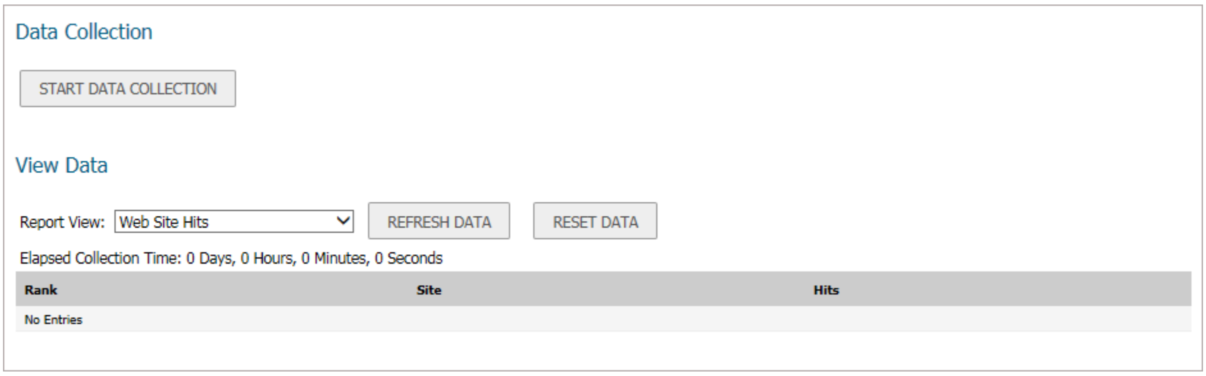
12 When the upload is complete, you can select any or all of these forms (the file has the name **swarm**):

- **CSV**
- **DOC**
- **PDF**

7

Log Reports

The firewall can complete a rolling analysis of the event log to show the top 25 most frequently accessed Web sites, the top 25 users of bandwidth by IP address, and the top 25 services consuming the most bandwidth. Generate these reports from the **Log > Reports** page.



Data Collection

View Data

Report View: Web Site Hits

Elapsed Collection Time: 0 Days, 0 Hours, 0 Minutes, 0 Seconds

Rank	Site	Hits
No Entries		

ⓘ **NOTE:** SonicWall Analyzer provides a comprehensive Web-based reporting solution for firewalls. For more information on SonicWall Analyzer, go to http://www.SonicWall.com.

Topics:

- Data Collection on page 43
- Viewing Data on page 43
- Persistent Logging on page 44

Data Collection

The **Report > Log Reports** page on the **INVESTIGATE** view includes these functions:

- **Data Collection** – Click **START DATA COLLECTION** to begin log analysis. When log analysis is enabled, the button label changes to **STOP DATA COLLECTION**.
- **Refresh Data** – Click **REFRESH DATA** to update the real-time data in the table.
- **View Data** – Click **RESET DATA** to clear the report statistics and begin a new sample period. The sample period is also reset when data collection is stopped or started, and when the firewall is restarted.

Viewing Data

Select the desired report from **Report View**:

- **Web Site Hits** (default)
- **Bandwidth Usage by IP Address**

- **Bandwidth Usage by Service**

The length of time analyzed by the report is displayed in the **Current Sample Period**.

Topics:

Web Site Hits

Selecting **Web Site Hits** from **Report View** displays a table showing the URLs for the 25 most frequently accessed Web sites and the number of hits to a site during the current sample period.

The **Web Site Hits** report ensures that the majority of Web access is to appropriate Web sites. If leisure, sports, or other inappropriate sites appear in the Web Site Hits Report, you can choose to block the sites. For information on blocking inappropriate Web sites refer to the **MANAGE | Security Configuration > Security Services > Content Filter** command in *SonicWall SonicOS 6.5 Security Configuration*.

Bandwidth Usage by IP Address

Selecting Bandwidth **Usage by IP Address** from **Report View** displays a table showing the IP address of the 25 top users of Internet bandwidth and the number of megabytes transmitted during the current sample period.

Bandwidth Usage by Service

Selecting **Bandwidth Usage by Service** from **Report View** displays a table showing the name of the 25 top Internet services, such as HTTP, FTP, RealAudio, and so on, and the number of megabytes received from the service during the current sample period.

The **Bandwidth Usage by Service** report shows whether the services being used are appropriate for your organization. If services such as video or push broadcasts are consuming a large portion of the available bandwidth, you can choose to block these services.

Persistent Logging

The new SonicWall appliances have been enhanced so that more logging information can be retained in an on-board database. It can also preserve the data in the event of a loss of power. These features apply if the appliance has had additional non-volatile storage built into the it and the appliance is running SonicOS 6.5.1 or later.

The maximum number of entries that can be stored on the log database is increased to 50,000 for all platforms, but the amount of space available is driven by the size of the built-in storage module and space allocated for logging. Estimated Storage by NSa Platform describes the estimated values for each of the NS*a* platforms.

Estimated Storage by NSa Platform

Platform	Storage Module Size	Logging Quota	Approximate Number of Backup Files
NS*a* 9650	128 GB	48 GB	3200
NS*a* 9450	128 GB	24 GB	1600
NS*a* 9250	128 GB	24 GB	1600
NS*a* 6650	64 GB	12 GB	800
NS*a* 5650	64 GB	12 GB	800
NS*a* 4650	32 GB	6 GB	400
NS*a* 3650	32 GB	6 GB	400
NS*a* 2650	16 GB	3 GB	200

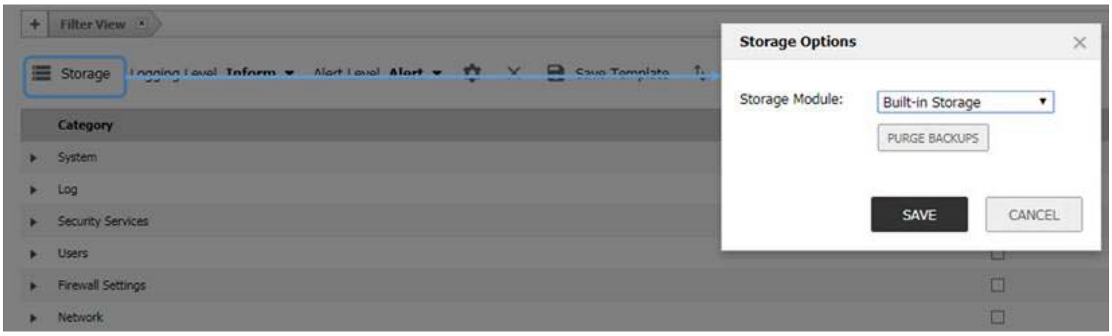
If storage is available, backups of the logs are taken automatically and requires no configuration. They can also be manually deleted.

ⓘ **NOTE:** Loading the Log Reports page can be slower when there are too many entries in the log database. Similarly, exporting a log report can be slower.

To delete backups:

1 Navigate to **MANAGE | Logs & Reporting > Log Settings > Base Setup**.

2 Click the **Storage** icon. The **Storage Options** pop-up displays.



Storage Module: Built-in Storage

3 Select the storage type from **Storage Module**.

4 Click **PURGE BACKUPS**.

5 Click **SAVE**.

For more information, see *SonicWall SonicOS 6.5 Logs and Reports*.

8

RF Analysis

Topics:

RF Analysis Overview

RF Analysis is a feature that helps you understand how wireless channels are utilized by the managed SonicWall access points and all other neighboring wireless access points. This section describes how to use the RF Analysis feature in SonicWall SonicOS to help best utilize the wireless bandwidth with wireless access point appliances.

ⓘ **NOTE:** SonicWall RF Analysis can analyze third-party access points and include these statistics in the RF data as long as at least one SonicWall access point is present and managed through the SonicWall firewall.

Choosing RF Analysis

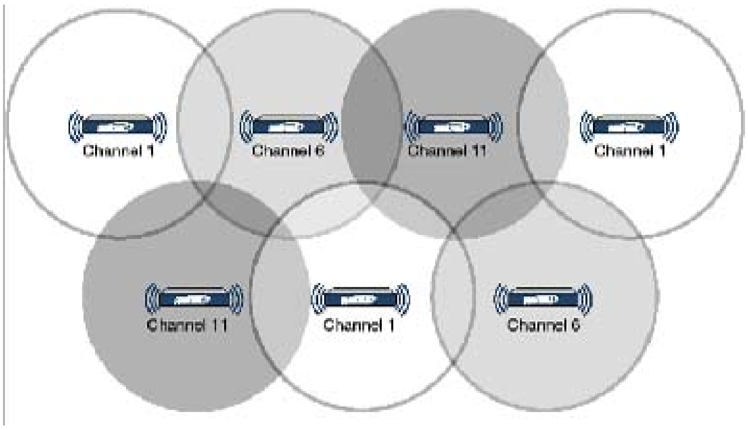
Deploying and maintaining wireless infrastructure can be a daunting task for the network administrator. Wireless issues, such as low performance and poor connectivity are issues that wireless network administrators often face, but ironically, these issues can usually be resolved simply analyzing and properly tuning radio settings.

RFA is a tool that brings awareness to these potential wireless issues. The two main issues that RFA deals with are overloaded channels and SonicWall access point interference with adjacent channels. RF Analysis calculates an RF score for each operational access point and displays the data in a way that allows you to identify access points operating in poor RF environment.

The RF Environment

The IEEE 802.11 specified that devices use ISM 2.4 GHz and 5 GHz bands, and most of the currently deployed wireless devices use the 2.4 GHz band. Because each channel occupies 20 MHz wide spectrum, only three channels out of the 11 available are not overlapping. In the United States, channels 1, 6, and 11 do not overlap. In most cases, these are the three channels used when deploying a large number of SonicWall access points.

SonicPoint Manual Channel Selection



The whole 2.4GHz band is segmented into three separate channels 1, 6, and 11. To achieve this ideal scenario, two factors are necessary: channel allocation and power adjustment. In most scenarios, it is best to assign neighboring SonicPoints to different channels. SonicPoint transmit power should also be watched carefully, as it needs to be strong enough for nearby clients to connect, but not so powerful that causes interference to other SonicPoints operating within the same channel.

Using RF Analysis on SonicWall Access Points

RF Analysis uses scores, graphs, and numbers to assist users to discover and identify potential or existing wireless problems.

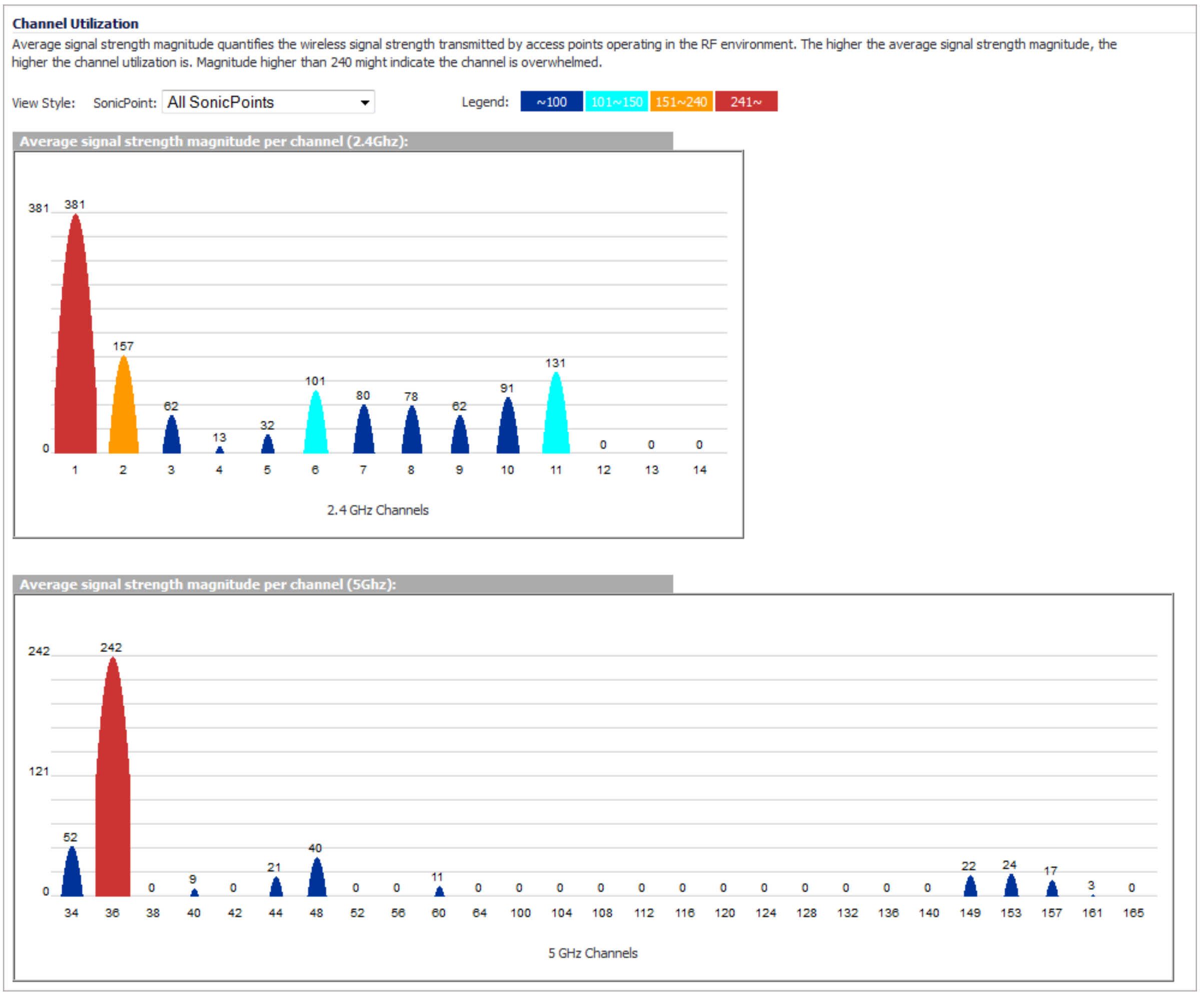
Although the best case scenario is to have the smallest number of access points working in the same channel at any given time, in the real world it is difficult to maintain that, especially when deploying many access points. Also, because the ISM band is free to the public, other devices outside of your control could be operating in that band.

Topics:

- Channel Utilization Graphs and Information on page 48
- Understanding the RF Score on page 49
- Viewing Overloaded Channels on page 49
- RFA Highly Interfered Channels on page 50

Channel Utilization Graphs and Information

Searching for a way to show how a channel is utilized for all connected SonicPoints resulted in channel utilization graphs:



Channel Utilization

Average signal strength magnitude quantifies the wireless signal strength transmitted by access points operating in the RF environment. The higher the average signal strength magnitude, the higher the channel utilization is. Magnitude higher than 240 might indicate the channel is overwhelmed.

View Style: SonicPoint: All SonicPoints

Legend: ~100 101~150 151~240 241~

Two color bars are displayed for each channel. The number on the top of each color bar indicates the number of SonicWall access points that detects the particular issue in that channel. SonicWall access points complete an IDS scan on all available channels upon boot-up, and RF Analysis analyzes these scan results to identify possible issues for each channel.

For example: If 10 SonicWall access points are connected, and 6 of these decide that channel 11 is overloaded, the number on the top of purple color bar is 6; if 8 SonicWall access points decide that channel 6 is highly interfered, the number on the top of the cyan color bar is 8. Zero is shown for channels no issues.

ⓘ **NOTE:** Channels 12, 13, 14 are shown, but in some countries these channels are not used. These channels are still monitored, however, because it is possible for a wireless cracker to set up a wireless jammer in channel 12, 13, or 14 to launch a denial-of-service attack to lower channels.

Understanding the RF Score

RF score is a calculated number on a scale of 1-10 that is used to represent the overall condition for a channel. The higher the score, the better the RF environment is. Low scores indicate that attention is needed.

SonicWall wireless drivers report signal strength in RSSI, this number is used in the preliminary RF score equation to get a raw score on a scale of 1 to 100:

rfaScore100 = 100-((rssiTotal-50)*7/10))

Simplified: *rfaScore100* = -0.7*rssiTotal + 135;

The final score is based on this *rfaScore100*:

- If the RFA score is greater than 96, it is reported as 10.
- If the RFA score is less than 15, it is reported as 1.
- All other scores are divided by 10 to make them fall into the 1-10 scale.

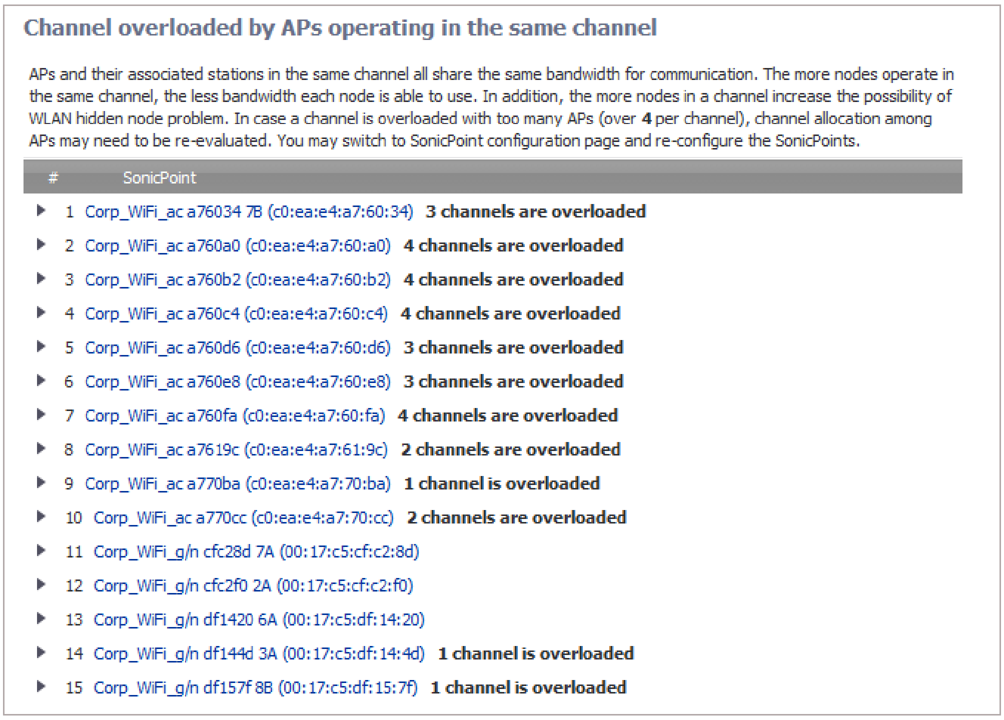
In the SonicOS interface, the RF Score is displayed for the channel that is being used by the SonicWall access points.

NOTE: This feature depends on the knowledge of what channel SonicPoint is operating in. If the channel number is unknown, RF Score is going to be not available.

Viewing Overloaded Channels

RF Analysis gives a warning when it detects more than four active access points in the same channel. No matter how strong its signal strength is, RF Analysis marks the channel as overloaded:

Overloaded Channels



Channel overloaded by APs operating in the same channel

APs and their associated stations in the same channel all share the same bandwidth for communication. The more nodes operate in the same channel, the less bandwidth each node is able to use. In addition, the more nodes in a channel increase the possibility of WLAN hidden node problem. In case a channel is overloaded with too many APs (over **4** per channel), channel allocation among APs may need to be re-evaluated. You may switch to SonicPoint configuration page and re-configure the SonicPoints.

#	SonicPoint	
1	Corp_WiFi_ac a76034 7B (c0:ea:e4:a7:60:34)	**3 channels are overloaded**
2	Corp_WiFi_ac a760a0 (c0:ea:e4:a7:60:a0)	**4 channels are overloaded**
3	Corp_WiFi_ac a760b2 (c0:ea:e4:a7:60:b2)	**4 channels are overloaded**
4	Corp_WiFi_ac a760c4 (c0:ea:e4:a7:60:c4)	**4 channels are overloaded**
5	Corp_WiFi_ac a760d6 (c0:ea:e4:a7:60:d6)	**3 channels are overloaded**
6	Corp_WiFi_ac a760e8 (c0:ea:e4:a7:60:e8)	**3 channels are overloaded**
7	Corp_WiFi_ac a760fa (c0:ea:e4:a7:60:fa)	**4 channels are overloaded**
8	Corp_WiFi_ac a7619c (c0:ea:e4:a7:61:9c)	**2 channels are overloaded**
9	Corp_WiFi_ac a770ba (c0:ea:e4:a7:70:ba)	**1 channel is overloaded**
10	Corp_WiFi_ac a770cc (c0:ea:e4:a7:70:cc)	**2 channels are overloaded**
11	Corp_WiFi_g/n cfc28d 7A (00:17:c5:cf:c2:8d)	
12	Corp_WiFi_g/n cfc2f0 2A (00:17:c5:cf:c2:f0)	
13	Corp_WiFi_g/n df1420 6A (00:17:c5:df:14:20)	
14	Corp_WiFi_g/n df144d 3A (00:17:c5:df:14:4d)	**1 channel is overloaded**
15	Corp_WiFi_g/n df157f 8B (00:17:c5:df:15:7f)	**1 channel is overloaded**

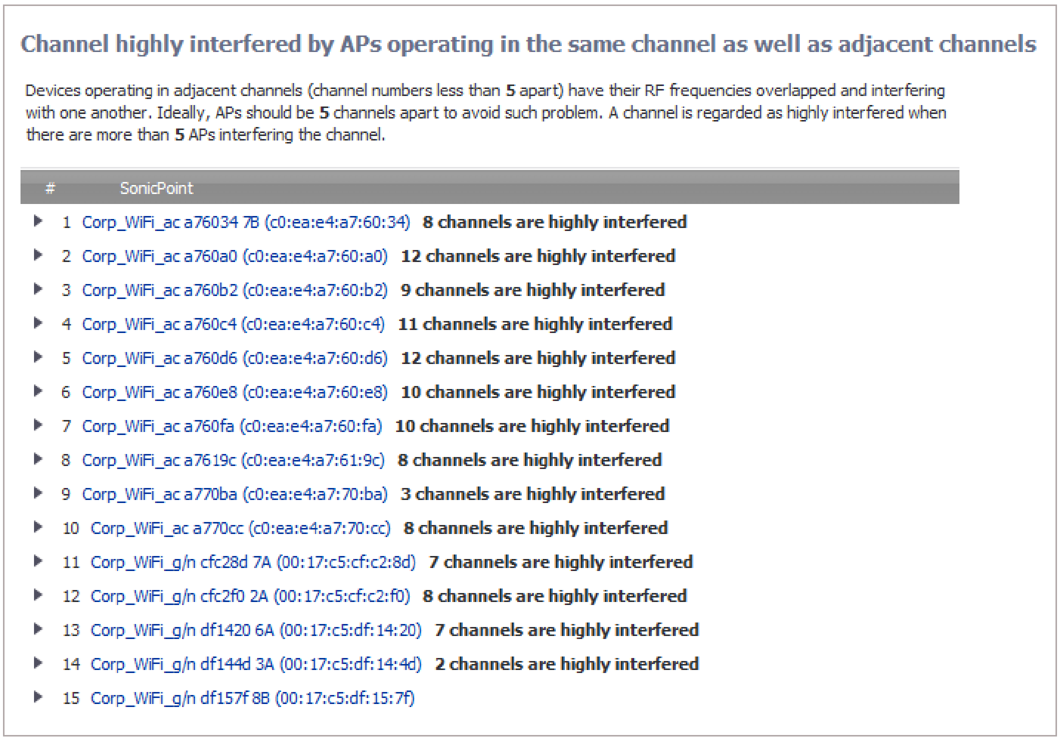
Information about each discovered access point includes: SSID, MAC, signal strength, and channel. Two values are shown for signal strength: dBm and percentage value.

RFA Highly Interfered Channels

Access points working in the same channel can create interference, as access points working in adjacent channels (channel number less than five apart) can also interfere with each other.

RFA delivers a warning when it detects that around a certain SonicPoint, there are more than five active APs in the channels that are less than five apart. No matter how strong their signal strength is, RFA marks the channel as highly interfered.

Highly Interfered Channels



Channel highly interfered by APs operating in the same channel as well as adjacent channels

Devices operating in adjacent channels (channel numbers less than **5** apart) have their RF frequencies overlapped and interfering with one another. Ideally, APs should be **5** channels apart to avoid such problem. A channel is regarded as highly interfered when there are more than **5** APs interfering the channel.

#	SonicPoint	
1	Corp_WiFi_ac a76034 7B (c0:ea:e4:a7:60:34)	**8 channels are highly interfered**
2	Corp_WiFi_ac a760a0 (c0:ea:e4:a7:60:a0)	**12 channels are highly interfered**
3	Corp_WiFi_ac a760b2 (c0:ea:e4:a7:60:b2)	**9 channels are highly interfered**
4	Corp_WiFi_ac a760c4 (c0:ea:e4:a7:60:c4)	**11 channels are highly interfered**
5	Corp_WiFi_ac a760d6 (c0:ea:e4:a7:60:d6)	**12 channels are highly interfered**
6	Corp_WiFi_ac a760e8 (c0:ea:e4:a7:60:e8)	**10 channels are highly interfered**
7	Corp_WiFi_ac a760fa (c0:ea:e4:a7:60:fa)	**10 channels are highly interfered**
8	Corp_WiFi_ac a7619c (c0:ea:e4:a7:61:9c)	**8 channels are highly interfered**
9	Corp_WiFi_ac a770ba (c0:ea:e4:a7:70:ba)	**3 channels are highly interfered**
10	Corp_WiFi_ac a770cc (c0:ea:e4:a7:70:cc)	**8 channels are highly interfered**
11	Corp_WiFi_g/n cfc28d 7A (00:17:c5:cf:c2:8d)	**7 channels are highly interfered**
12	Corp_WiFi_g/n cfc2f0 2A (00:17:c5:cf:c2:f0)	**8 channels are highly interfered**
13	Corp_WiFi_g/n df1420 6A (00:17:c5:df:14:20)	**7 channels are highly interfered**
14	Corp_WiFi_g/n df144d 3A (00:17:c5:df:14:4d)	**2 channels are highly interfered**
15	Corp_WiFi_g/n df157f 8B (00:17:c5:df:15:7f)	

Information about each discovered AP includes: SSID, MAC, signal strength, and channel. Two values are shown for signal strength: dBm and percentage value.

9

TCP Acceleration Reports

Topics:

About Reports > TCP Acceleration Reports

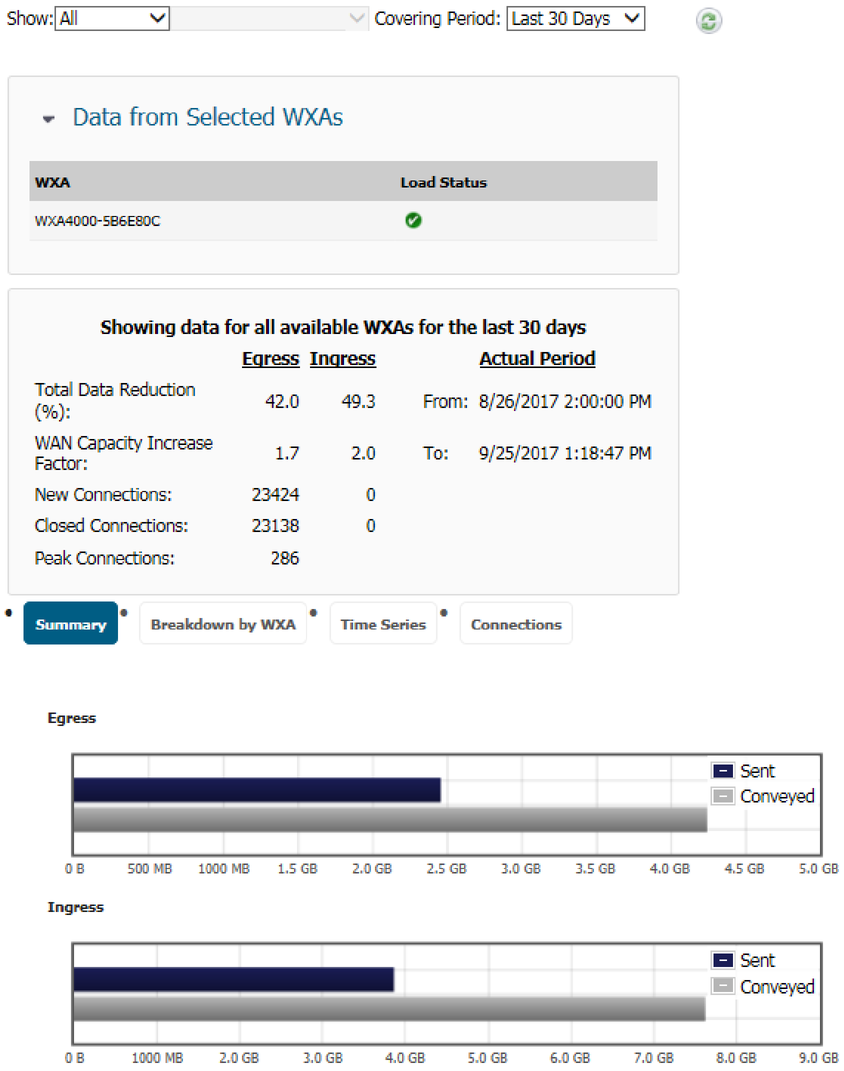
Reports > TCP Acceleration Reports on the **INVESTIGATE** view provides options to view and monitor the TCP Acceleration service on these pages: **Statistics, Breakdown Statistics,** and **Connections**.

Statistics

Navigate to **Reports > TCP Acceleration Reports > Statistics** on the **INVESTIGATE** view to select data from the WAN accelerators in the environment. The Statistics option shows graphs illustrating the following:

- Summary
- Breakdown by WXA
- Time Series

- Connections



Show: All

Covering Period: Last 30 Days

Data from Selected WXAs

WXA	Load Status
WXA4000-5B6E80C	✓

Showing data for all available WXAs for the last 30 days

	Egress	Ingress	Actual Period	
Total Data Reduction (%):	42.0	49.3	From:	8/26/2017 2:00:00 PM
WAN Capacity Increase Factor:	1.7	2.0	To:	9/25/2017 1:18:47 PM
New Connections:	23424	0		
Closed Connections:	23138	0		
Peak Connections:	286			

To set up the report for the Statistics view:

1 In the **Show** field, set the option for what data is displayed. Select from the following:

- **All**
- **For Group:**
- **For WXA:**

If you selected **For Group:** or **For WXA:** and additional field is shown so you can refine your selection further.

2 In the **Covering Period** field, select the period of time the data displays on the Statistics tab. Options include:

- Last hour
- Last 24 hours
- Last 3 days
- Last 5 days

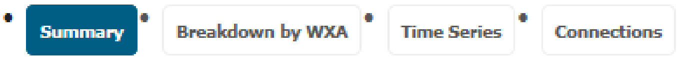
- Last 10 days
- Last 30 days

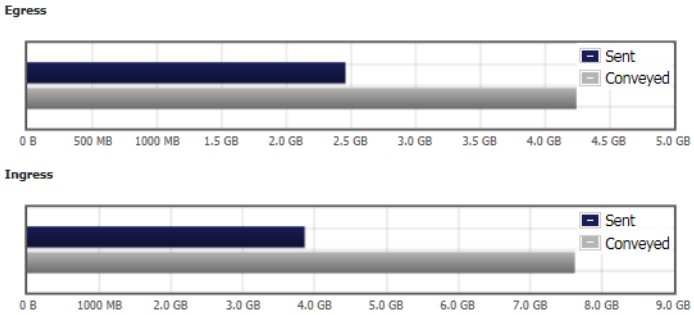
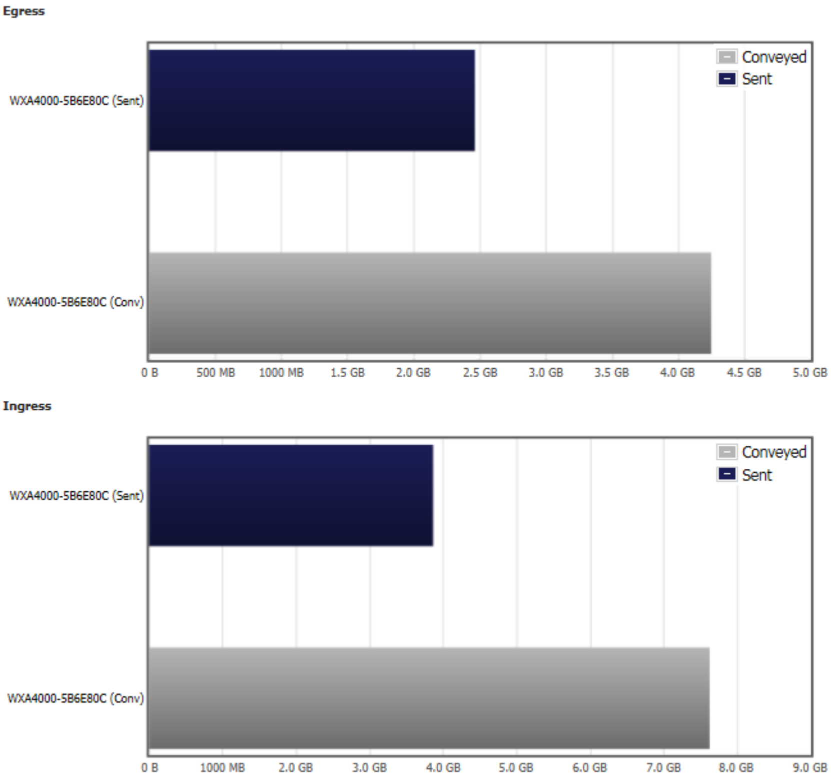
3 Click the **Refresh** icon to refresh the data being displayed.

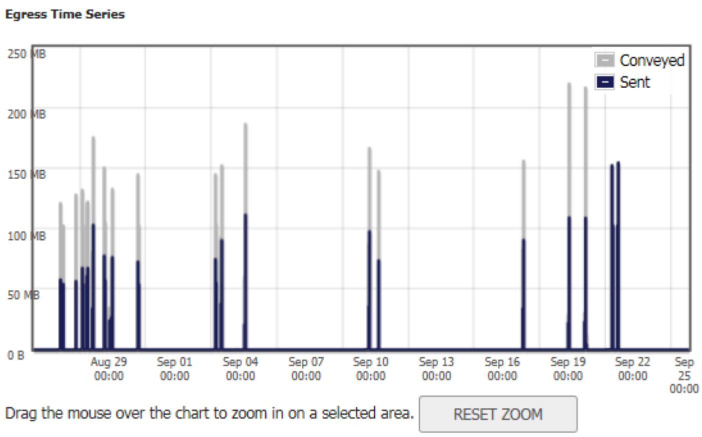
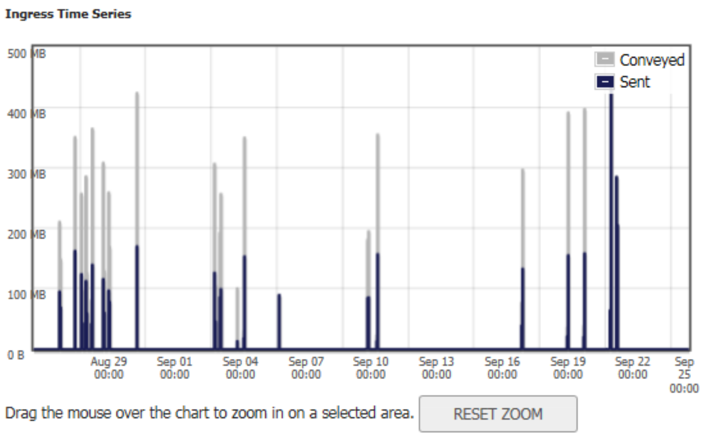
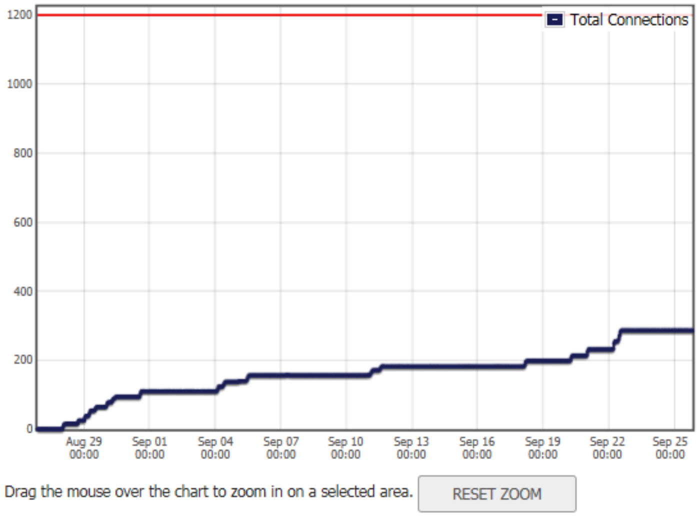
4 In the **Data from Selected WXAs** section, click the arrow to minimize or expand the WXA list. A left arrow indicates a minimized screen and the down arrow indicates and expanded screen.

The remainder of the page displays data relevant to the options selected. The first part is a data table **Showing data for all available WXAs fro the last 30 days**. It includes egress and ingress data for things like Total Data Reduction, WAN Capacity Increase Factor, New Connections, Closed Connections, and Peak Connections.

The bottom part of the page displays relevant information in graphical form. Change the graphical view by selecting one of the buttons below the data table.



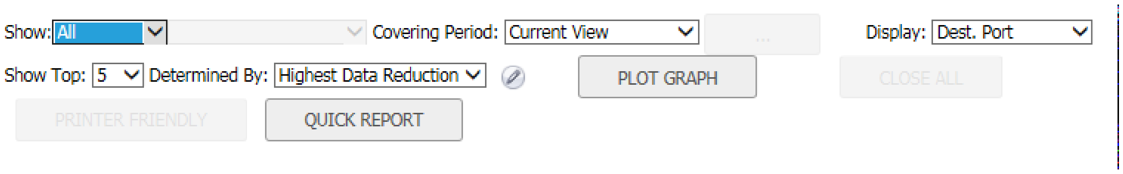
Name	Description
Summary	
Breakdown by WXA	

Name	Description
Time Series	 Drag the mouse over the chart to zoom in on a selected area.  Drag the mouse over the chart to zoom in on a selected area.
Connections	 Drag the mouse over the chart to zoom in on a selected area.

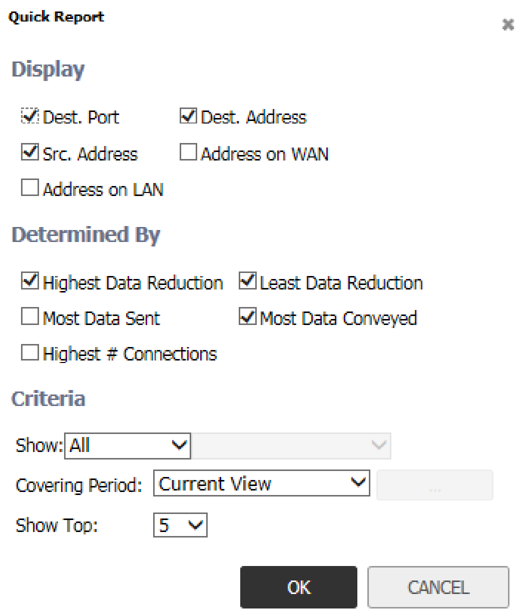
On the **Time Series** report and the **Connection** report, you can zoom in on a specific data set. With your mouse, just draw a square around the segment you want to enlarge. Click **RESET ZOOM** to reset the graph its original view.

Breakdown Statistics

With the **Breakdown Statistics** view, you can generate a TCP Acceleration report based on specific field definitions.

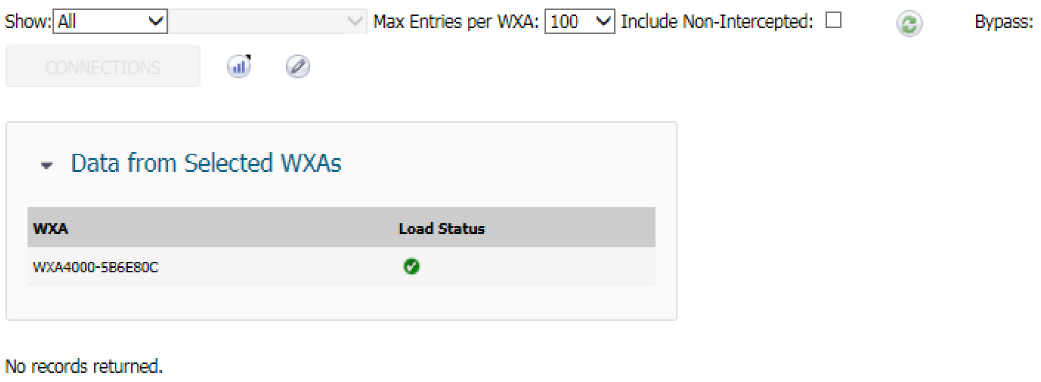


Name	Description
Show	From the **Show** menu, select the type of data you want displayed: • **All** • **For Group** • **For WXA** An additional field shows if you select **For Group** or **For WXA**. Select from the options in the drop-down menu to further refine your data.
Covering Period	Select the period of time the data displays on the Statistics tab. Options include: • **Last hour** • **Last 24 hours** • **Last 3 days** • **Last 5 days** • **Last 10 days** • **Last 30 days**
Display	Select the field for which data is shown in the chart. The **Display** menu options are: **Dest. Port** - Displays the volume of data (or “Determined By” value) compared to the destination port numbers of the accelerated connections. **Dest. Address** - Displays the volume of data compared to the destination IP address of the accelerated TCP connections. **Src. Address** - Displays the volume of data compared to the source IP address of the accelerated TCP connections. **Address on WAN** - Displays the volume of data compared to the destination address on the WAN of the accelerated TCP connections. **Address on LAN** - Displays the volume of data compared to the destination address on the LAN of the accelerated TCP connections. Connections can be initiated by a machine on the LAN or WAN.
Show Top	Selects how many ports or IP addresses to display in the graph. Options are **3**, **5**, **10** and **15**.
Determined By	Selects the criteria that displays in the graph. Options include: • Highest Data Reduction • Least Data Reduction • Most Data Sent • Most Data Conveyed • Highest # Connections

Name	Description
PLOT GRAPH	Displays a graphical representation of the selected criteria in a graph.
QUICK REPORT	 **Quick Report** **Display** ☑ Dest. Port ☑ Dest. Address ☑ Src. Address □ Address on WAN □ Address on LAN **Determined By** ☑ Highest Data Reduction ☑ Least Data Reduction □ Most Data Sent ☑ Most Data Conveyed □ Highest # Connections **Criteria** Show: All Covering Period: Current View Show Top: 5 OK CANCEL Allows selection of options to be used in the generation of a report that can be viewed on the screen and sent to a printer.

Connections

Navigate to **Reports > TCP Acceleration Reports > Connections** on the **INVESTIGATE** view to see a detailed list of the TCP Acceleration connection results. This report can show information such as start and end time stamps, source IP address and port, and destination IP address and port. Use these results to monitor the performance of your TCP Acceleration service.



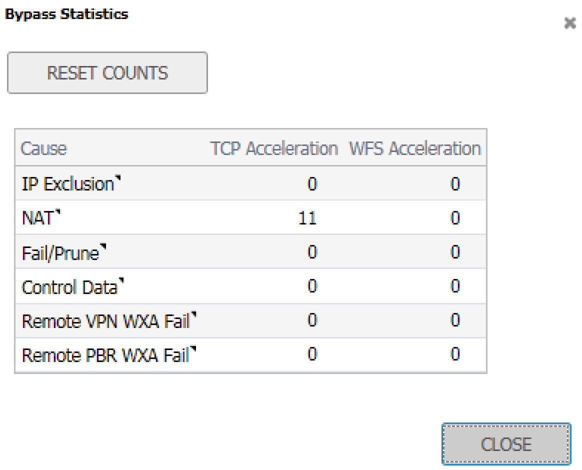
Show: All Max Entries per WXA: 100 Include Non-Intercepted: □ Bypass:

CONNECTIONS

Data from Selected WXAs

WXA	Load Status
WXA4000-5B6E80C	✓

No records returned.

Name	Description
Show	From the **Show** menu, select the type of data you want displayed: • **All** • **For Group** • **For WXA** An additional field shows if you select **For Group** or **For WXA**. Select from the options in the drop-down menu to further refine your data.
Max Entries per WXA	Selects the number of entries to display in the Connections table.
Include Non-Intercepted	Enables or disables the inclusion of non-intercepted traffic to display in the Connections table. The definition of "Non-intercepted" is traffic that is diverted from the firewall to the WXA series appliance, but is not accelerated.
Refresh button	Updates the displayed data whenever you change the criteria.
Bypass	Click **CONNECTIONS** to open a window that displays a list of the connections that are not accelerated, either because their data would not compress or the remote node WXA would not respond. Click **Bypass Statistics** to see the bypass data: 

Bypass Statistics

Cause	TCP Acceleration	WFS Acceleration
IP Exclusion	0	0
NAT	11	0
Fail/Prune	0	0
Control Data	0	0
Remote VPN WXA Fail	0	0
Remote PBR WXA Fail	0	0

The following defines the column headings for the data table.

Name	Description
Start Time	Indicates the starting time of a connection.
End Time	Indicates the ending time of a connection.
Initiator	Displays which end of the network initiated the connection. LAN for connections started locally, and WAN for connections started from a remote site.
Remote Node	Displays the WXA series appliance at the far end of the connection.
Src IP	Displays the IP address where the connection started.
Src Port	Displays the port number that the connection request was sent from.
Dest IP	Displays the destination IP address.
Dest Port	Displays the destination port number.
Egress	Displays a bar graph that represents outgoing traffic on the network. The blue colored bar is sent traffic and the grey bar is conveyed traffic.

Name	Description
Ingress	Displays a bar graph that represents incoming traffic on the network. The blue colored bar is sent traffic and the grey bar is conveyed traffic.
Filter by	Filter the results by entering text into the appropriate input box. A combination of fields can be filtered.

10

WFS Acceleration Reports

Topics:

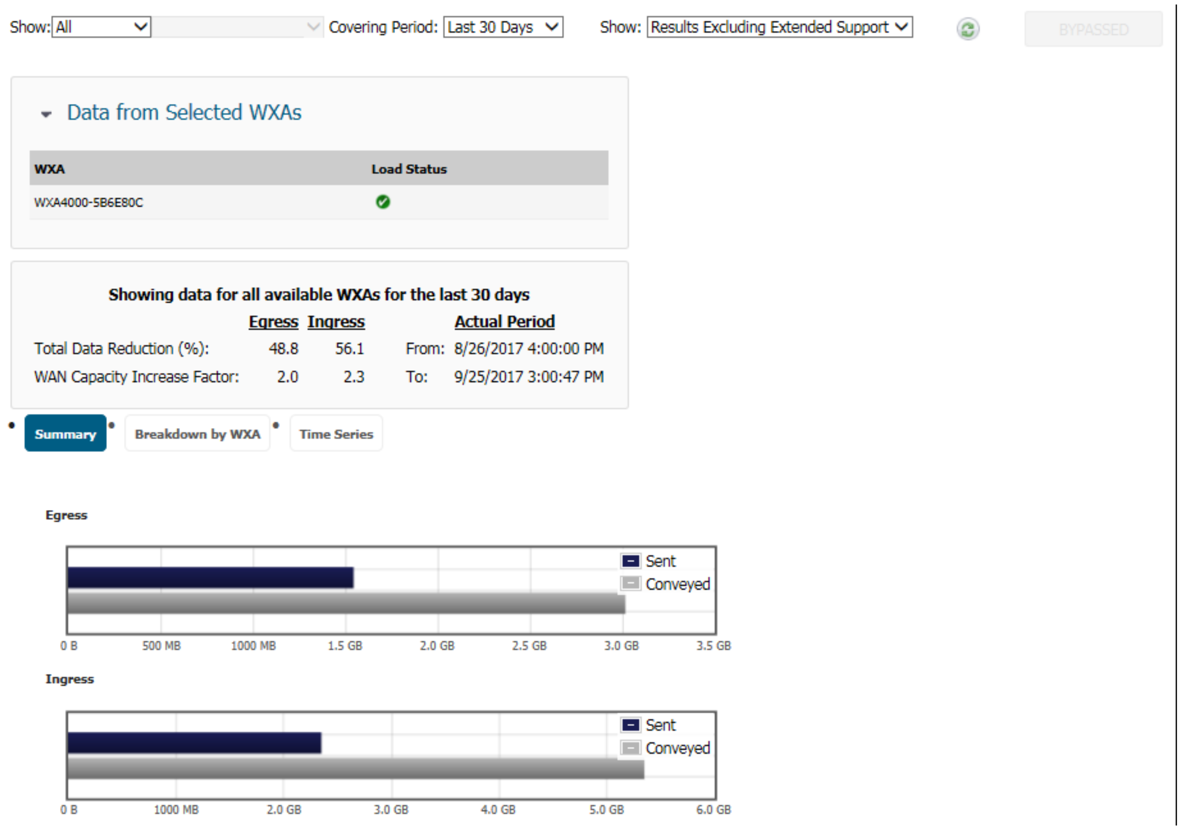
- Statistics on page 59
- Connections on page 62

Statistics

Navigate to **Reports > WFS Acceleration Reports > Statistics** on the **INVESTIGATE** view to select data from the WAN accelerators in the environment. The Statistics option shows graphs illustrating the following:

- Summary
- Breakdown by WXA
- Time Series

WFS Acceleration Reports > Statistics displays performance statistics for the WFS Acceleration service.



Show: All

Covering Period: Last 30 Days

Show: Results Excluding Extended Support

Data from Selected WXAs

WXA	Load Status
WXA4000-5B6E80C	✓

Showing data for all available WXAs for the last 30 days

	Egress	Ingress		Actual Period
Total Data Reduction (%):	48.8	56.1	From:	8/26/2017 4:00:00 PM
WAN Capacity Increase Factor:	2.0	2.3	To:	9/25/2017 3:00:47 PM

To set up the report for the Statistics view:

1 From **Show**, set the option for what data is displayed:

   - **All**
   - **For Group:**
   - **For WXA:**

   If you selected **For Group:** or **For WXA:** and additional field is shown so you can refine your selection further.

2 From **Covering Period**, select the period of time the data displays on Statistics page:

   - **Last hour**
   - **Last 24 hours**
   - **Last 3 days**
   - **Last 5 days**
   - **Last 10 days**
   - **Last 30 days**

3 From the next **Show**, select one:

   - **Only Extended Support Results**
   - **Results Excluding Extended Support**
   - **All Results**

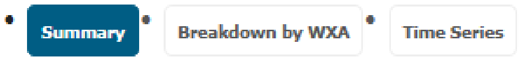
4 Click the **Refresh** icon to refresh the table data with the currently selected criteria.

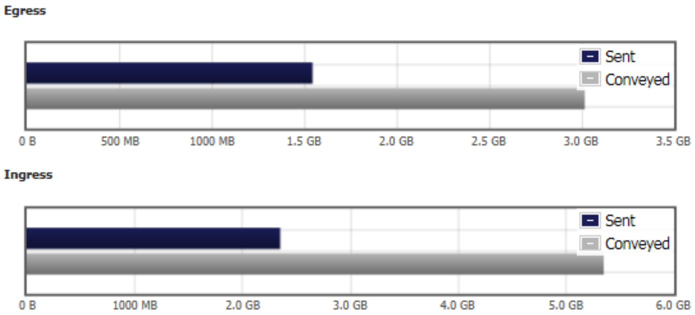
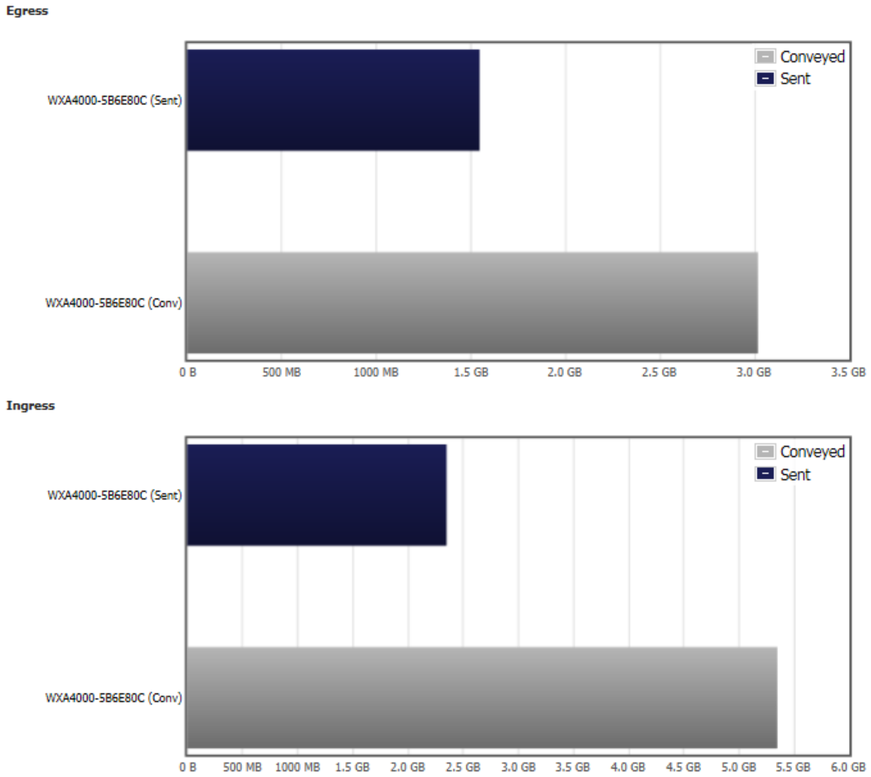
5 Click **BYPASS** to see the bypass data.

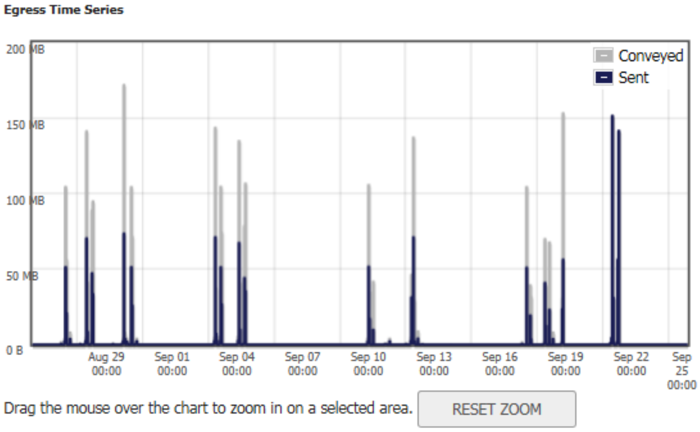
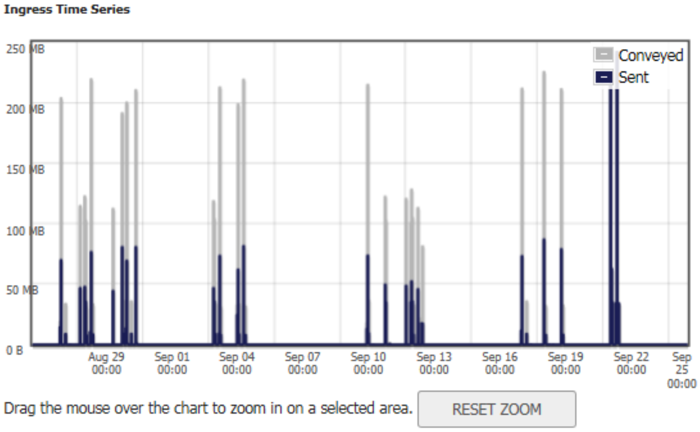
6 In the **Data from Selected WXAs** section, click the arrow to minimize or expand the WXA list. A left arrow indicates a minimized screen and the down arrow indicates and expanded screen.

The remainder of the page displays data relevant to the options selected. The first part is a data table **Showing data for all available WXAs from the last 30 days**. It includes egress and ingress data for things like **Total Data Reduction** and **WAN Capacity Increase Factor**.

The bottom part of the page displays relevant information in graphical form. Change the graphical view by selecting one of the buttons below the data table.

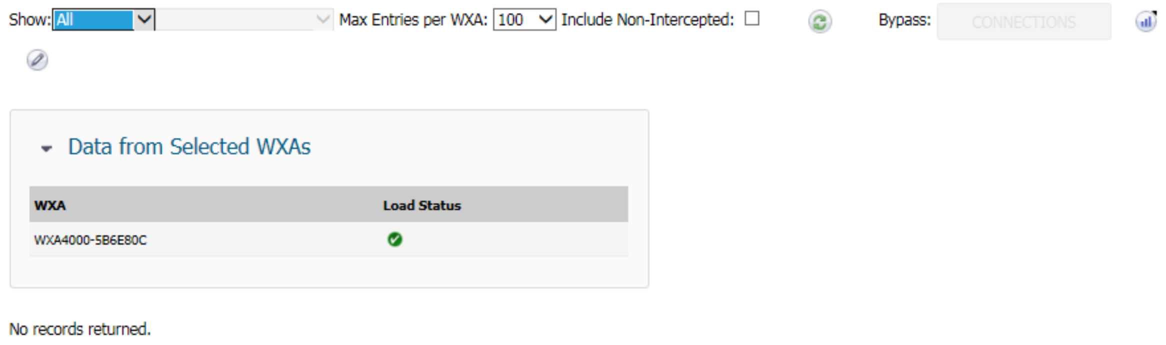


Name	Description
Summary	Displays two bar graphs that represent **Sent** or outgoing traffic and **Conveyed** or incoming traffic on the network over an actual period of time. The blue colored bar (Egress) is outgoing or sent data and the grey bar (Ingress) is incoming data. **Sent** refers to the actual amount of data that is physically sent across the connection. **Conveyed** refers to all of the data or information that is sent across the connection. 
Breakdown by WXA	

Name	Description
Time Series	 Drag the mouse over the chart to zoom in on a selected area.  Drag the mouse over the chart to zoom in on a selected area.

Connections

Navigate to **Reports > WFS Acceleration Reports > Connections** on the **INVESTIGATE** view to see a detailed list of the WFS Acceleration connection results. Use these results to monitor the performance of your WFS Acceleration service.



Show: All

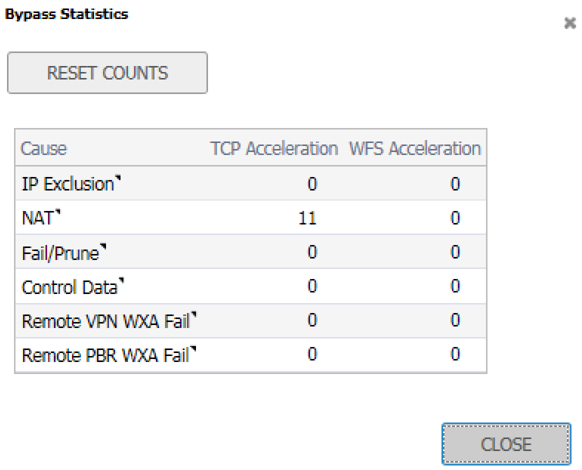
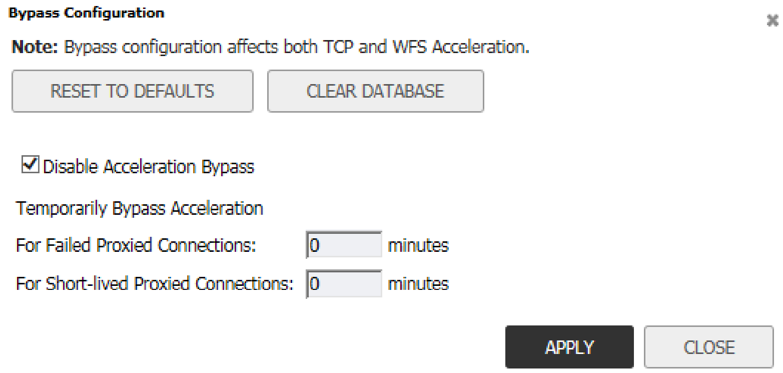
Max Entries per WXA: 100

Include Non-Intercepted: □

Bypass: CONNECTIONS

WXA	Load Status
WXA4000-5B6E80C	✓

No records returned.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td><b>Show</b></td><td>From the <b>Show</b> menu, select the type of data you want displayed:
• <b>All</b>
• <b>For Group</b>
• <b>For WXA</b>
An additional field shows if you select <b>For Group</b> or <b>For WXA</b>. Select from the options in the drop-down menu to further refine your data.</td></tr>
<tr><td><b>Max Entries per WXA</b></td><td>Selects the number of entries to display in the Connections table.</td></tr>
<tr><td><b>Include Non-Intercepted</b></td><td>Enables or disables the inclusion of non-intercepted traffic to display in the Connections table. The definition of “Non-intercepted” is traffic that is diverted from the firewall to the WXA series appliance, but is not accelerated.</td></tr>
<tr><td><b>Refresh</b> button</td><td>Updates the displayed data whenever you change the criteria.</td></tr>
<tr><td><b>Bypass</b></td><td>Click <b>CONNECTIONS</b> to open a window that displays a list of the connections that are not accelerated, either because their data would not compress or the remote node WXA would not respond.
Click the <b>Bypass Statistics</b> icon to see the bypass data:

<b>Bypass Statistics</b>
RESET COUNTS
<table><tr><th>Cause</th><th>TCP Acceleration</th><th>WFS Acceleration</th></tr><tr><td>IP Exclusion</td><td>0</td><td>0</td></tr><tr><td>NAT</td><td>11</td><td>0</td></tr><tr><td>Fail/Prune</td><td>0</td><td>0</td></tr><tr><td>Control Data</td><td>0</td><td>0</td></tr><tr><td>Remote VPN WXA Fail</td><td>0</td><td>0</td></tr><tr><td>Remote PBR WXA Fail</td><td>0</td><td>0</td></tr></table>CLOSE</td></tr>
<tr><td><b>Edit</b> icon</td><td>Click to define the Bypass Configuration options.
<b>NOTE:</b> Bypass configuration affects both TCP and WFS Acceleration.

<b>Bypass Configuration</b>
<b>Note:</b> Bypass configuration affects both TCP and WFS Acceleration.
RESET TO DEFAULTS CLEAR DATABASE
☑ Disable Acceleration Bypass
Temporarily Bypass Acceleration
For Failed Proxied Connections: 0 minutes
For Short-lived Proxied Connections: 0 minutes
APPLY CLOSE</td></tr>
</table>

11

WXA Web Cache Reports

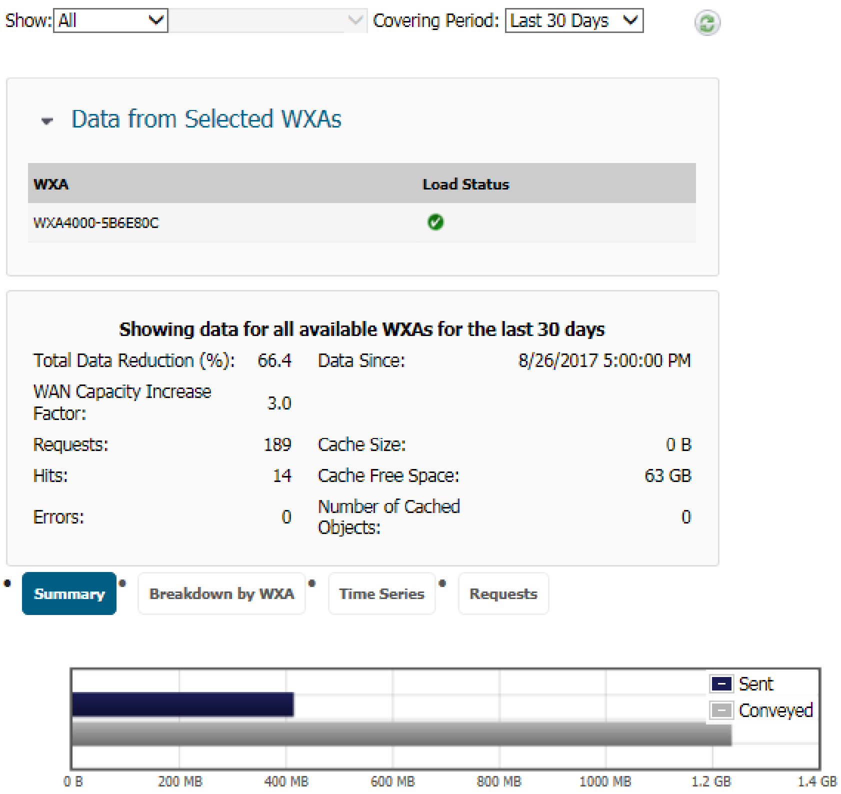
Topics:

- Statistics on page 64
- Breakdown Statistics on page 67

Statistics

Navigate to **Reports > WXA Web Cache Reports > Statistics** on the **INVESTIGATE** view to select data from the WAN accelerators in the environment. The **Statistics** page shows graphs illustrating:

- Summary
- Breakdown by WXA
- Time Series
- Requests



Show: All   Covering Period: Last 30 Days

Data from Selected WXAs

WXA	Load Status
WXA4000-5B6E80C	✓

Showing data for all available WXAs for the last 30 days

Total Data Reduction (%):	66.4	Data Since:	8/26/2017 5:00:00 PM
WAN Capacity Increase Factor:	3.0		
Requests:	189	Cache Size:	0 B
Hits:	14	Cache Free Space:	63 GB
Errors:	0	Number of Cached Objects:	0

To set up the report for the Statistics view:

1 From **Show**, set the option for what data is displayed:

   - **All**
   - **For Group:**
   - **For WXA:**

   If you selected **For Group:** or **For WXA:** and additional field is shown so you can refine your selection further.

2 From **Covering Period**, select the period of time the data displays on the **Statistics** page:

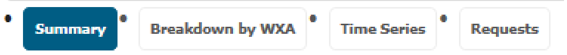
   - **Last hour**
   - **Last 24 hours**
   - **Last 3 days**
   - **Last 5 days**
   - **Last 10 days**
   - **Last 30 days**

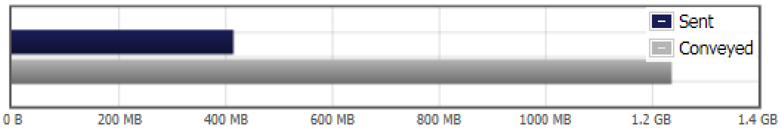
3 Click the **Refresh** icon to refresh the data being displayed.

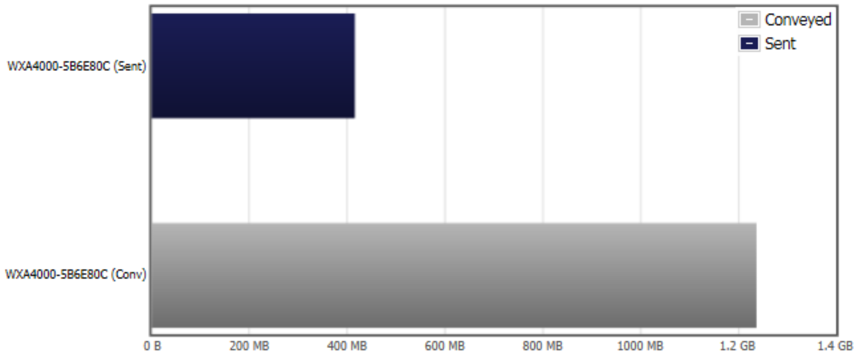
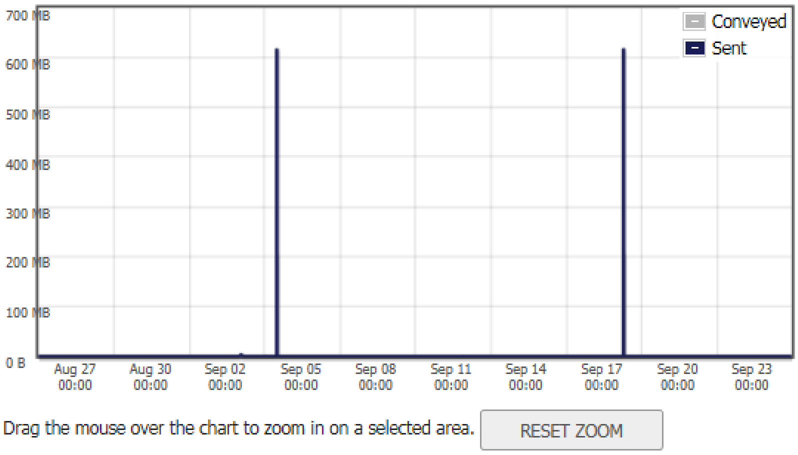
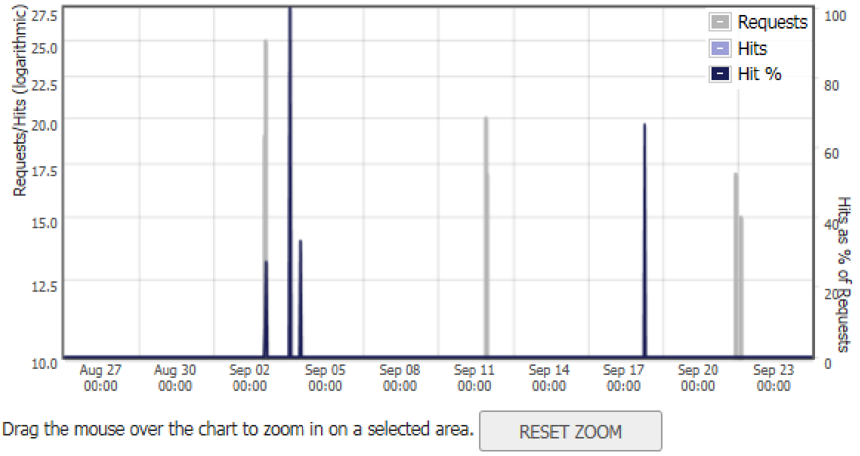
4 In the **Data from Selected WXAs** section, click the arrow to minimize or expand the WXA list. A left arrow indicates a minimized screen and the down arrow indicates and expanded screen.

The remainder of the page displays data relevant to the options selected. The first part is a data table **Showing data for all available WXAs from the last 30 days**. It includes data for things like Total Data Reduction, WAN Capacity Increase Factor, Requests, Hits, Errors and other information.

The bottom part of the page displays the Web Cache data for the selected Covering Period and Chart. The Conveyed data is the number of bytes that would be sent from a web server without the use of the WXA series appliance's Web Cache. The Sent data are the bytes that are actually sent from web servers in response to the user's web request, with the remainder being served from the cache. A "Hit" is when an object is served from the Web Cache instead of fetched from the Internet. The following Chart types are available:



Name	Description
Summary	

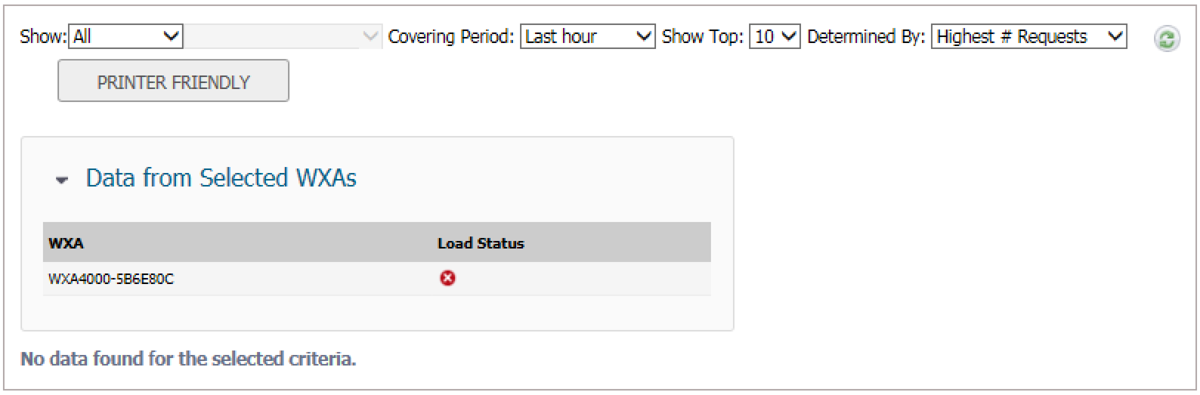
Name	Description
Breakdown by WXA	
Time Series	 Conveyed Sent 700 MB 600 MB 500 MB 400 MB 300 MB 200 MB 100 MB 0 B Aug 27 00:00 Aug 30 00:00 Sep 02 00:00 Sep 05 00:00 Sep 08 00:00 Sep 11 00:00 Sep 14 00:00 Sep 17 00:00 Sep 20 00:00 Sep 23 00:00 RESET ZOOM Drag the mouse over the chart to zoom in on a selected area.
Request	 Requests Hits Hit % Requests/Hits (logarithmic) 27.5 25.0 22.5 20.0 17.5 15.0 12.5 10.0 100 80 60 40 20 0 Hits as % of Requests Aug 27 00:00 Aug 30 00:00 Sep 02 00:00 Sep 05 00:00 Sep 08 00:00 Sep 11 00:00 Sep 14 00:00 Sep 17 00:00 Sep 20 00:00 Sep 23 00:00 RESET ZOOM Drag the mouse over the chart to zoom in on a selected area.

On the **Time Series** report and the **Requests** report, you can zoom in on a specific data set. With your mouse, just draw a square around the segment you want to enlarge.

Click **RESET ZOOM** to reset the graph to its original view.

Breakdown Statistics

With the **Breakdown Statistics** page, you can generate a WXA Web Cache report based on specific field definitions.



WXA	Load Status
WXA4000-5B6E80C	☒

No data found for the selected criteria.

Name	Description
Show	From **Show**, select the type of data you want displayed: • **All** • **For Group** • **For WXA** An additional field shows if you select For Group or For WXA. Select from the options in the drop-down menu to further refine your data.
Covering Period	Select the period of time the data displays on the Statistics tab. Options include: • **Last hour** • **Last 24 hours** • **Last 3 days** • **Last 5 days** • **Last 10 days** • **Last 30 days**
Show Top	Select how many ports or IP addresses to display in the graph: **3**, **5**, **10** and **15**.
Determined By	Select the criteria that displays in the graph. Options include: • **Highest # Requests** • **Most Data Requested**
Refresh button	Updates the displayed data whenever you change the criteria.
PRINTER FRIENDLY	Generates a printer friendly report.

12

Capture Threat Assessment

Topics:

About Capture Threat Assessment 2.0

SonicOS 6.5.4.6 introduces Capture Threat Assessment (CTA) 2.0. Capture Threat Assessment is a SonicWall service that provides network traffic and threat report generation in PDF format. The service is provided directly from the SonicOS web management interface. The **INVESTIGATE | Reports > Capture Threat Assessment** page allows you to generate the CTA report. The **GENERATE REPORT** button posts the SonicFlow Report (SFR) file, which contains the raw data, to the Capture Threat Assessment (CTA) service for the CTA report generation. Other options on this page provide a number of ways to customize the CTA report.

The **INVESTIGATE | Reports** > **Capture Threat Report** page has two screens accessed by buttons at the top:

- **Capture Threat Assessment**, where you set options for the CTA Report and generate the SFR file and the CTA report.
- **Previous Reports**, where you can download or delete prior reports. Previous reports are saved in the cloud and displayed as a table on the page, on the **Previous Reports** screen.

CTA v2.0 provides a number of enhancements to the earlier Capture Threat Assessment cloud service and reporting, as described below.

ⓘ | **NOTE:** App Visualization licensing is recommended for complete report data.

Topics:

New Report Template

A new report template design in CTA 2.0 provides the latest SonicOS look and feel.

SONICWALL

Capture Threat Assessment Report

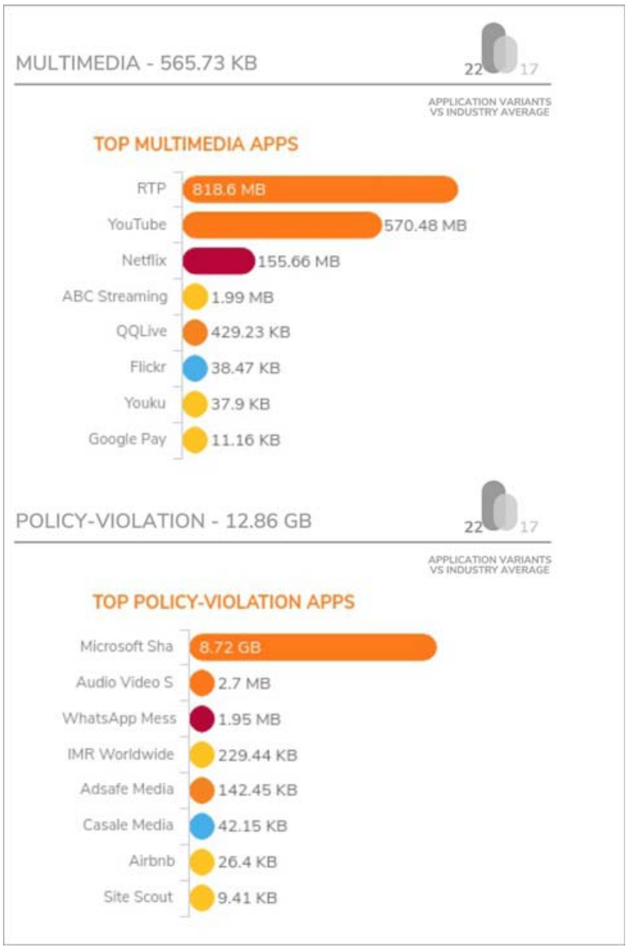
SonicWall
Jan 27 2020 10:07:54 +0530
Report Period: 6 Day(s)
Serial Number: C0EAE4FBAA7A

Prepared By:
SonicWall

SECURE MORE.
FEARLESS.

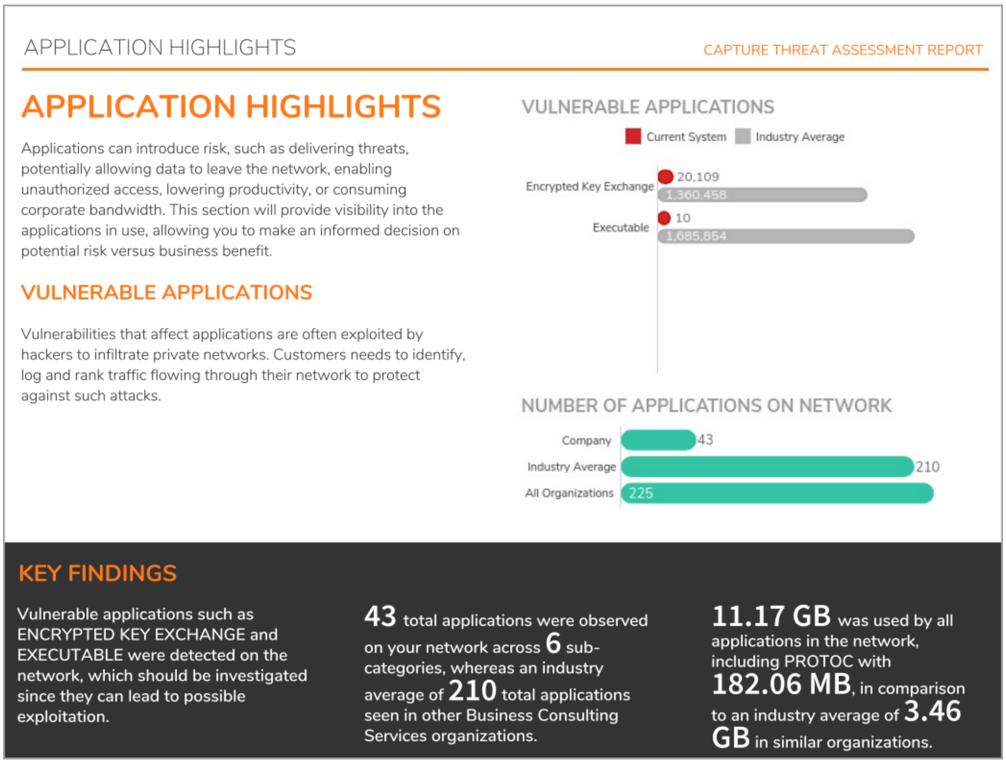
Meaningful Application Statistics

The new report template adds more meaningful application, threat, web and network data.



Industry and Global Level Statistics Comparison

Industry averages are provided so you can compare your statistics alongside industry and global data.



APPLICATION HIGHLIGHTS

CAPTURE THREAT ASSESSMENT REPORT

APPLICATION HIGHLIGHTS

Applications can introduce risk, such as delivering threats, potentially allowing data to leave the network, enabling unauthorized access, lowering productivity, or consuming corporate bandwidth. This section will provide visibility into the applications in use, allowing you to make an informed decision on potential risk versus business benefit.

VULNERABLE APPLICATIONS

Vulnerabilities that affect applications are often exploited by hackers to infiltrate private networks. Customers needs to identify, log and rank traffic flowing through their network to protect against such attacks.

VULNERABLE APPLICATIONS

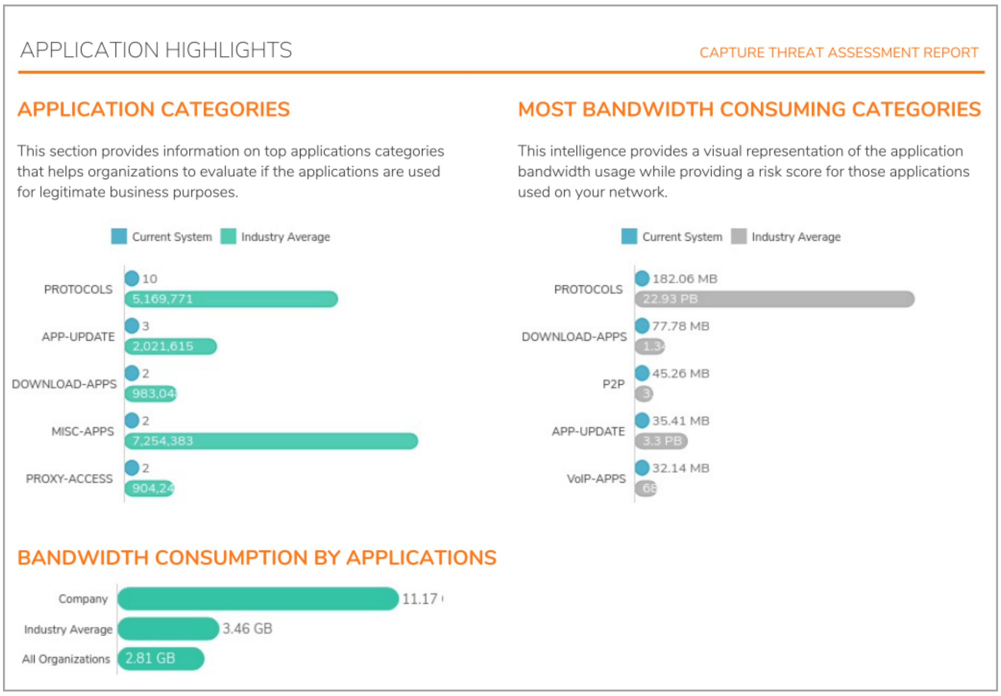
NUMBER OF APPLICATIONS ON NETWORK

KEY FINDINGS

Vulnerable applications such as ENCRYPTED KEY EXCHANGE and EXECUTABLE were detected on the network, which should be investigated since they can lead to possible exploitation.

43 total applications were observed on your network across 6 sub-categories, whereas an industry average of 210 total applications seen in other Business Consulting Services organizations.

11.17 GB was used by all applications in the network, including PROTOC with 182.06 MB, in comparison to an industry average of 3.46 GB in similar organizations.



APPLICATION HIGHLIGHTS

CAPTURE THREAT ASSESSMENT REPORT

APPLICATION CATEGORIES

This section provides information on top applications categories that helps organizations to evaluate if the applications are used for legitimate business purposes.

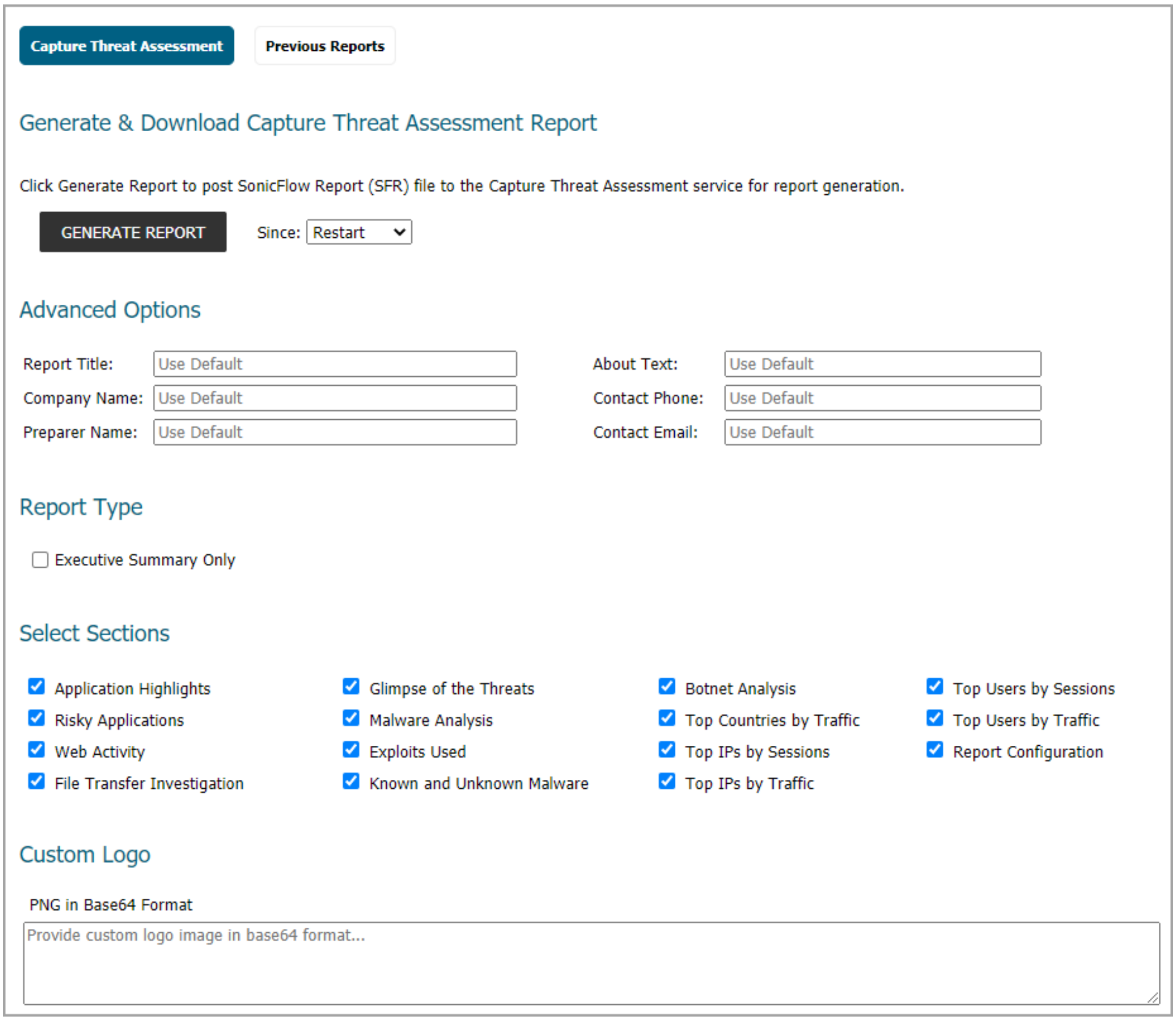
MOST BANDWIDTH CONSUMING CATEGORIES

This intelligence provides a visual representation of the application bandwidth usage while providing a risk score for those applications used on your network.

BANDWIDTH CONSUMPTION BY APPLICATIONS

Report Customization

Customizable settings on the **INVESTIGATE | Reports > Capture Threat Assessment** page provide a way to customize the report features, control the report title and company information, and add a custom logo so you can design the report according to your requirements.



Generate & Download Capture Threat Assessment Report

Click Generate Report to post SonicFlow Report (SFR) file to the Capture Threat Assessment service for report generation.

Since: Restart

Advanced Options

Report Title:	Use Default	About Text:	Use Default
Company Name:	Use Default	Contact Phone:	Use Default
Preparer Name:	Use Default	Contact Email:	Use Default

Report Type

☐ Executive Summary Only

Select Sections

☑ Application Highlights
☑ Risky Applications
☑ Web Activity
☑ File Transfer Investigation
☑ Glimpse of the Threats
☑ Malware Analysis
☑ Exploits Used
☑ Known and Unknown Malware
☑ Botnet Analysis
☑ Top Countries by Traffic
☑ Top IPs by Sessions
☑ Top IPs by Traffic
☑ Top Users by Sessions
☑ Top Users by Traffic
☑ Report Configuration

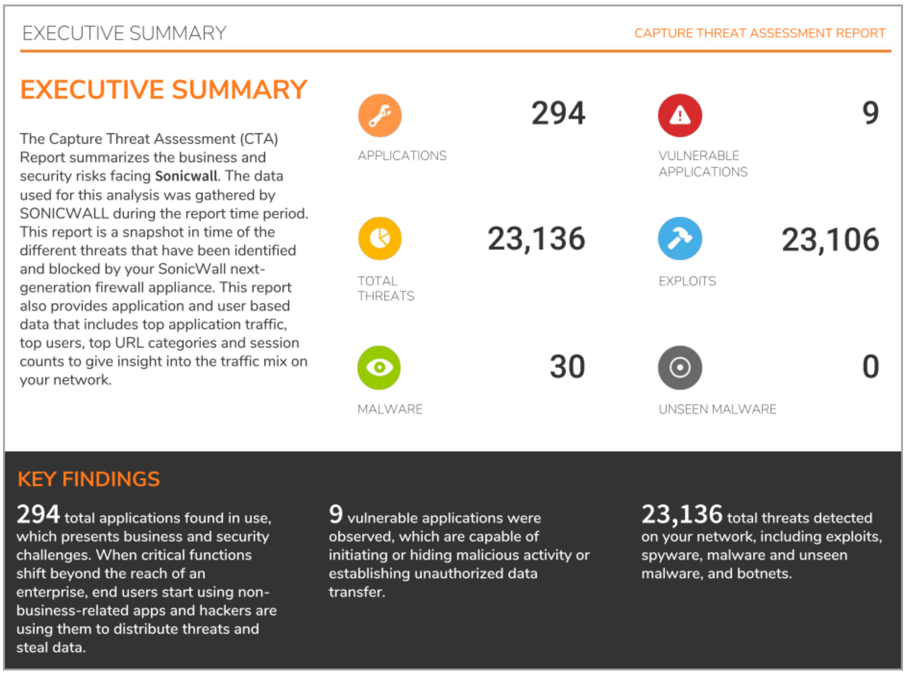
Custom Logo

PNG in Base64 Format

Provide custom logo image in base64 format...

Executive Summary with Key Findings

The Executive Summary page summarizes the overall pages into a single page for quick reference by busy executives. The **INVESTIGATE | Reports > Capture Threat Assessment** page provides an option to generate only this summary page in the CTA report.



EXECUTIVE SUMMARY

CAPTURE THREAT ASSESSMENT REPORT

EXECUTIVE SUMMARY

The Capture Threat Assessment (CTA) Report summarizes the business and security risks facing **Sonicwall**. The data used for this analysis was gathered by SONICWALL during the report time period. This report is a snapshot in time of the different threats that have been identified and blocked by your SonicWall next-generation firewall appliance. This report also provides application and user based data that includes top application traffic, top users, top URL categories and session counts to give insight into the traffic mix on your network.

APPLICATIONS 294

VULNERABLE APPLICATIONS 9

TOTAL THREATS 23,136

EXPLOITS 23,106

MALWARE 30

UNSEEN MALWARE 0

KEY FINDINGS

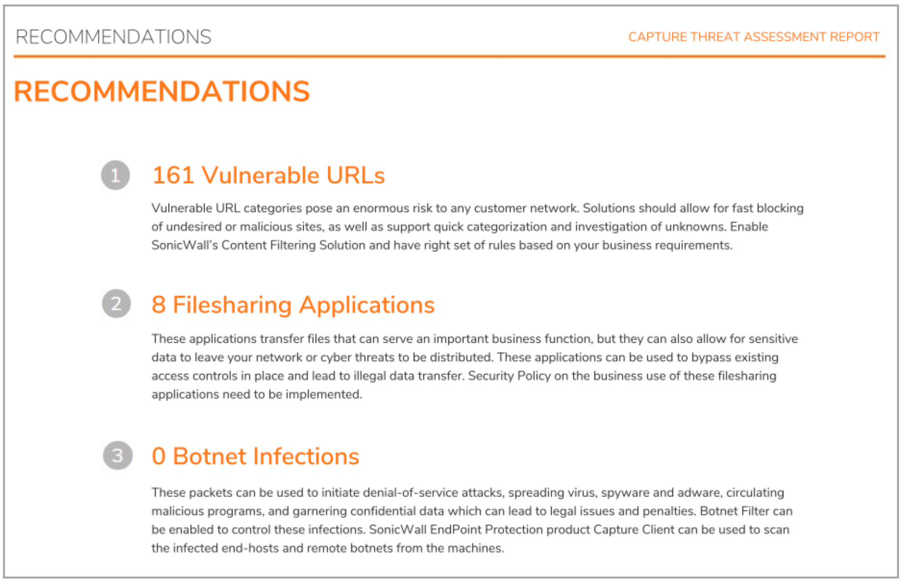
294 total applications found in use, which presents business and security challenges. When critical functions shift beyond the reach of an enterprise, end users start using non-business-related apps and hackers are using them to distribute threats and steal data.

9 vulnerable applications were observed, which are capable of initiating or hiding malicious activity or establishing unauthorized data transfer.

23,136 total threats detected on your network, including exploits, spyware, malware and unseen malware, and botnets.

Recommendations

The Recommendations pages provide a summary of steps you can take to fix the issues found during the reporting period.



RECOMMENDATIONS

CAPTURE THREAT ASSESSMENT REPORT

RECOMMENDATIONS

1 161 Vulnerable URLs

Vulnerable URL categories pose an enormous risk to any customer network. Solutions should allow for fast blocking of undesired or malicious sites, as well as support quick categorization and investigation of unknowns. Enable SonicWall's Content Filtering Solution and have right set of rules based on your business requirements.

2 8 Filesharing Applications

These applications transfer files that can serve an important business function, but they can also allow for sensitive data to leave your network or cyber threats to be distributed. These applications can be used to bypass existing access controls in place and lead to illegal data transfer. Security Policy on the business use of these filesharing applications need to be implemented.

3 0 Botnet Infections

These packets can be used to initiate denial-of-service attacks, spreading virus, spyware and adware, circulating malicious programs, and garnering confidential data which can lead to legal issues and penalties. Botnet Filter can be enabled to control these infections. SonicWall EndPoint Protection product Capture Client can be used to scan the infected end-hosts and remote botnets from the machines.

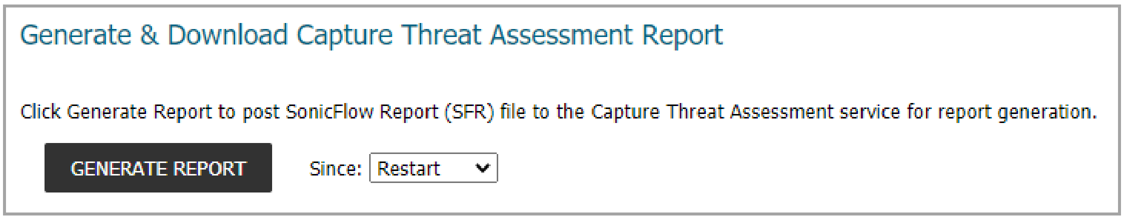
Generating a CTA Report

You can generate a customized Capture Threat Assessment report for your configuration. In the report, you receive an executive summary of your risks, recommendations, key findings, and top usage statistics as well as a list of the top applications presented by risk level, category, and bandwidth.

To generate a Capture Threat Assessment report:

1 Navigate to **INVESTIGATE | Reports > Capture Threat Assessment**.

2 Scroll to the **Generate & Download Capture Threat Assessment Report** section.



Generate & Download Capture Threat Assessment Report

Click Generate Report to post SonicFlow Report (SFR) file to the Capture Threat Assessment service for report generation.

Since: Restart

3 Select the time period for the report from the **Since** drop-down list.

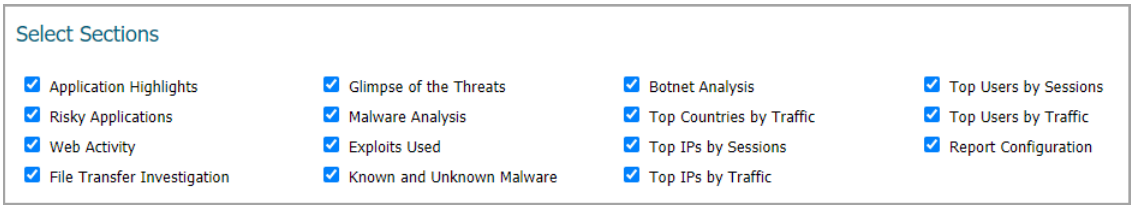
- **Restart** – since the firewall was last restarted
- **Last Reset**

4 In the **Advanced Options** section, you can customize the CTA report. Type the desired values into any of the following fields, or leave them unchanged to use the defaults:

- **Report Title**
- **Company Name**
- **Preparer Name**
- **About Text**
- **Contact Phone**
- **Contact Email**

5 Under **Report Type**, select the **Executive Summary Only** checkbox to generate a shorter report that includes the Executive Summary and the Recommendations pages. When unchecked, the full report will be generated.

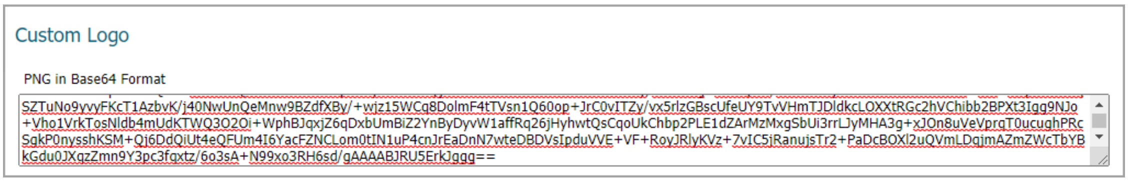
6 Under **Select Sections**, all sections are selected by default. To further customize your CTA Report, click on the check marks to remove any sections you do not want in the report.



Select Sections

☑ Application Highlights
☑ Risky Applications
☑ Web Activity
☑ File Transfer Investigation
☑ Glimpse of the Threats
☑ Malware Analysis
☑ Exploits Used
☑ Known and Unknown Malware
☑ Botnet Analysis
☑ Top Countries by Traffic
☑ Top IPs by Sessions
☑ Top IPs by Traffic
☑ Top Users by Sessions
☑ Top Users by Traffic
☑ Report Configuration

7 Under **Custom Logo**, paste in the Base64 representation of a PNG image to use on the cover of your report. There are a number of websites that will do the Base64 encoding for you.

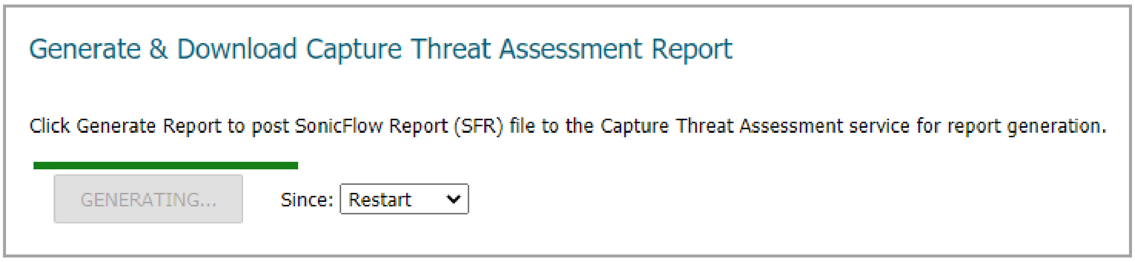


Custom Logo

PNG in Base64 Format

SZTuNo9yvyFKcT1AzbvK/j40NwUnQeMnw9BZdfXBy/+wjz15WCq8DolmF4tTVsn1Q60op+JrC0vITZy/vx5rlzGBscUfeUY9TvVHmTJDldkcLOXXtRGc2hVChibb2BPXt3Igg9NJo
+Vho1VrkTosNldb4mUdKTWQ3O2Oi+WphBJqxjZ6qDxbUmBiZ2YnByDyvW1affRq26jHyhwtQsCqoUkChbp2PLE1dZArMzMxgSbUi3rrLJyMHA3g+xJOn8uVeVprqT0ucughPRc
SgkP0nysshKSM+Qj6DdQiUt4eQFUm4I6YacFZNCLom0tIN1uP4cnJrEaDnN7wteDBDVsIpduVVE+VF+RoyJRlyKVz+7vIC5jRanujsTr2+PaDcBOXl2uQVmLDqjmAZmZWcTbYB
kGdu0JXqzZmn9Y3pc3fqxtz/6o3sA+N99xo3RH6sd/gAAAABJRU5ErkJggg==

8 Click **GENERATE REPORT**, or if a report has already been generated, click **GENERATE NEW REPORT**. A status line shows the progress of the report.

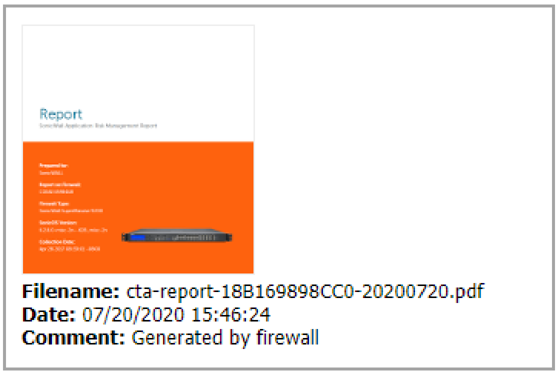


Generate & Download Capture Threat Assessment Report

Click Generate Report to post SonicFlow Report (SFR) file to the Capture Threat Assessment service for report generation.

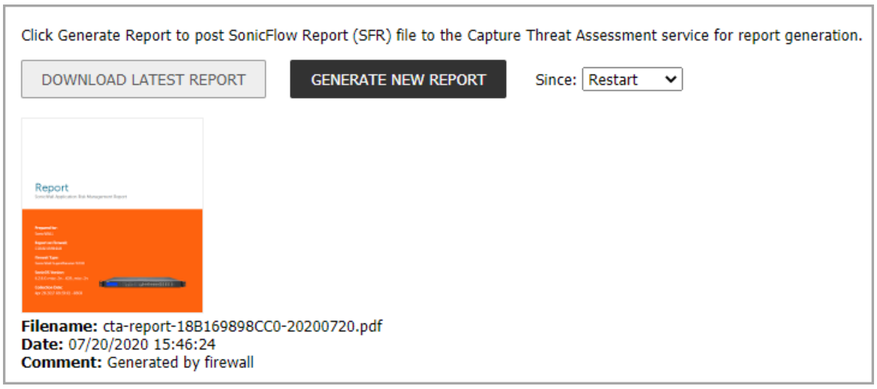
Since: Restart

When the report is generated, the current report status is updated on the page.



Filename: cta-report-18B169898CC0-20200720.pdf
Date: 07/20/2020 15:46:24
Comment: Generated by firewall

9 To download the report, click **DOWNLOAD LATEST REPORT**. The PDF is downloaded to your computer.



Click Generate Report to post SonicFlow Report (SFR) file to the Capture Threat Assessment service for report generation.

Since: Restart

Filename: cta-report-18B169898CC0-20200720.pdf
Date: 07/20/2020 15:46:24
Comment: Generated by firewall

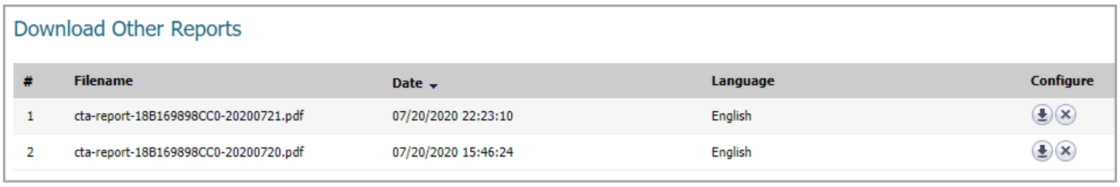
Downloading Previous Reports

You can download previous reports at any time. The **Download Other Reports** table lists previously generated CTA reports:

Filename	Name of the CTA report file
Date	Date the report was generated
Language	Language in which the report was generated
Configure	Displays the **Download** and **Delete** buttons for the report

To download previous reports:

1. Navigate to **INVESTIGATE | Reports > Capture Threat Assessment**.
2. Click **Previous Reports** to display the second screen.
3. The list of previous reports is displayed in the table under **Download Other Reports**.



Download Other Reports

#	Filename	Date ▾	Language	Configure
1	cta-report-18B169898CC0-20200721.pdf	07/20/2020 22:23:10	English	⬇ ⊗
2	cta-report-18B169898CC0-20200720.pdf	07/20/2020 15:46:24	English	⬇ ⊗

4. Click the **Download** icon for the report to download. The file is downloaded to your Downloads folder or other designated downloads location.

Deleting Previous Reports

To delete a previous report:

1. Navigate to **INVESTIGATE | Reports > Capture Threat Assessment**.
2. Click **Previous Reports**.

   The list of previous reports is displayed in the table under **Download Other Reports**.
3. Click the **Delete** button in the row for the file to delete.

Part 3

INVESTIGATE | Tools

- Packet Monitor
- Packet Replay
- Network Probes
- System Diagnostics

13

Packet Monitor

Topics:

About Packet Monitor

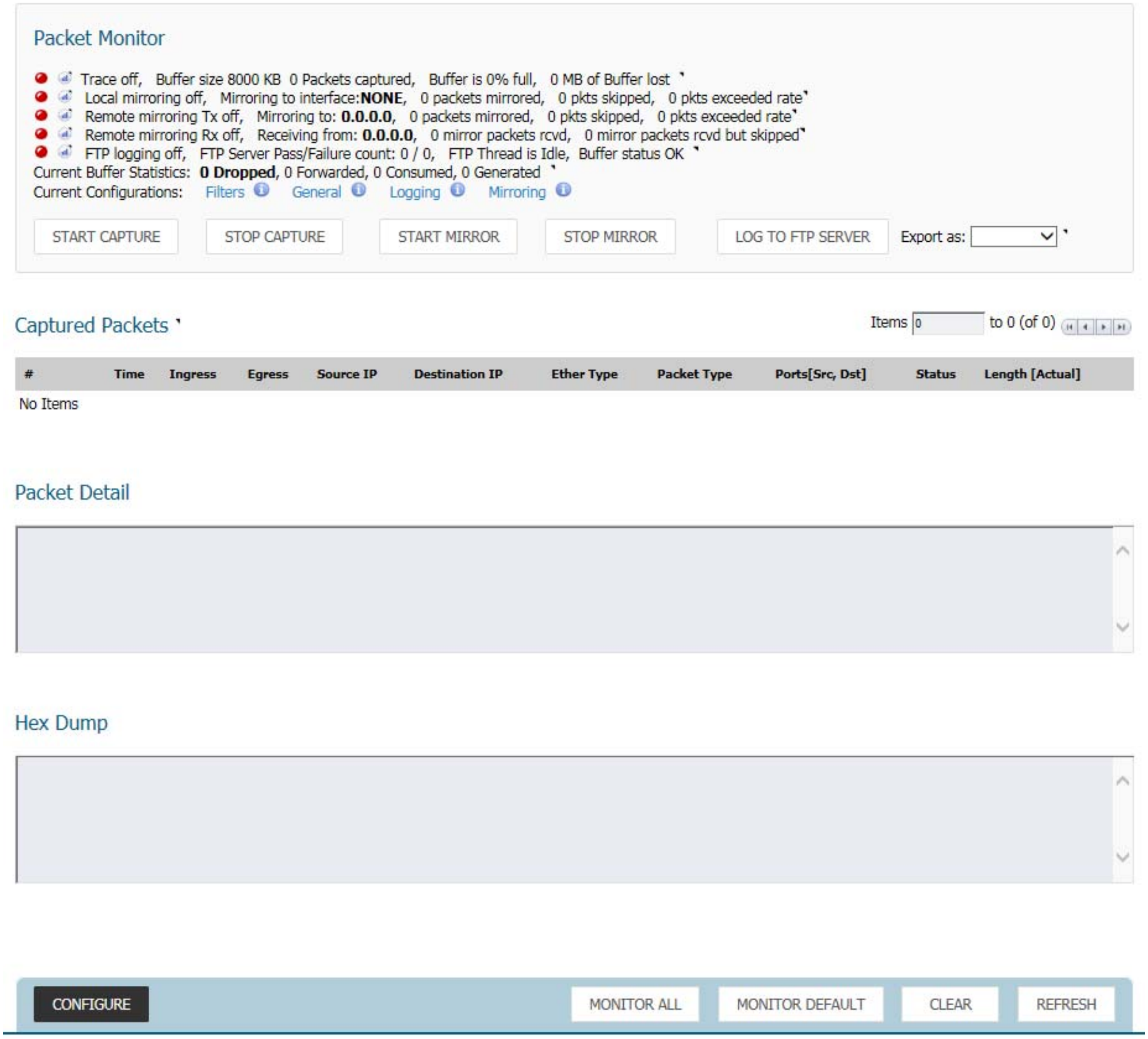
Packet monitor is a mechanism that allows you to monitor individual data packets that traverse your SonicWall appliance. Packets can be either monitored or mirrored. The monitored packets contain both data and addressing information.

The SonicOS packet monitor feature provides the functionality and flexibility that you need to examine network traffic without the use of external utilities.

Packet monitor includes the following features:

- Control mechanism with improved granularity for custom filtering (Monitor Filter)
- Display filter settings independent from monitor filter settings
- Packet status indicates if the packet was dropped, forwarded, generated, or consumed by the firewall
- Three output displays in the management interface:
  - List of captured packets
  - Packet detail
  - Hexadecimal dump of selected packet
- Export capabilities include text or HTML format with hex dump of packets, plus CAP file formats, pcap and pcapNG
- Automatic export to FTP server when the buffer is full
- Bidirectional packet monitor based on IP address and port

- Configurable wrap-around of packet monitor buffer when full



Packet Monitor

● Trace off, Buffer size 8000 KB 0 Packets captured, Buffer is 0% full, 0 MB of Buffer lost
● Local mirroring off, Mirroring to interface:**NONE**, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
● Remote mirroring Tx off, Mirroring to: **0.0.0.0**, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
● Remote mirroring Rx off, Receiving from: **0.0.0.0**, 0 mirror packets rcvd, 0 mirror packets rcvd but skipped
● FTP logging off, FTP Server Pass/Failure count: 0 / 0, FTP Thread is Idle, Buffer status OK

Current Buffer Statistics: **0 Dropped**, 0 Forwarded, 0 Consumed, 0 Generated

Current Configurations: Filters General Logging Mirroring

Export as:

Captured Packets

Items 0 to 0 (of 0)

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]

No Items

Packet Detail

Hex Dump

Topics:

- How Packet Monitor Works on page 78
- About Packet Mirroring on page 80
- Supported Packet Types on page 80
- File Formats for Exporting on page 81

How Packet Monitor Works

Configure the general settings, monitor filter, display filter, advanced filter settings, and FTP settings of the packet monitor tool. As network packets enter the packet monitor subsystem, the monitor filter settings are applied and the resulting packets are written to the capture buffer. The display filter settings are applied as you view the buffer contents in the management interface. Log the capture buffer to view in the management interface, or you can configure automatic transfer to the FTP server when the buffer is full.

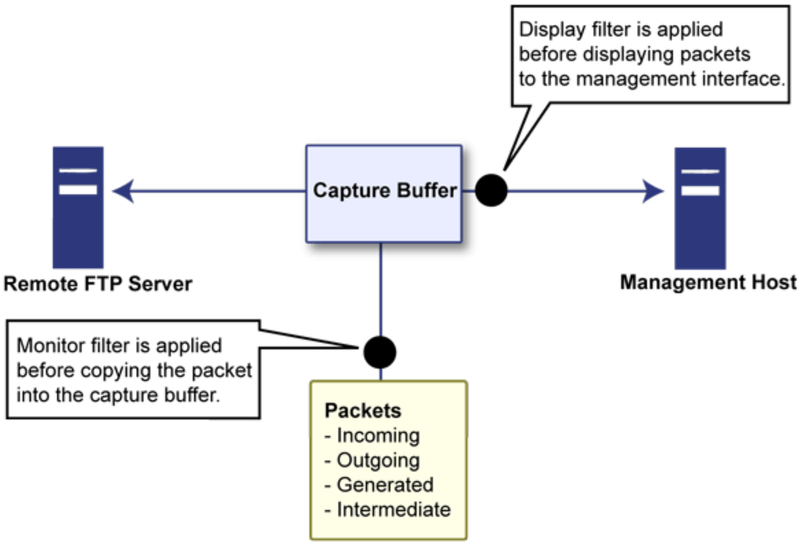
Default settings are provided so that you can start using packet monitor without configuring it first. The basic functionality is listed in the following table.

Packets: Basic Functionality

START CAPTURE	Click to begin capturing all packets except those used for communication between the firewall and the management interface on your console system.
STOP CAPTURE	Click to stop the packet capture.
START MIRROR	Click to begin the process of sending a copy of captured packets to another interface or to a remote SonicWall appliance.
STOP MIRROR	Click to stop sending captured packets to another unit.
LOG TO FTP SERVER	Click to log capture data to an FTP server.
Export As	Display or save a snapshot of the current buffer in the file format that you select from the drop-down menu. Exported files are placed on your local management system (where the management interface is running). • **Libpcap** - Select if you want to view the data with the Wireshark (formerly Ethereal) network protocol analyzer. This is also known as libcap or pcap format. A dialog allows you to open the buffer file with Wireshark or save it to your local hard drive with the extension **.pcap**. • **Html** - Select to view the data with a browser. Use **File > Save As** to save a copy of the buffer to your hard drive. • **Text** - Select to view the data in a text editor. A dialog allows you to open the buffer file with the registered text editor, or save it to your local hard drive with the extension **.wri**. • **App Data** - Select to view only application data contained in the packet. Packets containing no application data are skipped during the capture. Application data = captured packet minus L2, L3, and L4 headers.

Refer to Packet Monitor Subsystem Showing Filters for a high-level view of the packet monitor subsystem that shows the different filters and how they are applied.

Packet Monitor Subsystem Showing Filters


Display filter is applied before displaying packets to the management interface.
Capture Buffer
Remote FTP Server
Management Host
Monitor filter is applied before copying the packet into the capture buffer.
Packets
- Incoming
- Outgoing
- Generated
- Intermediate

About Packet Mirroring

Packet mirroring is the process of sending a copy of packets seen on one interface to another interface or to a remote SonicWall appliance.

There are two aspects of mirroring:

- **Classification** – Refers to identifying a selected set of packets to be mirrored. Incoming and outgoing packets to and from an interface are matched against a filter. If matched, the mirror action is applied.
- **Action** – Refers to sending a copy of the selected packets to a port or a remote destination. Packets matching a classification filter are sent to one of the mirror destinations. A particular mirror destination is part of the action identifier.

Every classification filter is associated with an action identifier. Up to two action identifiers can be defined, supporting two mirror destinations (a physical port on the same firewall and/or a remote SonicWall firewall). The action identifiers determine how a packet is mirrored. The following types of action identifiers are supported:

- Send a copy to a physical port.
- Encapsulate the packet and send it to a remote SonicWall appliance.
- Send a copy to a physical port with a VLAN configured.

Classification is completed on the **Monitor Filter** and **Advanced Monitor Filter** tab of the **Packet Monitor Configuration** dialog.

A local SonicWall firewall can be configured to receive remotely mirrored traffic from a remote SonicWall firewall. At the local firewall, received mirrored traffic can either be saved in the capture buffer or sent to another local interface. This is configured in the **Remote Mirror Settings (Receiver)** section on the **Mirror** tab of the **Packet Monitor Configuration** dialog.

SonicOS supports the following packet mirroring options:

- Mirror packets to a specified interface (Local Mirroring).
- Mirror only selected traffic.
- Mirror SSL decrypted traffic.
- Mirror complete packets including Layer 2 and Layer 3 headers as well as the payload.
- Mirror packets to a remote firewall (Remote Mirroring Tx).
- Receive mirrored packets from a remote SonicWall appliance (Remote Mirroring Rx).

Supported Packet Types

When specifying the Ethernet or IP packet types that you want to monitor or display, you can use either the standard acronym for the type, if supported, or the corresponding hexadecimal representation. To determine the hex value for a protocol, refer to the RFC for the number assigned to it by IANA. The protocol acronyms that SonicOS currently supports are shown in Supported Packet Types.

Supported Packet Types

Supported Types	Protocol Acronyms	
Supported Ethernet Types	ARP	
	IP	
	PPPoE-DIS	**NOTE:** To specify both PPPoE-DIS and PPPoE-SES, you can simply use PPPoE.
	PPPoE-SES	

Supported Packet Types (Continued)

Supported Types	Protocol Acronyms
Supported IP Types	TCP
	UDP
	ICMP
	IGMP
	GRE
	AH
	ESP

File Formats for Exporting

The **Export As** option on the **Tools | Packet Monitor** page on the **INVESTIGATE** view allows you to display or save a snapshot of the current buffer in the file format that you select from the drop-down menu. Saved files are placed on your local management system (where the management interface is running). For a description of the formats, see Packets: Basic Functionality.

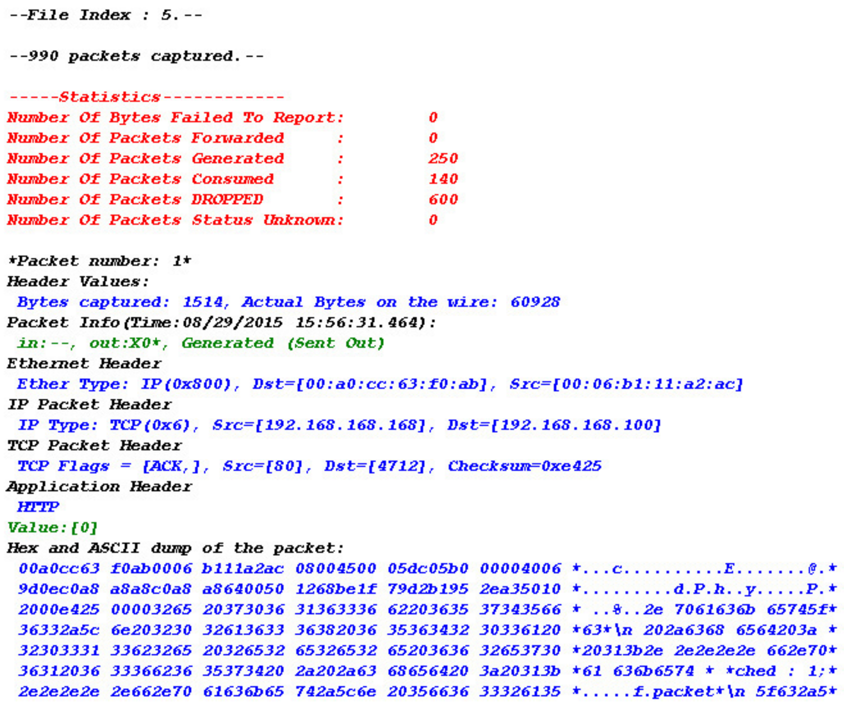
Examples of the HTML and Text formats are shown in:

- HTML Format on page 81
- Text File Format on page 82

HTML Format

View the HTML format in a browser. HTML Format Example shows the header and part of the data for the first packet in the buffer.

HTML Format Example

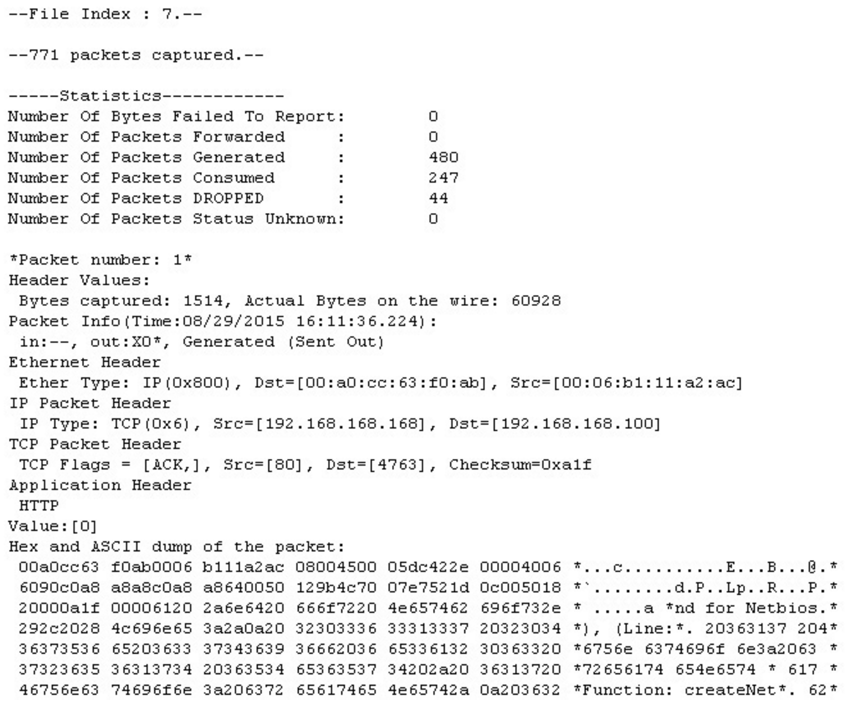


```
 --File Index : 5.--

 --990 packets captured.--

 -----Statistics------------
Number Of Bytes Failed To Report:        0
Number Of Packets Forwarded      :       0
Number Of Packets Generated      :       250
Number Of Packets Consumed       :       140
Number Of Packets DROPPED        :       600
Number Of Packets Status Unknown:        0

*Packet number: 1*
Header Values:
 Bytes captured: 1514, Actual Bytes on the wire: 60928
Packet Info(Time:08/29/2015 15:56:31.464):
 in:--, out:X0*, Generated (Sent Out)
Ethernet Header
 Ether Type: IP(0x800), Dst=[00:a0:cc:63:f0:ab], Src=[00:06:b1:11:a2:ac]
IP Packet Header
 IP Type: TCP(0x6), Src=[192.168.168.168], Dst=[192.168.168.100]
TCP Packet Header
 TCP Flags = [ACK,], Src=[80], Dst=[4712], Checksum=0xe425
Application Header
 HTTP
Value:[0]
Hex and ASCII dump of the packet:
 00a0cc63 f0ab0006 b111a2ac 08004500 05dc05b0 00004006 *...c.........E.......@.*
 9d0ec0a8 a8a8c0a8 a8640050 1268be1f 79d2b195 2ea35010 *.........d.P.h..y.....P.*
 2000e425 00003265 20373036 31363336 62203635 37343566 * ..%..2e 7061636b 65745f*
 36332a5c 6e203230 32613633 36382036 35363432 30336120 *63*\n 202a6368 6564203a *
 32303331 33623265 20326532 65326532 65203636 32653730 *20313b2e 2e2e2e2e 662e70*
 36312036 33366236 35373420 2a202a63 68656420 3a20313b *61 636b6574 * *ched : 1;*
 2e2e2e2e 2e662e70 61636b65 742a5c6e 20356636 33326135 *.....f.packet*\n 5f632a5*
```

Text File Format

View the text format output in a text editor. Text File Format Example shows the header and part of the data for the first packet in the buffer.

Text File Format Example



```
--File Index : 7.--

--771 packets captured.--

-----Statistics------------
Number Of Bytes Failed To Report:        0
Number Of Packets Forwarded     :        0
Number Of Packets Generated     :        480
Number Of Packets Consumed      :        247
Number Of Packets DROPPED       :        44
Number Of Packets Status Unknown:        0

*Packet number: 1*
Header Values:
 Bytes captured: 1514, Actual Bytes on the wire: 60928
Packet Info(Time:08/29/2015 16:11:36.224):
 in:--, out:X0*, Generated (Sent Out)
Ethernet Header
 Ether Type: IP(0x800), Dst=[00:a0:cc:63:f0:ab], Src=[00:06:b1:11:a2:ac]
IP Packet Header
 IP Type: TCP(0x6), Src=[192.168.168.168], Dst=[192.168.168.100]
TCP Packet Header
 TCP Flags = [ACK,], Src=[80], Dst=[4763], Checksum=0xa1f
Application Header
 HTTP
Value:[0]
Hex and ASCII dump of the packet:
 00a0cc63 f0ab0006 b111a2ac 08004500 05dc422e 00004006 *...c..........E...B...@.*
 6090c0a8 a8a8c0a8 a8640050 129b4c70 07e7521d 0c005018 *`........d.P..Lp..R...P.*
 20000a1f 00006120 2a6e6420 666f7220 4e657462 696f732e * .....a *nd for Netbios.*
 292c2028 4c696e65 3a2a0a20 32303336 33313337 20323034 *), (Line:*. 20363137 204*
 36373536 65203633 37343639 36662036 65336132 30363320 *6756e 6374696f 6e3a2063 *
 37323635 36313734 20363534 65363537 34202a20 36313720 *72656174 654e6574 * 617 *
 46756e63 74696f6e 3a206372 65617465 4e65742a 0a203632 *Function: createNet*. 62*
```

Configuring Packet Monitor

If you want to customize the features for Packet Monitor, access tool on the **Tools |Packet Monitor** page on the **INVESTIGATE** view of the SonicOS management interface. Packet Monitor has six main areas of configuration:

- Configuring the Settings Option on page 82
- Configuring Monitor Filter Option on page 84
- Configuring Display Filter Option on page 86
- Configuring Logging on page 88
- Configuring Advanced Monitor Filter Options on page 89
- Configuring Mirror Settings on page 91

Configuring the Settings Option

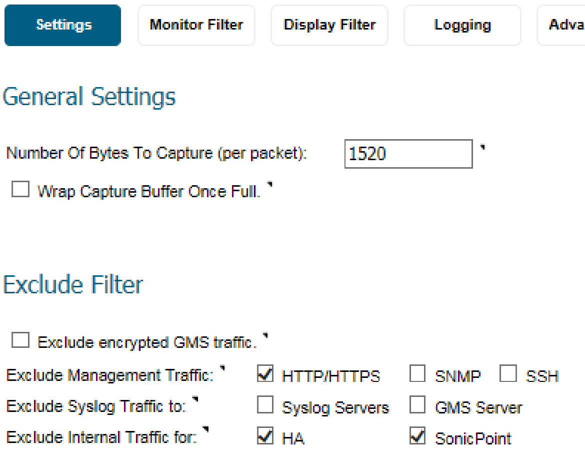
This section describes how to configure packet monitor settings, including the number of bytes to capture per packet and the buffer wrap option. Specify the number of bytes using either decimal or hexadecimal, with a minimum value of 64. The buffer wrap option enables the packet capture to continue even when the buffer becomes full, by overwriting the buffer from the beginning.

To configure the Settings option:

1 Navigate to the **Tools > Packet Monitor** page on the **INVESTIGATE** view.

2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.

Packet Monitor Configuration: Settings



General Settings

Number Of Bytes To Capture (per packet): 1520

□ Wrap Capture Buffer Once Full.

Exclude Filter

□ Exclude encrypted GMS traffic.

Exclude Management Traffic: ☑ HTTP/HTTPS □ SNMP □ SSH

Exclude Syslog Traffic to: □ Syslog Servers □ GMS Server

Exclude Internal Traffic for: ☑ HA ☑ SonicPoint

3 In the **Number of Bytes To Capture (per packet)** field, enter the number of bytes to capture from each packet. The minimum value is 64, the default value is **1520**. Enter this number as a hexadecimal figure.

4 To continue capturing packets after the buffer fills up, check the box for **Wrap Capture Buffer Once Full**. This option causes packet capture to start writing captured packets at the beginning of the buffer again after the buffer fills. It has no effect if FTP server logging is enabled on the **Logging** tab because the buffer is automatically wrapped when FTP is enabled. This option is not selected by default.

5 In the **Exclude Filter** section, select the **Exclude encrypted GMS traffic** to prevent capturing or mirroring encrypted management traffic or syslog traffic to or from SonicWall GMS. This setting only affects encrypted traffic within a configured primary or secondary GMS tunnel. GMS management traffic is not excluded if it is sent through a separate tunnel. This option is not selected by default.

6 Use the **Exclude Management Traffic** settings to prevent capturing or mirroring management traffic to the appliance. Check the box to exclude each type of traffic:

- **HTTP/HTTPS** (selected by default)
- **SNMP**
- **SSH**

If management traffic is sent through a tunnel, the packets are not excluded.

7 Use the **Exclude Syslog Traffic to** settings to prevent capturing or mirroring syslog traffic to the logging servers. Check the box for each type of server to exclude (by default, neither is selected):

- **Syslog Servers**
- **GMS Server**

If syslog traffic is sent through a tunnel, the packets are not excluded.

8 Use the **Exclude Internal Traffic for** settings to prevent capturing or mirroring internal traffic between the firewall and its High Availability partner or a connected access point. Check the box for each type of traffic to exclude:

- **HA** (selected by default)

- **SonicPoint** (selected by default; not supported on the SuperMassive 9800)

  > **NOTE:** The following options are for the SuperMassive 9800 only. When present, they are selected by default.

- **BCP**
- **Inter-Blade**
- **Back-Plane**

9 To save your settings and exit the **Packet Monitor Configuration** dialog, click **OK**.

To restore default settings, click **Default**.

Configuring Monitor Filter Option

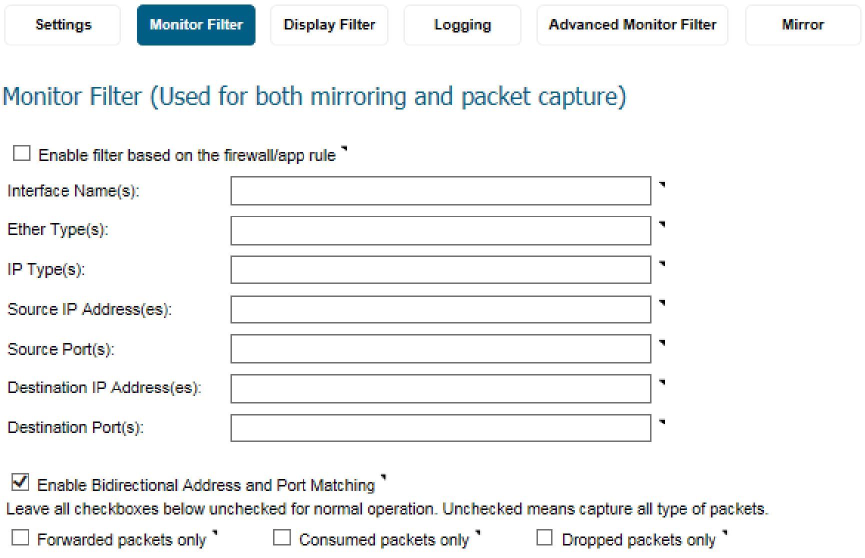
All filters set on this page are applied to both packet capture and packet mirroring.

To configure Monitor Filter settings:

1 Navigate to the **Tools > Packet Monitor** page on the **INVESTIGATE** view.

2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.

3 Click **Monitor Filter**.



Monitor Filter (Used for both mirroring and packet capture)

□ Enable filter based on the firewall/app rule

Interface Name(s):

Ether Type(s):

IP Type(s):

Source IP Address(es):

Source Port(s):

Destination IP Address(es):

Destination Port(s):

☑ Enable Bidirectional Address and Port Matching

Leave all checkboxes below unchecked for normal operation. Unchecked means capture all type of packets.

□ Forwarded packets only □ Consumed packets only □ Dropped packets only

4 If you are filtering based on firewall rules to capture specific traffic, select **Enable filter based on the firewall rule**.

> **NOTE:** Before selecting this option, be certain you have selected one or more access rules on which to monitor packet traffic. This configuration is done from the **Policies | Rules > Access Rules** page; refer to *SonicWall SonicOS 6.5 Policies* for more information.

5 Specify how Packet Monitor filters packets using these options:

> **NOTE:** If a field or option is left blank, no filtering is done on that field. Packets are captured or mirrored without regard to the value contained in that field of their headers.

- **Interface Name(s)** - Type the name of the interface where you want to complete the packet capture. Specify up to ten interfaces separated by commas. The specified interface names should be the same as those listed in the **System Setup |Network > Interface** page; for example:
  - NSA series: X0, X1, X2:V100
  - TZ family: WLAN, WWAN, Modem, OPT, WAN, LAN

  To configure all interfaces except the one(s) specified, use a negative value; for example: !X0, or !LAN.

- **Ether Type(s)** - Specify the name of the Ethernet type(s) where you want to complete filtering of the captured packets. Specify up to ten Ethernet types separated by commas. This option is not case-sensitive. Currently, the following Ethernet types are supported: ARP (arp), IP (ip), PPPoE-SES, and PPPoE-DIS. The latter two can be specified by PPPoE alone.

  For example, to capture all supported types, you could enter: ARP, ip, PPPOE. Use one or more negative values to capture all Ethernet types except those specified; for example: !ARP, !PPPoE.

  You can also use hexadecimal values to represent the Ethernet types, or mix hex values with the standard representations; for example: ARP, 0x800, ip. Normally you would only use hex values for Ethernet types that are not supported by acronym in SonicOS. Refer to Supported Packet Types for more information.

- **IP Type(s)** - Specify the name of the IP packet type where you want to complete packet capture. Specify up to ten IP types separated by commas. This option is not case-sensitive. The following IP types are supported: TCP, UDP, ICMP, GRE, IGMP, AH, ESP.

  Use one or more negative values to capture all IP types except those specified; for example: !TCP, !UDP.

  You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: TCP, 0x1, 0x6. Refer to Supported Packet Types for more information.

NOTE: The following option fields require either addresses or ports. Specify up to 10 addresses or ports separated by commas. For example:

- IP addresses: `10.1.1.1`, `192.2.2.2`, `1.2.3.4/24`, `2.3.4.5/61`
- TCP or UDP port numbers: 20, 21, 22, 25, 80, 8080

Use one or more negative values to capture packets from all but the specified addresses or ports; for example:

- IP addresses: `!10.3.3.3`, `!10.4.4.4.`, `!1.2.3.4/24`
- TCP or UDP port numbers: !80, !8080, !20

- **Source IP Address(es)** - Specify the source IP address where you want to complete packet capture.
- **Source Port(s)** - Specify the source port where you want to complete packet capture.
- **Destination IP Address(es)** - Specify the destination IP address where you want to complete packet capture.
- **Destination Port(s)** - Specify the destination port address where you want to complete packet capture.
- **Enable Bidirectional Address and Port Matching** - Select this option to match IP addresses and/or ports specified in the above source and/or destination fields against both the source and/or destination fields in each packet. This option is selected by default.

NOTE: For normal operation, leave the following options unselected to capture all types of packets. Selecting an option restricts the type of packets captured.

- **Forwarded packets only** - Select this option to monitor any packets forwarded by the firewall.
- **Consumed packets only** - Select this option to monitor all packets consumed by internal sources within the firewall.
- **Dropped packets only** - Select this option to monitor all packets dropped at the perimeter.

6 To save your settings and exit the configuration window, click **OK**.

Configuring Display Filter Option

This section describes how to configure Packet Monitor display filter settings. The values you provide here are compared to corresponding fields in the captured packets, and only those packets that match are displayed. These settings apply only to the display of captured packets on the management interface and do not affect packet mirroring.

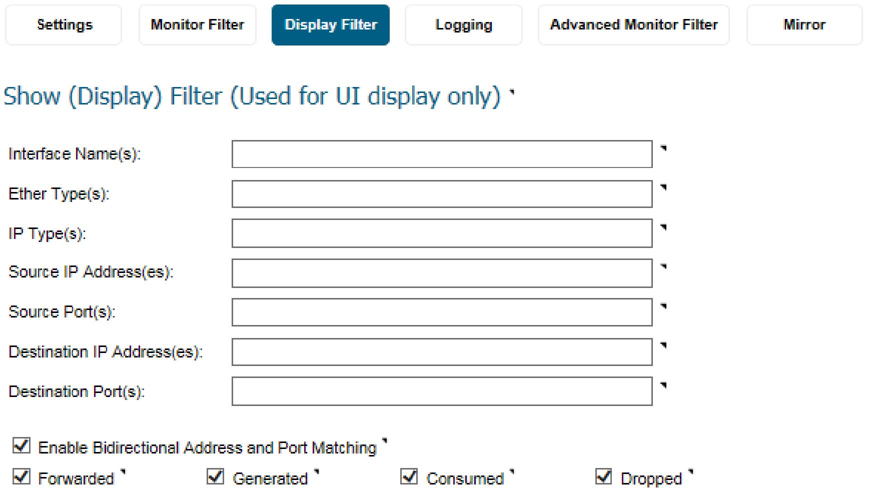
> **NOTE:** If a field is left blank, no filtering is done on that field. Packets are displayed without regard to the value contained in that field of their headers.

To configure Packet Monitor display filter settings:

1 Navigate to the **Tools > Packet Monitor** page on the **INVESTIGATE** view.

2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.

3 Click **Display Filter**.



Show (Display) Filter (Used for UI display only)

Interface Name(s):

Ether Type(s):

IP Type(s):

Source IP Address(es):

Source Port(s):

Destination IP Address(es):

Destination Port(s):

☑ Enable Bidirectional Address and Port Matching

☑ Forwarded ☑ Generated ☑ Consumed ☑ Dropped

4 Specify how Packet Monitor filters packets using these options:

> **NOTE:** If a field or option is left blank, no filtering is done on that field. Packets are captured or mirrored without regard to the value contained in that field of their headers.

- **Interface Name(s)** - Specify the name of the interface where you want to complete packet capture. Specify up to ten interfaces separated by commas. The specified interface names should be the same as those listed in the **System Setup |Network > Interface** page; for example:
  - NSA series: X0, X1, X2:V100
  - TZ family: WLAN, WWAN, Modem, OPT, WAN, LAN

  To configure all interfaces except the one(s) specified, use a negative value; for example: !X0, or !LAN.

- **Ether Type(s)** - Specify the name of the Ethernet type where you want to complete filtering of the captured packets. Specify up to ten Ethernet types separated by commas. This option is not case-sensitive. Currently, the following Ethernet types are supported: ARP (arp), IP (ip), PPPoE-SES, and PPPoE-DIS. The latter two can be specified by PPPoE alone.

  For example, to capture all supported types, you could enter: ARP, ip, PPPOE. Use one or more negative values to capture all Ethernet types except those specified; for example: !ARP, !PPPoE.

  You can also use hexadecimal values to represent the Ethernet types, or mix hex values with the standard representations; for example: ARP, 0x800, ip. Normally you would only use hex values for Ethernet types that are not supported by acronym in SonicOS. See Supported Packet Types.

- **IP Type(s)** - Specify the name(s) of the IP packet type where you want to complete packet capture. Specify up to ten IP types separated by commas. This option is not case-sensitive. The following IP types are supported: TCP, UDP, ICMP, GRE, IGMP, AH, ESP.

  Use one or more negative values to capture all IP types except those specified; for example: !TCP, !UDP.

  You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: TCP, 0x1, 0x6. See Supported Packet Types.

ⓘ **NOTE:** The following option fields require either addresses or ports. Specify up to 10 addresses or ports separated by commas. For example:

- IP addresses: `10.1.1.1`, `192.2.2.2`, `1.2.3.4/24`, `2.3.4.5/61`
- TCP or UDP port numbers: `20`, `21`, `22`, `25`, `80`, `8080`

Use one or more negative values to capture packets from all but the specified addresses or ports; for example:

- IP addresses: `!10.3.3.3`, `!10.4.4.4.`, `!1.2.3.4/24`
- TCP or UDP port numbers: `!80`, `!8080`, `!20`

- **Source IP Address(es)** - Specify the source IP address where you want to complete packet capture.
- **Source Port(s)** - Specify the source port where you want to complete packet capture.
- **Destination IP Address(es)** - Specify the destination IP address on which to complete packet capture.
- **Destination Port(s)** - Specify the destination port address where you want to complete packet capture.

ⓘ **NOTE:** The following options are selected by default.

- **Enable Bidirectional Address and Port Matching** - Select this option to match IP addresses and/or ports specified in the above source and/or destination fields against both the source and/or destination fields in each packet. This option is selected by default.
- **Forwarded** - To display captured packets that the firewall has forwarded, check this box.
- **Generated** - To display captured packets that the firewall has generated, check this box.
- **Consumed** - To display captured packets that the firewall has consumed, check this box.
- **Dropped** - To display captured packets that the firewall has dropped, check this box.

5 To save your settings and exit the dialog, click **OK**.

Configuring Logging

This section describes how to configure Packet Monitor logging. These settings provide a way to configure automatic logging of the capture buffer to an external FTP server. When the buffer fills up, the packets are transferred to the FTP server. The capture continues without interruption.

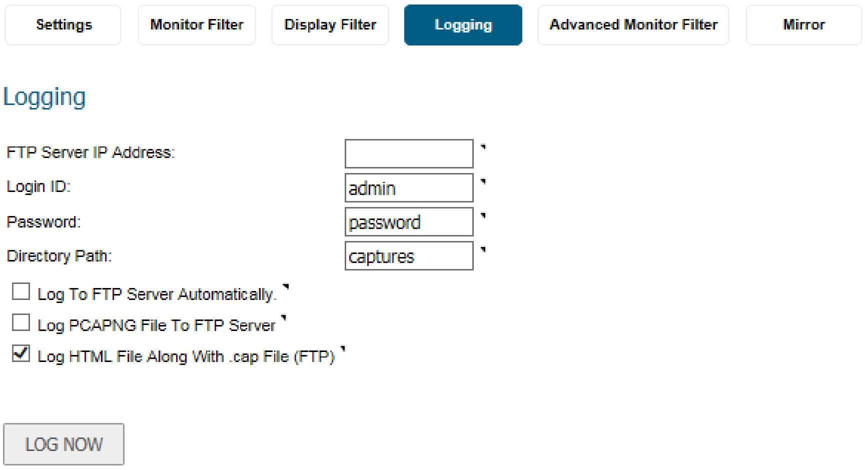
If you configure automatic FTP logging, this supersedes the setting for wrapping the buffer when full. With automatic FTP logging, the capture buffer is effectively wrapped when full, but you also retain all the data rather than overwriting it each time the buffer wraps.

Topics:

Configuring Logging Settings

To configure logging settings:

1. Navigate to the **Tools > Packet Monitor** page on the **INVESTIGATE** view.
2. Click **Configure**. The **Packet Monitor Configuration** dialog displays.
3. Click the **Logging** tab.



Logging

FTP Server IP Address:

Login ID: admin

Password: password

Directory Path: captures

☐ Log To FTP Server Automatically.

☐ Log PCAPNG File To FTP Server

☑ Log HTML File Along With .cap File (FTP)

4. In the **FTP Server IP Address** field, enter the IP address of the FTP server where captured packets are to be logged.

   > **NOTE:** Ensure that the FTP server IP address is reachable by the firewall. An IP address that is reachable only through a VPN tunnel is not supported.

5. In the **Login ID** field, enter the login name that the firewall should use to connect to the FTP server. The default value is **admin**.
6. In the **Password** field, enter the password that the firewall should use to connect to the FTP server. The default value is **password**.
7. In the **Directory Path** field, enter the directory path for the logged files. The captured files are written to this directory location at the FTP server relative to the default FTP root directory. The default value is **captures**.

   Examples of file names for the different formats:

- **libcap** format, files are named `packet-log--<>.cap`, where the <> contains a run number and date including hour, month, day, and year. For example, `packet-log-h3-22-06292017.cap`.
- **HTML** format, file are named `packet-log_h-<>.html`, where the <> contains a run number and date including hour, month, day, and year. For example: `packet-log_h-3-22-06292017.html`.

8 Check the box for **Log To FTP Server Automatically** to enable automatic logging of the capture file to a remote FTP server. Captured files are named (where the <> contains a run number and date including hour, month, day, and year):

- `packet-log-<>.cap` for libcap format; for example: `packet-log_3-22-06292017.cap`.
- `packet-log-<>.html` for HTML format; for example: `packet-log_3-22-06292017.html`.

This option is not selected by default.

ⓘ | **NOTE:** You must specify an FTP server address in the **FTP Server IP Address** field.

9 Check the box for **Log PCAPNG File To FTP Server** to enable logging of a new generation capture file with comments that include debug information to a remote FTP server. Captured files are named `packet-log-<>.pcapng`, where the <> contains a run number and date including hour, month, day, and year; for example: `packet-log_3-22-06292017.pcapng`. This option is selected by default.

10 Check the box for **Log HTML File Along With cap File (FTP)** to enable transfer of the file in HTML format as well as libcap format. This option is selected by default.

11 To test the connection to the FTP server and transfer the capture buffer contents to it, click the **Log Now**. In this case, the file name contains an F. For example, `packet-log-F-3-22-08292006.cap` or `packet-log_h-F-3-22-06292017.html`.

12 To save your settings and exit the dialog, click **OK**.

Restarting FTP Logging

If automatic FTP logging is off, either because of a failed connection or simply disabled, you can restart it in **Configure > Logging**.

To restart FTP logging:

1 Navigate to the **Tools > Packet Monitor** page on the **INVESTIGATE** view.

2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.

3 Click the **Logging** view.

4 Verify that the settings are correct for each item on the page. See Configuring Logging Settings.

5 To change the FTP logging status page to active, select **Log To FTP Server Automatically**.

6 Optionally, test the connection by clicking **Log Now**.

7 To save your settings and exit the dialog, click **OK**.

Configuring Advanced Monitor Filter Options

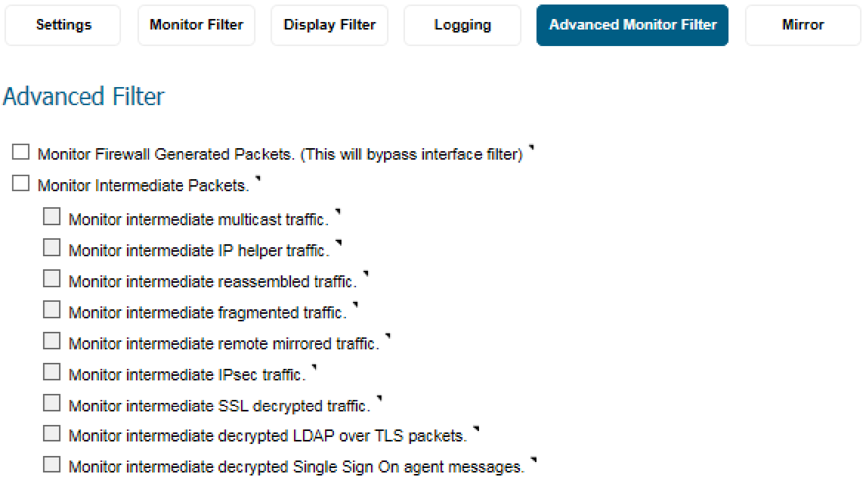
This section describes how to configure monitoring for packets generated by the firewall and for intermediate traffic.

To configure the Advanced Monitor Filter settings:

1 Navigate to the **Tools > Packet Monitor** page on the **INVESTIGATE** view.

2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.

3 Click the **Advanced Monitor Filter** tab.



Advanced Filter

☐ Monitor Firewall Generated Packets. (This will bypass interface filter)

☐ Monitor Intermediate Packets.

- ☐ Monitor intermediate multicast traffic.
- ☐ Monitor intermediate IP helper traffic.
- ☐ Monitor intermediate reassembled traffic.
- ☐ Monitor intermediate fragmented traffic.
- ☐ Monitor intermediate remote mirrored traffic.
- ☐ Monitor intermediate IPsec traffic.
- ☐ Monitor intermediate SSL decrypted traffic.
- ☐ Monitor intermediate decrypted LDAP over TLS packets.
- ☐ Monitor intermediate decrypted Single Sign On agent messages.

4 Select **Monitor Firewall Generated Packets (This will bypass interface filter)** to capture packets generated by the firewall. This option is not selected by default.

Even when other monitor filters do not match, this option ensures that packets generated by the firewall are captured. This includes packets generated by such protocols as HTTP(S), L2TP, DHCP servers, PPP, PPPOE, and routing. Captured packets are marked with `s` in the incoming interface area when they are from the system stack. Otherwise, the incoming interface is not specified.

> **NOTE:** Specify this option when firewall-generated packets need to be captured even when other capture filters fail to match.

5 Select **Monitor Intermediate Packets** to capture intermediate packets generated by the firewall as a result of various policies. Included are such packets as intermediate encrypted packets, IP help-generated packets, multicast packets that are replicated, and those generated as a result of fragmentation or reassembly.

Selecting this checkbox enables—but does not select—the subsequent options for monitoring specific types of intermediate traffic. This option is not selected by default.

6 Select any of the following options to capture or mirror that type of intermediate traffic. The Monitor filter is still applied on these packets. None of these options is selected by default.

- **Monitor intermediate multicast traffic** – For multicast traffic.
- **Monitor intermediate IP helper traffic** – For replicated IP Helper packets.
- **Monitor intermediate reassembled traffic** – For reassembled IP packets.
- **Monitor intermediate fragmented traffic** – For packets fragmented by the firewall.
- **Monitor intermediate remote mirrored traffic** – For remote mirrored packets after de-encapsulation.
- **Monitor intermediate IPsec traffic** – For IPSec packets after encryption and decryption.
- **Monitor intermediate SSL decrypted traffic** – For SSL decrypted packets.

ⓘ **NOTE:** SSL decrypted traffic are sent to the Packet Monitor, and some of the IP and TCP header fields might not be accurate in the monitored packets. IP and TCP checksums are not calculated on the decrypted packets. TCP port numbers are remapped to port 80.

DPI-SSL must be enabled to decrypt the packets along with any of the security services to be applied to such packets.

- **Monitor intermediate decrypted LDAP over TLS packets** – For decrypted LDAP over TLS (LDAPS) packets. The packets are marked with `ldp` in the ingress/egress interface fields and have dummy Ethernet, IP, and TCP headers with some inaccurate fields. The LDAP server port is set to 389 so an external capture analysis program decode it as LDAP. Passwords in captured LDAP bind requests are obfuscated.

  ⓘ **NOTE:** Decrypted LDAPS packets are sent to the Packet Monitor.

- **Monitor intermediate decrypted Single Sign On agent messages** – For decrypted messages to or from the SSO authentication agent. The packets are marked with `sso` in the ingress/egress interface fields and have dummy Ethernet, IP, and TCP headers with some inaccurate fields.

  ⓘ **NOTE:** Decrypted SSO packets are sent to the Packet Monitor.

7 To save your settings and exit the dialog, click **OK**.

Configuring Mirror Settings

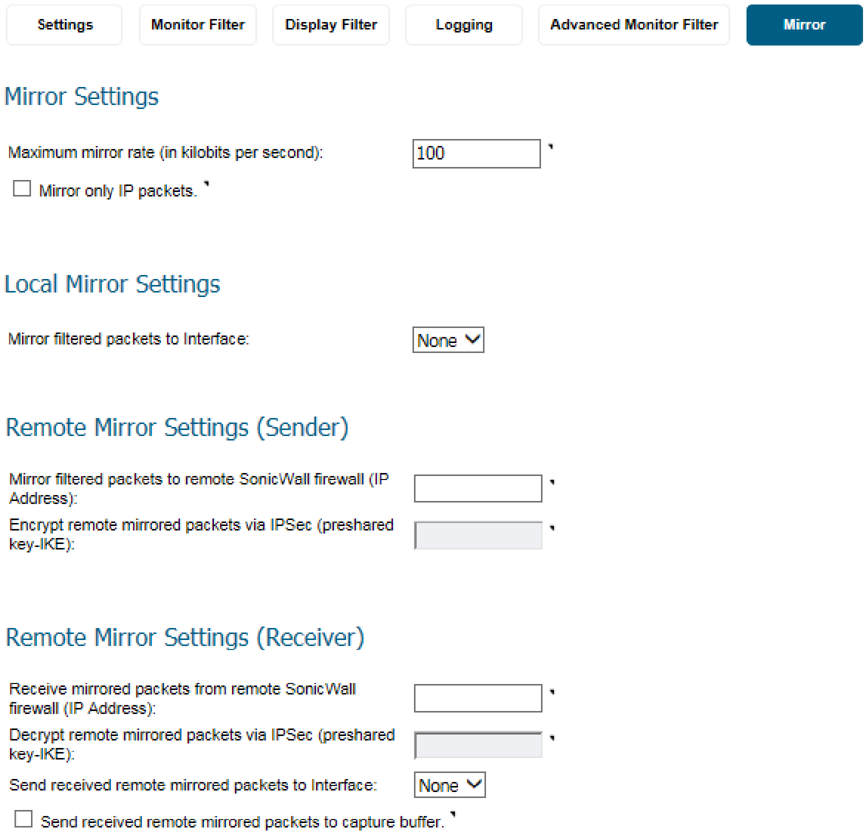
This section describes how to configure Packet Monitor mirror settings. Mirror settings provide a way to send packets to a different physical port of the same firewall or to send packets to, or receive them from, a remote SonicWall firewall.

To configure mirror settings:

1 Navigate to the **Tools > Packet Monitor** page on the **INVESTIGATE** view.

2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.

3 Click **Mirror**.



Mirror Settings

Maximum mirror rate (in kilobits per second): 100

□ Mirror only IP packets.

Local Mirror Settings

Mirror filtered packets to Interface: None

Remote Mirror Settings (Sender)

Mirror filtered packets to remote SonicWall firewall (IP Address):

Encrypt remote mirrored packets via IPSec (preshared key-IKE):

Remote Mirror Settings (Receiver)

Receive mirrored packets from remote SonicWall firewall (IP Address):

Decrypt remote mirrored packets via IPSec (preshared key-IKE):

Send received remote mirrored packets to Interface: None

□ Send received remote mirrored packets to capture buffer.

4 Under **Mirror Settings**, enter the desired **Maximum mirror rate (in kilobits per second)**. If this rate is exceeded during mirroring, the excess packets are not mirrored but counted as skipped packets. This rate applies to mirroring both locally to an interface or to a remote firewall. The default and minimum value is **100** kbps, and the maximum is 1 Gbps.

5 Select **Mirror only IP packets** to prevent mirroring of any non-IP packets, such as ARP or PPPoE. If selected, this option overrides any non-IP Ether types entered in the **Ether Type(s)** field on the **Monitor Filter** tab.

6 Under **Local Mirror Settings**, select the destination interface for locally mirrored packets in the **Mirror filtered packets to Interface** drop-down menu. The default is **None**.

7 Under **Remote Mirror Settings (Sender)**, in the **Mirror filtered packets to remote SonicWall firewall (IP Address)** field, enter the IP address of the remote SonicWall where mirrored packets are sent. Packets are encapsulated and set to the remote device (specified IP address).

> ⓘ **NOTE:** The remote SonicWall must be configured to receive the mirrored packets.

8 In the **Encrypt remote mirrored packets via IPSec (preshared key-IKE)** field, enter the preshared key to be used to encrypt traffic when sending mirrored packets to the remote firewall. Configuring this field enables an IPSec transport mode tunnel between this appliance and the remote firewall. This preshared key is used by IKE to negotiate the IPSec keys.

> ⓘ **NOTE:** Enabling this option also enables an IPSec transport mode tunnel between this appliance and the remote firewall.

9 Under **Remote Mirror Settings (Receiver)**, in the **Receive mirrored packets from remote SonicWall firewall (IP Address)** field, enter the IP address of the remote appliance that receives mirrored packets.

Packets are decapsulated and sent either to a local buffer or out of another interface as specified in the following options.

> **NOTE:** The remote SonicWall must be configured to send the mirrored packets.

10 In the **Decrypt remote mirrored packets via IPSec (preshared key-IKE)** field, enter the previously configured preshared key to be used to encrypt/decrypt traffic when receiving mirrored packets from the remote firewall. This preshared key is used by IKE to negotiate the IPSec keys.

> **NOTE:** Enabling this option also enables an IPSec transport mode tunnel between this appliance and the remote firewall.

11 To mirror received packets to another interface on the local SonicWall, select the interface from the **Send received remote mirrored packets to Interface** drop-down menu. The default is **None**.

12 Select **Send received remote mirrored packets to capture buffer** to save all remote mirrored packets in the local capture buffer. This option is independent of sending mirrored packets to another interface, and both can be enabled if desired.

13 To save your settings and exit the dialog, click **OK**.

Verifying Packet Monitor Activity

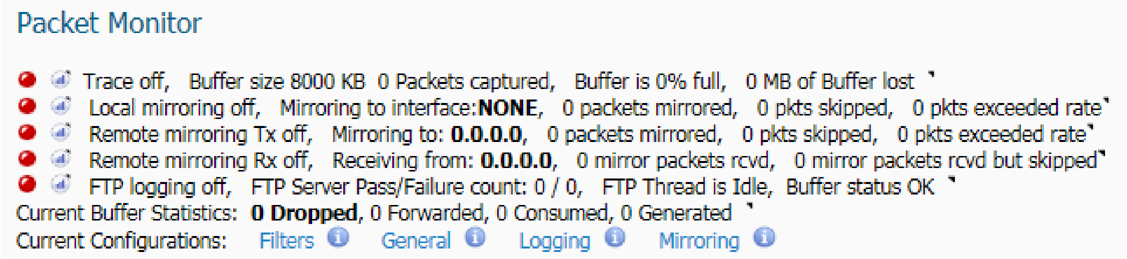
This section describes how to tell if your packet monitor, mirroring, or FTP logging is working correctly based on the configuration.

Topics:

- Understanding Status Indicators on page 93
- Clearing the Status Information on page 96

Understanding Status Indicators

The **Packet Monitor** section displays status indicators for packet capture (trace), mirroring, and FTP logging. Information pop-up tooltips display the configuration settings.



Packet Monitor

● Trace off, Buffer size 8000 KB 0 Packets captured, Buffer is 0% full, 0 MB of Buffer lost
● Local mirroring off, Mirroring to interface:**NONE**, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
● Remote mirroring Tx off, Mirroring to: **0.0.0.0**, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
● Remote mirroring Rx off, Receiving from: **0.0.0.0**, 0 mirror packets rcvd, 0 mirror packets rcvd but skipped
● FTP logging off, FTP Server Pass/Failure count: 0 / 0, FTP Thread is Idle, Buffer status OK
Current Buffer Statistics: **0 Dropped**, 0 Forwarded, 0 Consumed, 0 Generated
Current Configurations: Filters General Logging Mirroring

Topics:

- Packet Capture Status (Trace) on page 94
- Mirroring Status on page 94
- FTP Logging Status on page 95
- Current Buffer Statistics on page 95
- Current Configurations on page 96

Packet Capture Status (Trace)

The first line in the **Packet Monitor** section is the packet capture status indicator that is labeled **Trace**, and shows one of the following three conditions:

- **Red** – Capture is stopped
- **Green** – Capture is running and the buffer is not full
- **Yellow** – Capture is on, but the buffer is full

The **Trace** also displays:

- On/off indicator
- **Buffer size**, in KB
- Number of **Packets captured**
- Percentage of buffer space used (**Buffer is % full)**
- How much of the buffer has been lost (**MB of Buffer lost**). Lost packets occur when automatic FTP logging is turned on, but the file transfer is slow. If the transfer is not finished by the time the buffer is full again, the data in the newly filled buffer is lost.

  > ⓘ **NOTE:** Although the buffer wrap option clears the buffer upon wrapping to the beginning, this is not considered lost data.

Mirroring Status

There are three status indicators for packet mirroring:

- **Local mirroring –** Packets sent to another physical interface on the same SonicWall

  For local mirroring, the status indicator shows one of the following three conditions:

  - **Red** – Mirroring is off
  - **Green** – Mirroring is on
  - **Yellow** – Mirroring is on but disabled because the local mirroring interface is not specified

  The local mirroring row also displays the following statistics:

  - On/off indicator
  - **Mirroring to interface** – The specified local mirroring interface
  - **packets mirrored** – The total number of packets mirrored locally
  - **pkts skipped** – The total number of packets that skipped mirroring because of packets that are incoming/outgoing on the interface on which monitoring is configured
  - **pkts exceeded rate** – The total number of packets that skipped mirroring because of rate limiting
- **Remote mirroring Tx –** Packets sent to a remote SonicWall

  For Remote mirroring Tx, the status indicator shows one of the following three conditions:

  - **Red** – Mirroring is off
  - **Green** – Mirroring is on and a remote SonicWall IP address is configured
  - **Yellow** – Mirroring is on but disabled because the remote device rejects mirrored packets and sends port unreachable ICMP messages

  The Remote mirroring Tx row also displays the following statistics:

  - On/off indicator

  - **Mirroring to** – The specified remote SonicWall IP address
  - **packets mirrored** – The total number of packets mirrored to a remote SonicWall appliance
  - **pkts skipped** – The total number of packets that skipped mirroring because of packets that are incoming/outgoing on the interface on which monitoring is configured
  - **pkts exceeded rate** – The total number of packets that failed to mirror to a remote SonicWall, either because of an unreachable port or other network issues
- **Remote mirroring Rx –** Packets received from a remote SonicWall

  For Remote mirroring Rx, the status indicator shows one of the following two conditions:

  - **Red** – Mirroring is off
  - **Green** – Mirroring is on and a remote SonicWall IP address is configured

  The Remote mirroring Rx row also displays the following statistics:

  - On/off indicator
  - **Receiving from** – The specified remote SonicWall IP address
  - **mirror packets rcvd** – The total number of packets received from a remote SonicWall appliance
  - **mirror packets rcvd but skipped** – The total number of packets received from a remote SonicWall appliance that failed to get mirrored locally because of errors in the packets

FTP Logging Status

The FTP logging status indicator shows one of the following three conditions:

- **Red** – Automatic FTP logging is off
- **Green** – Automatic FTP logging is on
- **Yellow** – The last attempt to contact the FTP server failed, and logging is now off

  ⓘ **NOTE:** To restart automatic FTP logging, see Restarting FTP Logging on page 89.

The FTP logging row also displays the following statistics:

- On/off indicator
- **FTP Server Pass/Failure count: 0/0** – the number of successful and failed attempts to transfer the buffer contents to the FTP server
- **FTP Thread is Busy/Idle** – the current state of the FTP process thread
- **Buffer status** – the status of the capture buffer

Current Buffer Statistics

The **Current Buffer Statistics** row summarizes the number of each type of packet in the local capture buffer:

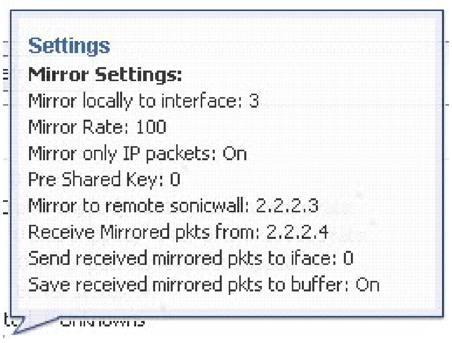
- **Dropped** – number of dropped packets
- **Forwarded** – number of dropped packets
- **Consumed** – number of dropped packets
- **Generated**, – number of dropped packets

Current Configurations

The **Current Configurations** row provides dynamic information about configured settings for:

- **Filters**, both **Capture Filters** and **Display Filters**
- **General**, both **General Settings** and **Advanced Settings**
- **Logging**
- **Mirroring**, **Mirror Settings**

When you hover your mouse pointer over one of the information icons or its label, a pop-up tooltip displays the current settings for that selection.



Settings
Mirror Settings:
Mirror locally to interface: 3
Mirror Rate: 100
Mirror only IP packets: On
Pre Shared Key: 0
Mirror to remote sonicwall: 2.2.2.3
Receive Mirrored pkts from: 2.2.2.4
Send received mirrored pkts to iface: 0
Save received mirrored pkts to buffer: On

Clearing the Status Information

To clear the packet monitor queue and the displayed statistics:

1. Navigate to the **Tools | Packet Monitor** page on the **INVESTIGATE** view.
2. Click **Clear**.

Using Packet Monitor and Packet Mirror

In addition to **Configure** , the bottom of the **Tools > Packet Monitor** page provides several buttons for general control of the packet monitor feature and display:

- **CONFIGURE** – Displays the **Packet Monitor Configuration** dialog. For more information refer to Configuring Packet Monitor on page 82.
- **MONITOR ALL** – Resets current monitor filter settings and advanced page settings so that traffic on all local interfaces is monitored. A confirmation dialog displays when you click this button.
- **MONITOR DEFAULT**– Resets current monitor filter settings and advanced page settings to factory default settings. A confirmation dialog displays when you click this button.
- **CLEAR** – Clears the packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging.
- **REFRESH** – Refreshes the packet display windows on this page to show new buffer data.

Other buttons and displays on this page are described in:

- Starting and Stopping Packet Capture on page 97
- Starting and Stopping Packet Mirror on page 97
- Viewing Captured Packets on page 97

Starting and Stopping Packet Capture

Start a packet capture that uses default settings without configuring specific criteria for packet capture, display, FTP export, and other settings. If you start a default packet capture, the SonicWall security appliance captures all packets except those for internal communication, and stops when the buffer is full or when you click **Stop Capture**.

1. Navigate to the **Tools > Packet Monitor** page on the **INVESTIGATE** view.
2. If you want to set the statistics back to zero, click **CLEAR** at the bottom of the page.
3. Under **Packet Monitor**, click **START CAPTURE**.
4. To refresh the packet displays to show new buffer data, click **REFRESH** at the bottom of the page.
5. To stop the packet capture, click **STOP CAPTURE**.

View the captured packets in the **Captured Packets**, **Packet Detail**, and **Hex Dump** sections of the **Packet Monitor** page.

Starting and Stopping Packet Mirror

Start packet mirroring that uses your configured mirror settings by clicking **START MIRROR**. It is not necessary to first configure specific criteria for display, logging, FTP export, and other settings. Packet mirroring stops when you click **STOP MIRROR**.

To start or stop Packet Monitor:

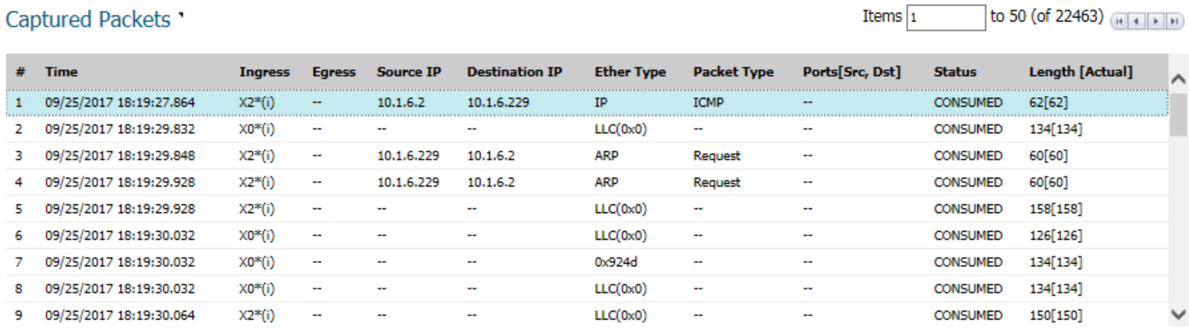
1. Navigate to the **Tools > Packet Monitor** page on the **INVESTIGATE** view.
2. Under **Packet Monitor**, click **START MIRROR** to start mirroring packets according to your configured settings.
3. To stop mirroring packets, click **STOP MIRROR**.

Viewing Captured Packets

The **Tools | Packet Monitor** page provides three sections to display different views of captured packets:

- Captured Packets on page 98
- Packet Detail on page 99
- Hex Dump on page 99

Captured Packets



Captured Packets

Items 1 to 50 (of 22463)

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
1	09/25/2017 18:19:27.864	X2*(i)	--	10.1.6.2	10.1.6.229	IP	ICMP	--	CONSUMED	62[62]
2	09/25/2017 18:19:29.832	X0*(i)	--	--	--	LLC(0x0)	--	--	CONSUMED	134[134]
3	09/25/2017 18:19:29.848	X2*(i)	--	10.1.6.229	10.1.6.2	ARP	Request	--	CONSUMED	60[60]
4	09/25/2017 18:19:29.928	X2*(i)	--	10.1.6.229	10.1.6.2	ARP	Request	--	CONSUMED	60[60]
5	09/25/2017 18:19:29.928	X2*(i)	--	--	--	LLC(0x0)	--	--	CONSUMED	158[158]
6	09/25/2017 18:19:30.032	X0*(i)	--	--	--	LLC(0x0)	--	--	CONSUMED	126[126]
7	09/25/2017 18:19:30.032	X0*(i)	--	--	--	0x924d	--	--	CONSUMED	134[134]
8	09/25/2017 18:19:30.032	X0*(i)	--	--	--	LLC(0x0)	--	--	CONSUMED	134[134]
9	09/25/2017 18:19:30.064	X2*(i)	--	--	--	LLC(0x0)	--	--	CONSUMED	150[150]

The **Captured Packets** section displays the following statistics about each packet:

- **#** - The packet number relative to the start of the capture.
- **Time** - The date and time that the packet was captured.
- **Ingress** - The firewall interface on which the packet arrived is marked with an asterisk (*). The subsystem type abbreviation is shown in parentheses. Subsystem type abbreviations are defined in Subsystem Type Abbreviations.

  Subsystem Type Abbreviations

Abbreviation	Definition
i	Interface
hc	Hardware-based encryption or decryption
sc	Software-based encryption or decryption
m	Multicast
r	Packet reassembly
s	System stack
ip	IP helper
f	Fragmentation

- **Egress** - The firewall interface on which the packet was captured when sent out. The subsystem type abbreviation is shown in parentheses. See Subsystem Type Abbreviations for definitions of subsystem type abbreviations.
- **Source IP** - The source IP address of the packet.
- **Destination IP** - The destination IP address of the packet.
- **Ether Type** - The Ethernet type of the packet from its Ethernet header.
- **Packet Type** - The type of the packet depending on the Ethernet type; for example:

Ethernet type	Packet type
IP packets	TCP, UDP, or another protocol that runs over IP
PPPoE packets	PPPoE Discovery or PPPoE Session
ARP packets	Request or Reply

- **Ports [Src, Dst]** - The source and destination TCP or UDP ports of the packet
- **Status** - The status field for the packet

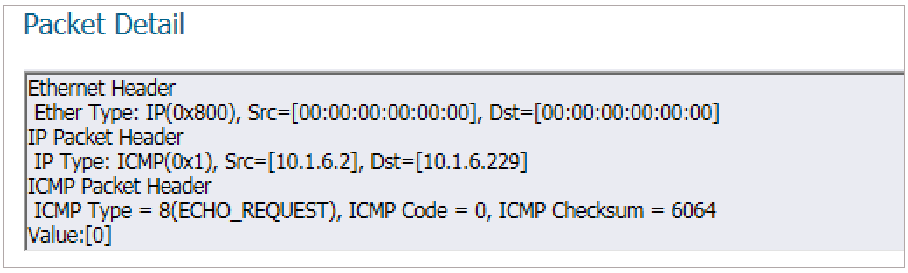
The **Status** field shows the state of the packet with respect to the firewall. A packet can be dropped, generated, consumed, or forwarded by the firewall. Position the mouse pointer over dropped or consumed packets to show this information:

Packet Status	Displayed Value	Definition of Displayed Value
Dropped	Module-ID = <*integer*>	Value for the protocol subsystem ID
	Drop-code = <*integer*>	Reason for dropping the packet
	Reference-ID: <*code*>	SonicWall-specific data
Consumed	Module-ID = <*integer*>	Value for the protocol subsystem ID

- **Length [Actual]** - Length value is the number of bytes captured in the buffer for this packet. Actual value, in brackets, is the number of bytes transmitted in the packet.

Packet Detail

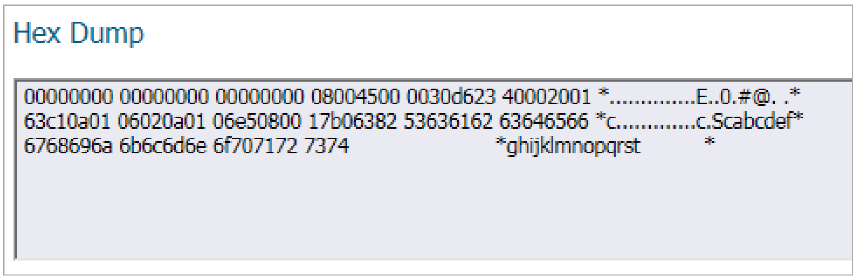
When you click a packet in the **Captured Packets** section, the packet header fields are displayed in the **Packet Detail** section. The display varies depending on the type of packet that you select.



```
Ethernet Header
 Ether Type: IP(0x800), Src=[00:00:00:00:00:00], Dst=[00:00:00:00:00:00]
IP Packet Header
 IP Type: ICMP(0x1), Src=[10.1.6.2], Dst=[10.1.6.229]
ICMP Packet Header
 ICMP Type = 8(ECHO_REQUEST), ICMP Code = 0, ICMP Checksum = 6064
Value:[0]
```

Hex Dump

When you click a packet in the **Captured Packets** section, the packet data is displayed in hexadecimal and ASCII format in the **Hex Dump** section. The hex format is shown on the left side of the window, with the corresponding ASCII characters displayed to the right for each line. When the hex value is zero, the ASCII value is displayed as a dot.



```
00000000 00000000 00000000 08004500 0030d623 40002001 *..............E..0.#@. .*
63c10a01 06020a01 06e50800 17b06382 53636162 63646566 *c............c.Scabcdef*
6768696a 6b6c6d6e 6f707172 7374                      *ghijklmnopqrst          *
```

14

Packet Replay

Topics:

About Packet Replay

Packet replay is an integrated tool to firewall for testing and debugging purposes. Replay packets three ways:

- Craft a packet

  Specify packet header fields and payload, one by one, through the management interface.
- Use packet buffer

  Input packet data (both header and payload) or just copy from other places and paste it.
- Replay Pcap file

  Replay a sequence of packets stored in a Pcap file.

Replayed packets are restrained from traveling outside this firewall; they are dropped before transmitting through interfaces.

Single Packets

The following procedures describes how to craft a packet for analysis. Some fields change when the IP type is changed.

- Packet Crafting on page 100
- Packet Buffer on page 102

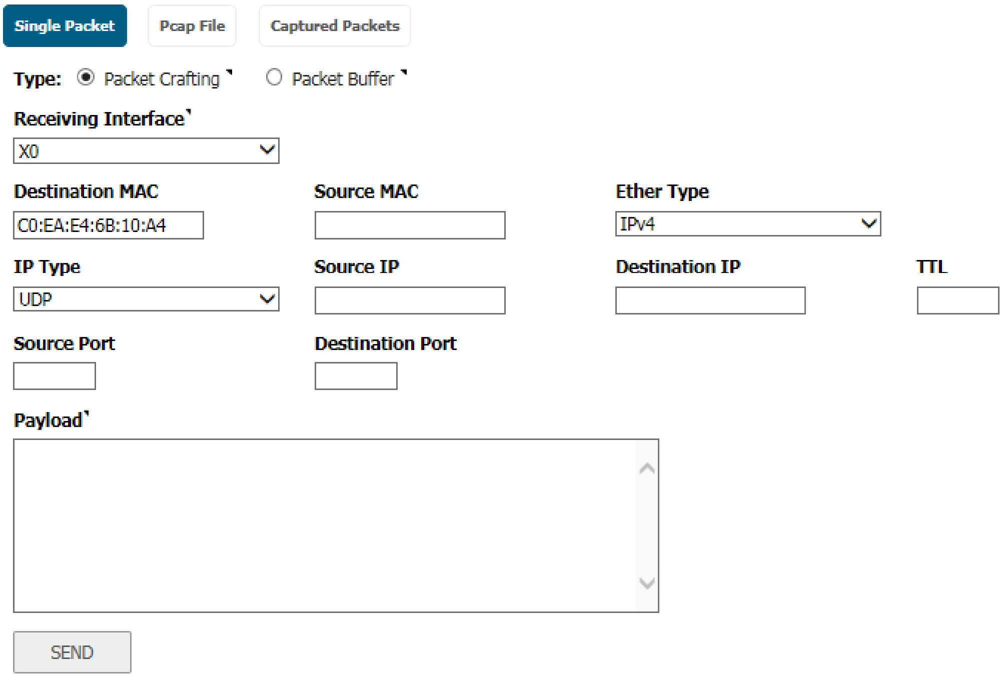
Packet Crafting

The following procedure uses **IP Type** = **UDP**.

To craft a packet:

1 Navigate to **Tools > Packet Replay** on the **INVESTIGATE** view.

2 Click **Single Packet**.



Type: ● Packet Crafting ○ Packet Buffer

Receiving Interface: X0

Destination MAC: C0:EA:E4:6B:10:A4

Source MAC:

Ether Type: IPv4

IP Type: UDP

Source IP:

Destination IP:

TTL:

Source Port:

Destination Port:

Payload:

3 Choose **Packet Crafting**.

4 Enter the following information; options change depending on your selection for **IP Type**:

IP Type = UDP

Field	Definition
Receiving Interface	Select the interface from which the packet is received.
Destination MAC	Enter the destination MAC address.
Source MAC	Enter the source MAC address.
Ether Type	Select the protocol type. The default is **IPv4**.
IP Type	Select **UDP**.
Source IP	Enter the source IP address.
Destination IP	Enter the destination IP address.
TTL	Enter the IP header.
Source Port	Enter the UDP source port number.
Destination Port	Enter the UDP destination port number.

If you select **IP Type** = **ICMP**, these fields are different from UDP:

IP Type = ICMP

Field	Definition
ICMP Type	Select **Echo Request** or **Echo Response** from the drop-down menu.
ID	Type in the ICMP identifier.
Sequence	Type in the ICMP sequence number.

If you select **IP Type** = **IGMP**, these fields are different from UDP:

IP Type = IGMP

Field	Definition
IGMP Type	Select **IGMP Type** from the drop-down menu. The default is **Membership Query**.
Max Response	Type in the IGMP maximum response timeout. Enter the value in seconds.
Group IP Address	Type in the group IP address for the query.

5 In the **Payload** field, enter or copy the payload hex data.

6 Click **SEND**.

The crafted packet is sent to the firewall engine.

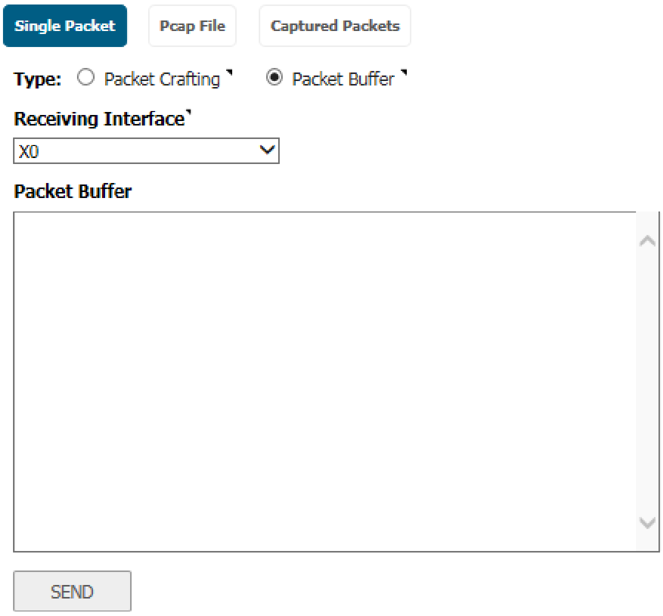
Packet Buffer

To build a packet buffer:

1 Navigate to **Tools > Packet Replay** on the **INVESTIGATE** view.

2 Click **Single Packet**.

3 Choose **Packet Buffer**.



Type: ○ Packet Crafting ● Packet Buffer

Receiving Interface: X0

Packet Buffer

4 Select the interface to receive the data from **Receiving Interface**.

5 Enter the **Packet Buffer** data, in hex.

6 Click **SEND**.

The crafted packet is sent to the firewall engine.

Replay Pcap File

The Pcap filter can be defined by IP address or MAC address.

Topics:

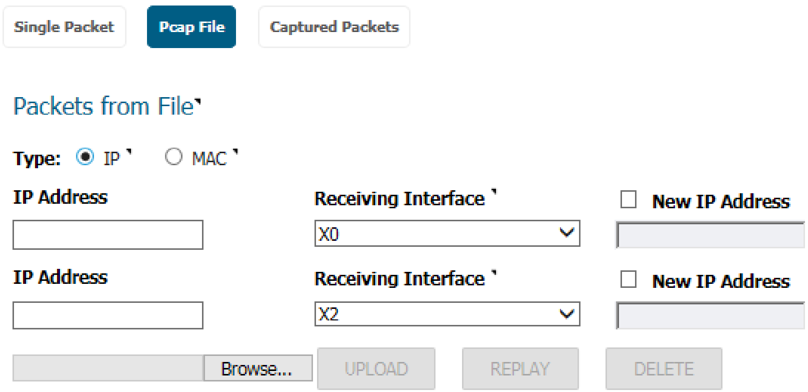
- Replaying an IP Pcap File on page 103
- Replaying a MAC Pcap File on page 104

Replaying an IP Pcap File

To define by IP:

1 Navigate to **Tools > Packet Replay** on the **INVESTIGATE** view.

2 Click **Pcap File**.



Packets from File

Type: ● IP ○ MAC

IP Address	Receiving Interface	New IP Address
	X0	□
	X2	□

3 Choose **IP** in the **Type** field. Two IP filters are provided.

4 For each IP filter complete the following:

Field	Definition
IP Address	Enter the destination address to be looked up.
Receiving Interface	Select the receiving interface. The IP packets that have the destination address listed in **IP Address** are assume to arrive from the interface selected in this option.
New IP Address	If enabled (the option is selected), the new IP address listed in this field replaces the filtered destination IP address when replaying the packets.

5 To search for and select a Pcap file to be replayed. click **Browse**.

6 To upload the selected file, click **UPLOAD**.

7 To replay the packets in the uploaded Pcap file, click **REPLAY**.

8 When done, to delete the uploaded file, click **DELETE**.

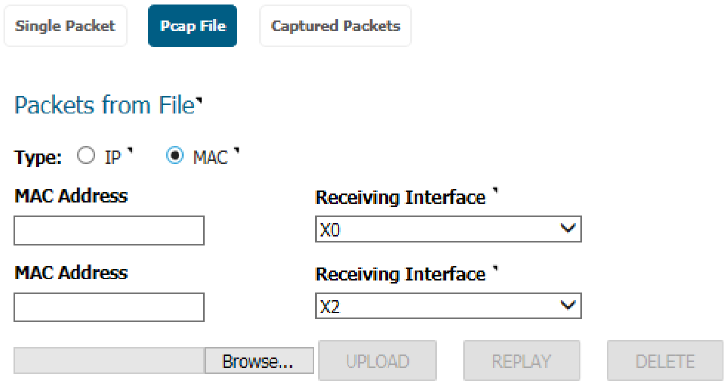
Replaying a MAC Pcap File

To define by MAC:

1 Navigate to **Tools > Packet Replay** on the **INVESTIGATE** view.

2 Click **Pcap File**.

3 Select **MAC** in the **Type** field. Two IP filters are provided.



4 For each IP filter, complete the following:

Field	Definition
MAC Address	Enter the destination address to be looked up.
Receiving Interface	Select the receiving interface. The packets that have the destination MAC address listed in **MAC Address** are assume to arrive from the interface selected in this field.
New IP Address	If enabled (the option is selected), the new IP address listed in this field replaces the filtered destination IP address when replaying the packets.

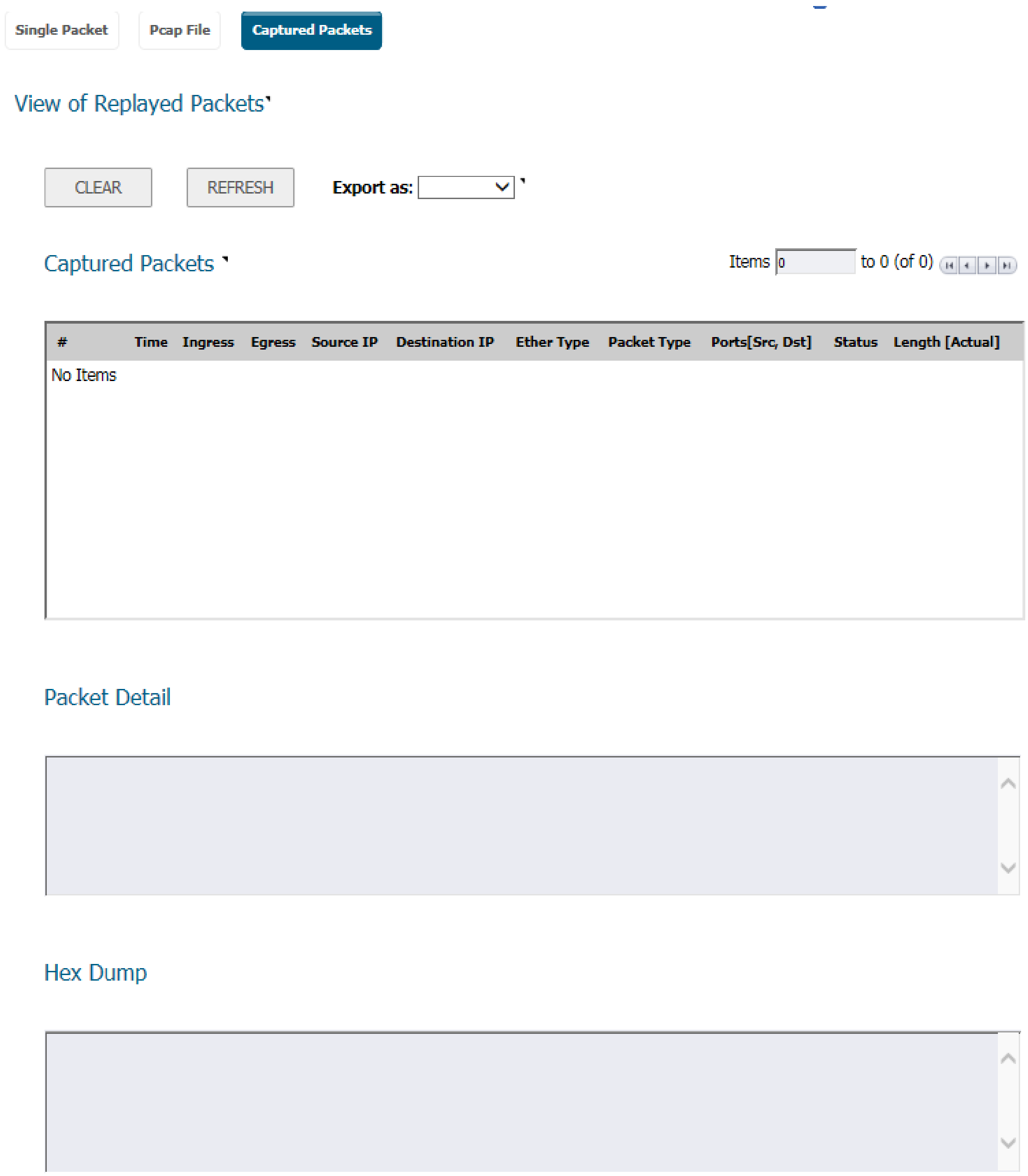
5 To search for and select a Pcap file to be replayed. click **Browse**.

6 To upload the selected file, click **UPLOAD**.

7 To replay the packets in the uploaded Pcap file, click **REPLAY**.

8 When done, to delete the uploaded file, click **DELETE**.

Captured Packets



View of Replayed Packets

Export as:

Captured Packets

Items 0 to 0 (of 0)

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
No Items										

Packet Detail

Hex Dump

Captured, replayed packets are displayed on the **Captured Packets** page. Navigate to **Tools > Packet Replay** on the **INVESTIGATE** view, and click **Captured Packets**. The **Captured Packets** page provides three sections to display different views of captured packets:

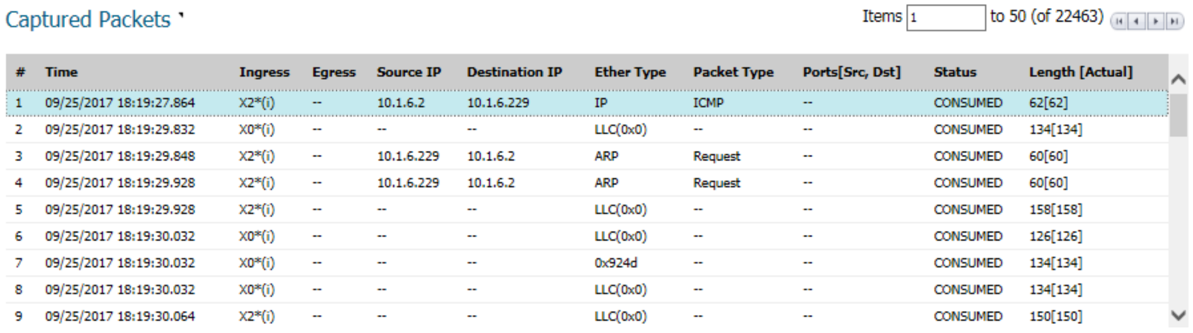
- Captured Packets on page 106
- Packet Detail on page 107
- Hex Dump on page 107

Use these options to manage the Captured Packets:

- **CLEAR** – Clears the packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging.

- **REFRESH** – Refreshes the packet display windows on this page to show new buffer data.
- **Export as** – Exports the file in the format you select from the drop-down menu. Saved files are placed on your local management system.

Captured Packets



Captured Packets

Items 1 to 50 (of 22463)

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
1	09/25/2017 18:19:27.864	X2*(i)	--	10.1.6.2	10.1.6.229	IP	ICMP	--	CONSUMED	62[62]
2	09/25/2017 18:19:29.832	X0*(i)	--	--	--	LLC(0x0)	--	--	CONSUMED	134[134]
3	09/25/2017 18:19:29.848	X2*(i)	--	10.1.6.229	10.1.6.2	ARP	Request	--	CONSUMED	60[60]
4	09/25/2017 18:19:29.928	X2*(i)	--	10.1.6.229	10.1.6.2	ARP	Request	--	CONSUMED	60[60]
5	09/25/2017 18:19:29.928	X2*(i)	--	--	--	LLC(0x0)	--	--	CONSUMED	158[158]
6	09/25/2017 18:19:30.032	X0*(i)	--	--	--	LLC(0x0)	--	--	CONSUMED	126[126]
7	09/25/2017 18:19:30.032	X0*(i)	--	--	--	0x924d	--	--	CONSUMED	134[134]
8	09/25/2017 18:19:30.032	X0*(i)	--	--	--	LLC(0x0)	--	--	CONSUMED	134[134]
9	09/25/2017 18:19:30.064	X2*(i)	--	--	--	LLC(0x0)	--	--	CONSUMED	150[150]

The **Captured Packets** section displays the following statistics about each packet:

- **#** - The packet number relative to the start of the capture.
- **Time** - The date and time that the packet was captured.
- **Ingress** - The firewall interface on which the packet arrived is marked with an asterisk (*). The subsystem type abbreviation is shown in parentheses. Subsystem type abbreviations are defined in Subsystem Type Abbreviations.

  Subsystem Type Abbreviations

Abbreviation	Definition
i	Interface
hc	Hardware-based encryption or decryption
sc	Software-based encryption or decryption
m	Multicast
r	Packet reassembly
s	System stack
ip	IP helper
f	Fragmentation

- **Egress** - The firewall interface on which the packet was captured when sent out. The subsystem type abbreviation is shown in parentheses. See Subsystem Type Abbreviations for definitions of subsystem type abbreviations.
- **Source IP** - The source IP address of the packet.
- **Destination IP** - The destination IP address of the packet.
- **Ether Type** - The Ethernet type of the packet from its Ethernet header.
- **Packet Type** - The type of the packet depending on the Ethernet type; for example:

Ethernet type	Packet type
IP packets	TCP, UDP, or another protocol that runs over IP

Ethernet type	Packet type
PPPoE packets	PPPoE Discovery or PPPoE Session
ARP packets	Request or Reply

- **Ports [Src, Dst]** - The source and destination TCP or UDP ports of the packet.
- **Status** - The status field for the packet.

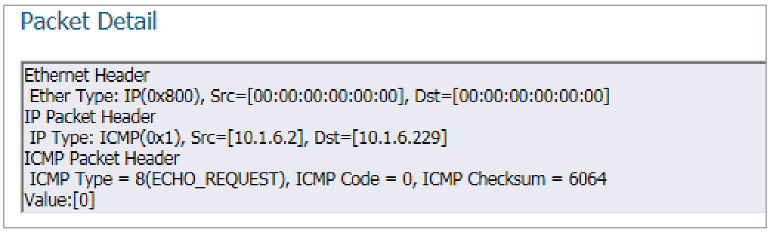
  The **Status** field shows the state of the packet with respect to the firewall. A packet can be dropped, generated, consumed, or forwarded by the firewall. Position the mouse pointer over dropped or consumed packets to show this information:

Packet Status	Displayed Value	Definition of Displayed Value
Dropped	Module-ID = <*integer*>	Value for the protocol subsystem ID
	Drop-code = <*integer*>	Reason for dropping the packet
	Reference-ID: <*code*>	SonicWall-specific data
Consumed	Module-ID = <*integer*>	Value for the protocol subsystem ID

- **Length [Actual]** - Length value is the number of bytes captured in the buffer for this packet. Actual value, in brackets, is the number of bytes transmitted in the packet.

Packet Detail

When you click a packet in the **Captured Packets** section, the packet header fields are displayed in the **Packet Detail** section. The display varies depending on the type of packet that you select.

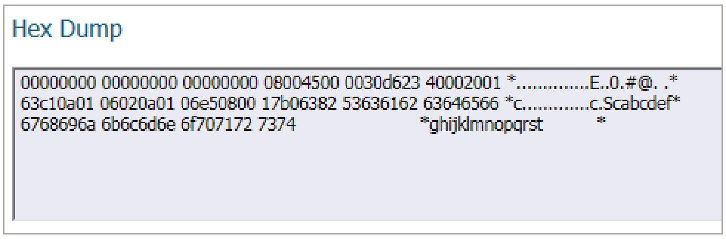


Packet Detail

```
Ethernet Header
 Ether Type: IP(0x800), Src=[00:00:00:00:00:00], Dst=[00:00:00:00:00:00]
IP Packet Header
 IP Type: ICMP(0x1), Src=[10.1.6.2], Dst=[10.1.6.229]
ICMP Packet Header
 ICMP Type = 8(ECHO_REQUEST), ICMP Code = 0, ICMP Checksum = 6064
Value:[0]
```

Hex Dump

When you click a packet in the **Captured Packets** section, the packet data is displayed in hexadecimal and ASCII format in the **Hex Dump** section. The hex format is shown on the left side of the window, with the corresponding ASCII characters displayed to the right for each line. When the hex value is zero, the ASCII value is displayed as a dot.



Hex Dump

```
00000000 00000000 00000000 08004500 0030d623 40002001 *..............E..0.#@. .*
63c10a01 06020a01 06e50800 17b06382 53636162 63646566 *c.............c.Scabcdef*
6768696a 6b6c6d6e 6f707172 7374                       *ghijklmnopqrst          *
```

15

Network Probes

Topics:

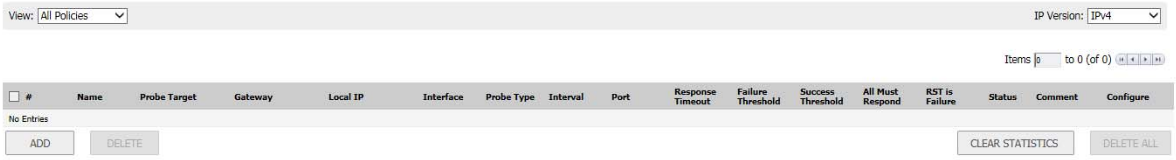
- About Network Probe
- Adding a Network Monitor Policy

About Network Probe

The **Tools > Network Probes** page, on the **INVESTIGATE** view, provides a flexible mechanism for monitoring network path viability. The results and status of this monitoring are displayed dynamically on the **Network Probes** page, and are also provided to affected client components and logged in the system log.

Each custom NM policy defines a destination Address Object to be probed. This Address Object could be a Host, Group, Range, or FQDN. When the destination Address Object is a Group, Range or FQDN with multiple resolved addresses, Network Monitor probes each probe target and derives the NM Policy state based on the results.

SonicOS monitors any remote host status in the local or remote network. SonicOS now checks the availability of the traffic between the appliance and the target host in real time, thereby ensuring the target host can receive network traffic. SonicOS also displays the status of the monitored host on the **Tools > Network Probes** page.



View: All Policies

IP Version: IPv4

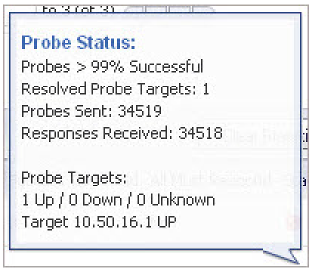
Items 0 to 0 (of 0)

□ #	Name	Probe Target	Gateway	Local IP	Interface	Probe Type	Interval	Port	Response Timeout	Failure Threshold	Success Threshold	All Must Respond	RST is Failure	Status	Comment	Configure
No Entries																

The **Status** column elements displays the status of the network connection to the target:

- Green indicates that the policy status is UP.
- Red indicates that the policy status is DOWN.
- Yellow indicates that the policy status is UNKNOWN.

View details of the probe status by hovering your mouse over the green, red, or yellow light for a policy.



Probe Status:
Probes > 99% Successful
Resolved Probe Targets: 1
Probes Sent: 34519
Responses Received: 34518

Probe Targets:
1 Up / 0 Down / 0 Unknown
Target 10.50.16.1 UP

This information is displayed in the probe status:

- The percent of successful probes.
- The number of resolved probe targets.

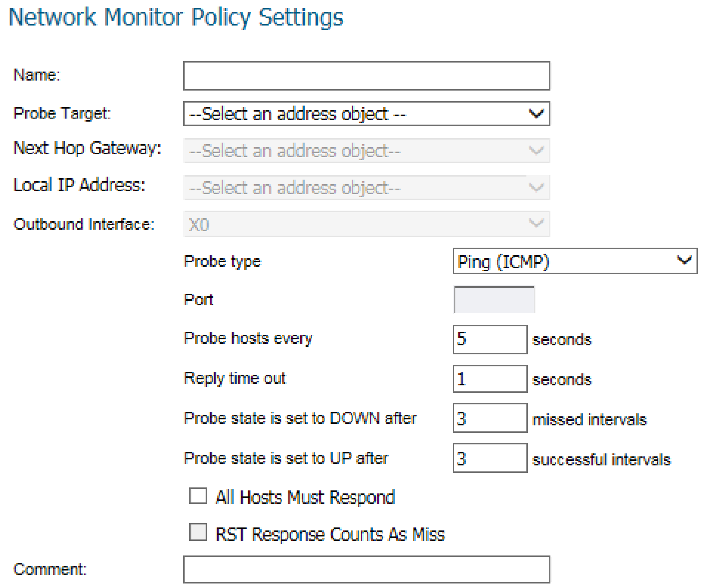
- The total number of probes sent.
- The total number of successful probe responses received.
- A list of resolved probe targets, and their status.

Adding a Network Monitor Policy

To add a network monitor policy:

1 Navigate to **Tools > Network Probes** on the **INVESTIGATE** view.

2 Click **ADD**.



Network Monitor Policy Settings

Name:		
Probe Target:	--Select an address object --	
Next Hop Gateway:	--Select an address object--	
Local IP Address:	--Select an address object--	
Outbound Interface:	X0	
Probe type	Ping (ICMP)	
Port		
Probe hosts every	5	seconds
Reply time out	1	seconds
Probe state is set to DOWN after	3	missed intervals
Probe state is set to UP after	3	successful intervals

☐ All Hosts Must Respond

☐ RST Response Counts As Miss

Comment:

3 Enter the following information to define the network monitor policy:

- **Name** - Enter a description of the Network Monitor policy.
- **Probe Target** - Select the Address Object or Address Group to be the target of the policy. Address Objects could be Hosts, Groups, Ranges, or FQDNs object. Objects within a Group object could be Host, Range, or FQDN Address Objects. Dynamically create a new address object by selecting Create New Address Object.
- **Next Hop Gateway** - Manually specifies the next hop that is used from the outbound interface to reach the probe target. This option must be configured for Explicit Route policies. For non-Explicit Route policies, the probe uses the appliance’s route table to determine the egress interface to reach the probe target. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network.
- **Local IP Address** - Select the local IP address.
- **Outbound Interface -** Manually specifies which interface is used to send the probe. This option must be configured for Explicit Route policies. For non-Explicit Route policies, the probe uses the appliance’s route table to determine the egress interface to reach the probe target.

4 From **Probe type**, select the appropriate type of probe for the network monitor policy:

- **Ping (ICMP)** - This probe uses the route table to find the egress interface and next-hop for the defined probe targets. A Ping echo-request is sent out the egress interface with the source IP address of the egress interface. An echo response must return on the same interface within the specified Response Timeout time limit for the ping to be counted as successful.

- **TCP** - This probe uses the route table to find the egress interface and next-hop for the defined probe targets. A TCP SYN packet is sent to the probe target with the source IP address of the egress interface. A successful response is counted independently for each probe target when the target responds with either an SYN/ACK or an RST through the same interface within the Response Timeout time window. When an SYN/ACK is received, an RST is sent to close the connection. When an RST is received, no response is returned.
- **Ping (ICMP) - Explicit Route** - This probe bypasses the route table and uses the source IP address of the interface specified in the Outbound Interface drop-down menu to send a Ping to the targets. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network.
- **TCP - Explicit Route** - This probe bypasses the route table and uses the source IP address of the interface specified in the Outbound Interface drop-down menu to send a TCP SYN packet to the targets. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network. When an SYN/ACK is received, an RST is sent to close the connection. If an RST is received, no response is returned.

5 Specify the destination **Port** of target hosts for TCP probes. A port is not specified for Ping probes.

6 Optionally, adjust the following thresholds for the probes:

- **Probe hosts every** - The number of seconds between each probe. This number cannot be less than the **Reply time out** field. The default value is **5** seconds.
- **Reply time out** - The number of seconds the Network Probe waits for a response for each individual probe before a missed-probe is counted for the specific probe target. The **Reply time out** cannot exceed the **Probe hosts every** field. The default value is **1** second.
- **Probe state is set to DOWN after** - The number of consecutive missed probes that triggers a host state transition to DOWN. The default is **3** missed intervals.
- **Probe state is set to UP after** - The number of consecutive successful probes that triggers a host state transition to UP. The default is **3** successful intervals.
- **All Hosts Must Respond** - Check this box to enable that all of the probe target Host States must be UP before the Policy State can transition to UP. If not checked, the Policy State is set to UP when any of the Host States are UP. This option is disabled by default.
- **RST Response Counts As Miss** - Check this box to enable that an RST response counts as a missed response.

7 Enter a descriptive comment about the policy in the **Comment** field.

8 Click **ADD** to submit the Network Monitor policy.

When configuring a static route, you can optionally configure a Network Monitor policy for the route. When a Network Monitor policy is used, the static route is dynamically disabled or enabled, based on the state of the probe for the policy. For more information, see **System Setup | Network > Routing** in *SonicWall SonicOS 6.5 System Setup*.

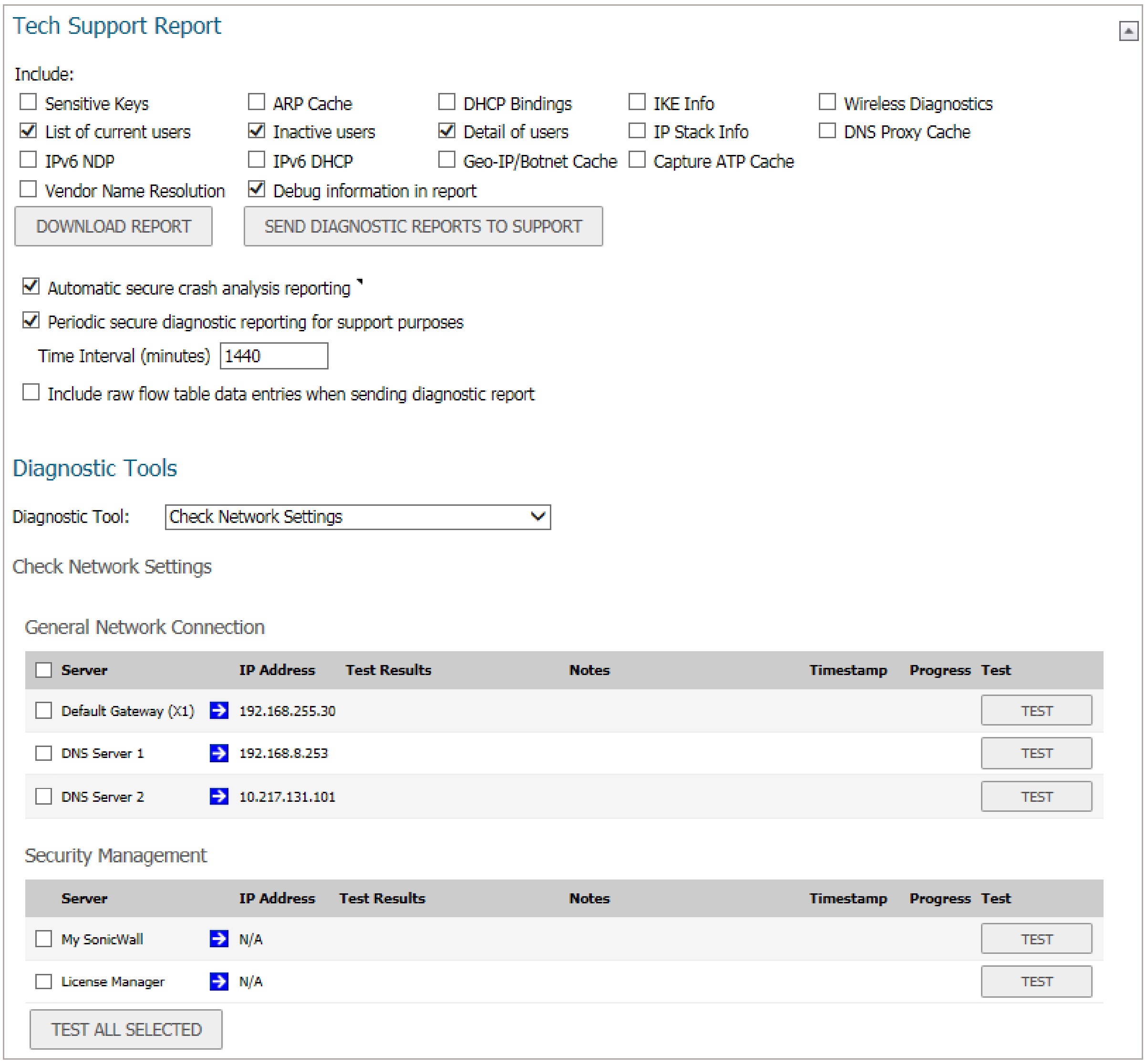
16

System Diagnostics

Topics:

Tools > System Diagnostics

The **INVESTIGATE | Tools > System Diagnostics** page provides several diagnostic tools that help troubleshoot various kinds of network problems and process monitors.



Tech Support Report

Include:

□ Sensitive Keys □ ARP Cache □ DHCP Bindings □ IKE Info □ Wireless Diagnostics
☑ List of current users ☑ Inactive users ☑ Detail of users □ IP Stack Info □ DNS Proxy Cache
□ IPv6 NDP □ IPv6 DHCP □ Geo-IP/Botnet Cache □ Capture ATP Cache
□ Vendor Name Resolution ☑ Debug information in report

DOWNLOAD REPORT SEND DIAGNOSTIC REPORTS TO SUPPORT

☑ Automatic secure crash analysis reporting

☑ Periodic secure diagnostic reporting for support purposes

Time Interval (minutes) 1440

□ Include raw flow table data entries when sending diagnostic report

Diagnostic Tools

Diagnostic Tool: Check Network Settings

Check Network Settings

General Network Connection

□ Server	IP Address	Test Results	Notes	Timestamp	Progress	Test
□ Default Gateway (X1)	192.168.255.30					TEST
□ DNS Server 1	192.168.8.253					TEST
□ DNS Server 2	10.217.131.101					TEST

Security Management

Server	IP Address	Test Results	Notes	Timestamp	Progress	Test
□ My SonicWall	N/A					TEST
□ License Manager	N/A					TEST

TEST ALL SELECTED

Tech Support Report

The **Tech Support Report** generates a detailed report of the SonicWall security appliance configuration and status and saves it to the local hard disk using **DOWNLOAD REPORT**. This file can then be emailed to SonicWall Technical Support to help assist with a problem.

ⓘ **TIP:** You must register your SonicWall security appliance on MySonicWall to receive technical support.

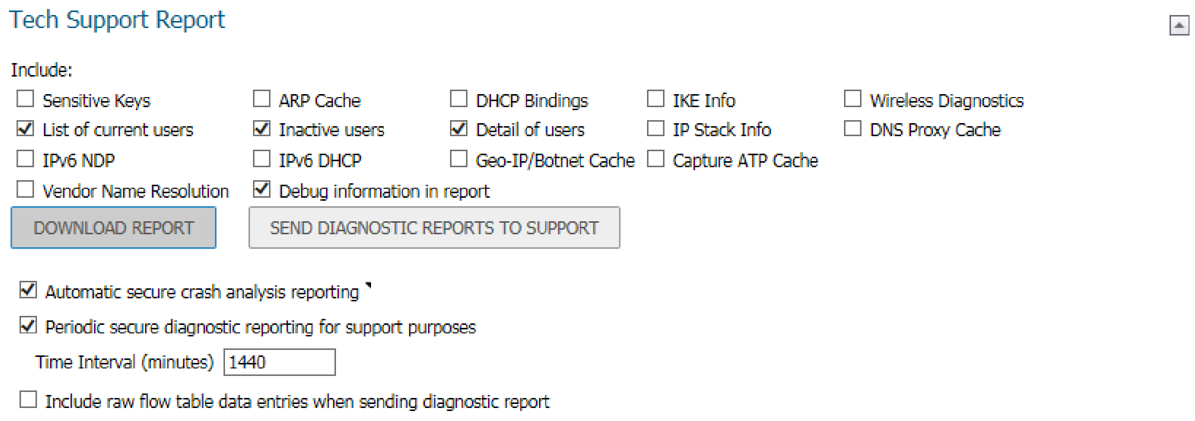
Topics:

- Completing a Tech Support Request on page 113
- Generating a Tech Support Report on page 113

Completing a Tech Support Request

Before emailing the Tech Support Report to the SonicWall Technical Support team, complete a Tech Support Request Form at https://www.MySonicWall.com. After the form is submitted, a unique case number is returned. Include this case number in all correspondence, as it allows SonicWall Technical Support to provide you with better service.

Generating a Tech Support Report



Tech Support Report

Include:

□ Sensitive Keys □ ARP Cache □ DHCP Bindings □ IKE Info □ Wireless Diagnostics
☑ List of current users ☑ Inactive users ☑ Detail of users □ IP Stack Info □ DNS Proxy Cache
□ IPv6 NDP □ IPv6 DHCP □ Geo-IP/Botnet Cache □ Capture ATP Cache
□ Vendor Name Resolution ☑ Debug information in report

☑ Automatic secure crash analysis reporting

☑ Periodic secure diagnostic reporting for support purposes

Time Interval (minutes) 1440

□ Include raw flow table data entries when sending diagnostic report

TIP: If you do not need to generate a report, click **Collapse** in the upper right corner, to provide more room for the diagnostic tools.

To generate a Tech Support Report (TSR):

1. Navigate to **INVESTIGATE | Tools > System Diagnostics**.
2. Scroll to the **Tech Support Report** section.
3. The TSR is organized in an easy-to-read format. You control whether to include debug information as a category. The debug information is enclosed by the `#Debug Information_START` and `#Debug Information_END` tags, at the end of the report. Debug information contains miscellaneous information that is not used by the average support engineer, but can be useful in certain circumstances. Select any of the report options; some are selected by default:
   - **Sensitive Keys** - Saves shared secrets, encryption, and authentication keys to the report. This option is not selected by default.
   - **ARP Cache** - Saves a table relating IP addresses to the corresponding MAC or physical addresses. This option is not selected by default.
   - **DHCP Bindings** - Saves entries from the firewall DHCP server. This option is not selected by default.
   - **IKE Info** - Saves current information about active IKE configurations. This option is not selected by default.
   - **Wireless Diagnostics** - Lists log data if the SonicPoint or internal wireless radio experiences a failure and reboots. Selected by default.

     NOTE: This option is only available when SonicWall access points are enabled or the appliance has an internal wireless radio.

- **List of current users** - Lists all currently logged in active local and remote users. This option is selected by default.

  > ⓘ **NOTE:** For reporting maximum user information, select both **List of current users** and **Detail of users**.

- **Inactive users** - Lists the users with inactive sessions. This option is selected by default.
- **Detail of users** - Lists additional details of user sessions, including timers, privileges, management mode if managing, group memberships, CFS policies, VPN client networks, and other information. The **Current users** report checkbox must be enabled first to obtain this detailed report. This option is selected by default.
- **IP Stack Info** - This option is not selected by default.
- **DNS Proxy Cache** - This option is not selected by default.
- **IPv6 NDP** - This option is not selected by default.
- **IPv6 DHCP** - This option is not selected by default.
- **Geo-IP/Botnet Cache** - Saves the currently cached Geo-IP and Botnet information. This option is not selected by default.
- **Extra Routing Info** – This option is not selected by default.
- **Capture ATP Cache** - Saves the currently cached Capture information.
- **Vendor Name Resolution** - This option is not selected by default.
- **Debug information in report** - Specifies whether the downloaded TSR is to contain debug information. This option is selected by default.
- **IP Report** – This option is not selected by default.
- **ABR Entries** – This option is not selected by default.

4 Click **DOWNLOAD REPORT** to save the file to your system. When you click **DOWNLOAD REPORT**, a warning message is displayed.

5 Click **OK** to save the file.

6 Attach the report to your **Tech Support Request** email.

7 To send the TSR, system preferences, and trace logs (also know as State and Critical logs) to SonicWall Engineering (not to SonicWall Technical Support), click **SEND DIAGNOSTIC REPORTS TO SUPPORT**.

> ⓘ **NOTE:** Last trace logs are not supported on TZ series appliances. Current logs, however, are preserved across reboots, but not power cycles. Current logs for TZ series appliances contain information similar to Last logs on NSA and higher appliances.

The **Status** indicator at the bottom of the page displays `Please wait!` while the report is sent, and then displays `Diagnostic reports sent successfully`. You would normally do this after talking to Technical Support.

8 To send diagnostic files to SonicWall Tech Support for crash analysis, select **Automatic secure crash analysis reporting**. This option is selected by default.

9 To periodically send the TSR, system preferences, and trace log to MySonicWall for SonicWall Engineering:

a Select **Periodic Secure diagnostic reporting for support purposes**. This option is selected by default.

b Enter the interval in minutes between the periodic reports in the **Time Interval (minutes)** field. The default is **1440** minutes (24 hours).

10 To include flow table data in the TSR, select **Include raw flow table data entries when sending diagnostic report**. This option is not selected by default.

Diagnostic Tools

Topics:

Diagnostic Tools Overview

SonicWall provides a series of diagnostic tools to help you resolve many of the common issues you might face. Each tool is different from the others so the display changes with the tool. However, some of the data management functions are common among the tools.

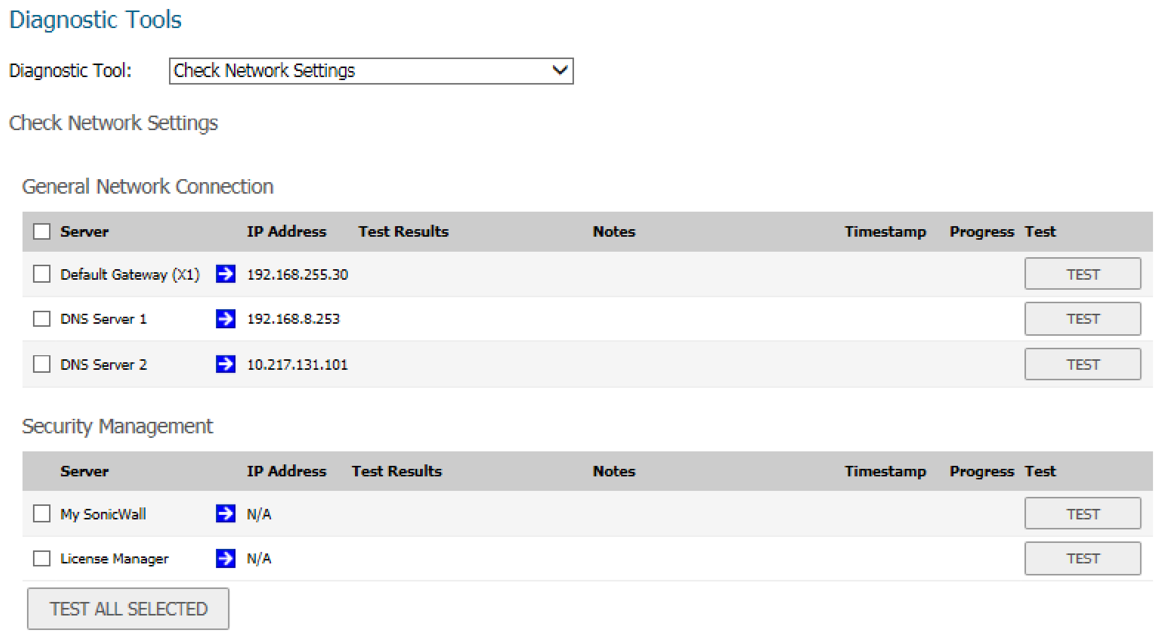
Some tools have management functions to help you manage lists of data. These operate much like the options on the other logs and reports.

- Search
- Filter

- Toggling between views (IPv4 vs. IPv6, for example)
- Refresh
- Export
- Clear

Select the tool you want from **Diagnostic Tool** in the **Tools > System Diagnostic** page.

Check Network Settings



Diagnostic Tools

Diagnostic Tool: Check Network Settings

Check Network Settings

General Network Connection

□ Server	IP Address	Test Results	Notes	Timestamp	Progress	Test
□ Default Gateway (X1)	192.168.255.30					TEST
□ DNS Server 1	192.168.8.253					TEST
□ DNS Server 2	10.217.131.101					TEST

Security Management

Server	IP Address	Test Results	Notes	Timestamp	Progress	Test
□ My SonicWall	N/A					TEST
□ License Manager	N/A					TEST

Check Network Settings is a diagnostic tool that automatically checks the network connectivity and service availability of several predefined functional areas of SonicOS, returns the results, and attempts to describe the causes if any exceptions are detected. This tool helps you locate the problem area when users encounter a network problem.

Specifically, **Check Network Settings** automatically tests the following functions:

- Default Gateway settings
- DNS settings
- MySonicWall server connectivity
- License Manager server connectivity
- Content Filter server connectivity

The return data consists of two parts:

- **Test Results** – Provides a summary of the test outcome
- **Notes** – Provides details to help determine the cause if any problems exist

The **Check Network Settings** tool is dependent on the **Network Monitor** feature available on the **Tools | Network Probes** on the **INVESTIGATE** view. Whenever the **Check Network Settings** tool is being executed (except during the Content Filter test), a corresponding Network Monitor Policy appears on the **Tools | Network Probes** page, with a special diagnostic tool policy name in the form:

```
diagTestPolicyAuto_<IP_address/Domain_name>_0
```

NOTE: Log messages show the up/down status of some of these special network objects. These objects, however, live for only three seconds and then are deleted automatically.

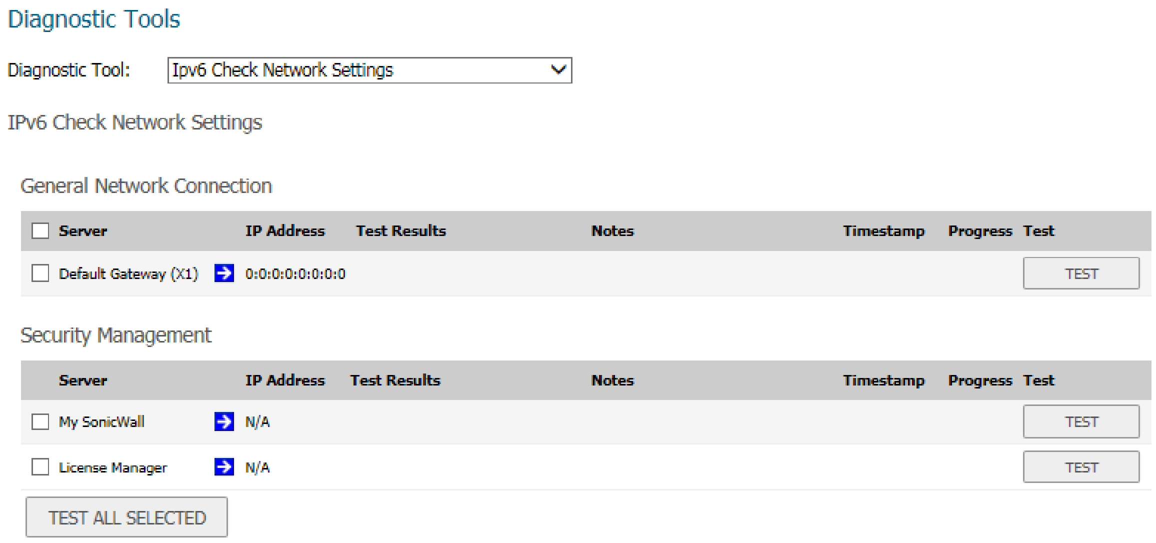
To use the **Check Network Settings** tool, first select it in the **Diagnostic Tools** drop-down list and then click **Test** in the row for the item that you want to test. The results are displayed in the same row. A green check mark signifies a successful test, and a red X indicates that there was a problem.

To test multiple items at the same time, check the box for each desired item and then click **TEST ALL SELECTED**.

If probes fail, you can click the blue arrow to the left of the I**P Address** field of the failed item to jump to the configuration page to investigate the root cause.

IPv6 Check Network Settings

The **IPv6 Check Network Settings** is a diagnostic tool that tests whether the firewall supports IPv6.



Diagnostic Tools

Diagnostic Tool: Ipv6 Check Network Settings

IPv6 Check Network Settings

General Network Connection

□ Server		IP Address	Test Results	Notes	Timestamp	Progress	Test
□ Default Gateway (X1)	➔	0:0:0:0:0:0:0:0					TEST

Security Management

Server		IP Address	Test Results	Notes	Timestamp	Progress	Test
□ My SonicWall	➔	N/A					TEST
□ License Manager	➔	N/A					TEST

TEST ALL SELECTED

The tool checks various connections, such as the General Network Connection and Security Management, and displays the results:

- **Server**
- **IP Address**
- **Test Results**
- **Notes**
- **Timestamp**
- **Progress**

To test for IPv6 settings:

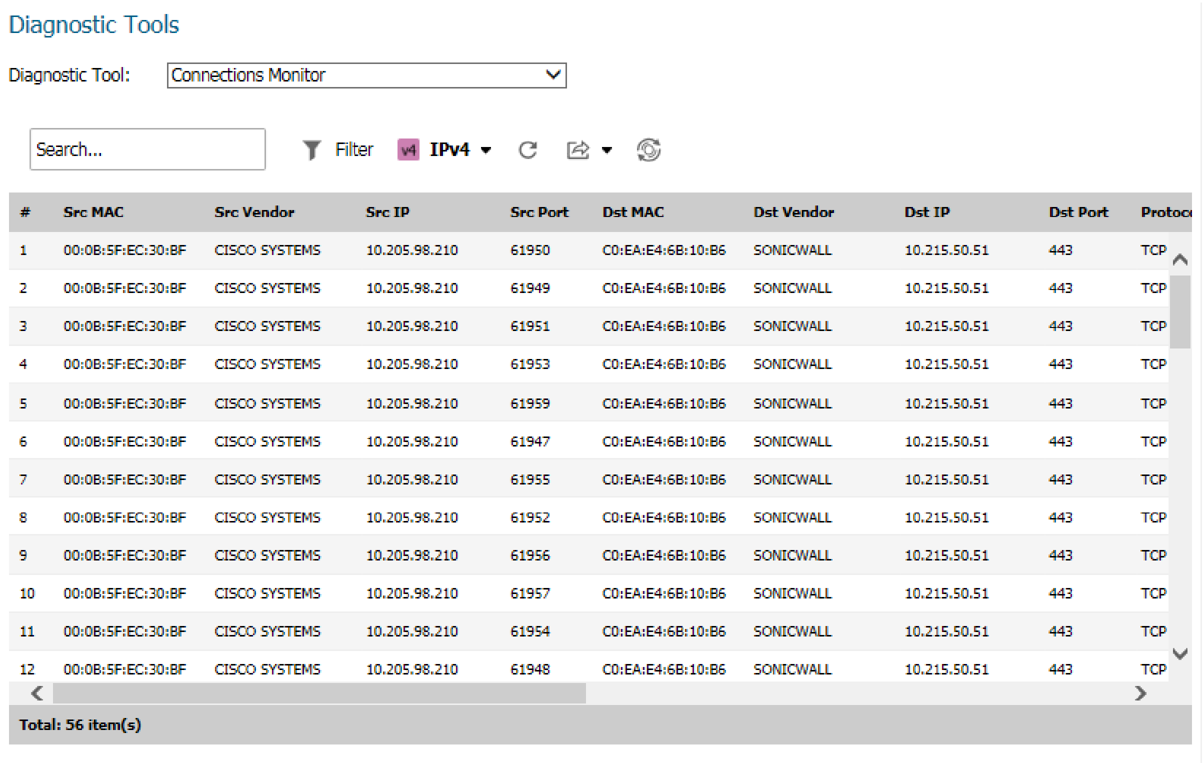
1 Select **IPv6 check Network Settings** from **Diagnostic Tool**.

2 To test:

  - A single connection, click **TEST**.
  - Two or more connections from any or all tables, check the boxes for the connections and then click **TEST ALL SELECTED**.

Connections Monitor

The **Connections Monitor** displays real-time, exportable (plain text or CSV), and filterable views of all connections to and through the firewall.



Diagnostic Tools

Diagnostic Tool: Connections Monitor

#	Src MAC	Src Vendor	Src IP	Src Port	Dst MAC	Dst Vendor	Dst IP	Dst Port	Protoco
1	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61950	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP
2	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61949	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP
3	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61951	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP
4	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61953	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP
5	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61959	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP
6	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61947	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP
7	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61955	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP
8	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61952	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP
9	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61956	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP
10	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61957	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP
11	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61954	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP
12	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61948	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP

Total: 56 item(s)

Topics:

- Connections Monitor Settings on page 118
- Connections Monitor Data on page 119

Connections Monitor Settings

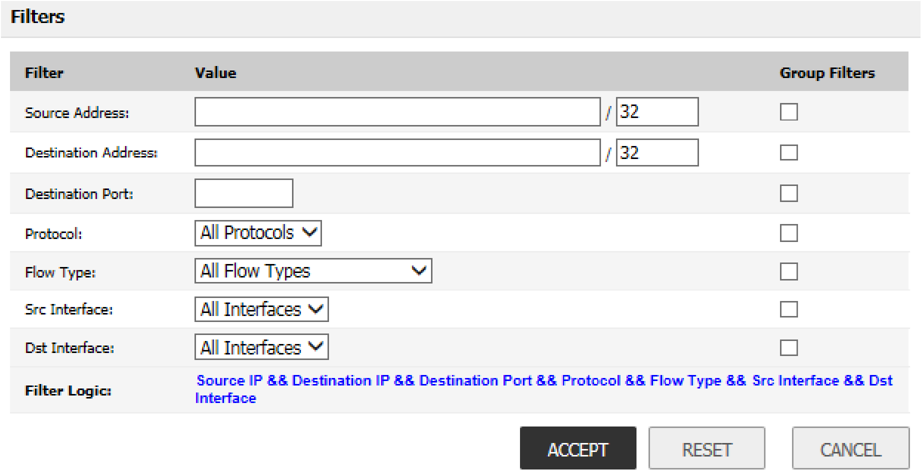
Filter the results to display only connections matching certain criteria.

To enter the filter criteria:

1 Navigate to **Tools > System Diagnostics** on the **INVESTIGATE** view.

2 From **Diagnostic Tool**, select **Connections Monitor**.

3 Click **Filter**.



Filters

Filter	Value	Group Filters
Source Address:	/ 32	☐
Destination Address:	/ 32	☐
Destination Port:		☐
Protocol:	All Protocols	☐
Flow Type:	All Flow Types	☐
Src Interface:	All Interfaces	☐
Dst Interface:	All Interfaces	☐
Filter Logic:	Source IP && Destination IP && Destination Port && Protocol && Flow Type && Src Interface && Dst Interface	

4 Enter values in the fields you want to filter on: **Source Address, Destination Address, Destination Port, Protocol, Flow Type**, **Src Interface**, and **Dst Interface**.

The fields you enter values into are combined into a search string with a logical **AND**. The search string is shown in the **Filter Logic** field. For example, if you enter values for **Source IP** and **Destination IP**, the search string looks for connections matching:

```
Source IP AND Destination IP
```

5 Select **Group Filters** next to any two or more criteria to combine them with a logical **OR**.

For example, if you enter values for **Source Address, Destination Address**, and **Protocol**, and check **Group Filters** next to **Source Address** and **Destination Address**, the search string looks for connections matching:

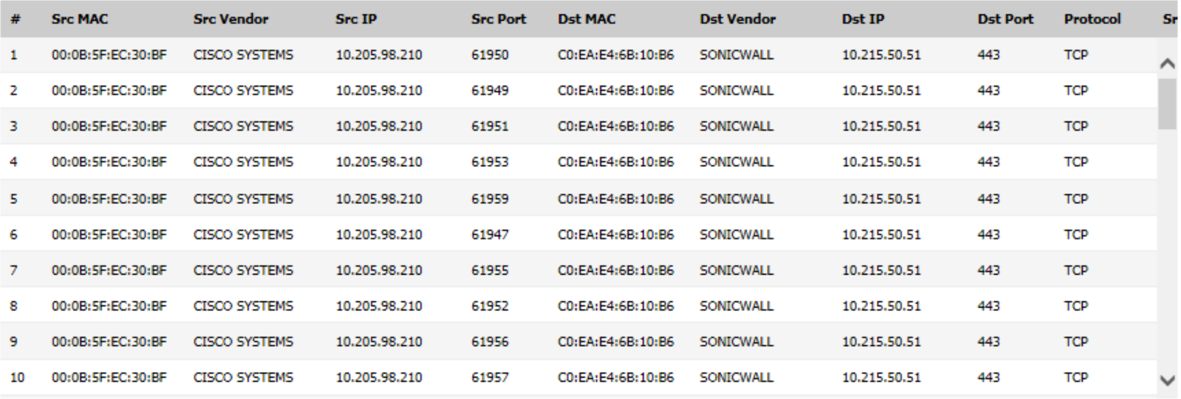
```
(Source IP OR Destination IP) AND Protocol
```

6 Click **ACCEPT** to apply the filter.

7 Click **RESET** to clear the filter and display the unfiltered results again.

Export the list of active connections to a file. Click **Export** and choose whether you want the results exported to a plain text file or to a CSV file. If you are prompted to **Open** or **Save** the file, select **Save**. Then enter a filename and path and click **OK**.

Connections Monitor Data



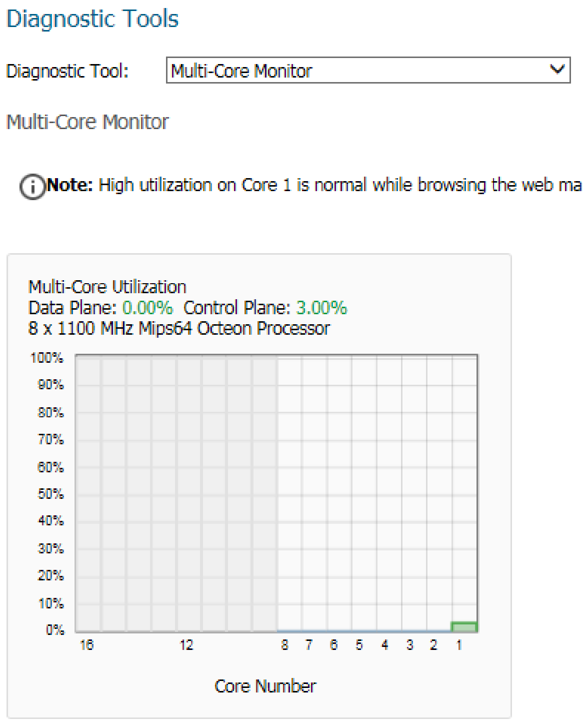
#	Src MAC	Src Vendor	Src IP	Src Port	Dst MAC	Dst Vendor	Dst IP	Dst Port	Protocol	Sr
1	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61950	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP	
2	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61949	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP	
3	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61951	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP	
4	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61953	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP	
5	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61959	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP	
6	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61947	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP	
7	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61955	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP	
8	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61952	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP	
9	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61956	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP	
10	00:0B:5F:EC:30:BF	CISCO SYSTEMS	10.205.98.210	61957	C0:EA:E4:6B:10:B6	SONICWALL	10.215.50.51	443	TCP	

The **Connection Monitor** table shows information about all the active connections: **Src MAC**, **Src Vendor**, **Src IP**, **Src Port**, **Dst MAC**, **Dst Vendor**, **Dst IP**, **Dst Port**, **Protocol**, **Src Iface**, **Dst Iface**, **Flow Type**, **IPS Category**, **Expiry (sec)**, **TX Bytes**, **Rx Bytes**, **Tx Pkts**, **Rx Pkts**. Click the column heading to sort by that column. You can also search for a specific string in that data table.

To refresh the data, click **REFRESH** at the top of the table. Flush an individual connection by clicking **Delete** in the **Flush** column.

Multi-Core Monitor

The **Multi-Core Monitor** displays dynamically updated statistics on utilization of the individual cores of the SonicWall security appliance.



Diagnostic Tools

Diagnostic Tool: Multi-Core Monitor

Multi-Core Monitor

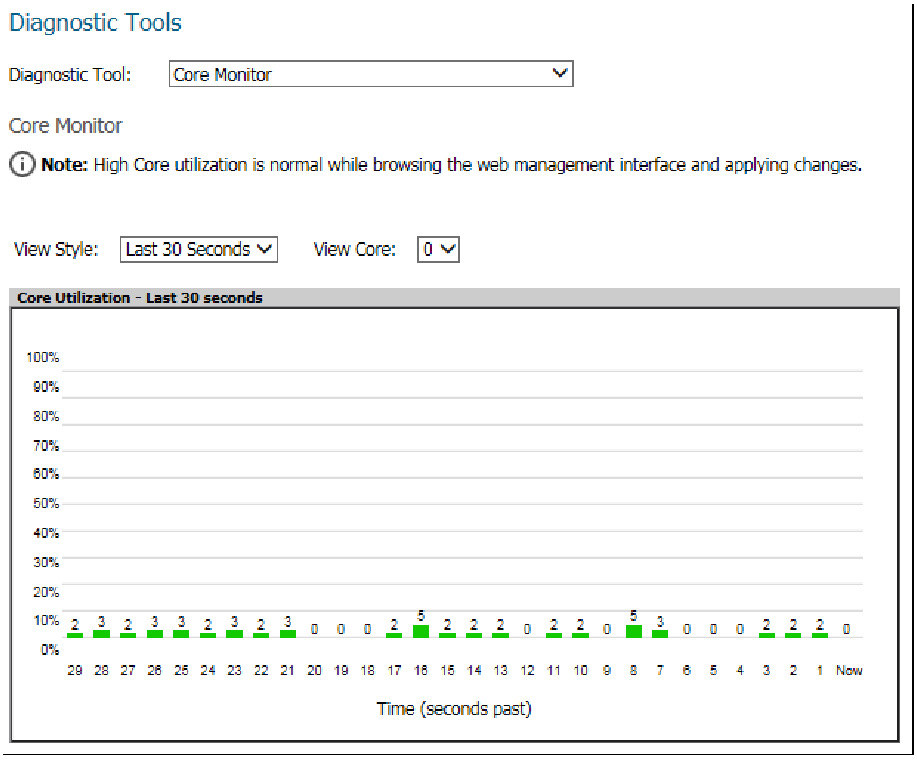
Note: High utilization on Core 1 is normal while browsing the web management interface and applying changes.

Multi-Core Utilization
Data Plane: 0.00% Control Plane: 3.00%
8 x 1100 MHz Mips64 Octeon Processor

If your system is configured for high availability, the cores for both the Primary and Secondary firewalls are displayed. To view the two monitors side by side, click the small triangle in the header of the first monitor.

Core Monitor

The **Core Monitor** displays dynamically updated statistics on the utilization of a single specified core on the SonicWall security appliances. The **View Style** provides a wide range of time intervals that can be displayed to review core usage.



Diagnostic Tools

Diagnostic Tool: Core Monitor

Core Monitor

Note: High Core utilization is normal while browsing the web management interface and applying changes.

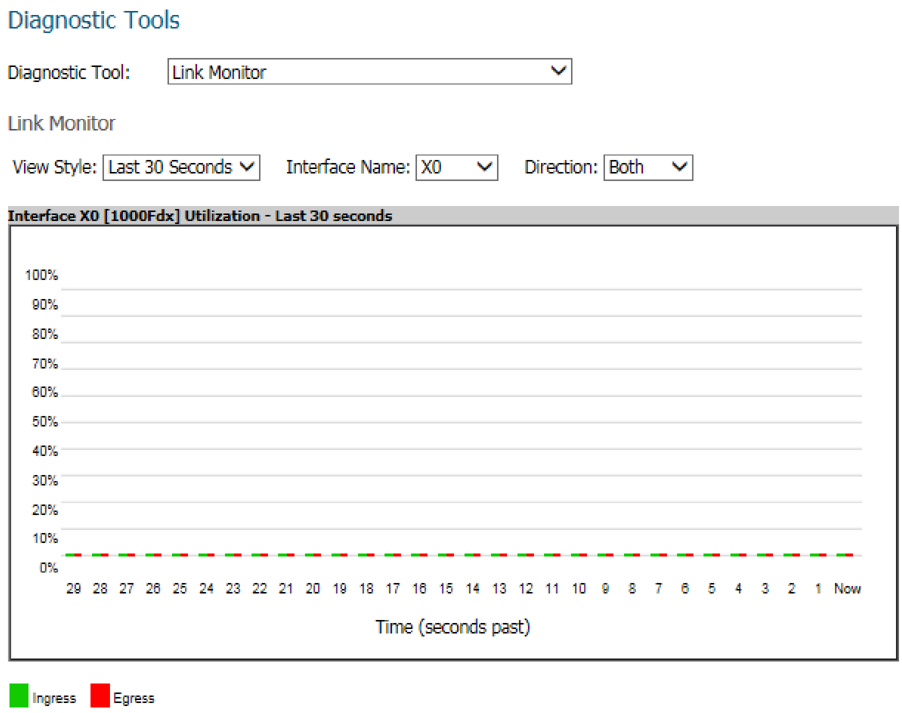
View Style: Last 30 Seconds

View Core: 0

Core Utilization - Last 30 seconds
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2 3 2 3 3 2 3 2 3 0 0 0 2 5 2 2 2 0 2 2 0 5 3 0 0 0 2 2 2 0
29 28 27 26 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 Now
Time (seconds past)

Link Monitor

The **Link Monitor** displays bandwidth utilization for the interfaces on the firewall. Bandwidth utilization is shown as a percentage of total capacity. The Link Monitor can be configured to display inbound traffic, outbound traffic or both for each of the physical interfaces on the appliance.



Diagnostic Tools

Diagnostic Tool: Link Monitor

Link Monitor

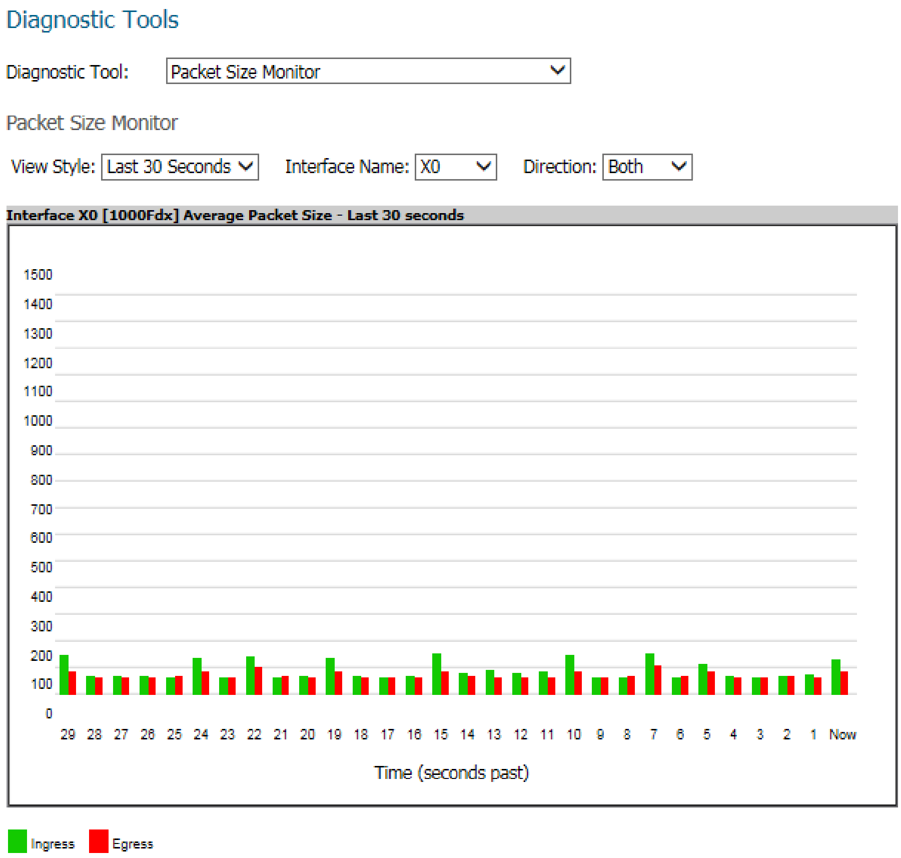
View Style: Last 30 Seconds   Interface Name: X0   Direction: Both

Interface X0 [1000Fdx] Utilization - Last 30 seconds

100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
29 28 27 26 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 Now
Time (seconds past)
🟩 Ingress
🟥 Egress

Packet Size Monitor

The **Packet Size Monitor** displays sizes of packets on the interfaces on the firewall. Select from four time periods, ranging from the last 30 seconds to the last 30 days. The Packet Size Monitor can be configured to display inbound traffic, outbound traffic or both for each of the physical interfaces on the appliance.



Diagnostic Tools

Diagnostic Tool: Packet Size Monitor

Packet Size Monitor

View Style: Last 30 Seconds Interface Name: X0 Direction: Both

Interface X0 [1000Fdx] Average Packet Size - Last 30 seconds
1500
1400
1300
1200
1100
1000
900
800
700
600
500
400
300
200
100
0
29 28 27 26 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 Now
Time (seconds past)
🟩 Ingress
🟥 Egress

To configure the Packet Size Monitor:

1 Select one of the following from **View Style**:

- **Last 30 Seconds**
- **Last 30 Minutes**
- **Last 24 Hours**
- **Last 30 Days**

2 Select the physical interface to view from **Interface Name**.

3 From **Direction**, select one of the following:

- **Both** – Select for packets traveling both inbound and outbound
- **Ingress** – Select for packets arriving on the interface
- **Egress** – Select for packets departing from the interface

The packets are displayed in the Average Packet Size graph, where the X axis specifies when the packets crossed the interface and the Y axis specifies the average packet size at that time. Ingress packets are displayed in green, and egress packets are displayed in red.

DNS Name Lookup

The DNS lookup tool returns the IPv4 and/or IPv6 IP address of a domain name or the IP address of a domain. If you enter an IPv4 and/or IPv6 IP address, the tool returns the domain name for that address. If you enter a domain name, the tool returns the DNS server used and the resolved address.

With the **DNS Server** radio buttons, you can select either a **System** or **Customized** DNS server. The options change, depending on which you choose.

The **IPv4/IPv6 DNS Server** fields display the IP addresses of the DNS Servers configured on the firewall. If there is no IP address (`0.0.0.0` for IPv4 or `::` for IPv6) in the fields, you must configure them on the **Network > Settings** page.

The **Type** drop-down menu allows you to specify:

- **IPv4**, the default that resolves only IPv4 domain names.
- **IPv6** that resolves only IPv6 domain names.
- **All** that resolves both types of domain names.

ⓘ **IMPORTANT:** When specifying a domain name, do not add *http* or *https* to the name.

The firewall queries the DNS Server and displays the results in the **Result** section.

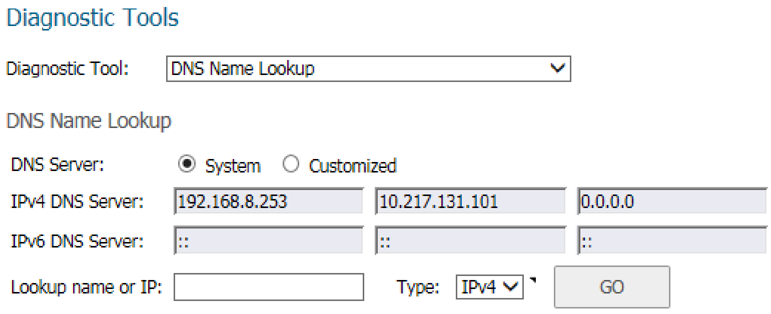
Topics:

- Resolving a System DNS Server on page 124
- Resolving a Customized DNS Server on page 125

Resolving a System DNS Server

To resolve a system DNS Server:

1 Select **System** for the DNS Server.



Diagnostic Tools

Diagnostic Tool: DNS Name Lookup

DNS Name Lookup

DNS Server:	● System	○ Customized	
IPv4 DNS Server:	192.168.8.253	10.217.131.101	0.0.0.0
IPv6 DNS Server:	::	::	::
Lookup name or IP:		Type: IPv4	GO

2 In the **Lookup name or IP** field, enter either the domain name or the IP address to be resolved.

3 Select the type of IP DNS server from **Type**:

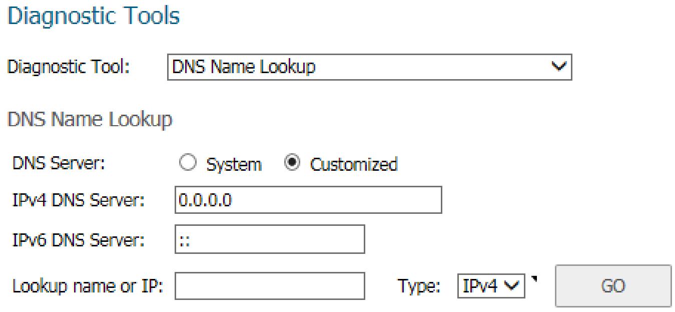
- **IPv4** (default)
- **IPv6**
- **All** (both IPv4 and IPv6)

4 Click **GO**. The firewall returns the matching pair of addresses and domain names.

Resolving a Customized DNS Server

To resolve a customized DNS Server:

1 Select **Customized** as the **DNS Server**.



Diagnostic Tools

Diagnostic Tool: DNS Name Lookup

DNS Name Lookup

DNS Server: ○ System ● Customized

IPv4 DNS Server: 0.0.0.0

IPv6 DNS Server: ::

Lookup name or IP:

Type: IPv4

2 If the DNS Server IP address has not been populated, enter it in the IPv4 or IPv6 field.

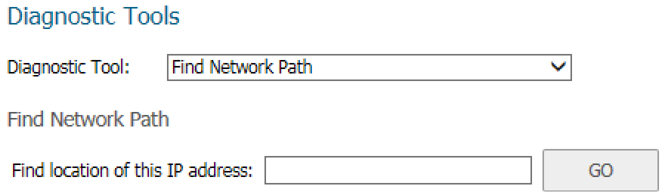
3 In the **Lookup name or IP** field, enter either the domain name or the IP address to be resolved.

4 Select the type of IP DNS server from **Type**:

- **IPv4** (default)
- **IPv6**
- **All** (both IPv4 and IPv6)

5 Click **GO**. The firewall returns the same information as for a System DNS Server.

Find Network Path



Diagnostic Tools

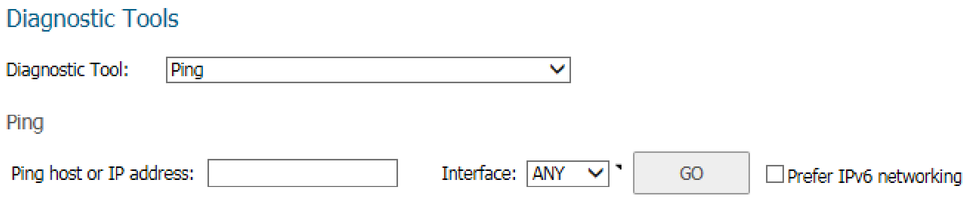
Diagnostic Tool: Find Network Path

Find Network Path

Find location of this IP address:

Enter an IP address to determine if the network path is located on a specific network interface, if it reached a router gateway IP address, and if it reached through an Ethernet address.

Ping



Diagnostic Tools

Diagnostic Tool: Ping

Ping

Ping host or IP address:

Interface: ANY

□ Prefer IPv6 networking

The **Ping** test bounces a packet off a machine on the Internet and returns it to the sender. This test shows if the firewall is able to contact the remote host. If users on the LAN are having problems accessing services on the

Internet, try pinging the DNS server, or another machine at the ISP location. If the test is unsuccessful, try pinging devices outside the ISP. If you can ping devices outside of the ISP, then the problem lies with the ISP connection.

1 Select **Ping** from the **Diagnostic Tool** menu.

2 Enter the IP address or host name of the target device.

3 In the **Interface** drop-down menu, select which WAN interface you want to test the ping from. Selecting **ANY** allows the appliance to choose among all interfaces—including those not listed in the drop-down menu.

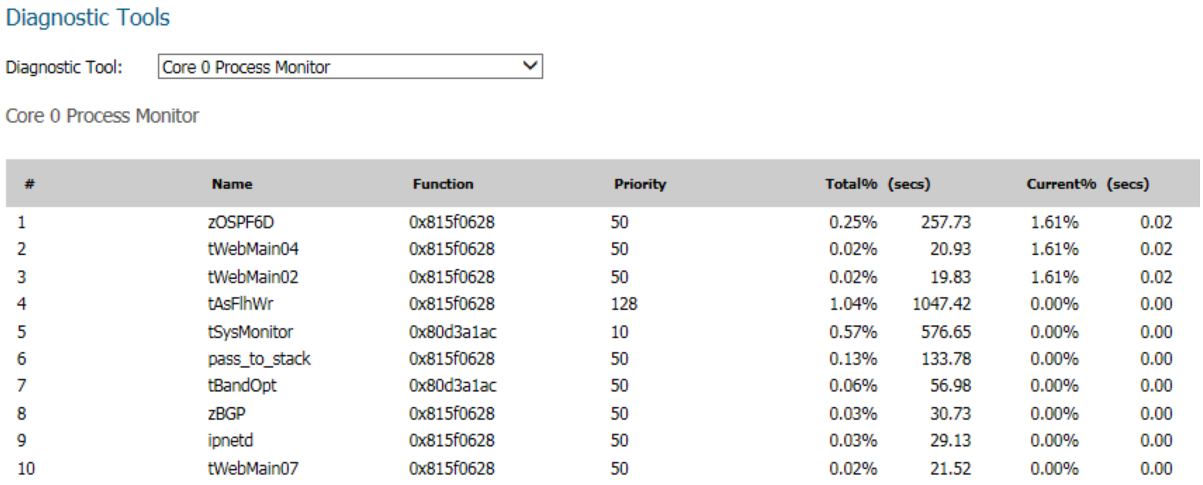
4 Check the box if you **Prefer IPv6 networking**.

5 Click **GO**.

If the test is successful, the firewall returns a message, stating that the IP address is alive and showing the time to return in milliseconds (ms).

Core 0 Process Monitor

The **Core 0 Process Monitor** shows the individual system processes on core 0, their CPUutilization, and their system time. The **Core 0 Process Monitor** is available on the multi-core SuperMassive 9000 series and multi-core NSA series appliances.



Diagnostic Tools

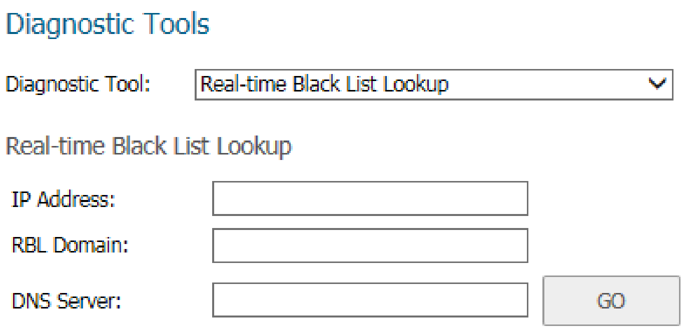
Diagnostic Tool: Core 0 Process Monitor

Core 0 Process Monitor

#	Name	Function	Priority	Total%	(secs)	Current%	(secs)
1	zOSPF6D	0x815f0628	50	0.25%	257.73	1.61%	0.02
2	tWebMain04	0x815f0628	50	0.02%	20.93	1.61%	0.02
3	tWebMain02	0x815f0628	50	0.02%	19.83	1.61%	0.02
4	tAsFlhWr	0x815f0628	128	1.04%	1047.42	0.00%	0.00
5	tSysMonitor	0x80d3a1ac	10	0.57%	576.65	0.00%	0.00
6	pass_to_stack	0x815f0628	50	0.13%	133.78	0.00%	0.00
7	tBandOpt	0x80d3a1ac	50	0.06%	56.98	0.00%	0.00
8	zBGP	0x815f0628	50	0.03%	30.73	0.00%	0.00
9	ipnetd	0x815f0628	50	0.03%	29.13	0.00%	0.00
10	tWebMain07	0x815f0628	50	0.02%	21.52	0.00%	0.00

Real-Time Black List Lookup

The **Real-Time Black List Lookup** tool allows you to test SMTP IP addresses, RBL services, or DNS servers. Enter an IP address in the **IP Address** field, a FQDN for the RBL in the **RBL Domain** field and DNS server information in the **DNS Server** field. Click **Go**.



Diagnostic Tools

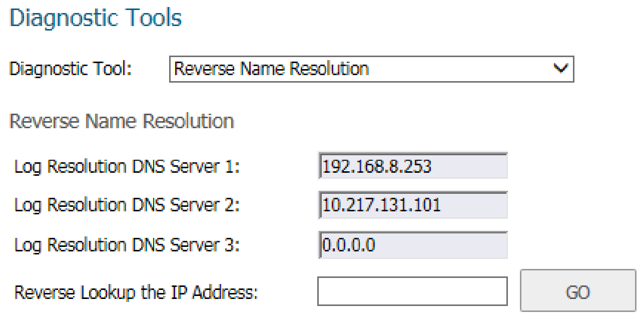
Diagnostic Tool: Real-time Black List Lookup

Real-time Black List Lookup

IP Address:	
RBL Domain:	
DNS Server:	

Reverse Name Resolution

The **Reverse Name Resolution** tool is similar to the DNS name lookup tool, except that it looks up a server name, given an IP address.



Diagnostic Tools

Diagnostic Tool: Reverse Name Resolution

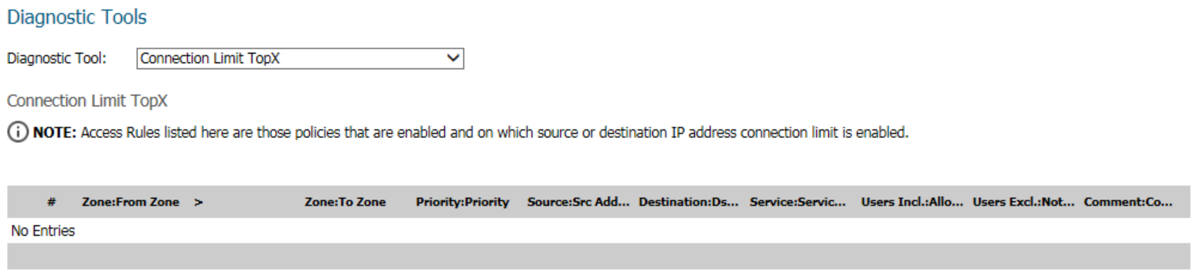
Reverse Name Resolution

Log Resolution DNS Server 1:	192.168.8.253
Log Resolution DNS Server 2:	10.217.131.101
Log Resolution DNS Server 3:	0.0.0.0
Reverse Lookup the IP Address:	

Enter an IP address in the **Reverse Lookup the IP Address** field, and it checks all DNS servers configured for your security appliance to resolve the IP address to a server name.

Connection Limit TopX

The **Connection Limit TopX** tool lists the top 10 connections by the source and destination IP addresses. Before you can use this tool, you must enable source IP limiting and/or destination IP limiting for your appliance. If these are not enabled, the page displays a message to tell you where you can enable them.



Diagnostic Tools

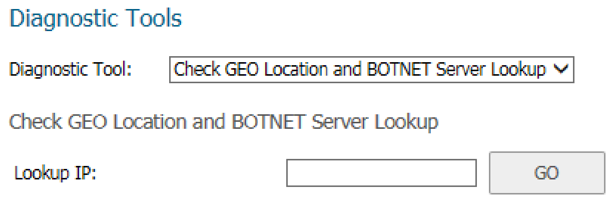
Diagnostic Tool: Connection Limit TopX

Connection Limit TopX

ⓘ **NOTE:** Access Rules listed here are those policies that are enabled and on which source or destination IP address connection limit is enabled.

#	Zone:From Zone	>	Zone:To Zone	Priority:Priority	Source:Src Add...	Destination:Ds...	Service:Servic...	Users Incl.:Allo...	Users Excl.:Not...	Comment:Co...
No Entries										

Check GEO Location and BOTNET Server Lookup


Diagnostic Tools

Diagnostic Tool: Check GEO Location and BOTNET Server Lookup

Check GEO Location and BOTNET Server Lookup

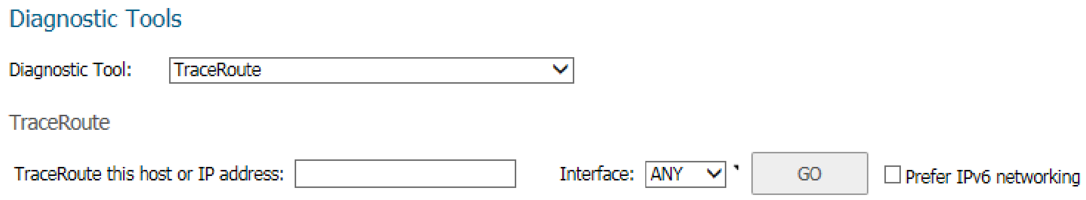
Lookup IP:

The **GEO Location and Botnet Server Lookup** feature allows you to block connections to or from a geographic location based on IP address and to or from Botnet command and control servers. Additional functionality for this feature is available on the **MANAGE** view under **Security Configuration | Security Services > Geo-IP Filter** and **Botnet Filter** pages. For more information, refer to *SonicWall SonicOS 6.5 Security Configuration*.

To troubleshoot with GEO Location and BOTNET Server Lookup:

1. Select **GEO Location and BOTNET Server Lookup** from the **Diagnostic Tool** drop-down menu.
2. Type the IP address or domain name of the destination host in the **Lookup IP** field.
3. Click **GO**. The result displays underneath the **Lookup IP** field.

TraceRoute


Diagnostic Tools

Diagnostic Tool: TraceRoute

TraceRoute

TraceRoute this host or IP address:

Interface: ANY

☐ Prefer IPv6 networking

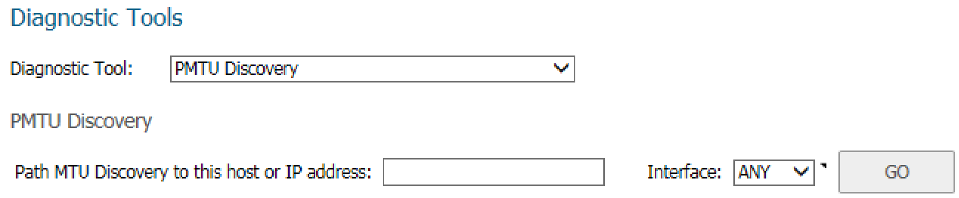
Trace Route is a diagnostic utility that assists in diagnosing and troubleshooting router connections on the Internet. By using Internet UDP packets similar to Ping packets, **Trace Route** can test interconnectivity with routers and other hosts that are farther and farther along the network path until the connection fails or until the remote host responds.

The TraceRoute tool includes a **Prefer IPv6 networking** option. When testing interconnectivity with routers and other hosts, SonicOS uses the first IP address that is returned and shows the actual TraceRoute address. If both IPv4 and IPv6 addresses are returned, by default, the firewall TraceRoutes the IPv4 address. If the **Prefer IPv6 networking** option is enabled, the firewall TraceRoutes the IPv6 address.

To troubleshoot with Trace Route:

1. Select **TraceRoute** from **Diagnostic Tool**.
2. Type the IP address or domain name of the destination host in the **TraceRoute this host or IP address** field.
3. From **Interface**, select which WAN-specific interface you want to test the trace route from. Selecting **ANY**, the default, allows the firewall to choose among all interfaces—including those not listed in **Interface**.
4. To TraceRoute for IPv6, select **Prefer IPv6 networking**.
5. Click **GO**. Depending on the route, this might take a few minutes. A pop-up table displays with each hop to the destination host. By following the route, you can diagnose where the connection fails between the firewall and the destination.

PMTU Discovery



Diagnostic Tools

Diagnostic Tool: PMTU Discovery

PMTU Discovery

Path MTU Discovery to this host or IP address:

Interface: ANY

PMTU Discovery is a diagnostic tool that uses a standardized technique for determining the maximum transmission unit (MTU) size on the network path between two Internet Protocol (IP) hosts, usually with the goal of avoiding IP fragmentation. PMTU Discovery works with both IPv4 and IPv6.

To troubleshoot with PMTU Discovery:

1 Select **PMTU Discovery** from **Diagnostic Tool**.

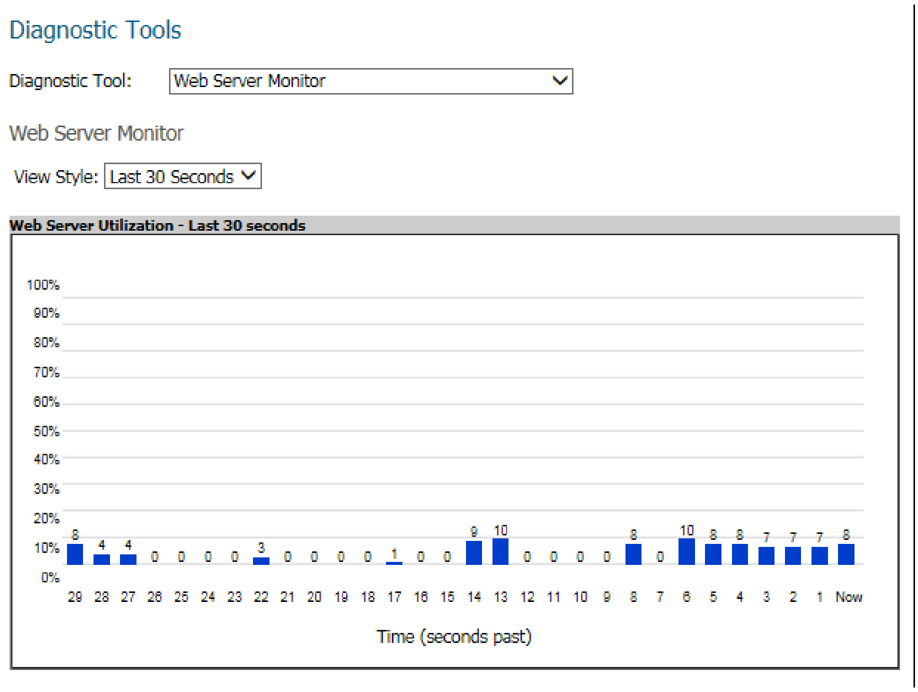
2 Type the IP address or domain name of the destination host in the **Path MTU Discovery to this host or IP address** field.

3 From **Interface**, select which WAN-specific interface you want to test the trace route from. Selecting **ANY**, the default, allows the firewall to choose among all interfaces—including those not listed in **Interface**.

4 Click **GO**.

Depending on the route, this might take a few minutes. A pop-up table displays with each hop to the destination host. By following the route, you can diagnose where the connection fails between the firewall and the destination.

Web Server Monitor



Diagnostic Tools

Diagnostic Tool: Web Server Monitor

Web Server Monitor

View Style: Last 30 Seconds

Web Server Utilization - Last 30 seconds

The **Web Server Monitor** tool displays the CPU utilization of the Web server over time.

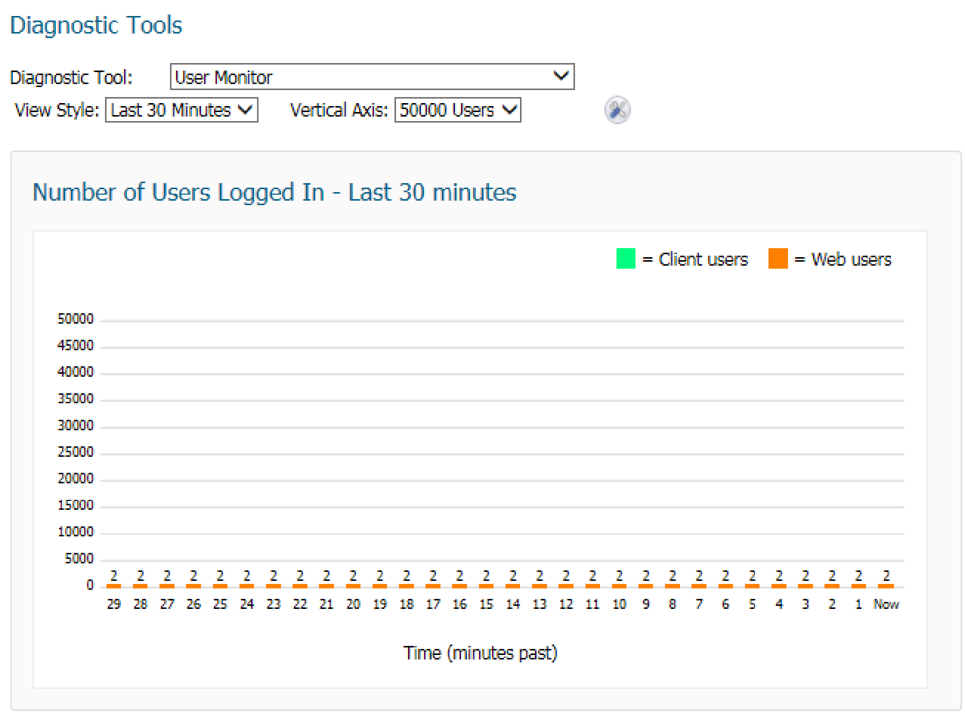
To troubleshoot with Web Server Monitor:

1 Select **Web Server Monitor** from **Diagnostic Tool**.

2 From **View Style**, select the time period displayed:

- **Last 30 seconds** (default)
- **Last 30 minutes**
- **Last 24 hours**
- **Last 30 days**

User Monitor



Diagnostic Tools

Diagnostic Tool: User Monitor

View Style: Last 30 Minutes

Vertical Axis: 50000 Users

The **User Monitor** tool displays the number users of logged in over time.

To troubleshoot with User Monitor:

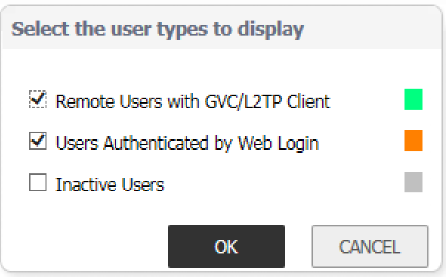
1 Select **User Monitor** from **Diagnostic Tool**.

2 From **View Style**, select the time period displayed:

- **Last 30 seconds** (default)
- **Last 30 minutes**
- **Last 24 hours**
- **Last 30 days**

3 From **Vertical Axis**, select the maximum number of users for the vertical axis.

4 To specify the types of users to display, click **Configure**. A pop-up menu displays.



Select the user types to display

☑ Remote Users with GVC/L2TP Client 🟩

☑ Users Authenticated by Web Login 🟧

☐ Inactive Users ⬜

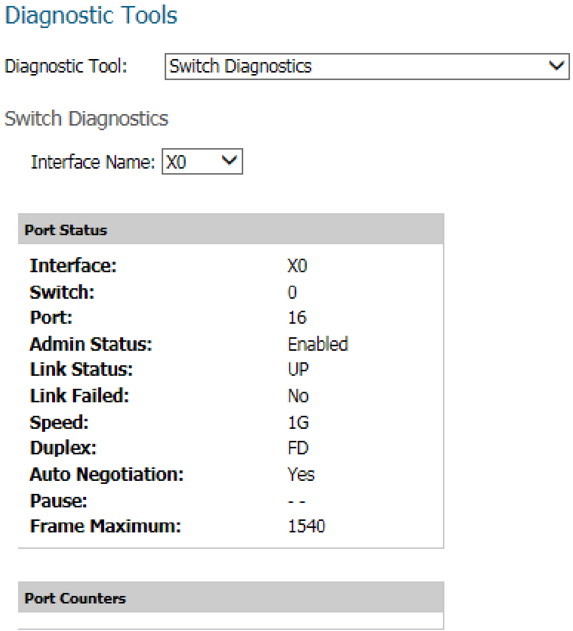
> **NOTE:** The types of users displayed depend on how your users log in. For example, if you do not use SSL VPN, that option does not display.

a Select the checkboxes of the user types to be displayed.

b Clear the checkboxes of the user types to hide.

c Click **OK**.

Switch Diagnostics



Diagnostic Tools

Diagnostic Tool: Switch Diagnostics

Switch Diagnostics

Interface Name: X0

Port Status	
Interface:	X0
Switch:	0
Port:	16
Admin Status:	Enabled
Link Status:	UP
Link Failed:	No
Speed:	1G
Duplex:	FD
Auto Negotiation:	Yes
Pause:	- -
Frame Maximum:	1540

Port Counters

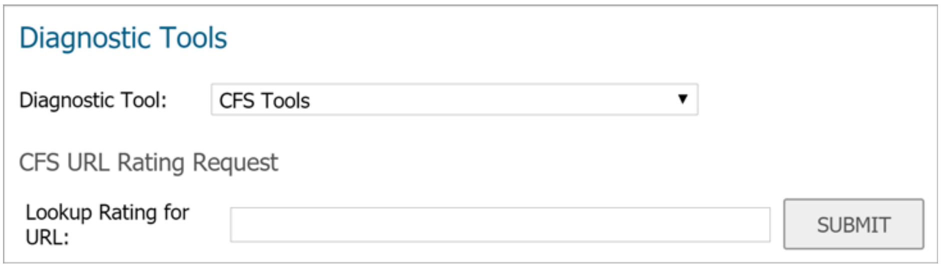
The **Switch Diagnostics** tool displays the status of and counters of a switch associated with an interface.

To troubleshoot with Switch Diagnostics:

1 Select **Switch Diagnostics** from **Diagnostic Tool**.

2 Select the interface from **Interface Name**.

CFS Tools



Diagnostic Tools

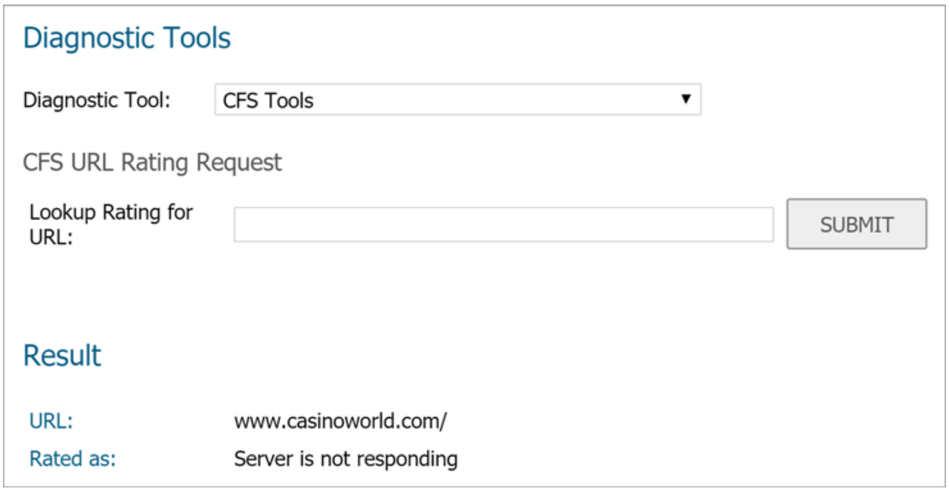
Diagnostic Tool: CFS Tools

CFS URL Rating Request

The **CFS Tools** tool provides a way to look up the content filtering rating for a URL.

To look up the content filtering rating with CFS Tools:

1. Select **CFS Tools** from **Diagnostic Tool**.
2. Type the URL to look up into the **Lookup Rating for URL** field and click **SUBMIT**.
3. The **Result** section displays below.



Diagnostic Tools

Diagnostic Tool: CFS Tools

CFS URL Rating Request

Result

URL: www.casinoworld.com/

Rated as: Server is not responding

Part 4

INVESTIGATE | Appendix

- SonicWall Support

17

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 MySonicWall
- 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

Legend

⚠ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

△ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ⓘ **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

SonicOS 6.5 Investigate
Updated - July 2020
Software Version - 6.5.4
232-002149-04 Rev C

The information in this document is provided in connection with SonicWall Inc. 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 SonicWall 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. SonicWall Inc. 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/en-us/legal/license-agreements.

Open Source Code

SonicWall 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
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035