SonicOS and SonicOSX 7 Tools & Monitors

Administration Guide

SONICWALL®

Contents

Using Packet Monitor **3**
Benefits of Packet Monitor 3
How Does Packet Monitor Work? 4
Supported Packet Types 5
Configuring Packet Monitor 5
Configuring General Settings 5
Starting and Stopping Packet Mirror 11
Monitoring Captured Packets 12
Starting and Stopping Packet Capture 12
Configuring Mirror Settings 12
Viewing Packet Monitoring Statistics 13
Capture Statistics 14
Local Mirror Statistics 14
Remote Mirror TX Statistics 14
Remote Mirror RX Statistics 15
FTP Statistics 15
Current Buffer Statistics 16

Viewing Connections **17**
Searching the Connections 18
Filtering the Connection Log 18
Connections Log Functions 19

Monitoring Core 0 Processes **20**

Using Packet Replay **21**
Single Packets 21
Packet Crafting 21
Packet Buffer 23
Replay Pcap File 23
Replaying an IP Pcap File 23
Replaying a MAC Pcap File 24
Captured Packets 24
Captured Packets 25
Packet Detail 26
Hex Dump 26

SonicWall Support **27**
About This Document 28

1

Using Packet Monitor

The Packet Monitor is a mechanism that allows you to monitor individual data packets that traverse your SonicWall network security appliance. Packets can be either monitored or mirrored. The monitored packets contain both data and addressing information. Addressing information from the packet header includes the following:

- Interface identification
- MAC addresses
- Ethernet type
- Internet Protocol (IP) type
- Source and destination IP addresses
- Port numbers
- L2TP payload details
- PPP negotiations details

You can configure the packet monitor feature in the enhanced management interface. The management interface provides a way to configure the monitor criteria, display settings, mirror settings, and file export settings, and displays the captured packets.

Current configurations are displayed on this page, hover over the information symbols to view the details.

Topics:

- Benefits of Packet Monitor
- How Does Packet Monitor Work?
- Supported Packet Types
- Monitoring Captured Packets
- Configuring Packet Monitor
- Viewing Packet Monitoring Statistics

Benefits of Packet Monitor

The packet monitor feature provides the functionality and flexibility that you need to examine network traffic without the use of external utilities, such as Wireshark (formerly known as Ethereal). 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 packets
  - Decoded output of selected packet
  - 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

How Does Packet Monitor Work?

As an administrator, you can 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. You can 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.

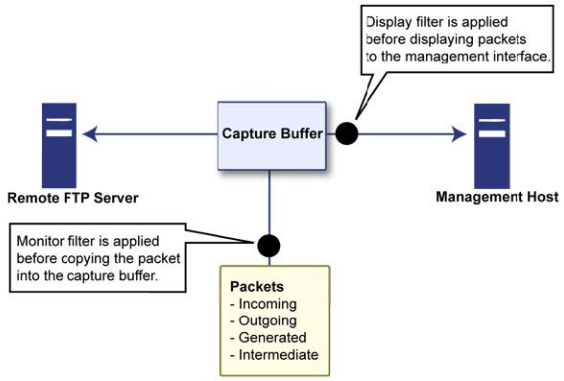
Default settings are provided so that you can start using packet monitor without configuring it first. The basic functionality is:

PACKETS: BASIC FUNCTIONALITY

Start:	Click Start Capture to begin capturing all packets except those used for communication between the firewall and the management interface on your console system.
Stop:	Click Stop Capture to stop the packet capture.

Refer to Configuring Packet Monitor 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



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.

Supported Types	Protocol Acronyms	Notes
Supported Ethernet Types	• ARP • IP • PPPoE-DIS • PPPoE SES	To specify both PPPoE DIS and PPPoE SES, you can simply use PPPoE.
Supported IP Types	• TCP • UDP • ICMP • IGMP • GRE • AH • ESP	

Configuring Packet Monitor

You can access the packet monitor tool on the **Monitor > Tools & Monitors > Packet Monitor** page of the management interface. There are six main areas of configuration for packet monitor, one of which is specifically for packet mirror. The following sections describe the configuration options, and provide procedures for accessing and configuring the filter settings, log settings, and mirror settings:

Topics:

- Monitoring Captured Packets
- Configuring General Settings
- Viewing Packet Monitoring Statistics

Configuring General Settings

Topics:

- Configuring General Settings
- Configuring the Monitor Filter
- Configuring Display Filter Settings
- Configuring Logging Settings
- Configuring Advanced Monitor Filter Settings
- Configuring Mirror Settings

Configuring General Settings

This section describes how to configure packet monitor general settings, including the number of bytes to capture per packet and the buffer wrap option. You can 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 general settings:

1. Navigate to the **Tools & Monitors > Packet Monitor** page.
2. Select the **General** tab.
3. Select the **Settings** tab.
4. In the **Number of Bytes To Capture (per packet)** box, type the number of bytes to capture from each packet. The minimum value is 64 and the maximum value is 65535.
5. To continue capturing packets after the buffer fills up, select **Wrap Capture Buffer Once Full**. Selecting this option causes packet capture to start writing captured packets at the beginning of the buffer again after the buffer fills. This option has no effect if FTP server logging is enabled on the **Logging** tab, because the buffer is automatically wrapped when FTP is enabled.
6. Under Exclude Filter, select **Exclude encrypted GMS traffic** to prevent capturing or mirroring of encrypted management 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.
7. Use the **Exclude Management Traffic** settings to prevent capturing or mirroring of management traffic to the appliance. Select the checkbox for each type of traffic (HTTP/HTTPS, SNMP, or SSH) to exclude. If management traffic is sent through a tunnel, the packets are not excluded.
8. Use the **Exclude Syslog Traffic** to settings to prevent capturing or mirroring of syslog traffic to the logging servers. Select the checkbox for each type of server (Syslog Servers or GMS Server) to exclude. If syslog traffic is sent through a tunnel, the packets are not excluded.
9. Use the **Exclude Internal Traffic** for settings to prevent capturing or mirroring of internal traffic between the SonicWall network security appliance and its High Availability partner or a connected SonicPoint. Select the checkbox for each type of traffic (HA, SonicPoint, BCP, Inter-Blade, or Back-Plane) to exclude.
10. To save your settings and exit the configuration window, click **Save**.

Configuring the Monitor Filter

All filters set on the Monitor Filter page are applied to both packet capture and packet mirroring.

To configure Monitor Filter settings:

1. Navigate to the **Tools & Monitors > Packet Monitor** page.
2. Select the **General** tab.
3. Select the **Monitor Filter** tab.
4. Choose **Enable filter based on the firewall/app rule** if you are using firewall rules to capture specific traffic.

Before the **Enable filter based on the firewall rule** option is selected, be certain you have selected one or more access rules on which to monitor packet traffic. This configuration is done from the **POLICY > Rules and Policies > Access Rules** page.

5. Specify how Packet Monitor filters packets using these options:

   - **Interface Name(s)** - You can specify up to ten interfaces separated by commas. Refer to the **Network > Interfaces** page in the management interface for the available interface names. You can use a negative value to configure all interfaces except the one(s) specified; for example: !X0, or !LAN.
   - **Ether Type(s)** - You can specify up to ten Ethernet types separated by commas. Currently, the following Ethernet types are supported:

     - ARP
     - IP
     - PPPoE-SES
     - PPPoE-DIS

     The latter two can be specified by PPPoE alone.

     This option is not case-sensitive. For example, to capture all supported types, you could enter: `ARP`, `IP`, `PPPOE`. You can 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/X. (Refer to Supported Packet Types for more information.)
   - **IP Type(s)** - You can specify up to ten IP types separated by commas. These IP types are supported:

     - TCP
     - UDP
     - ICMP
     - GRE
     - IGMP
     - AH
     - ESP

     You can 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.) This option is not case-sensitive.
   - **Source IP Address(es)** - You can specify up to ten IP addresses separated by commas; for example: 10.1.1.1, 192.2.2.2. You can use one or more negative values to capture packets from all but the specified addresses; for example: `!10.3.3.3`, `!10.4.4.4`.
   - **Source Port(s)** - You can specify up to ten TCP or UDP port numbers separated by commas; for example: 20, 21, 22, 25. You can use one or more negative values to capture packets from all but the specified ports; for example: `!80`, `!8080`.
   - **Destination IP Address(es)** - You can specify up to ten IP addresses separated by commas; for example: 10.1.1.1, 192.2.2.2. You can use one or more negative values to capture packets destined for all but the specified addresses; for example: `!10.3.3.3`, `!10.4.4.4`.

- **Destination Port(s)** - You can specify up to ten TCP or UDP port numbers separated by commas; for example: 20, 21, 22, 25. You can use one or more negative values to capture packets destined for all but the specified ports; for example: `!80, !8080`.
- **Enable Bidirectional Address and Port Matching** - When this option is selected, IP addresses and ports specified in the **Source** or **Destination** fields on this page are matched against both the source and destination fields in each packet.
- **Forwarded packets only** - Select this option to monitor any packets that are forwarded by the firewall.
- **Consumed packets only** - Select this option to monitor all packets that are consumed by internal sources within the firewall.
- **Dropped packets only** - Select this option to monitor all packets that are dropped at the perimeter.

  NOTE: If a field 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.

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

Configuring Display Filter Settings

This section describes how to configure packet monitor display filter settings. The values that 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.

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 & Monitors > Packet Monitor** page.
2. Select the **General** tab.
3. Select the **Display Filter** tab.
4. In the **Interface Name(s)** box, type the SonicWall network security interfaces for which to display packets, or use the negative format (!X0) to display packets captured from all interfaces except those specified. You can specify up to ten interfaces separated by commas. Refer to the **Network > Interfaces** screen in the management interface for the available interface names.
5. In the **Ether Type(s)** box, enter the Ethernet types for which you want to display packets, or use the negative format (`!ARP`) to display packets of all Ethernet types except those specified. You can specify up to ten Ethernet types separated by commas. Currently, these Ethernet types are supported:

   - ARP
   - IP
   - PPPoE-SES
   - PPPoE-DIS

   The latter two can be specified by PPPoE alone.

   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/X. (Refer to Supported Packet Types for more information.)

6. In the **IP Type(s)** box, enter the IP packet types for which you want to display packets, or use the negative format (!UDP) to display packets of all IP types except those specified. You can specify up to ten IP types separated by commas. These IP types are supported:
   - TCP
   - UDP
   - ICMP
   - GRE
   - IGMP
   - AH
   - ESP

   You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: `TCP`, `0x1`, `0x6`. To display all IP types, leave blank. (Refer to Supported Packet Types for more information.)
7. In the **Source IP Address(es)** box, type the IP addresses from which you want to display packets, or use the negative format (`!10.1.2.3`) to display packets captured from all source addresses except those specified.
8. In the **Source Port(s)** box, type the port numbers from which you want to display packets, or use the negative format (`!25`) to display packets captured from all source ports except those specified.
9. In the **Destination IP Address(es)** box, type the IP addresses for which you want to display packets, or use the negative format (`!10.1.2.3`) to display packets with all destination addresses except those specified.
10. In the **Destination Port(s)** box, type the port numbers for which you want to display packets, or use the negative format (`!80`) to display packets with all destination ports except those specified.
11. Select **Enable Bidirectional Address and Port Matching** to match the values in the source and destination fields against either the source or destination information in each captured packet.
12. Select **Forwarded** to display captured packets that the SonicWall network security appliance forwarded, .
13. Select **Generated** to display captured packets that the SonicWall network security appliance generated.
14. Select **Consumed** to display captured packets that the SonicWall network security appliance consumed.
15. Select **Dropped** to display captured packets that the SonicWall network security appliance dropped, .
16. To save your settings and exit the configuration window, click **Save**.

Configuring Logging Settings

This section describes how to configure Packet Monitor logging settings. 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.

To configure logging settings:

1. Navigate to the **Tools & Monitors > Packet Monitor** page.
2. Select the **General** tab.
3. Select the **Logging** tab.
4. In the **FTP Server IP Address** box, type the IP address of the FTP server.

   NOTE: Make sure that the FTP server IP address is reachable by the SonicWall network security appliance. An IP address that is reachable only through a VPN tunnel is not supported.
5. In the **Login ID** box, type the login name that the SonicWall network security appliance should use to connect to the FTP server.
6. In the **Password** box, type the password that the SonicWall network security appliance should use to connect to the FTP server.
7. In the **Directory Path** box, type the directory location for the transferred files. The files are written to this location relative to the default FTP root directory.

   For 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--3-22-08292006.cap`.
8. For HTML format, file names are in the form `packet-log_h-<>.html`. For example, an HTML file name is: `packet-log_h-3-22-08292006.html`.
9. Select **Log To FTP Server Automatically** to enable automatic transfer of the capture file to the FTP server when the buffer is full. Files are transferred in both libcap and HTML format.
10. Select **Log HTML File Along With .cap File (FTP)** to enable transfer of the file in HTML format as well as libcap format.
11. Click **Log Now** to test the connection to the FTP server and transfer the capture buffer contents to it.
12. For example, `packet-log-F-3-22-08292006.cap` or `packet-log_h-F-3-22-08292006.html`.
13. To save your settings and exit the configuration window, click **Save**.

Configuring Advanced Monitor Filter Settings

This section describes how to configure monitoring for packets generated by the SonicWall network security appliance and for intermediate traffic.

To configure the Advanced Monitor Filter settings:

1. Navigate to **Tools & Monitors > Packet Monitor**.
2. Click the **General** tab.
3. Click the **Advanced Monitor Filter** tab.
4. To monitor packets generated by the SonicWall network security appliance, select **Monitor Firewall Generated Packets**.
5. Even when other monitor filters do not match, this option ensures that packets generated by the SonicWall network security appliance are captured. This includes packets generated by HTTP(S), L2TP, DHCP servers, PPP, PPPOE, and routing protocols. 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.
6. To monitor intermediate packets generated by the SonicWall network security appliance, select **Monitor Intermediate Packets**. Selecting this checkbox enables, but does not select, the subsequent checkboxes for monitoring specific types of intermediate traffic. Select the checkbox for

any of the following options to monitor that type of intermediate traffic:

- **Monitor intermediate multicast traffic** – Capture or mirror replicated multicast traffic.
- **Monitor intermediate IP helper traffic** – Capture or mirror replicated IP Helper packets.
- **Monitor intermediate reassembled traffic** – Capture or mirror reassembled IP packets.
- **Monitor intermediate fragmented traffic** – Capture or mirror packets fragmented by the firewall.
- **Monitor intermediate remote mirrored traffic** – Capture or mirror remote mirrored packets after de-encapsulation.
- **Monitor intermediate IPsec traffic** – Capture or mirror IPSec packets after encryption and decryption.
- **Monitor intermediate SSL decrypted traffic** – Capture or mirror decrypted SSL packets. Certain IP and TCP header fields might not be accurate in the monitored packets, including IP and TCP checksums and TCP port numbers (remapped to port 80). DPI-SSL must be enabled to decrypt the packets.

7. **Restore original ports on SSL decrypted traffic** – Select to restore the original TCP ports from the encrypted connection in the SSL decrypted packets.

   - **Monitor intermediate decrypted LDAP over TLS packets** – Capture or mirror decrypted LDAPS packets. The packets are marked with “(ldp)” in the ingress/egress interface fields and has dummy Ethernet, IP, and TCP headers with some inaccurate fields. The LDAP server is set to 389. Passwords in captured LDAP bind requests are obfuscated.
   - **Monitor intermediate decrypted Single Sign On agent messages** – Capture or mirror decrypted messages to or from the SSO Agent. The packets are marked with “(sso)” in the ingress/egress interface fields and has dummy Ethernet, IP, and TCP headers with some inaccurate fields.

   ⓘ | **NOTE:** Monitor filters are still applied to all selected intermediate traffic types.
8. To save your settings and exit the configuration window, click **Save**.

Starting and Stopping Packet Mirror

You can 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 mirroring packets according to your configured settings, in the **Packet Monitor** section, click **Start Mirror**.
- stop mirroring packets, click **Stop Mirror**.

Topics:

- Configuring Mirror Settings

Monitoring Captured Packets

The **Captured Packets** page provides several buttons for general control of the packet monitor feature and display.

- **Monitor All** – Resets current monitor filter settings and advanced page settings so that traffic on all local interfaces is monitored. A confirmation dialog box displays when you click this button.
- **Monitor Default** – Resets current monitor filter settings and advanced page settings to factory default settings. A confirmation dialog box displays when you click this button.
- **Clear** – Clears the packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging. A confirmation dialog box displays when you click this button.

The other buttons and displays on this page are described in these sections:

- Starting and Stopping Packet Capture
- Starting and Stopping Packet Mirror

Starting and Stopping Packet Capture

You can 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 network security appliance captures all packets, except those for internal communication, and stops when the buffer is full or when you click **Stop Capture**.

To:

- set the statistics back to zero, click **Clear**.
- start the packet capture, in the **Packet Monitor** section, click **Start Capture**.
- stop the packet capture, click **Stop Capture**.

Topics:

- Monitoring Captured Packets

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 network security appliance.

To configure mirror settings:

1. Navigate to the **Tools & Monitors > Packet Monitor** page.
2. Select the **General** tab.
3. Select the **Mirror** tab.
4. In the **Mirror Settings** section, type the desired maximum mirror rate into the Maximum mirror rate (in kilobits per second) field. If this rate is exceeded during mirroring, the excess packets are not

mirrored and are counted as skipped packets. This rate applies to both local and remote mirroring. The default and minimum value is 100kbps, and the maximum is 1Gbps.

5. Select **Mirror only IP packets** to prevent mirroring of other Ether type packets, such as ARP or PPPoE. If selected, this option overrides any non-IP Ether types selected on the Monitor Filter view.
6. In the **Local Mirror Settings** section, select the destination interface for locally mirrored packets in the Mirror filtered packets to Interface (NSA platforms only) drop-down menu.
7. In the **Remote Mirror Settings (Sender) section**, in the **Mirror filtered packets to remote SonicWall firewall (IP Address)** field, type the IP address of the remote SonicWall to which mirrored packets are sent.

   NOTE: The remote SonicWall network security appliance must be configured to receive the mirrored packets.
8. In the **Encrypt remote mirrored packets via IPSec (preshared key-IKE)** field, type the preshared key to be used to encrypt traffic when sending mirrored packets to the remote SonicWall network security appliance. Configuring this field enables an IPSec transport mode tunnel between this appliance and the remote SonicWall network security appliance. This pre-shared key is used by IKE to negotiate the IPSec keys.
9. In the **Remote Mirror Settings (Receiver)** section, in the **Receive mirrored packets from remote SonicWall firewall (IP Address)** field, type the IP address of the remote SonicWall network security appliance from which mirrored packets are received.

   NOTE: The remote SonicWall network security appliance must be configured to send the mirrored packets.
10. In the **Decrypt remote mirrored packets via IPSec (preshared key-IKE)** field, type the pre-shared key to be used to decrypt traffic when receiving mirrored packets from the remote SonicWall network security appliance. Configuring this field enables an IPSec transport mode tunnel between this appliance and the remote SonicWall network security appliance. This pre-shared key is used by IKE to negotiate the IPSec keys.
11. Select the interface from the **Send received remote mirrored packets to Interface (NSA platforms only)** drop-down menu to mirror received packets to another interface on the local SonicWall network security appliance.
12. Select **Send received remote mirrored packets to capture buffer** to save received packets in the local capture buffer. This option is independent of sending received packets to another interface, and both can be enabled.
13. To save your settings and exit the configuration window, click **Save**.

Viewing Packet Monitoring Statistics

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

Topics:

- Capture Statistics
- Local Mirror Statistics
- Remote Mirror TX Statistics
- Remote Mirror RX Statistics
- FTP Statistics
- Current Buffer Statistics

Capture Statistics

The first section in the **Capture Statistics** 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 **Capture Statistics** section 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.

Local Mirror Statistics

The **Local Mirror Statistics** section displays this information about packets sent to another physical interface on the same SonicWall network security appliance:

- 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
- 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 Mirror TX Statistics

The **Remote Mirror TX Statistics** status indicator shows one of these three conditions:

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

It also displays these statistics:

- On/off indicator
- **Mirroring to** – The specified remote SonicWall IP address
- **packets mirrored** – The total number of packets mirrored to a remote SonicWall network security 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 network security appliance, either because of an unreachable port or other network issues

Remote Mirror RX Statistics

Remote Mirror RX Statistics track the packets received from a remote SonicWall network security appliance.

The status indicator shows one of these conditions:

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

It also displays these 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 Statistics

FTP Statistics displays one of these 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

To restart automatic FTP logging, see Restarting FTP Logging on page 85.

It also displays these statistics:

- On/off indicator
- **FTP Server Pass/Failure count** – 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

Topics:

- Restarting FTP Logging

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 & Monitors > Packet Monitor** page.
2. Select the **General** tab.
3. Select the **Logging** tab.
4. Verify that the settings are correct for each item on the page. (Refer to Configuring Logging Settings for more information.)
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 **Save**.

Current Buffer Statistics

The **Current Buffer Statistics** 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
- **Unknown** - number of unidentified packets

2

Viewing Connections

Your SonicWall network security appliance maintains a connections log for tracking all active connections to the SonicWall network security appliance.

To view the Connections table:

1. Navigate to **MONITOR | Tools & Monitors > Connections**.
2. Click **IPv4** or **IPv6** to view the connections for that IP type.

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.

Topics:

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

Searching the Connections

Use **Search** to find connections that meet specific search criteria.

- Type a search string into the **Search** field and the **Connections** table 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 **Connections** table so it displays only those connections matching the criteria specified in the **Filter** option.

Filter by

- Source Address
- Destination Address
- Destination PortProtocol
- 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.
- Click **Export**, 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:

1. Select **Save**.
2. Enter a filename and path.
3. Click **OK**.

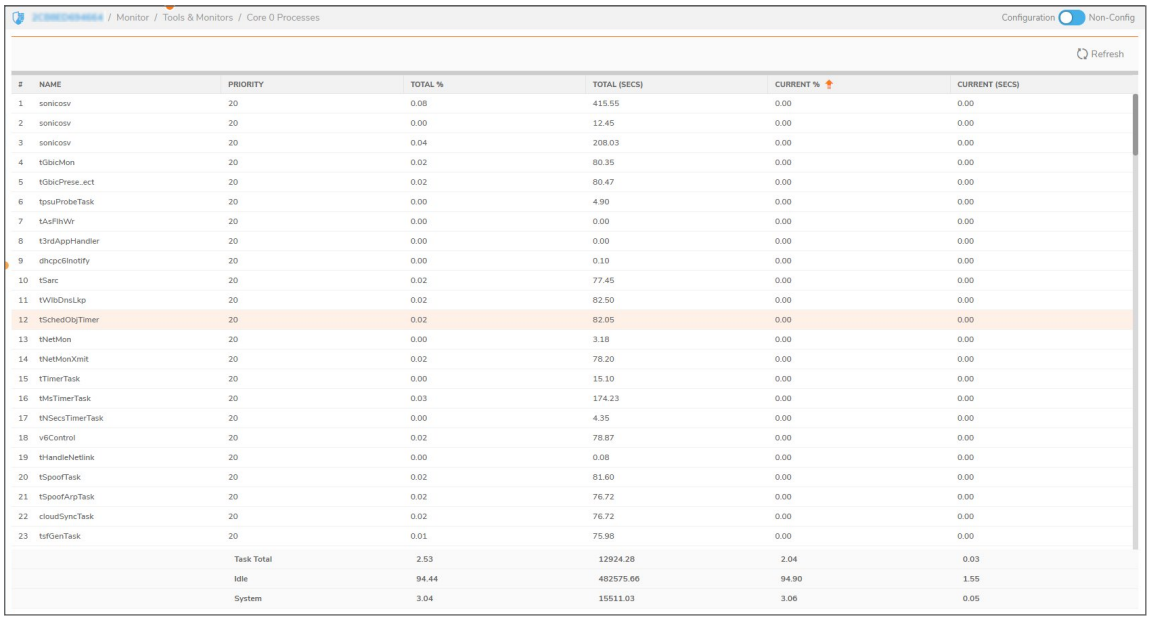
Connections Log Functions

EVENT LOG FUNCTIONS

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.

Monitoring Core 0 Processes

The **Core 0 Processes** page shows the individual system processes on core 0, their CPU utilization, and their system time.



#	NAME	PRIORITY	TOTAL %	TOTAL (SECS)	CURRENT %	CURRENT (SECS)
1	sonicosv	20	0.08	415.55	0.00	0.00
2	sonicosv	20	0.00	12.45	0.00	0.00
3	sonicosv	20	0.04	208.03	0.00	0.00
4	tGbicMon	20	0.02	80.35	0.00	0.00
5	tGbicPrese..ect	20	0.02	80.47	0.00	0.00
6	tpsuProbeTask	20	0.00	4.90	0.00	0.00
7	tAsFlhWr	20	0.00	0.00	0.00	0.00
8	t3rdAppHandler	20	0.00	0.00	0.00	0.00
9	dhcpc6Inotify	20	0.00	0.10	0.00	0.00
10	tSarc	20	0.02	77.45	0.00	0.00
11	tWlbDnsLkp	20	0.02	82.50	0.00	0.00
12	tSchedObjTimer	20	0.02	82.05	0.00	0.00
13	tNetMon	20	0.00	3.18	0.00	0.00
14	tNetMonXmit	20	0.02	78.20	0.00	0.00
15	tTimerTask	20	0.00	15.10	0.00	0.00
16	tMsTimerTask	20	0.03	174.23	0.00	0.00
17	tNSecsTimerTask	20	0.00	4.35	0.00	0.00
18	v6Control	20	0.02	78.87	0.00	0.00
19	tHandleNetlink	20	0.00	0.08	0.00	0.00
20	tSpoofTask	20	0.02	81.60	0.00	0.00
21	tSpoofArpTask	20	0.02	76.72	0.00	0.00
22	cloudSyncTask	20	0.02	76.72	0.00	0.00
23	tsfGenTask	20	0.01	75.98	0.00	0.00
	Task Total		2.53	12924.28	2.04	0.03
	Idle		94.44	482575.66	94.90	1.55
	System		3.04	15511.03	3.06	0.05

4

Using Packet Replay

Packet replay is an integrated tool to firewall for testing and debugging purposes. You can replay packets in these 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.

Topics:

- Single Packets
- Replay Pcap File
- Captured Packets

Single Packets

These procedures describe how to craft a packet for analysis. Some fields may change when the **IP Type** is changed.

Topics:

- Packet Crafting
- Packet Buffer

Packet Crafting

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

To craft a packet:

1. Navigate to **MONITOR > Tools &Monitor > Packet Replay**.
2. Click **Single Packet**.

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.

5. 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.

6. 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.

7. In the **Payload** field, enter or copy the payload hex data.
8. Click **Send**.

The crafted packet is sent to the firewall engine.

Packet Buffer

To build a packet buffer:

1. Navigate to **MONITOR > Tools &Monitor > Packet Replay**.
2. Click **Single Packet**.
3. Choose **Packet Buffer**.
4. From **Receiving Interface**, select the interface to receive the data.
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
- Replaying a MAC Pcap File

Replaying an IP Pcap File

To define by IP:

1. Navigate to **MONITOR > Tools &Monitor > Packet Replay**.
2. Click **Packets from File**.
3. Click **IP**.
4. Two IP filters are provided.
5. 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 assumed 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.

6. To search for and select a Pcap file to be replayed. click **Choose File**.
   - To upload the selected file, click **Upload**.
   - To replay the packets in the uploaded Pcap file, click **Replay**.
   - When done, to delete the uploaded file, click **Delete**.

Replaying a MAC Pcap File

To define by Mac:

1. Navigate to **MONITOR > Tools &Monitor > Packet Replay**.
2. Click **Packets from File**.
3. Click **MAC**.
4. Two IP filters are provided.
5. 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 IP packets that have the destination address listed in **MAC Address** are assumed 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.

6. To search for and select a Pcap file to be replayed. click **Choose File**.
    - To upload the selected file, click **Upload**.
    - To replay the packets in the uploaded Pcap file, click **Replay**.
    - When done, to delete the uploaded file, click **Delete**.

Captured Packets

Captured and replayed packets are displayed on the **Captured Packets** page.

The Captured Packets page provides three sections to display different views of captured packets:

- Captured Packets
- Packet Detail
- Hex Dump

To view the list of captured packets:

1. Navigate to **MONITOR > Tools &Monitor > Packet Replay**.
2. Click **Captured Packets**.

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.
Export	Exports the file in the format you select from the drop-down menu. Saved files are placed on your local management system.
Reload	Refreshes the packet display windows on this page to show new buffer data.
Grid Settings	Allows you to customize which columns are displayed.

Captured Packets

The **Captured Packets** page displays these 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 as:

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.

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

- **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 on the **Captured Packets** page, the packet header fields are displayed on the **Packet Detail** page. The display varies depending on the type of packet that you select.

Hex Dump

When you click a packet in the **Captured Packets** page, the packet data is displayed in hexadecimal and ASCII format on the **Hex Dump** page.

- 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.

5

SonicWall Support

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

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

The Support Portal enables you to:

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

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

About This Document

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information.

TIP: A TIP icon indicates helpful information.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

SonicOS and SonicOSX Tools & Monitors Administration Guide
Updated - August 2020
Software Version - 7
232-005352-00 Rev B

End User Product Agreement

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

Open Source Code

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

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