Packet Capture

Packet Capture

The Packet Capture tool is a valuable asset for use in debugging connectivity and configuration issues and for understanding traffic flows through your Firepower 9300 chassis. You can use the Packet Capture tool to log traffic that is going through specific interfaces on your Firepower 9300 chassis.

You can create multiple packet capture sessions, and each session can capture traffic on multiple interfaces. For each interface included in a packet capture session, a separate packet capture (PCAP) file will be created.

Backplane Port Mappings

The Firepower 9300 chassis uses the following mappings for internal backplane ports:

Security Module	Port Mapping	Description
Security Module 1/Security Engine	Ethernet1/9	Internal-Data0/0
Security Module 1/Security Engine	Ethernet1/10	Internal-Data0/1
Security Module 2	Ethernet1/11	Internal-Data0/0
Security Module 2	Ethernet1/12	Internal-Data0/1
Security Module 3	Ethernet1/13	Internal-Data0/0
Security Module 3	Ethernet1/14	Internal-Data0/1

Guidelines and Limitations for Packet Capture

The Packet Capture tool has the following limitations:

- Can capture only up to 100 Mbps.
- Packet capture sessions can be created even when there is not enough storage space available to run the packet capture session. You should verify that you have enough storage space available before you start a packet capture session.
- Does not support multiple active packet capturing sessions.
- There is no option to filter based on source or destination IPv6 address.
- Captures only at the ingress stage of the internal switch.
- Filters are not effective on packets that cannot be understood by the internal switch (for example Security Group Tag and Network Service Header packets).
- You cannot capture packets for an EtherChannel as a whole. However, for an EtherChannel allocated to a logical device, you can capture packets on each member interface of the EtherChannel.
- You cannot copy or export a PCAP file while the capture session is still active.
- When you delete a packet capture session, all packet capture files associated with that session are also deleted.

Creating or Editing a Packet Capture Session

Procedure

Step 1 Choose **Tools** > **Packet Capture**.

The **Capture Session** tab displays a list of currently configured packet capture sessions. If no packet capture sessions are currently configured, a message stating so is displayed instead.

Step 2 Do one of the following:

- To create a packet capture session, click the **Capture Session** button.
- To edit an existing packet capture session, click the **Edit** button for that session.

The left side of the window lets you select a specific application instance and then shows a representation of that instance. This representation is used to select the interfaces on which you would like to capture packets. The right side of the window contains fields for defining the packet capture session.

Step 3 On the left side of the window, click the name of the application instance for which you would like to capture packets.

Step 4 Click the interfaces on which you want to capture traffic. Selected interfaces show a check mark.

Step 5 To capture traffic from the logical device going out over the backplane ports:

a) Click the box representing the application instance.

The **Capture On**, **Application Port**, and **Application Capture Direction** fields are made available on the right side of the **Configure Packet Capture Session** window.

b) Select the backplane port you wish to capture traffic on or select **All Backplane Ports** from the **Capture On** drop-down list.

Step 6 Enter a name for the packet capture session in the **Session Name** field.

Step 7 Specify the buffer size to use for this packet capture session by selecting one of the pre-defined values from the **Buffer Size** list, or by selecting **Custom in MB** and then entering the desired buffer size. The specified buffer size must be between 256 and 2048 MB.

Step 8 Specify whether you want to overwrite existing PCAP files or append data to the PCAP files when this packet capture session is executed.

Step 9 To capture traffic between the application instance and a specific interface:

a) Click the box representing the logical device.
b) From the **Capture On** drop-down list, choose the application type (for example, **asa**).
c) Select the **Application Port** that you would like to capture traffic coming from or going to.
d) To capture only the traffic going from the logical device toward the specified interface, click the **Egress Packets** option next to **Application Capture Direction**.

Note If you choose **Egress Packets**, traffic will be captured only on the selected backplane ports—traffic will not be captured on physical ports even if you have selected them.

e) To capture traffic coming from or going to the specified interface, click the **All Packets** option next to **Application Capture Direction**.

Step 10 To filter the traffic being captured:

a) Click the **Apply Filter** option for the **Capture Filter** field.

You are given a set of fields for configuring the filter.

b) If you need to create the filter, click **Create Filter**.

You see the **Create Packet Filter** dialog box. For more information, see Configuring Filters for Packet Capture, on page 4.

c) Select the filter you want to use from the **Apply** drop-down list.
d) Select the interface to which you want to apply the filter from the **To** drop-down list.
e) To apply additional filters, click **Apply Another Filter** and then repeat the steps above to apply the additional filter.

Step 11 Do one of the following:

- To save this packet capture session and run it now, click the **Save and Run** button. This option is only available if no other packet capture sessions are currently running.
- To save this packet capture session so that it can be ran at a later time, click the **Save** button.

You see the **Capture Session** tab with your session listed along with any other sessions that have been created. If you selected **Save and Run**, your packet capture session will be capturing packets. You will need to stop capturing before you can download the PCAP files from your session.

Configuring Filters for Packet Capture

You can create filters to limit the traffic that is included in a packet capture session. You can select which interfaces should use a specific filter while creating a packet capture session.

Note If you modify or delete a filter that is applied to a packet capture session that is currently running, the changes will not take affect until you disable that session and then reenable it.

Procedure

Step 1 Choose **Tools** > **Packet Capture**.

The **Capture Session** tab displays a list of currently configured packet capture sessions. If no packet capture sessions are currently configured, a message stating so is displayed instead.

Step 2 Do one of the following:

- To create a filter, click the **Add Filter** button.
- To edit an existing filter, click the **Edit** button for that fitler.

You see the **Create or Edit Packet Filter** dialog box.

Step 3 Enter a name for the packet capture filter in the **Filter Name** field.

Step 4 To filter on a specific protocol, select it from the **Protocol** list, or select**Custom** and then enter the desired protocol. The custom protocol must be an IANA defined protocol in decimal format (0-255).

Step 5 To filter on a specific EtherType, select it from the **EtherType** list, or select**Custom** and then enter the desired EtherType. The custom EhterType must be an IANA defined EtherType in decimal format (for example, IPv4 = 2048, IPv6 = 34525, ARP = 2054, and SGT = 35081).

Step 6 To filter traffic based on an Inner VLAN (VLAN ID while ingressing the port) or Outer VLAN (VLAN ID added by the Firepower 9300 chassis), enter the VLAN ID in the specified field.

Step 7 To filter traffic from a specific source or destination, enter the IP address and port or enter the MAC address in the specified source or destination fields.

Step 8 Click **Save** to save the filter,

You see the **Filter List** tab with your filter listed along with any other filters that have been created.

Starting and Stopping a Packet Capture Session

Procedure

Step 1 Choose **Tools** > **Packet Capture**.

The **Capture Session** tab displays a list of currently configured packet capture sessions. If no packet capture sessions are currently configured, a message stating so is displayed instead.

Step 2 To start a packet capture session, click the **Enable Session** button for that session and then click **Yes** to confirm.

Note You cannot start a packet capture session while another session is running.

The PCAP files for the interfaces included in the session will start collecting traffic. If the session is configured to overwrite session data, the existing PCAP data will be erased. If not, data will be appended to the existing file (if any).

While the packet capture session is running, the file size for the individual PCAP files will increase as traffic is captured. Once the Buffer Size limit is reached, the system will start dropping packets and you will see the Drop Count field increase.

Step 3 To stop a packet capture session, click the **Disable Session** button for that session and then click **Yes** to confirm.

After the session has been disabled, you can then download the PCAP files (see Downloading a Packet Capture File, on page 5).

Downloading a Packet Capture File

You can download the Packet Capture (PCAP) files from a session to your local computer so that they can be analyzed using a network packet analyzer.

Procedure

Step 1 Choose **Tools** > **Packet Capture**.

The **Capture Session** tab displays a list of currently configured packet capture sessions. If no packet capture sessions are currently configured, a message stating so is displayed instead.

Step 2 To download the PCAP file for a specific interface from a packet capture session, click the **Download** button that corresponds to that interface.

Note You cannot download a PCAP file while a packet capture session is running.

Depending on your browser, the specified PCAP file is either automatically downloaded to your default download location or you are prompted to save the file.