Configure packet capture

Published: 2024-04-02

Packet capture enables you to collect, store, and retrieve data packets from your network traffic. You can download a packet capture file for analysis in a third-party tool, such as Wireshark. Packets can be inspected to diagnose and resolve network problems and to verify that security policies are being followed.

By adding a packet capture disk to the ExtraHop sensor, you can store the raw payload data sent to your ExtraHop system. This disk can be added to your virtual sensor or an SSD that is installed in your physical sensor.

These instructions only apply to ExtraHop systems that have a precision packet capture disk. To store packets on an ExtraHop packetstore appliance, see the packetstore deployment guides.

Important: Systems with self-encrypting disks (SEDs) cannot be configured for software encryption on packet captures. For information on enabling security on these systems, see Configure self-encrypting disks (SEDs).

Packet slicing

By default, the packetstore saves whole packets. If packets are not already sliced, you can configure the sensor to store packets sliced to a fixed number of bytes for improved privacy and lookback.

For more information on configuring this feature in your running configuration file, contact ExtraHop Support.

Enable packet capture

Your ExtraHop system must be licensed for packet capture and configured with a dedicated storage disk. Physical sensors require an SSD storage disk and virtual sensors require a disk configured on your hypervisor.

Before you begin

- Verify that your ExtraHop system is licensed for Packet Capture by logging in to the Administration settings and clicking **License**. Packet Capture is listed under Features and **Enabled** should appear.

  Important: The capture process restarts when you enable the packet capture disk.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Appliance Settings section, click **Disks**.
3. Depending on your sensor type and menu options, configure the following settings.
   - For physical sensors click **Enable** next to SSD Assisted Packet Capture, and then click **OK**.
   - For virtual sensors, verify that `running` appears in the Status column and that the disk size you configured for packet capture appears in the Size column. Click **Enable** next to Triggered Packet Capture, and then click **OK**.

Next steps

Your packet capture disk is now enabled and ready to store packets. Click **Configure** if you want to encrypt the disk, or configure global or precision packet captures.

Encrypt the packet capture disk

Packet capture disks can be secured with 256-bit AES encryption.

Here are some important considerations before you encrypt a packet capture disk:

- You cannot decrypt a packet capture disk after it is encrypted. You can clear the encryption, but the disk is formatted, and all data is deleted.
- You can lock an encrypted disk to prevent any read or write access to stored packet capture files. If the ExtraHop system is restarted, encrypted disks are automatically locked and remain locked until they are unlocked with the passphrase. Unencrypted disks cannot be locked.
- You can reformat an encrypted disk, but all data is permanently deleted. You can reformat a locked disk without unlocking the disk first.
- You can perform a secure delete (or system wipe) of all system data. For instructions, see the ExtraHop Rescue Media Guide.

Important: Systems with self-encrypting disks (SEDs) cannot be configured for software encryption on packet captures. For information on enabling security on these systems, see Configure self-encrypting disks (SEDs).

1. In the Appliance Settings section, click **Disks**.
2. On the Disks page, select one of the following options based on your sensor type.
   - For virtual sensors, click **Configure** next to Triggered Packet Capture.
   - For physical sensors, click **Configure** next to SSD Assisted Packet Capture.
3. Click **Encrypt Disk**.
4. Specify a disk encryption key from one of the following options:
   - Type a passphrase into the Passphrase and Confirm fields.
   - Click **Choose File** and select an encryption key file.
5. Click **Encrypt**.

Next steps
You can change the disk encryption key by returning to the Disks page and clicking **Configure** and then **Change Disk Encryption Key**.

Format the packet capture disk

You can format an encrypted packet capture disk to permanently remove all packet captures. Formatting an encrypted disk removes the encryption. If you want to format an unencrypted packet capture disk, you must remove the disk, and then enable the disk again.

Warning: This action cannot be reversed.

1. In the Appliance Settings section, click **Disks**.
2. On the Disks page, choose one of the following options based on your appliance platform.
   - For virtual sensors, click **Configure** next to Triggered Packet Capture.
   - For physical sensors, click **Configure** next to SSD Assisted Packet Capture.
3. Click **Clear Disk Encryption**.
4. Click **Format**.

Remove the packet capture disk

If you want to replace a packet capture disk, you must first remove the disk from the system. When a packet capture disk is removed from the system, all of the data on the disk is permanently deleted.

Removing the disk requires selecting a format option. On physical appliances, you can safely remove the disk from the appliance after this procedure is complete.

1. In the Appliance Settings section, click **Disks**.

2. On the Disks page, choose one of the following options based on your appliance platform.
   - For virtual appliances, click **Configure** next to Triggered Packet Capture.
   - For physical devices, click **Configure** next to SSD Assisted Packet Capture.
3. Click **Remove Disk**.
4. Select one of the following format options:
   - **Quick Format**
   - **Secure Erase**
5. Click **Remove**.

Configure a global packet capture

A global packet capture collects every packet that is sent to the ExtraHop system for the duration that matches the criteria.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Packet Captures section, click **Global Packet Capture**.
3. In the Start Global Packet Capture section, complete the following fields. You only need to specify the criteria you want for the packet capture:

   • **Name:** A name to identify the packet capture.

   • **Max Packets:** The maximum number of packets to capture.

   • **Max Bytes:** The maximum number of bytes to captures.

   • **Max Duration (milliseconds):** The maximum duration of the packet capture in milliseconds. We recommend the default value of 1000 (1 second), or configure up to 60000 milliseconds (1 minute).

   • **Snaplen:** The maximum number of bytes copied per frame. The default value is 96 bytes, but you can set this value to a number between 1 and 65535.
4. Click **Start**.

   Tip: Make a note of the time you start the capture to make it easier to locate the packets.
5. Click **Stop** to stop the packet capture before any of the maximum limits are reached.

Download your packet capture.

- On Reveal(x) Enterprise systems, click **Packets** from the top menu and then click **Download PCAP**.

  To help locate your packet capture, click and drag on the Packet Query timeline to select the time range when you started the packet capture.
- On ExtraHop Performance systems, click the System Settings icon, click **All Administration**, and then click **View and Download Packet Captures** in the Packet Capture section.

Configure a precision packet capture

Precision packet captures require ExtraHop Triggers, which enable you to capture only the packets that meet your specifications. Triggers are highly customizable user-defined code that run upon defined system events.

Before you begin
Packet capture must be licensed and enabled on your ExtraHop system.

It is recommended that you have familiarity with writing triggers before configuring a precision packet capture. Here are some resources to help you learn about ExtraHop Triggers:

- Trigger concepts
- Build a trigger
- Trigger API Reference
- Walkthough: Initiate precision packet captures to analyze zero window conditions

In the following example, the trigger captures an HTTP flow with the name `HTTP host <hostname>` and stops the capture after a maximum of 10 packets are collected.

1. Click the System Settings icon and then click **Triggers**.
2. Click **Create**.
3. Type a name for the trigger and select the HTTP_REQUEST and HTTP_RESPONSE events.
4. Type or paste the following trigger code in the right pane.

```
Flow.captureStart("HTTP host " + HTTP.host, {maxPackets: 10});
```

5. Assign the trigger to a device or group of devices.

   Warning: Running triggers on unnecessary devices and networks exhausts system resources. Minimize performance impact by assigning a trigger only to the specific sources that you need to collect data from.

6. Select **Enable trigger**.
7. Click **Save**.

Next steps
Download the packet capture file.

- On Reveal(x) Enterprise systems, click **Records** from the top menu. Select **Packet Capture** from the Record Type drop-down list. After the records associated with your packet capture appear, click the Packets icon, and then click **Download PCAP**.
- On ExtraHop Performance systems, click the System Settings icon, click **All Administration**, and then click **View and Download Packet Captures** in the Packet Capture section.

View and download packet captures

If you have packet captures stored on a virtual disk or on an SSD disk in your sensor, you can manage those files from the View Packet Captures page in the Administration settings. For Reveal(x) systems and on ExtraHop packetstores, view the Packets page.

The View and Download Packet Captures section only appears on ExtraHop Performance systems. On Reveal(x) systems, precision packet capture files are found by searching Records for the packet capture record type.

- Click **Configure packet capture settings** to automatically delete stored packet captures after the specified duration (in minutes).
- View statistics about your packet capture disk.
- Specify criteria to filter packet captures and limit the number of files displayed in the Packet Capture List.
- Select a file from the Packet Capture list and then download or delete the file.

  Note: You cannot delete individual packet capture files from Reveal(x) systems.