Analyze Traffic with Monitoring Interfaces and Packet Forwarding

Published: 2018-02-06

This guide explains how to configure an ExtraHop appliance to analyze network traffic using both monitoring interfaces and packet forwarding with remote packet capture system (RPCAP). This guide is intended for ExtraHop users with firmware version 3.10 and later.

Activate your license for the ExtraHop appliance

If you have not yet activated your license, you must do so before you can configure your ExtraHop appliance.

To activate your license, complete the following steps.

1. After the ExtraHop appliance has booted, browse to the Admin UI (`https://<extrahop_management_ip/admin`). The license agreement appears.
2. Review the license agreement.
3. Select **I Agree** and click **Submit**.
4. On the Login page, enter `setup` for the username.
   - The password for virtual appliances is `default`.
   - The password for physical appliances is the service tag number on the pullout tab on the front of the appliance.
5. Go to the System Settings section and click **License**.
6. Click **Register** to enter the product key.
7. Enter the product key and then click **Register**.
   The ExtraHop system contacts the license server and validates the product key. After the product key is validated, the license is downloaded. License information is displayed in the System Information section on the License Administration page. The ExtraHop is now able to receive traffic from packet forwarders.

Configuration examples for ExtraHop appliances

You can use packet forwarding on 1GbE interfaces only. This reduces the packet processing resources available on other interfaces, which affects the total throughput. Refer to the following table for the maximum throughput of each ExtraHop appliance with monitoring interfaces and packet forwarding enabled.

ExtraHop Appliance	Throughput	Throughput with Packet Forwarding
EDA 2000v/EDA 3000	3GbE	3GbE
EDA 6000	10GbE	5GbE + 3GbE
EDA 8000	20GbE	10GbE + 3GbE

You can use interfaces 1 through 4 as management interfaces. You can use interfaces 2 through 4 for monitoring only, or you can disable them.

The following examples assume your network is DHCP-enabled.

Note: If your network does not support DHCP, refer to Appendix B to set a static IP address.

Example: Configure 10GbE + 1GbE RPCAP (EDA 5000/6000/8000)

The following configuration captures traffic on the 10GbE interfaces normally, and also shows how to configure interface 2 to use RPCAP. ExtraHop does not recommend sending RPCAP traffic to the management interface because it might overload the management plane.

1. Go to the Network Settings section.
2. Click **Connectivity**.
3. Go to the Interface 2 section.
4. Click **Change**.
5. Click the **Interface Mode** drop-down list and select **Management Port + RPCAP/ERSPAN Target**.
6. Click the **DHCP** checkbox.

   Note: If your network does not support DHCP, refer to Appendix B to configure a static IP address.
7. Type information into the IP Address and Netmask fields.
8. Click **Save**.
9. Go to the 10GbE Monitoring Interfaces section and click the **Enabled** checkbox.
10. Click **Save**.

Example: Configure two 1GbE + 1GbE RPCAP (EDA 2000v/3000)

DHCP is enabled for interface 2 (the 1GbE interface closest to the management interface) and RPCAP traffic is sent to that address. The other 1GbE interfaces, interfaces 3 and 4, capture traffic through the physical feed.

The default configuration on the EDA 2000v/3000 uses interfaces 2 through 4 for monitoring. To use interface 2 for RPCAP, complete the following steps.

1. Go to the Network Settings section and click **Connectivity**.
2. Go to the Interface 1 section and verify the **Interface Mode** uses the Management Port.
3. Go to the Interface 2 section and click **Change**.
4. Click the **Interface Mode** drop-down list, select **Management Port + RPCAP/ERSPAN Target**.
5. Click the **DHCP** checkbox.

   Note: If your network does not support DHCP, refer to Appendix B to configure a static IP address.
6. Type information into the IP Address and Netmask fields.
7. Click **Save**.
8. Go to the Interface 3 section and click **Change**.
9. Click the **Interface Mode** drop-down list and select **Monitoring Port (receive only)**.
10. Click **Save**.
11. Go to the Interface 4 section and click **Change**.
12. Click the **Interface Mode** drop-down list, select **Monitoring Port (receive only)**.
13. Click **Save**.

Example: Configure 10GbE + One 1GbE Monitoring + 2GbE RPCAP (EDA 5000/6000/8000)

By default, the ExtraHop appliance has 10GbE interfaces enabled. Interface 1 is used for management and interface 2 through 4 are disabled. To configure two interfaces for RPCAP, follow the steps below.

In this example, DHCP is enabled for interface 2 and interface 3, and RPCAP traffic is sent to those addresses. The 1GbE interface, interface 4, and the 10GbE interfaces capture traffic through the physical feed.

1. Go to the Network Settings section and click **Connectivity**.
2. Go to the Interface 2 section and click **Change**.
3. Click the **Interface Mode** drop-down list and select **Management Port + RPCAP/ERSPAN Target**.
4. Click the **DHCP** checkbox.
5. Type information into the IP Address and Netmask fields.
6. Click **Save**.
7. Go to the Interface 3 section and click **Change**.
8. Click the **Interface Mode** drop-down list, select **Management Port + RPCAP/ERSPAN Target**.
9. Click the **DHCP** checkbox.
10. Type information into the IP Address and Netmask fields.
11. Click **Save**.
12. Go to the Interface 4 section and click **Change**.
13. Click the **Interface Mode** drop-down list and select **Monitoring Port (receive only)**.
14. Click **Save**.
15. Go to the 10GbE Monitoring Interfaces section and ensure the **Enabled** checkbox is selected.

Example: Configure 10GbE + Three 1GbE Monitoring (EDA 5000/6000/8000)

By default, the ExtraHop appliance has 10GbE interfaces enabled. Interface 1 is used for management and interface 2 through 4 are disabled. In order to configure three interfaces for monitoring, follow the steps below.

In this example, DHCP is enabled for the management interface, interface 1, and all interfaces capture traffic through the physical feed.

1. Go to the Network Settings section and click **Connectivity**.
2. Go to the Interface 1 section and verify the **Interface Mode** uses the **Management Port**.
3. Go to the Interface 2 section and click **Change**.
4. Click the **Interface Mode** drop-down list, select **Monitoring Port (receive only)**.
5. Click **Save**.
6. Go to the Interface 3 section and click **Change**.
7. Click the **Interface Mode** drop-down list, select **Monitoring Port (receive only)**.
8. Click **Save**.
9. Go to the Interface 4 section and click **Change**.
10. Click the **Interface Mode** drop-down list, select **Monitoring Port (receive only)**.
11. Click **Save**.
12. Go to the 10GbE Monitoring Interfaces section and make sure the **Enabled** checkbox is selected.

Open ports on the firewall

The following ports must be open for packet forwarder traffic to reach the ExtraHop:

TCP ports 80 and 443 inbound to ExtraHop

These ports are used to download the installer. If opening these ports is difficult, you can copy the installer to each rpcapd machine manually. Refer to Installing the High-Speed Packet Forwarder on the Server Sending Traffic.

TCP/UDP port 2003 inbound to ExtraHop

By default, RPCAP will function correctly on port 2003 alone, but you may configure other ports as needed.

Note: By default, the ExtraHop system accepts RPCAP forwarded packets on port 2003. If you configure a port other than 2003 for the packet forwarder, you must modify the default ExtraHop configuration to listen on that port.

Monitor servers using RPCAP

To monitor servers using RPCAP, you must do the following:

1. Ensure the high-speed packet forwarder is enabled on the ExtraHop appliance. Refer to Appendix C for optional settings.
2. Install the high-speed packet forwarder on the servers sending traffic.
3. Analyze packet-forwarding traffic in the ExtraHop Web UI.

Install the high-speed packet forwarder on a Linux server sending traffic

You must run the packet forwarder command on each server to be monitored to forward packets to the ExtraHop system.

1. Run the following command to download the packet forwarder on the server:

```
export RPCAP_HOST_IP=<extrahop_management_ip>
curl --connect-timeout 10 --fail \
-k "http://$RPCAP_HOST_IP/tools/install-rpcapd.sh" > \
install-rpcapd.sh
```

   Where <*extrahop_management_ip*> is the ExtraHop system's interface 1 (management) IP address.
2. Run the following command to install and run the packet forwarder on the server:

```
sudo sh ./install-rpcapd.sh <extrahop_rpcap_target_ip>
<extrahop_rpcapd_port>
```

   Where <*extrahop_rpcap_target_ip*> is the IP addresses on the ExtraHop system's interface that is listening for the remote packet capture. You can look up IP addresses in the Admin UI, by going to Network Settings and clicking **Connectivity**.

   Where <*extrahop_rpcapd_port*> is the port used for the packet forwarder, which is port 2003 by default.
3. To start, stop, restart, reload, or check the status of the packet forwarder, run the command:

```
sudo /etc/init.d/rpcapd {start|stop|status|restart|force-reload}
```

4. To view packet forwarder messages, run the command:

```
tail /var/log/messages or tail /var/log/syslog
```

5. To run the packet forwarder manually for debugging purposes only, run the command:

```
sudo /opt/extrahop/sbin/rpcapd -a
 <extrahop_rpcap_target_ip>,<extrahop_rpcapd_port>-n –v
```

6. To run the packet forwarder on servers with multiple interfaces, refer to Appendix E.

Install the high-speed packet forwarder on a Windows server sending traffic

You must run the packet forwarder command on each server to be monitored to forward packets to the ExtraHop system.

1. Open a PowerShell shell with Administrator privileges on the Windows server.
2. Change the PowerShell execution policy to `unrestricted` by running the following command:

```
set-executionpolicy unrestricted
```

3. Download the packet forwarder on the server by running the following command:

```
(new-object system.net.webclient).downloadfile("http://
<extrahop_management_ip>/tools/install-rpcapd.ps1","install-rpcapd.ps1");
```

4. Install the packet forwarder on the server:

```
.\install-rpcapd.ps1 -MgmtIp <extrahop_management_ip> -RpcapIp
 <extrahop_rpcap_target_id> -RpcapPort <extrahop_rpcapd_port>
```

Where *<extrahop_management_ip>* is the ExtraHop system's interface 1 IP address, *<extrahop_rpcap_target_ip>* is the IP addresses on the ExtraHop system's interface that is listening for the remote packet capture, and *<extrahop_rpcap_port>* is the port used for the packet forwarder, typically port 2003.

You can verify IP addresses in the Admin UI, by going to Network Settings and clicking **Connectivity**.

5. To set the PowerShell execution policy back to the default, run the following command:

```
set-executionpolicy restricted
```

6. To start, stop, restart, or check the status of the packet forwarder, run the following commands:
   a) Start the service:

```
Start-Service rpcapd
```

   b) Stop the service:

```
Stop-Service rpcapd
```

   c) Restart the service:

```
Restart-Service rpcapd
```

   d) Check the status of the rpcapd service:

```
Get-Service rpcapd
```

7. To view packet forwarder messages, open the Event Viewer, click **Windows Logs**, and select **Application**. In the Application panel, sort by source and scroll down to **rpcapd**.

   Note: When reinstalling rpcapd, if a message appears that rpcapd is being used by another process, make sure the Event Viewer is closed.

8. To run the packet forwarder manually for debugging purposes only, run the command:

```
"C:\Program Files\rpcapd\rpcapd" -a
 <extrahop_rpcap_target_ip>,<extrahop_rpcapd_port> -n –v
```

9. To run the packet forwarder on servers with multiple interfaces, refer to Appendix E.

Analyze packet forwarding traffic in the ExtraHop Web UI

To find out how much forwarded traffic the ExtraHop system is receiving, complete the following steps.

1. Log in to the ExtraHop Web UI (`https://<extrahop_management_ip>/extrahop`) and click **Settings** at the top right corner.
2. Click **System Health** to get more information about the packet forwarding traffic. This page displays charts for each packet forwarder connected to the ExtraHop system. These charts contain the following metrics:

   Encapsulation

   The total number of RPCAP encapsulation packets received by the ExtraHop system.

   Tunnel Eligible

   Total number of packets eligible to be forwarded to the ExtraHop system.

   Tunnel Sent

   Total number of RPCAP-tunneled packets forwarded to the ExtraHop system.

   Tunnel Received

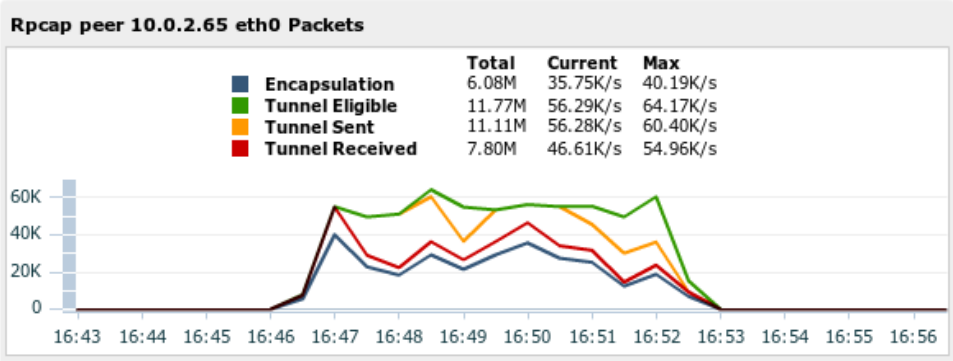
   Total number of RPCAP-tunneled packets received by the ExtraHop system.

   The Tunnel Eligible, Tunnel Sent, and Tunnel Received values should be equal if the ExtraHop system is receiving and processing all the packets sent by the server. If these values are not equal, use the following reference for troubleshooting:

   - If Tunnel Sent is less than Tunnel Eligible, the server is not able to forward out all the traffic. This might indicate that packet forwarding requires more processing or outbound bandwidth resources on the server. Consider separating the forwarding process onto a separate CPU or allocating a dedicated interface for forwarding traffic.
   - If Tunnel Received is less than Tunnel Sent, the ExtraHop system is not receiving all the traffic forwarded by the server. This might be related to network congestion or insufficient resources on the ExtraHop system. If you suspect it is related to resources, contact ExtraHop Support.

Appendix A: Advanced Troubleshooting

In the example below, Tunnel Eligible is 11.77M, peer sent is 11.11M, and processed is 7.8M. This means the ExtraHop system is seeing 7.8M out of 11.77M packets, or 66% of the traffic from this server running rpcapd.



In the example above, the interface eth0 of 10.0.2.65 had 11.77M (Tunnel Eligible) packets to forward. Ideally, the ExtraHop system would have processed all 11.77M packets. However, the ExtraHop system processed only 11.11M (Tunnel Sent) packets. This should match the number above, Tunnel Eligible, of 11.77M.

Possible reasons for the drops:

Issue	Symptom	Solution
Rpcapd is not pulling packets from libpcap fast enough.	krnldrops in the rpcapd stats.	Increase the libpcap buffer size in the rpcapd parameters, -z, as explained later.
The network is saturated, so rpcapd is blocked and waiting to send packets.	High RPCAP protocol throughput. Check the RPCAP protocol throughput graph. (Refer to the picture with both graphs above. The max is 473.11Mbps.) Displays as eagain or enobufs in the rpcapd stats.	Make sure RPCAP traffic is using a different interface than the monitored interface. For example, when monitoring eth0, make sure rpcapd is connecting to the ExtraHop system over eth1.

In the example above, the number of packets the ExtraHop system processed is lower than the number of Tunnel Sent packets. The number of processed packets is 7.80M. This should match the number of Tunnel Sent packets, which is 11.11M.

Possible reasons for the low processing:

Issue	Symptom	Solution
The RPCAP packets were dropped before reaching the ExtraHop system. The packet forwarder sends packets over UDP.	High RPCAP protocol throughput.	The ExtraHop system supports 1G of throughput on each interface. Refer to the throughput table earlier in this document to ensure traffic being sent to the ExtraHop system does not exceed the maximum throughput.
The ExtraHop is receiving too much traffic.	Go to the System Health page and view the **ExtraHop Rpcap Thread X Packets** charts. If a thread is processing near 100K packets per second, the thread could be saturated and is receiving too many packets.	Spin up another ExtraHop appliance and point half of the rpcapd forwarders at the new appliance.

Appendix B: Configure a static IP address

The ExtraHop system is delivered with DHCP enabled, but you can instead configure a static IP address.

If your network does not support DHCP, you can set a route manually to determine where the traffic goes. To manually set a route:

1. Go to the Network Settings section and click **Connectivity**.
2. In the Interfaces section, click on the interface you would like to manually set a route for.
3. On the Network Settings for Interface <x> page, where <*x*> is the interface number you selected, make sure that the **IP Address** and **Netmask** fields are complete and saved.
4. Click **Edit Routes**.
5. In the Add Route section, complete the **Network** and **Via IP** fields
6. Click **Add**.
7. Repeat the previous step for each route you want to add.
8. Click **Save**.

Note: The default time server setting is `pool.ntp.org`.To configure the time servers manually, refer to the System Settings section of the ExtraHop Admin UI Users Guide.

Appendix C: Additional RPCAP setting options

By default, the ExtraHop system accepts RPCAP forwarded packets on port 2003. The servers using the packet forwarder are directed to forward all traffic as denoted by the wildcard in the **Interface Address** column.

(Optional) To specify another port, subnet, or filter, complete the following steps.

1. Go to the RPCAP Settings section and click **Change**.
2. Change and modify the following settings on the Add RPCAP Port Definition page.

Port

Specifies the listening port on the ExtraHop system. Each port must be unique for each interface subnet on the same device. Different subnets across servers can use the same port. This is both a TCP and UDP port. If you are configuring multiple software taps and multiple software tap listeners, the payload might traverse a range of UDP ports. The range consists 16 ports starting with the port defined.

Interface Address

Specifies a subnet to choose the interface from which to forward packets. If the server has multiple interfaces that match the interface address, the first interface on the server sends traffic to the ExtraHop system.

Interface Name

Indicates the interface on the packet-forwarding server from which to forward packets.

Note: You must specify an interface address or an interface name. If you specify both, then both criteria will apply.

Filter

Specifies the traffic to forward using Berkeley Packet Filter syntax. For example, `TCP port 80` forwards only TCP traffic on port 80, and `not TCP port 80` forwards only non-TCP traffic on port 80.

Appendix D: Install the RPCAP file manually in Linux

Learn how to download and install the packet forwarder manually with Linux.

1. Go to `https://<extrahop_management_ip>/tools`.
2. Download the rpcapd file for Linux.
3. Install it on the server by running the following command:

```
sudo sh ./install-rpcapd.sh <extrahop_rpcap_target_ip>
      <extrahop_rpcapd_port>
```

Appendix E: Install the RPCAP file manually in Windows

Learn how to download and install the packet forwarder manually with Windows.

1. Go to `https://<extrahop_management_ip>/tools`.
2. Download and unzip the rpcapd file for Windows..
3. Open PowerShell and navigate to the directory containing the unzipped files.

4. Run the following command:

```
./install-rpcapd.ps1 -InputDir . -RpcapIp <extrahop_rpcap_target_ip> -
RpcapPort
              <extrahop_rpcapd_port>
```

Appendix F: Configure the packet forwarder on Linux servers with multiple interfaces

For servers with multiple interfaces, the packet forwarder can be configured to forward packets from a particular interface, or from multiple interfaces, by editing its configuration file on the server.

To edit the configuration file, complete the following steps.

1. After installing the packet forwarder, open the configuration file on the server:`/opt/extrahop/etc/rpcapd.ini`

   The configuration file contains this text or similar:

   ```
   ActiveClient = 10.0.0.100,2003
   NullAuthPermit = YES
   ```

2. Modify the existing `ActiveClient` line and create an `ActiveClient` line for each additional interface to be monitored. Specify each interface by its interface name or IP address.

   ```
   ActiveClient = <extrahop_management_ip>, <extrahop_rpcapd_port>,
    ifname=<interface_name>
   ```

   or

   ```
   ActiveClient = <extrahop_management_ip>, <extrahop_rpcapd_port>,
       ifaddr=<interface_address>
   ```

   Where <*interface_name*> is the name of the interface from which you want to forward packets.

   Where <*interface_address*> specifies the IP address of the interface from which the packets are forwarded. The <*interface_address*>might be either an individual IP address, such as 10.10.1.100, or a CIDR specification (network IP address/subnet prefix length) that contains the IP address, such as 10.10.1.0/24.

Appendix G: Configure the packet forwarder on Windows servers with multiple interfaces

For servers with multiple interfaces, the packet forwarder can be configured to forward packets from a particular interface, or from multiple interfaces, by editing its configuration file on the server.

To edit the configuration file, complete the following steps.

1. After installing the packet forwarder, open the configuration file on the server: `C:\Program Files\rpcapd\rpcapd.ini`

   After installation, the file contains this text or similar:

   ```
   ActiveClient = 10.0.0.100,2003
   NullAuthPermit = YES
   ```

2. Modify the existing `ActiveClient` line and create an `ActiveClient` line for each additional interface to be monitored. Specify each interface by its interface name or IP address. For every

`ActiveClient` line, the packet forwarder will independently forward packets from the interface specified in the line:

```
ActiveClient = <extrahop_management_ip>, <extrahop_rpcapd_port>,
    ifname=<interface_address>
```

or

```
ActiveClient = <extrahop_management)ip>, <extrahop_rpcapd_port>,
    ifaddr=<interface_name>
```

Where <*interface_address*> specifies the IP address of the interface from which the packets are forwarded. The <*interface_address*> may be either the IP address itself, such as 10.10.1.100, or a CIDR specification (network IP address/subnet prefix length) that contains the IP address, such as 10.10.1.0/24.

Where <*interface_name*> is the name of the interface from which the packets are forwarded. The name is formatted as `\Device\NPF_{<GUID>}`, where <*GUID*> is the globally unique identifier (GUID) of the interface. For example, if the interface GUID is `2C2FC212-701D-42E6-9EAE-BEE969FEFB3F`, the interface name is `\Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}`.

The following is an example of the configuration file specifying two interfaces using CIDR specifications that contain the interface IP address:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.0/24
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.0/24
NullAuthPermit = YES
```

The following is an example of the configuration file specifying two interfaces using the interface name:

```
ActiveClient = 10.10.6.45, 2003,
        ifname=\Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}
ActiveClient = 10.10.6.45, 2003,
        ifname=\Device\NPF_{3C2FC212-701D-42E6-9EAE-BEE969FEFB3F}
NullAuthPermit = YES
```

3. Save the configuration file and restart the packet forwarder by running the command `restart-service rpcapd`

   To reinstall the packet forwarder after changing the configuration file, run the installation command and replace –RpcapIp and –RpcapPort with the -KeepConfig flag in order to preserve the modified configuration file. For example:

   ```
   .\install-rpcapd.ps1 -MgmtIp <extrahop_management_ip> -KeepConfig
   ```

   or

   ```
   .\install-rpcapd.ps1 –InputDir . -KeepConfig
   ```

Appendix H: Tuning the Packet-Forwarding Configuration

To use the installer to change the packet-forwarding configuration, connect to the server running rpcapd and download the installer:

1. Run the command:

   ```
   curl --connect-timeout 10 --fail
         –k
   ```

```
'https://<extrahop_management_ip>/tools/install-rpcapd.sh' > install-
rpcapd.sh
```

Where <*extrahop_management_ip*> with the ExtraHop system's management IP address.

2. Each of the following tweaks adjusts the DAEMON_ARGS in `/etc/init.d/rpcapd`. You can edit this file directly instead of using the installer. Afterward, remember to restart rpcapd by running the command `sudo /etc/init.d/rpcapd restart`

   If Tunnel Eligible does not match Tunnel Sent, and the network is not saturated, try increasing the libpcap buffer size. The default size is 16MiB (16777216B). Try increasing the size to 32MiB (33554432B) or even 64MiB (67108864B) if the server has enough memory.

   - `rpcapd parameter: -z 33554432`
   - In Linux: `sudo sh ./install-rpcapd.sh <extrahop_rpcap_target_ip> <port_in_Running_Config> -S`
   - In Windows: `.\install-rpcapd.ps1 -MgmtIp <extrahop_management_ip> -RpcapIp <extrahop_rpcap_target_ip> -RpcapPort <extrahop_rpcapd_port> -DaemonAddlArgs "-S"`

   Make sure to stop this process when you are finished or it will fill the syslog.