Configure RPCAP for an ExtraHop packetstore

Published: 2024-04-01

If you have configured your ExtraHop sensor for RPCAP, you can configure a second feed of packets to be forwarded from your remote environment to the ExtraHop packetstore.

Before you begin

- Complete the procedures in the Packet Forwarding with RPCAP guide to configure your sensor.
- Deploy the Trace appliance. (See our deployment content.)
- Make sure the lowest port numbers are the same for both sensors and packetstores.

Deployment overview

The following steps outline the key procedures that are required to implement RPCAP with an ExtraHop Trace appliance.

1. First, configure the Trace appliance to accept RPCAP traffic and add packet-forwarding rules.
2. Next, download the rpcapd software for the Discover appliance that applies to your remote devices. (Linux and Windows are both supported.)
3. Next, install the rpcapd software on every Linux or Windows device that you want to forward traffic from. You must modify the configuration file (rpcapd.ini) to specify device interfaces or to direct traffic to the Discover appliances.
4. Finally, If your environment has a firewall, open ports on your firewall for the requisite RPCAP traffic.

Configure RPCAP on the ExtraHop system

We recommend that you configure a second interface only for RPCAP, rather than configuring both RPCAP and management on the the same interface. Configuring a dedicated RPCAP interface improves the likelihood that all packets will be successfully forwarded to the ExtraHop system.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **Connectivity**.
3. Select interface 1, 2, 3, or 4.

   The EDA 1000v and ETA 1150v only have interfaces 1 and 2.
4. From the Interface Mode drop-down list, select **Management + RPCAP/ERSPAN/VXLAN/GENEVE Target**.
5. Configure IPv4 addresses for the interface by choosing one of the following options:
   - Specify a static IPv4 address in the **IPv4 address** field, and then specify a netmask and gateway IP address.
   - Enable dynamic IPv4 addresses by clicking **Enable DHCPv4**.

   Note: Although you can enable IPv6 addresses on the interface, you cannot forward RPCAP packets over IPv6. You must configure an IPv4 address on the interface to enable RPCAP. For more information about configuring a management + capture interface, see the ExtraHop Hardware FAQ.
6. Click **Save**.

Configure packet-forwarding rules on the ExtraHop system

After you configure the interface as an RPCAP target, you must configure packet-forwarding rules. Packet forwarding rules limit what traffic is allowed to be sent to the ExtraHop system through RPCAP.

By default, an entry is configured for port 2003 that accepts traffic from all interface addresses. You can modify the default entry for your environment, delete the default entry, and add additional entries. Make sure that you specify port numbers greater than 1023 to avoid conflicts with reserved ports. It is a good practice to set these rules first, so that when you configure rpcapd on your remote devices, the ExtraHop system is ready to receive the forwarded packets.

You can configure up to 16 rules for packet forwarding in the ExtraHop system; each rule must have a single TCP port over which the ExtraHop system communicates the packet-forwarding rules to rpcapd devices.

Important: The information in the rpcapd configuration file on the devices that are forwarding packets must not contradict the rules set in the ExtraHop system.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **Connectivity**.
3. In the RPCAP Settings section, complete one of the following actions:
   - Click on **2003** to open the default entry.
   - Click **Add** to add a new entry.

     Important: Port numbers must be 1024 or greater.
4. In the Add RPCAP Port Definition section, complete the following information:
   a) In the Port field, type the TCP port that will communicate information about this packet forwarding rule. Port entries must be unique for each interface subnet on the same server.
   b) In the Interface Address field, type the IP address or CIDR range of the interface on the device that you want the ExtraHop system to receive traffic from. For example, 10.10.0.0/24 will forward all traffic on the system that is part of that CIDR range, * is a wildcard that will match all traffic on the system, or 10.10.0.5 will only send traffic on the interface that matches the 10.10.0.5 IP address.

      Note: If a machine has multiple interfaces, and you do not specify an interface in the traffic rules or the rpcapd.ini file, the ExtraHop system will pick a single interface to forward traffic from. The ExtraHop system usually picks the interface with the name that comes first alphabetically. However, we recommend that you specify the interface in the traffic rules to ensure consistent behavior. We also recommend that you select the interface by address, rather than name.
   c) In the Interface Name field, type the name of the interface on the device that will send traffic to the ExtraHop system. For example, `eth0` in a Linux environment or `\Device \NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}` in a Windows environment.
   d) In the Filter field, type the ports for the traffic that you want to forward to the ExtraHop system in Berkeley Packet Filter (BPF) syntax. For example, you can type `tcp port 80` to forward all traffic on TCP port 80 from your remote network device to the ExtraHop system. For more information about BPF syntax, see Filter packets with Berkeley Packet Filter syntax.
5. Click **Save**, which saves the settings and restarts the capture.
6. Repeat these steps to configure additional rules. You can add up to 16 rules.

Save the running configuration file

After you configure the interface and configure packet forwarding rules, you must save the changes to the running configuration file.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **Connectivity**.
3. Click **View and Save Changes**.
4. Review the changes in the Current running config (not yet saved) pane.
5. Click **Save**.
6. Click **Done**.

Add entries for the Trace appliance to your rpcapd Linux devices

Complete the following steps to begin sending packets to the Trace appliance from remote Linux devices.

1. Open the rpcapd configuration file (/opt/extrahop/etc/rpcapd.ini) in a text editor. The configuration file contains text similar to the following example:

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

2. Add another ActiveClient entry to the end of the file with the IP address of your Trace appliance and the lowest port that your Discover appliance is configured with. In the following example, the IP address for the Discover appliance is 10.0.0.100 and the IP address for the Trace appliance is 10.1.20.1, and both appliances are listening on TCP port 2003.

```
ActiveClient = 10.0.0.100,2003
ActiveClient = 10.1.20.1,2003
NullAuthPermit = YES
```

3. After editing the configuration (rpcapd.ini) file, restart the RPCAP process.

For sample configurations, see the Packet Forwarding with RPCAP guide.

Add entries for the Trace appliance to your rpcapd Windows devices

Complete the following steps to begin sending packets to the Trace appliance from remote Windows devices.

1. Open the rpcapd configuration file (C:\Program Files\rpcapd\rpcapd.ini).The file contains text similar to the following:

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

2. Add another ActiveClient entry to the end of the file with the IP address of your Trace appliance and the lowest port that your Discover appliance is configured with. In the following example, the IP address for the Discover appliance is 10.0.0.100 and the IP address for the Trace appliance is 10.1.20.1, and both appliances are listening on TCP port 2003.

```
ActiveClient = 10.0.0.100,2003
ActiveClient = 10.1.20.1,2003
NullAuthPermit = YES
```

3. After editing the configuration (rpcapd.ini) file, restart the rpcapd process.

For sample configurations, see the Packet Forwarding with RPCAP guide.