

Configure RPCAP for a Trace Appliance

Published: 2018-07-07

If you have configured your Discover appliance for RPCAP, you can configure a second feed of packets to be forwarded from your remote environment to the Trace appliance.

Before you begin

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

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 from 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 appliance

You can configure RPCAP and management on the same interface, but you might want to configure a second interface only for RPCAP to avoid unnecessary performance degradation.


1. Log into the Admin UI of the ExtraHop appliance that you want to forward packets to.
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 Port + RPCAP/ERSPAN Target**.
5. DHCPv4 is enabled by default. If your remote devices do not support DHCP, you can disable DHCP and configure a static IP address. Or, you can click on IPv6 to configure your IP address through DHCP or through a static IP address or range on an IPv6 network. Make sure the management interfaces are not configured with overlapping subnets.
6. Click **Save**.

Configure packet-forwarding rules on the ExtraHop appliance

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 appliance 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. It is a good practice to set these rules first, so that when you configure rpcapd on your remote devices, the ExtraHop appliance is ready to receive the forwarded packets.

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

1. In the Network Settings section, click **Connectivity**.
2. 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.
3. 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 appliance 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.
 - c) In the Interface Name field, type the name of the interface on the device that will send traffic to the ExtraHop appliance. 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 appliance 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 appliance. For more information about BPF syntax, see <http://biot.com/capstats/bpf.html>.
4. Click **Save**, which saves the settings and restarts the capture.
5. 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. In the Network Settings section, click **Connectivity**.
2. Click **View and Save Changes**.
3. Review the changes in the Current running config (not yet saved) pane.
4. Click **Save**.
5. 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.