Packet Forwarding with RPCAP

Published: 2018-07-17

The ExtraHop Discover appliance generates metrics about your network and applications through a wire data feed, which is typically mirrored from a switch. However, you might not always have access to a switch or you might want to monitor a specific device that is outside of your wire data network. Additionally, in a cloud environment, such as Microsoft Azure or Amazon Web Services (AWS), you cannot directly access switch hardware. For these types of environments, you can forward packets to a Discover appliance through a software tap such as Remote Packet Capture (RPCAP).

This guide provides concepts about the ExtraHop RPCAP implementation along with instructions for all required procedures.

You must have experience with ExtraHop appliances, port mirroring, network concepts, and installing utilities on servers to complete the procedures in this guide.

Deployment overview

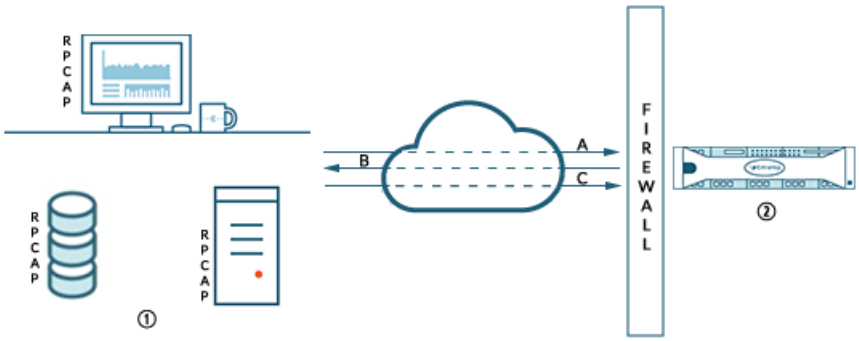
The following steps outline the key procedures that are required to implement RPCAP with a Discover appliance.

1. First, configure the Discover appliance to accept RPCAP traffic and add packet-forwarding rules.
2. Next, download the rpcapd software for your operating system from the Discover appliance.
3. If your environment has a firewall, open ports on your firewall for the requisite RPCAP traffic.
4. Finally, 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 multiple Discover appliances.

Implementing RPCAP with the ExtraHop system

RPCAP is implemented through a small binary file that runs as a daemon (rpcapd) on each device that you want to monitor traffic for. The RPCAP installation package for Windows or Linux can be downloaded directly from your Discover appliance.

The following figure shows a simple RPCAP implementation with a single Discover appliance behind a firewall. Your network configuration might vary.



① Devices with rpcapd installed and configured with the Discover appliance information.

② Discover appliance with RPCAP enabled and packet-forwarding rules configured.

A Devices initiate connection over a TCP port.

B Discover appliances send packet-forwarding rules to devices.

C Packets are forwarded over a UDP port range.

The ExtraHop implementation of RPCAP operates in active mode, which means that devices installed with rpcapd software initiate a TCP connection to the Discover appliance over defined ports. After the TCP connection is established, the Discover appliance responds with packet-forwarding rules that identify the allowed traffic. When the allowed traffic is detected on the monitored rpcapd device, packets are forwarded to the Discover appliance over a designated UDP port range.

Each rpcap-installed device contains a configuration file (`rpcapd.ini`) with the IP addresses of the Discover appliances where traffic should be sent, and the TCP port over which the connection should be initiated.

Each Discover appliance must have an interface configured to monitor RPCAP traffic. In addition, your ExtraHop appliance must be configured with packet-forwarding rules that determine which packets are forwarded by the remote devices.

Configure RPCAP on the Discover appliance

When you configure your Discover appliance to receive RPCAP traffic, your overall system capacity to process wire data is reduced. In some network environments, you might need to dedicate an additional Discover appliance to only accept RPCAP traffic. 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.

Note: When configuring multiple L3 interfaces on the Discover appliance, make sure that the interface networks do not overlap.

1. Log into the Admin UI of the Discover 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 only has interface 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.
6. Click **Save**.

Configure packet-forwarding rules on the Discover 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 Discover 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 Discover appliance is ready to receive the forwarded packets.

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

Installing rpcapd on your remote devices

You can access preformatted, up-to-date download and installation commands through `https://<extrahop_management_ip>/tools`, where *<extrahop_management_ip>* is the IP address of your Discover appliance. Information is provided for Linux distributions and Windows.

Important: These options should not be modified without an understanding of how the change might affect your workflow.

When you run the installation command, rpcapd automatically starts and initiates communication to the IP address and destination port specified in the command. For example, on a Linux device, where 172.18.10.25 is the IP address of the Discover appliance and the TCP port is 2003, the installation command is `sudo ./install.sh -k 172.18.10.25 2003`.

Running the install command creates a configuration file (`rpcapd.ini`) with an ActiveClient entry that defines the IP address and destination port of the Discover appliance, such as `ActiveClient = 10.0.0.100,2003`. The configuration file can be modified to change the Discover appliance information or to further filter the traffic that is sent to the Discover appliance. In addition, you can create multiple ActiveClient entries for multiple Discover appliances if your environment requires high availability.

The standard Linux startup script (`/etc/init.d/rpcap`) calls rpcapd with the following options:

-v

Runs rpcap in active mode only instead of both active and passive modes.

-d

Runs rpcap as a daemon (in Linux) or as a service (in Windows).

-L

Sends log messages to a syslog server.

Install and start rpcapd on a Linux device

Before you begin
The minimum Linux kernel version required to run rpcapd is 2.6.32.

1. In a web browser, navigate to `https://<extrahop_management_ip>/tools`, where the *<extrahop_management_ip>* is the IP address of your Discover appliance.
2. Follow the installation instructions to download the package for the Linux distribution of your device. (Optionally, you can view instructions for Generic/Other Linux and then copy and paste the commands to download and install rpcapd.)
3. Copy and paste the commands to install and start rpcapd. The command will be similar to the following example: `sudo ./install.sh -k 172.18.10.25 2003`, where 172.18.10.25 is the IP address of your Discover appliance and 2003 is the TCP port you want to communicate through.

All traffic that matches the packet forwarding rules is sent to the configured IP address for the Discover appliance.

Configure rpcapd on a Linux device with multiple interfaces

For devices with multiple interfaces, rpcapd can be configured to forward packets by interface. You can also configure rpcapd to send traffic to multiple Discover appliances.

To edit the configuration file, complete the following steps.

1. After installing rpcapd, 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 = 10.0.0.100,2003NullAuthPermit = YES`.
2. Specify an interface to monitor by adding one of the following lines: `ifaddr=<interface_ip_addr>` or `ifname =<interface_name>`.

3. Send traffic to multiple Discover appliances or from multiple interfaces on your device by adding another ActiveClient entry:

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

or

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

where <*interface_name*> is the name of the interface from which you want to forward packets and <*interface_ip_address*> is the IP address of the interface from which the packets are forwarded. The <*interface_ip_address*> can be either an individual IP address, such as 10.10.1.100, or a CIDR specification that contains the IP address, such as 10.10.1.0/24

4. Save the configuration file.
5. Restart rpcapd by running the following command: `sudo /etc/init.d/rpcap restart`.

Example Linux configurations

The following example shows an interface in CIDR format.

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

The following example shows a configuration that forwards packets by interface name:

```
ActiveClient = 10.10.6.45, 2003, ifname=eth0
NullAuthPermit = YES
```

Install rpcapd on a Windows device with Powershell

Note: Windows RPCAP support requires 64-bit versions for Windows 7, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012 R2, and Windows Server 2016.

1. In a web browser, navigate to `https://<extrahop_management_ip>/tools`.
2. Download and unzip the rpcapd file for Windows.
3. Open PowerShell and navigate to the directory with the unzipped files.
4. Run the following command, where <*extrahop_rpcap_target_ip*> is the IP address of the Discover appliance where you want to forward packets to and <*extrahop_rpcapd_port*> is the port you the device should connect through: the following command: `./install-rpcapd.ps1 -InputDir . -RpcapIp <extrahop_rpcap_target_ip> -RpcapPort <extrahop_rpcapd_port>`

Configure rpcapd on a Windows device with multiple interfaces

For network devices with multiple interfaces, rpcapd can be configured to forward packets from multiple interfaces.

To edit the configuration file, complete the following steps.

1. After installing rpcapd, open the rpcapd configuration file (`C:\Program Files\rpcapd\rpcapd.ini`).The file contains text similar to the following: `ActiveClient = 10.0.0.100,2003NullAuthPermit = YES`.
2. Specify an interface to monitor by adding the following line: `ifaddr=<interface_ip_addr>` or `ifname=<interface_name>`.

3. Send traffic to multiple Discover appliances or from multiple interfaces on your device by adding another ActiveClient entry:

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

or

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

where <*interface_name*> is the name of the interface from which you want to forward packets and <*interface_ip_address*> is the IP address of the interface from which the packets are forwarded. The <*interface_ip_address*> can be either an individual IP address, such as 10.10.1.100, or a CIDR specification that contains the IP address, such as 10.10.1.0/24.

The <*interface_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}`.

4. Save the configuration file.
5. Restart rpcapd by running the following command:restart-service rpcapd

Example Windows configurations

The following example shows two interfaces in CIDR format.

```
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 example shows a configuration that forwards packets by 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
```

To reinstall rpcapd after changing the configuration file, run one of the following installation commands and replace –RpcapIp and –RpcapPort with the -KeepConfig flag to preserve the modified configuration file:

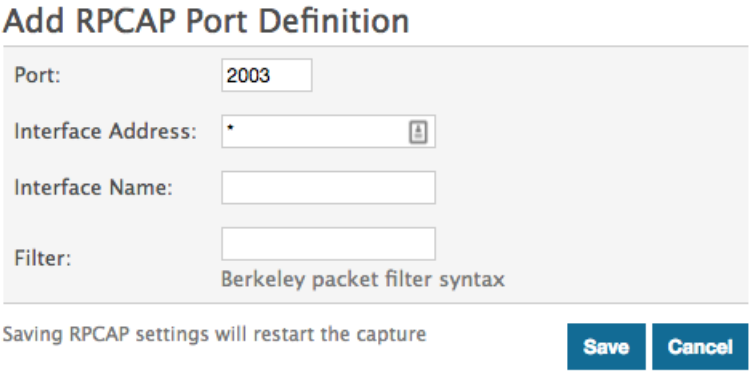
```
.\install-rpcapd.ps1 -MgmtIp <extrahop_management_ip> -KeepConfig
or
.\install-rpcapd.ps1 –InputDir . -KeepConfig
```

Sample RPCAP configuration

The following sample configurations illustrate how traffic rules apply to packet forwarding.

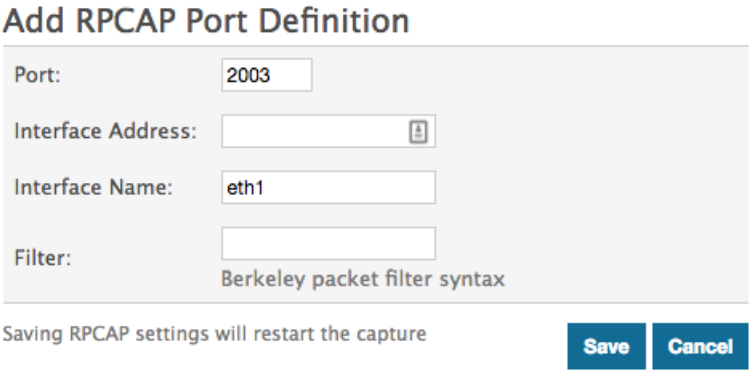
In all scenarios below, the ExtraHop Discover appliance (EDA) interface has a network configuration of 172.25.26.5, 172.25.26.0/24 and is configured for RPCAP, as displayed in the following figure.

Scenario 1: The Discover appliance is configured to accept all interface traffic, as displayed in the following figure.



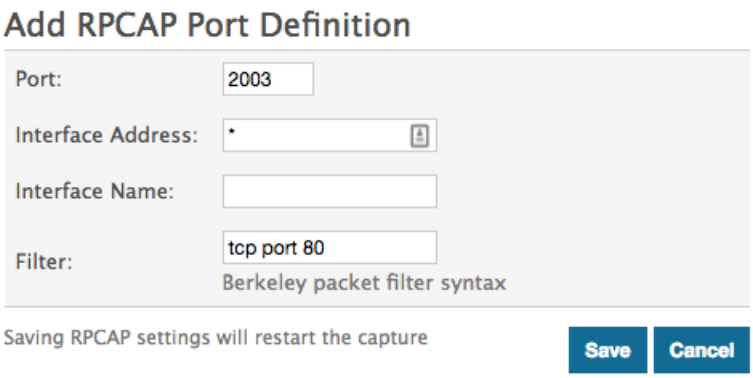
Client Network Configuration	RPCAP Configuration (rpcapd.ini)	Traffic Forwarded
`eth0 = 10.10.1.20, 10.10.1.0/24`	`ActiveClient=172.25.26.5, 2003`	All traffic on `eth0`.
`eth0 = 10.10.1.21 10.10.1.0/24` `eth1 = 192.168.4.21, 192.168.4.0/24`	`ActiveClient=172.25.26.5, 2003`	All traffic on `eth0`. No traffic from `eth1`.
`eth0 = 10.10.1.21, 10.10.1.0/24` `eth1 = 192.168.4.21, 192.168.4.0/24`	`ActiveClient=172.25.26.5, 2003, ifname=eth1`	All traffic on `eth1`. No traffic from `eth0`.
`eth0 = 10.10.1.21, 10.10.1.0/24` `eth1 = 192.168.4.21, 192.168.4.0/24`	`ActiveClient=172.25.26.5, 2003, ifname= eth0` `ActiveClient=172.25.26.5, 2003, ifname = eth1`	All traffic on both `eth0` and `eth1`.

Scenario 2: The Discover appliance is configured to accept traffic from only the device `eth1` interface, as displayed in the following figure.



Client Network Configuration	RPCAP Configuration (rpcapd.ini)	Traffic Forwarded
`eth0 = 10.10.1.20, 10.10.1.0/24`	`ActiveClient=172.25.26.5, 2003`	No traffic is forwarded.
`eth0 = 10.10.1.21, 10.10.1.0/24` `eth1 = 192.168.4.21, 192.168.4.0/24`	`ActiveClient=172.25.26.5, 2003`	No traffic is forwarded.
`eth0 = 10.10.1.21, 10.10.1.0/24` `eth1 = 192.168.4.21, 192.168.4.0/24`	`ActiveClient=172.25.26.5, 2003, ifname=eth1`	All traffic on `eth1`. No traffic from `eth0`.
`eth0 = 10.10.1.21, 10.10.1.0/24` `eth1 = 192.168.4.21, 192.168.4.0/24`	`ActiveClient=172.25.26.5, 2003, ifname= eth0` `ActiveClient=172.25.26.5, 2003, ifname = eth1`	All traffic on `eth1`. No traffic from `eth0`.

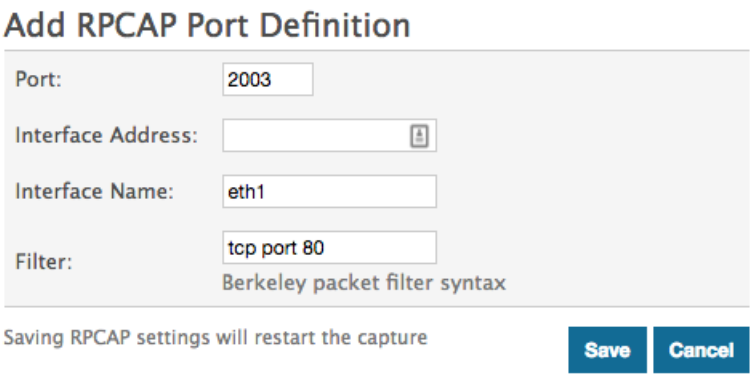
Scenario 3: The Discover appliance is configured to accept all interface traffic for TCP port 80, as displayed in the following figure.



Client Network Configuration	RPCAP Configuration (rpcapd.ini)	Traffic Forwarded
`eth0 = 10.10.1.20, 10.10.1.0/24`	`ActiveClient=172.25.26.5, 2003`	Only port 80 traffic on `eth0`.
`eth0 = 10.10.1.21, 10.10.1.0/24` `eth1 = 192.168.4.21, 192.168.4.0/24`	`ActiveClient=172.25.26.5, 2003`	Only port 80 traffic on `eth0`. No traffic from `eth1`.
`eth0 = 10.10.1.21, 10.10.1.0/24` `eth1 = 192.168.4.21, 192.168.4.0/24`	`ActiveClient=172.25.26.5, 2003, ifname=eth1`	Only port 80 traffic on `eth1`. No traffic from `eth0`.

Client Network Configuration	RPCAP Configuration (rpcapd.ini)	Traffic Forwarded
`eth0 = 10.10.1.21, 10.10.1.0/24` `eth1 = 192.168.4.21, 192.168.4.0/24`	`ActiveClient=172.25.26.5, 2003, ifname=eth0` `ActiveClient=172.25.26.5, 2003, ifname=eth1`	Only port 80 traffic on both `eth1` and `eth0`.

Scenario 2: The Discover appliance is configured to only accept TCP port 80 traffic from the `eth1` interface, as displayed in the following figure.



Client Network Configuration	RPCAP Configuration (rpcapd.ini)	Traffic Forwarded
`eth0 = 10.10.1.20, 10.10.1.0/24`	`ActiveClient=172.25.26.5, 2003`	No traffic is forwarded.
`eth0 = 10.10.1.21, 10.10.1.0/24` `eth1 = 192.168.4.21, 192.168.4.0/24`	`ActiveClient=172.25.26.5, 2003`	No traffic is forwarded.
`eth0 = 10.10.1.21, 10.10.1.0/24` `eth1 = 192.168.4.21, 192.168.4.0/24`	`ActiveClient=172.25.26.5, 2003, ifname=eth1`	Port 80 traffic on `eth1`. No traffic from `eth0`.
`eth0 = 10.10.1.21, 10.10.1.0/24` `eth1 = 192.168.4.21, 192.168.4.0/24`	`ActiveClient=172.25.26.5, 2003, ifname=eth0` `ActiveClient=172.25.26.5, 2003, ifname=eth1`	Only port 80 traffic on both `eth1` and `eth0`.

Opening ports on your firewall

RPCAP forwards packets over a range of UDP ports that are determined by the TCP ports configured in the Discover appliance and the model of your appliance.

Important: Opening four ports might be sufficient for most environments. However, we recommend that you open a full 32 ports to avoid losing traffic from your RPCAP-

installed devices. If opening 32 ports on your firewall is a concern, you can follow the guidelines in the table below. If you are not receiving all expected traffic, contact ExtraHop Support.

To determine the range of UDP ports that should be opened on your firewall, complete the following calculations:

- For the lower end of the UDP port range, take the lowest TCP port listed in the set of rules on the Discover appliance.
- For the higher end of the UDP range, take the lowest number and add the number associated with your ExtraHop appliance model, as listed in the following table.

ExtraHop Appliance	Number of Ports	Example Range
EDA 1000v	1	2003
EDA 2000v	4	2003-2006
EDA 6100v	8	2003-2010
EDA 3100	4	2003-2006
EDA 6100	8	2003-2010
EDA 8100	16	2003-2018
EDA 9100	32	2003-2034

For advanced users, you can also manually modify the lowest port of the UDP range through the following Running Configuration file setting: rpcap:udp_port_start.