Paketweiterleitung mit RPCAP

Veröffentlicht: 2024-08-09

Das ExtraHop-System generiert Metriken über Ihr Netzwerk und Ihre Anwendungen über einen kabelgebundenen Datenfeed, der normalerweise von einem Switch gespiegelt wird. Möglicherweise haben Sie jedoch nicht immer Zugriff auf einen Switch, oder Sie möchten möglicherweise ein bestimmtes Gerät überwachen, das sich außerhalb Ihres wire data Datennetzwerks befindet. Darüber hinaus können Sie in einer Cloud-Umgebung wie Microsoft Azure oder Amazon Web Services (AWS) nicht direkt auf Switch-Hardware zugreifen. Für diese Arten von Umgebungen können Sie Pakete an einen ExtraHop weiterleiten Sensor über eine Paketweiterleitung wie Remote Packet Capture (RPCAP).

Bevor Sie beginnen

- Sie müssen Erfahrung mit der Netzwerkadministration und der Installation von Dienstprogrammen auf Servern haben, um die Verfahren in diesem Handbuch ausführen zu können.
- WARNUNG: Beachten Sie die Datengebühren, die bei AWS und Azure anfallen. Beispielsweise können für mehrere AWS-VPC-Peers innerhalb einer Region zusätzliche Kosten anfallen. Informationen zur Preisgestaltung finden Sie in der AWS-Datenübertragung Seite und die Preise für Azure Bandwidth Seite.

Dieses Handbuch enthält Konzepte zur ExtraHop RPCAP-Implementierung sowie Anweisungen für alle erforderlichen Verfahren. Hier sind einige bewährte Methoden, die Sie vor der Bereitstellung von RPCAP berücksichtigen sollten:

- Um optimale Ergebnisse zu erzielen, beginnen Sie mit der Bereitstellung einiger RPCAP-Sender und bewerten Sie die Auswirkungen auf Ihre Umgebung. Überwachen Sie beim Hinzufügen von Absendern zur Bereitstellung die CPU-Auslastung auf Ihren RPCAP-überwachten Systemen, da der CPU- und Speicheraufwand mit der Anzahl der Absender korreliert, die Pakete an dasselbe senden Sensor.
- Beschränken Sie die Anzahl der RPCAP-Sender, die Pakete an das ExtraHop-System senden. Insbesondere empfehlen wir, weniger als 400 RPCAP-Sender pro Sensor. Wenn RPCAP Pakete an beide sendet Sensor und einen Packetstore, wir empfehlen, 200 Absender oder weniger zu konfigurieren. Diese Empfehlungen basieren auf unseren internen Laborergebnissen. Ihre Erfahrung kann je nach Komplexität Ihrer Konfiguration oder Umgebung variieren.
- Wenn Ihr ExtraHop-System Packetstore enthält, können Sie konfigurieren Sie einen zweiten Feed mit Paketen von Ihrer Remote-Umgebung zum Packetstore.

Überblick über die Bereitstellung

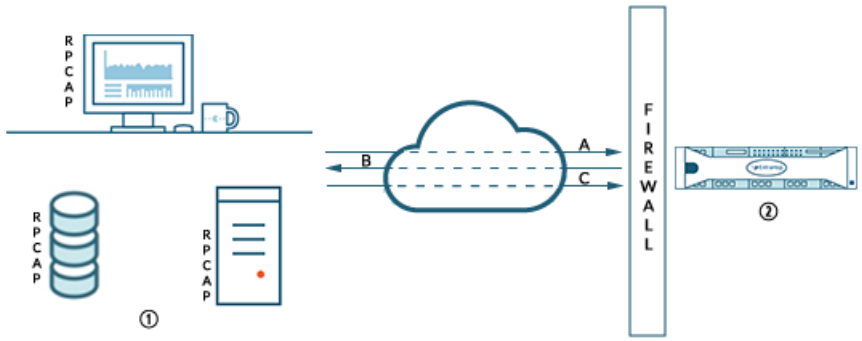
In den folgenden Schritten werden die wichtigsten Verfahren beschrieben, die für die Implementierung von RPCAP mit einem ExtraHop erforderlich sind. Sensor.

1. Zuerst den Sensor so konfigurieren, dass er RPCAP-Verkehr akzeptiert und Regeln für die Paketweiterleitung hinzufügen.
2. Als Nächstes laden Sie die rpcapd-Software herunter für Ihr Betriebssystem von der ExtraHop Downloads und Ressourcen Webseite.
3. Wenn Ihre Umgebung über eine Firewall verfügt, öffne Ports auf deiner Firewall für den erforderlichen RPCAP-Verkehr.
4. Installieren Sie abschließend die rpcapd-Software auf jedem Linux und Windows Gerät, von dem Sie den Verkehr weiterleiten möchten. Sie müssen die Konfigurationsdatei (rpcapd.ini) ändern, um Geräteschnittstellen anzugeben oder den Verkehr an den Sensor weiterzuleiten.
5. Wenn Sie einen ExtraHop-Packetstore haben, müssen Sie konfiguriere es so, dass es RPCAP-Verkehr akzeptiert, fügen Sie Regeln für die Paketweiterleitung hinzu und aktualisieren Sie Ihre Dateien rpcapd.ini, um den Datenverkehr sowohl an Sensoren als auch an Paketspeicher weiterzuleiten.

Implementierung von RPCAP mit dem ExtraHop-System

RPCAP wird durch eine kleine Binärdatei implementiert, die als Daemon (rpcapd) auf jedem Gerät läuft, für das Sie den Verkehr überwachen möchten.

Das RPCAP-Installationspaket für Windows oder Linux kann heruntergeladen werden von ExtraHop Downloads und Ressourcen Webseite. Die folgende Abbildung zeigt eine einfache RPCAP-Implementierung mit einem einzelnen Sensor hinter einer Firewall. Ihre Netzwerkkonfiguration kann variieren.



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.

Die ExtraHop-Implementierung von RPCAP arbeitet im aktiven Modus, was bedeutet, dass Geräte, auf denen die rpcapd-Software installiert ist, über definierte Ports eine TCP-Verbindung zum ExtraHop-System aufbauen. Nachdem die TCP-Verbindung hergestellt wurde, antwortet das ExtraHop-System mit Paketweiterleitungsregeln, die den erlaubten Verkehr identifizieren. Wenn der zulässige Verkehr auf dem überwachten rpcapd-Gerät erkannt wird, werden Pakete über einen bestimmten UDP-Portbereich an das ExtraHop-System weitergeleitet.

Jedes mit rpcap installierte Gerät enthält eine Konfigurationsdatei (`rpcapd.ini`) mit den IP-Adressen der Sensoren, an die der Verkehr gesendet werden soll, und dem TCP-Port, über den die Verbindung initiiert werden soll.

Jedes ExtraHop-System muss über eine Schnittstelle verfügen, die zur Überwachung des RPCAP-Datenverkehrs konfiguriert ist. Darüber hinaus muss Ihr ExtraHop-System mit Paketweiterleitungsregeln konfiguriert sein, die festlegen, welche Pakete von den Remote-Geräten weitergeleitet werden.

Wichtig: Jede Schnittstelle, die den RPCAP-Verkehr überwacht, kann maximal 1 Gbit/s verarbeiten.

RPCAP auf dem ExtraHop-System konfigurieren

Es wird empfohlen, eine zweite Schnittstelle nur für RPCAP zu konfigurieren, anstatt sowohl RPCAP als auch Management auf derselben Schnittstelle zu konfigurieren. Die Konfiguration einer dedizierten RPCAP-Schnittstelle erhöht die Wahrscheinlichkeit, dass alle Pakete erfolgreich an das ExtraHop-System weitergeleitet werden.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerk-Einstellungen Abschnitt, klicken **Konnektivität**.

3. Wählen Sie Schnittstelle 1, 2, 3 oder 4.
   Der ETA 1150v hat nur die Schnittstellen 1 und 2.
4. Aus dem Schnittstellenmodus Drop-down-Liste, wählen **Geschäftsleitung + RPCAP/ERSPAN/VXLAN/GENEVE Target**.
5. Konfigurieren Sie IPv4-Adressen für die Schnittstelle, indem Sie eine der folgenden Optionen wählen:
   - Geben Sie eine statische IPv4-Adresse in der **IPv4-Adresse** Feld, und geben Sie dann eine Netzmaske und eine Gateway-IP-Adresse IP-Adresse.
   - Aktivieren Sie dynamische IPv4-Adressen, indem Sie auf **DHCPv4 aktivieren**.

   Hinweis: Sie können zwar IPv6-Adressen auf der Schnittstelle aktivieren, aber Sie können RPCAP-Pakete nicht über IPv6 weiterleiten. Sie müssen eine IPv4-Adresse auf der Schnittstelle konfigurieren, um RPCAP zu aktivieren. Weitere Informationen zur Konfiguration einer Management + Capture-Schnittstelle finden Sie in Häufig gestellte Fragen zu ExtraHop Hardware.
6. klicken **Speichern**.

Regeln für die Paketweiterleitung auf dem ExtraHop-System konfigurieren

Nachdem Sie die Schnittstelle als RPCAP-Ziel konfiguriert haben, müssen Sie Regeln für die Paketweiterleitung konfigurieren. Die Regeln für die Paketweiterleitung schränken ein, welcher Datenverkehr über RPCAP an das ExtraHop-System gesendet werden darf.

Standardmäßig ist ein Eintrag für Port 2003 konfiguriert, der Datenverkehr von allen Schnittstellenadressen akzeptiert. Sie können den Standardeintrag für Ihre Umgebung ändern, den Standardeintrag löschen und weitere Einträge hinzufügen. Stellen Sie sicher, dass Sie Portnummern über 1023 angeben, um Konflikte mit reservierten Ports zu vermeiden. Es empfiehlt sich, diese Regeln zuerst festzulegen, damit das ExtraHop-System bereit ist, die weitergeleiteten Pakete zu empfangen, wenn Sie rpcapd auf Ihren Remote-Geräten konfigurieren.

Sie können bis zu 16 Regeln für die Paketweiterleitung im ExtraHop-System konfigurieren. Jede Regel muss einen einzigen TCP-Port haben, über den das ExtraHop-System die Paketweiterleitungsregeln an rpcapd-Geräte kommuniziert.

Wichtig: Die Informationen in der rpcapd-Konfigurationsdatei auf den Geräten , die Pakete weiterleiten, dürfen nicht den im ExtraHop-System festgelegten Regeln widersprechen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerk-Einstellungen Abschnitt, klicken **Konnektivität**.
3. In der RPCAP-Einstellungen Abschnitt, führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf **2003** um den Standardeintrag zu öffnen.
   - klicken **Hinzufügen** um einen neuen Eintrag hinzuzufügen.

     Wichtig: Die Portnummern müssen 1024 oder höher sein.
4. In der RPCAP-Portdefinition hinzufügen Geben Sie im Abschnitt die folgenden Informationen ein:
   a) In der Hafen Feld, geben Sie den TCP-Port ein, der Informationen zu dieser Paketweiterleitungsregel übermittelt. Porteinträge müssen für jedes Schnittstellensubnetz auf demselben Server eindeutig sein.
   b) In der Schnittstellenadresse Feld, geben Sie die IP-Adresse oder den CIDR-Bereich der Schnittstelle auf dem Gerät ein, von dem das ExtraHop-System Datenverkehr empfangen soll. Beispielsweise leitet 10.10.0.0/24 den gesamten Datenverkehr auf dem System weiter, der Teil dieses CIDR-Bereichs ist, * ist ein Platzhalter, der dem gesamten Datenverkehr auf dem System entspricht, oder 10.10.0.5 sendet nur Verkehr auf der Schnittstelle, die der 10.10.0.5-IP-Adresse entspricht.

Hinweis: Wenn eine Maschine über mehrere Schnittstellen verfügt und Sie in den Verkehrsregeln oder in der Datei rpcapd.ini keine Schnittstelle angeben, wählt das ExtraHop-System eine einzige Schnittstelle aus, von der der Datenverkehr weitergeleitet wird. Das ExtraHop-System wählt normalerweise die Schnittstelle mit dem Namen aus, der alphabetisch an erster Stelle steht. Wir empfehlen jedoch, dass Sie die Schnittstelle in den Verkehrsregeln angeben, um ein konsistentes Verhalten sicherzustellen. Wir empfehlen außerdem, die Schnittstelle nach Adresse und nicht nach Namen auszuwählen.

c) In der Name der Schnittstelle Feld, geben Sie den Namen der Schnittstelle auf dem Gerät ein, die den Datenverkehr an das ExtraHop-System sendet. Zum Beispiel `eth0` in einer Linux-Umgebung oder `\Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}` in einer Windows-Umgebung.

d) In der Filter Feld, geben Sie die Ports für den Verkehr, den Sie an das ExtraHop-System weiterleiten möchten, in der Berkeley Packet Filter (BPF) -Syntax ein. Sie können beispielsweise eingeben `TCP-Anschluss 80` um den gesamten Verkehr auf TCP-Port 80 von Ihrem Remote-Netzwerkgerät an das ExtraHop-System weiterzuleiten. Weitere Hinweise zur BPF-Syntax finden Sie unter Pakete mit der Berkeley-Paketfilter-Syntax filtern.

5. klicken **Speichern**, wodurch die Einstellungen gespeichert und die Erfassung neu gestartet werden.
6. Wiederholen Sie diese Schritte, um zusätzliche Regeln zu konfigurieren. Sie können bis zu 16 Regeln hinzufügen.

Speichern Sie die laufende Konfigurationsdatei

Nachdem Sie die Schnittstelle konfiguriert und die Regeln für die Paketweiterleitung konfiguriert haben, müssen Sie die Änderungen in der laufenden Konfigurationsdatei speichern.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerk-Einstellungen Abschnitt, klicken **Konnektivität**.
3. klicken **Änderungen ansehen und speichern**.
4. Überprüfen Sie die Änderungen in der Aktuelle laufende Konfiguration (noch nicht gespeichert) Fensterscheibe.
5. klicken **Speichern**.
6. klicken **Erledigt**.

Installation von rpcapd auf Ihren Remote-Geräten

Sie können die rpcapd-Installation anpassen, indem Sie die folgenden Konfigurationsoptionen angeben.

Wichtig: Diese Optionen sollten nicht geändert werden, ohne zu wissen, wie sich die Änderung auf Ihren Arbeitsablauf auswirken könnte.

Wenn Sie den Installationsbefehl ausführen, startet rpcapd automatisch und initiiert die Kommunikation mit der im Befehl angegebenen IP-Adresse und dem Zielport. Zum Beispiel auf einem Linux-Gerät, wo 172.18.10.25 die IP-Adresse des Sensor und der TCP-Port ist 2003, der Installationsbefehl ist `sudo ./install.sh -k 172.18.10.25 2003`.

Durch Ausführen des Installationsbefehls wird eine Konfigurationsdatei erstellt (`rpcapd.ini`) mit einem ActiveClient-Eintrag, der die IP-Adresse und den Zielport des Sensor definiert, wie `ActiveClient = 10.0.0.100,2003`. Der Eintrag kann auch den Namen der Schnittstelle angeben, von der der Datenverkehr weitergeleitet werden soll. Wenn nicht angegeben, leitet der Eintrag den Datenverkehr von eth0 weiter. Wir empfehlen, keinen Datenverkehr von einer Schnittstelle weiterzuleiten, die auch den Netzwerkverkehr erfasst, um Leistungseinbußen zu vermeiden. Wenn beispielsweise die Schnittstelle zwischen dem RPCAP-Peer und dem Sensor 1 Gbit/s beträgt und der RPCAP-Peer sowohl

den Datenverkehr von dieser Schnittstelle erfasst als auch weiterleitet, kann RPCAP nur 500 Mbit/s weiterleiten, da die anderen 500 Mbit/s für die Erfassung des eingehenden Netzwerkverkehrs verbraucht werden.

Wenn Sie den Datenverkehr von mehreren Schnittstellen weiterleiten möchten, müssen Sie mehrere angeben `ActiveClient` Werte in der Datei rpcapd.ini. Es wird empfohlen, die Schnittstellennamen explizit anzugeben. Die folgende Konfiguration leitet beispielsweise den Datenverkehr von beiden weiter `eth0` und `eth1`:

```
ActiveClient=172.25.26.5, 2003, ifname=eth0
ActiveClient=172.25.26.5, 2003, ifname=eth1
```

Standardskript

Das Standard-Startskript (`/etc/init.d/rpcapd`) ruft rpcapd mit den folgenden Optionen auf:

`-v`
: Führt rpcap nur im aktiven Modus aus, anstatt sowohl im aktiven als auch im passiven Modus.

`-d`
: Führt rpcap als Daemon (unter Linux) oder als Dienst (in Windows) aus.

`-L`
: Sendet Protokollnachrichten an einen Syslog-Server.

Skriptfilter

Ändern Sie das Startskript, um den Datenverkehr zu verfeinern, der an die Sensor.

`-F`
: Geben Sie einen lokalen Filter in BPF-Syntax an, der mit allen RPCAP-Filtern kombiniert wird, die auf Ihrem Sensor durch den AND-Operator. Während Standard-BPF-Standardausdrücke unterstützt werden, unterstützt RPCAP zusätzlich die folgenden Qualifizierer.

`hatype <num>`
: Filtern Sie nach dem Hardwaretyp. Setzen Sie diesen Wert beispielsweise auf `1` für Ethernet oder zu `772` für Loopback. Eine vollständige Liste der Hardwaretypen finden Sie in den ARPHRD_*-Konstanten in der Linux-Header-Datei if_arp.h.

`-i <interface>`
: Geben Sie eine Schnittstelle für den RPCAP-Verkehr an.

`-i any-eth`
: Erfasst jede Ethernet-Schnittstelle und behält das erforderliche Ethernet-Framing bei. (Nur Linux).

`ifidx <num>`
: Filtert nach dem Schnittstellenindex. (Nur Linux).

`ifn <name>`
: Filtern Sie nach dem Schnittstellennamen. Zum Beispiel `not ifn eth0` schließt alle Pakete auf eth0 von der Erfassung aus.

Debian-Ubuntu-Linux-Distributionen

Bevor Sie beginnen
Auf dem Server muss eine der folgenden Linux-Distributionen ausgeführt werden:

- `Ubuntu 18.04`
- `Ubuntu 20.04`
- `Ubuntu 22.04`

Die folgenden Pakete müssen auf dem Server installiert sein:

- `debconf`
- `libc6`
- `libcap-ng`
- `libcrypt1`

> **Hinweis:** Das `libcrypt1` Paket ist nur erforderlich für `Ubuntu 20.04` und später.

1. Loggen Sie sich auf Ihrem Debian- oder Ubuntu-Linux-Server ein.
2. Herunterladen die neueste Version der RPCAP-Forwarder-Software .
3. Öffnen Sie eine Terminal-Anwendung und führen Sie den folgenden Befehl aus.

```
sudo dpkg --install <path to installer file>
```

4. Geben Sie die IP-Adresse des ExtraHop ein Sensor Sie leiten den Verkehr weiter an und drücken Sie dann die EINGABETASTE.
5. Drücken Sie die EINGABETASTE, um die Standard-Portkonfiguration von 2003 zu akzeptieren.
6. Wenn Sie keine zusätzlichen Argumente konfigurieren, lassen Sie das Feld leer und drücken Sie dann die EINGABETASTE.
7. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass RPCAP korrekt konfiguriert ist:

```
sudo service rpcapd status
```

Wenn Sie eine der Konfigurationsoptionen ändern müssen, führen Sie den folgenden Befehl aus und wiederholen Sie die obigen Verfahren:

```
sudo dpkg-reconfigure rpcapd
```

RPM-basierte Linux-Distributionen

Bevor Sie beginnen
Auf dem Server muss eine der folgenden Linux-Distributionen ausgeführt werden:

- `CentOS 6`
- `CentOS 7`
- `CentOS 8`
- `CentOS 9`
- `RHEL 6`
- `RHEL 7`
- `RHEL 8`
- `RHEL 9`
- `Amazon Linux 2`

Die folgenden Pakete müssen auf dem Server installiert sein:

- chkconfig
- Initskripte
- Glibc
- libcap-ng
- libxcrypt

> **Hinweis:** Das `libxcrypt` Paket ist nur für CentOS 8, CentOS 9, RHEL 8, RHEL 9 und Amazon Linux 2 erforderlich.

1. Melden Sie sich bei Ihrem RPM-basierten Linux-Server an.

2. Herunterladen die neueste Version der RPCAP-Forwarder-Software.
3. Öffnen Sie eine Terminal-Anwendung und führen Sie den folgenden Befehl aus:

```
sudo rpm --install <path to installer file>
```

4. Öffnen Sie das Initialisierungsskript in einem Texteditor (z. B. vi oder vim).

```
sudo vi /opt/extrahop/etc/rpcapd.ini
```

5. Löschen Sie das Hash-Symbol aus dem `ActiveClient` Linie.
6. Ersetzen `<TARGETIP>` mit der IP-Adresse des Sensor, an den Sie den Verkehr weiterleiten.
7. Ersetzen `<TARGETPORT>` mit `2003`.
Der Inhalt der Datei rpcapd.ini sollte dem folgenden Beispiel ähneln:

```
ActiveClient = 10.10.115.216,2003
NullAuthPermit = YES
UserName = rpcapd
```

Hinweis Ändern Sie nicht die `NullAuthPermit` oder `UserName` Felder.

8. Speichern und schließen Sie die Datei.
9. Geben Sie den folgenden Befehl ein, um den rpcapd-Dienst zu starten:

```
sudo /etc/init.d/rpcapd start
```

Andere Linux-Distributionen

1. Loggen Sie sich auf Ihrem Linux-Server ein.
2. Herunterladen die neueste Version der RPCAP-Forwarder-Software.
3. Öffnen Sie eine Terminal-Anwendung und führen Sie den folgenden Befehl aus, um das Installationsskript aus der Datei zu extrahieren:

```
tar xf rpcapd-8.0.5.3940.tar.gz
```

4. Wechseln Sie in das Verzeichnis rpcapd:

```
cd rpcapd
```

5. Führen Sie den folgenden Befehl aus, um den Forwarder zu installieren. Ersetzen `<ip address>` mit der IP-Adresse des Sensor, an den Sie den Traffic weiterleiten und ersetzen `<port>` mit `2003`:

```
sudo ./install.sh -k <ip address> <port>
```

Zum Beispiel `sudo ./install.sh -k 10.10.115.215 2003`

Konfiguriere rpcapd auf einem Linux-Gerät mit mehreren Schnittstellen

Für Geräte mit mehreren Schnittstellen kann rpcapd so konfiguriert werden, dass Pakete per Schnittstelle weitergeleitet werden.

Gehen Sie wie folgt vor, um die Konfigurationsdatei zu bearbeiten.

1. Öffnen Sie nach der Installation von rpcapd die rpcapd-Konfigurationsdatei (`/opt/extrahop/etc/rpcapd.ini`) in einem Texteditor. Die Konfigurationsdatei enthält Text, der dem folgenden Beispiel ähnelt:

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

```
UserName = rpcapd
```

Hinweis: Ändern Sie nicht die `NullAuthPermit` oder `UserName` Felder.

2. Geben Sie eine zu überwachende Schnittstelle an, indem Sie eine der folgenden Klauseln an die ActiveClient-Zeile anhängen: `ifaddr=<interface_ip_addr>` oder `ifname=<interface_name>`.
3. Verkehr an mehrere senden Sensoren oder von mehreren Schnittstellen auf Ihrem Gerät, indem Sie einen weiteren ActiveClient-Eintrag hinzufügen:

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

oder

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

woher *<interface_name>* ist der Name der Schnittstelle, von der Sie Pakete weiterleiten möchten und *<interface_ip_address>* ist die IP-Adresse der Schnittstelle, von der die Pakete weitergeleitet werden. Das *<interface_ip_address>* kann entweder eine einzelne IP-Adresse sein, z. B. 10.10.1.100, oder eine CIDR-Spezifikation, die die IP-Adresse enthält, z. B. 10.10.1.0/24

4. Speichern Sie die Konfigurationsdatei.
5. Starte rpcapd neu, indem du den folgenden Befehl ausführst: `sudo /etc/init.d/rpcapd restart`.

Beispiel für Linux-Konfigurationen

Das folgende Beispiel zeigt eine Schnittstelle im CIDR-Format.

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

Das folgende Beispiel zeigt eine Konfiguration, die Pakete nach Schnittstellennamen weiterleitet:

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

Deinstalliere die Software

Gehen Sie wie folgt vor, um die RPCAP-Software zu deinstallieren.

1. Melden Sie sich beim Linux-Server an.
2. Öffnen Sie eine Terminalanwendung und wählen Sie eine der folgenden Optionen, um die Software zu entfernen.
   - Führen Sie für RPM-basierte Server den folgenden Befehl aus:

     ```
     sudo rpm --erase rpcapd
     ```

   - Führen Sie für Debian- und Ubuntu-Server den folgenden Befehl aus:

     ```
     sudo apt-get --purge remove rpcapd
     ```

3. Typ Y wenn Sie aufgefordert werden, das Entfernen der Software zu bestätigen, und drücken Sie dann die EINGABETASTE.

Installieren Sie rpcapd auf einem Windows-Server

Installieren Sie rpcapd mit dem Installationsassistenten auf einem Windows-Server

Bevor Sie beginnen
Auf dem Server muss Windows 10, Windows 11 oder Windows Server 2016 oder höher ausgeführt werden.

1. Melden Sie sich auf dem Windows-Computer an, auf dem Sie RPCAP installieren möchten.
2. Laden Sie das Installationspaket für Windows Server aus dem ExtraHop herunter Downloads und Ressourcen Webseite.
3. Öffnen Sie eine Eingabeaufforderung mit dem **Als Administrator ausführen** Option.
4. Navigieren Sie zu dem Verzeichnis, in das Sie das Installationspaket heruntergeladen haben.
5. Führen Sie den folgenden Befehl aus:

   ```
   msiexec /i ExtraHopRemotePacketCapture-<version>.msi /lv
    ExtraHopRmotePacketCapture-install.log
   ```

   Der Installationsassistent wird geöffnet.
6. klicken **Als Nächstes**.
7. In der Zusätzliche Hop-IP In diesem Feld geben Sie die IP-Adresse des Sensor ein, an den Sie Pakete weiterleiten möchten.
8. In der ExtraHop-Anschluss In diesem Feld geben Sie die Nummer für den Port ein , über den Sie Pakete weiterleiten möchten. Der Standardport ist 2003.
9. klicken **Als Nächstes**.
10. klicken **Installieren**.
11. Klicken Sie nach Abschluss der Installation auf **Schliessen**.

Installieren Sie rpcapd auf einem Windows-Server mit der Kommandozeile

Bevor Sie beginnen
Auf dem Server muss Windows 10, Windows 11 oder Windows Server 2016 oder höher ausgeführt werden.

1. Melden Sie sich auf dem Windows-Computer an, auf dem Sie rpcapd installieren möchten.
2. Laden Sie das Installationspaket für Windows-Server von der ExtraHop-Webseite für Downloads und Ressourcen herunter.
3. Öffnen Sie eine Eingabeaufforderung mit dem **Als Administrator ausführen** Option.
4. Navigieren Sie zu dem Verzeichnis, in das Sie das Installationspaket heruntergeladen haben.
5. Führen Sie den folgenden Befehl aus und ersetzen Sie `YOUR_ADDRESS` mit der IP-Adresse des Sensor, an den Sie Pakete weiterleiten möchten:

   ```
   msiexec /i ExtraHopRemotePacketCapture-<version>.msi /qn /lv
    ExtraHopRmotePacketCapture-install.log RPCAP_IP="YOUR_ADDRESS"
   ```

   Weitere Informationen zu den rpcapd-Installationsoptionen finden Sie unter Parameter des Rpcapd-Installationsprogramms.

Konfiguriere rpcapd auf einem Windows-Gerät mit mehreren Schnittstellen

Für Netzwerkgeräte mit mehreren Schnittstellen kann rpcapd so konfiguriert werden, dass Pakete von mehreren Schnittstellen weitergeleitet werden.

Gehen Sie wie folgt vor, um die Konfigurationsdatei zu bearbeiten.

1. Aktivieren Sie nach der Installation von rpcapd die Schreibrechte für die rpcapd-Konfigurationsdatei.
   a) Klicken Sie mit der rechten Maustaste auf die Konfigurationsdatei (`C:\ProgramData\ExtraHop\rpcap\rpcapd.ini`).
   b) Klicken Sie **Eigenschaften**.
   c) Deaktivieren Sie das **Nur lesbar** Ankreuzfeld.
2. Öffnen Sie die Konfigurationsdatei. Die Datei enthält Text ähnlich dem folgenden:

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

   Hinweis: Ändern Sie nicht die `NullAuthPermit` oder `UserName` Felder.
3. Geben Sie eine zu überwachende Schnittstelle an, indem Sie die folgende Zeile hinzufügen: `ifaddr=<interface_ip_addr>` oder `ifname=<interface_name>`.
4. Senden Sie Traffic an mehrere ExtraHop-Systeme oder von mehreren Schnittstellen auf Ihrem Gerät, indem Sie einen weiteren ActiveClient-Eintrag hinzufügen:

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

   oder

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

   woher *<interface_name>* ist der Name der Schnittstelle, von der Sie Pakete weiterleiten möchten und *<interface_ip_address>* ist die IP-Adresse der Schnittstelle, von der die Pakete weitergeleitet werden. Das *<interface_ip_address>* kann entweder eine einzelne IP-Adresse sein, z. B. 10.10.1.100, oder eine CIDR-Spezifikation, die die IP-Adresse enthält, z. B. 10.10.1.0/24.

   Das *<interface_name>* ist formatiert als `\Device\NPF_{<GUID>}`, wo *<GUID>* ist der Globally Unique Identifier (GUID) der Schnittstelle. Wenn die Schnittstellen-GUID beispielsweise 2C2FC212-701D-42E6-9EAE-BEE969FEFB3F lautet, lautet der Schnittstellenname `\Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}`.
5. Speichern Sie die Konfigurationsdatei.
6. Starte rpcapd neu, indem du den folgenden Befehl ausführst:

```
start-service ExtraHopRpcapd
```

Parameter des Rpcapd-Installationsprogramms

Sie können die folgenden Parameter angeben, wenn Sie das rpcapd-Installationsprogramm ausführen.

`RPCAP_IP:` ***Schnur***

Die IP-Adresse des Sensor, an den Sie Pakete weiterleiten möchten. Dieser Parameter ist erforderlich.

`RPCAP_PORT:` ***Schnur***

Der Port auf dem Windows-Server, über den Sie Pakete weiterleiten möchten.

`RPCAP_OPTSVCPARAMS:` ***Schnur***

Filteroptionen für rpcapd. Beispielsweise spezifiziert der folgende Befehl einen BPF-Filter für Pakete an oder von der IP-Adresse 10.10.10.10:

```
RPCAP_OPTSVCPARAMS="-F host 10.10.10.10"
```

Weitere Hinweise zu rpcapd-Optionen finden Sie unter Skriptfilter.

Das rpcapd-Installationsprogramm unterstützt auch die Befehlszeilenoptionen von Microsoft Standard Installer. Eine vollständige Liste der Optionen finden Sie in der Microsoft-Dokumentationswebsite.

Hinweis: Wenn Sie die angeben `/passive` oder `/qn` Optionen, die Microsoft C- und C++ (MSVC) - Laufzeitbibliotheken müssen auf dem Server installiert sein, bevor Sie rpcapd installieren. Sie können die Bibliotheken installieren, indem Sie das Visual C++ Redistributable-Paket von der Microsoft-Dokumentationswebsite. Laden Sie das Paket für Visual Studio 2015, 2017, 2019 und 2022 mit x64-Architektur herunter.

Beispiel für Windows-Konfigurationen

Das folgende Beispiel zeigt zwei Schnittstellen im 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
UserName = rpcapd
```

Das folgende Beispiel zeigt eine Konfiguration, die Pakete nach Schnittstellennamen weiterleitet.

```
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
UserName = rpcapd
```

Deinstalliere die Software

Gehen Sie wie folgt vor, um die RPCAP-Software über das Bedienfeld „Windows-Programme“ zu deinstallieren.

1. Melden Sie sich bei dem Windows-Computer an, auf dem die RPCAP-Software installiert ist.
2. Öffnen Sie das Control Panel und klicken Sie auf **Programm deinstallieren**.
3. Wählen **RPCAP-Dienst für Windows** in der Liste und dann klicken **Deinstallieren/Ändern**.
4. klicken **entfernen**.
5. Nachdem die Software entfernt wurde, klicken Sie auf **Schliessen**.

Überprüfen Sie Ihren RPCAP-Verkehr

Nachdem Ihre Konfiguration abgeschlossen ist, können Sie RPCAP-Pakete und Durchsatzmetriken auf der Seite Systemstatus einsehen, um zu überprüfen, ob der richtige Datenverkehr an das ExtraHop-System weitergeleitet wird.

Erfahre mehr über Systemintegritäts-Dashboard.

Weitergeleitet von Peer

Ein Listendiagramm, das die folgenden Informationen zu Paketen und Frames anzeigt, die von einem RPCAP-Peer weitergeleitet werden:

Weitergeleitete Pakete

Die Anzahl der Pakete, die ein RPCAP-Peer versucht hat, an ein ExtraHop-System weiterzuleiten.

Forwarder-Schnittstellenpakete

Die Gesamtzahl der Pakete, die vom Forwarder angesehen wurden. Forwarder auf RPCAP-Geräten koordinieren sich miteinander, um zu verhindern, dass mehrere Geräte dasselbe Paket senden. Dies ist die Anzahl der Pakete, die angesehen wurden, bevor Frames entfernt wurden, um den weitergeleiteten Verkehr zu reduzieren, und bevor Frames durch benutzerdefinierte Filter entfernt wurden.

Forwarder-Kernel-Frame-Drops

Die Anzahl der Frames, die gelöscht wurden, weil der Kernel des RPCAP-Peers mit dem Stream ungefilterter Frames überlastet war. Ungefilterte Frames wurden vom Kernel nicht gefiltert, um doppelte Pakete oder Pakete zu entfernen, die aufgrund benutzerdefinierter Regeln nicht weitergeleitet werden sollten.

Die Forwarder-Schnittstelle wird unterbrochen

Die Anzahl der Pakete, die verworfen wurden, weil der RPCAP-Forwarder mit dem Stream ungefilterter Frames überlastet war. Ungefilterte Frames wurden nicht gefiltert, um doppelte Pakete oder Pakete zu entfernen, die aufgrund benutzerdefinierter Regeln nicht weitergeleitet werden sollten.

Wie diese Informationen Ihnen helfen können

Jedes Mal, wenn Sie Pakete sehen, die vom RPCAP-Peer verworfen wurden, deutet dies darauf hin, dass ein Problem mit der RPCAP-Software vorliegt.

Vom ExtraHop-System empfangen

Ein Listendiagramm, das die folgenden Informationen zu Paketen und Frames anzeigt, die von einem ExtraHop-System von einem Remote Packet Capture (RPCAP) -Peer empfangen werden:

Gekapselte Bytes

Die Gesamtgröße aller Pakete, die sich auf den UDP-Fluss vom RPCAP-Gerät zum ExtraHop-System beziehen, in Byte. Diese Information zeigt Ihnen, wie viel Traffic der RPCAP-Forwarder Ihrem Netzwerk hinzufügt.

Gekapselte Pakete

Die Anzahl der Pakete, die sich auf den UDP-Fluss vom RPCAP-Gerät zum ExtraHop-System beziehen.

Tunnel-Bytes

Die Gesamtgröße der Pakete, ohne Kapselungsheader, die das ExtraHop-System von einem RPCAP-Gerät empfangen hat, in Byte.

Tunnel-Pakete

Die Anzahl der Pakete, die das ExtraHop-System von einem RPCAP-Peer empfangen hat. Diese Zahl sollte der Zahl der weitergeleiteten Pakete in der Tabelle Vom Remote-Gerät gesendet sehr ähnlich sein. Wenn zwischen diesen beiden Zahlen eine große Lücke besteht, fallen Pakete zwischen dem RPCAP-Gerät und dem ExtraHop-System ab.

Wie diese Informationen Ihnen helfen können

Die Verfolgung der gekapselten Pakete und Bytes ist eine gute Methode, um sicherzustellen, dass RPCAP-Forwarder Ihr Netzwerk nicht unnötig belasten. Sie können Tunnelpakete und Bytes überwachen, um sicherzustellen, dass das ExtraHop-System alles empfängt, was das RPCAP-Gerät sendet.

Problembehebung

Wenn die Anzahl der weitergeleiteten Pakete nicht der Anzahl der Forwarder-Schnittstellenpakete entspricht, werden Pakete irgendwann im RPCAP-Prozess verworfen. Dies ist in der Regel auf eines der folgenden Probleme zurückzuführen:

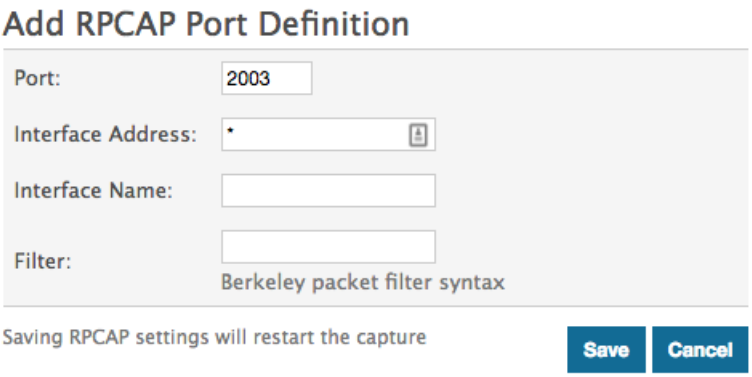
- Ein interner Prozess auf dem RPCAP-Peer ist überlastet.
  - Wenn es Forwarder Kernel Frame Drops gibt, ist der Kernel des RPCAP-Peers überlastet.
  - Wenn es Forwarder Interface Drops gibt, versucht der libpcap-Prozess des RPCAP-Peers, zu viele Pakete pro Sekunde zu senden, und der Prozess verbraucht wahrscheinlich fast 100% CPU-Auslastung auf einem einzelnen Kern.
  - Wenn die Metriken für verworfene Pakete den Unterschied zwischen den Forwarder Packets und den Forwarder Interface Packets nicht berücksichtigen, kann dies darauf hindeuten, dass der Thread auf dem RPCAP-Peer, der die Pakete sendet, überlastet ist.
- Die Netzwerkverbindung zwischen dem Peer und dem Sensor ist zu langsam.
  - Wenn die gekapselten Bytes gleich oder fast gleich der Geschwindigkeit der Netzwerkverbindung zwischen dem Sensor und dem Peer sind, ist die Verbindung wahrscheinlich nicht schnell genug.

Beispiel für eine RPCAP-Konfiguration

Die folgenden Beispielkonfigurationen veranschaulichen, wie Verkehrsregeln für die Paketweiterleitung gelten.

In allen unten aufgeführten Szenarien ist Sensor Die Schnittstelle hat eine Netzwerkkonfiguration von 172.25.26.5, 172.25.26.0/24 und ist für RPCAP konfiguriert, wie in der folgenden Abbildung dargestellt.

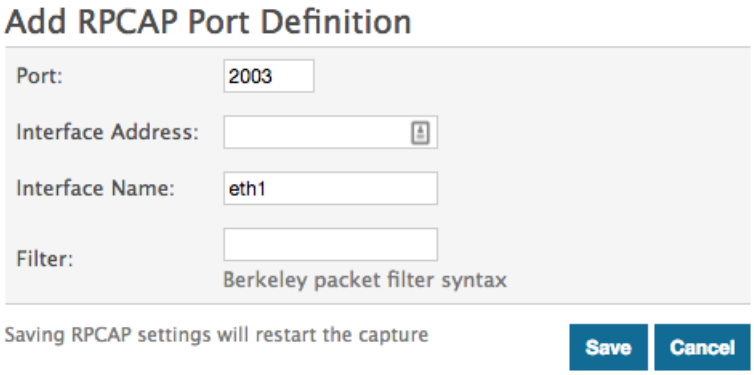
Szenario 1: Das Sensor ist so konfiguriert, dass er den gesamten Schnittstellenverkehr akzeptiert, wie in der folgenden Abbildung dargestellt.



Client-Netzwerkkonfiguration	RPCAP-Konfiguration (rpcapd.ini)	Weitergeleiteter Verkehr
`eth0 = 10.10.1.20, 10.10.1.0/24`	`ActiveClient=172.25.26.5, 2003`	Gesamter Verkehr auf `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`	Gesamter Verkehr auf `eth0`. Kein Verkehr von `eth1`.
`eth0 = 10.10.1.21, 10.10.1.0/24`	`ActiveClient=172.25.26.5, 2003, ifname=eth1`	Gesamter Verkehr auf `eth1`. Kein Verkehr von `eth0`.

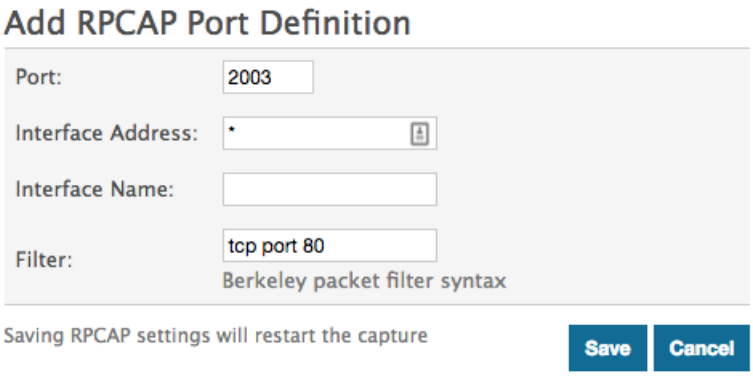
Client-Netzwerkkonfiguration	RPCAP-Konfiguration (rpcapd.ini)	Weitergeleiteter Verkehr
`eth1 = 192.168.4.21, 192.168.4.0/24`		
`eth0 = 10.10.1.21, 10.10.1.0/24` `eth1 = 192.168.4.21, 192.168.4.0/24`	`ActiveClient=172.25.26.5, 2003, ifname= eth0` `ActiveClient=172.25.26.5, 2003, ifname = eth1`	Der gesamte Verkehr auf beiden `eth0` und `eth1`.

Szenario 2: Das Sensor ist so konfiguriert, dass nur Datenverkehr vom Gerät akzeptiert wird `eth1` Schnittstelle, wie in der folgenden Abbildung dargestellt.



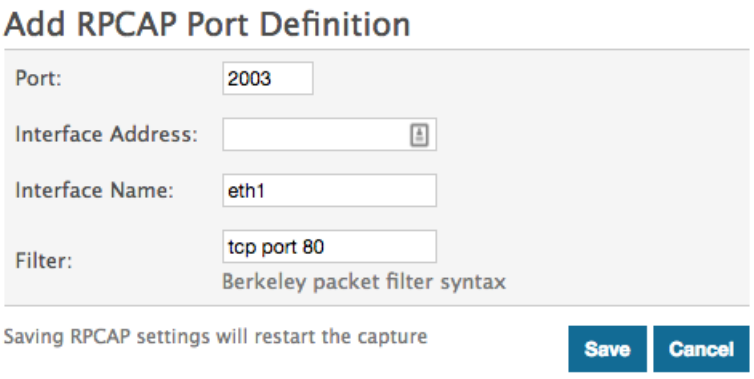
Client-Netzwerkkonfiguration	RPCAP-Konfiguration (rpcapd.ini)	Weitergeleiteter Verkehr
`eth0 = 10.10.1.20, 10.10.1.0/24`	`ActiveClient=172.25.26.5, 2003`	Es wird kein Verkehr weitergeleitet.
`eth0 = 10.10.1.21, 10.10.1.0/24` `eth1 = 192.168.4.21, 192.168.4.0/24`	`ActiveClient=172.25.26.5, 2003`	Gesamter Verkehr auf `eth1`. Kein Verkehr von `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=eth1`	Gesamter Verkehr auf `eth1`. Kein Verkehr von `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`	Gesamter Verkehr auf `eth1`. Kein Verkehr von `eth0`.

Szenario 3: Das Sensor ist so konfiguriert, dass er den gesamten Schnittstellenverkehr für TCP-Port 80 akzeptiert, wie in der folgenden Abbildung dargestellt.



Client-Netzwerkkonfiguration	RPCAP-Konfiguration (rpcapd.ini)	Weitergeleiteter Verkehr
`eth0 = 10.10.1.20, 10.10.1.0/24`	`ActiveClient=172.25.26.5, 2003`	Nur Port 80-Verkehr aktiviert `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`	Nur Port 80-Verkehr aktiviert `eth0`. Kein Verkehr von `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`	Nur Port 80-Verkehr aktiviert `eth1`. Kein Verkehr von `eth0`.
`eth0 = 10.10.1.21, 10.10.1.0/24`	`ActiveClient=172.25.26.5, 2003, ifname=eth0`	Nur Port 80-Verkehr aktiviert `eth0`.

Szenario 4: Das Sensor ist so konfiguriert, dass es nur TCP-Port 80-Verkehr vom akzeptiert `eth1` Schnittstelle, wie in der folgenden Abbildung dargestellt.



Client-Netzwerkkonfiguration	RPCAP-Konfiguration (rpcapd.ini)	Weitergeleiteter Verkehr
`eth0 = 10.10.1.20, 10.10.1.0/24`	`ActiveClient=172.25.26.5, 2003`	Es wird kein Verkehr weitergeleitet.

Client-Netzwerkkonfiguration	RPCAP-Konfiguration (rpcapd.ini)	Weitergeleiteter Verkehr
`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`	Port 80-Verkehr auf eth1. Kein Verkehr von 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=eth1`	Port 80-Verkehr an `eth1`. Kein Verkehr von `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`	Port 80-Verkehr an `eth1`. Kein Verkehr von `eth0`.

Ports auf Ihrer Firewall öffnen

RPCAP leitet Pakete über eine Reihe von UDP-Ports weiter, die durch die TCP-Ports bestimmt werden, die in der Sensor und Packetstore und das Modell Ihres Geräts.

Wichtig: Das Öffnen von vier Ports kann für die meisten Umgebungen ausreichend sein. Wir empfehlen jedoch, dass Sie volle 32 Ports öffnen, um zu vermeiden, dass der Datenverkehr Ihrer auf RPCAP installierten Geräte verloren geht. Wenn das Öffnen von 32 Ports an Ihrer Firewall ein Problem darstellt, können Sie die Richtlinien in der folgenden Tabelle befolgen. Wenn Sie nicht den gesamten erwarteten Traffic erhalten, wenden Sie sich an ExtraHop-Unterstützung.

Führen Sie die folgenden Berechnungen durch, um den Bereich der UDP-Ports zu ermitteln, der an Ihrer Firewall geöffnet werden sollte:

- Verwenden Sie für das untere Ende des UDP-Portbereichs den niedrigsten TCP-Port, der im Regelsatz auf der Sensor oder Packetstore.
- Nehmen Sie für das obere Ende des UDP-Bereichs die niedrigste Zahl und fügen Sie die Ihrem ExtraHop-Appliance-Modell zugeordnete Nummer hinzu, wie in der folgenden Tabelle aufgeführt.

ExtraHop-Gerät	Anzahl der Anschlüsse	Beispiel für einen Bereich
ETA 1150 v	1	2003
EDA 6100 v, ETA 6150, ETA 6150 v	8	2003-2010
VON 1020	72	2003-2074

Für fortgeschrittene Benutzer können Sie den niedrigsten Port des UDP-Bereichs auch manuell ändern, indem Sie `rpcap:udp_port_start` laufende Einstellung der Konfigurationsdatei.