Stellen Sie den ExtraHop EFC 1292v NetFlow Sensor bereit

Veröffentlicht: 2024-02-21

In diesem Handbuch wird erklärt, wie die virtuelle EFC 1292v NetFlow-Sensor-Appliance bereitgestellt wird.

Der EFC 1292v ist so konzipiert, dass er eine Verbindung zu Reveal (x) 360 und Reveal (x) Enterprise herstellt und NetFlow-Datensätze aus Ihrem Netzwerk erfasst. Eine Paketanalyse ist nicht verfügbar.

Voraussetzungen

Ihre Umgebung muss die folgenden Anforderungen erfüllen, um einen EFC 1292v-Sensor einsetzen zu können:

- Zugriff auf einen virtuellen Sensor (ExtraHop 1100v) auf Linux KVM oder VMWare
- Ein EFC 1292v-Produktschlüssel

Überblick über die Bereitstellung

Das Sammeln von NetFlow-Datensätzen erfordert die folgende Konfiguration.

- Stellen Sie eine ExtraHop-Sensorinstanz in Linux KVM oder VMware bereit. Weitere Informationen finden Sie unter Stellen Sie einen ExtraHop-Sensor auf Linux KVM bereit oder Stellen Sie den ExtraHop-Sensor mit VMware bereit.
- Schnittstellen konfigurieren.
- Konfigurieren Sie die NetFlow-Einstellungen auf dem ExtraHop-System.

Schnittstellen konfigurieren

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken Sie **Konnektivität**.
3. In der Schnittstellen Klicken Sie im Abschnitt auf den Namen der Schnittstelle, die Sie konfigurieren möchten.
4. Auf dem Netzwerkeinstellungen für die Schnittstelle *<interface number>* Seite, von der **Schnittstellenmodus** Drop-down-Liste, wählen **Management + Flow-Ziel**.
5. Deaktivieren Sie alle verbleibenden Schnittstellen, da der Sensor NetFlow- und wire data nicht gleichzeitig verarbeiten kann:
   a) In der Schnittstellen Klicken Sie im Abschnitt auf den Namen der Schnittstelle, die Sie konfigurieren möchten.
   b) Aus dem **Schnittstellenmodus** Drop-down-Liste, wählen **Deaktiviert**.
   c) Wiederholen Sie den Vorgang, bis alle zusätzlichen Schnittstellen deaktiviert sind.
6. Klicken Sie **Speichern**.

Configure NetFlow settings

You must configure port and network settings on the EFC 1292v NetFlow sensor before you can collect NetFlow records. The ExtraHop system supports the following flow technologies: Cisco NetFlow v5/v9 and IPFIX.

You must log in as a user with System and Access Administration privileges to complete the following steps.

Configure the flow type and UDP port

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 **NetFlow**.
3. In the Ports section, from the Port field, type the UDP port number.
   The default port for Net Flow is `2055`. You can add additional ports as needed for your environment.

   Note: Port numbers must be 1024 or greater
4. From the Flow Type drop-down menu, select **NetFlow**.
5. Click the plus icon (**+**) to add the port.

Add approved networks

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 **NetFlow**.
3. In the Approved Networks section, click **Add Approved Network**.
4. From the Flow Type drop-down menu, select **NetFlow**.
5. For IP address, type the IPv4 or IPv6 address.
6. For Network ID, type a name to identify this approved network.
7. Click **Save**.

Discover NetFlow devices

You can configure the ExtraHop system to discover NetFlow devices by adding a range of IP addresses.

Important considerations about Remote L3 Discovery:

- With NetFlow, devices that represent the gateways exporting records are automatically discovered. You can configure the ExtraHop system to discover devices that are representing the IP addresses observed in NetFlow records by adding a range of IP addresses.
- Exercise caution when specifying CIDR notation. A /24 subnet prefix might result in 255 new devices discovered by the ExtraHop system. A wide /16 subnet prefix might result in 65,535 new devices discovered, which might exceed your device limit.
- If an IP address is removed from the Device Discovery settings, the IP address will persist in the ExtraHop system as a remote L3 device as long as there are existing active flows for that IP address or until the capture is restarted. After a restart, the device is listed as an inactive remote L3 device.

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 **NetFlow**.
3. In the NetFlow Device Discovery section, type the IP address in the IP address ranges field.
   You can specify one IP address or a CIDR notation, such as `192.168.0.0/24` for an IPv4 network or `2001:db8::/32` for an IPv6 network.

   Important: Every actively-communicating remote IP address that matches the CIDR block will be discovered as a single device in the ExtraHop system. Specifying wide subnet prefixes such as /16 might result in thousands of discovered devices, which might exceed your device limit.
4. Click the green plus icon (**+**) to add the IP address.

Next steps

You can add another IP address or range of IP addresses by repeating steps 3-4.