Stellen Sie den ExtraHop EFC 1292v NetFlow Sensor bereit

Veröffentlicht: 2024-10-25

In diesem Handbuch wird erklärt, wie Sie den EFC 1292v NetFlow Virtual bereitstellen Sensor.

Der EFC 1292v wurde entwickelt, um eine Verbindung zu RevealX 360 und RevealX Enterprise herzustellen und NetFlow-Datensätze aus Ihrem Netzwerk zu sammeln. Eine Paketanalyse ist nicht verfügbar.

Anforderungen an das System

Ihre Umgebung muss die folgenden Anforderungen erfüllen, um einen virtuellen EFC 1292v-Sensor auf Linux KVM oder VMware vSphere bereitzustellen:

- Sie müssen mit der Verwaltung von Linux KVM oder VMware VMware vertraut sein.
- Sie benötigen die ExtraHop-Bereitstellungsdatei, die auf der ExtraHop Kundenportal.
- Sie müssen einen ExtraHop EFC 1292v haben Sensor Produktschlüssel.
- Sie sollten ein Upgrade auf den neuesten Patch für die Linux-KVM- oder vSphere-Umgebung durchführen, um bekannte Probleme zu vermeiden.

Anforderungen an virtuelle Maschinen

Sie müssen einen Hypervisor bereitstellen, der den folgenden Spezifikationen für den virtuellen Computer am ehesten entspricht Sensor.

Fühler	vCPUs	RAM	Festplatte
1100 V	4	8 GB	46 GB

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 auf 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 **Konnektivität**.
3. In der Schnittstellen Abschnitt, klicken Sie auf den Namen der Schnittstelle, die Sie konfigurieren möchten.
4. Auf dem Netzwerkeinstellungen für die Schnittstelle *<interface number>* Seite, von der **Schnittstellen-Modus** Drop-down-Menü, 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 Abschnitt, klicken Sie auf den Namen der Schnittstelle, die Sie konfigurieren möchten.
b) Aus dem **Schnittstellen-Modus** Drop-down-Menü, wählen **Deaktiviert**.
c) Wiederholen Sie diesen 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 virtual sensor before you can collect NetFlow records. The EFC 1292v sensor 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.

Required NetFlow fields

ExtraHop parses only NetFlow v5 fields, and all v5 fields must be present in records sent to the sensor.

Field	Description
srcaddr	Source IP address
dstaddr	Destination IP address
nexthop	IP address of next hop router
input	SNMP index of input interface
output	SNMP index of output interface
dPkts	Packets in the flow
dOctets	Total number of Layer 3 bytes in the packets of the flow
First	SysUptime at start of flow
Last	SysUptime at the time the last packet of the flow was received
srcport	TCP/UDP source port number or equivalent
dstport	TCP/UDP destination port number or equivalent
tcp_flags	Cumulative OR of TCP flags
prot	IP protocol type (for example, TCP = 6; UDP = 17)
tos	IP type of service (ToS)
src_as	Autonomous system number of the source, either origin or peer
dst_as	Autonomous system number of the destination, either origin or peer
src_mask	Source address prefix mask bits
dst_mask	Destination address prefix mask bits

For more information, see NetFlow V5 formats.

Configure the flow type and UDP port

1. In the Network Settings section, click **NetFlow**.
2. 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

3. From the Flow Type drop-down menu, select **NetFlow**.
4. Click the plus icon (**+**) to add the port.

Add approved networks

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

Discover NetFlow devices

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

Note: ExtraHop systems do not support sampled NetFlow. Including sampled NetFlow in your traffic might result in inaccurate device metrics, but device discovery should still function as normal.

Here are some 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. In the Network Settings section, click **NetFlow**.
2. 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.
3. 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.