

Erfassen Sie den Datenverkehr von NetFlow- und sFlow-Geräten

Veröffentlicht: 2024-02-12

Sie müssen die Netzwerkschnittstellen- und Porteinstellungen auf dem ExtraHop-System konfigurieren, bevor Sie NetFlow- oder sFlow-Daten aus Remote-Flow-Netzwerken (Flow-Exportern) sammeln können. Flow-Netzwerke können auf Reveal (x) Enterprise-Systemen nicht konfiguriert werden. Das ExtraHop-System unterstützt die folgenden Flow-Technologien: Cisco NetFlow v5 und v9, AppFlow, IPFIX und sFlow.


 **Hinweis** Informationen zur virtuellen NetFlow-Sensor-Appliance EFC 1292v finden Sie unter [Stellen Sie den ExtraHop EFC 1292v NetFlow Sensor bereit](#).

Sie müssen sich als Benutzer anmelden mit [Rechte für die System- und Zugriffsverwaltung](#) um die folgenden Schritte abzuschließen.

Konfigurieren Sie die Schnittstelle auf Ihrem ExtraHop-System

Zusätzlich zur Konfiguration des ExtraHop-Systems müssen Sie Ihre Netzwerkgeräte so konfigurieren, dass sie sFlow- oder NetFlow-Verkehr senden. Schlagen Sie in der Dokumentation Ihres Anbieters nach oder sehen Sie sich das Beispiel an [Cisco-Konfigurationen](#) am Ende dieses Dokuments. Beachten Sie, dass Cisco ASA-Firewalls mit NetFlow Secure Event Logging (NSEL) nicht unterstützt werden.


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. Klicken Sie im Abschnitt Schnittstellen auf den Namen der Schnittstelle, die die Flow-Daten empfangen soll.
4. Aus dem Schnittstellenmodus Drop-down-Liste, wählen **Management + Flow-Ziel**.

 **Hinweis** Der EDA 1100v muss entweder für Durchflussdaten oder wire data konfiguriert werden, da dieser Sensor Durchflussdaten und wire data nicht gleichzeitig verarbeiten kann. Wenn der Sensor für Durchflussdaten konfiguriert ist, müssen Sie den Überwachungsanschluss auf einstellen **Deaktiviert**.

5. Wenn DHCPv4 aktivieren ist ausgewählt, klicken Sie **Speichern**.
Andernfalls konfigurieren Sie die verbleibenden Netzwerkeinstellungen und klicken Sie dann auf **Speichern**.

Konfigurieren Sie den Flow-Typ und den UDP-Port

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. In der Netzwerkeinstellungen Abschnitt, klicken Sie **Flow-Netzwerke**.
3. Im Abschnitt Ports, von der Hafen Feld, geben Sie die UDP-Portnummer ein.
Der Standardport für Net Flow ist 2055, und der Standardport für sFlow ist 6343. Sie können je nach Bedarf weitere Ports für Ihre Umgebung hinzufügen.

 **Hinweis** Die Portnummern müssen 1024 oder höher sein

4. Aus dem Art des Flusses Drop-down-Menü, wählen **NetFlow** oder **sFlow**.
Wählen Sie für AppFlow-Verkehr **NetFlow**.
5. Klicken Sie auf das Plus-Symbol (+), um den Port hinzuzufügen.

6. Speichern Sie die laufende Konfigurationsdatei, um Ihre Änderungen beizubehalten, indem Sie auf **Änderungen ansehen und speichern** oben auf der Flow Networks-Seite.
7. Klicken Sie **Speichern**.

Fügen Sie die ausstehenden Flow-Netzwerke hinzu

Sie können jetzt ausstehende Flow-Netzwerke hinzufügen.

Bevor Sie beginnen

Sie müssen sich als Benutzer anmelden mit [Rechte für die System- und Zugriffsadministration](#) um die folgenden Schritte abzuschließen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. In der Netzwerkeinstellungen Abschnitt, klicken Sie **Flow-Netzwerke**.
3. Klicken Sie im Abschnitt Pending Flow Networks auf **Flow-Netzwerk hinzufügen**.
4. Geben Sie im Feld Flussnetz ID einen Namen zur Identifizierung dieses Flow-Netzwerks ein.
5. Wählen Sie den **Automatische Aufzeichnungen** Checkbox, um Datensätze aus diesem Flussnetz an einen verbundenen Recordstore zu senden.
6. Wählen Sie den **SNMP-Polling aktivieren** Kontrollkästchen, um SNMP-Polling zu aktivieren.
7. Wenn Sie SNMP-Polling aktivieren, wählen Sie im Dropdownmenü SNMP-Anmeldeinformationen eine der folgenden Optionen aus:
 - **Von CIDR erben**. Wenn Sie diese Option auswählen, werden die SNMP-Anmeldeinformationen auf der Grundlage der Einstellungen für gemeinsame SNMP-Anmeldeinformationen angewendet.
 - **Benutzerdefinierte Anmeldeinformationen**. Wählen Sie v1, v2 oder v3 aus der Dropdownliste SNMP-Version aus, und konfigurieren Sie dann die verbleibenden Einstellungen für den jeweiligen Abfragetyp.
8. Klicken Sie **Speichern**.

Das Flussnetz wird in der Tabelle Genehmigte Flow-Netzwerke angezeigt. Wenn Sie das Flussnetz nicht sehen, können Sie es manuell hinzufügen, indem Sie auf **Flow Network hinzufügen** in der Zugelassene Flow-Netzwerke Abschnitt und Vervollständigung der Informationen wie oben beschrieben.

Konfigurierte Flow-Netzwerke anzeigen

Nachdem Sie Ihre Flow-Netzwerke konfiguriert haben, melden Sie sich beim ExtraHop-System an, um die integrierten Diagramme anzusehen und Einstellungen und Konfigurationen zu ändern.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Vermögenswerte**, und klicken Sie dann auf **Netzwerke**.
3. Klicken Sie auf den Dropdown-Pfeil neben dem Namen des Flussnetz, um eine Liste der Flow-Schnittstellen und ihrer Attribute anzuzeigen.
4. Aktivieren Sie das Kontrollkästchen neben dem Namen des Flussnetz oder der Schnittstelle.
In der oberen Leiste können Sie ein Diagramm erstellen, einen Auslöser zuweisen, einen Alarm zuweisen, die Flussschnittstelle umbenennen und die Schnittstellengeschwindigkeit festlegen.

ExtraHop Dashboards Detections Alerts **Assets** Records Packets Search... 8.4.0 1488

Last 6 hours 5 minutes ago **Networks**

Any Field ≈ 1 of 9 selected

Devices	Name ↑	Type	Devices	IP Address	Sensor	Description	Interface Speed
> <input type="checkbox"/>	Capture 4E:D5:00:0F:93:C6 (56 VLANs)	Site	2,689	192.168.191...	–	dfasdfasd	–
> <input type="checkbox"/>	Cisco NX-OS(n7000-s1-dk9)-13 (8 interfaces)	Flow Network	–	192.168.243...	–	–	–
> <input type="checkbox"/>	Flow Network aristastic-sflow (10 interfaces)	Flow Network	–	192.168.166...	–	–	–
> <input type="checkbox"/>	Flow Network OfficeFeed (1 interface)	Flow Network	–	192.168.203...	–	–	–
∨ <input type="checkbox"/>	Flow Network 192.168.0.24 (4 interfaces)	Flow Network	–	192.168.223...	–	–	–
<input type="checkbox"/>	GigabitEthernet0/0	Flow Interface	–	–	–	–	1.000 Gb/s
<input checked="" type="checkbox"/>	GigabitEthernet0/1	Flow Interface	–	–	–	–	1.000 Gb/s
<input type="checkbox"/>	GigabitEthernet0/2	Flow Interface	–	–	–	–	1.000 Gb/s
<input type="checkbox"/>	Interface 0	Flow Interface	–	–	–	–	–

Hinweis: Jeder NetFlow-Datensatz enthält den Schnittstellenindex (ifIndex) der Berichtsschnittstelle. Die Schnittstellentabelle (ifTable) wird dann vom ExtraHop-System abgefragt, um die Schnittstellengeschwindigkeit (ifSpeed) zu ermitteln.

5. Klicken Sie auf den Namen des Flussnetz oder die Flussschnittstelle, um die integrierten Diagramme auf den Übersichtsseiten anzuzeigen.

Auf den Übersichtsseiten können Sie auf die Regionen und Diagramme klicken und sie einem neuen oder vorhandenen Dashboard hinzufügen.

Cisco NetFlow-Geräte konfigurieren

Veröffentlicht: 2024-02-12

Die folgenden Beispiele für die grundlegende Cisco-Router-Konfiguration für NetFlow. NetFlow wird pro Schnittstelle konfiguriert. Wenn NetFlow auf der Schnittstelle konfiguriert ist, werden IP-Paketflussinformationen in das ExtraHop-System exportiert.

- ! **Wichtig:** NetFlow nutzt den SNMP ifIndex-Wert, um Eingangs- und Ausgangsschnittstelleninformationen in Flow-Datensätzen darzustellen. Um die Konsistenz der Schnittstellenberichte zu gewährleisten, aktivieren Sie die SNMP ifIndex-Persistenz auf Geräten, die NetFlow an das ExtraHop-System senden. Weitere Informationen zur Aktivierung der SNMP ifIndex-Persistenz auf Ihren Netzwerkgeräten finden Sie in der vom Gerätehersteller bereitgestellten Konfigurationsanleitung.

Weitere Informationen zur Konfiguration von NetFlow auf Cisco Switches finden Sie in der Dokumentation zu Ihrem Cisco Router oder auf der Cisco-Website unter www.cisco.com.

Konfigurieren Sie einen Exporter auf dem Cisco Nexus-Switch

Definieren Sie einen Flow-Exporter, indem Sie das Exportformat, das Protokoll und das Ziel angeben.

1. Melden Sie sich bei der Switch-Befehlszeilenschnittstelle an und führen Sie die folgenden Befehle aus.
2. Rufen Sie den globalen Konfigurationsmodus auf.

```
config t
```

3. Erstellen Sie einen Fluss Exporter und wechseln Sie in den Fluss Exporter-Konfigurationsmodus.

```
flow exporter <name>
```

Zum Beispiel:

```
flow exporter Netflow-Exporter-1
```

4. (Optional) Geben Sie eine Beschreibung ein.

```
description <string>
```

Zum Beispiel:

```
description Production-Netflow-Exporter
```

5. Legen Sie die IPv4- oder IPv6-Zieladresse für den Exporter fest.

```
destination <eda_mgmt_ip_address>
```

Zum Beispiel:

```
destination 192.168.11.2
```

6. Geben Sie die Schnittstelle an, die benötigt wird, um den NetFlow-Collector am konfigurierten Ziel zu erreichen.

```
source <interface_type> <number>
```

Zum Beispiel:

```
source ethernet 2/2
```

7. Geben Sie die NetFlow-Exportversion an.

```
version 9
```

Konfiguration von Cisco Switches über die Cisco IOS CLI

1. Melden Sie sich bei der Cisco IOS-Befehlszeilenschnittstelle an und führen Sie die folgenden Befehle aus.
2. Rufen Sie den globalen Konfigurationsmodus auf.

```
config t
```

3. Geben Sie die Schnittstelle an, und wechseln Sie dann in den Schnittstellenkonfigurationsmodus.

- Cisco Router der Serie 7500:

```
interface <type> <slot>/<port-adapter>/<port>
```

Zum Beispiel:

```
interface fastethernet 0/1/0
```

- Cisco Router der Serie 7200:

```
interface <type> <slot>/<port>
```

Zum Beispiel:

```
interface fastethernet 0/1
```

4. Aktivieren Sie NetFlow.

```
ip route-cache flow
```

5. NetFlow-Statistiken exportieren, wobei *<ip-address>* ist die Management + Flow Target-Schnittstelle auf dem ExtraHop-System und *<udp-port>* ist die konfigurierte Collector-UDP-Portnummer.

```
ip flow-export <ip-address> <udp-port> version 5
```