Collectez le trafic depuis les appareils NetFlow et sFlow

Publié: 2024-11-04

Vous devez configurer l'interface réseau et les paramètres de port sur le système ExtraHop avant de pouvoir collecter des données NetFlow ou sFlow à partir de réseaux de flux distants (exportateurs de flux). Les réseaux de flux ne peuvent pas être configurés sur les systèmes RevealX Enterprise. Le système ExtraHop prend en charge les technologies de flux suivantes : Cisco NetFlow v5 et v9, AppFlow, IPFIX et sFlow.

Note: Pour plus d'informations sur l'appliance virtuelle à sonde NetFlow EFC 1292v, voir Déployez le capteur NetFlow ExtraHop EFC 1292v.

Vous devez vous connecter en tant qu'utilisateur avec Privilèges d'administration du système et des accès pour effectuer les étapes suivantes.

Configurez l'interface de votre système ExtraHop

Outre la configuration du système ExtraHop, vous devez configurer vos périphériques réseau pour envoyer du trafic sFlow ou NetFlow. Reportez-vous à la documentation de votre fournisseur ou consultez l' exemple Configurations Cisco à la fin de ce document. Notez que les pare-feux Cisco ASA dotés de la fonction NetFlow Secure Event Logging (NSEL) ne sont pas pris en charge.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
3. Dans le Interfaces section, cliquez sur le nom de l'interface qui doit recevoir les données de flux.
4. À partir du Mode d'interface liste déroulante, sélectionnez **Gestion + Cible de flux**.

   Note: L'EDA 1100v doit être configuré pour les données de flux ou les données filaires car cette sonde ne peut pas traiter simultanément les données de flux et les données de fil. Si la sonde est configurée pour les données de flux, vous devez régler le port de surveillance sur **Désactivé**.
5. Si Activer DHCPv4 est sélectionné, cliquez sur **Enregistrer**.

   Sinon, configurez les autres paramètres réseau, puis cliquez sur **Enregistrer**.

Configurer le type de flux et le port UDP

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Dans le Paramètres réseau section, cliquez sur **Réseaux de flux**.
3. Dans le Ports section, dans la Port dans ce champ, saisissez le numéro de port UDP.

   Le port par défaut pour Net Flow est `2055`, et le port par défaut pour sFlow est `6343`. Vous pouvez ajouter des ports supplémentaires selon les besoins de votre environnement.

   Note: Les numéros de port doivent être de 1024 ou plus
4. À partir du Type de flux liste déroulante, sélectionnez **NetFlow** ou **flux S**.

   Pour le trafic AppFlow, sélectionnez **NetFlow**.
5. Cliquez sur l'icône plus (**+**) pour ajouter le port.
6. Enregistrez le fichier de configuration en cours pour conserver vos modifications en cliquant sur **Afficher et enregistrer les modifications** en haut de la page Flow Networks.

7. Cliquez **Enregistrer**.

Ajouter les réseaux de flux en attente

Vous pouvez désormais ajouter des réseaux de flux en attente.

Avant de commencer
Vous devez vous connecter en tant qu'utilisateur avec Privilèges d'administration du système et des accès pour effectuer les étapes suivantes.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Dans le Paramètres réseau section, cliquez sur **Réseaux de flux**.
3. Dans le Réseaux de flux en attente section, cliquez sur **Ajouter un réseau Flow**.
4. Dans le ID réseau Flow dans le champ, saisissez un nom pour identifier ce réseau de flux.
5. Sélectionnez le **Enregistrements automatiques** case à cocher pour envoyer des enregistrements de ce réseau de flux vers un espace de stockage des enregistrements connecté.
6. Sélectionnez le **Activer le sondage SNMP** case à cocher pour activer le sondage SNMP.
7. Si vous activez le sondage SNMP, sélectionnez l'une des options suivantes dans la liste déroulante des informations dcessations d'identification SNMP :
   - **Hériter du CIDR**. Si vous sélectionnez cette option, les informations d'identification SNMP sont appliquées en fonction des paramètres d'identification SNMP partagées.
   - **informations d_identification personnalisées**. Sélectionnez v1, v2 ou v3 dans la liste déroulante des versions du SNMP, puis configurez les paramètres restants pour le type de sondage spécifique.
8. Cliquez **Enregistrer**.

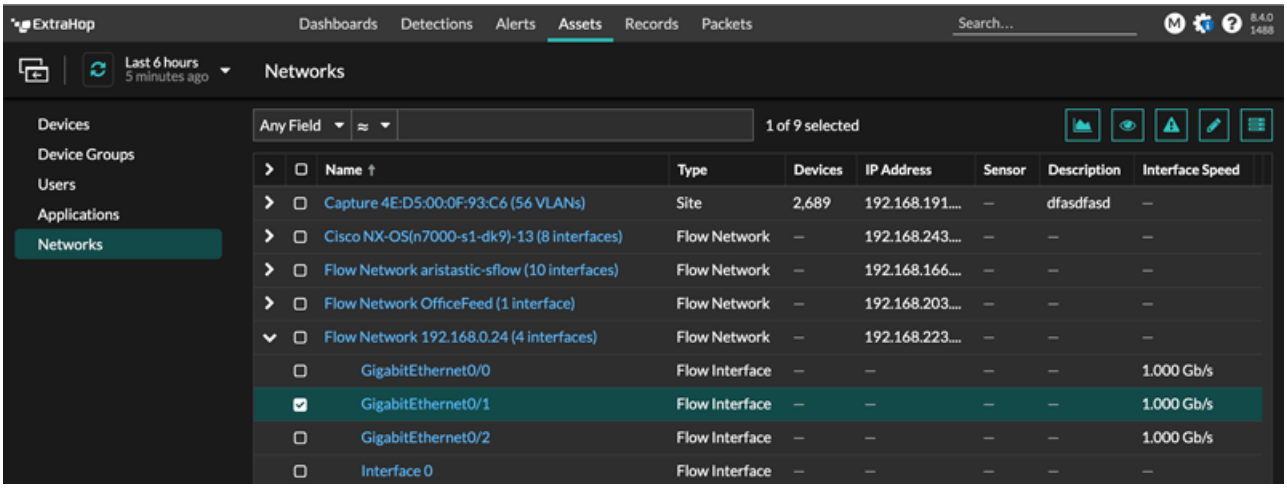
Le réseau de flux apparaît dans le tableau Réseaux de flux approuvés. Si vous ne voyez pas le réseau de flux, vous pouvez l'ajouter manuellement en cliquant **Ajouter un réseau Flow** dans le Réseaux de flux approuvés section et en complétant les informations comme décrit ci-dessus.

Afficher les réseaux de flux configurés

Après avoir configuré vos réseaux de flux, connectez-vous au système ExtraHop pour afficher les graphiques intégrés et modifier les paramètres et les configurations.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Actifs**, puis cliquez sur **Réseaux**.
3. Cliquez sur la flèche déroulante à côté du nom du réseau de flux pour afficher la liste des interfaces de flux et leurs attributs.
4. Cochez la case à côté du nom du réseau de flux ou de l'interface.

   Dans la barre supérieure, vous pouvez créer un graphique, attribuer un déclencheur, attribuer une alerte , renommer l'interface de flux et définir la vitesse de l'interface.



Note: Chaque enregistrement NetFlow contient l'index d'interface (ifIndex) de l'interface de reporting. La table d'interface (ifTable) est ensuite interrogée par le système ExtraHop pour obtenir la vitesse de l'interface (ifSpeed).

5. Cliquez sur le nom du réseau de flux ou sur le nom de l'interface de flux pour afficher les graphiques intégrés sur les pages de résumé.

   Dans les pages de résumé, vous pouvez cliquer sur les régions et les graphiques et les ajouter à un tableau de bord nouveau ou existant.

Configuration des appareils Cisco NetFlow

Publié: 2024-11-04

Les exemples suivants de configuration de base d'un routeur Cisco pour NetFlow. NetFlow est configuré pour chaque interface. Lorsque NetFlow est configuré sur l'interface, les informations de flux de paquets IP sont exportées vers le système ExtraHop.

Important: NetFlow tire parti de la valeur IFindex du SNMP pour représenter les informations d'interface d'entrée et de sortie dans les enregistrements de flux. Pour garantir la cohérence des rapports d'interface, activez la persistance SNMP iFindex sur les appareils qui envoient NetFlow au système ExtraHop. Pour plus d' informations sur la façon d'activer la persistance SNMP iFindex sur les périphériques de votre réseau, reportez-vous au guide de configuration fourni par le fabricant de l'équipement.

Pour plus d'informations sur la configuration de NetFlow sur les commutateurs Cisco, consultez la documentation de votre routeur Cisco ou le site Web de Cisco à l'adresse www.cisco.com.

Configuration d'un exportateur sur le commutateur Cisco Nexus

Définissez un exportateur de flux en spécifiant le format, le protocole et la destination d'exportation.

1. Connectez-vous à l'interface de ligne de commande du commutateur et exécutez les commandes suivantes .
2. Entrez en mode de configuration globale.

   ```
   config t
   ```

3. Créez un exportateur de flux et passez en mode de configuration de l'exportateur de flux.

   ```
   flow exporter <name>
   ```

   Par exemple :

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

4. (Facultatif) Entrez une description.

   ```
   description <string>
   ```

   Par exemple :

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

5. Définissez l'adresse IPv4 ou IPv6 de destination pour l'exportateur.

   ```
   destination <eda_mgmt_ip_address>
   ```

   Par exemple :

   ```
   destination 192.168.11.2
   ```

6. Spécifiez l'interface nécessaire pour atteindre le collecteur NetFlow à la destination configurée .

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

Par exemple :

```
source ethernet 2/2
```

7. Spécifiez la version d'exportation de NetFlow.

```
version 9
```

Configuration des commutateurs Cisco par le biais de l'interface de ligne de commande Cisco IOS

1. Connectez-vous à l'interface de ligne de commande Cisco IOS et exécutez les commandes suivantes .
2. Entrez en mode de configuration globale.

```
config t
```

3. Spécifiez l'interface, puis passez en mode de configuration de l'interface.
   - Routeurs de la gamme Cisco 7500 :

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

     Par exemple :

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

   - Routeurs de la gamme Cisco 7200 :

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

     Par exemple :

     ```
     interface fastethernet 0/1
     ```

4. Activez NetFlow.

```
ip route-cache flow
```

5. Exportez les statistiques NetFlow, où <*ip-address*> est l'interface Management + Flow Target sur le système ExtraHop et <*udp-port*> est le numéro de port UDP du collecteur configuré.

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