Dépannage de NetFlow/IPFIX Telemetry Ingest dans Secure Network Analytics

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Guides de configuration
  - Composants utilisés
- Informations générales
  - Champs obligatoires
- Processus de dépannage
    - Vérification de la réception de télémétrie NetFlow/IPFIX
    - Vérification du modèle NetFlow/IPFIX
    - Vérifiez la réception de télémétrie NetFlow/IPFIX après avoir ajouté les champs manquants
    - Vérification du port d'entrée de télémétrie NetFlow/IPFIX
    - Vérifier que l'option NetFlow d'arrivée de télémétrie NetFlow est activée
- Informations connexes

Introduction

Ce document décrit comment dépanner la réception télémétrique Netflow dans Secure Network Analytics (SNA).

Conditions préalables

- Connaissances de Cisco SNA
- Connaissances NetFlow/IPFIX

Exigences

- Secure Network Analytics version 7.5.0 ou ultérieure
- Collecteur de flux de la version 7.5.0 ou ultérieure
- Accès CLI en tant que sysadmin au collecteur de flux
- Accès administrateur de l'interface utilisateur en tant qu'administrateur du collecteur de flux

Guides de configuration

- Configuration de NetFlow/IPFIX pour l'accès télémétrique sur Secure Network Analytics

Composants utilisés

- SNA Manager et collecteur de flux sur 7.5.0
- Logiciel Wireshark

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le collecteur de flux est une appliance SNA chargée de collecter, traiter et stocker les flux envoyés à Secure Network Analytics. Pour NetFlow version 9 ou IPFIX, plusieurs champs peuvent être inclus dans le modèle NetFlow/IPFIX pour ajouter des informations relatives au trafic réseau. Toutefois, 9 champs spécifiques doivent être inclus dans le modèle NetFlow/IPFIX pour que le collecteur de flux puisse traiter ces flux. Le collecteur de flux ne traite pas les flux entrants qui incluent un modèle non valide. Par conséquent, SNA n'affiche pas les informations de flux de ces exportateurs sous l'interface utilisateur Web ou le client Desktop.

Champs obligatoires

Les champs suivants doivent être inclus dans le modèle NetFlow/IPFIX pour l'acquisition de télémétrie. Assurez-vous que ces 9 champs sont inclus dans le modèle NetFlow/IPFIX, afin que Secure Network Analytics traite les flux entrants.

- Adresse IP source
- Adresse IP de destination
- Port source
- Port de destination
- Protocole de couche 3
- Nombre d'octets
- Nombre de paquets
- Heure de début du flux
- Heure de fin du flux

Remarque : D'autres champs peuvent être inclus dans la configuration NetFlow/IPFIX. Toutefois, les champs précédents constituent la configuration minimale requise par Secure Network Analytics pour l'acquisition de données de télémétrie.

Processus de dépannage

Vérification de la réception de télémétrie NetFlow/IPFIX

Pour confirmer si le collecteur de flux SNA reçoit et insère la télémétrie NetFlow/IPFIX des exportateurs :

1. Connectez-vous à l'interface administrateur du collecteur de flux SNA avec les identifiants admin : https://<Adresse IP du collecteur de flux>/swa/login.html
2. Dans le panneau de gauche, accédez à Support > Browse Files
3. Accédez au dossier suivant : logiciel > aujourd'hui > journaux
4. Cliquez sur le fichier sw.log pour le télécharger sur votre machine locale et l'ouvrir dans un éditeur de texte.
5. Recherchez ces lignes au bas du journal, ce résumé est créé toutes les cinq minutes :

```
18:45:00 I-sch-t: process_5_min_period: begin
18:45:00 I-sch-t: process_5_min_period: periods(177)
18:45:00 S-per-t: Performance Period 177
18:45:00 S-per-t:     Engine status Status normal
18:45:00 S-per-t:     Processed 6948 flows at 24 fps this period
18:45:00 S-per-t:     Processed 4226 biflows at 15 fps this period
18:45:00 S-per-t:     Dropped 0 flows this period
18:45:00 S-per-t:     Discarded 4358 flows this period due to insufficient template data
18:45:00 S-per-t:     Processed 1838743 flows at 35 fps today
18:45:00 S-per-t:     Dropped 0 flows today
18:45:00 S-per-t:     Discarded 11069 flows today due to insufficient template data
18:45:00 S-per-t:     Process instance 0 processed 3372 flows at 12 fps this period
18:45:00 S-per-t:     Process instance 0 processed 2066 biflows at 7 fps this period
18:45:00 S-per-t:     Process instance 1 processed 3576 flows at 12 fps this period
18:45:00 S-per-t:     Process instance 1 processed 2160 biflows at 8 fps this period
18:45:00 S-per-t:     Inserted 2048 flow stats at 7 fps this period
18:45:00 S-per-t:     Inserted 2013 interface stats at 7 fps this period
18:45:00 S-per-t:     Inserted 470932 flow stats at 9 fps today
18:45:00 S-per-t:     Inserted 678994 interface stats at 13 fps today
```

Remarque : La ligne 8 indique que des flux ont été rejetés en raison d'un manque de données de modèle pour la dernière période.

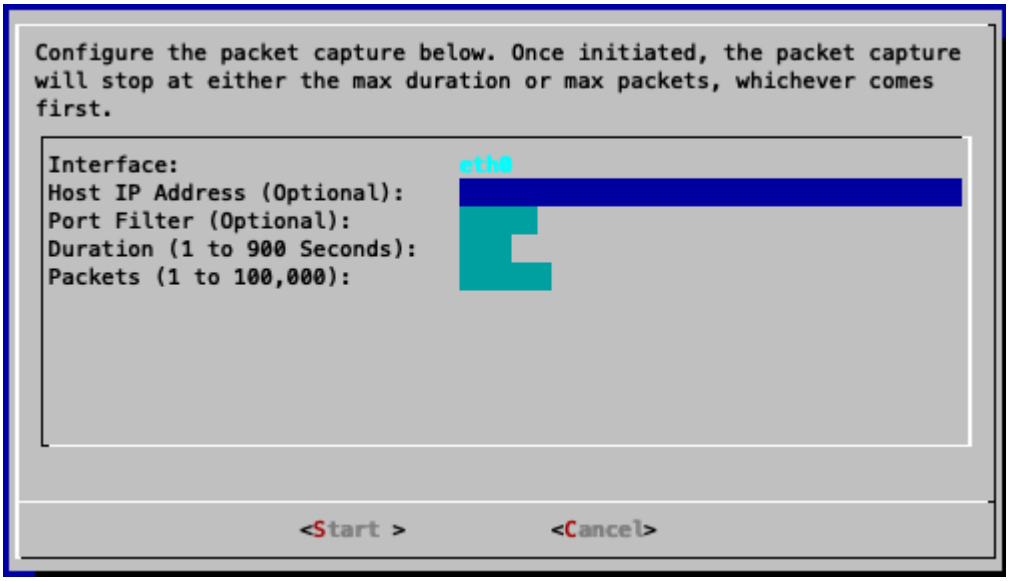
Vérification du modèle NetFlow/IPFIX

Pour confirmer les champs inclus dans le modèle NetfFlow/IPFIX :

1. Connectez-vous à l'interface de ligne de commande du collecteur de flux SNA avec les informations d'identification sysadmin.

2. Dans le menu SystemConfig, accédez à : Avancé > Capture de paquets

3. Entrez les informations de l’exportateur qui n’indiquent pas les flux dans le SCN :



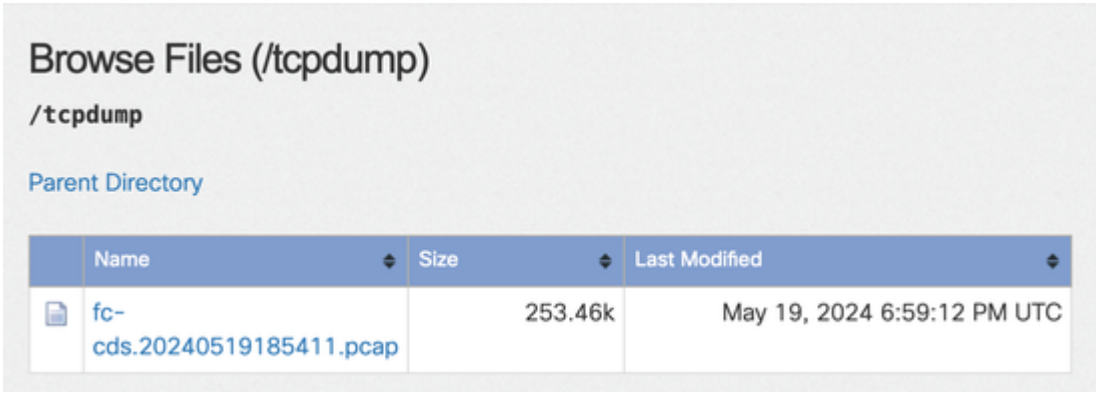
4. Attendez que le processus soit terminé.

5. Pour télécharger le fichier, connectez-vous à l'interface utilisateur Admin du collecteur de flux SNA avec les informations d'identification admin : https://<Adresse IP du collecteur de flux>/swa/login.html

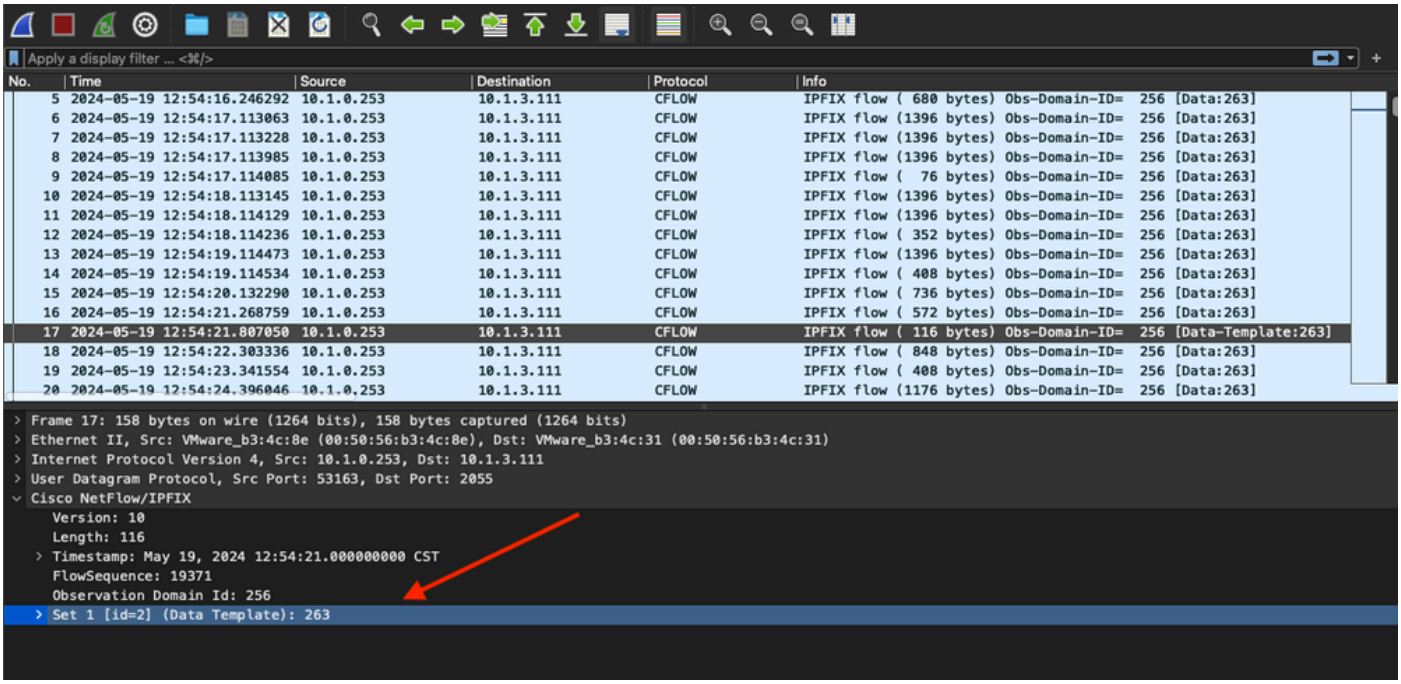
6.Dans le panneau de gauche, accédez à Support > Browse Files

7. Accédez au dossier suivant : tcpdump

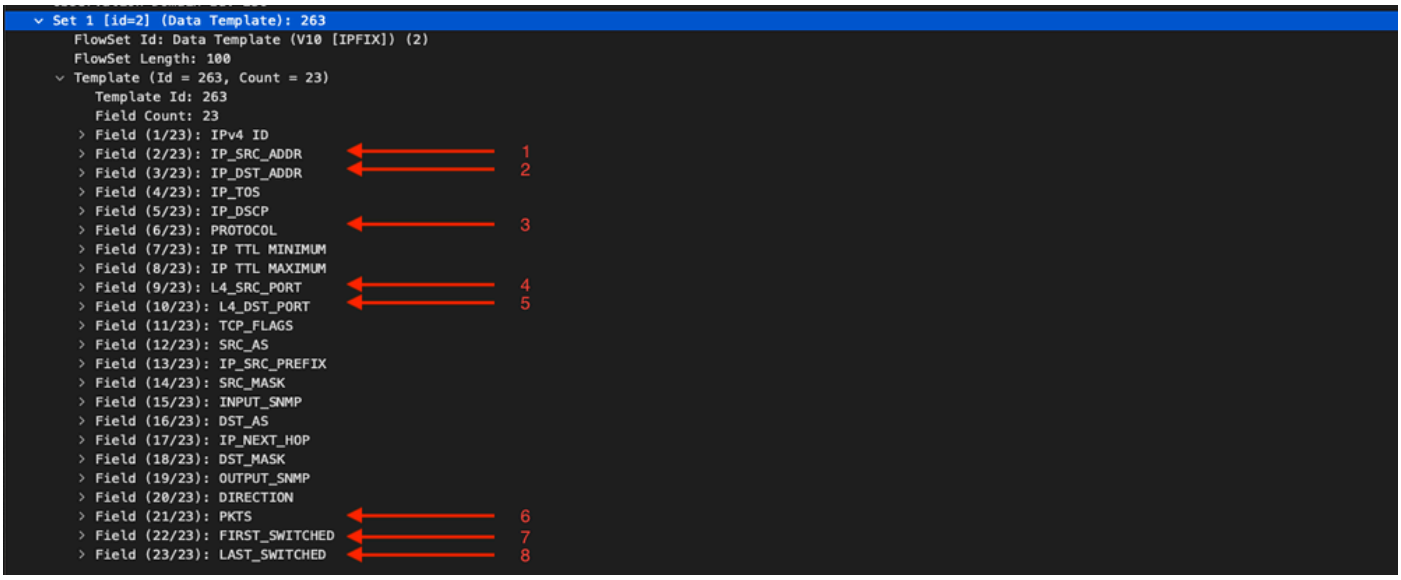
8. Cliquez sur le fichier de capture de paquets pour le télécharger sur votre ordinateur local et l’ouvrir sur Wireshark :



9. Identifiez la trame dans laquelle le modèle NetFlow/IPFIX a été reçu.



10. Vérifiez que les 9 champs obligatoires apparaissent sur le modèle



Remarque : Notez que sur le modèle, il n'y a que 8 des 9 champs obligatoires requis par SNA pour Telemetry Ingest. Pour ce scénario, le champ BYTES est manquant.

Vérifiez la réception de télémétrie NetFlow/IPFIX après avoir ajouté les champs manquants

Pour confirmer si le collecteur de flux SNA reçoit et insère la télémétrie NetFlow/IPFIX de l'exportateur après la modification :

1. Connectez-vous à l'interface administrateur du collecteur de flux SNA avec les informations d'identification admin : https://<Adresse IP du collecteur de flux>/swa/login.html
2. Dans le panneau de gauche, accédez à Support > Browse Files
3. Accédez au dossier suivant : log > aujourd'hui > journaux
4. Cliquez sur le fichier sw.log pour le télécharger sur votre machine locale et ouvrez-le dans un éditeur de texte.
5. Recherchez ces lignes au bas du journal

```
19:20:00 I-sch-t: process_5_min_period: begin
19:20:00 I-sch-t: process_5_min_period: periods(184)
19:20:00 S-per-t: Performance Period 184
19:20:00 S-per-t:     Engine status Status normal
19:20:00 S-per-t:     Processed 10992 flows at 37 fps this period
19:20:00 S-per-t:     Processed 4176 biflows at 14 fps this period
19:20:00 S-per-t:     Dropped 0 flows this period
19:20:00 S-per-t:     Discarded 0 flows this period due to insufficient template data
19:20:00 S-per-t:     Processed 1896017 flows at 35 fps today
19:20:00 S-per-t:     Dropped 0 flows today
19:20:00 S-per-t:     Discarded 36041 flows today due to insufficient template data
19:20:00 S-per-t:     Process instance 0 processed 5575 flows at 19 fps this period
19:20:00 S-per-t:     Process instance 0 processed 2195 biflows at 8 fps this period
19:20:00 S-per-t:     Process instance 1 processed 5417 flows at 19 fps this period
```

```
19:20:00 S-per-t:     Process instance 1 processed 1981 biflows at 7 fps this period
19:20:00 S-per-t:     Inserted 2878 flow stats at 10 fps this period
19:20:00 S-per-t:     Inserted 4510 interface stats at 16 fps this period
19:20:00 S-per-t:     Inserted 486734 flow stats at 9 fps today
19:20:00 S-per-t:     Inserted 696260 interface stats at 13 fps today
```

Remarque : La ligne 8 indique qu'aucun flux n'a été rejeté au cours de la dernière période.

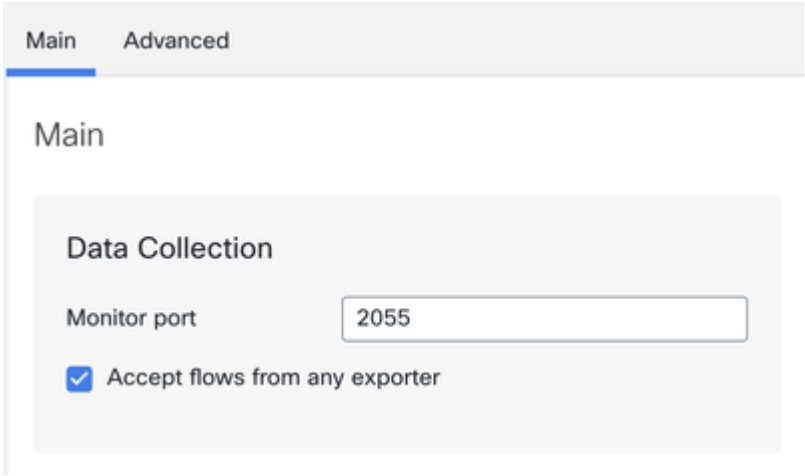
Vérification du port d'entrée de télémétrie NetFlow/IPFIX

Pour confirmer que le collecteur de flux SNA reçoit la télémétrie NetFlow/IPFIX des exportateurs sur le port approprié :

1. Connectez-vous à l'interface utilisateur Web SNA avec un utilisateur disposant d'autorisations d'administrateur.

2. Dans le menu supérieur, accédez à Configurer et sélectionnez Collecteurs de flux

3. Vérifiez que le collecteur de flux SNA utilise le même port que celui que les exportateurs ont configuré pour envoyer NetFlow/IPFIX



Remarque : Le port par défaut pour NetFlow est 2055. Toutefois, vous pouvez sélectionner un autre port. Veillez à utiliser le même port lors de la première installation sur les collecteurs de flux.

Vérifier que l'option NetFlow d'arrivée de télémétrie NetFlow est activée

Pour vérifier si l'option SNA Flow Collector pour l'acquisition télémétrique de NetFlow/IPFIX est activée :

1. Connectez-vous à l'interface administrateur du collecteur de flux SNA avec les informations d'identification : https://<Adresse IP du collecteur de flux>/swa/login.html
2. Dans le volet de gauche, accédez à Support > Advanced Settings
3. Vérifiez que l'option enable_netflow est définie sur 1 :



Informations connexes

- Pour obtenir de l'aide supplémentaire, veuillez contacter le Centre d'assistance technique (TAC). Un contrat d'assistance valide est requis : Cisco Worldwide Support Contacts.
- Vous pouvez également visiter la communauté Cisco Security Analytics ici.
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.