Dépannage des problèmes de base de télémétrie du module de visibilité réseau AnyConnect dans Secure Network Analytics

Contenu

Introduction

Ce document décrit la procédure de dépannage des problèmes de télémétrie NVM (Network Visibility Module) dans Secure Network Analytics (SNA).

Conditions préalables

- Connaissances Cisco SNA
- Connaissances Cisco AnyConnect

Guides de configuration

- Guide de configuration des modules NVM (Secure Network Analytics Endpoint License) et NVM (Network Visibility Module)
- Cisco AnyConnect Administrator Guide Network Visibility Module, version 4.10

Conditions requises

- SNA Manager et Flow Collector dans la version 7.3.2 ou ultérieure
- Licence de terminaux SNA
- Cisco AnyConnect avec Network Visibility Module 4.3 ou ultérieur

Components Used

- SNA Manager et Flow Collector version 7.4.0 et licence de terminaux
- Cisco AnyConnect 4.10.03104 avec VPN et module de visibilité réseau
- Ordinateur virtuel Windows 10
- 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.

Processus de dépannage

Configuration SNA

Vérifier la licence

Assurez-vous que le compte virtuel Smart Licensing auquel le SNA Manager est enregistré dispose des licences de point de terminaison.

Vérifier l'entrée de télémétrie NVM

Pour vérifier si le collecteur de flux SNA reçoit et insère la télémétrie NVM des points d'extrémité, procédez comme suit :

1. Connectez-vous au collecteur de flux via SSH ou la console avec les informations d'identification **racine**.

2. Exécutez la commande **grep 'NVM enregistre cette période : ' /lancope/var/sw/today/logs/sw.log**.

3. À partir de la sortie renvoyée, vérifiez si le collecteur de flux ingère des enregistrements NVM et les insère dans la base de données.

```
ao-fc01-cds:~# grep 'NVM records this period:' /lancope/var/sw/today/logs/sw.log
04:00:01 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
04:05:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
04:10:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
04:15:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
```

Àpartir de cette sortie, il semble que le collecteur de flux n'a reçu aucun enregistrement NVM, mais vous devez confirmer s'il est configuré pour écouter la télémétrie NVM.

Vérifier si le collecteur de flux est configuré pour écouter la télémétrie NVM

1. Connectez-vous à l'interface utilisateur de Flow Collector Admin.

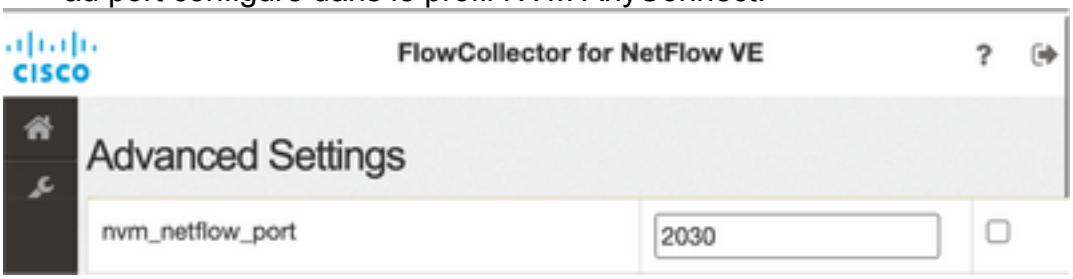
2. Accédez à **Support > Advanced Settings**.

3. Assurez-vous que les attributs requis sont configurés correctement :

SNA version 7.3.2 ou 7.4.0

==========
==========
==========
==========

- Recherchez l'attribut **nvm_netflow_port** et vérifiez la valeur configurée. Cela doit correspondre au port configuré dans le profil NVM AnyConnect.



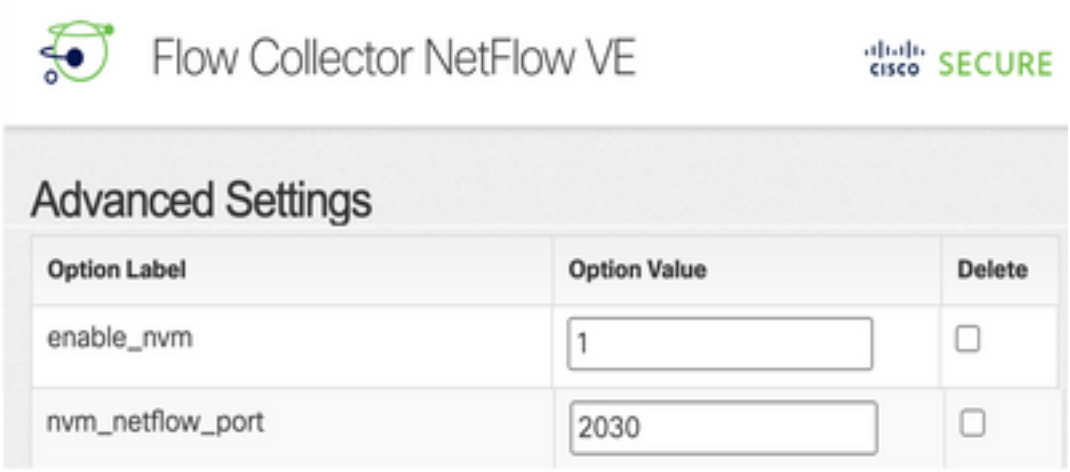
Remarque : assurez-vous que le port configuré est un port non réservé et qu'il n'est pas 2055, 514 ou 8514. Si la valeur configurée est 0, la fonction est désactivée.

Remarque : si aucun champ n'est affiché, faites défiler la page jusqu'en bas. Cliquez sur le champ **Ajouter une nouvelle option**. Pour plus d'informations sur les paramètres avancés du collecteur de flux, reportez-vous à la rubrique d'aide en ligne Paramètres avancés.

SNA version 7.4.1

==========
==========
==========
==========

- Recherchez l'attribut **nvm_netflow_port** et vérifiez la valeur configurée. Cela doit correspondre au port configuré dans le profil NVM AnyConnect.
- Recherchez l'attribut **enable_nvm** et assurez-vous que la valeur est définie sur **1**, sinon la fonction est désactivée.



Remarque : assurez-vous que le port configuré est un port non réservé et qu'il n'est pas 2055, 514 ou 8514.

Remarque : si aucun champ n'est affiché, faites défiler la page jusqu'en bas. Cliquez sur le champ **Ajouter une nouvelle option**. Pour plus d'informations sur les paramètres avancés du collecteur de flux, reportez-vous à la rubrique d'aide en ligne Paramètres avancés.

4. Une fois que les paramètres avancés du collecteur de flux ont été configurés correctement, vérifiez si la télémétrie est maintenant ingérée, avec la même procédure que celle décrite dans la section **Vérifier la télémétrie NVM**.

5. Si la configuration du point de terminaison avec AnyConnect NVM et les paramètres du collecteur de flux sont corrects, le fichier **sw.log** doit le refléter :

```
ao-fc01-cds:~# grep 'NVM records this period:' /lancope/var/sw/today/logs/sw.log
04:35:00 I-pro-t: NVM records this period: received 78 at 0 rps, inserted 78 at 0 rps, discarded
0
04:40:00 I-pro-t: NVM records this period: received 66 at 0 rps, inserted 66 at 0 rps, discarded
0
04:45:00 I-pro-t: NVM records this period: received 91 at 0 rps, inserted 91 at 0 rps, discarded
0
04:50:00 I-pro-t: NVM records this period: received 80 at 0 rps, inserted 80 at 0 rps, discarded
0
```

6. Si le collecteur de flux n'ingère toujours pas d'enregistrements NVM, vérifiez si le collecteur reçoit les paquets sur l'interface et, dans tous les cas, assurez-vous que la configuration des points de terminaison est correcte.

Configuration des points de terminaison

Vous pouvez déployer AnyConnect NVM de deux manières : a) wavec le package AnyConnect ou b) wavec le package NVM autonome (sur le bureau AnyConnect uniquement).

La configuration requise est la même pour les deux déploiements, la différence réside dans la configuration de Trusted Network Detection.

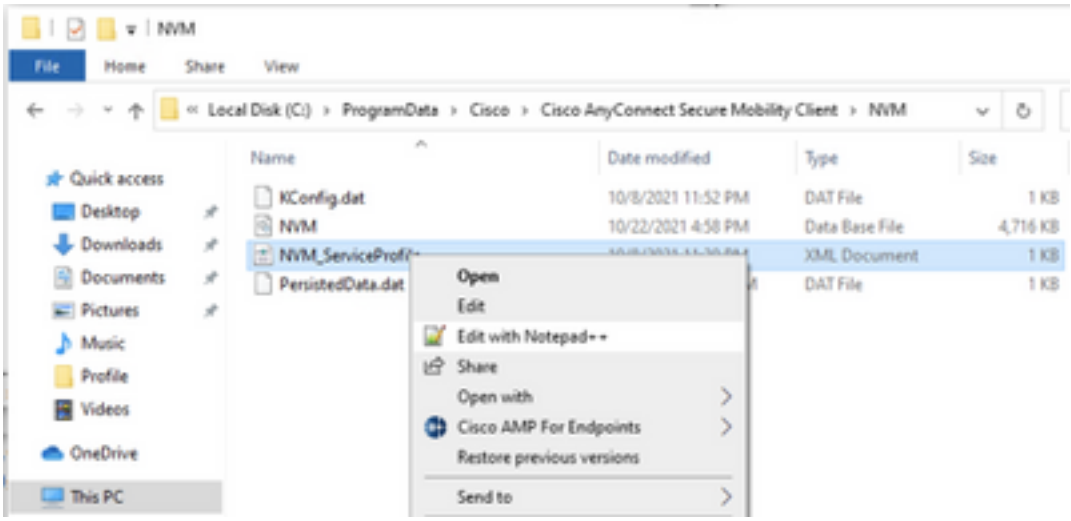
Vérifier le profil NVM

Recherchez le profil NVM utilisé par le point de terminaison et confirmez les paramètres **de configuration du collecteur**.

Emplacement du profil NVM :

- Fenêtres: **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM**
- Mac : **/opt/cisco/anyconnect/nvm**

Note: Le nom du profil NVM doit être **NVM_ServiceProfile**, sinon le module de visibilité réseau ne collecte pas et n'envoie pas de données.



Le contenu du profil NVM dépend de votre configuration, mais les éléments du profil qui sont pertinents pour SNA sont indiqués en gras. Vérifiez les notes après l'exemple de profil NVM :

Note: Assurez-vous que le **port configuré est un port non réservé et qu'il n'est pas 2055, 514 ou 8514**. Le port configuré dans ce profil doit être identique à celui configuré sur le collecteur de flux.

Note: Assurez-vous que si le profil NVM possède l'élément **Secure** XML, il est défini sur **false**, sinon les flux sont envoyés chiffrés avec DTLS et le collecteur de flux ne peut pas les

traiter.

Vérifier les paramètres TND (Trusted Network Detection)

Le module de visibilité réseau envoie des informations de flux uniquement lorsqu'il se trouve sur le réseau approuvé. Par défaut, aucune donnée n'est collectée. Les données sont collectées uniquement lorsqu'elles sont configurées en tant que telles dans le profil, et les données continuent d'être collectées lorsque le point de terminaison est connecté. Si la collecte est effectuée sur un réseau non approuvé, elle est mise en cache et envoyée au collecteur lorsque le point d'extrémité est sur un réseau approuvé. Le collecteur de flux Secure Network Analytics doit disposer d'une configuration supplémentaire pour traiter les flux mis en cache (voir Configurer le collecteur de flux pour les flux mis en cache hors réseau pour la configuration requise).

L'état du réseau approuvé peut être déterminé par la fonction TND du VPN (configuré dans le profil VPN) ou par la configuration TND du profil NVM :

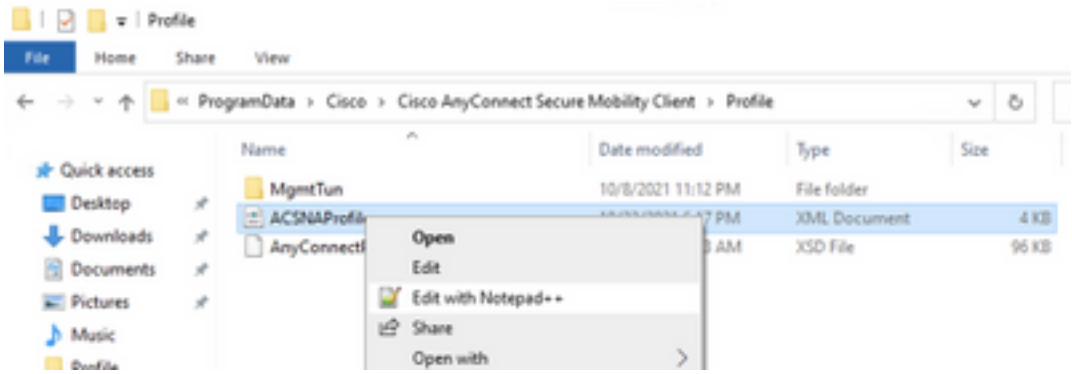
Configuration TND dans le profil VPN

Note: Il ne s'agit pas d'une option pour les déploiements autonomes NVM.

1. Localisez le profil VPN utilisé par le point de terminaison et confirmez les paramètres **de stratégie VPN automatique** configurés

   Emplacement du profil VPN :

- Fenêtres: **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile**
- Mac : **/opt/cisco/anyconnect/profile**
  Dans cet exemple, le profil VPN est nommé **ACSNAProfile**.



2. Modifiez le profil à l'aide d'un éditeur de texte et localisez l'élément **AutomaticVPNPolicy**. Assurez-vous que la stratégie configurée est correcte pour une détection réussie du réseau de confiance. Dans ce cas :

. . .

Note: Pour la pertinence NVM : si la stratégie de réseau approuvé et la stratégie de réseau non approuvé sont toutes deux définies sur Do Nothing, la détection de réseau approuvé du profil VPN est désactivée.

Configuration TND dans le profil NVM

Recherchez le profil NVM utilisé par le point de terminaison et vérifiez que les paramètres configurés de la **liste de serveurs approuvés** sont corrects.

Emplacement du profil NVM :

- Fenêtres: **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM**
- Mac : **/opt/cisco/anyconnect/nvm**

...

```
</NVMProfile>
```

Note: Une sonde SSL est envoyée à la tête de réseau de confiance configurée, qui répond avec un certificat, si accessible. L'empreinte numérique (hachage SHA-256) est ensuite extraite et mise en correspondance avec le jeu de hachages dans l'éditeur de profils. Une correspondance réussie signifie que le point de terminaison se trouve dans un réseau de confiance ; toutefois, si la tête de réseau est inaccessible ou si le hachage de certificat ne correspond pas, le point de terminaison est considéré comme se trouvant dans un réseau non fiable.

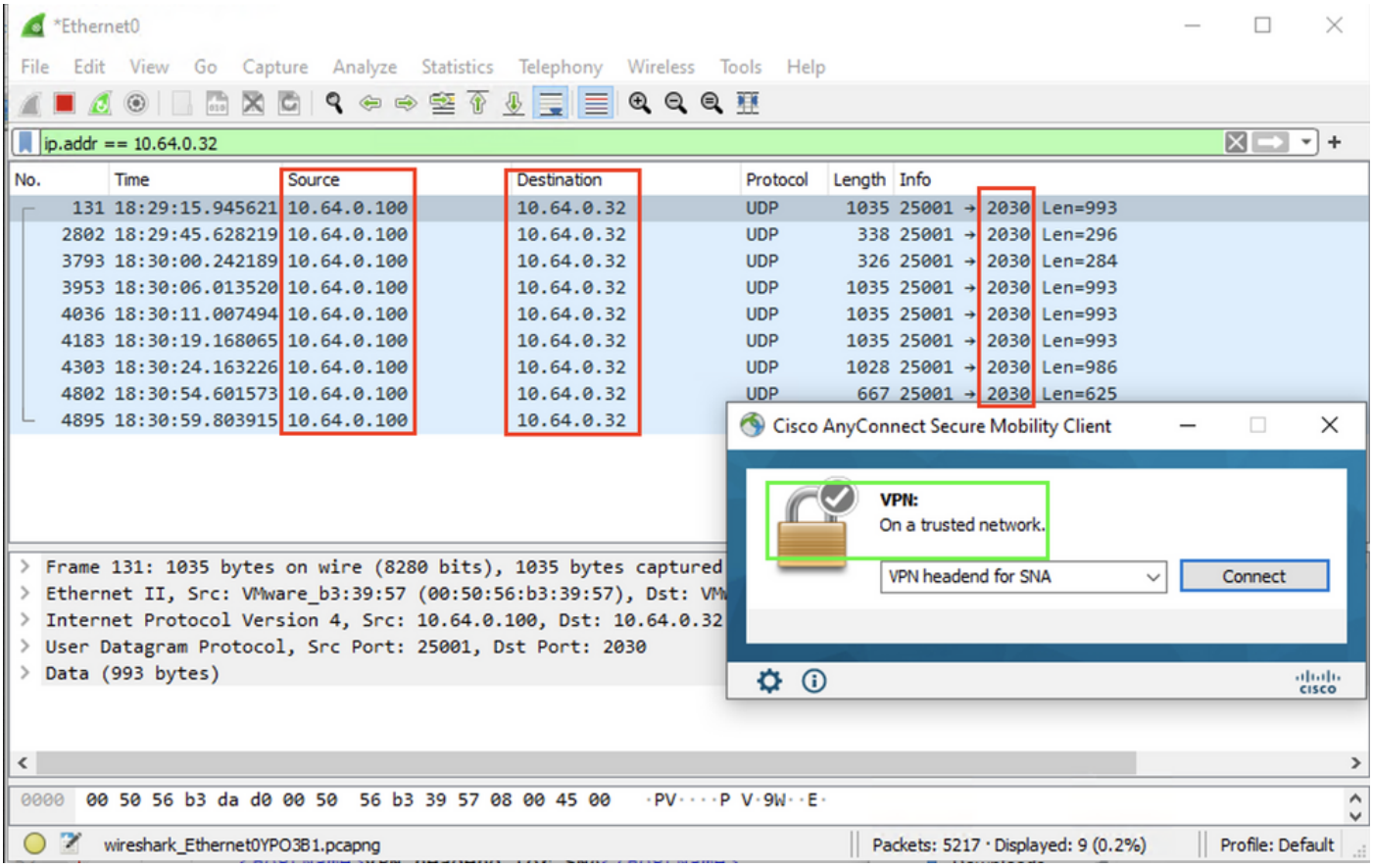
Note: Les serveurs approuvés derrière les serveurs proxy ne sont pas pris en charge.

Collecter les captures de paquets

Vous pouvez collecter une capture de paquets sur la carte réseau du point de terminaison pour vérifier que les flux sont envoyés au collecteur de flux.

a. Si le point de terminaison se trouve sur un réseau de confiance mais NON connecté au VPN, la capture doit être activée sur la carte réseau physique.

Dans ce cas, le client Anyconnect indique que le point de terminaison se trouve sur un réseau de confiance, ce qui signifie que les flux sont envoyés au collecteur de flux configuré sur le port configuré via l'adaptateur réseau physique du point de terminaison, comme nous pouvons le voir dans la fenêtre AnyConnect et la fenêtre Wireshark affichée ensuite.

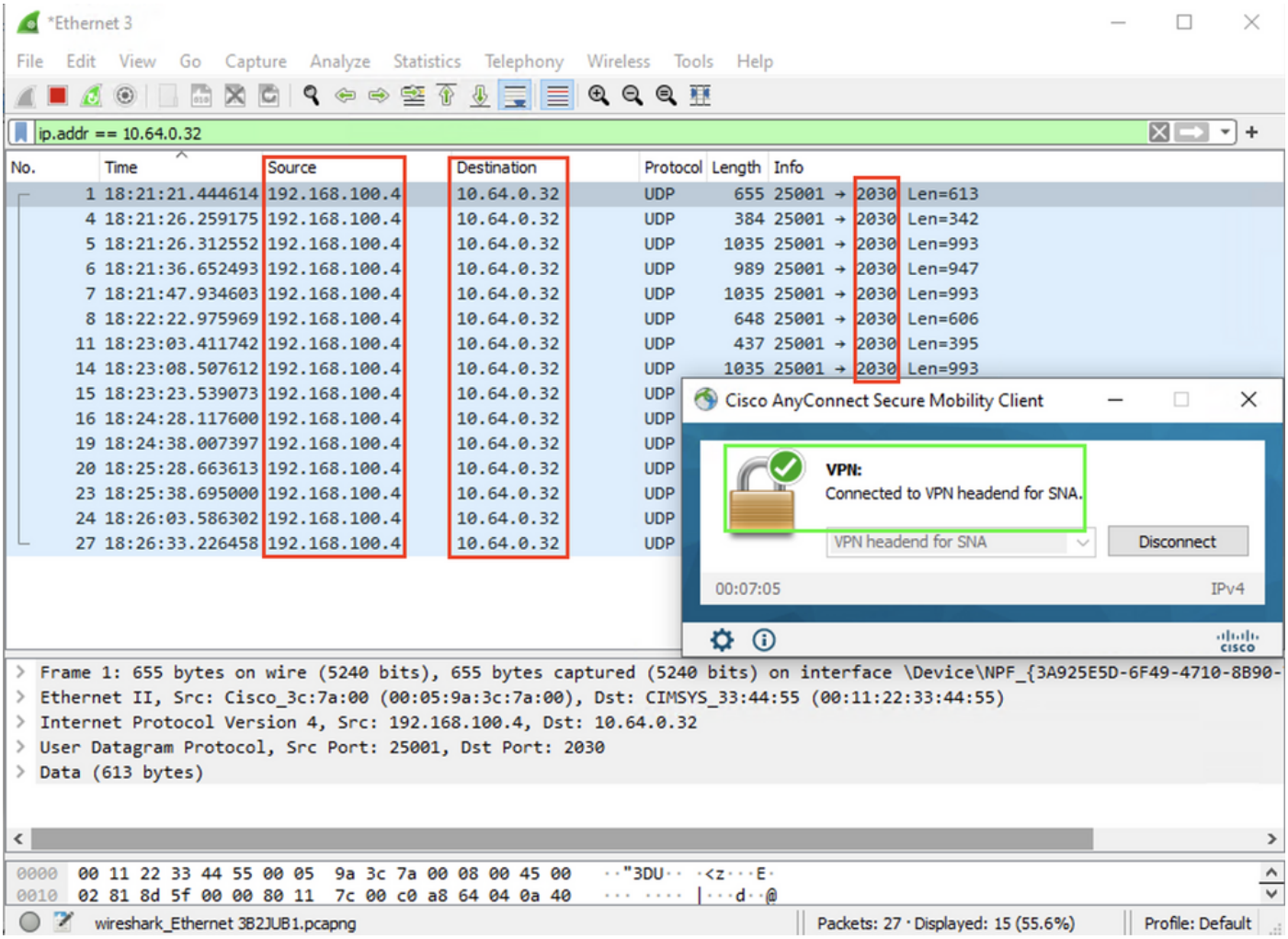


b. Si le point de terminaison est connecté à AnyConnect VPN, il est automatiquement considéré comme étant sur le réseau approuvé, par conséquent la capture doit être activée sur l'adaptateur réseau virtuel.

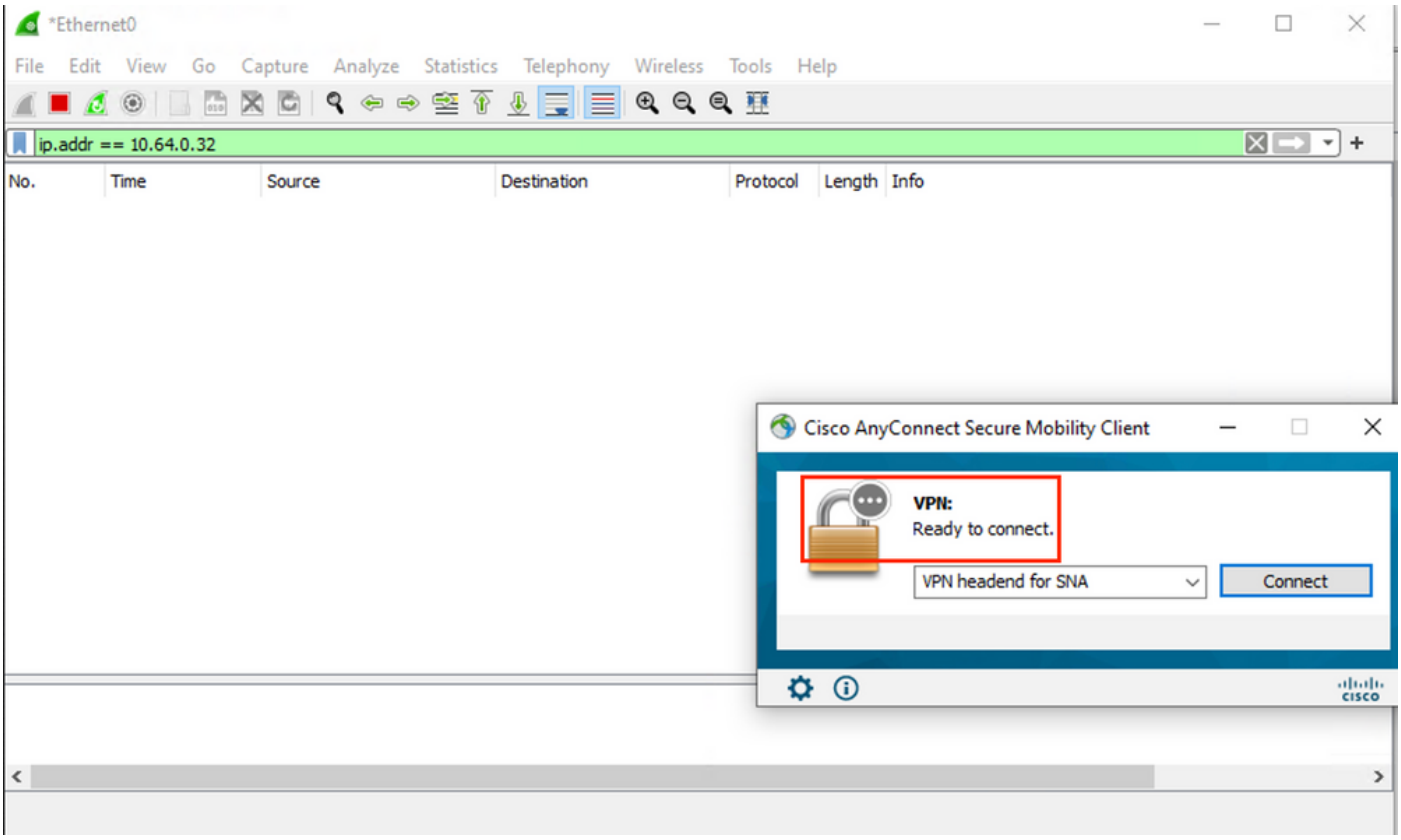
> **Note**: Si le module VPN est installé et que TND est configuré dans le profil du module de visibilité réseau, le module de visibilité réseau effectue une détection de réseau fiable même à l'intérieur du réseau VPN.

Le client AnyConnect indique que le point de terminaison est connecté au VPN, ce qui signifie que les flux sont envoyés au collecteur de flux configuré sur le port configuré via l'adaptateur réseau virtuel du point de terminaison (tunnel VPN), comme nous pouvons le voir dans la fenêtre AnyConnect et la fenêtre Wireshark affichée suivante.

> **Note**: La configuration du tunnel partagé du profil VPN auquel le point de terminaison est connecté doit inclure l'adresse IP du collecteur de flux, sinon les flux ne sont pas envoyés à travers le tunnel VPN.



c. Si le point de terminaison n'est pas sur un réseau de confiance, les flux ne sont pas envoyés au collecteur de flux.



Défauts associés

Il existe actuellement deux défauts connus qui peuvent affecter le processus d'entrée de données de télémétrie NVM sur Secure Network Analytics :

- Le moteur FC ne peut pas ingérer la télémétrie NVM sur eth1. Voir ID de bogue Cisco CSCwb84013
- Collecteur de flux n'insérant pas d'enregistrements NVM à partir de AnyConnect version 4.10.04071 ou ultérieure. Voir ID de bogue Cisco CSCwb91824

Informations connexes

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