Probleemoplossing met AnyConnect Network Visibility and Module: Telemetrie in beveiligde netwerkanalyses

Inhoud

Inleiding

In dit document wordt de procedure beschreven om NVM-telemetrie (Network Visibility Module) te implementeren in Secure Network Analytics (SNA).

Voorwaarden

- Cisco SNA-kennis
- Cisco AnyConnect-kennis

Configuratiehandleidingen

- Configuratie-gids voor Secure Network Analytics Endpoint License and Network Visibility Module (NVM)
- Cisco AnyConnect Administrator Guide netwerkzichtbaarheidsmodule, release 4.10

Vereisten

- SNA Manager en Flow Collector in versie 7.3.2 of nieuwer
- Licentie voor SNA Endpoint
- Cisco AnyConnect met netwerkzichtbaarheidsmodule 4.3 of nieuwer

Gebruikte componenten

- SNA Manager en Flow Collector, versie 7.4.0 en Endpoint Licentie
- Cisco AnyConnect 4.10.3104 met VPN en netwerkzichtbaarheidsmodule
- Windows 10 virtuele machine
- Software voor draadloos shark

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleemoplossing

SNA-configuratie

Controleer de licenties

Zorg ervoor dat de Smart Licensing Virtual-account waarop SNA Manager is geregistreerd, de Endpoint Licenties heeft.

Controleer de NVM-telemetrie-index

Om te bevestigen of de SNA Flow Collector NVM-telemetrie van de eindpunten ontvangt en plaatst, gaat u als volgt te werk:

1. Meld u aan bij de Flow Collector via SSH of console met basisreferenties.

2. Start de **grop 'NVM registreert deze periode:' /lancope/var/sw/today/logs/sw.log** opdracht.

3. bevestig of de Flow Collector NVM records inneemt en deze in de database plaatst.

```
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
```

Uit deze output blijkt dat de Flow Collector helemaal geen NVM-bestanden heeft ontvangen, maar u moet wel bevestigen of het is ingesteld om te luisteren voor NVM-telemetrie.

Controleer of de Flow Collector is ingesteld om te luisteren naar NVM-telemetrie

1. Meld u aan bij de Flow Collector Admin User Interface (UI).

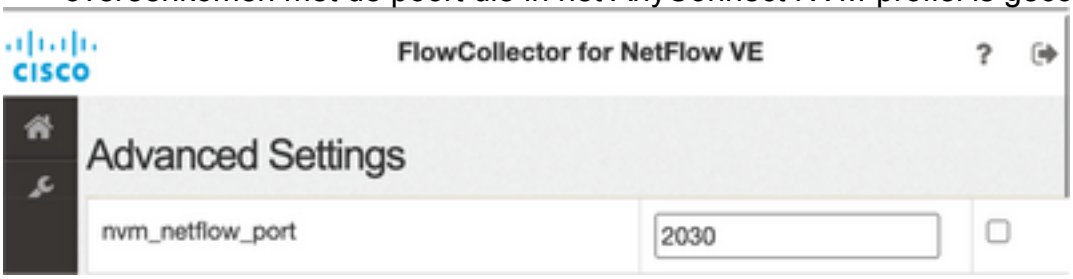
2. Navigeer naar **Ondersteuning > Geavanceerde instellingen**.

3. Zorg ervoor dat de vereiste eigenschappen correct zijn geconfigureerd:

SNA versie 7.3.2 of 7.4.0

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

- Pak de **nvm_netflow_port** eigenschap vast en controleer de geconfigureerde waarde. Dit moet overeenkomen met de poort die in het AnyConnect NVM-profiel is geconfigureerd.



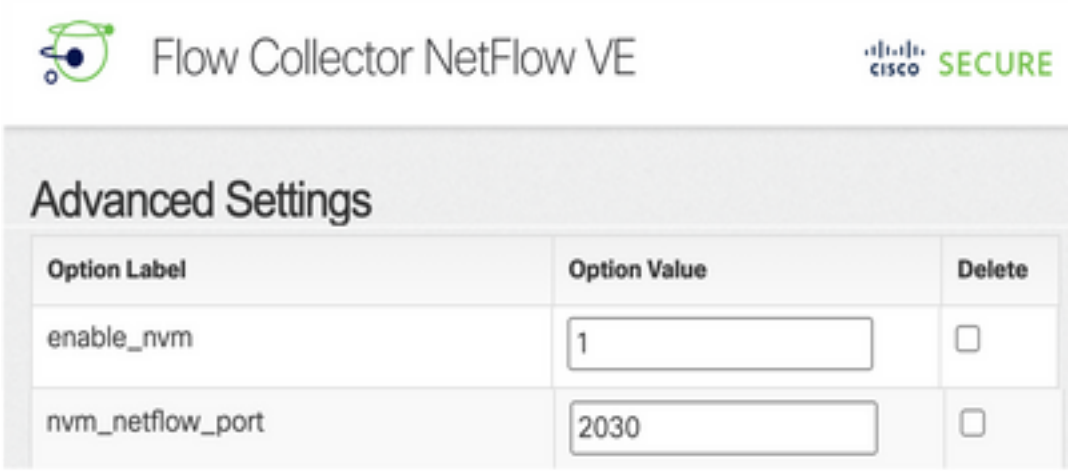
> **Opmerking**: Zorg ervoor dat de geconfigureerde poort een niet-gereserveerde poort is en niet 2055, 514 of 8514. Als de ingestelde waarde "0" is, wordt de optie uitgeschakeld.

> **N.B.**: Als een veld niet wordt weergegeven, scrollen we naar de onderkant van de pagina. Klik op het veld **Nieuwe optie toevoegen**. Raadpleeg voor meer informatie over geavanceerde instellingen in de Flow Collector het online Help-onderwerp Geavanceerde instellingen.

SNA versie 7.4.1

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

- Pak de **nvm_netflow_port** eigenschap vast en controleer de geconfigureerde waarde. Dit moet overeenkomen met de poort die in het AnyConnect NVM-profiel is geconfigureerd.
- Pak de eigenschap **Enable_nvm vast** en zorg ervoor dat de waarde is ingesteld op **1**, anders wordt de functie uitgeschakeld.



Opmerking: Zorg ervoor dat de geconfigureerde poort een niet-gereserveerde poort is en niet 2055, 514 of 8514.

N.B.: Als een veld niet wordt weergegeven, scrollen we naar de onderkant van de pagina. Klik op het veld **Nieuwe optie toevoegen**. Raadpleeg voor meer informatie over geavanceerde instellingen in de Flow Collector het online Help-onderwerp Geavanceerde instellingen.

4. Controleer, zodra de geavanceerde instellingen op de Flow Collector correct zijn geconfigureerd, of de telemetrie nu wordt opgenomen, met dezelfde procedure als in het gedeelte **Controleer NVM Telemetry Ingest**.

5. Als de configuratie van het eindpunt met AnyConnect NVM en de instellingen op de Flow Collector juist zijn, moet het **sw.log**-bestand het volgende weergeven:

```
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. Als de Flow Collector nog steeds geen NVM-gegevens inneemt, controleert u of de verzamelaar de pakketten op de interface ontvangt en in ieder geval of de configuratie van de eindpunten juist is.

Endpoint configuratie

U kunt AnyConnect NVM op twee manieren implementeren: a) wmet het AnyConnect-pakket of b)Met het Standalone NVM-pakket (alleen op AnyConnect-desktop).

De gewenste configuratie is hetzelfde voor beide implementaties, het verschil is aanwezig in de configuratie van Trusted Network Detectie.

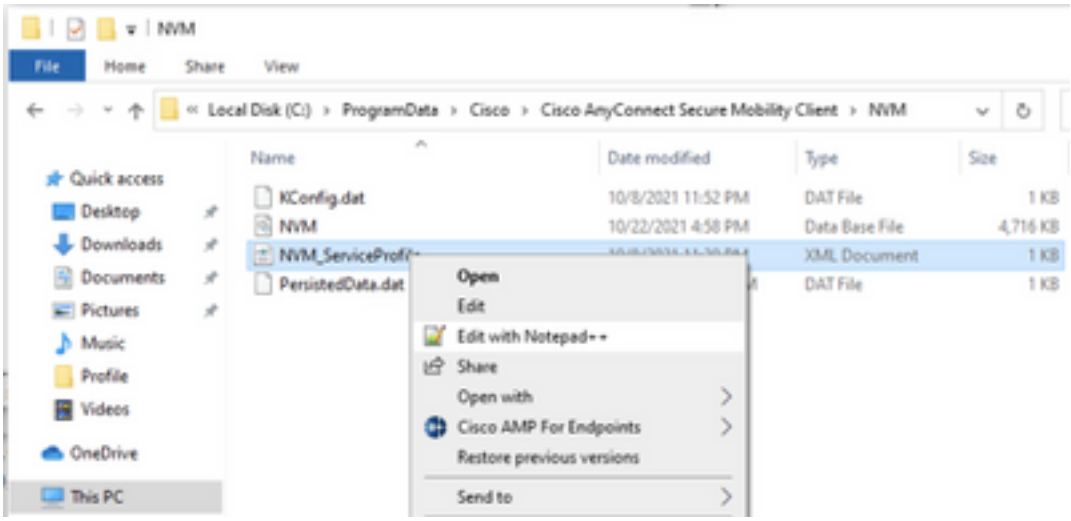
Controleer NVM-profiel

Zoek het NVM Profile dat door het eindpunt wordt gebruikt en bevestig de **Collector Configuration**-instellingen.

NVM-profiel:

- Windows: **%Program Data%\Cisco AnyConnect Secure Mobility Client\NVM**
- Mac: **/opt/cisco/anyconnect/nvm**

Opmerking: De naam van het NVM-profiel moet **NVM_ServiceProfile** zijn, anders worden er geen gegevens verzameld en verzonden door Network Visibility Module.



De inhoud van het NVM-profiel hangt af van uw configuratie, maar de elementen van het profiel die relevant zijn voor SNA worden vet weergegeven. Zorg ervoor dat de opmerkingen na het voorbeeld van het NVM-profiel worden bekeken:

Opmerking: Zorg ervoor dat de **geconfigureerde poort een niet-gereserveerde poort is en niet 2055, 514 of 8514**. De geconfigureerde poort in dit profiel moet dezelfde zijn als de poort die in de Flow Collector is ingesteld.

Opmerking: Zorg ervoor dat als het NVM Profile het **Secure** XML-element heeft, het op **vals**

is ingesteld, anders worden de stromen versleuteld met DTLS en kan de Flow Collector ze niet verwerken.

Controleer de TND-instellingen (Trusted Network Detection)

De Network Visibility Module stuurt alleen stroominformatie als deze op het vertrouwde netwerk is aanwezig. Standaard worden geen gegevens verzameld. Er worden alleen gegevens verzameld wanneer deze als zodanig in het profiel zijn geconfigureerd en de gegevens blijven verzameld worden wanneer het eindpunt is verbonden. Als de collectie op een onbetrouwbaar netwerk wordt gedaan, wordt het gecached en naar de verzamelaar gestuurd wanneer het eindpunt op een vertrouwd netwerk is. De Secure Network Analytics Flow Collector moet beschikken over een extra configuratie voor het verwerken van gecacheerde stromen (zie het configureren van de Flow Collector voor buiten het netwerk gecompileerde stromen voor de benodigde configuratie).

De vertrouwde netwerkstatus kan worden bepaald door de TND-functie van VPN (geconfigureerd in het VPN-profiel) of door de TND-configuratie in het NVM-profiel:

TND-configuratie in VPN-profiel

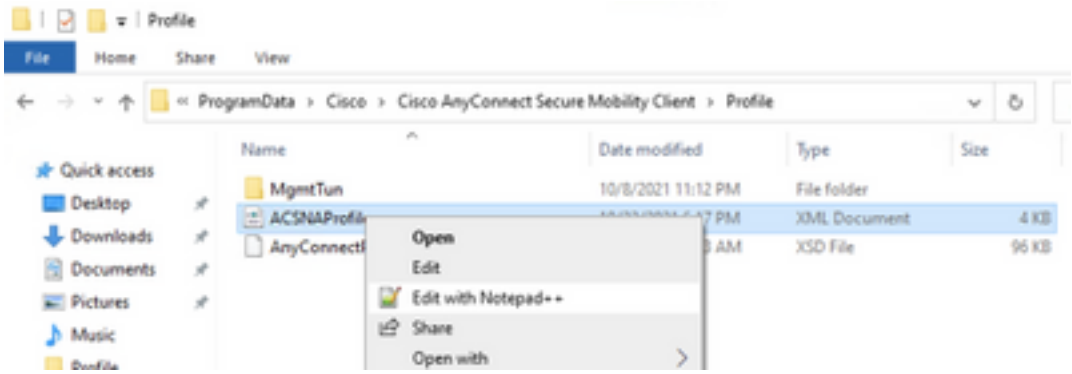
Opmerking: Dit is geen optie voor standalone NVM-implementaties.

1. Pak het VPN-profiel vast dat door het eindpunt wordt gebruikt en bevestig de geconfigureerde **automatische VPN-**beleidsinstellingen

VPN-profiellocatie:

- Windows: **%Program Data%\Cisco AnyConnect Secure Mobility Client\Profile**
- Mac: **/opt/cisco/anyconnect/profile**

In dit voorbeeld wordt het VPN-profiel **ACSNAProfile** genoemd.



2. Bewerk het profiel met een teksteditor en plaats het beleidselement **Automatisch** uitvoeren. Zorg ervoor dat het geconfigureerde beleid correct is voor het met succes detecteren van het Trusted Network. In dat geval:

. . .

Opmerking: Voor NVM-relevantie: Als zowel het Trusted Network Policy als het Onvertrouwde netwerkbeleid zijn ingesteld op Niets doen, wordt de vertrouwde netwerkdetectie van het VPN-profiel uitgeschakeld.

TND-configuratie in NVM-profiel

Zoek het NVM profiel dat door het eindpunt wordt gebruikt en bevestig dat de geconfigureerde **Trusted Server List** instellingen correct zijn.

NVM-profiel:

- Windows: **%Program Data%\Cisco AnyConnect Secure Mobility Client\NVM**
- Mac: **/opt/cisco/anyconnect/nvm**

...

```
</NVMProfile>
```

Opmerking: Een SSL sonde wordt naar het gevormde vertrouwde head-end verzonden, dat met een certificaat reageert indien bereikbaar. De thumbprint (SHA-256 shash) wordt dan geëxtraheerd en afgesloten tegen de hash die in de profieleditor is ingesteld. Een succesvolle match betekent dat het eindpunt in een betrouwbaar netwerk ligt. als het head-end echter onbereikbaar is of als de certificaathash niet overeenkomt, wordt het eindpunt geacht in een onbetrouwbaar netwerk te liggen.

Opmerking: Trusted servers achter proxy's worden niet ondersteund.

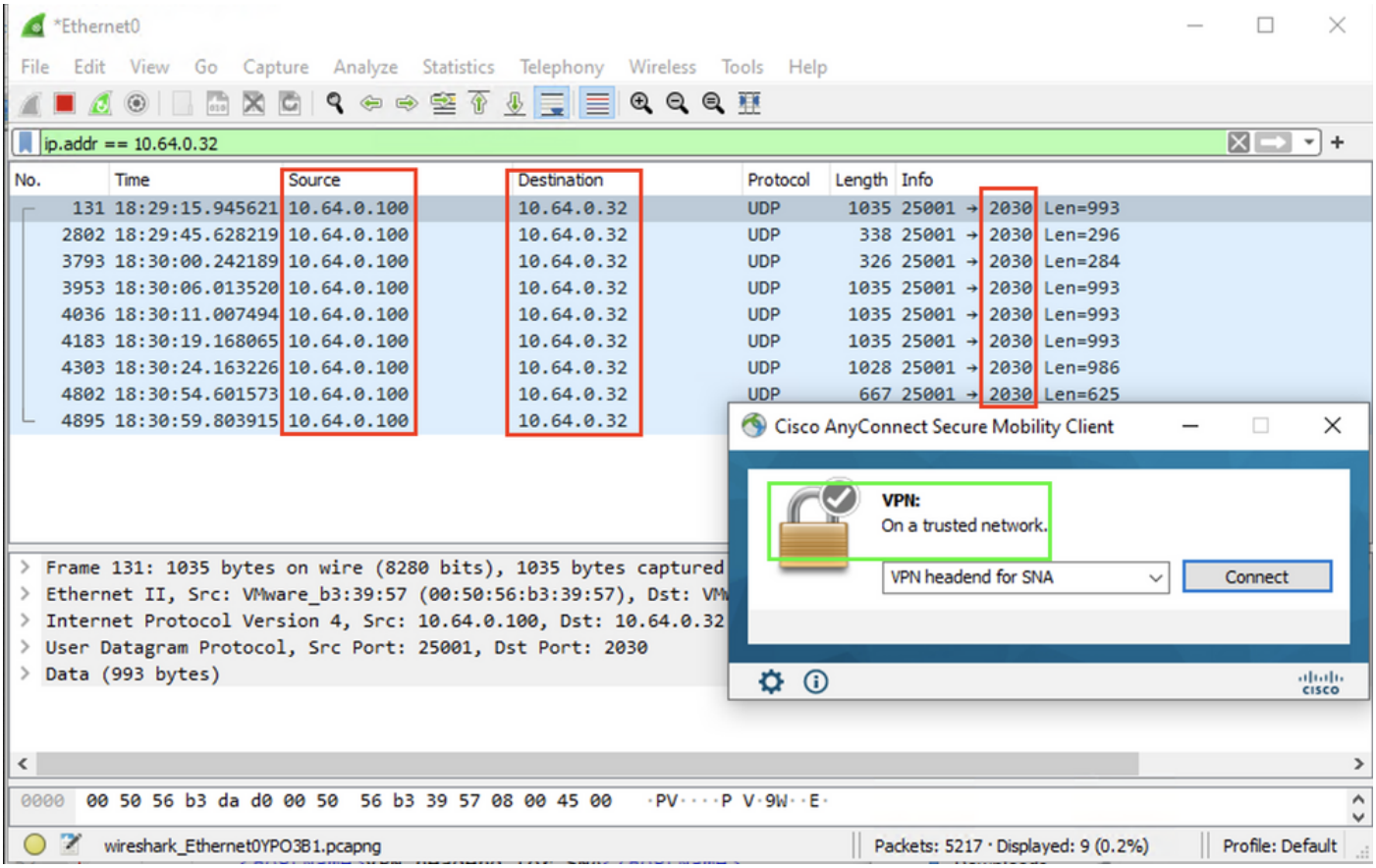
Verzamelen van pakketvastlegging

U kunt een pakketvastlegging op de netwerkadapter van Endpoint verzamelen om te controleren

of de stromen naar de Flow Collector worden verzonden.

a. Als het Endpoint op een Trusted Network is aangesloten maar NIET op VPN is aangesloten, moet de opname op de fysieke netwerkadapter zijn ingeschakeld.

In dit geval geeft de AnyConnect-client aan dat het eindpunt op een betrouwbaar netwerk is gelegen, wat betekent dat de stromen naar de geconfigureerde Flow Collector via de geconfigureerde poort worden verzonden door de Physical Network Adapter van het eindpunt, zoals we in het AnyConnect-venster en het venster Wireshark hierna kunnen zien.

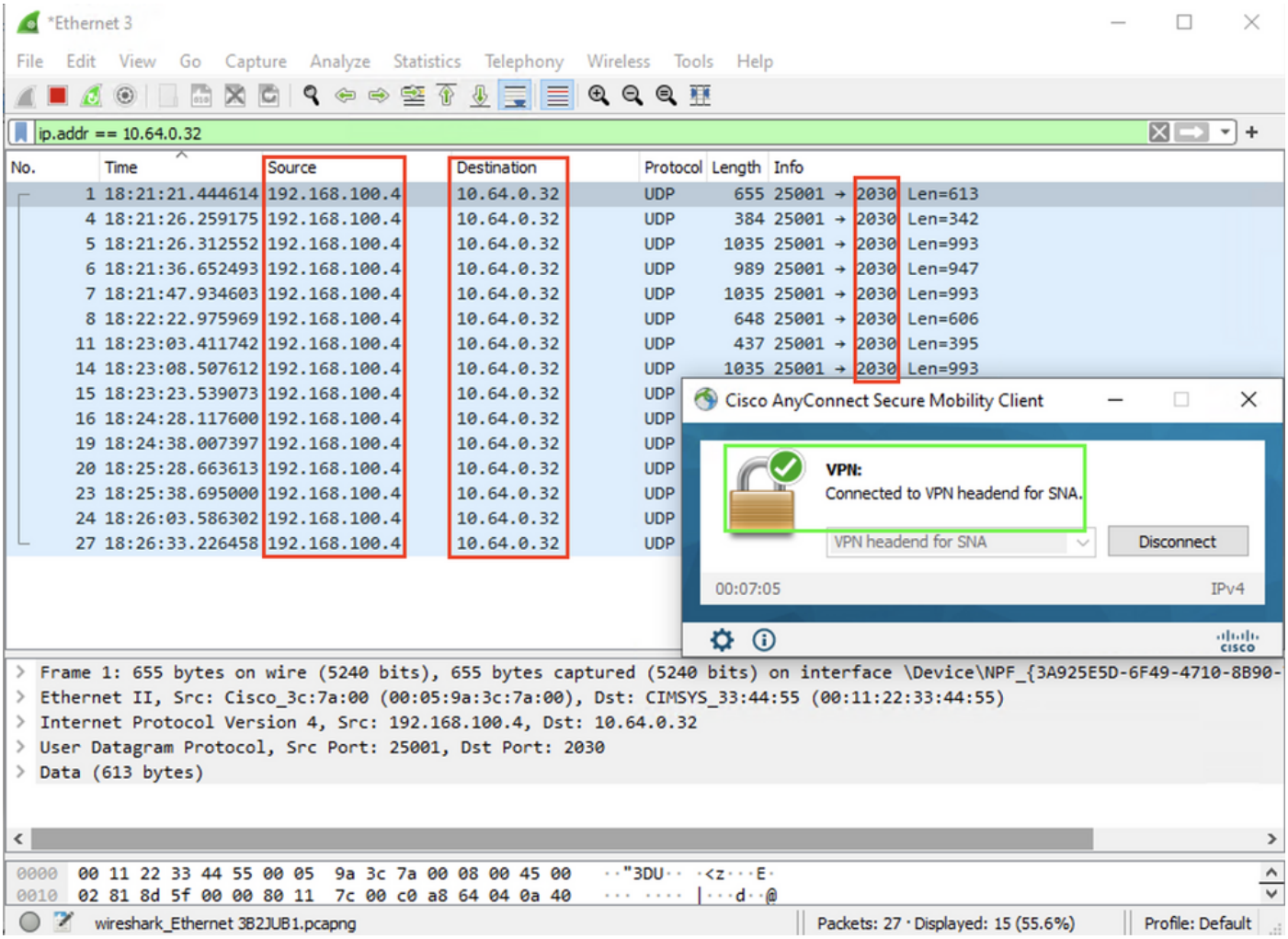


b. Als het Endpoint is verbonden met AnyConnect VPN wordt het automatisch geacht op het Trusted Network te zijn geïnstalleerd en moet de opname daarom op de Virtual Network Adapter zijn ingeschakeld.

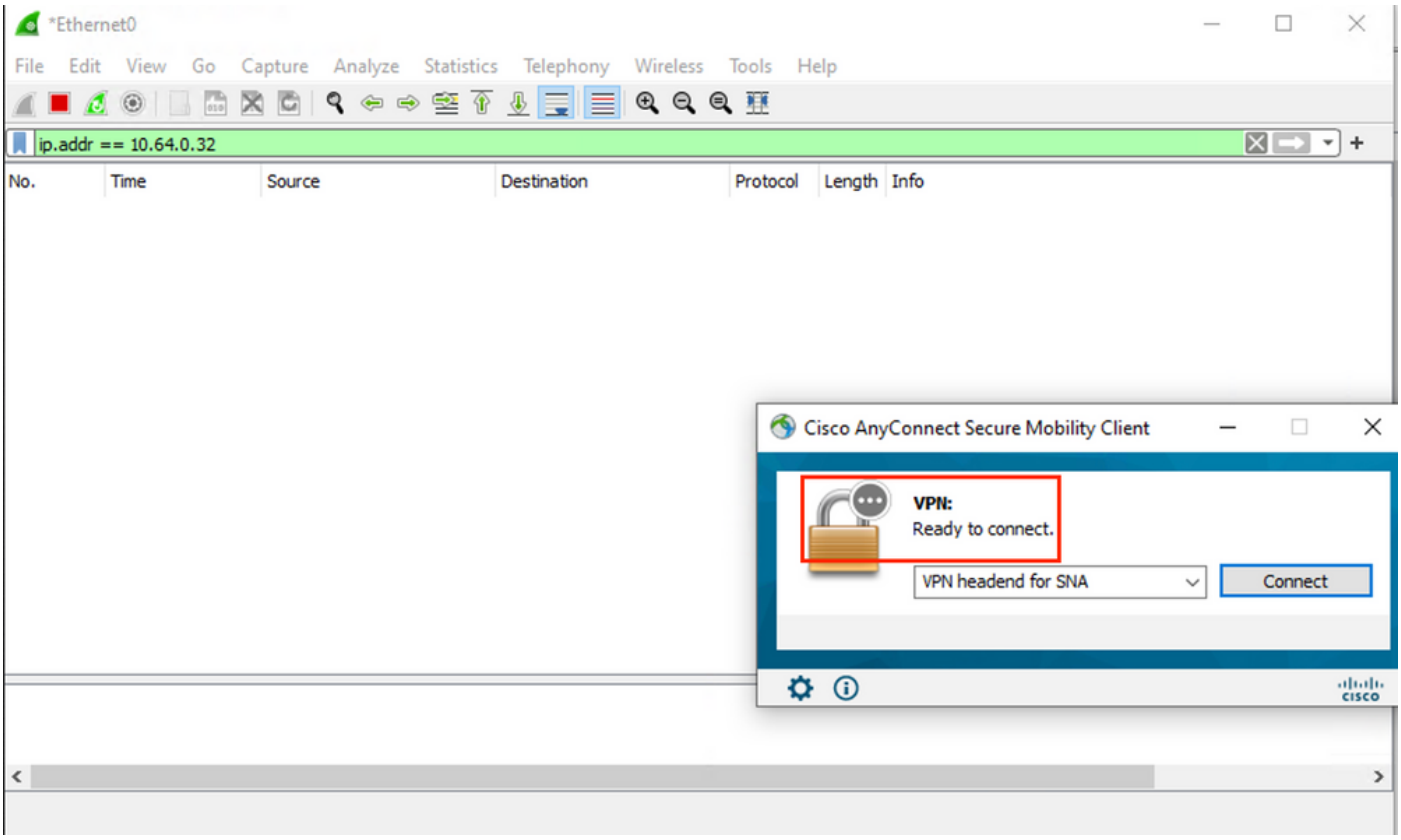
> **Opmerking:** Als de VPN-module is geïnstalleerd en TND is geconfigureerd in het profiel van Netwerkzichtbaarheidsmodule, dan voert de netwerkzichtbaarheidsmodule een betrouwbare netwerkdetectie uit, zelfs in het VPN-netwerk.

De AnyConnect-client geeft aan dat het eindpunt met VPN is verbonden, wat betekent dat de stromen naar de geconfigureerde Flow Collector via de geconfigureerde poort worden verzonden door de Virtual Network Adapter of the Endpoint (VPN-tunnelheid), zoals we in het AnyConnect-venster en het Wireshark-venster hieronder kunnen zien.

> **Opmerking:** De configuratie van de Split-tunnelconfiguratie van het VPN-profiel dat het Endpoint is verbonden met inbegrip van het IP-adres van de Flow Collector, anders worden de stromen niet over de VPN-tunnel verzonden.



c. Als het Endpoint niet op een betrouwbaar netwerk is, worden er geen stromen naar de Flow Collector verzonden.



Verwante tekortkomingen

Er zijn momenteel twee bekende defecten die van invloed kunnen zijn op het ingeslikte NVM-telemetrie-proces bij Secure Network Analytics:

- FC Engine kan NVM-telemetrie niet op eth1 innemen. Zie Cisco bug-id CSCwb84013
- Flow Collector voegt geen NVM records in vanaf AnyConnect versie 4.10.04071 of hoger. Zie Cisco bug-id CSCwb91824

Gerelateerde informatie

- Voor extra hulp kunt u contact opnemen met het Technical Assistance Center (TAC). Een geldig ondersteuningscontract is vereist: Cisco's wereldwijde contactgegevens voor ondersteuning.
- U kunt hier ook de Cisco Security Analytics-community bezoeken.
- Technische ondersteuning en documentatie – Cisco Systems