Fehlerbehebung bei Telemetrie-Installationsproblemen des AnyConnect Network Visibility Module in der sicheren Netzwerkanalyse

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zur Fehlerbehebung bei NVM-Telemetriedaten (Network Visibility Module) in Secure Network Analytics (SNA) beschrieben.

Voraussetzungen

- Kenntnisse zu Cisco SNA
- Cisco AnyConnect

Konfigurationsanleitungen

- Konfigurationsleitfaden für Secure Network Analytics Endpoint License and Network Visibility Module (NVM)
- Cisco AnyConnect Administrator Guide Network Visibility Module, Version 4.10

Anforderungen

- SNA Manager und Flow Collector ab Version 7.3.2
- SNA Endpoint-Lizenz
- Cisco AnyConnect mit Network Visibility Module 4.3 oder höher

Verwendete Komponenten

- SNA Manager und Flow Collect Version 7.4.0 und Endpoint-Lizenz
- Cisco AnyConnect 4.10.03104 mit VPN und Network Visibility-Modul
- Virtuelles Windows 10-System
- Wireshark-Software

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Fehlerbehebungsprozess

SNA-Konfiguration

Lizenzierung überprüfen

Stellen Sie sicher, dass das virtuelle Smart Licensing-Konto, bei dem der SNA Manager registriert ist, über Endgerätelizenzen verfügt.

Überprüfen der NVM-Telemetrieingabe

So prüfen Sie, ob der SNA Flow Collector NVM-Telemetrie von den Endgeräten empfängt und einfügt:

1. Melden Sie sich über SSH oder die Konsole mit **Root-**Anmeldeinformationen beim Flow Collector an.

2. Führen Sie den Befehl **grep 'NVM record this period:' /lancope/var/sw/today/logs/sw.log aus**.

3. Überprüfen Sie anhand der zurückgegebenen Ausgabe, ob Flow Collector NVM-Datensätze einfügt und in die Datenbank einfügt.

```
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
```

Aus dieser Ausgabe scheint es, dass Flow Collector keinerlei NVM-Datensätze erhalten hat. Sie müssen jedoch bestätigen, ob es für die Überwachung der NVM-Telemetrie konfiguriert ist.

Überprüfen Sie, ob Flow Collector für die Überwachung von NVM-Telemetrie konfiguriert ist.

1. Melden Sie sich bei der Flow Collector Admin User Interface (UI) an.

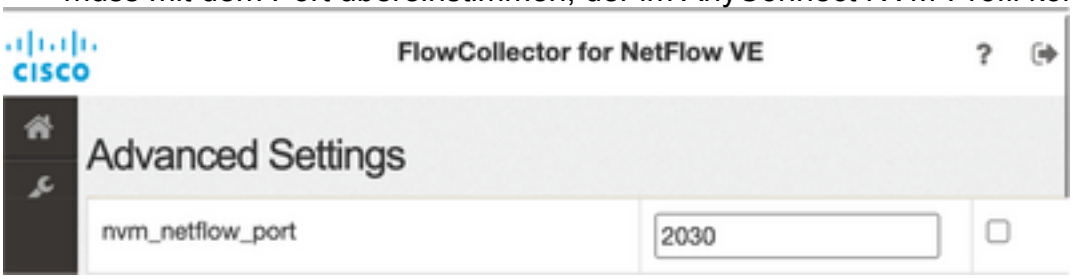
2. Navigieren Sie zu **Support > Erweiterte Einstellungen**.

3. Stellen Sie sicher, dass die erforderlichen Attribute korrekt konfiguriert sind:

SNA Version 7.3.2 oder 7.4.0

==========

- Suchen Sie das Attribut **nvm_netflow_port**, und überprüfen Sie den konfigurierten Wert. Dies muss mit dem Port übereinstimmen, der im AnyConnect NVM-Profil konfiguriert wurde.



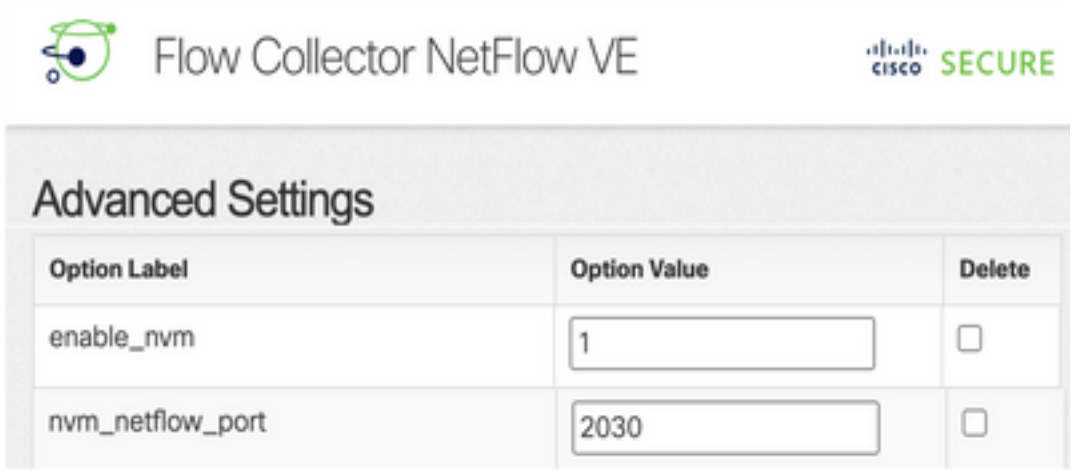
Hinweis: Stellen Sie sicher, dass der konfigurierte Port ein nicht reservierter Port ist und nicht 2055, 514 oder 8514 ist. Wenn der konfigurierte Wert "0" lautet, ist die Funktion deaktiviert.

Hinweis: Wenn kein Feld angezeigt wird, blättern Sie zum Ende der Seite. Klicken Sie auf das Feld **Neue Option hinzufügen**. Weitere Informationen zu erweiterten Einstellungen auf Flow Collector finden Sie im Online-Hilfethema Erweiterte Einstellungen.

SNA Version 7.4.1

==========

- Suchen Sie das Attribut **nvm_netflow_port**, und überprüfen Sie den konfigurierten Wert. Dies muss mit dem Port übereinstimmen, der im AnyConnect NVM-Profil konfiguriert wurde.
- Suchen Sie das **enable_nvm-**Attribut, und stellen Sie sicher, dass der Wert auf **1** festgelegt ist, andernfalls wird das Feature deaktiviert.



Hinweis: Stellen Sie sicher, dass der konfigurierte Port ein nicht reservierter Port ist und nicht 2055, 514 oder 8514 ist.

Hinweis: Wenn kein Feld angezeigt wird, blättern Sie zum Ende der Seite. Klicken Sie auf das Feld **Neue Option hinzufügen**. Weitere Informationen zu erweiterten Einstellungen auf Flow Collector finden Sie im Online-Hilfethema Erweiterte Einstellungen.

4. Nachdem die erweiterten Einstellungen für Flow Collector korrekt konfiguriert wurden, überprüfen Sie, ob die Telemetrie nun mit dem gleichen Verfahren wie im Abschnitt **Verify NVM Telemetry Ingest (NVM-Telemetrieingaben verifizieren**) integriert ist.

5. Wenn die Konfiguration des Endpunkts mit AnyConnect NVM und die Einstellungen für Flow Collector korrekt sind, muss die Datei **sw.log** Folgendes enthalten:

```
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. Wenn Flow Collector immer noch keine NVM-Datensätze erfasst, überprüfen Sie, ob der Collector die Pakete auf der Schnittstelle empfängt, und stellen Sie in jedem Fall sicher, dass die Konfiguration der Endpunkte korrekt ist.

Endgerätekonfiguration

Sie können AnyConnect NVM auf zwei Arten bereitstellen: a) wmit dem AnyConnect-Paket oder b) wmit dem eigenständigen NVM-Paket (nur auf AnyConnect-Desktop).

Die erforderliche Konfiguration ist für beide Bereitstellungen identisch. Der Unterschied liegt in der Konfiguration der Erkennung vertrauenswürdiger Netzwerke.

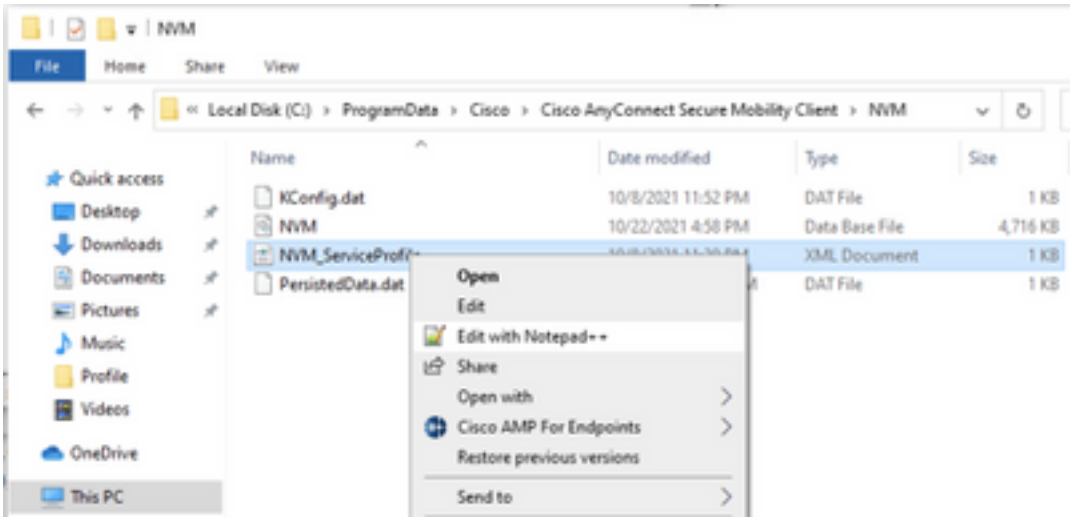
NVM-Profil überprüfen

Suchen Sie das vom Endpunkt verwendete NVM-Profil, und bestätigen Sie die **Collector-**Konfigurationseinstellungen.

Speicherort des NVM-Profils:

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

Anmerkung: Der Name des NVM-Profils muss **NVM_ServiceProfile** sein, da das Network Visibility Module keine Daten erfassen und senden kann.



Der Inhalt des NVM-Profils hängt von Ihrer Konfiguration ab. Die für SNA relevanten Elemente des Profils sind jedoch fett markiert. Überprüfen Sie die Hinweise nach dem NVM-Profilbeispiel:

Anmerkung: Stellen Sie sicher, dass der **konfigurierte Port ein nicht reservierter Port ist und nicht 2055, 514 oder 8514 ist**. Der konfigurierte Port in diesem Profil muss mit dem auf dem FlowCollector konfigurierten Port identisch sein.

Anmerkung: Stellen Sie sicher, dass das NVM-Profil das **Secure** XML-Element aufweist, es auf **false** festgelegt ist, andernfalls werden die Datenflüsse mit DTLS verschlüsselt gesendet, und der Flow Collector kann sie nicht verarbeiten.

Überprüfen der TND-Einstellungen (Trusted Network Detection)

Das Network Visibility-Modul sendet Flow-Informationen nur im vertrauenswürdigen Netzwerk. Standardmäßig werden keine Daten gesammelt. Daten werden nur erfasst, wenn sie als solche im Profil konfiguriert sind, und die Daten werden weiter erfasst, wenn der Endpunkt verbunden ist. Wenn die Erfassung in einem nicht vertrauenswürdigen Netzwerk erfolgt, wird sie zwischengespeichert und an den Collector gesendet, wenn sich der Endpunkt in einem vertrauenswürdigen Netzwerk befindet. Der Secure Network Analytics Flow Collector benötigt eine

zusätzliche Konfiguration für die Verarbeitung zwischengespeicherter Datenflüsse (siehe Konfigurieren des Flow Collectors für außerhalb des Netzwerks gespeicherte Datenflüsse für die erforderliche Konfiguration).

Der Status eines vertrauenswürdigen Netzwerks kann durch die TND-Funktion des VPN (konfiguriert im VPN-Profil) oder durch die TND-Konfiguration im NVM-Profil bestimmt werden:

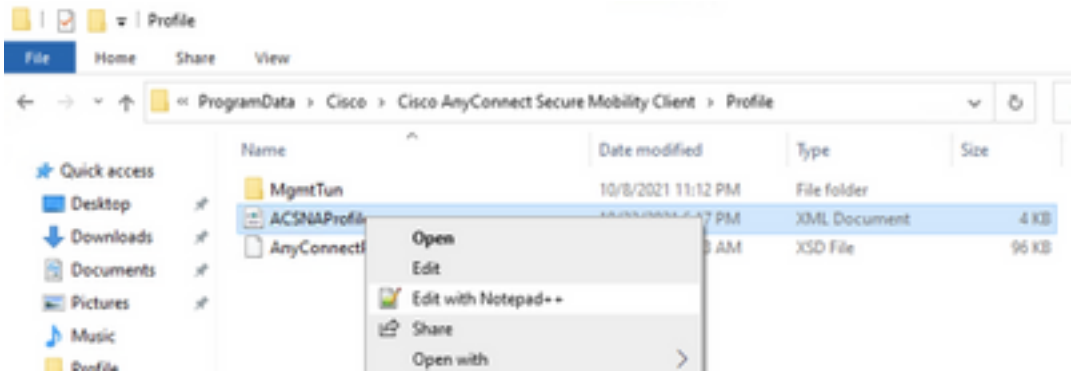
TND-Konfiguration in VPN-Profil

Anmerkung: Dies ist keine Option für eigenständige NVM-Bereitstellungen.

1. Suchen Sie das vom Endpunkt verwendete VPN-Profil, und bestätigen Sie die konfigurierten Einstellungen für **automatische VPN-Richtlinien.**

Standort des VPN-Profils:

- Windows: **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile**
- Mac: **/opt/cisco/anyconnect/profile**
  In diesem Beispiel trägt das VPN-Profil den Namen **ACSNAProfile**.



2. Bearbeiten Sie das Profil mit einem Text-Editor, und suchen Sie das **AutomaticVPNPolicy-**Element. Stellen Sie sicher, dass die konfigurierte Richtlinie korrekt ist, um das vertrauenswürdige Netzwerk erfolgreich erkennen zu können. In diesem Fall:

. . .

Anmerkung: Für NVM-Relevanz: Wenn sowohl die Trusted Network Policy als auch die UnTrusted Network Policy (Vertrauenswürdige Netzwerkrichtlinie) auf Do Nothing (Nichts tun) festgelegt sind, wird die Erkennung vertrauenswürdiger Netzwerke aus dem VPN-Profil deaktiviert.

TND-Konfiguration im NVM-Profil

Suchen Sie das vom Endpunkt verwendete NVM-Profil, und überprüfen Sie, ob die konfigurierten Einstellungen für die **Liste vertrauenswürdiger Server** korrekt sind.

Speicherort des NVM-Profils:

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

...

```
</NVMProfile>
```

Anmerkung: Eine SSL-Anfrage wird an das konfigurierte vertrauenswürdige Headend gesendet, das mit einem Zertifikat antwortet, wenn es erreichbar ist. Der Daumenabdruck (SHA-256-Hash) wird extrahiert und dem Hashsatz im Profil-Editor zugeordnet. Eine erfolgreiche Übereinstimmung bedeutet, dass sich der Endpunkt in einem vertrauenswürdigen Netzwerk befindet. Wenn das Headend jedoch nicht erreichbar ist oder der Zertifikats-Hash nicht übereinstimmt, gilt der Endpunkt als in einem nicht vertrauenswürdigen Netzwerk.

Anmerkung: Vertrauenswürdige Server hinter Proxys werden nicht unterstützt.

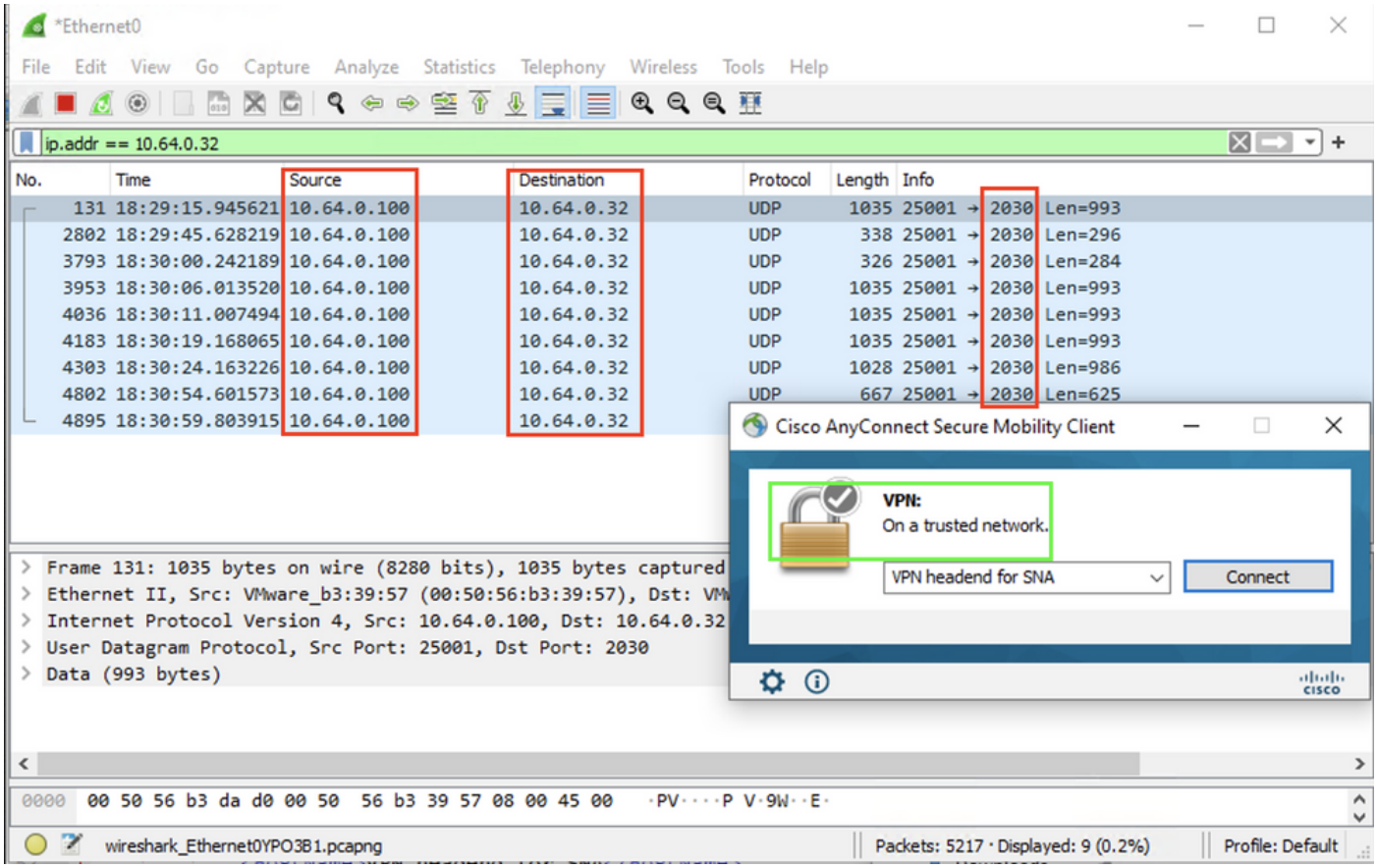
Paketerfassung erfassen

Sie können eine Paketerfassung auf dem Endpunkt-Netzwerkadapter sammeln, um zu überprüfen, ob Datenflüsse an Flow Collector gesendet werden.

antwort: Wenn sich der Endpunkt in einem vertrauenswürdigen Netzwerk befindet, aber NICHT mit dem VPN verbunden ist, muss die Erfassung auf dem physischen Netzwerkadapter aktiviert sein.

In diesem Fall gibt der AnyConnect-Client an, dass sich der Endpunkt in einem vertrauenswürdigen Netzwerk befindet. Dies bedeutet, dass die Datenflüsse über den konfigurierten Port über den physischen Netzwerkadapter des Endpunkts an den konfigurierten Flow Collector gesendet werden, wie im AnyConnect-Fenster und im nächsten Fenster von

Wireshark zu sehen ist.

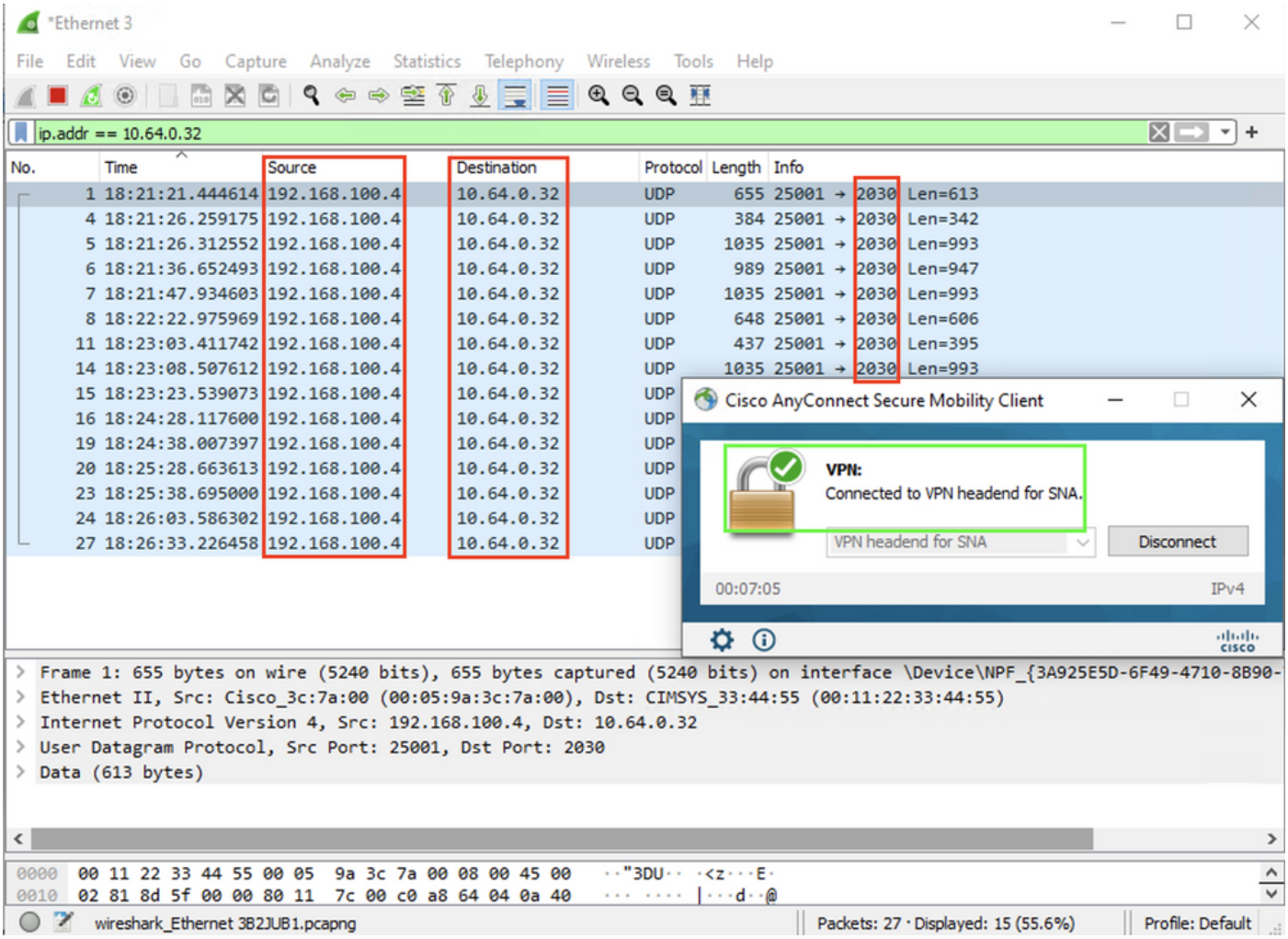


b. Wenn der Endpunkt mit AnyConnect VPN verbunden ist, wird er automatisch als im vertrauenswürdigen Netzwerk registriert. Daher muss die Erfassung auf dem virtuellen Netzwerkadapter aktiviert werden.

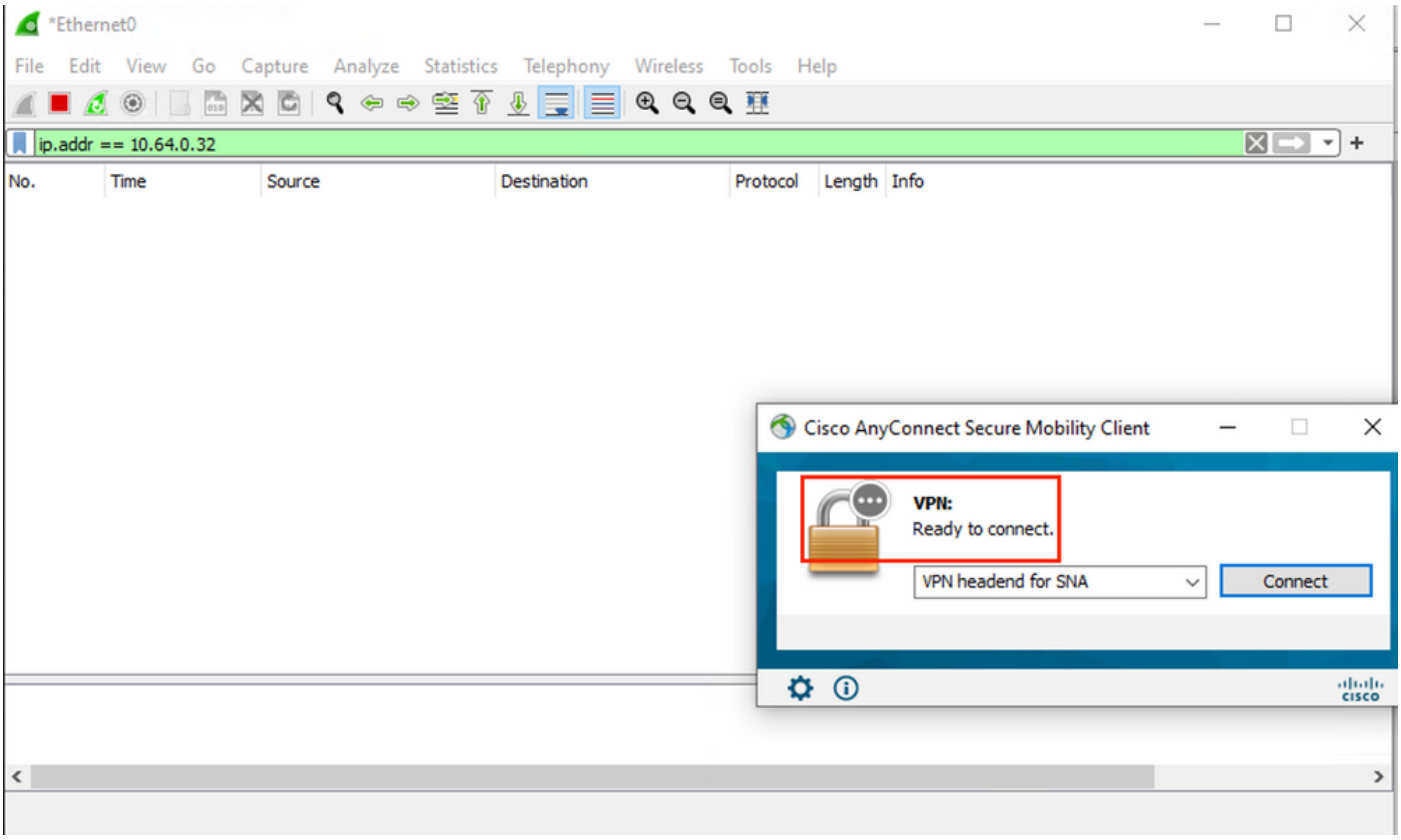
> **Anmerkung:** Wenn das VPN-Modul installiert ist und TND im Netzwerktransparenzmodul-Profil konfiguriert ist, führt das Network Visibility Module die Erkennung vertrauenswürdiger Netzwerke auch innerhalb des VPN-Netzwerks durch.

Der AnyConnect-Client gibt an, dass der Endpunkt mit dem VPN verbunden ist. Dies bedeutet, dass die Datenflüsse über den konfigurierten Port über den virtuellen Netzwerkadapter des Endpunkts (VPN-Tunnel) an den konfigurierten Flow Collector gesendet werden, wie im AnyConnect-Fenster und im anschließend angezeigten Wireshark-Fenster zu sehen ist.

> **Anmerkung:** Die Split-Tunnel-Konfiguration des VPN-Profils, mit dem der Endpunkt verbunden ist, muss die IP-Adresse des FlowCollectors enthalten. Andernfalls werden die Datenflüsse nicht über den VPN-Tunnel gesendet.



c. Wenn sich der Endpunkt nicht in einem vertrauenswürdigen Netzwerk befindet, werden die Datenflüsse nicht an den Flow Collector gesendet.



Verwandte Fehler

Derzeit gibt es zwei bekannte Fehler, die sich auf den NVM-Telemetrie-Aufnahmeprozess für sichere Netzwerkanalysen auswirken können:

- FC Engine kann NVM-Telemetrie nicht auf eth1 empfangen. Siehe Cisco Bug-ID CSCwb84013
- Flow Collector fügt keine NVM-Datensätze von AnyConnect Version 4.10.04071 oder höher ein. Siehe Cisco Bug-ID CSCwb91824

Zugehörige Informationen

- Weitere Unterstützung erhalten Sie vom Technical Assistance Center (TAC). Ein gültiger Support-Vertrag ist erforderlich: Weltweiter Kontakt zum Cisco Support.
- Sie können auch die Cisco Security Analytics Community hier besuchen.
- Technischer Support und Dokumentation für Cisco Systeme