Risoluzione dei problemi di acquisizione della telemetria di AnyConnect Network Visibility Module in Secure Network Analytics

Sommario

Introduzione

Questo documento descrive la procedura per risolvere i problemi di caricamento della telemetria di Network Visibility Module (NVM) in Secure Network Analytics (SNA).

Prerequisiti

- Conoscenza SNA Cisco
- Cisco AnyConnect

Guide alla configurazione

- Guida alla configurazione di Secure Network Analytics Endpoint License e Network Visibility Module (NVM)
- Cisco AnyConnect Administrator Guide Network Visibility Module, versione 4.10

Requisiti

- SNA Manager e Flow Collector nella versione 7.3.2 o successive
- Licenza SNA per endpoint
- Cisco AnyConnect con Network Visibility Module 4.3 o versione successiva

Componenti usati

- SNA Manager e Flow Collect versione 7.4.0 e licenza per l'endpoint
- Cisco AnyConnect 4.10.03104 con VPN e Network Visibility Module
- Windows 10 Virtual Machine
- Software Wireshark

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Risoluzione dei problemi

Configurazione SNA

Verifica delle licenze

Verificare che l'account virtuale di Smart Licensing a cui è registrato SNA Manager disponga delle licenze per gli endpoint.

Verifica del caricamento della telemetria NVM

Per verificare se SNA Flow Collector riceve e inserisce la telemetria NVM dagli endpoint, procedere come segue:

1. Accedere al Flow Collector tramite SSH o la console con le credenziali **radice**.

2. Eseguire il comando **grep 'NVM records this period:' /lancope/var/sw/today/logs/sw.log**.

3. Dall'output restituito, verificare se il Flow Collector acquisisce i record NVM e li inserisce nel database.

```
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
```

Da questo output sembra che il Flow Collector non abbia ricevuto alcun record NVM, ma è necessario confermare se è configurato per l'ascolto della telemetria NVM.

Verificare se Flow Collector è configurato per l'ascolto della telemetria NVM

1. Accedere all'interfaccia utente di amministrazione di Flow Collector.

2. Passare a **Supporto > Impostazioni avanzate**.

3. Assicurarsi che gli attributi richiesti siano configurati correttamente:

SNA versione 7.3.2 o 7.4.0

==========

- Individuare l'attributo **nvm_netflow_port** e verificare il valore configurato. Questa condizione deve corrispondere alla porta configurata nel profilo NVM di AnyConnect.

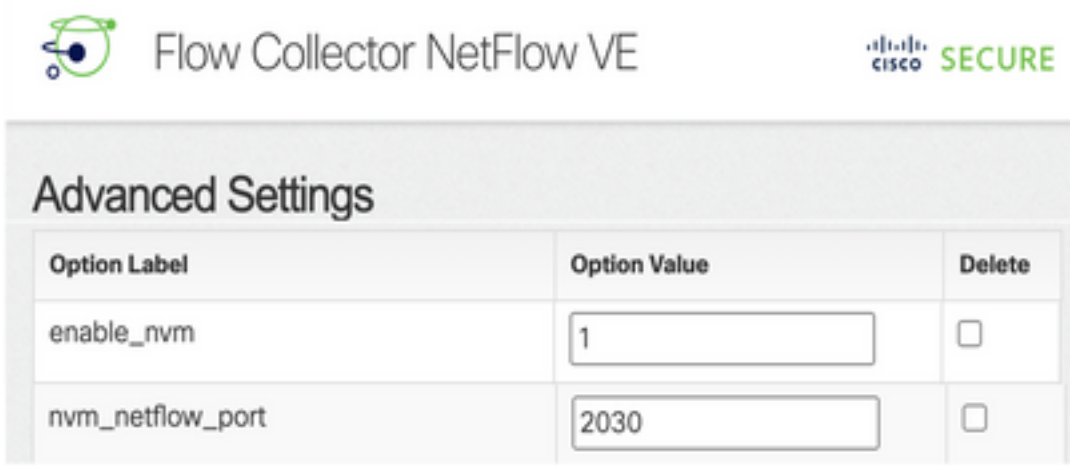
Nota: verificare che la porta configurata sia una porta non riservata e non sia 2055, 514 o 8514. Se il valore configurato è "0", la funzione è disabilitata.

Nota: se un campo non è visualizzato, scorrere fino alla fine della pagina. Fare clic sul campo **Aggiungi nuova opzione**. Per ulteriori informazioni sulle impostazioni avanzate di Flow Collector, consultare l'argomento della Guida in linea relativo alle impostazioni avanzate.

SNA versione 7.4.1

==========

- Individuare l'attributo **nvm_netflow_port** e verificare il valore configurato. Questa condizione deve corrispondere alla porta configurata nel profilo NVM di AnyConnect.
- Individuare l'attributo **enable_nvm** e verificare che il valore sia impostato su **1**, in caso contrario la funzione viene disabilitata.



Nota: verificare che la porta configurata sia una porta non riservata e non sia 2055, 514 o 8514.

Nota: se un campo non è visualizzato, scorrere fino alla fine della pagina. Fare clic sul campo **Aggiungi nuova opzione**. Per ulteriori informazioni sulle impostazioni avanzate di Flow Collector, consultare l'argomento della Guida in linea relativo alle impostazioni avanzate.

4. Una volta configurate correttamente le impostazioni avanzate sul Flow Collector, verificare se la telemetria è stata acquisita, con la stessa procedura descritta nella sezione **Verifica inserimento telemetria NVM**.

5. Se la configurazione dell'endpoint con AnyConnect NVM e le impostazioni sul Flow Collector sono corrette, il file **sw.log** deve rifletterlo:

```
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. Se il Flow Collector continua a non acquisire i record NVM, verificare se il dispositivo di raccolta riceve i pacchetti sull'interfaccia e, in ogni caso, verificare che la configurazione degli endpoint sia corretta.

Configurazione degli endpoint

È possibile implementare AnyConnect NVM in uno dei due modi seguenti: a) scon il pacchetto AnyConnect o b) wcon il pacchetto NVM standalone (solo sul desktop AnyConnect).

La configurazione richiesta è la stessa per entrambe le distribuzioni, la differenza risiede nella configurazione di Trusted Network Detection.

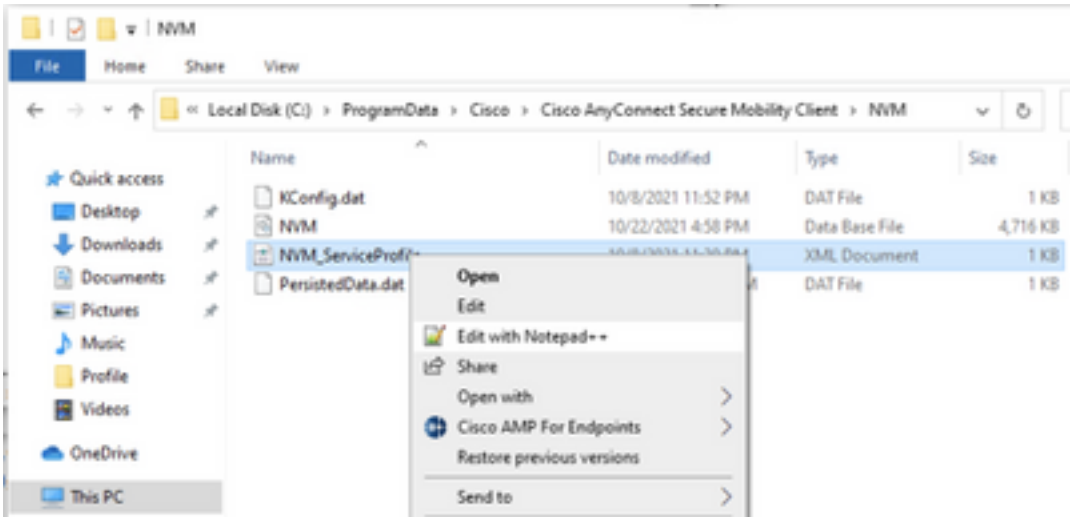
Verifica del profilo NVM

Individuare il profilo NVM utilizzato dall'endpoint e confermare le impostazioni **di configurazione** del **raccoglitore**.

Percorso profilo NVM:

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

Nota: Il nome del profilo NVM deve essere **NVM_ServiceProfile**, in caso contrario Network Visibility Module non riesce a raccogliere e inviare i dati.



Il contenuto del profilo NVM dipende dalla configurazione, ma gli elementi del profilo rilevanti per la SNA sono contrassegnati in grassetto. Assicurarsi di rivedere le note dopo l'esempio del profilo NVM:

Nota: Verificare che la **porta configurata sia una porta non riservata e non sia 2055, 514 o 8514**. La porta configurata in questo profilo deve essere la stessa configurata nel Flow Collector.

Nota: Verificare che se il profilo NVM ha l'elemento **Secure** XML, sia impostato su **false**, altrimenti i flussi vengono inviati criptati con DTLS e il Flow Collector non è in grado di elaborarli.

Verificare le impostazioni TND (Trusted Network Detection)

Network Visibility Module invia le informazioni sul flusso solo quando si trova sulla rete attendibile. Per impostazione predefinita, non viene raccolto alcun dato. I dati vengono raccolti solo se configurati come tali nel profilo e continuano a essere raccolti quando l'endpoint è connesso. Se la raccolta viene eseguita in una rete non attendibile, viene memorizzata nella cache e inviata all'agente di raccolta quando l'endpoint si trova in una rete attendibile. È necessario configurare ulteriormente lo strumento di raccolta dei flussi di analisi della rete sicura affinché elabori i flussi

memorizzati nella cache (per informazioni sulla configurazione necessaria, vedere Configurare lo strumento di raccolta dei flussi per i flussi memorizzati fuori rete).

Lo stato TND (Trusted Network State) può essere determinato dalla funzionalità TND della VPN (configurata nel profilo VPN) o dalla configurazione TND nel profilo NVM:

Configurazione TND nel profilo VPN

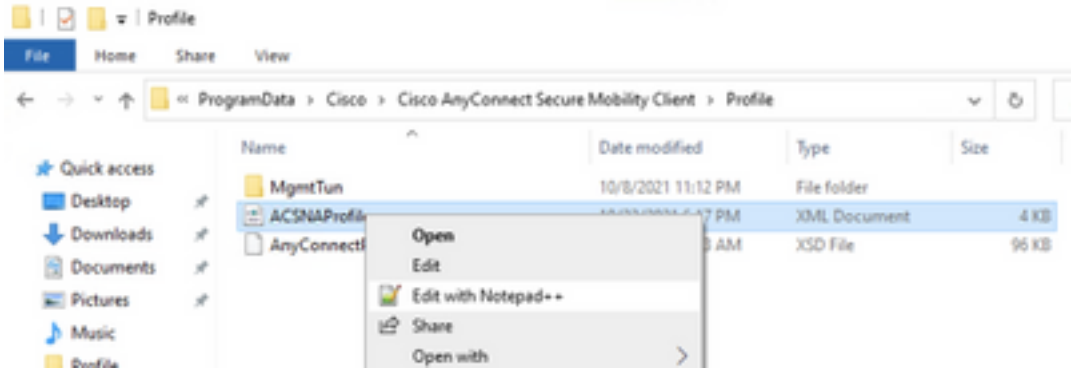
Nota: Questa opzione non è disponibile per le implementazioni NVM Standalone.

1. Individuare il profilo VPN utilizzato dall'endpoint e confermare le impostazioni dei **criteri VPN automatici** configurate

   Percorso profilo VPN:

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

  In questo esempio il profilo VPN è denominato **ACSNAProfile**.



2. Modificare il profilo con un editor di testo e individuare l'elemento **AutomaticVPNPolicy**. Verificare che i criteri configurati siano corretti per il corretto rilevamento della rete attendibile. In questo caso:

...

Nota: Per la rilevanza NVM: se sia il criterio di rete attendibile che il criterio di rete non

attendibile sono impostati su Nessuna operazione, il rilevamento di reti attendibili dal profilo VPN viene disattivato.

Configurazione TND nel profilo NVM

Individuare il profilo NVM utilizzato dall'endpoint e verificare che le impostazioni configurate per l'**elenco dei server trusted** siano corrette.

Percorso profilo NVM:

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

...

```
</NVMProfile>
```

Nota: Un probe SSL viene inviato all'headend trusted configurato, che risponde con un certificato, se raggiungibile. L'identificazione personale (hash SHA-256) viene quindi estratta e confrontata con l'hash impostato nell'editor dei profili. Una corrispondenza riuscita indica che l'endpoint si trova in una rete attendibile; tuttavia, se l'headend non è raggiungibile o l'hash del certificato non corrisponde, l'endpoint viene considerato come incluso in una rete non attendibile.

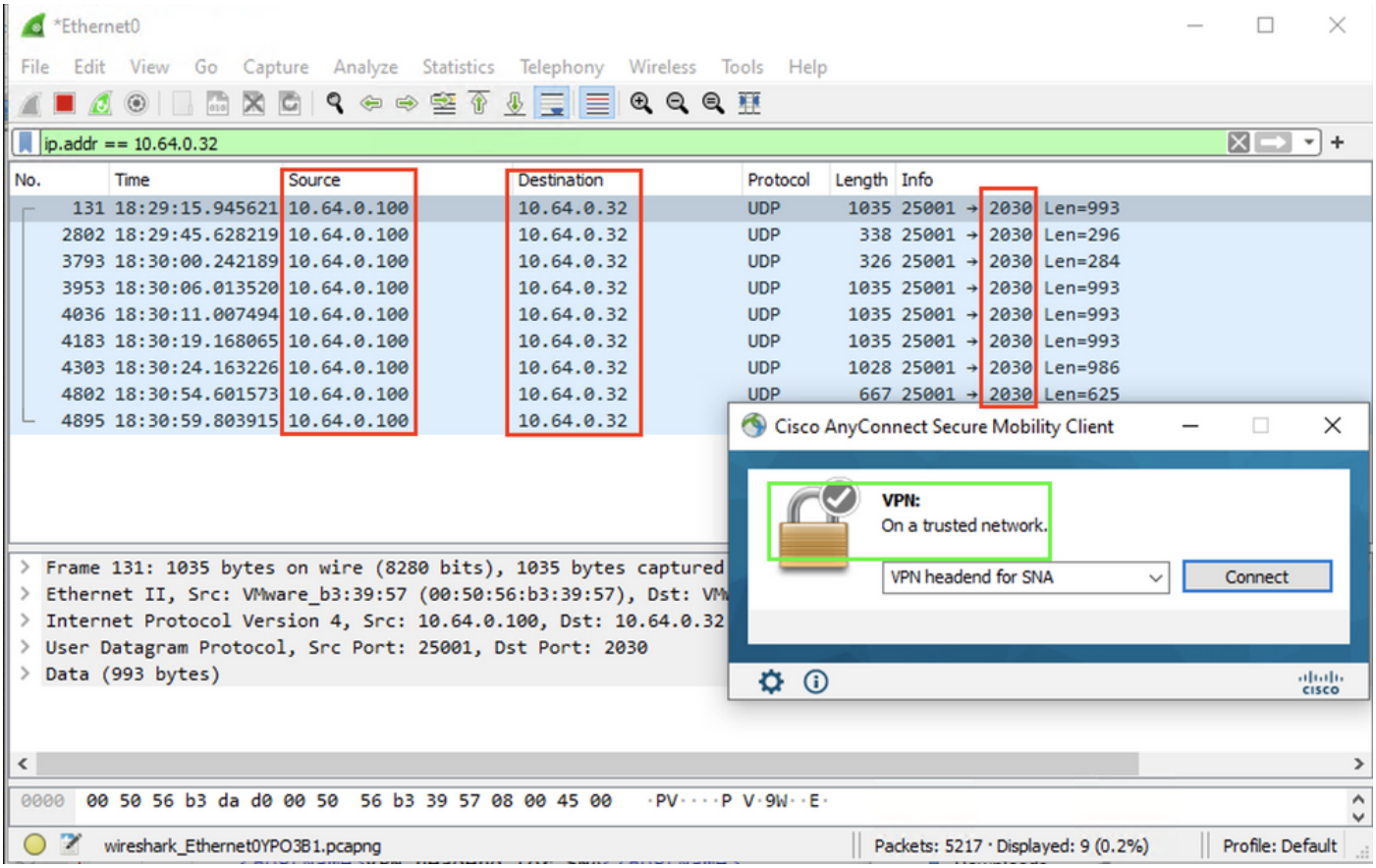
Nota: I server trusted dietro i proxy non sono supportati.

Raccogli acquisizioni pacchetti

Èpossibile raccogliere un'acquisizione di pacchetto sulla scheda di rete dell'endpoint per verificare che i flussi vengano inviati al Flow Collector.

r. Se l'endpoint si trova su una rete attendibile ma NON è connesso a VPN, l'acquisizione deve essere abilitata sulla scheda di rete fisica.

In questo caso, il client Anyconnect indica che l'endpoint si trova su una rete attendibile, ossia che i flussi vengono inviati al Flow Collector configurato sulla porta configurata tramite l'adattatore di rete fisico dell'endpoint, come mostrato nella finestra AnyConnect e nella finestra Wireshark visualizzate di seguito.

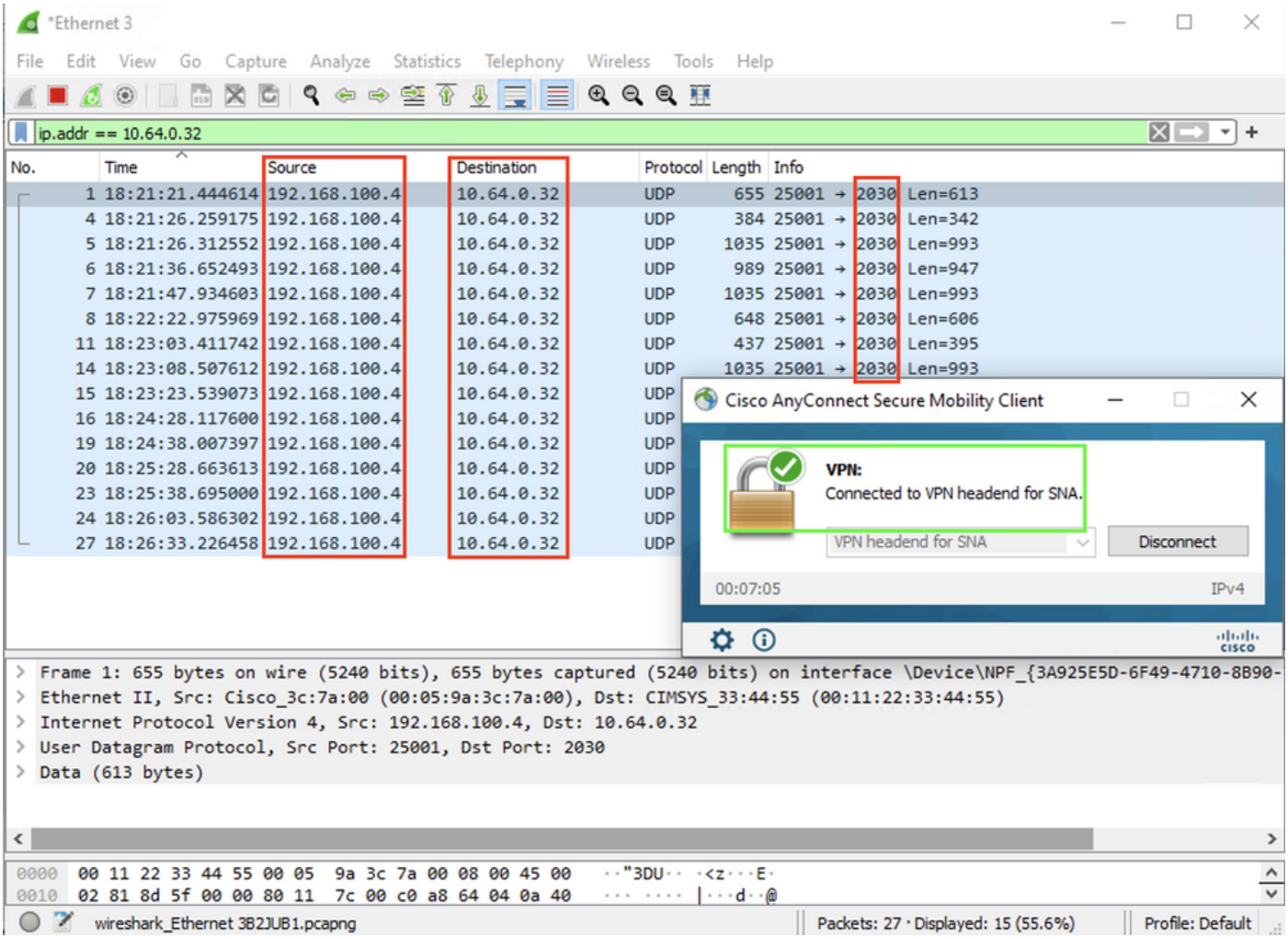


b. Se l'endpoint è connesso a una VPN AnyConnect, viene automaticamente considerato come appartenente alla rete attendibile. Pertanto, l'acquisizione deve essere abilitata sulla scheda di rete virtuale.

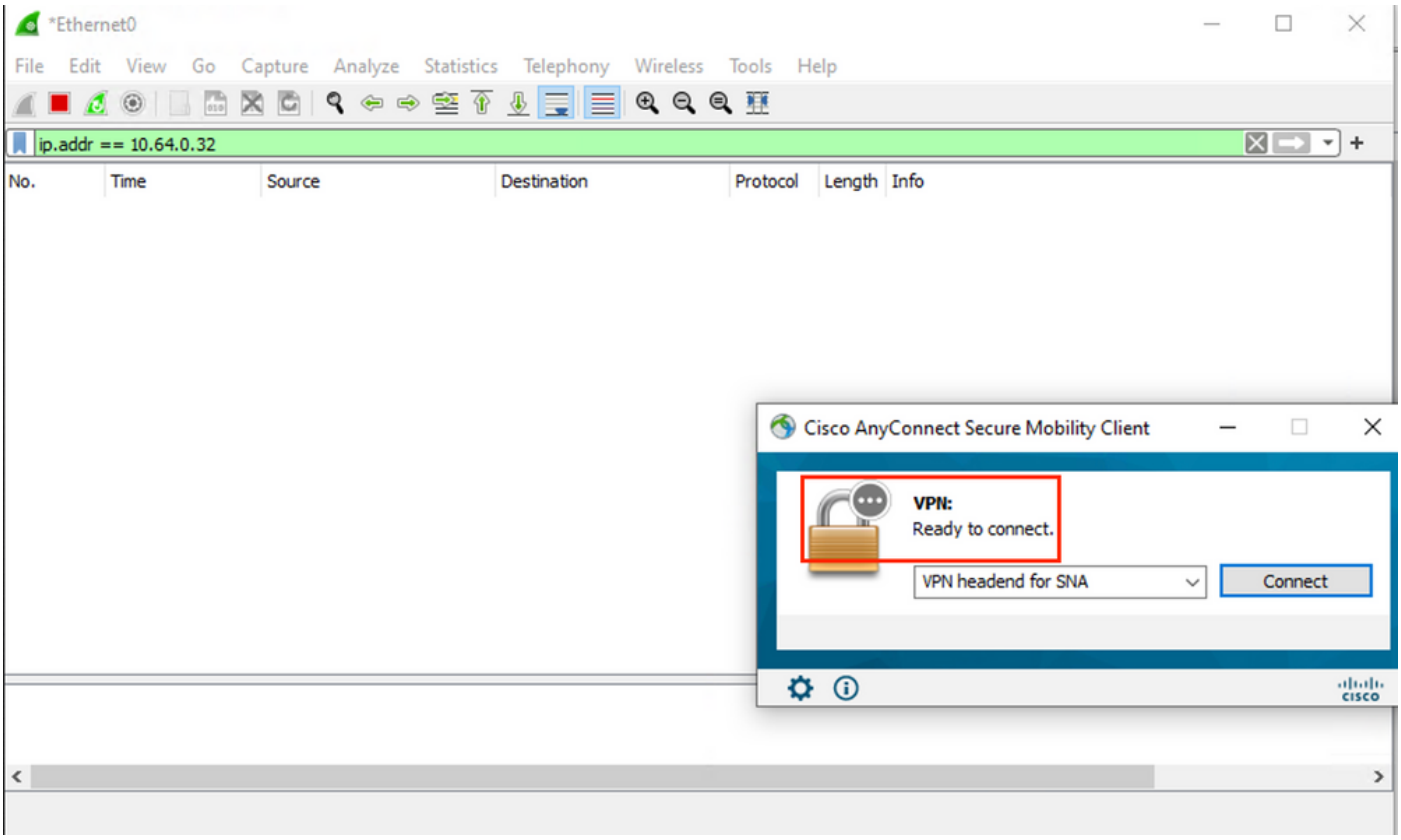
> **Nota:** Se il modulo VPN è installato e TND è configurato nel profilo Network Visibility Module, Network Visibility Module esegue il rilevamento di reti attendibili anche all'interno della rete VPN.

Il client AnyConnect indica che l'endpoint è connesso alla VPN, ossia i flussi vengono inviati al Flow Collector configurato tramite la scheda di rete virtuale dell'endpoint (tunnel VPN), come mostrato nella finestra AnyConnect e nella finestra Wireshark visualizzate di seguito.

> **Nota:** La configurazione del tunnel suddiviso del profilo VPN a cui è connesso l'endpoint deve includere l'indirizzo IP del Flow Collector, altrimenti i flussi non verranno inviati attraverso il tunnel VPN.



c. Se l'endpoint non si trova in una rete attendibile, i flussi non vengono inviati all'agente di raccolta flussi.



Difetti correlati

Al momento esistono due difetti noti che possono influire sul processo di acquisizione della telemetria NVM su Secure Network Analytics:

- Il motore FC non è in grado di acquisire la telemetria NVM su eth1. Vedere l'ID bug Cisco CSCwb84013
- Flow Collector non inserisce record NVM da AnyConnect versione 4.10.04071 o successive. Vedere l'ID bug Cisco CSCwb91824

Informazioni correlate

- Per ulteriore assistenza, contattare il Technical Assistance Center (TAC). È necessario un contratto di supporto valido: Contatti del supporto Cisco internazionali.
- Qui è possibile anche visitare la Cisco Security Analytics Community.
- Documentazione e supporto tecnico – Cisco Systems