Solución de problemas de entrada de Telemetría del módulo de visibilidad de red AnyConnect en Secure Network Analytics

Contenido

Introducción

Este documento describe el procedimiento para resolver problemas de entrada de telemetría del módulo de visibilidad de red (NVM) en Secure Network Analytics (SNA).

Prerequisites

- Conocimiento de Cisco SNA
- Conocimiento de Cisco AnyConnect

Guías de Configuración

- Guía de configuración de Secure Network Analytics Endpoint License y Network Visibility Module (NVM)
- Guía del administrador de Cisco AnyConnect Network Visibility Module, versión 4.10

Requirements

- SNA Manager y Flow Collector en la versión 7.3.2 o posterior
- Licencia de terminal SNA
- Cisco AnyConnect con Network Visibility Module 4.3 o posterior

Componentes Utilizados

- Licencia de SNA Manager y Flow Collection versión 7.4.0 y terminal
- Cisco AnyConnect 4.10.03104 con VPN y Network Visibility Module
- Máquina virtual Windows 10
- software 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Proceso de Troubleshooting

Configuración SNA

Verificación de licencias

Asegúrese de que la cuenta virtual de licencias inteligentes a la que está registrado el administrador SNA tenga las licencias de terminales.

Verificar entrada de telemetría NVM

Para confirmar si el colector de flujo SNA recibe e inserta telemetría NVM desde los terminales, proceda de la siguiente manera:

1. Inicie sesión en Flow Collector a través de SSH o consola con credenciales **raíz**.

2. Ejecute el comando **grep 'NVM graba este período:' /lancope/var/sw/today/logs/sw.log**.

3. En la salida devuelta, confirme si el Flow Collector ingiere los registros NVM e los inserta en la base de datos.

```
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
```

A partir de este resultado, parece que el Flow Collector no ha recibido ningún registro NVM, sin embargo, debe confirmar si está configurado para escuchar la telemetría NVM.

Verifique si el Flow Collector está configurado para escuchar la telemetría NVM

1. Inicie sesión en la interfaz de usuario de administrador de Flow Collector (IU).

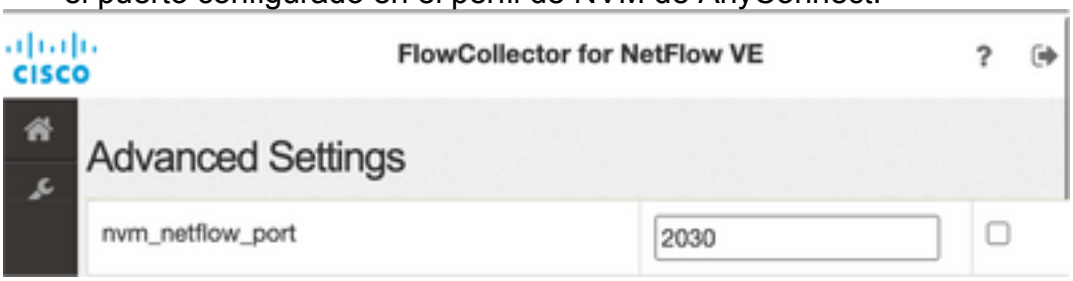
2. Vaya a **Support > Advanced Settings**.

3. Asegúrese de que los atributos necesarios estén configurados correctamente:

SNA versión 7.3.2 o 7.4.0

==========

- Busque el atributo **nvm_netflow_port** y verifique el valor configurado. Esto debe coincidir con el puerto configurado en el perfil de NVM de AnyConnect.



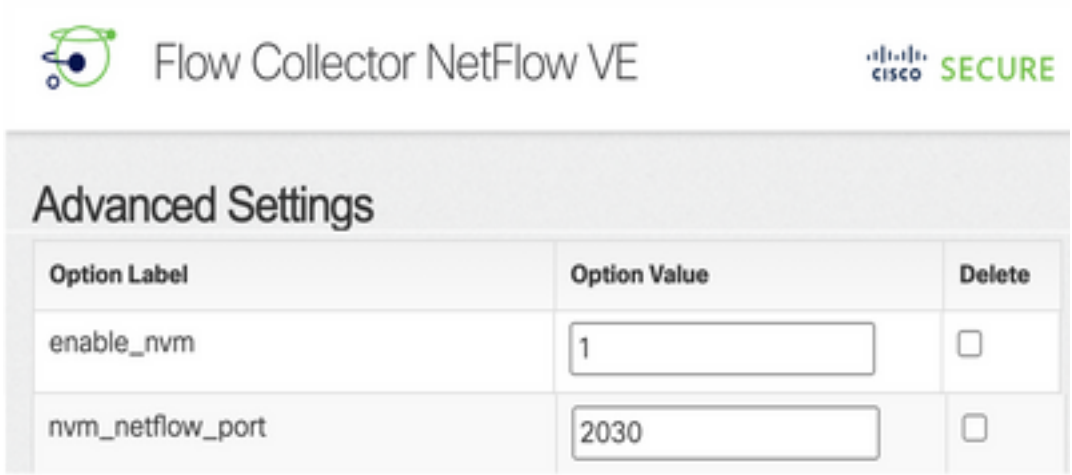
Nota: Asegúrese de que el puerto configurado sea un puerto no reservado y no sea 2055, 514 ni 8514. Si el valor configurado es "0", la función se inhabilita.

Nota: Si no se muestra un campo, desplácese hasta la parte inferior de la página. Haga clic en el campo **Agregar nueva opción**. Para obtener más información sobre los parámetros avanzados del Flow Collector, consulte el tema de ayuda en línea Advanced Settings.

SNA versión 7.4.1

==========

- Busque el atributo **nvm_netflow_port** y verifique el valor configurado. Esto debe coincidir con el puerto configurado en el perfil de NVM de AnyConnect.
- Localice el atributo **enable_nvm** y asegúrese de que el valor esté establecido en **1**, de lo contrario la función se desactivará.



Nota: Asegúrese de que el puerto configurado sea un puerto no reservado y no sea 2055, 514 ni 8514.

Nota: Si no se muestra un campo, desplácese hasta la parte inferior de la página. Haga clic en el campo **Agregar nueva opción**. Para obtener más información sobre los parámetros avanzados del Flow Collector, consulte el tema de ayuda en línea Advanced Settings.

4. Una vez que los parámetros avanzados del Flow Collector se han configurado correctamente, verifique si la telemetría se ha ingerido ahora, con el mismo procedimiento que se describe en la sección **Verificar entrada de telemetría de NVM**.

5. Si la configuración del punto final con AnyConnect NVM y la configuración en Flow Collector son correctas, el archivo **sw.log** debe reflejarlo:

```
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 el Flow Collector aún no ingesta registros NVM, verifique si el colector recibe los paquetes en la interfaz y, en cualquier caso, asegúrese de que la configuración de los terminales sea correcta.

Configuración del terminal

Puede implementar AnyConnect NVM de una de estas dos maneras: a) wcon el paquete AnyConnect o b) wcon el paquete de NVM independiente (sólo en el escritorio de AnyConnect).

La configuración requerida es la misma para ambas implementaciones, la diferencia reside en la configuración de la detección de red de confianza.

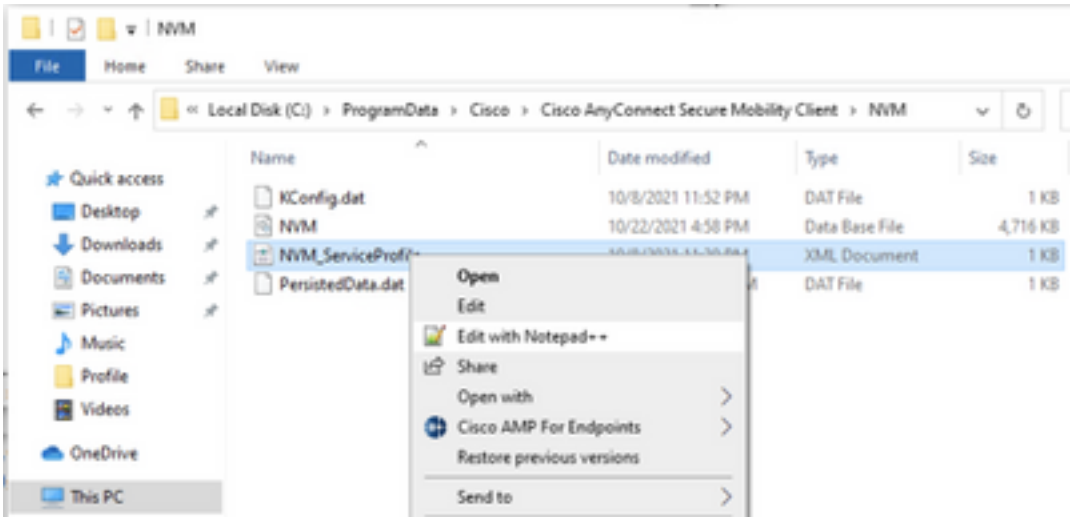
Verificar el perfil NVM

Localice el perfil NVM utilizado por el terminal y confirme la configuración **del colector**.

Ubicación del perfil de NVM:

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

Nota: El nombre del perfil NVM debe ser **NVM_ServiceProfile**; de lo contrario, Network Visibility Module no puede recopilar y enviar datos.



El contenido del perfil NVM depende de su configuración, sin embargo, los elementos del perfil que son relevantes para SNA se marcan en negrita. Asegúrese de revisar las notas después del ejemplo de perfil de NVM:

Nota: Asegúrese de que el **puerto configurado sea un puerto no reservado y no sea 2055, 514 o 8514**. El puerto configurado en este perfil debe ser el mismo que el configurado en el Flow Collector.

Nota: Asegúrese de que si el perfil de NVM tiene el elemento **Secure** XML, se establezca en **false**, de lo contrario los flujos se envían cifrados con DTLS y el colector de flujo no puede procesarlos.

Verificar la configuración de la detección de red de confianza (TND)

El módulo Network Visibility envía información de flujo sólo cuando se encuentra en la red de confianza. De forma predeterminada, no se recopila ningún dato. Los datos se recopilan sólo cuando se configuran como tales en el perfil y los datos se siguen recopilando cuando se conecta el terminal. Si la recolección se realiza en una red no confiable, se almacena en caché y se envía al recopilador cuando el terminal está en una red de confianza. El colector de flujo de Secure Network Analytics necesita tener una configuración adicional para procesar los flujos

almacenados en caché (consulte Configuración del colector de flujo para los flujos almacenados en caché fuera de la red para la configuración necesaria).

El estado de la red de confianza se puede determinar por la función TND de VPN (configurada en el perfil VPN) o por la configuración TND en el perfil NVM:

Configuración de TND en el perfil de VPN

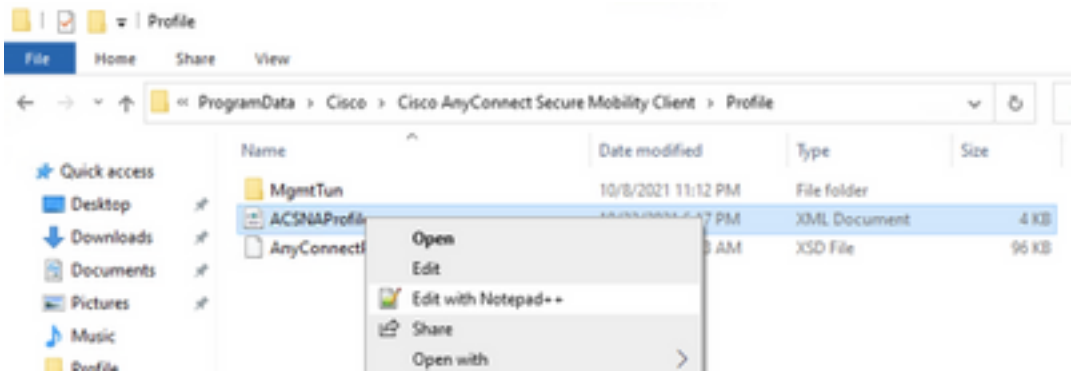
Nota: Esta no es una opción para las implementaciones independientes de NVM.

1. Localice el perfil VPN que utiliza el terminal y confirme los parámetros configurados de **Política de VPN Automática**

   Ubicación del perfil VPN:

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

  En este ejemplo, el perfil VPN se denomina **ACSNAProfile**.



2. Edite el perfil con un editor de texto y localice el elemento **AutomaticVPNPolicy**. Asegúrese de que la política configurada sea correcta para detectar correctamente la red de confianza. En este caso:

. . .

Nota: Para la relevancia de NVM: si la política de red de confianza y la política de red no

fiable están configuradas en No hacer nada, la detección de red de confianza del perfil VPN se inhabilita.

Configuración de TND en el Perfil de NVM

Localice el perfil NVM utilizado por el terminal y confirme que la configuración **lista de servidores de confianza** sea correcta.

Ubicación del perfil de NVM:

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

...

```
</NVMProfile>
```

Nota: Se envía una sonda SSL a la cabecera de confianza configurada, que responde con un certificado, si se puede alcanzar. La huella digital (hash SHA-256) se extrae y coincide con el conjunto de hash del editor de perfiles. Una coincidencia exitosa significa que el terminal está en una red de confianza; sin embargo, si la cabecera es inalcanzable, o si el hash del certificado no coincide, el punto final se considera en una red no confiable.

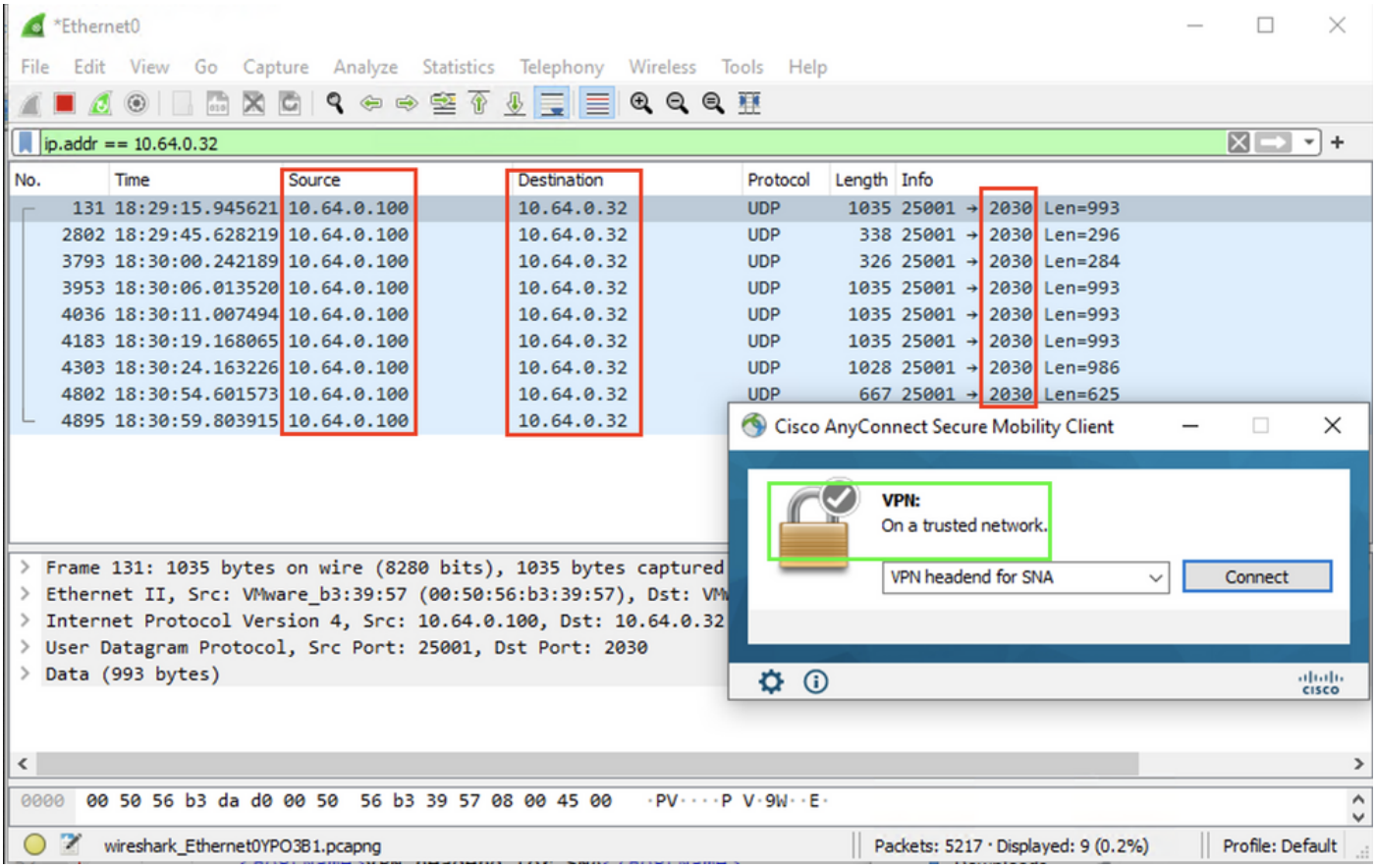
Nota: No se admiten servidores de confianza detrás de proxies.

Recopilar capturas de paquetes

Puede recopilar una captura de paquetes en el adaptador de red del punto final para verificar que los flujos se envían al Flow Collector.

a. Si el terminal se encuentra en una red de confianza pero NO está conectado a VPN, la captura se debe habilitar en el adaptador de red físico.

En este caso, Anyconnect Client indica que el terminal está en una red de confianza, lo que significa que los flujos se envían al Flow Collector configurado sobre el puerto configurado a través del adaptador de red físico del terminal, como podemos ver en la ventana de AnyConnect y en la ventana de Wireshark que se muestra a continuación.

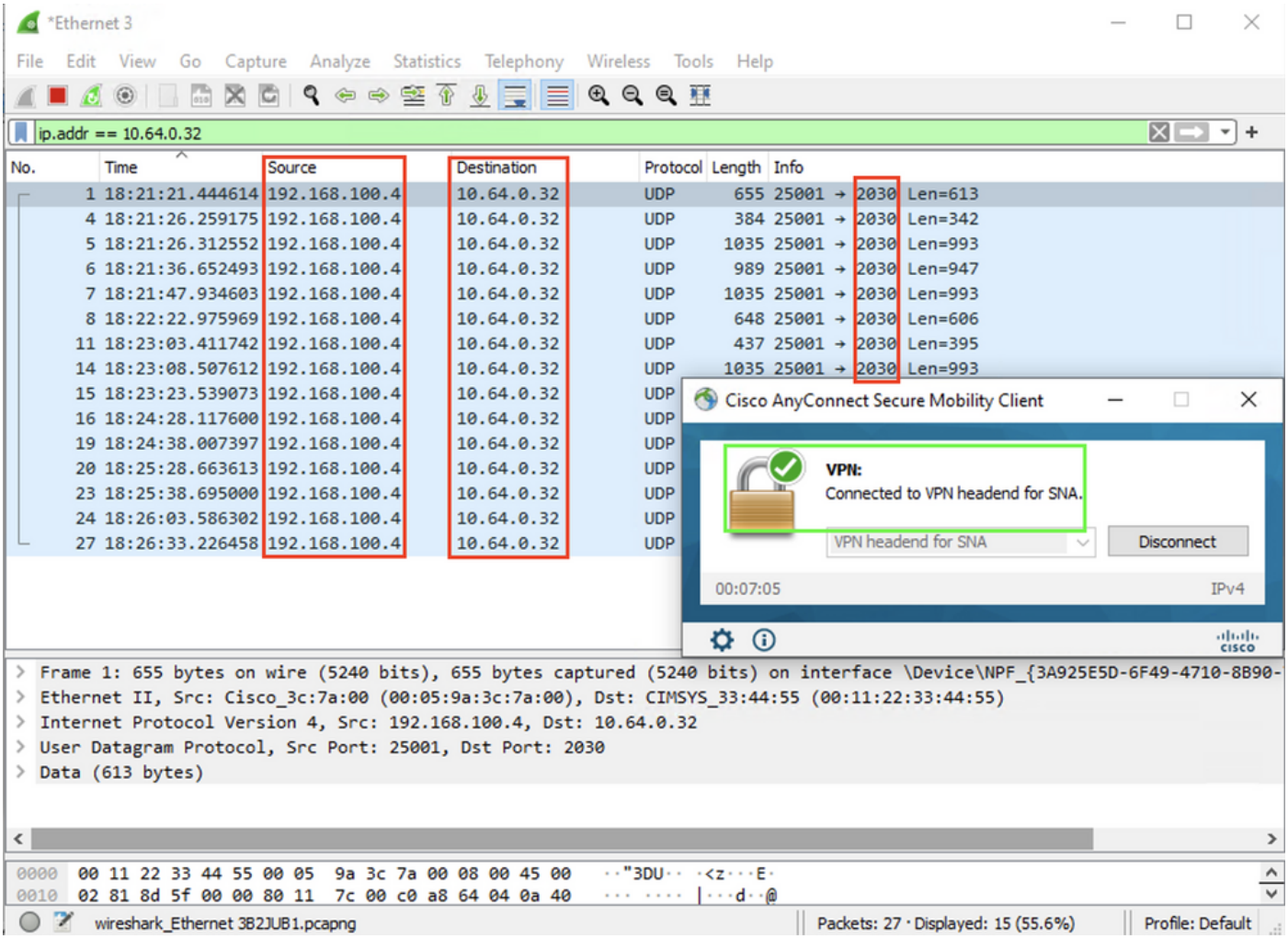


b. Si el terminal está conectado a AnyConnect VPN, se considera automáticamente que se encuentra en la red de confianza, por lo tanto, la captura debe estar habilitada en el adaptador de red virtual.

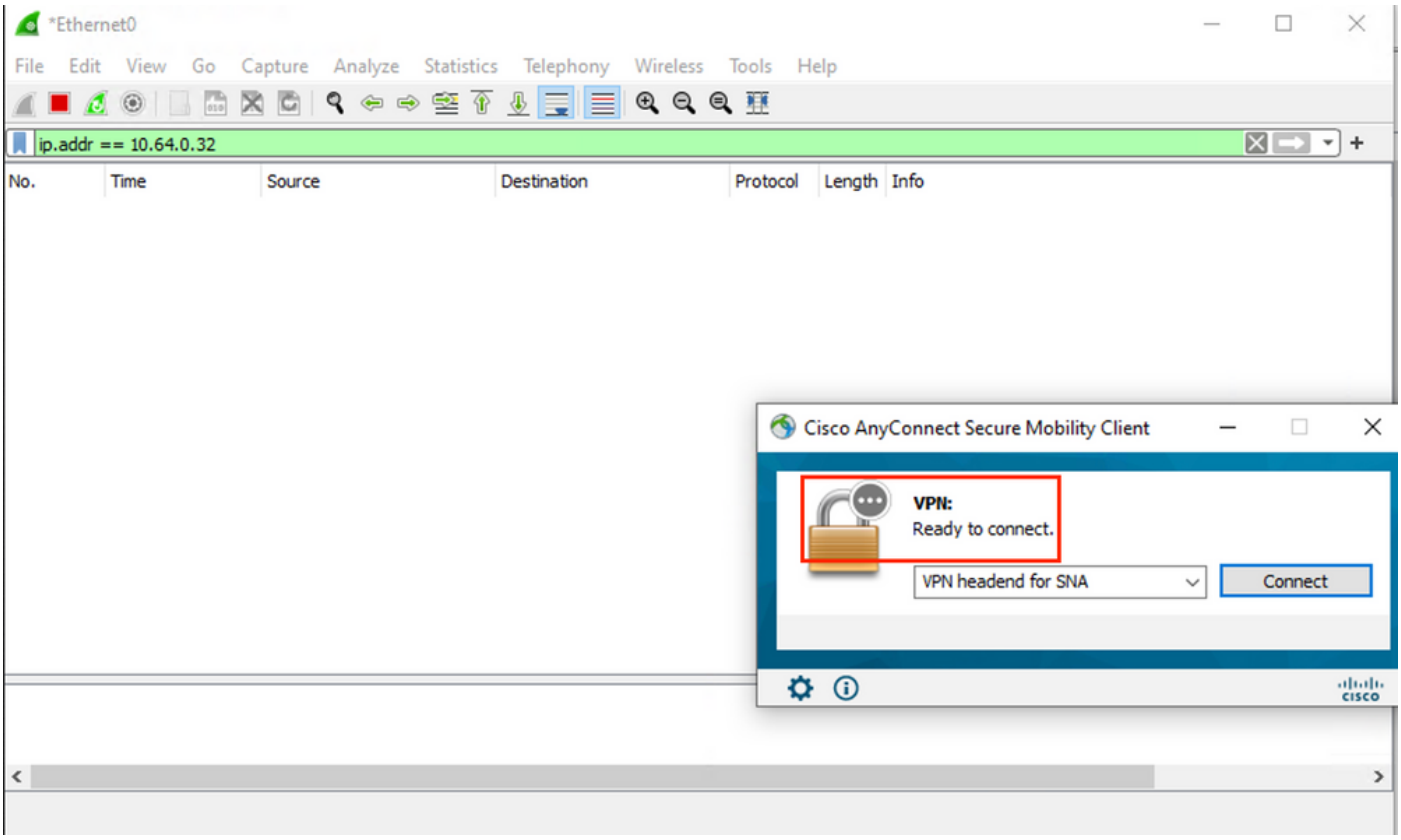
> **Nota:** Si se instala el módulo VPN y TND se configura en el perfil del Módulo de visibilidad de red, el Módulo de visibilidad de red realiza la detección de red de confianza incluso dentro de la red VPN.

AnyConnect Client indica que el terminal está conectado a VPN, lo que significa que los flujos se envían al Flow Collector configurado sobre el puerto configurado a través del adaptador de red virtual del terminal (túnel VPN), como podemos ver en la ventana de AnyConnect y en la ventana de Wireshark que se muestra a continuación.

> **Nota:** La configuración del túnel dividido del perfil VPN al que está conectado el terminal debe incluir la dirección IP del Flow Collector; de lo contrario, los flujos no se envían a través del túnel VPN.



c. Si el terminal no se encuentra en una red de confianza, los flujos no se envían al Flow Collector.



Defectos relacionados

Actualmente existen dos defectos conocidos que pueden afectar al proceso de ingreso de telemetría de NVM en Secure Network Analytics:

- El motor FC no puede ingerir telemetría NVM en eth1. Consulte Cisco bug ID CSCwb84013
- Flow Collector no inserta registros NVM de la versión 4.10.04071 o posterior de AnyConnect. Consulte Cisco bug ID CSCwb91824

Información Relacionada

- Para obtener asistencia adicional, póngase en contacto con el Centro de Asistencia Técnica (TAC). Se requiere un contrato de soporte válido: Contactos de soporte a nivel mundial de Cisco.
- También puede visitar Cisco Security Analytics Community aquí.
- Soporte Técnico y Documentación - Cisco Systems