Solucione problemas de telemetria do módulo de visibilidade de rede do AnyConnect em Secure Network Analytics

Contents

Introduction

Este documento descreve o procedimento para solucionar problemas de ingestão de telemetria do Network Visibility Module (NVM) no Secure Network Analytics (SNA).

Prerequisites

- Conhecimento do Cisco SNA
- Conhecimento do Cisco AnyConnect

Guias de configuração

- Guia de configuração do Secure Network Analytics Endpoint License and Network Visibility Module (NVM)
- Guia do administrador do Cisco AnyConnect Módulo de visibilidade de rede, versão 4.10

Requirements

- SNA Manager e Flow Collector na versão 7.3.2 ou mais recente
- Licença de ponto de extremidade SNA
- Cisco AnyConnect com Network Visibility Module 4.3 ou mais recente

Componentes Utilizados

- SNA Manager e Flow Collect versão 7.4.0 e Licença de endpoint
- Cisco AnyConnect 4.10.03104 com módulo de visibilidade de rede e VPN
- Máquina virtual do 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Processo de solução de problemas

Configuração de SNA

Verificar o licenciamento

Certifique-se de que a Smart Licensing Virtual Account para a qual o SNA Manager está registrado tem as Licenças de endpoint.

Verificar a entrada de telemetria NVM

Para confirmar se o coletor de fluxo SNA recebe e insere telemetria NVM dos endpoints, faça o seguinte:

1. Faça login no Flow Collector via SSH ou console com credenciais **raiz**.

2. Execute o comando **grep 'NVM registra este ponto:' /lancope/var/sw/today/logs/sw.log**.

3. Na saída retornada, confirme se o Flow Collector ingere registros NVM e os insere no banco de dados.

```
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 dessa saída, parece que o Flow Collector não recebeu nenhum registro NVM, mas você deve confirmar se ele está configurado para ouvir a telemetria NVM.

Verifique se o Flow Collector está configurado para ouvir a telemetria NVM

1. Faça login na interface de usuário (UI) do Flow Collector Admin.

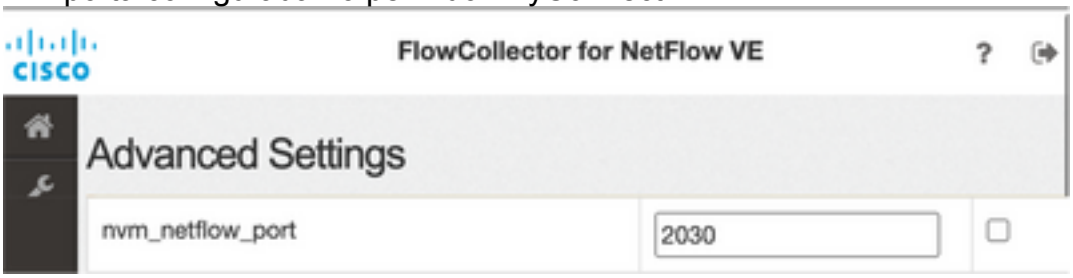
2. Navegue até **Suporte > Configurações avançadas**.

3. Verifique se os atributos necessários estão configurados corretamente:

SNA versão 7.3.2 ou 7.4.0

==========

- Localize o atributo **nvm_netflow_port** e verifique o valor configurado. Isso deve corresponder à porta configurada no perfil do AnyConnect NVM.



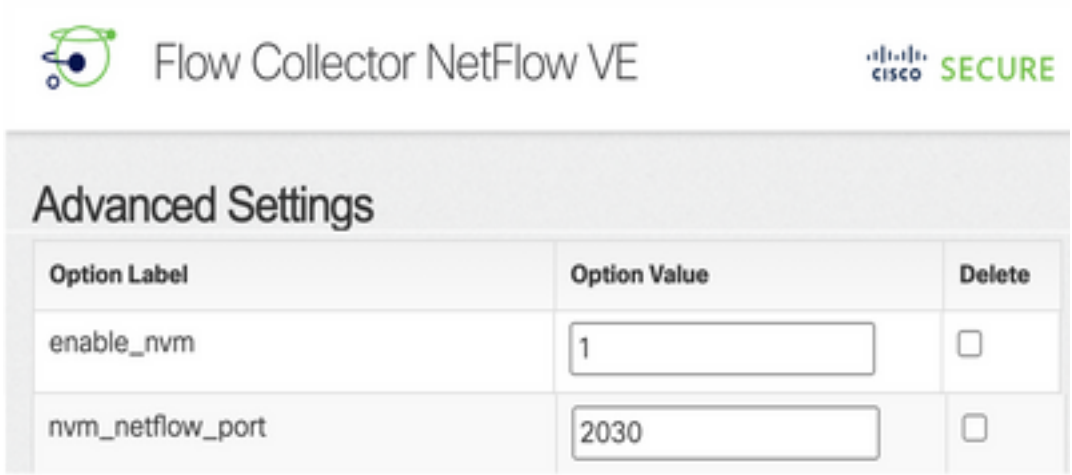
Observação: certifique-se de que a porta configurada seja uma porta não reservada e não seja 2055, 514 ou 8514. Se o valor configurado for "0", o recurso será desativado.

Observação: se um campo não for exibido, role até a parte inferior da página. Clique no campo **Adicionar nova opção**. Para obter mais informações sobre configurações avançadas no Flow Collector, consulte o tópico da ajuda on-line das Configurações avançadas.

SNA versão 7.4.1

==========

- Localize o atributo **nvm_netflow_port** e verifique o valor configurado. Isso deve corresponder à porta configurada no perfil do AnyConnect NVM.
- Localize o atributo **enable_nvm** e verifique se o valor está definido como **1**, caso contrário o recurso será desabilitado.



Observação: certifique-se de que a porta configurada seja uma porta não reservada e não seja 2055, 514 ou 8514.

Observação: se um campo não for exibido, role até a parte inferior da página. Clique no campo **Adicionar nova opção**. Para obter mais informações sobre configurações avançadas no Flow Collector, consulte o tópico da ajuda on-line das Configurações avançadas.

4. Depois que as configurações avançadas no Flow Collector tiverem sido configuradas corretamente, verifique se a telemetria está sendo ingerida agora, com o mesmo procedimento descrito na seção **Verify NVM Telemetry Ingest**.

5. Se a configuração do endpoint com o AnyConnect NVM e as configurações no Flow Collector estiverem corretas, o arquivo **sw.log** deverá refletir:

```
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 o Flow Collector ainda não ingerir registros NVM, verifique se o coletor recebe os pacotes na interface e, em qualquer caso, se a configuração dos endpoints está correta.

Configuração de endpoint

Você pode implantar o AnyConnect NVM de duas maneiras: a)com o pacote do AnyConnect ou b) wcom o pacote NVM independente (somente no desktop AnyConnect).

A configuração necessária é a mesma para ambas as implantações, a diferença reside na configuração da Trusted Network Detection.

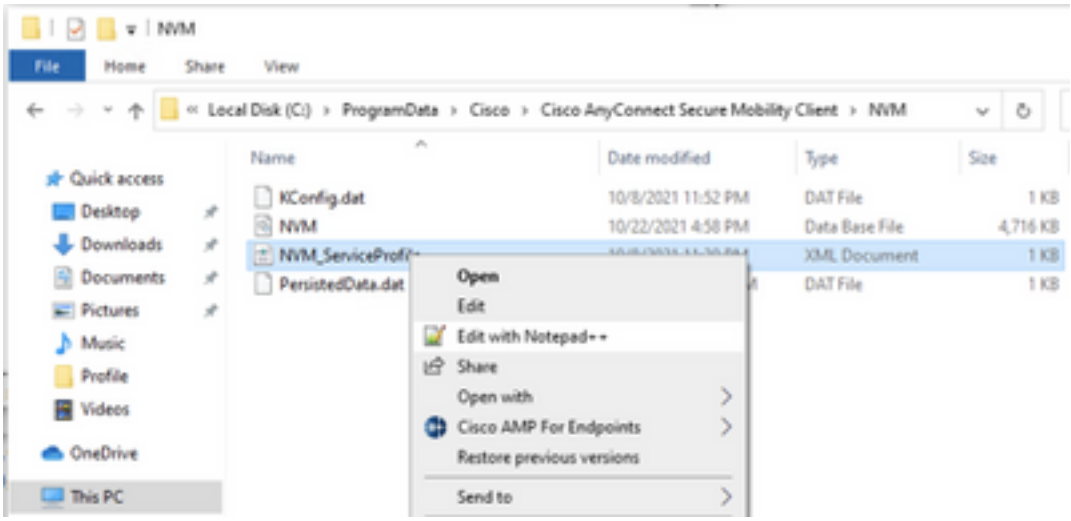
Verificar o perfil NVM

Localize o Perfil NVM usado pelo endpoint e confirme as configurações **de configuração do coletor**.

Localização do perfil NVM:

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

Note: O nome do perfil NVM deve ser **NVM_ServiceProfile**, caso contrário, o Network Visibility Module não coleta e envia dados.



O conteúdo do perfil NVM depende da sua configuração, no entanto, os elementos do perfil que são relevantes para SNA são marcados em negrito. Certifique-se de revisar as notas após o exemplo de perfil NVM:

Note: Verifique se a **porta configurada é uma porta não reservada e não é 2055, 514 ou 8514**. A porta configurada neste perfil precisa ser a mesma configurada no Flow Collector.

Note: Certifique-se de que, se o Perfil NVM tiver o elemento XML **seguro**, ele esteja definido como **falso**, caso contrário, os fluxos serão enviados criptografados com DTLS e o coletor de fluxo não poderá processá-los.

Verificar configurações de TND (Trusted Network Detection, Detecção de rede confiável)

O Network Visibility Module envia informações de fluxo somente quando está na rede confiável. Por padrão, nenhum dado é coletado. Os dados são coletados somente quando configurados como tal no perfil, e os dados continuam a ser coletados quando o endpoint está conectado. Se a coleta for feita em uma rede não confiável, ela será armazenada em cache e enviada ao coletor quando o endpoint estiver em uma rede confiável. O Secure Network Analytics Flow Collector precisa ter uma configuração adicional para que ele processe fluxos em cache (consulte Configurar o Flow Collector para fluxos em cache fora da rede para a configuração necessária).

O estado de rede confiável pode ser determinado pelo recurso TND de VPN (configurado no perfil de VPN) ou pela configuração de TND no perfil de NVM:

Configuração de TND no perfil de VPN

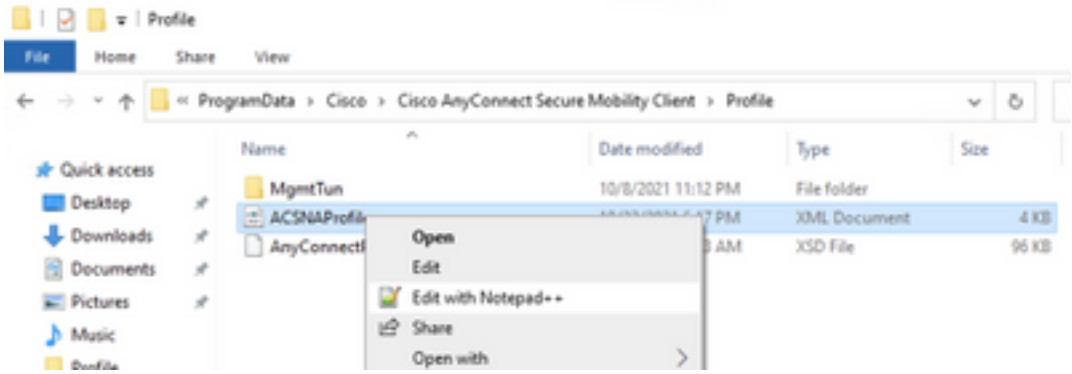
> **Note**: Esta não é uma opção para implantações independentes de NVM.

1. Localize o Perfil VPN usado pelo ponto final e confirme as configurações configuradas da **Política de VPN Automática**

   Local do perfil VPN:

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

  Neste exemplo, o perfil VPN é chamado **ACSNAProfile**.



2. Edite o perfil com um editor de texto e localize o elemento **AutomaticVPNPpolicy**. Verifique se a política configurada está correta para a detecção bem-sucedida da rede confiável. Nesse caso:

```
...
```

> **Note**: Para relevância de NVM: se tanto a Política de rede confiável quanto a Política de rede não confiável estiverem configuradas para Não fazer nada, a Detecção de rede confiável do perfil VPN será desativada.

Configuração de TND no perfil NVM

Localize o Perfil NVM usado pelo endpoint e confirme se as configurações configuradas da **Lista de servidores confiáveis** estão corretas.

Localização do perfil NVM:

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

...

```
</NVMProfile>
```

Note: Uma sonda SSL é enviada ao headend confiável configurado, que responde com um certificado, se acessível. A impressão digital (hash SHA-256) é então extraída e comparada ao conjunto de hash no editor de perfil. Uma correspondência bem-sucedida significa que o endpoint está em uma rede confiável; no entanto, se o headend não puder ser alcançado ou se o hash do certificado não corresponder, o endpoint será considerado como em uma rede não confiável.

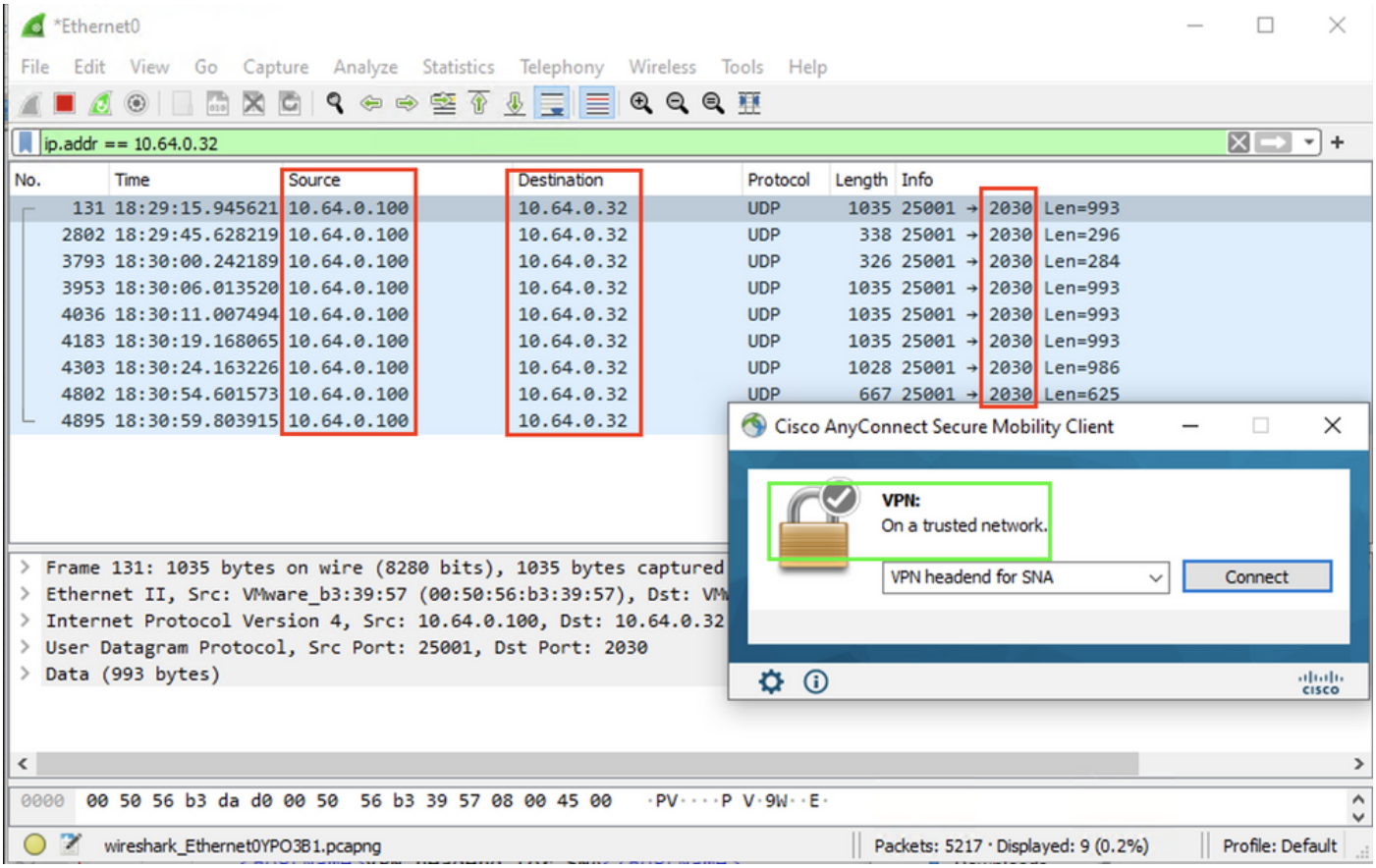
Note: Não há suporte para servidores confiáveis por trás de proxies.

Coletar capturas de pacotes

Você pode coletar uma captura de pacote no adaptador de rede do endpoint para verificar se os fluxos são enviados ao Flow Collector.

a. Se o endpoint estiver em uma rede confiável, mas NÃO estiver conectado à VPN, a captura deverá ser ativada no adaptador de rede físico.

Nesse caso, o Anyconnect Client indica que o endpoint está em uma rede confiável, o que significa que os fluxos são enviados ao Flow Collector configurado pela porta configurada através do Physical Network Adapter do endpoint, como podemos ver na janela do AnyConnect e na janela do Wireshark exibida a seguir.

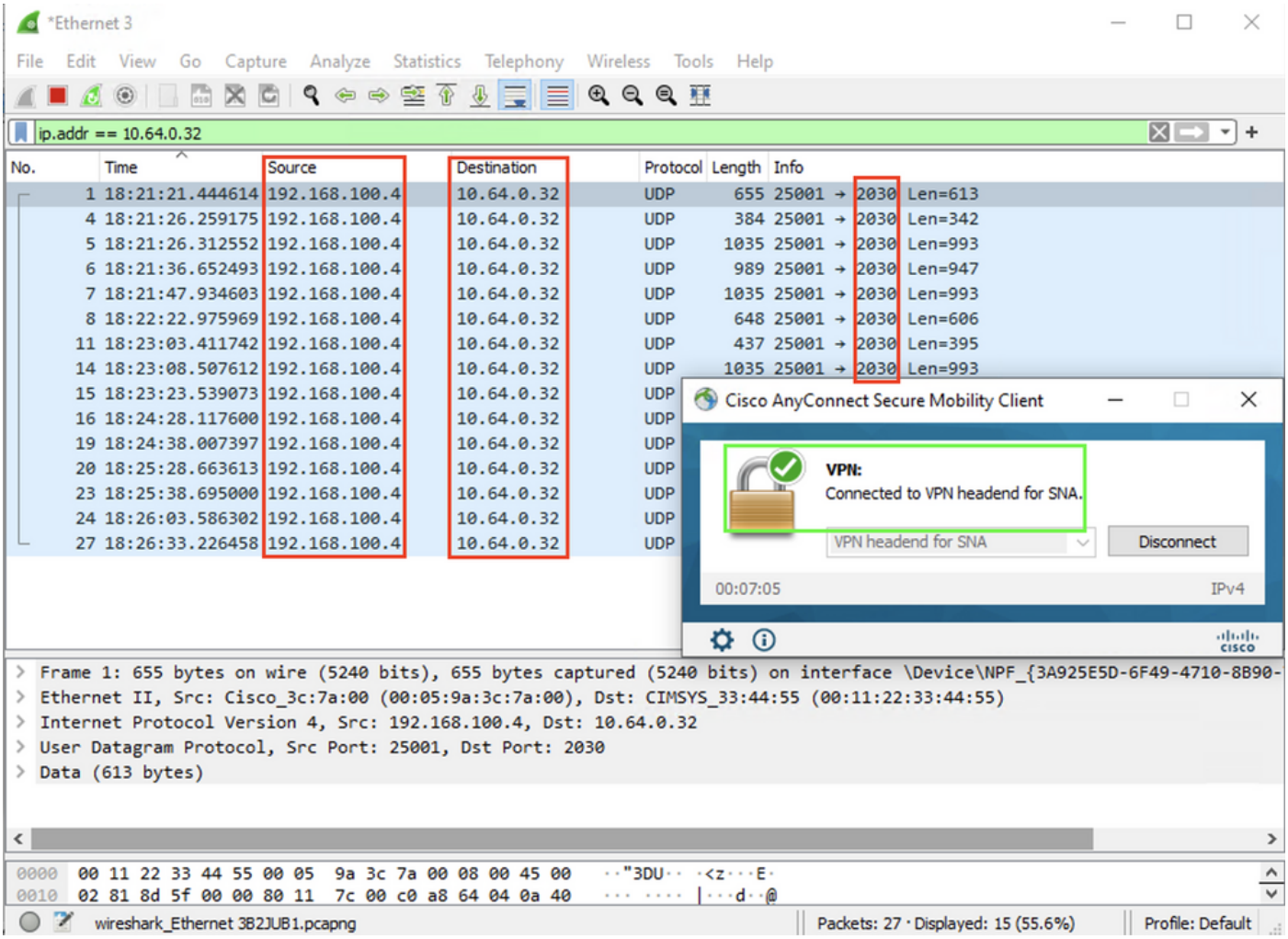


b. Se o Endpoint estiver conectado ao AnyConnect VPN, ele será automaticamente considerado como estando na rede confiável, portanto, a captura deve ser habilitada no Virtual Network Adapter.

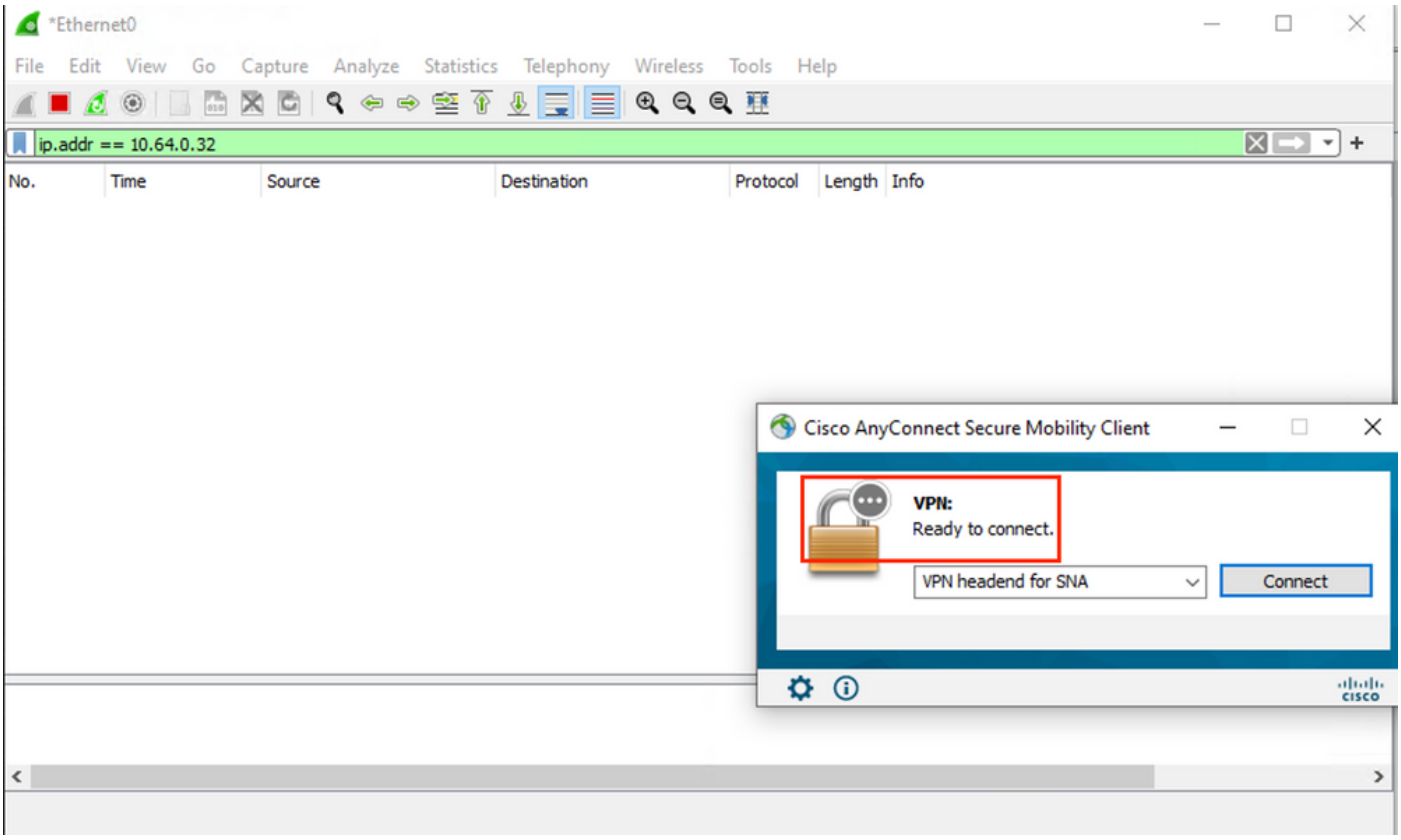
> **Note**: Se o módulo VPN estiver instalado e o TND estiver configurado no perfil do módulo de visibilidade de rede, o módulo de visibilidade de rede executará a detecção de rede confiável mesmo dentro da rede VPN.

O AnyConnect Client indica que o endpoint está conectado à VPN, o que significa que os fluxos são enviados ao Flow Collector configurado pela porta configurada através do Virtual Network Adapter do endpoint (túnel VPN), como podemos ver na janela do AnyConnect e na janela do Wireshark exibida a seguir.

> **Note**: A configuração do túnel dividido do perfil VPN ao qual o endpoint está conectado deve incluir o endereço IP do Flow Collector, caso contrário, os fluxos não serão enviados pelo túnel VPN.



c. Se o endpoint não estiver em uma rede confiável, os fluxos não serão enviados ao Flow Collector.



Defeitos relacionados

Atualmente, há dois defeitos conhecidos que podem afetar o processo de ingestão de telemetria do NVM no Secure Network Analytics:

- O mecanismo FC não pode ingerir telemetria NVM em eth1. Consulte o bug da Cisco ID CSCwb84013
- O Flow Collector não está inserindo registros NVM do AnyConnect versão 4.10.04071 ou superior. Consulte o bug da Cisco ID CSCwb91824

Informações Relacionadas

- Para obter assistência adicional, entre em contato com o Centro de Assistência Técnica (TAC). É necessário um contrato de suporte válido: Contatos de suporte da Cisco no mundo inteiro.
- Você também pode visitar a Comunidade do Cisco Security Analytics aqui.
- Suporte Técnico e Documentação - Cisco Systems