AnyConnect Network Visibility ModuleのSecure Network Analyticsでのテレメトリ取り込みの問題のトラブルシューティング

内容

概要

このドキュメントでは、Secure Network Analytics(SNA)でNetwork Visibility Module(NVM)テレメトリ取り込みの問題をトラブルシューティングする手順について説明します。

前提条件

- Cisco SNAの知識
- Cisco AnyConnectの知識

設定ガイド

- Secure Network AnalyticsエンドポイントライセンスおよびNetwork Visibility Module(NVM)構成ガイド
- Cisco AnyConnect Administrator Guide Network Visibility Module、リリース4.10

要件

- バージョン7.3.2以降のSNAマネージャおよびフローコレクタ
- SNAエンドポイントライセンス
- Cisco AnyConnectとNetwork Visibility Module 4.3以降

使用するコンポーネント

- SNA ManagerおよびFlow Collectバージョン7.4.0とエンドポイントライセンス
- Cisco AnyConnect 4.10.03104 with VPN and Network Visibility Module
- Windows 10仮想マシン
- Wiresharkソフトウェア

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

トラブルシューティングプロセス

SNA設定

ライセンスの確認

SNAマネージャが登録されているスマートライセンス仮想アカウントにエンドポイントライセンスがあることを確認します。

NVMテレメトリ取り込みの確認

SNAフローコレクタがエンドポイントからNVMテレメトリを受信して挿入するかどうかを確認するには、次の手順に従います。

1. SSHまたは**ルート**クレデンシャルを使用したコンソール経由でフローコレクタにログインします。

2. grep 'NVM records this period:' /lancope/var/sw/today/logs/sw.logコマンドを実行します。

3.返された出力から、Flow CollectorがNVMレコードを取り込んでデータベースに挿入するかどうかを確認します。

```
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
```

この出力から、フローコレクタはNVMレコードをまったく受信していないように見えますが、NVMテレメトリをリッスンするように設定されているかどうかを確認する必要があります。

フローコレクタがNVMテレメトリをリッスンするように設定されているかどうかを確認する

1.フローコレクタ管理ユーザインターフェイス(UI)にログインします。

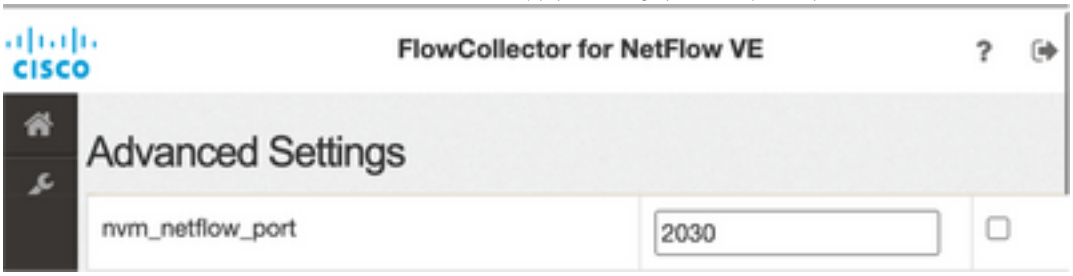
2. [Support] > [Advanced Settings] に移動します。

3.必要な属性が正しく設定されていることを確認します。

SNAバージョン7.3.2または7.4.0

==========

- **nvm_netflow_port**属性を見つけて、設定値を確認します。これは、AnyConnect NVMプロファイルで設定されたポートと一致する必要があります。



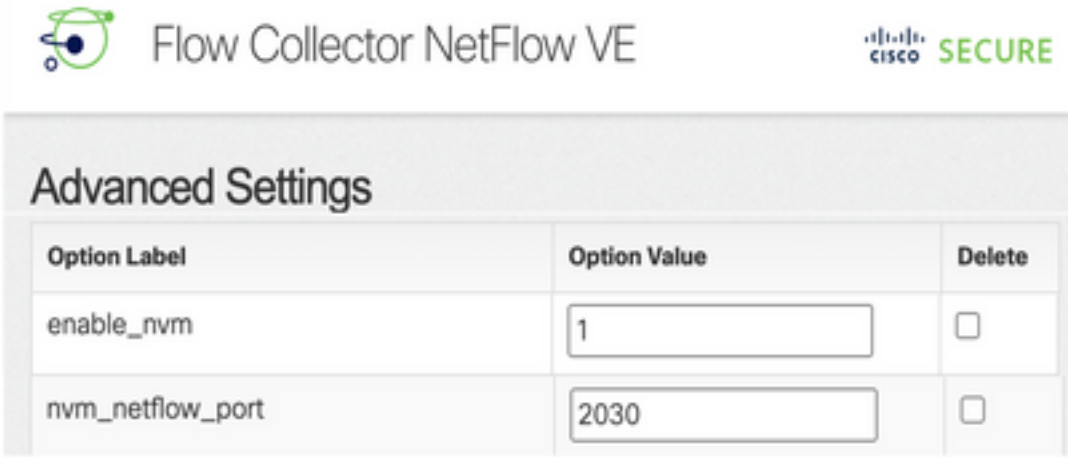
注：設定されているポートが非予約ポートであり、2055、514、または8514でないことを確認します。設定値が「0」の場合、機能は無効になります。

注：フィールドが表示されていない場合は、ページの一番下までスクロールします。[Add New Option] フィールドをクリックします。フローコレクタの詳細設定の詳細については、オンラインヘルプのトピック「詳細設定」を参照してください。

SNAバージョン7.4.1

==========

- **nvm_netflow_port**属性を見つけて、設定値を確認します。これは、AnyConnect NVMプロファイルで設定されたポートと一致する必要があります。
- **enable_nvm**属性を見つけ、値が**1**に設定されていることを確認します。そうでない場合、機能は無効になります。



注：設定されているポートが非予約ポートであり、2055、514、または8514でないことを

確認します。

注：フィールドが表示されていない場合は、ページの一番下までスクロールします。[Add New Option] フィールドをクリックします。フローコレクタの詳細設定の詳細については、オンラインヘルプのトピック「詳細設定」を参照してください。

4.フローコレクタの詳細設定が正しく設定されたら、「**NVMテレメトリ取り込みの確認**」セクションで説明した手順で、テレメトリが取り込まれたことを確認します。

5. AnyConnect NVMを使用したエンドポイントの設定とフローコレクタの設定が正しい場合は、**sw.log**ファイルに次の内容が反映されている必要があります。

```
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.フローコレクタが引き続きNVMレコードを取り込まない場合は、コレクタがインターフェイスでパケットを受信しているかどうかを確認し、いずれの場合もエンドポイントの設定が正しいことを確認します。

エンドポイントの設定

AnyConnect NVMは、次の2つの方法のいずれかで導入できます。a) wAnyConnectパッケージまたはb)wスタンドアロンNVMパッケージを使用します（AnyConnectデスクトップのみ）。

必要な設定は両方の導入で同じですが、違いは信頼ネットワーク検出の設定にあります。

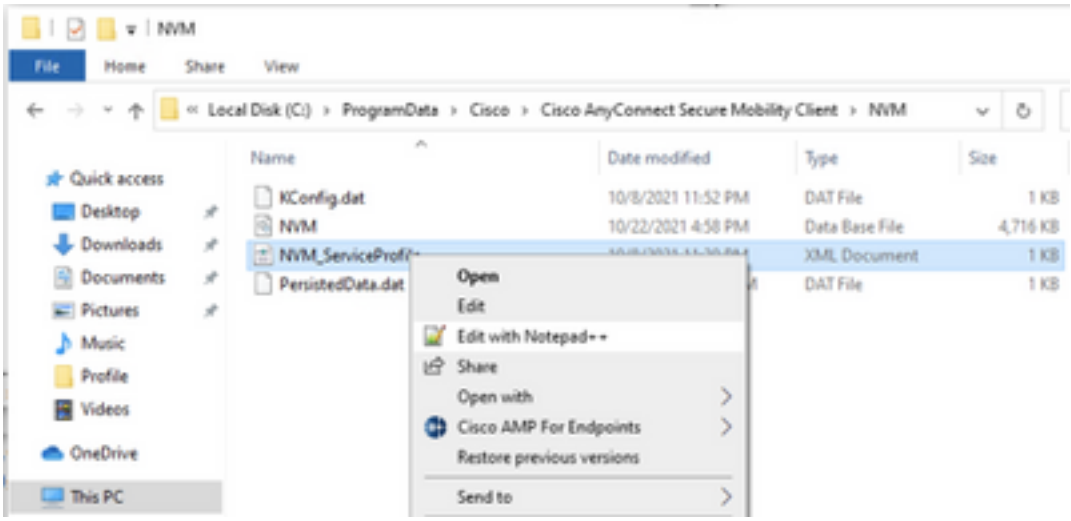
NVMプロファイルの確認

エンドポイントで使用されているNVMプロファイルを見つけ、[Collector Configuration] 設定を確認します。

NVMプロファイルの場所：

- Windows：**%ProgramData%\Cisco\Cisco AnyConnectセキュアモビリティクライアント\NVM**
- MAC：**/opt/cisco/anyconnect/nvm**

注：NVMプロファイルの名前は**NVM_ServiceProfile**にする必要があります。そうしないと、Network Visibility Module(NVISM)がデータの収集と送信に失敗します。



NVMプロファイルの内容は設定によって異なりますが、SNAに関連するプロファイルの要素は太字で示されています。NVMプロファイルの例の後の注意事項を確認してください。

注：設定されているポートが非予約ポートであり、2055、514、または8514でないことを確認します。このプロファイルで設定するポートは、フローコレクタで設定するポートと同じである必要があります。

注：NVMプロファイルに**Secure** XML要素が含まれている場合は、**false**に設定されていることを確認してください。含まれていない場合、フローはDTLSで暗号化されて送信され、フローコレクタでは処理できません。

Trusted Network Detection(TND)設定の確認

Network Visibility Moduleは、信頼できるネットワーク上にある場合にのみフロー情報を送信します。デフォルトでは、データは収集されません。データは、プロファイルでそのように設定されている場合にのみ収集され、エンドポイントが接続されている場合は引き続き収集されます。信頼できないネットワークで収集が行われると、エンドポイントが信頼できるネットワーク上にあるときにキャッシュされ、コレクタに送信されます。Secure Network Analytics Flow Collectorは、キャッシュされたフローを処理するために追加の設定を必要とします(必要な設定については、「オフネットワークキャッシュされたフローのフローコレクタの設定」を参照してください)。

信頼できるネットワークの状態は、VPNのTND機能（VPNプロファイルで設定）またはNVMプロファイルのTND設定によって判断できます。

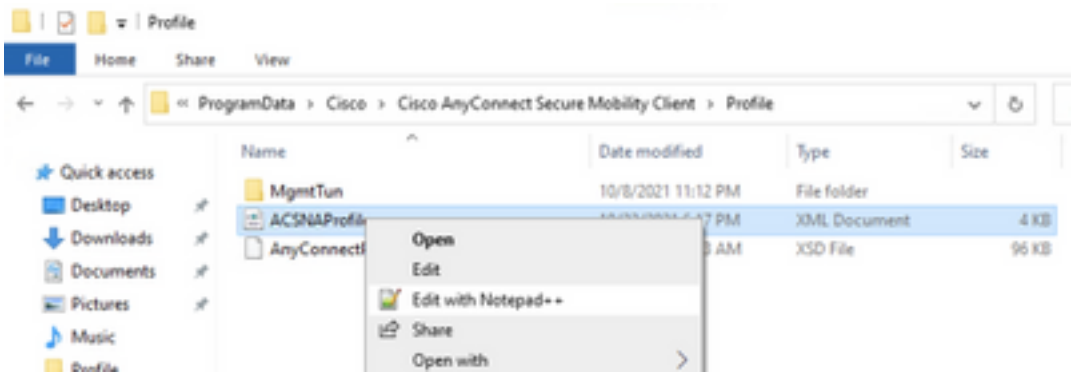
VPNプロファイルのTND設定

> **注**：これは、NVMスタンドアロン導入のオプションではありません。

1.エンドポイントで使用されているVPNプロファイルを特定し、設定されている**自動VPNポリシー**設定を確認します

VPNプロファイルの場所：

- Windows：**%ProgramData%\Cisco\Cisco AnyConnectセキュアモビリティクライアント\プロファイル**
- MAC：**/opt/cisco/anyconnect/profile**
  この例では、VPNプロファイル名は**ACSNAProfile**です。



2.テキストエディタでプロファイルを編集し、**AutomaticVPNPolicy**要素を見つけます。設定したポリシーが、信頼できるネットワークを正常に検出できる正しいものであることを確認します。その場合、次のようになります。

...

> **注**：NVMの関連性：[Trusted Network Policy]と[Untrusted Network Policy]の両方が[Do Nothing]に設定されている場合、VPNプロファイルからの信頼ネットワーク検出は無効になります。

NVMプロファイルのTND設定

エンドポイントで使用されているNVMプロファイルを探し、設定されている信頼できるサーバリストの設定が正しいことを確認します。

NVMプロファイルの場所：

- Windows：%ProgramData%\Cisco\Cisco AnyConnectセキュアモビリティクライアント\NVM
- MAC：/opt/cisco/anyconnect/nvm

...

```
</NVMProfile>
```

注：SSLプローブが設定済みの信頼できるヘッドエンドに送信され、ヘッドエンドが到達可能であれば証明書で応答します。次に、拇印（SHA-256ハッシュ）が抽出され、プロファイルエディタのハッシュセットと照合されます。一致が成功すると、エンドポイントが信頼できるネットワーク内にあることが示されます。ただし、ヘッドエンドが到達不能な場合、または証明書ハッシュが一致しない場合、エンドポイントは信頼できないネットワークにあると見なされます。

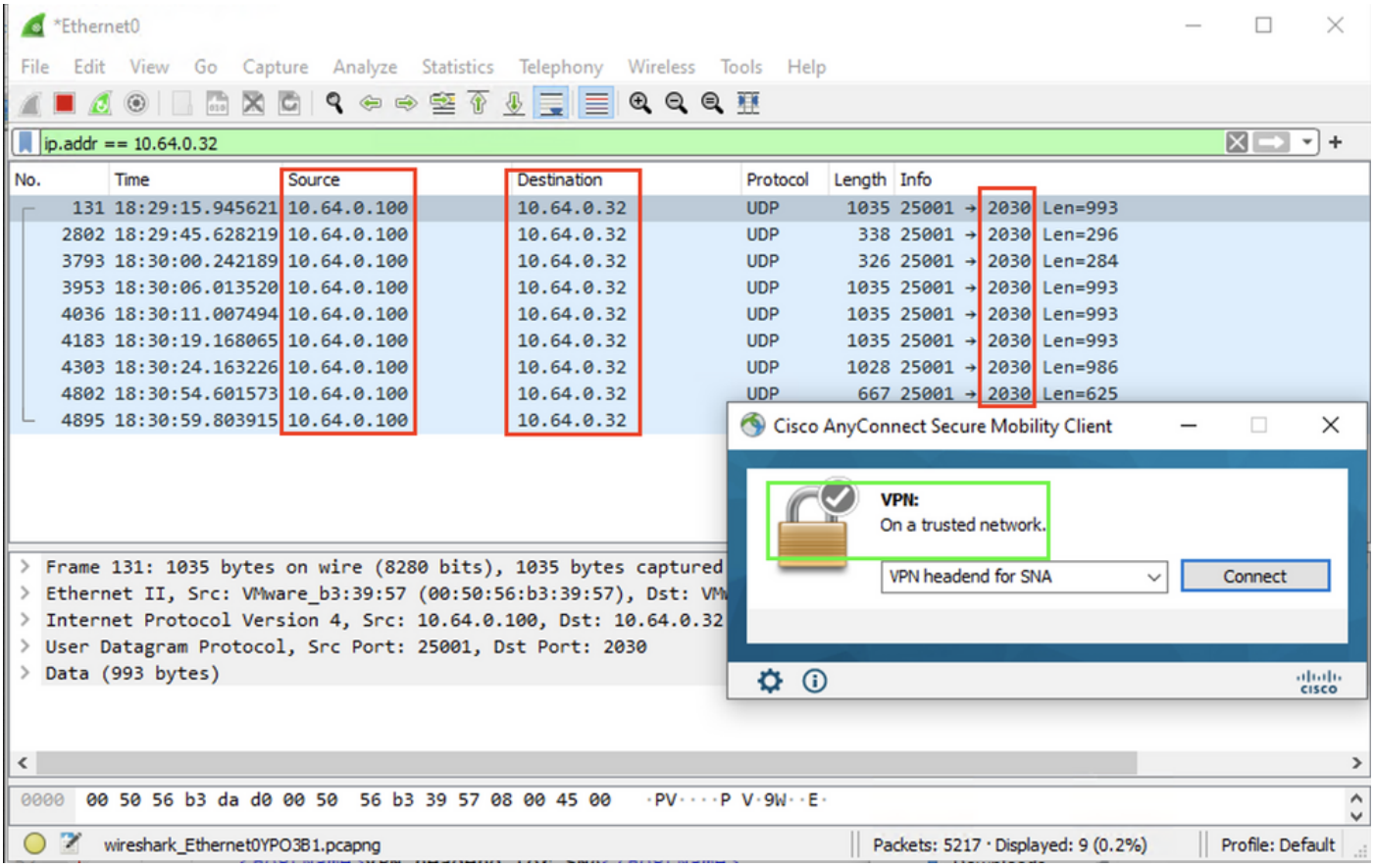
注：プロキシの背後にある信頼されたサーバはサポートされません。

パケットキャプチャの収集

エンドポイントネットワークアダプタでパケットキャプチャを収集して、フローがフローコレクタに送信されたことを確認できます。

a.エンドポイントが信頼できるネットワーク上にあるものの、VPNに接続されていない場合は、物理ネットワークアダプタでキャプチャを有効にする必要があります。

この場合、Anyconnectクライアントは、エンドポイントが信頼できるネットワーク上にあることを示します。つまり、フローは、エンドポイントの物理ネットワークアダプタを介して、設定されたポート経由で、設定されたフローコレクタに送信されます。これは、AnyConnectウィンドウと次に表示されるWiresharkウィンドウで確認できます。

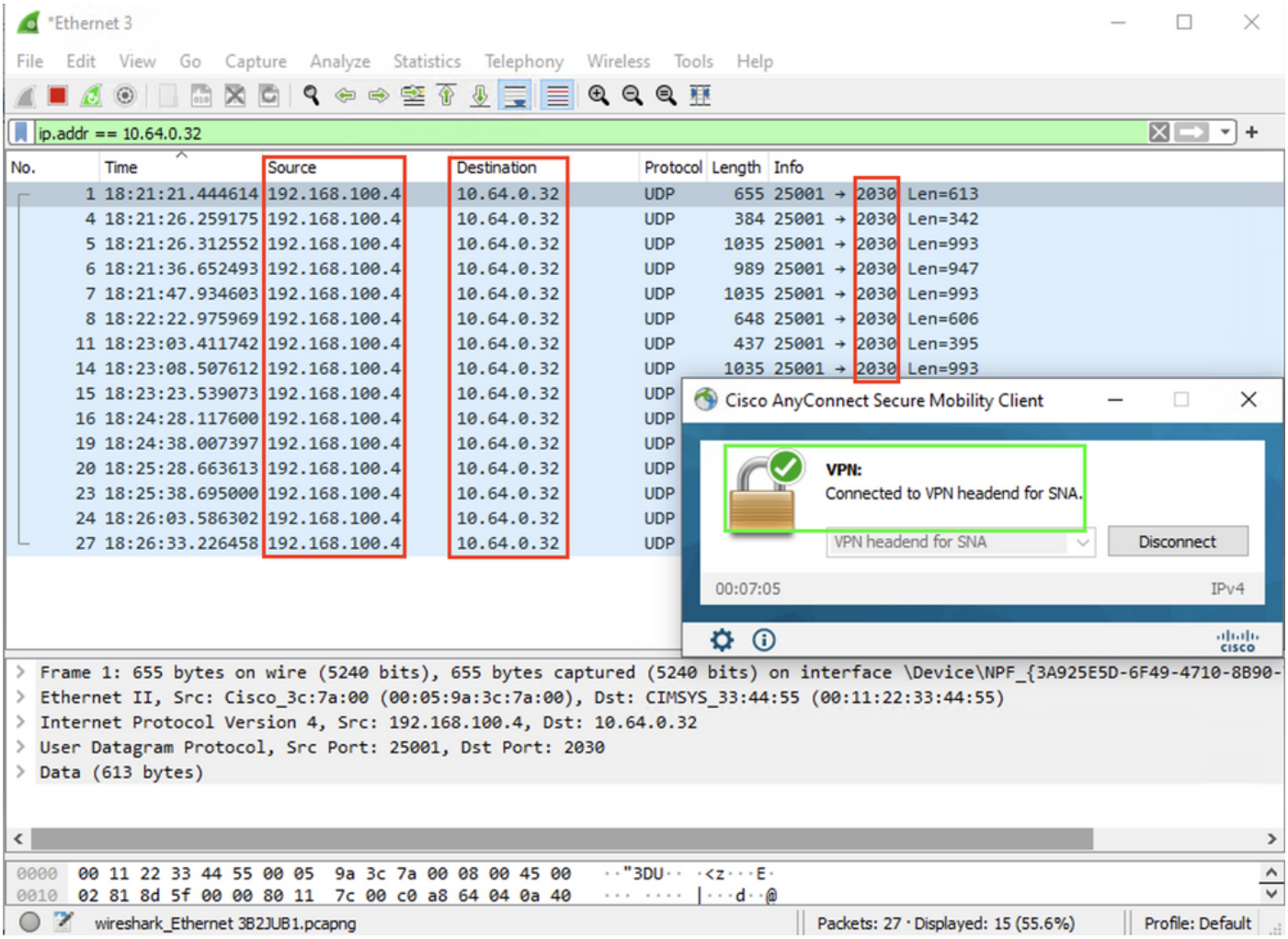


b.エンドポイントがAnyConnect VPNに接続されている場合、そのエンドポイントは自動的に信頼ネットワーク上にあると見なされます。したがって、仮想ネットワークアダプタ上でキャプチャを有効にする必要があります。

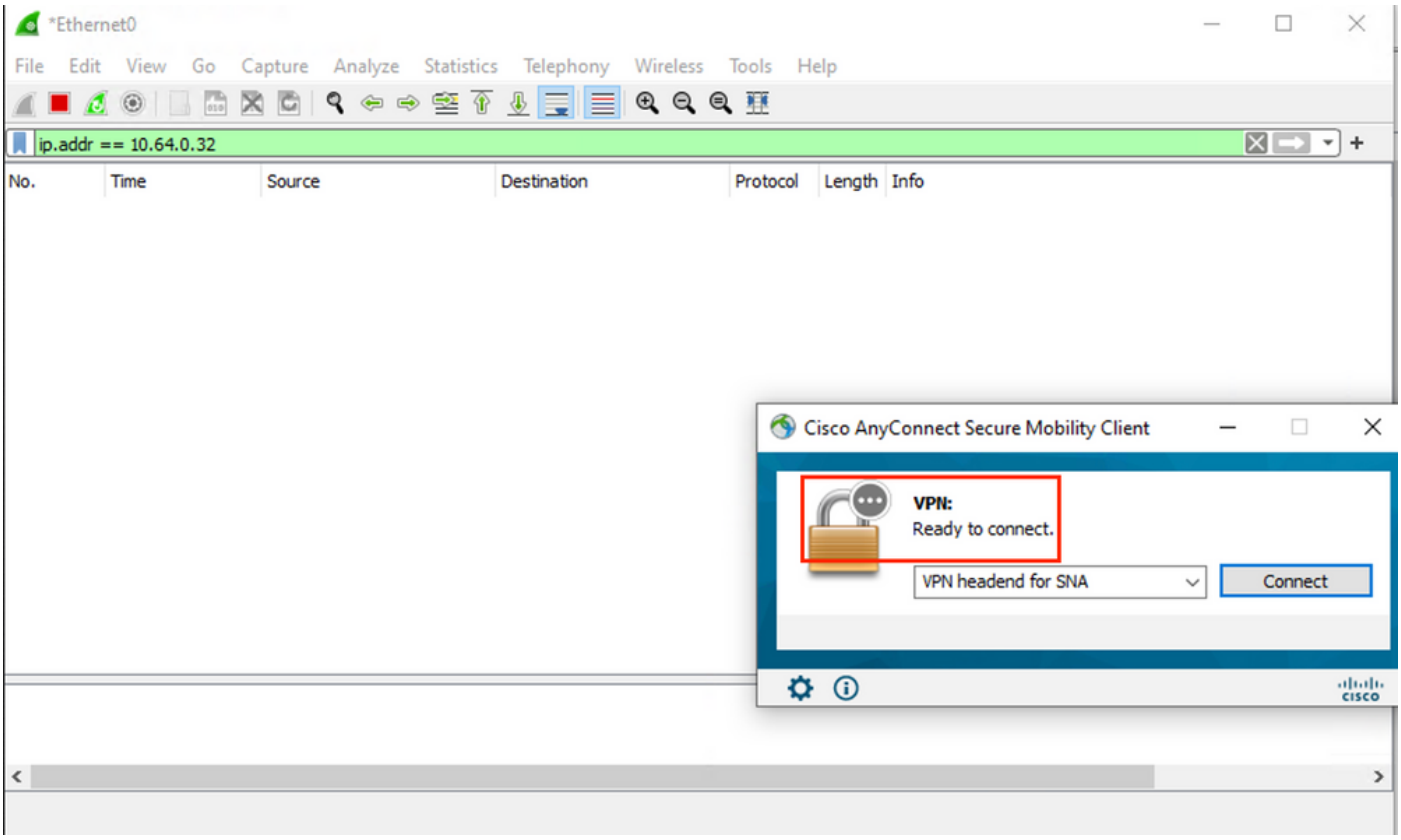
> **注**：VPNモジュールがインストールされ、Network Visibility Moduleプロファイルで**TND**が設定されている場合、Network Visibility ModuleはVPNネットワーク内でも信頼ネットワーク検出を実行します。

AnyConnect Clientは、エンドポイントがVPNに接続されていることを示します。つまり、AnyConnectウィンドウと次に表示されるWiresharkウィンドウで確認できるように、フローは、エンドポイント（VPNトンネル）の仮想ネットワークアダプタを介して、設定されたポート経由で、設定されたフローコレクタに送信されます。

> **注**：エンドポイントが接続されているVPNプロファイルのスプリットトンネル設定には、フローコレクタのIPアドレスが含まれている必要があります。含まれていない場合、フローはVPNトンネルを介して送信されません。



c.エンドポイントが信頼ネットワーク上にない場合、フローはフローコレクタに送信されません。



関連する不具合

現在、Secure Network AnalyticsのNVMテレメトリ取り込みプロセスに影響を与える可能性のある不具合は2つあります。

- FCエンジンがeth1でNVMテレメトリを取り込めません。Cisco Bug ID CSCwb84013を参照してください。
- フローコレクタがAnyConnectバージョン4.10.04071以降のNVMレコードを挿入しない。Cisco Bug ID CSCwb91824

関連情報

- 詳細については、Technical Assistance Center(TAC)にお問い合わせください。有効なサポート契約が必要です。 各国のシスコ サポートの連絡先.
- Cisco Security Analytics Communityには、ここからアクセスすることもできます。
- テクニカル サポートとドキュメント – Cisco Systems