排除AnyConnect网络可视性模块遥测接收安全网络分析中的问题

目录

简介

本文档介绍排除安全网络分析(SNA)中网络可视性模块(NVM)遥测接收问题的过程。

先决条件

- 思科SNA知识
- Cisco AnyConnect知识

配置指南

- 安全网络分析终端许可证和网络可视性模块(NVM)配置指南
- Cisco AnyConnect管理员指南网络可视性模块，版本4.10

要求

- 7.3.2版或更高版本中的SNA Manager和流量收集器
- SNA终端许可证

- 带网络可视性模块4.3或更高版本的Cisco AnyConnect

使用的组件

- SNA Manager和流收集7.4.0版和终端许可证
- 带VPN和网络可视性模块的Cisco AnyConnect 4.10.03104
- Windows 10虚拟机
- Wireshark软件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

故障排除过程

SNA配置

验证许可

确保SNA管理器注册到的智能许可虚拟帐户具有终端许可证。

验证NVM遥测接收

要确认SNA流量收集器是否从终端接收并插入NVM遥测，请按如下步骤操作：

1.通过SSH或具有根凭证的控制台登录到流**量收集**器。

2.运行grep **'NVM records this period:' /lancope/var/sw/today/logs/sw.log命**令。

3.从返回的输出中，确认流量收集器是否接收NVM记录并将其插入数据库。

```
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
```

从此输出中，流量收集器似乎根本没有收到任何NVM记录，但是，您必须确认它是否配置为侦听NVM遥测。

验证流量收集器是否配置为侦听NVM遥测

1.登录到流量收集器管理员用户界面(UI)。

2.导航至“支持”**>“高级设置”**。

3.确保正确配置所需属性：

SNA版本7.3.2或7.4.0

==========

- 找到**nvm_netflow_port属**性并验证配置的值。这必须与AnyConnect NVM配置文件中配置的端口匹配。

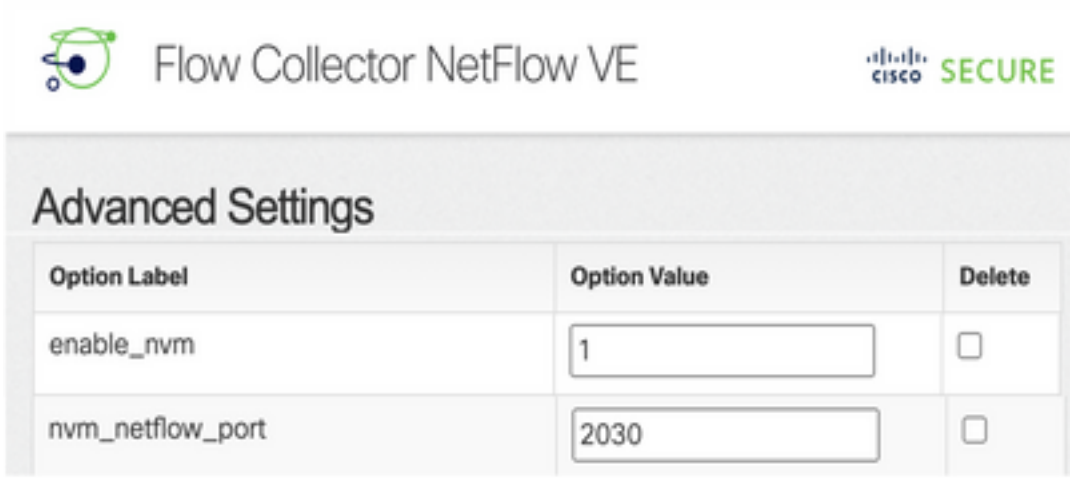
注：确保配置的端口是非保留端口，而不是2055、514或8514。如果配置的值为“0”，则禁用功能。

注意：如果未显示字段，请滚动到页面底部。单击“添**加新选项”**字段。有关流量收集器上高级设置的详细信息，请参阅高级设置联机帮助主题。

SNA版本7.4.1

==========

- 找到**nvm_netflow_port属**性并验证配置的值。这必须与AnyConnect NVM配置文件中配置的端口匹配。
- 找到**enable_nvm属**性并确保将值设置为**1**，否则功能被禁用。



注：确保配置的端口是非保留端口，而不是2055、514或8514。

注意：如果未显示字段，请滚动到页面底部。单击“添**加新选项”**字段。有关流量收集器上高级设置的详细信息，请参阅高级设置联机帮助主题。

4.正确配置流量收集器上的高级设置后，使用与验证NVM遥测接收部分中所述的步骤，验证是否已接收遥测**，以验**证。

5.如果使用AnyConnect NVM的终端配置和流量收集器上的设置正确，则sw.log**文件必**须反映它：

```
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.如果流量收集器仍未接收NVM记录，请验证收集器是否在接口上收到数据包，并在任何情况下确保终端配置正确。

终端配置

您可以通过以下两种方式之一部署AnyConnect NVM:a)w或b)w独立NVM软件包（仅在AnyConnect桌面上）。

两种部署所需的配置相同，差异在于受信任网络检测的配置。

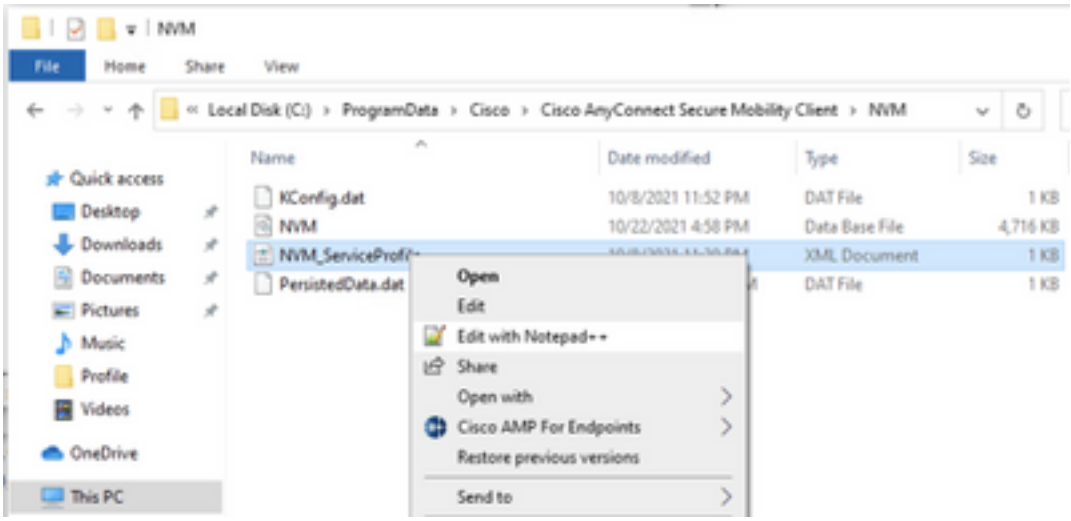
验证NVM配置文件

找到终端使用的NVM配置文件并确认收集器**配置**设置。

NVM配置文件位置：

- Windows 窗口版本:**%ProgramData%\Cisco\Cisco AnyConnect安全移动客户端\NVM**
- MAC :**/opt/cisco/anyconnect/nvm**

注意：NVM配置文件的名称必须是**NVM_ServiceProfile**，否则网络可视性模块无法收集和发送数据。



NVM配置文件的内容取决于您的配置，但与SNA相关的配置文件元素以粗体标记。确保在NVM配置文件示例后查看注释：

注意：确保已**配置的端口是非保留端口，而不是2055、514或8514**。此配置文件中配置的端口需要与流量收集器上配置的端口相同。

注意：确保如果NVM配置文件具有**Secure** XML元素，则其设置为**false**，否则流将使用DTLS进行加密，并且流量收集器无法处理它们。

验证受信任网络检测(TND)设置

网络可视性模块仅在其位于受信任网络时发送流信息。默认情况下，不收集任何数据。只有在配置文件中进行配置时，才会收集数据，并在连接终端时继续收集数据。如果收集是在不受信任的网络上完成的，则当终端在受信任网络上时，收集器会被缓存并发送到收集器。安全网络分析流量收集器需要具有附加配置，以便其处理缓存的流量(请参阅为所需配置的离网缓存流量配置流量收集器)。

可以通过VPN的TND功能（在VPN配置文件中配置）或NVM配置文件中的TND配置确定受信任网络状态：

VPN配置文件中的TND配置

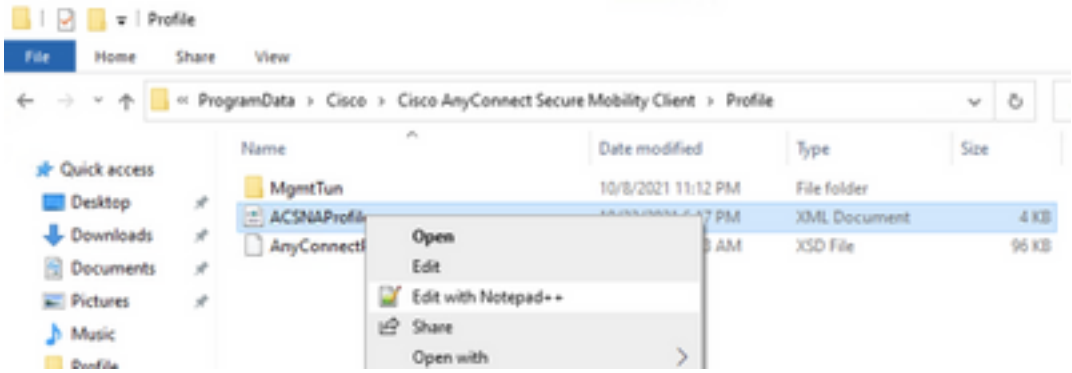
注意：这不是NVM独立部署的选项。

1.找到终端使用的VPN配置文件并确认已配置的“**自动VPN策略”设置**

VPN配置文件位置：

- Windows 窗口版本:**%ProgramData%\Cisco\Cisco AnyConnect安全移动客户端\配置文件**
- MAC :**/opt/cisco/anyconnect/profile**

在本示例中，VPN配置文件名**为ACSNAProfile**。



2.使用文本编辑器编辑配置文件并找到**AutomaticVPNPolicy元**素。确保配置的策略正确，以成功检测受信任网络。在这种情况下：

...

注意：对于NVM相关性：如果“受信任网络策略”(Trusted Network Policy)和“不受信任网络策略”(Untrusted Network Policy)均设置为“不执行任何操作”(Do Nothing)，则会禁用来自VPN配置文件的受信任网络检测(Trusted Network Detection)。

NVM配置文件中的TND配置

找到终端使用的NVM配置文件，并确认已配置的受信**任服务器列**表设置正确。

NVM配置文件位置：

- Windows 窗口版本:**%ProgramData%\Cisco\Cisco AnyConnect安全移动客户端\NVM**
- MAC :**/opt/cisco/anyconnect/nvm**

...

```
</NVMProfile>
```

注意：SSL探测功能将发送到已配置的受信任头端，该头端会以证书（如果可访问）作出响应。然后提取指纹（SHA-256哈希值）并根据配置文件编辑器中的哈希集进行匹配。成功匹配表示终端位于受信任网络中；但是，如果头端不可达，或者证书哈希不匹配，则终端被视为处于不受信任的网络中。

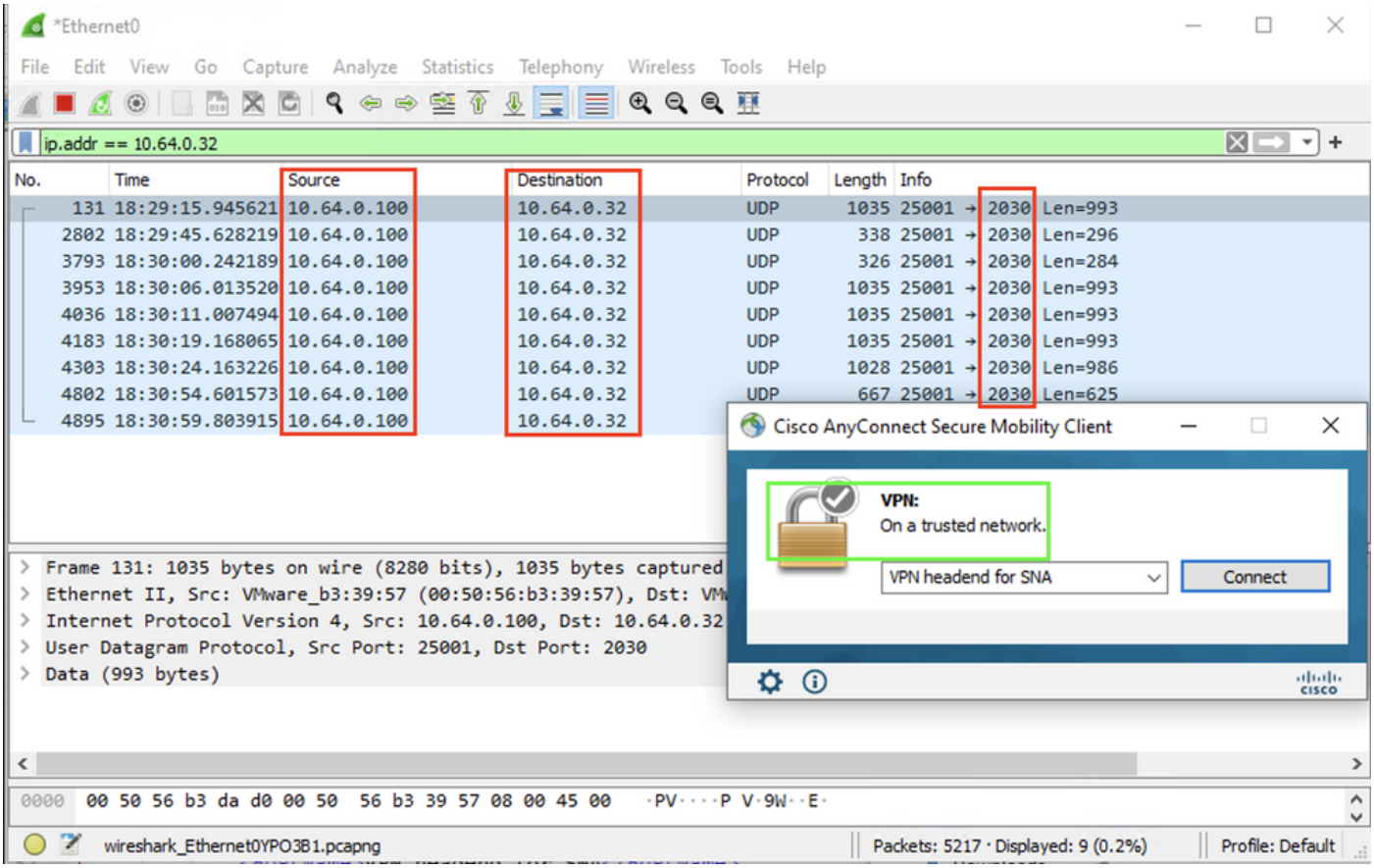
注意：不支持代理后面的受信任服务器。

收集数据包捕获

您可以在终端网络适配器上收集数据包捕获，以验证流是否发送到流量收集器。

a.如果终端在受信任网络上，但未连接到VPN，则必须在物理网络适配器上启用捕获。

在这种情况下，AnyConnect客户端指示终端在受信任网络上，这意味着流通过终端的物理网络适配器通过已配置端口发送到已配置的流量收集器，如我们在AnyConnect窗口和下面显示的Wireshark窗口中所示。

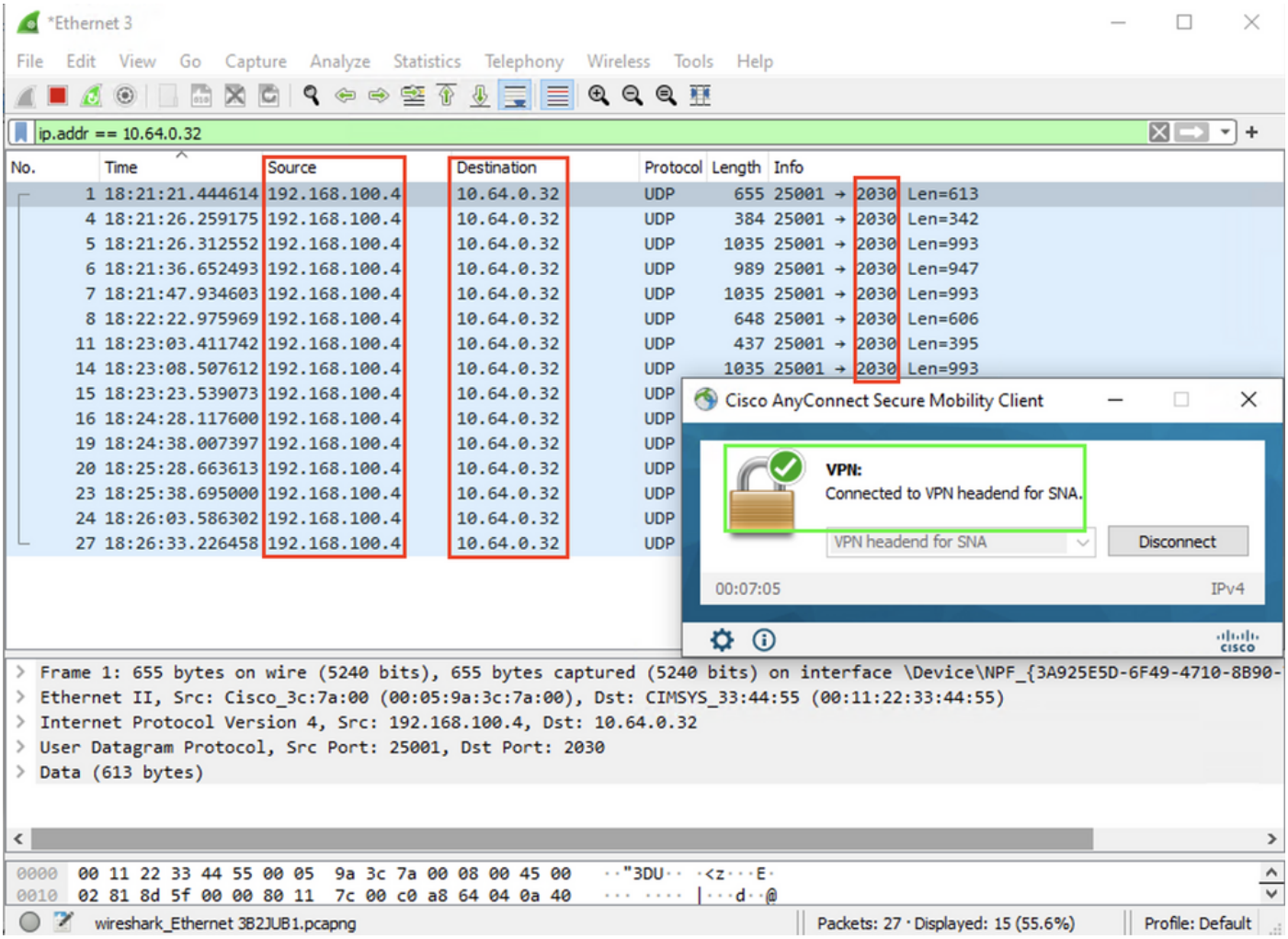


b.如果终端连接到AnyConnect VPN，则自动将其视为在受信任网络上，因此必须在虚拟网络适配器上启用捕获。

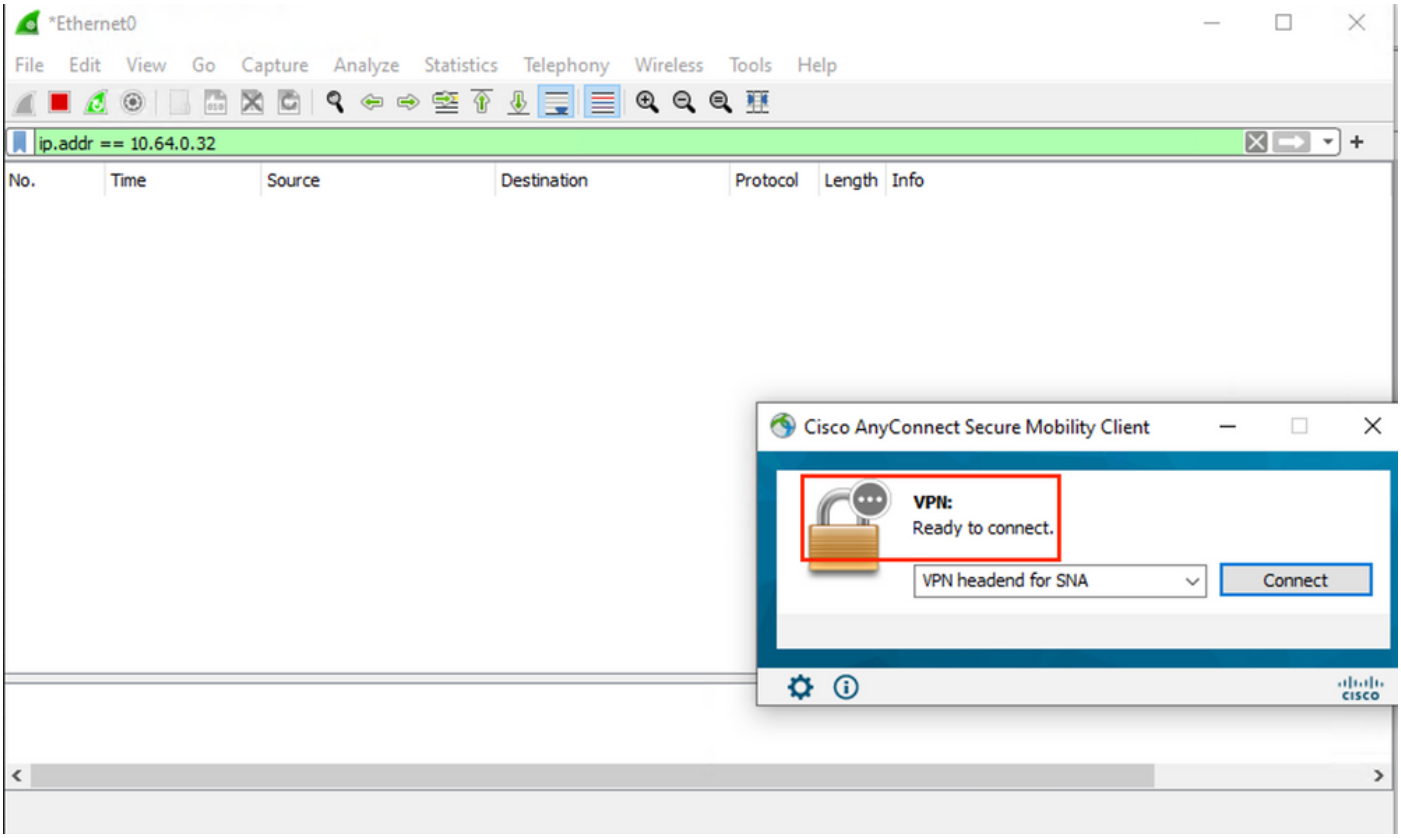
注意：如果VPN模块已安装，且TND已在网络可视性模块配置文件中配置，则网络可视性模块即使在VPN网络内也会执行受信任网络检测。

AnyConnect客户端指示终端已连接到VPN，这意味着流通过终端的虚拟网络适配器（VPN隧道）通过已配置端口发送到已配置的流量收集器，如我们在AnyConnect窗口和下面显示的Wireshark窗口中所示。

> **注意**：终端连接的VPN配置文件的拆分隧道配置必须包括流量收集器的IP地址，否则流不会通过VPN隧道发送。



c.如果终端不在受信任网络上，流不会发送到流量收集器。



相关问题

目前有两个已知缺陷可能影响安全网络分析的NVM遥测接收过程：

- FC引擎无法在eth1上接收NVM遥测。请参阅Cisco Bug ID CSCwb84013
- 流量收集器不从AnyConnect版本4.10.04071或更高版本插入NVM记录。请参阅Cisco Bug ID CSCwb91824

相关信息

- 如需其他帮助，请联系技术支持中心(TAC)。需要有效的支持合同： 思科全球支持联系方式.
- 您还可以访问思科安全分析社区。
- 技术支持和文档 - Cisco Systems