在安全網路分析中排除AnyConnect網路可視性模組遙測接收問題

目錄

[簡介](#)
[必要條件](#)
[疑難排解技術筆記](#)
[需求](#)
[採用元件](#)
[疑難排解程式](#)
[SNA配置](#)
[驗證許可](#)
[驗證NVM遙測接收](#)
[驗證流量收集器是否配置為偵聽NVM遙測](#)
[終端配置](#)
[驗證NVM配置檔案](#)
[驗證受信任網路檢測(TND)設定](#)
[VPN配置檔案中的TND配置](#)
[NVM配置檔案中的TND配置](#)
[收集資料包捕獲](#)
[相關缺陷](#)
[相關資訊](#)

簡介

本檔案介紹在安全網路分析(SNA)中排解網路可見性模組(NVM)遙測接收問題疑難問題的程式。

必要條件

- Cisco SNA知識
- Cisco AnyConnect知識

疑難排解技術筆記

- 安全網路分析端點許可證和網路可視性模組(NVM)配置指南
- Cisco AnyConnect管理員指南網路可視性模組版本4.10

需求

- 7.3.2版或更新版本中的SNA管理員和流量收集器
- SNA終端許可證

- Cisco AnyConnect with Network Visibility Module 4.3或更高版本

採用元件

- SNA管理員和流量收集版本7.4.0和終端許可證
- 含VPN和網路可視性模03104的Cisco AnyConnect 4.10.1
- Windows 10虛擬機器
- Wireshark軟體

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

疑難排解程式

SNA配置

驗證許可

確保SNA管理器註冊到的智慧許可虛擬帳戶具有終端許可證。

驗證NVM遙測接收

要確認SNA流量收集器是否從終端接收和插入NVM遙測，請按照以下步驟操作：

1.使用**root**憑據通過SSH或控制檯登入到流量收集器。

2.運行**grep 'NVM records this period:' /lancope/var/sw/today/logs/sw.log**命令。

3.從返回的輸出中，確認流量收集器是否接收NVM記錄並將其插入資料庫。

```
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
```

從此輸出中，流量收集器似乎根本沒有收到任何NVM記錄，但是您必須確認它是否配置為偵聽NVM遙測。

驗證流量收集器是否配置為偵聽NVM遙測

1.登入到流量收集器管理使用者介面(UI)。

2.導航至**支援>高級設定**。

3.確保所需的屬性配置正確：

SNA 7.3.2或7.4.0版

==========

- 找到**nvm_netflow_port**屬性並驗證配置的值。此配置必須與AnyConnect NVM配置檔案中配置的埠匹配。

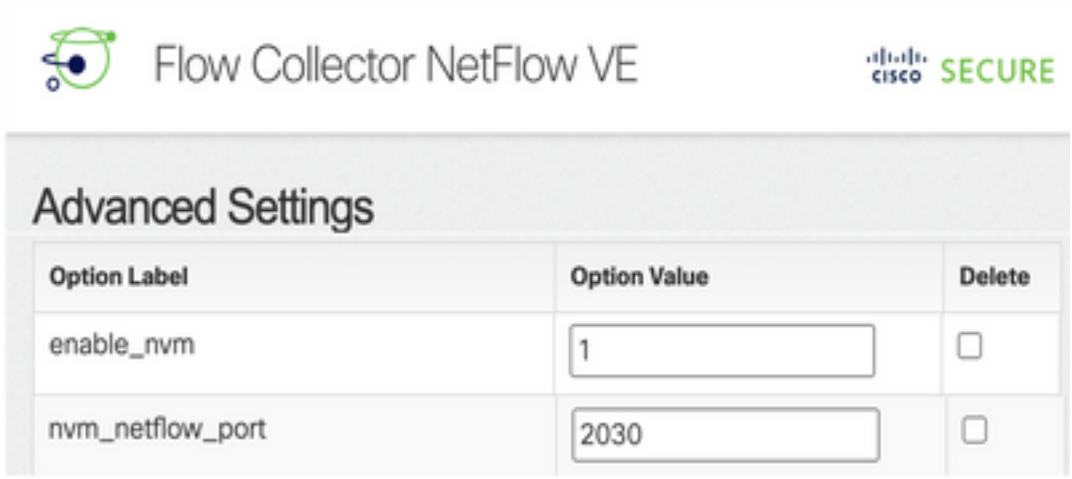
註：確保配置的埠是非保留埠，不是2055、514或8514。如果配置的值為「0」，則禁用該功能。

註：如果未顯示欄位，請滾動到頁面底部。按一下**Add New Option**欄位。有關流量收集器上的高級設定的詳細資訊，請參閱「高級設定」聯機幫助主題。

SNA版本7.4.1

==========

- 找到**nvm_netflow_port**屬性並驗證配置的值。此配置必須與AnyConnect NVM配置檔案中配置的埠匹配。
- 找到**enable_nvm**屬性並確保將該值設定為**1**，否則禁用該功能。



註：確保配置的埠是非保留埠，不是2055、514或8514。

註：如果未顯示欄位，請滾動到頁面底部。按一下**Add New Option**欄位。有關流量收集器上的高級設定的詳細資訊，請參閱「高級設定」聯機幫助主題。

4.正確配置流量收集器上的高級設定後，使用**驗證NVM遙測接收**部分中所述的相同步驟驗證遙測現在是否已被接收。

5.如果使用AnyConnect NVM的終端配置以及流量收集器上的設定正確，**sw.log**檔案必須反映它：

```
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.如果流量收集器仍不接收NVM記錄，請驗證收集器是否在該介面上收到資料包，在任何情況下，確保端點的配置正確。

終端配置

您可以通過以下兩種方式之一部署AnyConnect NVM:a)w使用AnyConnect軟體包或b)w使用獨立NVM包（僅限AnyConnect案頭）。

兩種部署所需的配置相同，不同之處在於受信任網路檢測的配置。

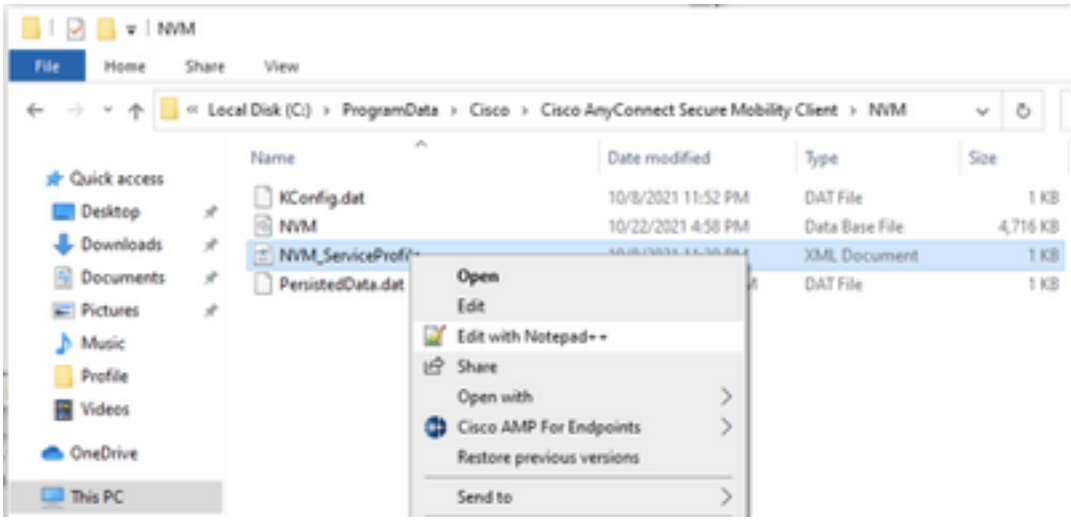
驗證NVM配置檔案

找到終端使用的NVM配置檔案並確認收集器**配置**設定。

NVM配置檔案位置：

- Windows:**%ProgramData%\Cisco\Cisco AnyConnect安全移動客戶端\NVM**
- Mac:**/opt/cisco/anyconnect/nvm**

附註：NVM配置檔案的名稱必須是**NVM_ServiceProfile**，否則網路可視性模組無法收集和傳送資料。



NVM配置檔案的內容取決於您的配置，但是與SNA相關的配置檔案元素以粗體標籤。確保在NVM配置檔案示例之後檢視註釋：

附註：請確保已**配置的埠是非保留埠，不是2055、514或8514**。此配置檔案中配置的埠必須與流量收集器上配置的埠相同。

附註：確保NVM配置檔案具有**Secure** XML元素，將其設定為**false**，否則將使用DTLS對流進行加密並且流收集器無法處理這些流。

驗證受信任網路檢測(TND)設定

網路可視性模組僅在流量資訊位於可信網路時才傳送該資訊。預設情況下，不收集任何資料。僅當在配置檔案中如此配置時才會收集資料，並且在端點連線時繼續收集資料。如果收集是在不受信任的網路上完成的，則當終端在受信任的網路上時，將快取收集並將其傳送到收集器。安全網路分析流量收集器需要具有其他配置才能處理快取流(有關所需配置，請參閱為離網快取流配置流量收集器)。

可信網路狀態可以由VPN的TND功能（在VPN配置檔案中配置）或NVM配置檔案中的TND配置確定：

VPN配置檔案中的TND配置

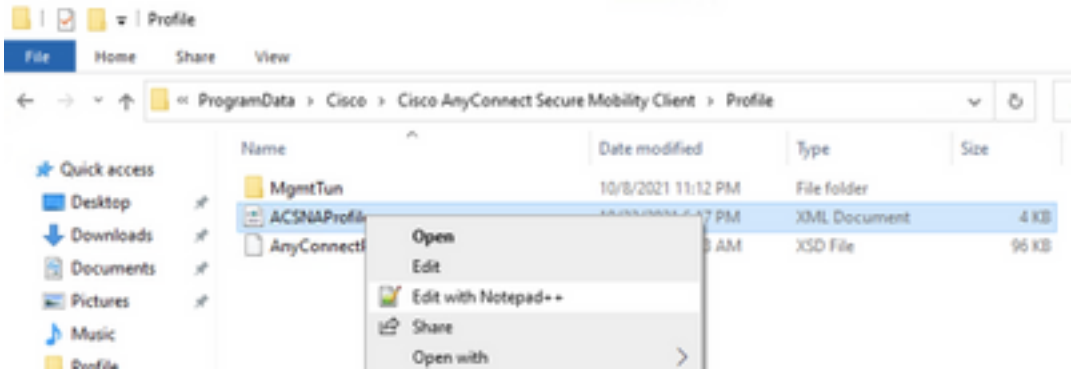
附註：這不是用於NVM獨立部署的選項。

1.找到終端使用的VPN配置檔案，並確認已配置的**自動VPN策略**設定

VPN配置檔案位置：

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

在此示例中，VPN配置檔名為**ACSNAProfile**。



2.使用文本編輯器編輯配置檔案，並找到**AutomaticVPNPolicy**元素。確保配置的策略正確，以便成功檢測受信任網路。在這種情況下：

...

附註：對於NVM相關性：如果受信任網路策略和不受信任網路策略都設定為Do Nothing，則會禁用VPN配置檔案中的受信任網路檢測。

NVM配置檔案中的TND配置

找到終端使用的NVM配置檔案，並確認配置的「受信任**伺服器清單**」設定正確。

NVM配置檔案位置：

- Windows:**%ProgramData%\Cisco\Cisco AnyConnect安全移動客戶端\NVM**
- Mac:**/opt/cisco/anyconnect/nvm**

...

```
</NVMProfile>
```

附註：將SSL探測傳送到已配置的可信任頭端，如果可以訪問，則使用證書進行響應。然後提取指紋（SHA-256雜湊）並與配置檔案編輯器中的雜湊集進行匹配。成功的匹配表示端點位於受信任網路中；但是，如果頭端無法訪問，或者證書雜湊不匹配，則認為端點位於不受信任的網路中。

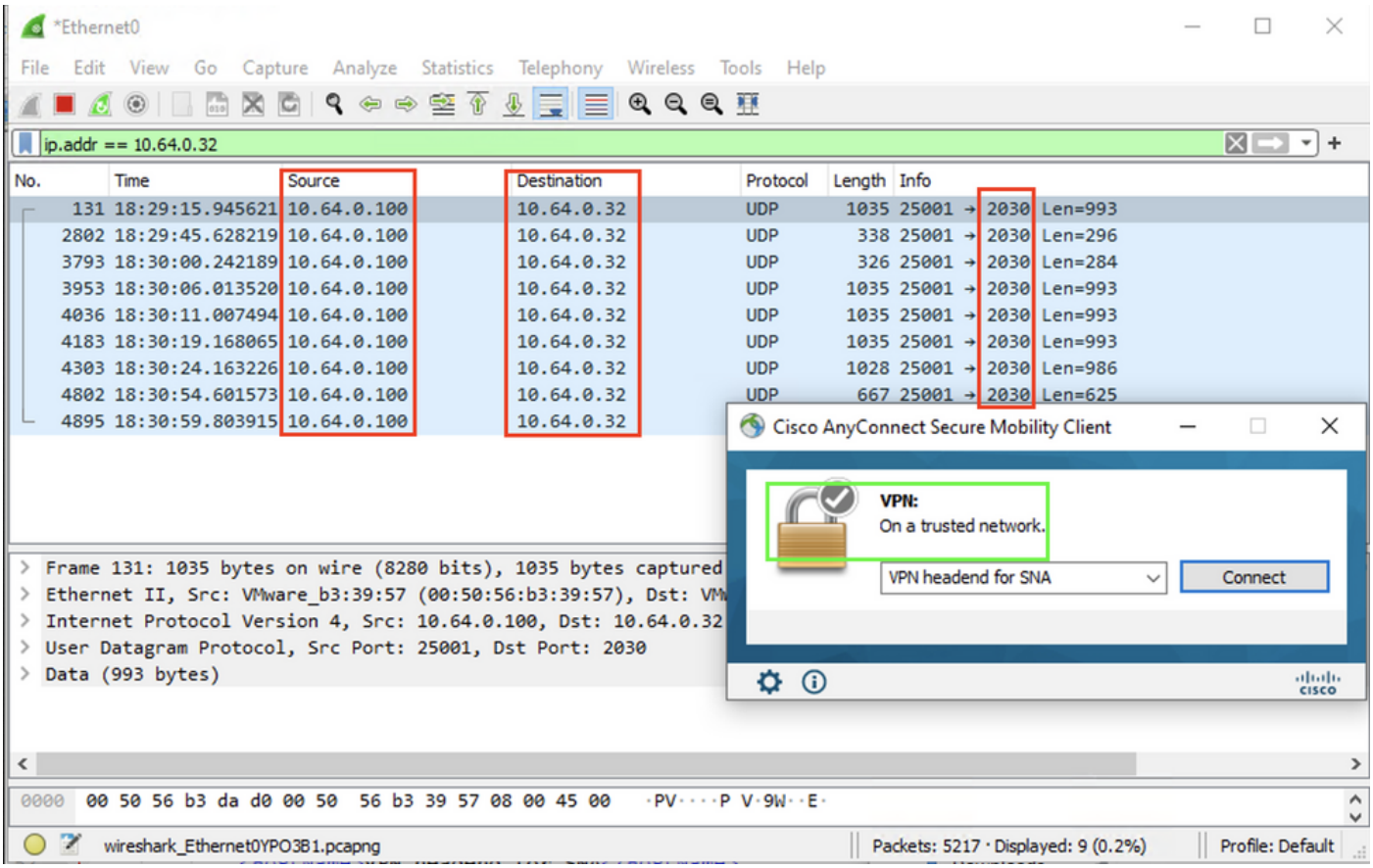
附註：不支援代理背後的受信任伺服器。

收集資料包捕獲

您可以在終端網路介面卡上收集資料包捕獲，以驗證流是否已傳送到流量收集器。

a.如果終端位於受信任網路但未連線到VPN，則必須在物理網路介面卡上啟用捕獲。

在這種情況下，Anyconnect客戶端指示端點位於受信任網路上，這意味著流通過端點的物理網路介面卡通過已配置的埠傳送到已配置的流量收集器，如我們在AnyConnect視窗和隨後顯示的Wireshark視窗中所看到的。



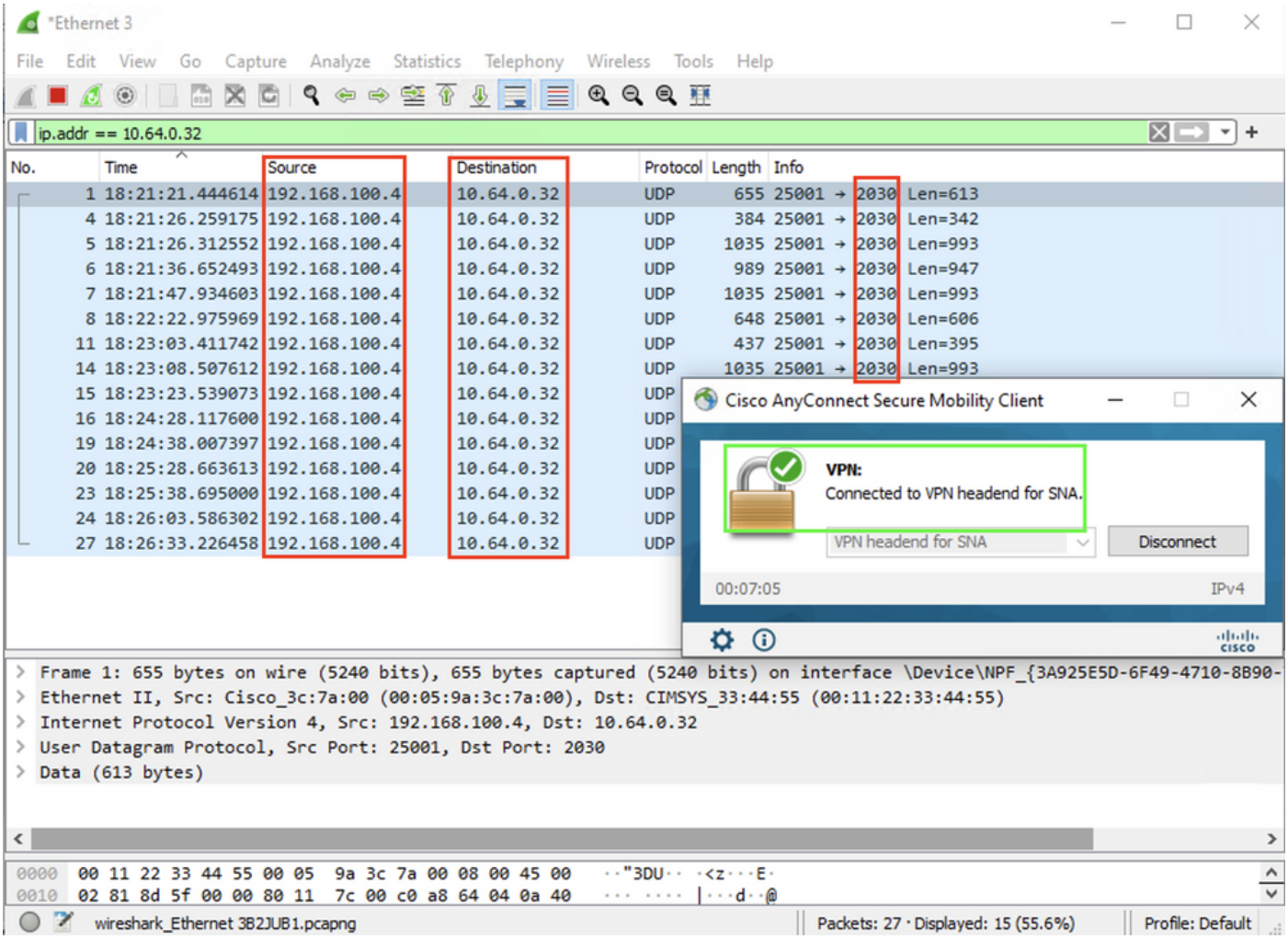
b.如果終端已連線到AnyConnect VPN，則會自動將其視為在受信任網路上，因此必須在虛擬網路介面卡上啟用捕獲。

附註：如果安裝了VPN模組並在網路可視性模組配置檔案中配置了TND，則網路可視性模組即使在VPN網路內部也會執行受信任的網路檢測。

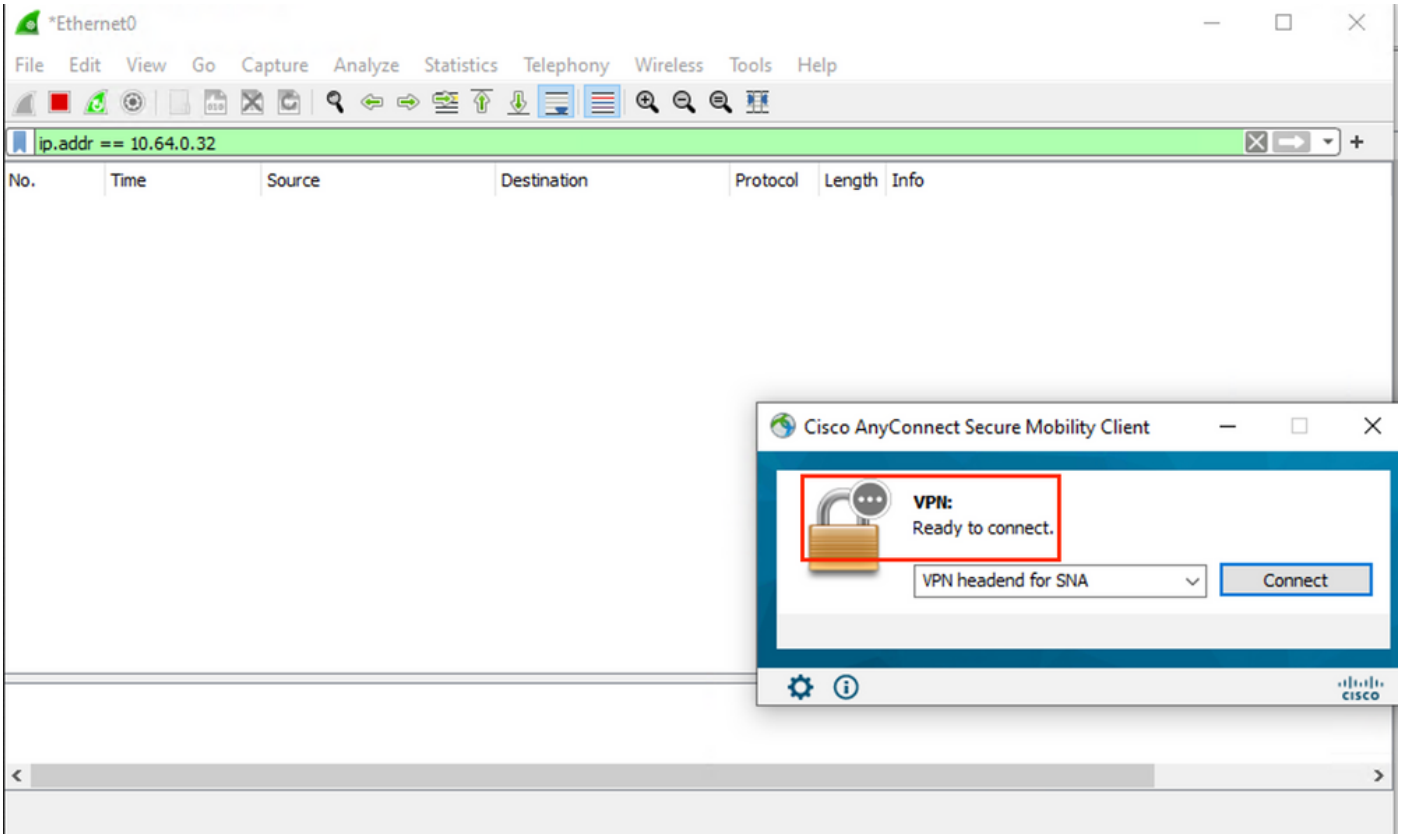
AnyConnect客戶端指示終端已連線到VPN，這意味著流通過終端的虛擬網路介面卡（VPN隧道）通

過配置的埠傳送到已配置的流量收集器，我們可以在下面顯示的AnyConnect視窗和Wireshark視窗中看到。

> **附註**：終端所連線的VPN配置檔案的拆分隧道配置必須包括流量收集器的IP地址，否則不會通過VPN隧道傳送流。



c.如果終端不在受信任網路上，則不會將流傳送到流量收集器。



相關缺陷

當前存在兩個已知缺陷，可能會影響安全網路分析上的NVM遙測接收流程：

- FC引擎無法在eth1上接收NVM遙測。請參閱思科錯誤ID CSCwb84013
- Flow Collector未插入來自AnyConnect 4.10.0版或更高版04071的NVM記錄。請參閱思科錯誤ID CSCwb91824

相關資訊

- 如需其他協助，請聯絡技術協助中心(TAC)。需要有效的支援合約： 思科全球支援聯絡人.
- 您還可以在此處訪問思科安全分析社群。
- 技術支援與文件 - Cisco Systems