보안 네트워크 분석에서 AnyConnect Network Visibility Module 텔레메트리 수집 문제 해결

목차

소개

이 문서에서는 SNA(Secure Network Analytics)에서 NVM(Network Visibility Module) 텔레메트리 수집 문제를 해결하는 절차에 대해 설명합니다.

사전 요구 사항

- Cisco SNA 지식
- Cisco AnyConnect 지식

구성 가이드

- Secure Network Analytics 엔드포인트 라이센스 및 NVM(Network Visibility Module) 컨피그레이션 가이드
- Cisco AnyConnect 관리자 가이드 Network Visibility Module, 릴리스 4.10

요구 사항

- 버전 7.3.2 이상의 SNA Manager 및 Flow Collector

- SNA 엔드포인트 라이센스
- Cisco AnyConnect with Network Visibility Module 4.3 이상

사용되는 구성 요소

- SNA Manager 및 Flow Collect 버전 7.4.0 및 엔드포인트 라이센스
- Cisco AnyConnect 4.10.03104 with VPN and Network Visibility Module
- Windows 10 가상 컴퓨터
- Wireshark 소프트웨어

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제 해결 프로세스

SNA 컨피그레이션

라이센스 확인

SNA Manager가 등록된 Smart Licensing Virtual Account에 엔드포인트 라이센스가 있는지 확인합니다.

NVM 텔레메트리 수집 확인

SNA Flow Collector가 엔드포인트에서 NVM 텔레메트리를 수신하고 삽입하는지 확인하려면 다음과 같이 진행합니다.

1. SSH 또는 **루트** 자격 증명을 사용하여 Flow Collector에 로그인합니다.

2. grep **'NVM records this period:' /lancope/var/sw/today/logs/sw.log** 명령을 실행합니다.

3. 반환된 출력에서 플로우 수집기가 NVM 레코드를 수집하여 데이터베이스에 삽입하는지 확인합니다.

```
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
```

이 출력에서 플로우 컬렉터가 NVM 레코드를 전혀 받지 못한 것으로 보이지만 NVM 텔레메트리를 수신하도록 구성되었는지 확인해야 합니다.

플로우 컬렉터가 NVM 텔레메트리를 수신하도록 구성되었는지 확인합니다.

1. Flow Collector Admin User Interface(UI)에 로그인합니다.

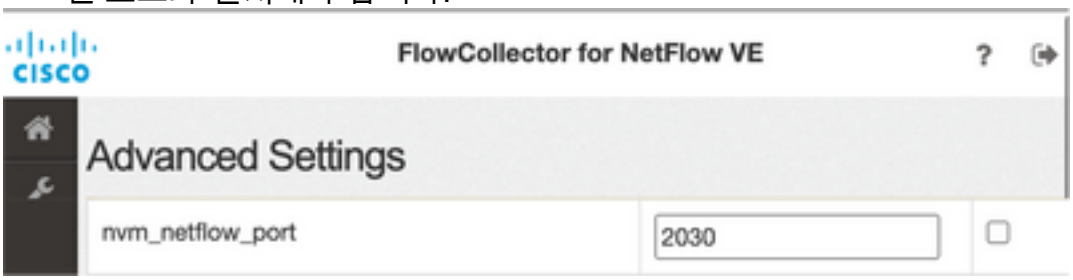
2. **지원 > 고급 설정으로 이동합니다**.

3. 필요한 속성이 올바르게 구성되었는지 확인합니다.

SNA 버전 7.3.2 또는 7.4.0

==========

- nvm_**netflow_port** 특성을 찾고 구성된 값을 확인합니다. 이는 AnyConnect NVM 프로필에 구성된 포트와 일치해야 합니다.



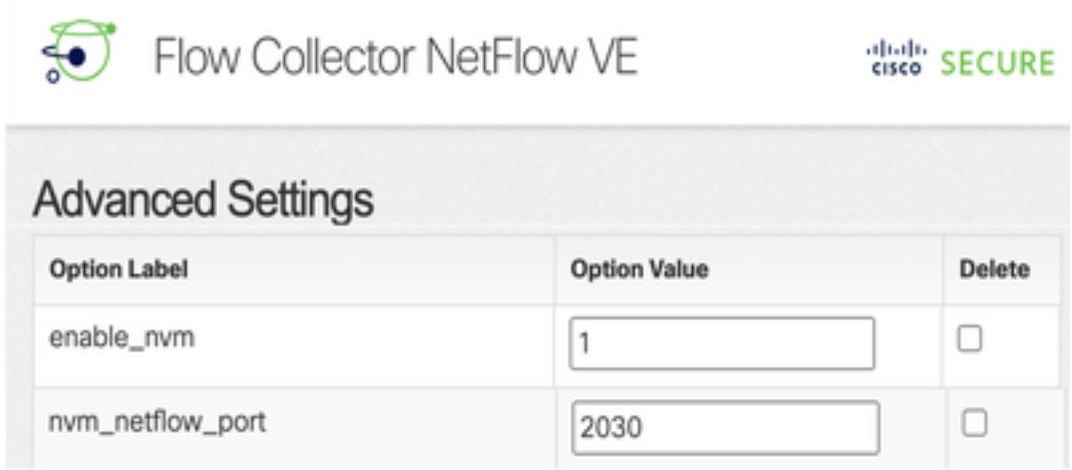
참고: 구성된 포트가 예약되지 않은 포트이며 2055, 514 또는 8514가 아닌지 확인합니다. 구성된 값이 "0"이면 기능이 비활성화됩니다.

참고: 필드가 표시되지 않으면 페이지 아래쪽으로 스크롤합니다. Add **New Option** 필드를 클릭합니다. 플로우 컬렉터의 고급 설정에 대한 자세한 내용은 고급 설정 온라인 도움말 항목을 참조하십시오.

SNA 버전 7.4.1

==========

- nvm_**netflow_port** 특성을 찾고 구성된 값을 확인합니다. 이는 AnyConnect NVM 프로필에 구성된 포트와 일치해야 합니다.
- enable_**nvm** 특성을 찾고 값이 **1**로 설정되어 있는지, 그렇지 않으면 기능이 비활성화됩니다.



참고: 구성된 포트가 예약되지 않은 포트이며 2055, 514 또는 8514가 아닌지 확인합니다.

참고: 필드가 표시되지 않으면 페이지 아래쪽으로 스크롤합니다. Add **New Option** 필드를 클릭합니다. 플로우 컬렉터의 고급 설정에 대한 자세한 내용은 고급 설정 온라인 도움말 항목을 참조하십시오.

4. Flow Collector의 고급 설정이 올바르게 구성되면 Verify NVM Telemetry Ingest(**NVM 텔레메트리 수집 확인**) 섹션에 설명된 것과 동일한 절차를 사용하여 텔레메트리를 지금 **사용하는지** 확인합니다 .

5. AnyConnect NVM을 사용하는 엔드포인트의 컨피그레이션 및 플로우 컬렉터의 설정이 올바르면 sw.log 파일에 다음 항목이 반영되어야 합니다.

```
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. Flow Collector가 여전히 NVM 레코드를 수집하지 않는 경우, 컬렉터가 인터페이스에서 패킷을 수신하는지 확인하고, 어떤 경우든 엔드포인트의 구성이 올바른지 확인합니다.

엔드포인트 컨피그레이션

다음 두 가지 방법 중 하나로 AnyConnect NVM을 구축할 수 있습니다. a) wAnyConnect 패키지 또는 b) w독립형 NVM 패키지 사용(AnyConnect 데스크톱에만 해당)

필요한 컨피그레이션은 두 구축 모두에 대해 동일하며, 차이점은 Trusted Network Detection 컨피그레이션에 있습니다.

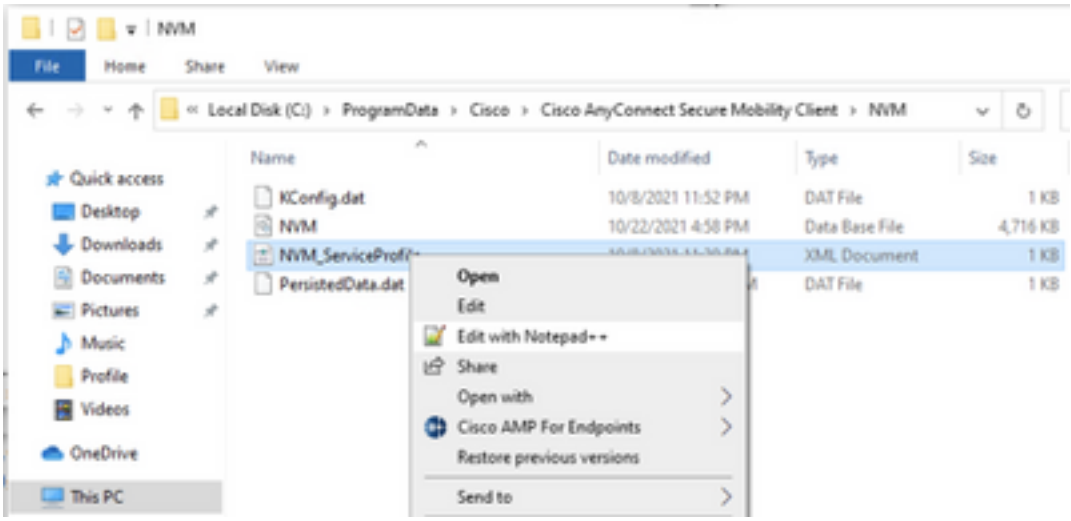
NVM 프로필 확인

엔드포인트에서 사용하는 NVM 프로파일을 찾고 **컬렉터 컨피그레이션** 설정을 확인합니다.

NVM 프로필 위치:

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

참고: NVM 프로필의 이름은 **NVM_ServiceProfile**이어야 합니다. 그렇지 않으면 Network Visibility Module이 데이터를 수집 및 전송하지 못합니다.



NVM 프로파일의 내용은 컨피그레이션에 따라 다르지만, SNA와 관련된 프로파일의 요소는 굵은 글꼴로 표시됩니다. NVM 프로파일 예시 후 메모를 검토하려면 다음을 수행합니다.

참고: 구성된 **포트가 예약되지 않은 포트이며 2055, 514 또는 8514가 아닌지 확인합니다**. 이 프로파일의 구성된 포트는 플로우 컬렉터에 구성된 포트와 동일해야 합니다.

참고: NVM 프로파일에 **Secure** XML 요소가 있는 경우 이 요소가 **false로** 설정되어 있는지, 그렇지 않으면 플로우가 DTLS로 암호화되어 전송되고 Flow 컬렉터에서 처리할 수 없는지 확인합니다.

TND(Trusted Network Detection) 설정 확인

Network Visibility Module은 플로우 정보가 신뢰할 수 있는 네트워크에 있는 경우에만 흐름 정보를 전송합니다. 기본적으로 어떤 데이터도 수집되지 않습니다. 데이터는 프로파일에 이와 같이 구성된 경우에만 수집되며 엔드포인트가 연결될 때 데이터는 계속 수집됩니다. 신뢰할 수 없는 네트워크에서 수집을 수행하는 경우, 엔드포인트가 신뢰할 수 있는 네트워크에 있을 때 컬렉터로 캐시되고 전송됩니다. Secure Network Analytics Flow Collector는 캐시된 플로우를 처리하려면 추가 컨피그레이션을 가져야 합니다(필요한 컨피그레이션에 대해서는 네트워크 외 캐시 플로우에 대한 플로우 컬렉터 구성을 참조하십시오.)

신뢰할 수 있는 네트워크 상태는 VPN의 TND 기능(VPN 프로파일에서 구성) 또는 NVM 프로파일의 TND 컨피그레이션에 의해 결정됩니다.

VPN 프로파일의 TND 컨피그레이션

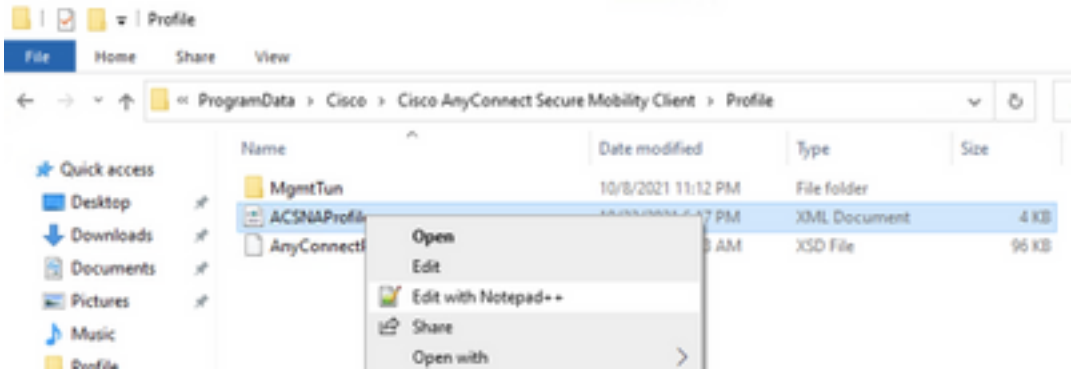
> **참고:** 이는 NVM 독립형 구축에 대한 옵션이 아닙니다.

1. 엔드포인트에서 사용하는 VPN 프로파일을 찾고 구성된 **자동 VPN 정책** 설정을 확인합니다.

   VPN 프로파일 위치:

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

   이 예에서 VPN 프로파일의 이름은 ACSNAProfile**입니다**.



2. 텍스트 편집기로 프로파일을 편집하고 AutomaticVPNPolicy 요소를 찾습니다. 구성된 정책이 신뢰할 수 있는 네트워크를 성공적으로 탐지하도록 올바른지 확인합니다. 이 경우:

. . .

> **참고:** NVM 관련성: Trusted Network Policy(신뢰할 수 있는 네트워크 정책)와 Untrusted Network Policy(신뢰할 수 없는 네트워크 정책)가 모두 Do Nothing(아무 작업도 하지 않음)으로 설정되어 있으면 VPN 프로필의 Trusted Network Detection(신뢰할 수 있는 네트워크 탐지)이 비활성화됩니다.

NVM 프로파일의 TND 컨피그레이션

엔드포인트에서 사용하는 NVM 프로파일을 찾고 구성된 **신뢰할 수 있는 서버 목록** 설정이 올바른지 확인합니다.

NVM 프로필 위치:

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

...

```
</NVMProfile>
```

참고: SSL 프로브는 구성된 신뢰할 수 있는 헤드엔드로 전송되며, 이 헤드엔드는 연결 가능한 경우 인증서로 응답합니다. 그런 다음 지문(SHA-256 해시)을 추출하여 프로파일 편집기의 해시 세트에 대해 확인합니다. 성공적인 매칭은 엔드포인트가 신뢰할 수 있는 네트워크에 있음을 의미합니다. 그러나 헤드엔드에 연결할 수 없거나 인증서 해시가 일치하지 않으면 엔드포인트가 신뢰할 수 없는 네트워크에 있는 것으로 간주됩니다.

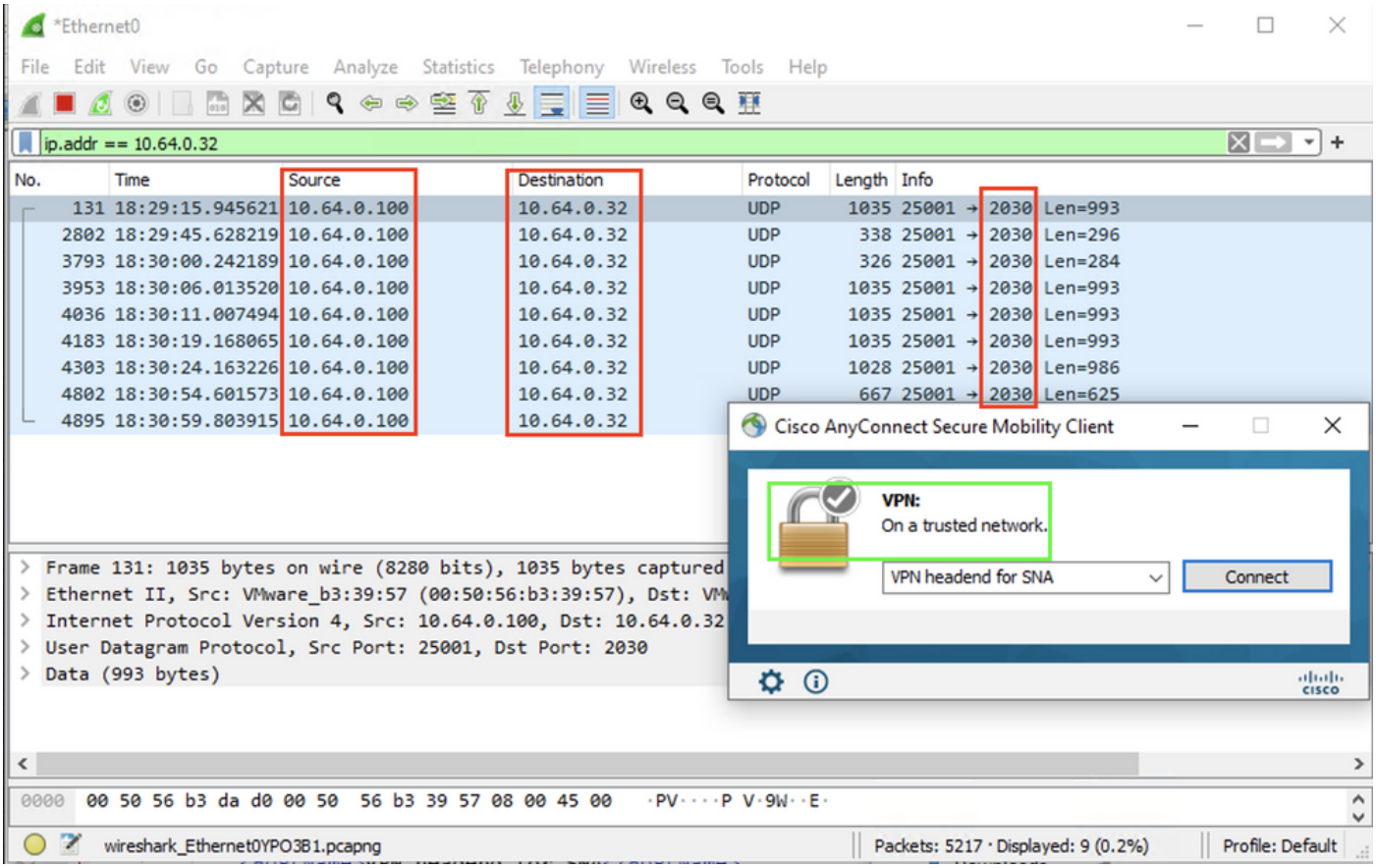
참고: 프록시 뒤에 있는 신뢰할 수 있는 서버는 지원되지 않습니다.

패킷 캡처 수집

엔드포인트 네트워크 어댑터에서 패킷 캡처를 수집하여 플로우가 플로우 컬렉터로 전송되는지 확인할 수 있습니다.

a. 엔드포인트가 신뢰할 수 있는 네트워크에 있지만 VPN에 연결되지 않은 경우 물리적 네트워크 어댑터에서 캡처를 활성화해야 합니다.

이 경우 AnyConnect 클라이언트는 엔드포인트가 신뢰할 수 있는 네트워크에 있음을 나타냅니다. 즉, AnyConnect 창 및 다음에 표시되는 Wireshark 창에서 볼 수 있듯이, 플로우는 엔드포인트의 물리적 네트워크 어댑터를 통해 구성된 포트를 통해 구성된 플로우 컬렉터로 전송됩니다.

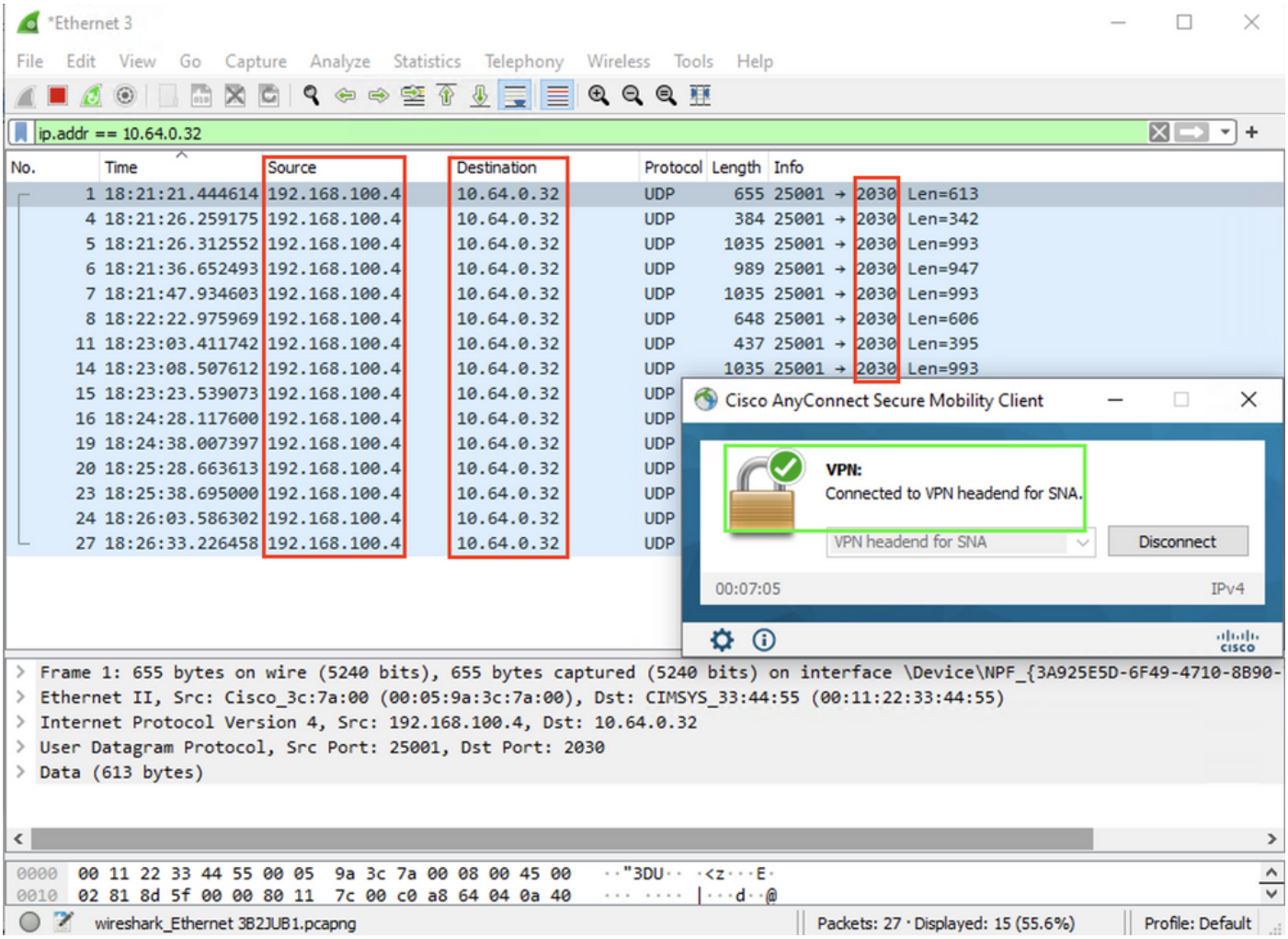


b. 엔드포인트가 AnyConnect VPN에 연결된 경우 자동으로 신뢰할 수 있는 네트워크에 있는 것으로 간주되므로 가상 네트워크 어댑터에서 캡처를 활성화해야 합니다.

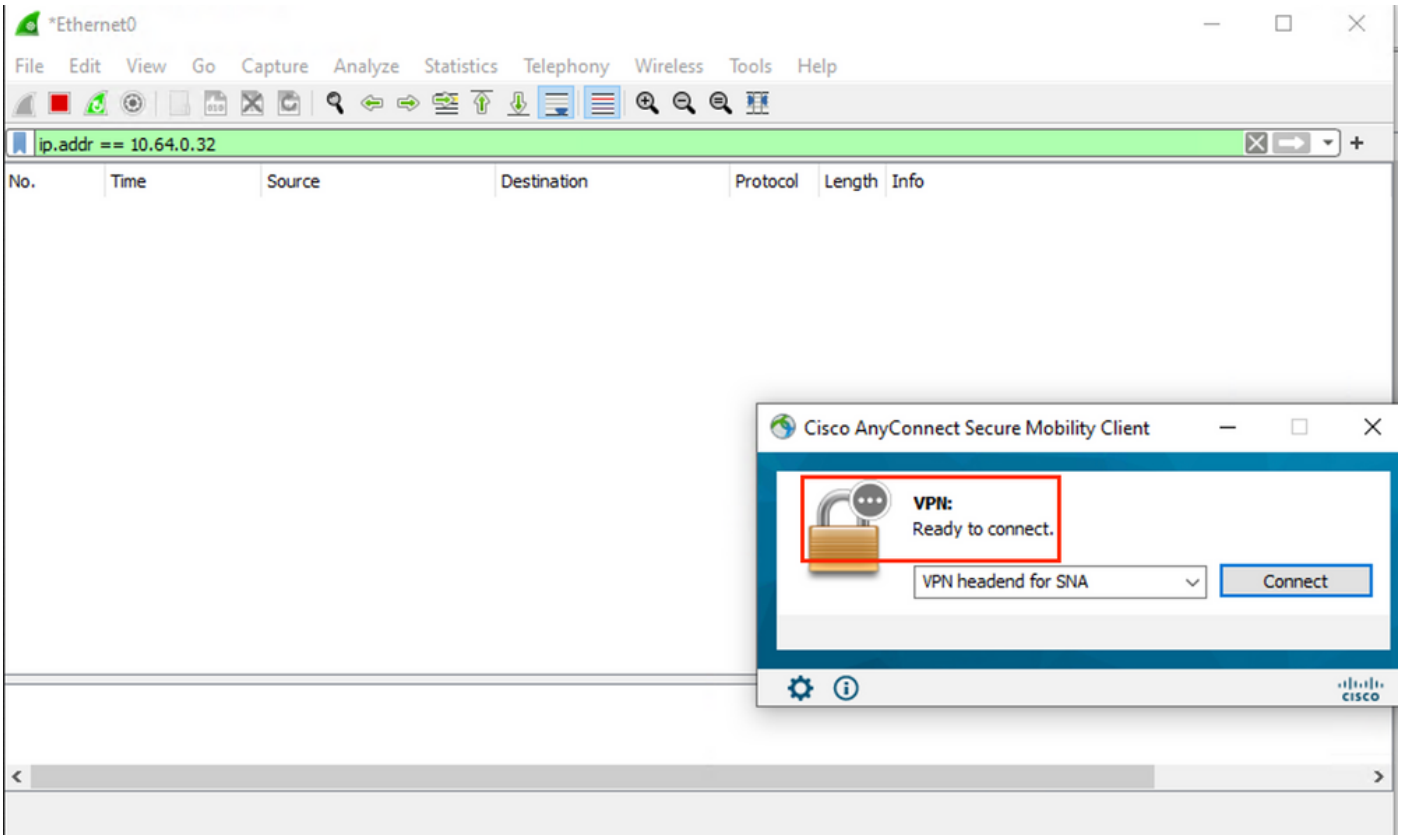
> **참고:** VPN 모듈이 설치되고 TND가 Network Visibility Module 프로필에 구성된 경우 Network Visibility Module은 VPN 네트워크 내에서도 신뢰할 수 있는 네트워크 탐지를 수행합니다.

AnyConnect Client는 엔드포인트가 VPN에 연결되었음을 나타냅니다. 즉, AnyConnect Window 및 다음에 표시되는 Wireshark 창에서 볼 수 있듯이, 플로우는 엔드포인트의 가상 네트워크 어댑터(VPN 터널)를 통해 구성된 포트를 통해 구성된 플로우 컬렉터로 전송됩니다.

> **참고:** 엔드포인트가 연결된 VPN 프로파일의 스플릿 터널 컨피그레이션에는 흐름 컬렉터의 IP 주소가 포함되어야 하며, 그렇지 않으면 플로우는 VPN 터널을 통해 전송되지 않습니다.



c. 엔드포인트가 신뢰할 수 있는 네트워크에 있지 않으면 플로우는 플로우 컬렉터로 전송되지 않습니다.



관련 결함

현재 Secure Network Analytics에 대한 NVM 텔레메트리 수집 프로세스에 영향을 줄 수 있는 두 가지 알려진 결함이 있습니다.

- FC 엔진이 eth1에서 NVM 텔레메트리를 수집할 수 없습니다. Cisco 버그 ID CSCwb84013을 참조하십시오.
- Flow Collector에서 AnyConnect 버전 4.10.04071 이상의 NVM 레코드를 삽입하지 않습니다. Cisco 버그 ID CSCwb91824 참조

관련 정보

- 추가 지원이 필요한 경우 TAC(Technical Assistance Center)에 문의하십시오. 유효한 지원 계약이 필요합니다. Cisco 전 세계 지원 문의처.
- Cisco Security Analytics Community도 여기에 방문해 보십시오.
- 기술 지원 및 문서 – Cisco Systems