CESA용 AnyConnect NVM 4.7.x 이상 및 관련 Splunk 엔터프라이즈 구성 요소 설치 및 구성

목차

소개

이 문서에서는 AnyConnect 4.7.x 이상을 사용하는 최종 사용자 시스템에 Cisco AnyConnect NVM(Network Visibility Module)을 설치 및 구성하는 방법과 관련 Splunk Enterprise 구성 요소 및 NVM 컬렉터를 설치 및 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- NVM을 사용하는 AnyConnect 4.7.x 이상
- AnyConnect 라이센싱
- ASDM 7.5.1 이상
- Splunk Enterprise에 대한 숙지 및 Splunk 앱 및 애드온 설치 방법

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco AnyConnect Security Mobility Client 4.7.x 이상
- Cisco AnyConnect 프로파일 편집기
- Cisco ASA(Adaptive Security Appliance), 버전 9.5.2
- Cisco ASDM(Adaptive Security Device Manager), 버전 7.5.1
- Splunk Enterprise 7.x 이상(지원되는 모든 Linux에서 올인원(CentOS 선호)

- 컬렉터 디바이스로 지원되는 모든 linux 설치(컬렉터는 동일한 서버에서도 실행할 수 있음, 자세한 내용은 cs.co/cesa-pov 참조)

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

배경 정보

- Splunk를 사용한 CESA의 전체 개요 POV는 cs.co/cesa-pov을 참조하십시오.
- Splunk의 CESA NVM 대시보드에 대한 설명서 http://cs.co/cesa-guide
- 솔루션에 대한 자세한 내용은 www.cisco.com/go/cesa을 참조하십시오.

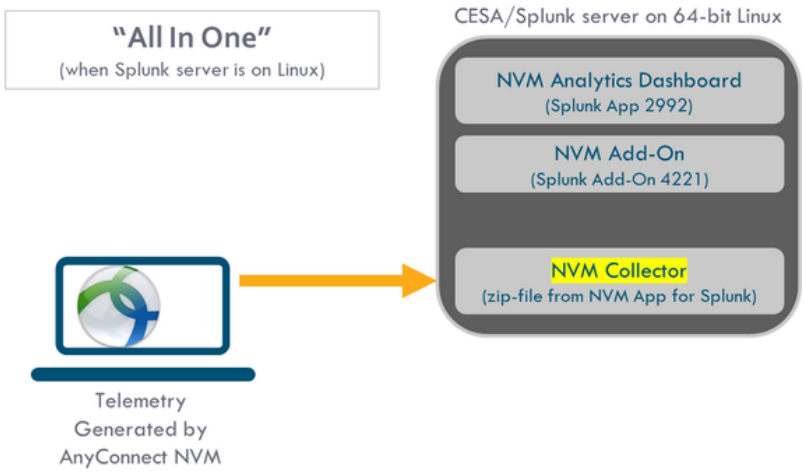
솔루션을 구성하는 구성 요소는 다음과 같습니다.

- NVM(Network Visibility Module)이 활성화된 Cisco AnyConnect Secure Mobility Client
- Splunk용 Cisco AnyConnect NVM(Network Visibility Module) 앱
- Splunk용 Cisco NVM 기술 애드온
- NVM 컬렉터(NVM TA 추가 기능과 함께 zip 파일로 번들됨)

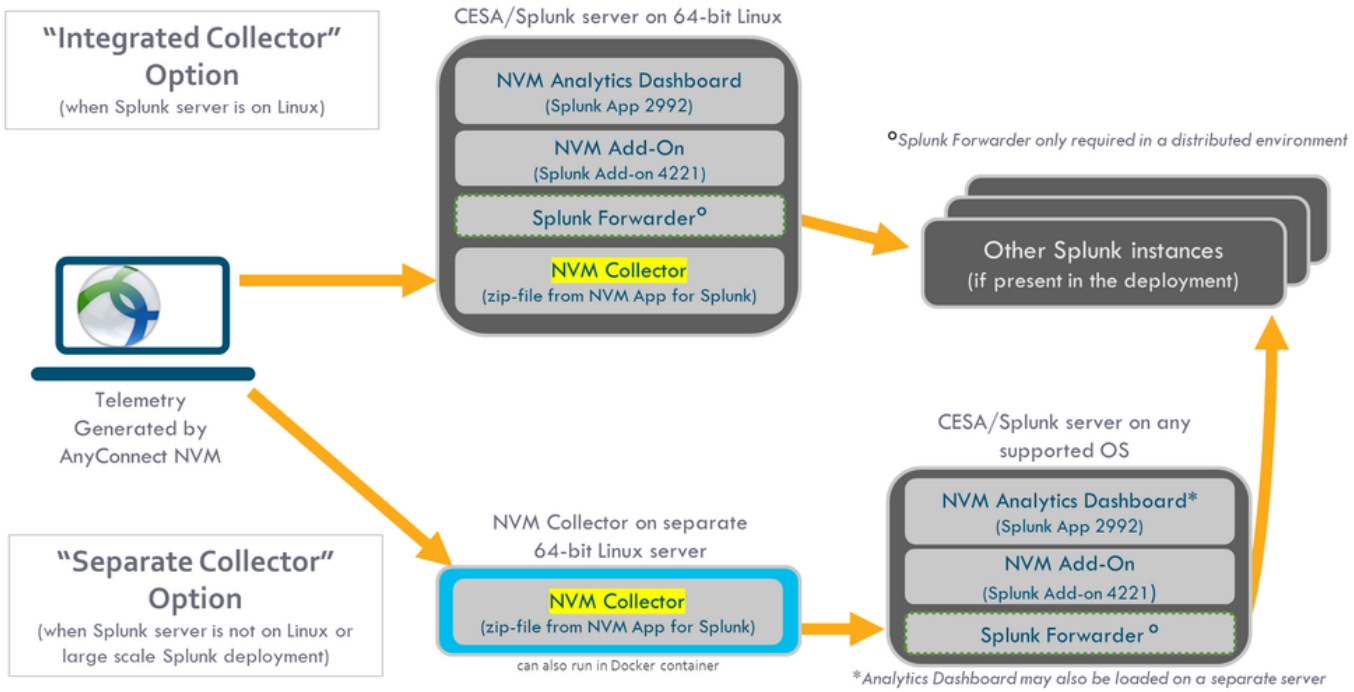
구축 개요

간단한 형태의 구축에 대한 개괄적인 개요입니다.64비트 Linux에서 실행되는 올인원 컨피그레이션입니다.

이 컨피그레이션은 대부분의 데모가 설정되는 방식이며 소규모 프로덕션 구축에서도 유용합니다.



이는 구축에 사용할 수 있는 보다 포괄적인 옵션 집합입니다.일반적으로 프로덕션 설정이 분산되고 여러 Splunk Enterprise 노드가 있습니다.



배경 정보

Cisco AnyConnect Network Visibility Module은 고가치 엔드포인트 텔레메트리를 지속적으로 제공합니다.NVM은 조직에서 네트워크에서 엔드포인트 및 사용자 동작을 확인하고, 온프레미스 및 오프프레미스 엔드포인트에서 흐름을 수집하며, 사용자, 애플리케이션, 디바이스, 위치, 목적지와 같은 중요한 컨텍스트도 수집합니다.Splunk Enterprise는 텔레메트리 데이터를 사용하며 분석 기능 및 보고서를 제공합니다.

이 테크노트는 새로운 CESA 솔루션의 일부로서 Splunk Enterprise를 사용하는 AnyConnect NVM에 대한 컨피그레이션 예입니다.

Cisco AnyConnect Secure Mobility Client - VPN 이상

Cisco AnyConnect는 기업을 보호하기 위해 여러 보안 서비스를 제공하는 통합 에이전트입니다.AnyConnect는 엔터프라이즈 VPN 클라이언트로 가장 일반적으로 사용되지만 엔터프라이즈 보안의 다양한 측면을 지원하는 추가 모듈도 지원합니다.추가 모듈은 상태 평가, 웹 보안, 악성코드 차단, 네트워크 가시성 등의 보안 기능을 지원합니다.

이 기술 자료는 Cisco AnyConnect와 통합되어 관리자가 엔드포인트 애플리케이션 사용을 모니터링할 수 있는 기능을 제공하는 NVM(Network Visibility Module)에 대한 것입니다.

Cisco AnyConnect에 대한 자세한 내용은 Cisco AnyConnect Secure Mobility Client 관리자 설명서, 릴리스 4.7을 참조하십시오.

IPFIX(Internet Protocol Flow Information Export)

IPFIX는 회계/감사/보안과 같은 다양한 목적으로 IP 플로우 정보를 내보내는 표준을 정의하는 IETF 프로토콜입니다.IPFIX는 직접 호환되지 않지만 Cisco NetFlow 프로토콜 v9를 기반으로 합니다. Cisco nvzFlow는 IPFIX 프로토콜을 기반으로 하는 프로토콜 사양입니다.IPFIX는 확장 가능한 프로토콜로, 새로운 매개변수를 정의하여 정보를 전달할 수 있습니다.Cisco nvzFlow 프로토콜은 IPFIX 표준을 확장하고 새 정보 요소를 정의하며 AnyConnect NVM에서 사용하는 텔레메트리의 일부로 전달되는 표준 IPFIX 템플릿 집합을 정의합니다.

IPFIX에 대한 자세한 내용은 rfc5101, rfc7011,rfc7012,rfc7013,rfc7014,rfc7015를 참조하십시오.

IPFIX NVM 컬렉터

http://cs.co/nvm-collector폴더에 대한 자세한 내용은 확인하십시오.

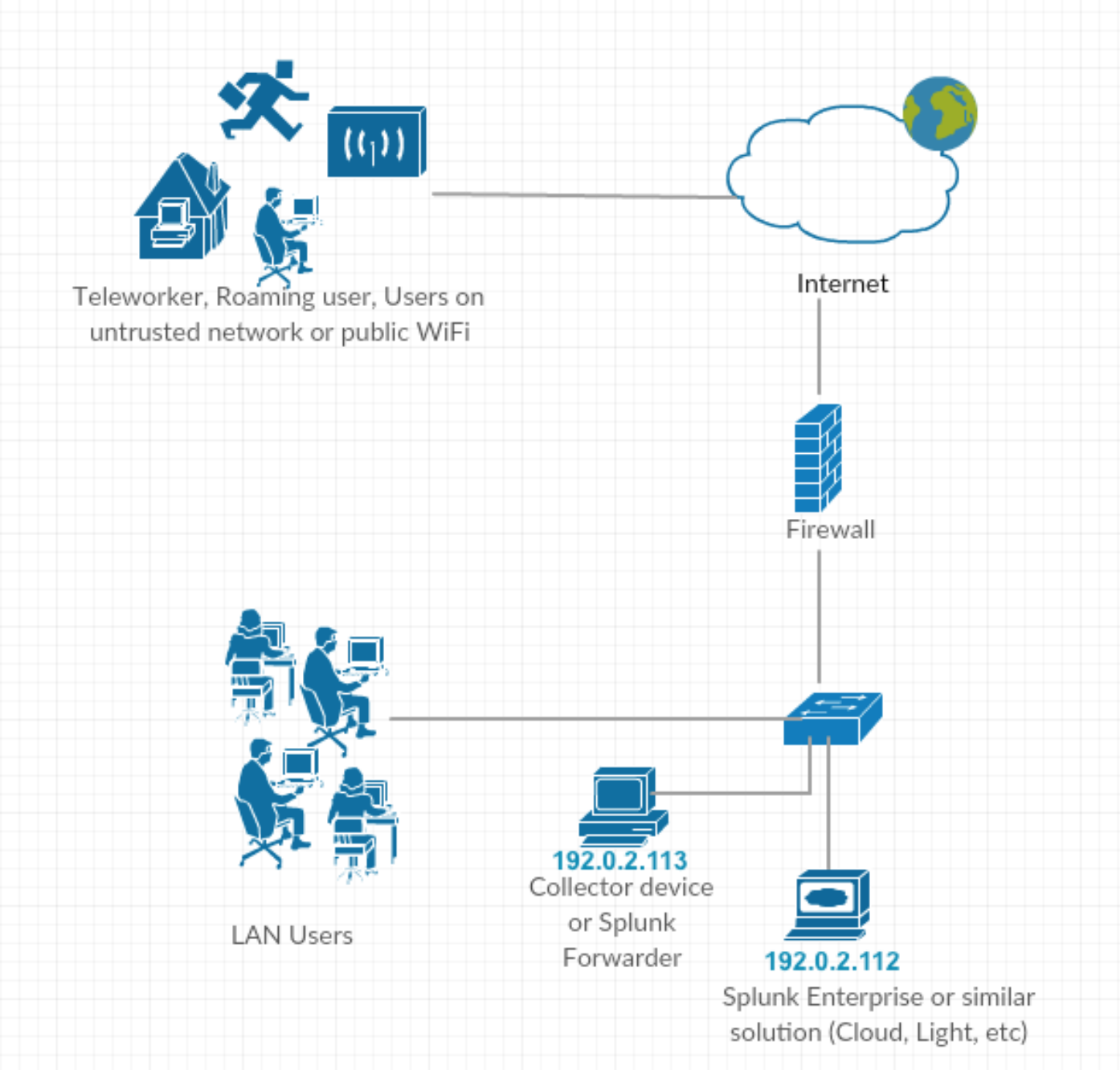
- 컬렉터는 IPFIX 데이터를 수신하고 저장하는 서버입니다.그런 다음 이 데이터를 Splunk에 제공할 수 있습니다.
- Cisco는 nvzFlow 프로토콜용으로 특별히 설계되었으며 Splunk App(NVM TA Add-On)과 함께 번들로 구성된 컬렉터를 제공합니다.
- 컬렉터는 Splunk 서버와 동일한 박스(올인원)에 설치할 수 있습니다.전달자가 많습니다.또는 독립형 Linux 상자에서도 사용할 수 있습니다.

Splunk 엔터프라이즈

Splunk Enterprise는 진단 데이터를 수집하고 분석하여 IT 인프라에 대한 의미 있는 정보를 제공하는 강력한 툴입니다.관리자는 네트워크 상태를 파악하는 데 중요한 데이터를 한 곳에서 수집할 수 있습니다.

Splunk는 Cisco의 파트너이며, CESA 솔루션은 Cisco와 협력하여 개발되었습니다.

토폴로지



이 기술 메모의 IP 주소 규칙:

컬렉터 IP 주소:192.0.2.123

Splunk IP 주소: 192.0.2.113

구성

이 섹션에서는 Cisco NVM 구성 요소에 대해 설명합니다.

AnyConnect NVM 및 컨피그레이션 프로파일 구축에 대한 개요는 AnyConnect Network Visibility Module 구현 방법을 참조하십시오.

DTLS 지원

이제 DTLS를 통해 컬렉터에 데이터를 안전하게 전송하도록 NVM을 구성할 수 있습니다.이 모드는

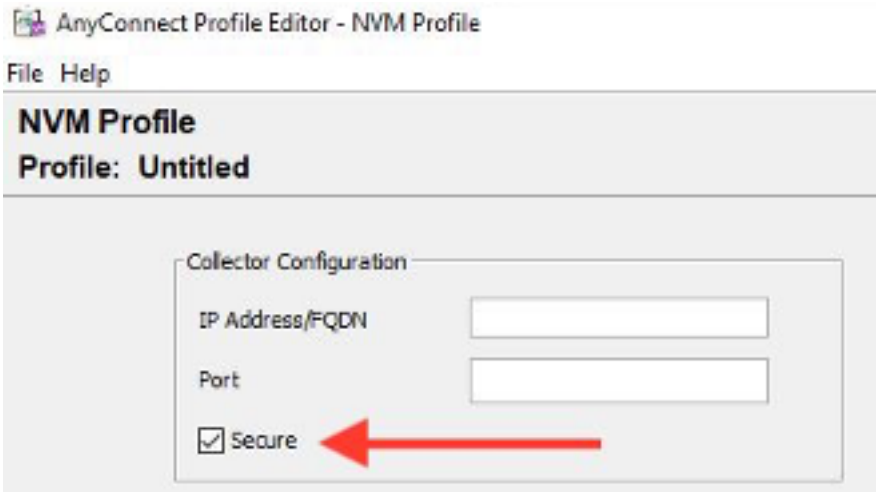
NVM 프로파일 편집기에서 구성할 수 있습니다.'보안' 확인란을 선택하면 NVM은 DTLS를 전송으로 사용합니다. DTLS 연결을 통과하려면 엔드포인트에서 DTLS 서버(컬렉터) 인증서를 신뢰해야 합니다.신뢰할 수 없는 인증서가 자동으로 거부됩니다. DTLS 1.2가 지원되는 최소 버전입니다.DTLS 지원을 위해서는 CESA Splunk App v3.1.2+의 일부인 컬렉터가 필요합니다.컬렉터는 보안 또는 비보안 모드를 하나만 사용합니다.

인증서 요구 사항

- 컬렉터 인증서는 클라이언트에서 신뢰해야 합니다(인증서 체인을 신뢰할 수 있어야 함). Anyconnect에 컨피그레이션이 없습니다.
- 인증서는 PEM 형식이어야 합니다.
- 인증서 키 비밀번호를 지원하지 않습니다(Cisco ISE 내부 CA에는 하나 필요).
- AnyConnect 클라이언트 시스템이 신뢰하는 경우(내부 PKI, 잘 알려진 등) 모든 인증서를 컬렉터에서 사용할 수 있습니다.
- 컨피그레이션 파일이 업데이트되면 anyconnect NVM 서비스를 다시 시작해야 합니다(단일 클라이언트 테스트용). ISE/ASA에서 푸시된 프로파일의 경우 네트워크에 대한 연결 해제/재연결이 필요합니다.
- AC NVM 프로필 컬렉터 구성은 IP 또는 FQDN이어야 합니다.이는 인증서의 CN에 사용되는 항목에 따라 달라집니다.IP 주소 변경 시 FQDN이 항상 기본 설정됩니다. IP 주소를 사용하는 경우 컬렉터 인증서 CN 또는 SAN에 해당 IP가 있어야 합니다.인증서에 FQDN이 CN인 경우 NVM 프로파일은 컬렉터와 동일한 FQDN을 가져야 합니다.

AnyConnect 구성(4.9.3043 이상) **- 컬렉터 정보 참조**

NVM 프로필에는 Secure라는 컬렉터 IP/포트 아래에 새 확인란이 있습니다.



독립형 AnyConnect NVM 모듈

이를 위해서는 Anyconnect 4.8.01090 이상이 필요합니다. NVM용 AnyConnect 관리 설명서

또한 독립형 가이드 - How To Implement the AnyConnect Network Visibility Module을 참조하십시오.

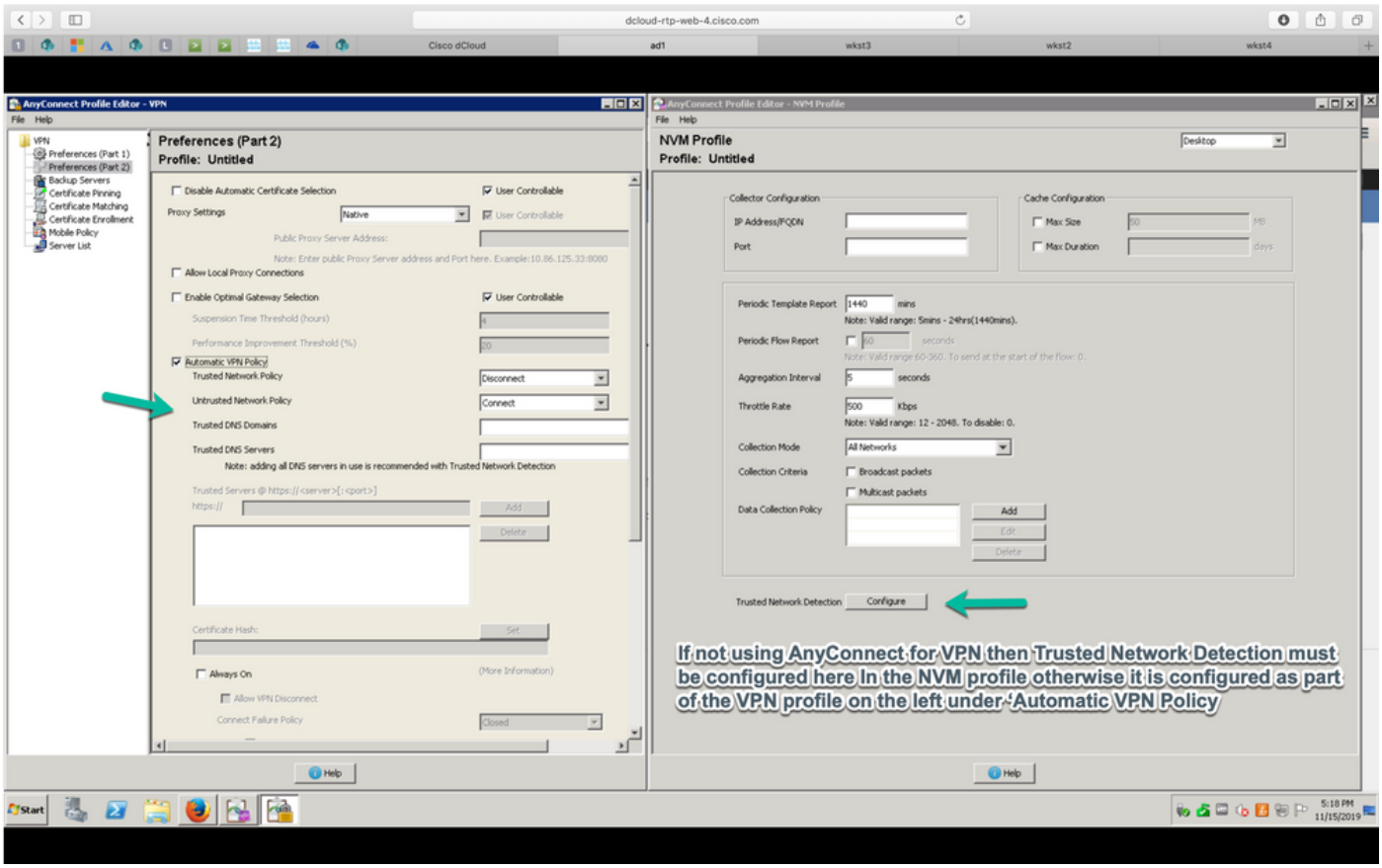
AnyConnect 구축이 없거나 다른 VPN 솔루션을 사용 중인 경우 NVM 요구 사항에 맞게 NVM 독립형 패키지를 설치할 수 있습니다.이 패키지는 독립적으로 작동하지만 엔드포인트에서 기존 AnyConnect NVM 솔루션과 동일한 수준의 플로우 수집을 제공합니다.독립형 NVM을 설치하는 경우 활성 프로세스(예: macOS의 Activity Monitor)가 사용을 나타냅니다.

독립형 NVM은NVM 프로파일 편집기 및 TND(Trusted Network Detection) 컨피그레이션은 필수입니다.NVM은 TND 컨피그레이션을 사용하여 엔드포인트가 기업 네트워크에 있는지 확인한 다음 적절한 정책을 적용합니다.

문제 해결 및 로깅은 AnyConnect 패키지에서 설치할 수 있는 AnyConnect DART에서 계속 수행됩니다.

독립형 제품보다 먼저 Trusted Network Detection(신뢰할 수 있는 네트워크 탐지)을 활용하기 위해 Core VPN 모듈을 설치해야 했습니다. 이 경우 사용자는 UI에서 핵심 VPN 타일을 볼 수 있으며, 이는 최종 사용자가 다른 벤더 VPN 솔루션을 사용하는 경우 특히 혼동될 수 있습니다.

독립 실행형 사용 시 코어 VPN 프로파일을 사용하여 TND를 구성하지 않습니다. 이제 NVM 프로파일을 TND에 직접 구성할 수 있습니다.



AnyConnect NVM 클라이언트 프로파일

AnyConnect NVM 컨피그레이션은 컬렉터 IP 주소 및 포트 번호에 대한 정보와 기타 정보가 포함된 XML 파일에 저장됩니다.컬렉터 IP 주소 및 포트 번호는 NVM 클라이언트 프로필에 올바르게 구성해야 합니다.

NVM 모듈의 올바른 작동을 위해서는 다음 디렉토리에 XML 파일을 배치해야 합니다.

- Windows 7 이상의 경우:**%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM**
- Mac OSX의 경우:/opt/cisco/anyconnect/nvm

프로파일이 Cisco ASA/ISE(Identity Services Engine)에 있는 경우 AnyConnect NVM 구축과 함께 자동으로 구축됩니다.

XML 프로파일 예:

```
<?xml version="1.0" encoding="UTF-8"?>
-<NVMProfile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="NVMProfile.xsd">
-<CollectorConfiguration>
<CollectorIP>192.0.2.123</CollectorIP>
<Port>2055</Port>
</CollectorConfiguration>
<Anonymize>false</Anonymize>
<CollectionMode>all</CollectionMode>
</NVMProfile>
```

NVM 프로파일은 다음 툴을 사용하여 생성할 수 있습니다.

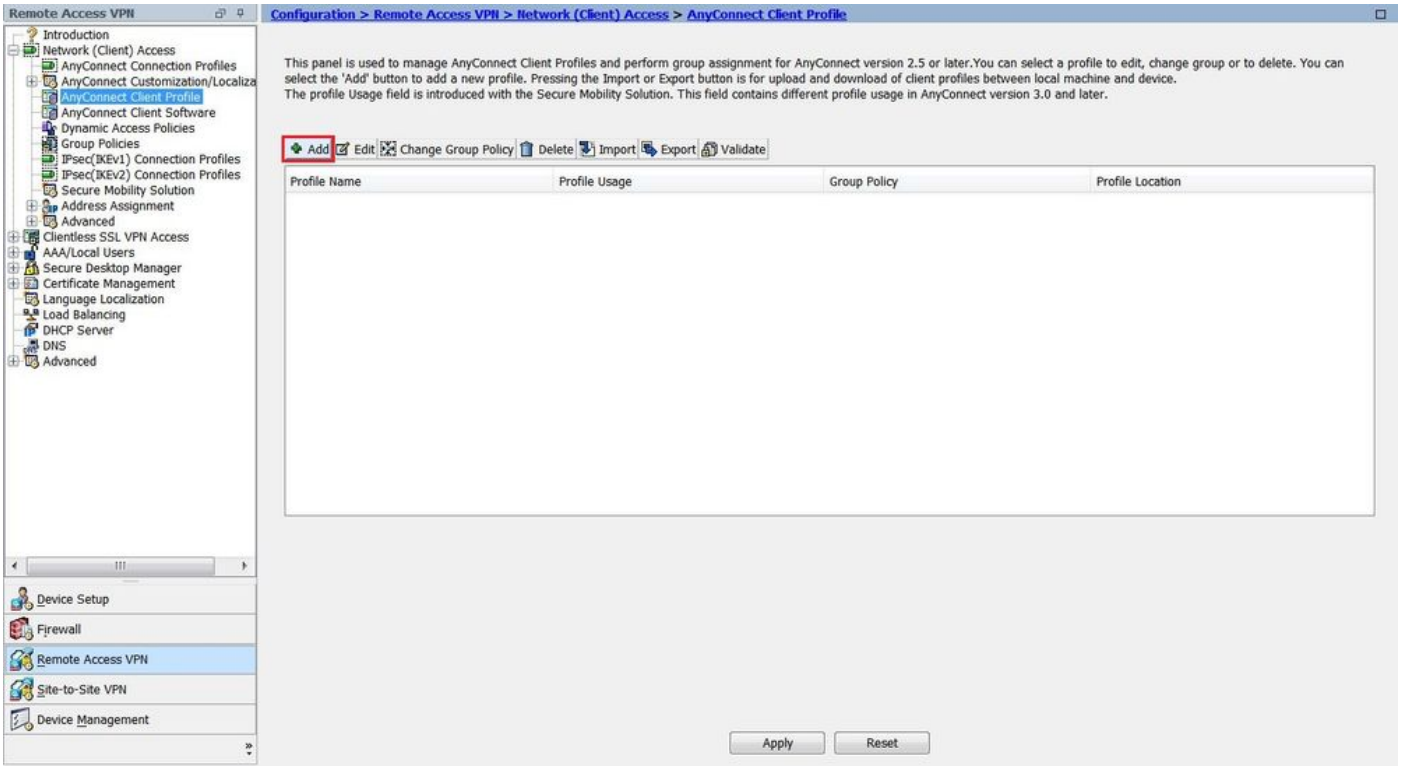
- Cisco ASDM
- Anyconnect 프로파일 편집기
- Identity Services Engine

ASDM을 통해 NVM 클라이언트 프로파일 구성

Cisco ASA를 통해 AnyConnect NVM을 구축하는 경우 이 방법을 사용하는 것이 좋습니다.

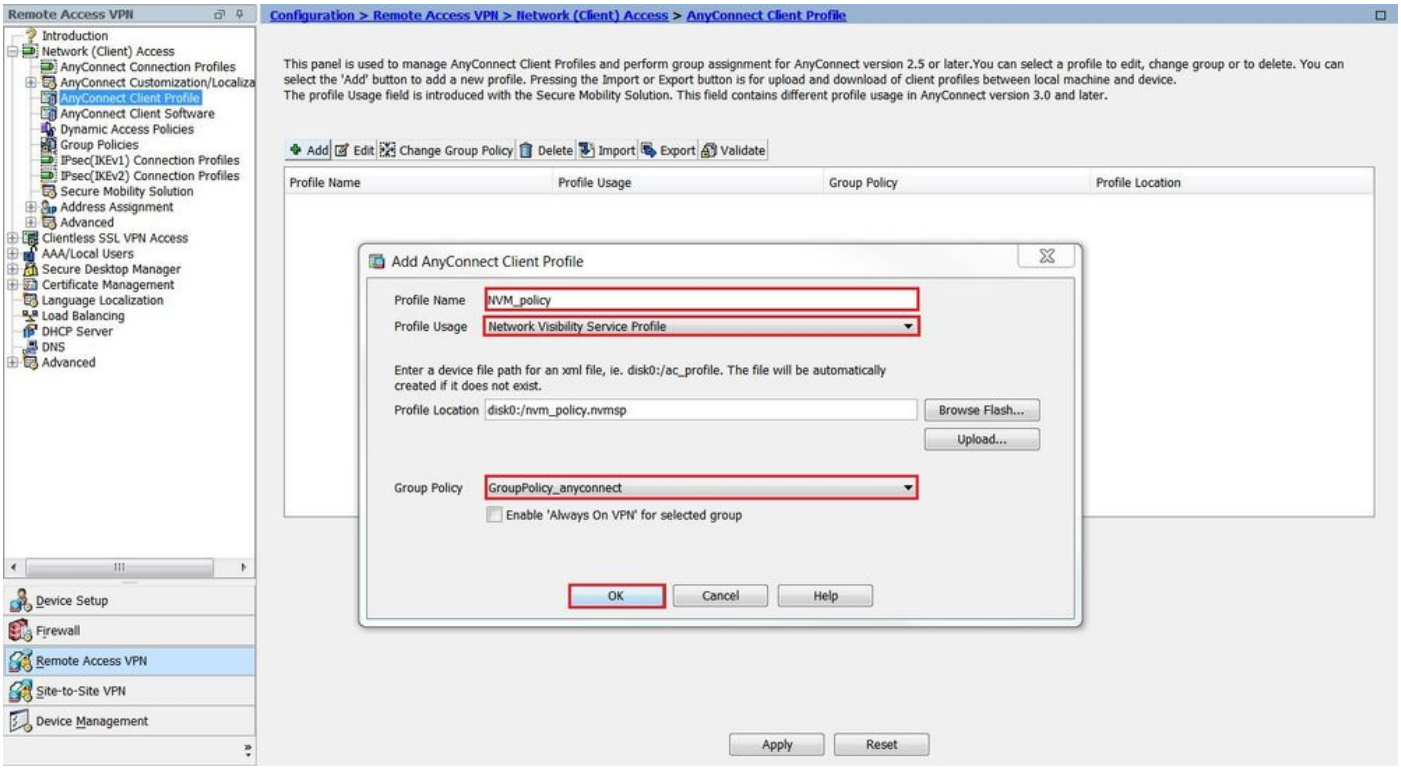
1. Configuration(구성) **> Remove Access VPN(액세스 VPN 제거) > Network (Client) Access(네트워크(클라이언트) 액세스) > Anyconnect Client Profile(Anyconnect 클라이언트 프로파일)으로 이동합니다.**

2. 이미지에 표시된 대로 **추가**를 클릭합니다.

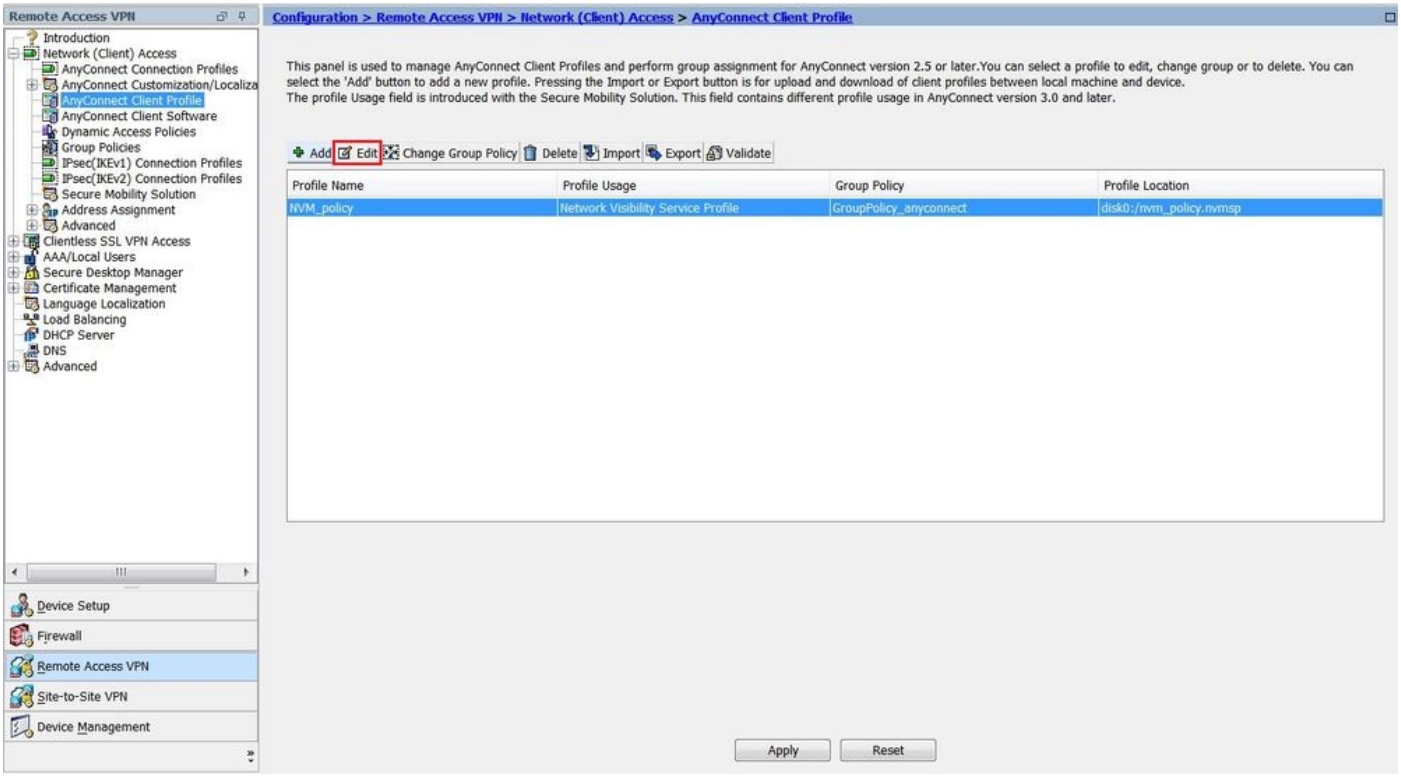


3. 프로파일 이름을 지정합니다.Profile Usage**에서** Network **Visibility Service Profile을 선택합니다.**

4. AnyConnect 사용자가 사용하는 그룹 정책에 이를 할당하고 이미지에 표시된 대로 **확인**을 클릭합니다.

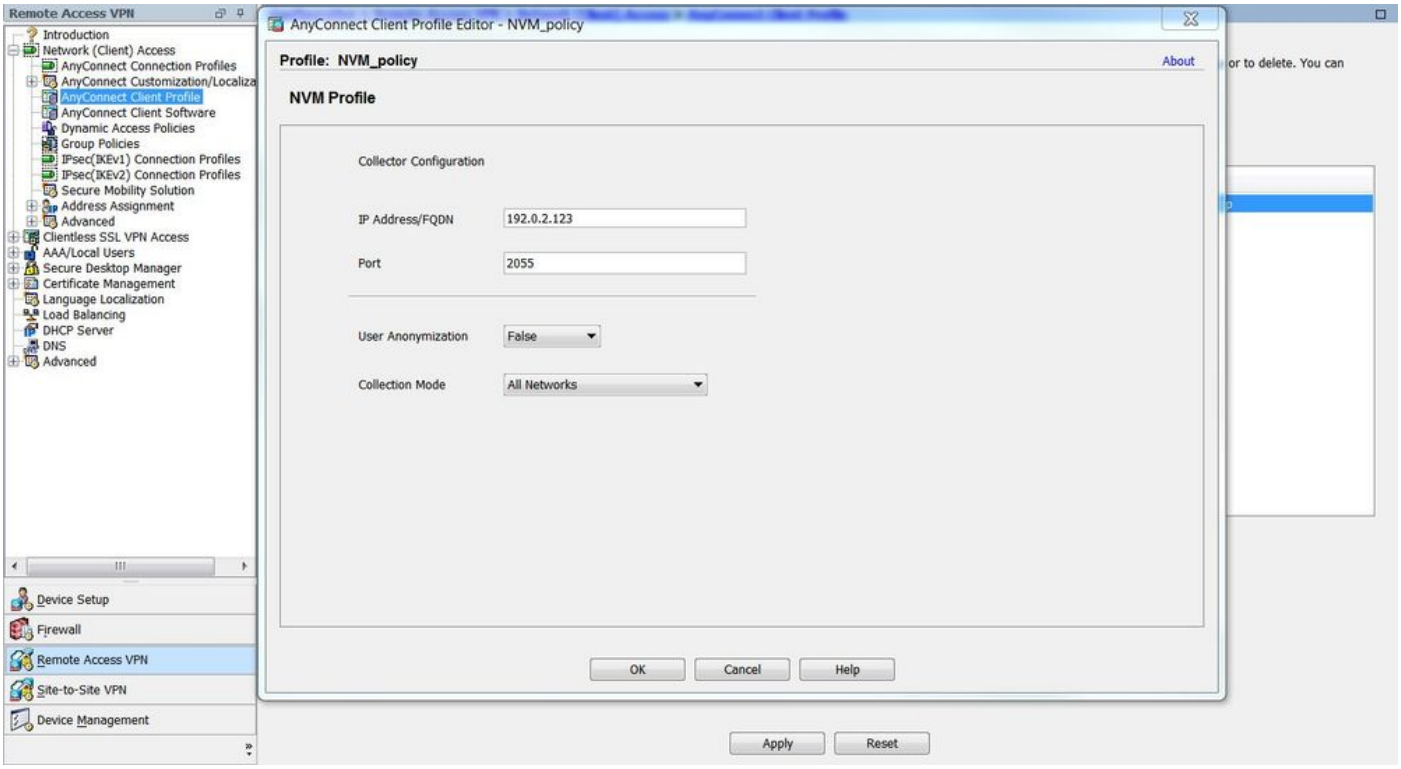


5. 새 정책이 생성되면 이미지에 표시된 대로 **Edit**를 클릭합니다.



6. 컬렉터 IP 주소 및 포트 번호에 대한 정보를 입력하고 **OK**(확인)를 클릭합니다.

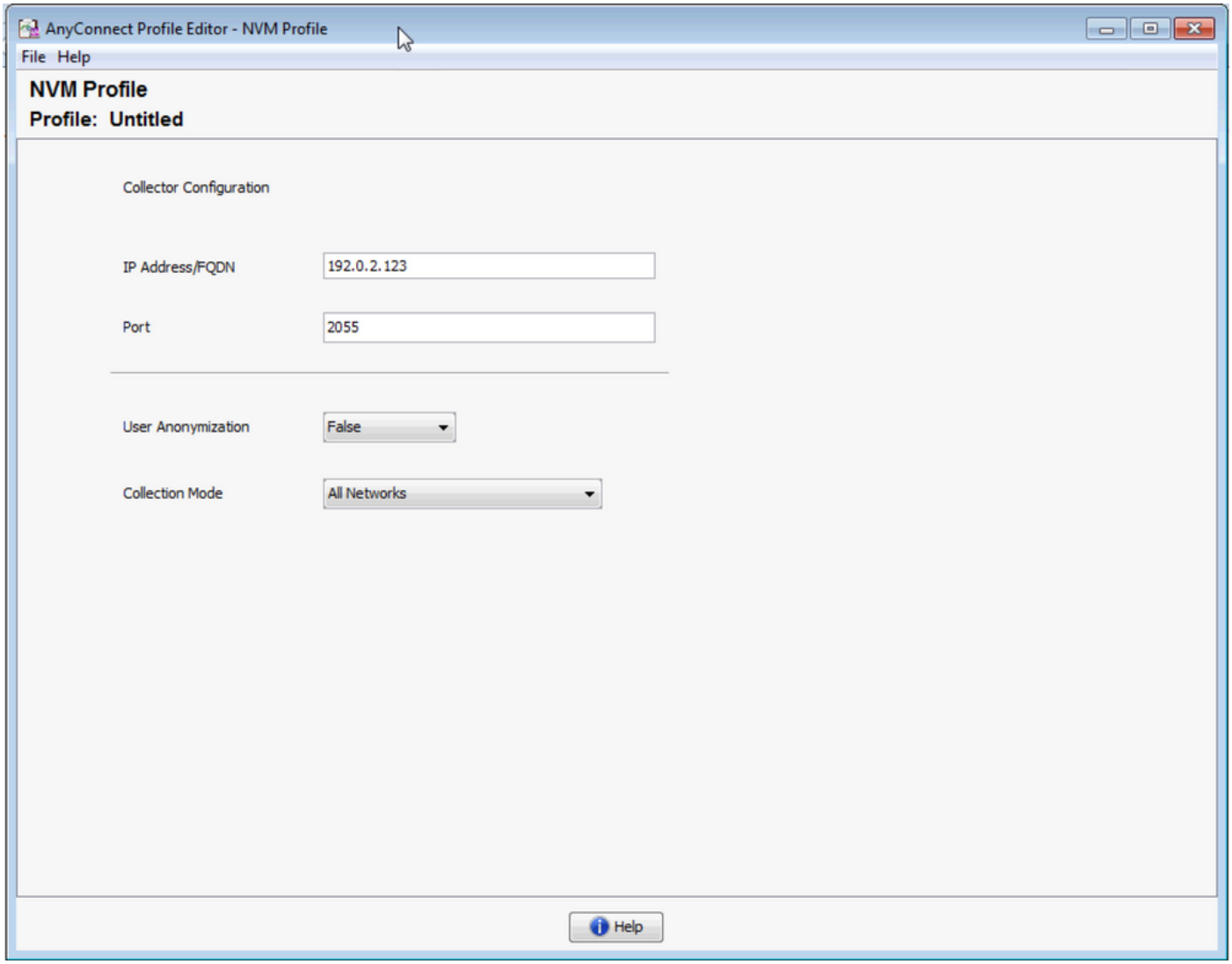
7. 이미지에 표시된 대로 Apply(적용)를 클릭합니다.



Anyconnect 프로파일 편집기를 통해 NVM 클라이언트 프로파일 구성

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect49/administration/guide/b_AnyConnect_Administrator_Guide_4-9/anyconnect-profile-editor.html#ID-1430-00000061

이 툴은 Cisco.com에서 사용할 수 있습니다.AnyConnect NVM이 Cisco ISE를 통해 구축되는 경우 이 방법을 사용하는 것이 좋습니다.이 도구를 사용하여 생성된 NVM 프로파일은 Cisco ISE에 업로드하거나 엔드포인트에 직접 복사할 수 있습니다.



Anyconnect 프로파일 편집기에 대한 자세한 내용은 다음을 참조하십시오.

AnyConnect 프로파일 편집기

Cisco ASA에서 웹 구축 구성

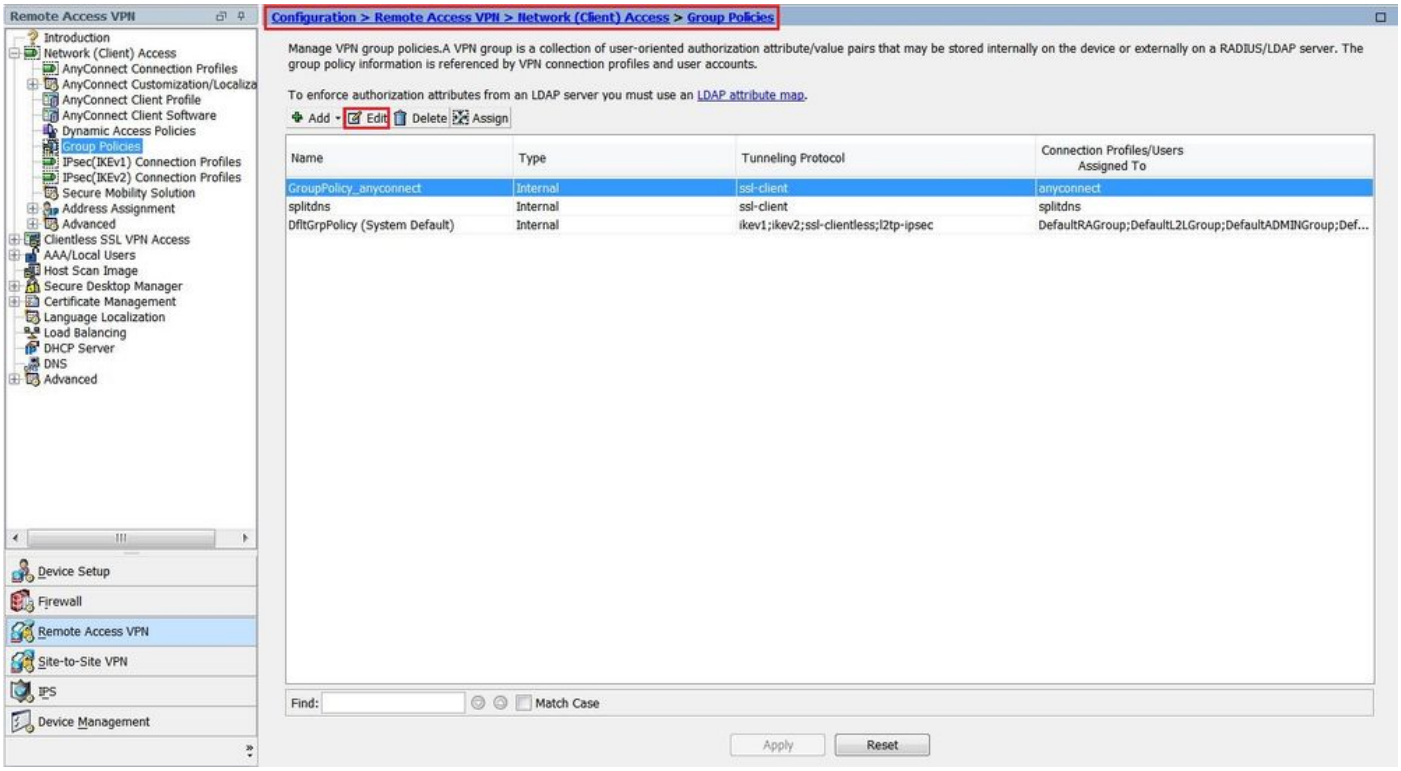
이 테크노에서는 AnyConnect가 ASA에 이미 구성되어 있으며 NVM 모듈 컨피그레이션만 추가해야 한다고 가정합니다.ASA Anyconnect 컨피그레이션에 대한 자세한 내용은 다음을 참조하십시오.

ASDM Book 3:Cisco ASA Series VPN ASDM 컨피그레이션 가이드, 7.5

Cisco ASA에서 AnyConnect NVM 모듈을 활성화하려면 다음 단계를 수행하십시오.

1. Configuration(구성) **> Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Group Policies(그룹 정책)로 이동합니다**.

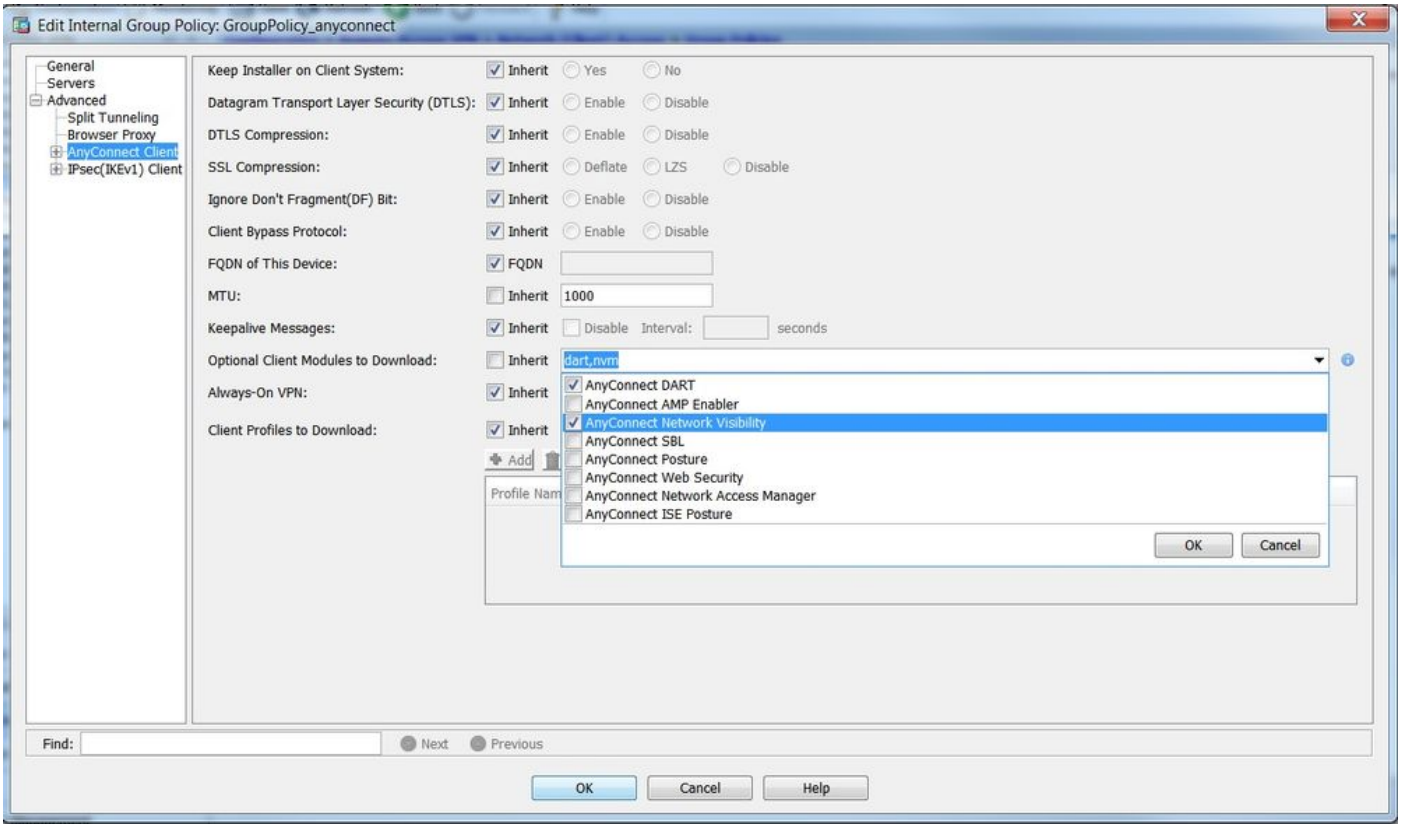
2. 이미지에 표시된 대로 관련 그룹 정책을 선택하고 **편집**을 클릭합니다.



3. 그룹 정책 팝업 창에서 Advanced(고급) **> Anyconnect Client(Anyconnect 클라이언트)로 이동합니다.**

4. Optional **Client Modules to Download(다운로드할 선택적 클라이언트 모듈)를** 확장하고 Anyconnect **Network Visibility(Anyconnect 네트워크 가시성)를 선택합니다.**

5. 확인을 **누르고** 변경 사항을 적용합니다.



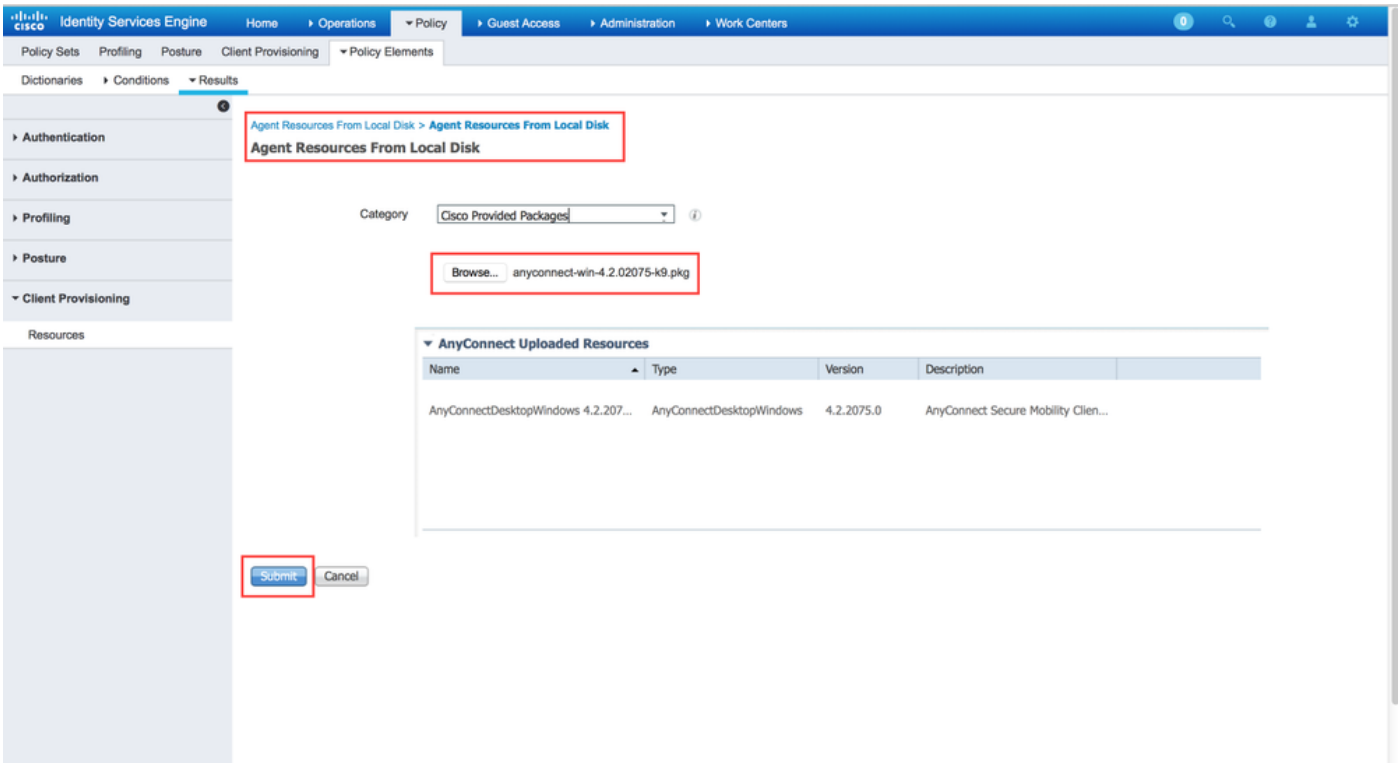
Cisco ISE에서 웹 구축 구성

AnyConnect 웹 구축을 위한 Cisco ISE를 구성하려면 다음 단계를 수행합니다.

1. Cisco ISE GUI에서 Policy(정책) **> Policy Elements(정책 요소) > Results(결과)로 이동합니다**.
2. Client **Provisioning(클라이언트 프로비저닝)**을 확장하여 **Resources(리소스)**를 **표시하고 Resources(리소스)**를 **선택합니다**.

Anyconnect 이미지 추가:

1단계. **Add(추가) > Agent Resources(에이전트 리소스)를 선택하고 Anyconnect** 패키지 파일을 업로드합니다.



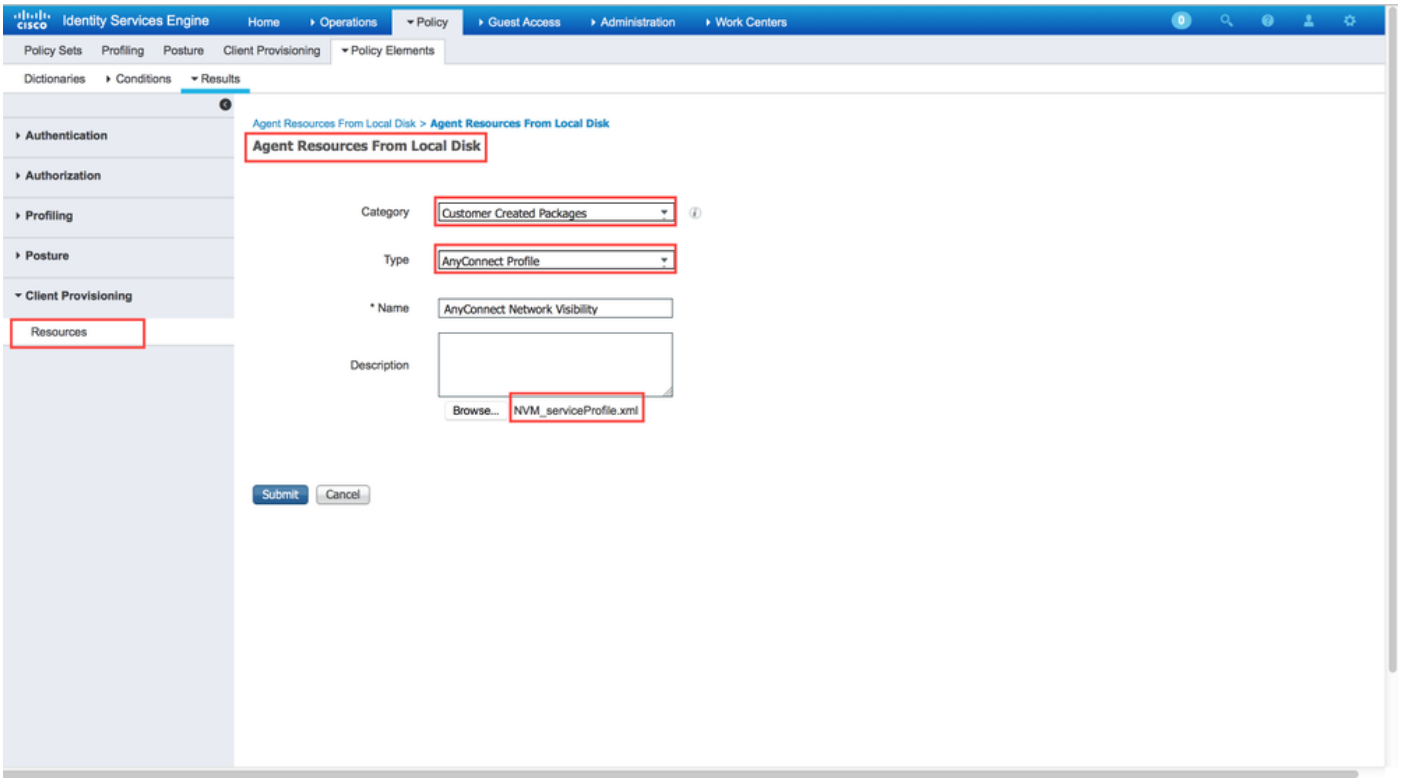
2단계. 팝업에서 패키지의 해시를 확인합니다.

파일 해시는 Cisco.com 다운로드 페이지 또는 서드파티 툴을 사용하여 확인할 수 있습니다.

이 단계를 반복하여 여러 AnyConnect 이미지를 추가할 수 있습니다.(Mac OSX 및 Linux OS용)

AnyConnect NVM 프로필 추가:

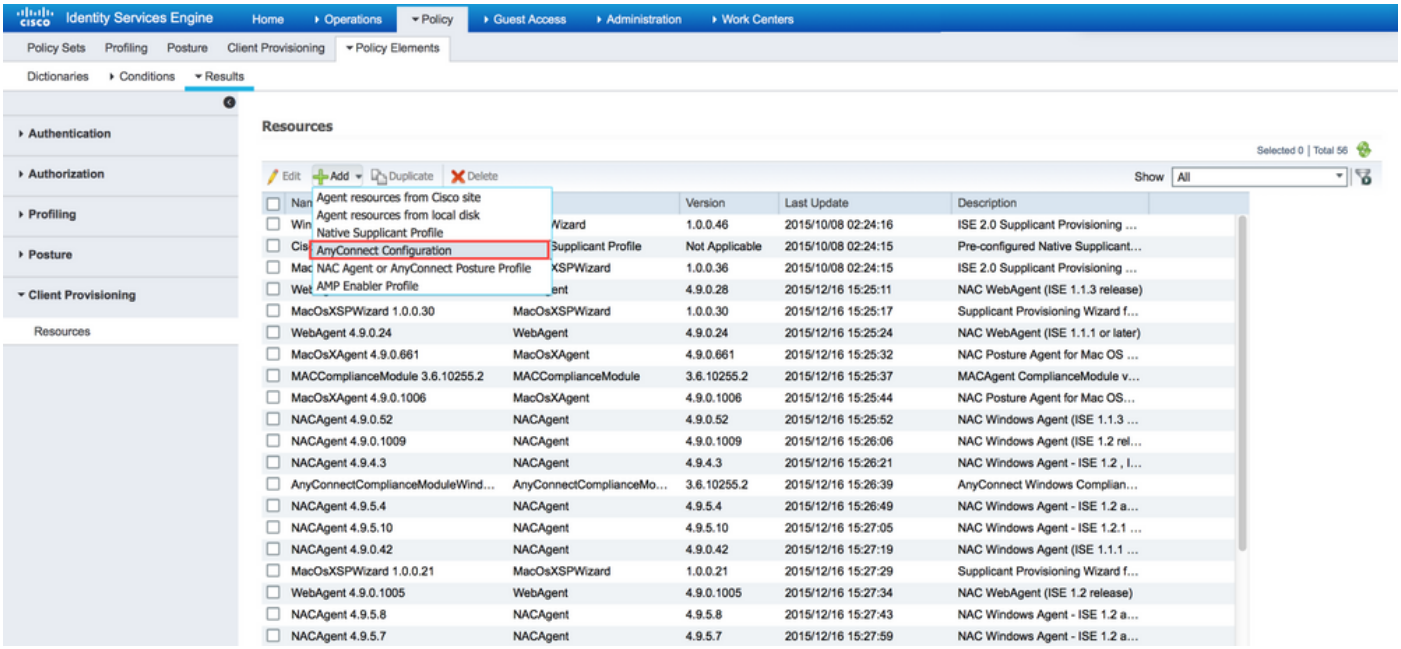
1단계. **Add(추가) > Agent Resources(에이전트 리소스)를 선택하고** NVM 클라이언트 프로파일을 업로드합니다.



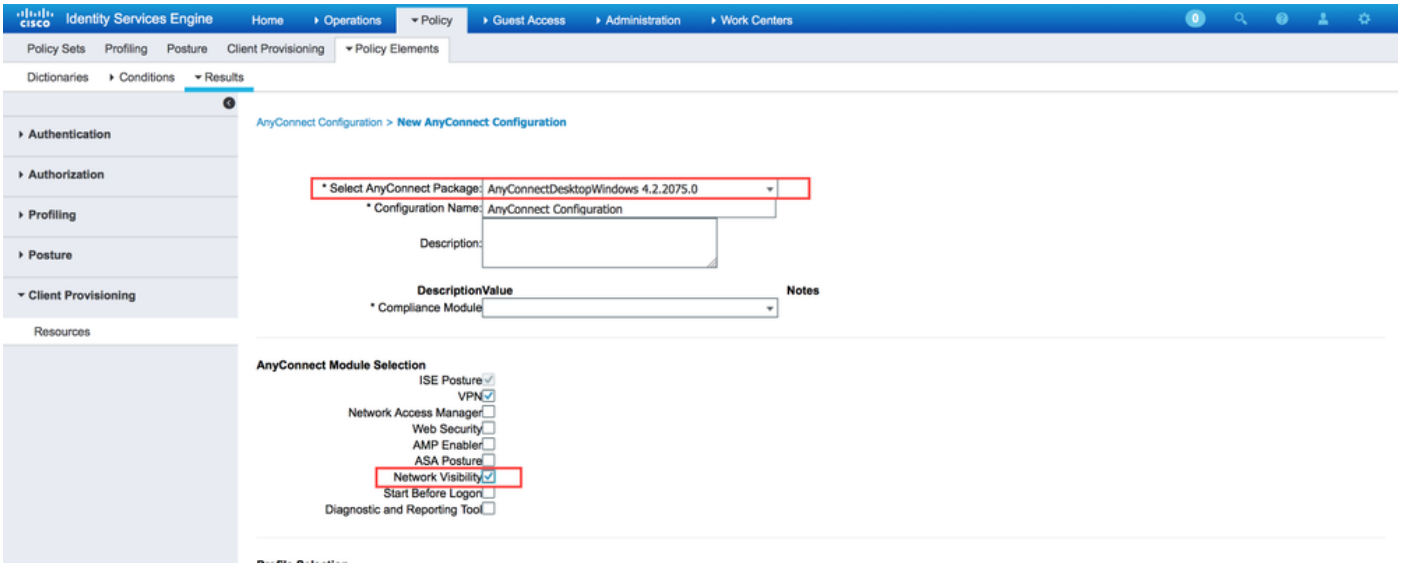
Anyconnect 구성 파일 추가:

1단계. Add(추가)를 클릭하고 AnyConnect **Configuration(AnyConnect 컨피그레이션)을 선택합니다**.

이전 단계에서 업로드한 패키지를 선택합니다.



2단계. AnyConnect **모듈 선택**에서 **NVM**을 필요한 정책과 함께 활성화합니다.



이 섹션에서는 AnyConnect 클라이언트 모듈, 프로파일, 사용자 지정/언어 패키지 및 Opswat 패키지를 활성화합니다.

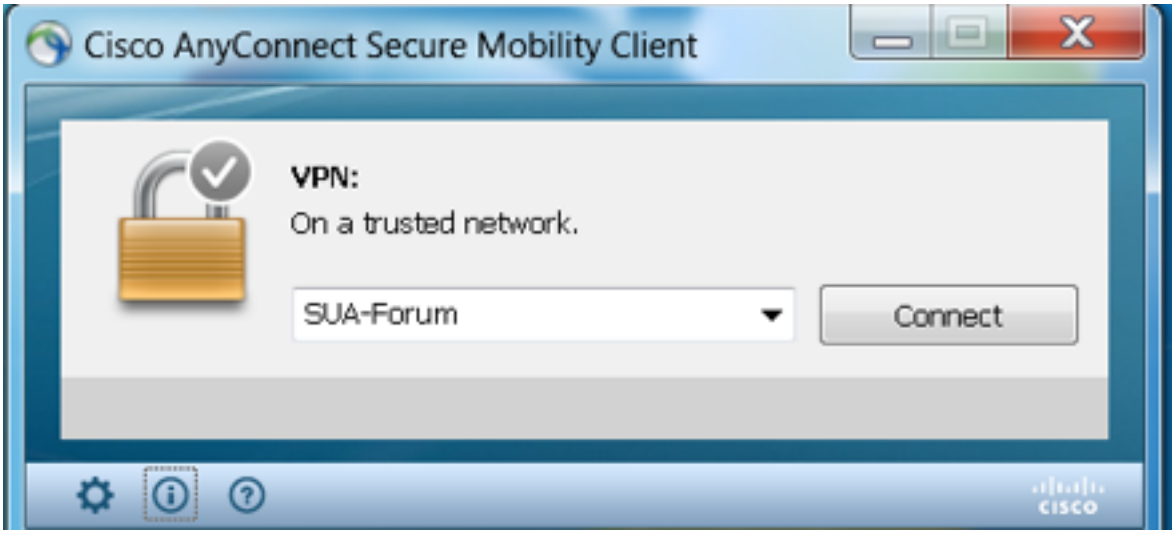
Cisco ISE의 웹 구축 컨피그레이션에 대한 자세한 내용은 다음을 참조하십시오.

AnyConnect 웹 구축

신뢰할 수 있는 네트워크 탐지

AnyConnect NVM은 신뢰할 수 있는 네트워크에 있는 경우에만 흐름 정보를 전송합니다.엔드포인트가 신뢰할 수 있는 네트워크에 있는지 여부를 알아보려면 AnyConnect 클라이언트의 TND 기능을 사용합니다.

VPN 구성 요소가 환경에서 사용되고 있는지 여부에 관계없이 VPN에 사용되는 AnyConnect 클라이언트 프로파일(XML)에서 신뢰할 수 있는 네트워크 탐지가 구성됩니다. TND는 프로필에서 Automatic VPN Policy(자동 VPN 정책) 섹션을 구성하여 활성화됩니다. 최소한 하나의 신뢰할 수 있는 DNS 도메인 또는 신뢰할 수 있는 DNS 서버를 채워야 합니다. AnyConnect에서 클라이언트가 신뢰할 수 있는 네트워크에 있다고 확인한 경우 Trusted 및 Untrusted Network Policy의 풀다운을 사용하여 DoNothing 모드로 설정할 수 있습니다.



TND .

—

구축

AnyConnect NVM 솔루션 구축에는 다음 단계가 포함됩니다.

1. Cisco ASA/ISE에서 AnyConnect NVM을 구성합니다.

2. IPFIX 컬렉터 구성 요소(Linux의 NVM 컬렉터 - TA 추가 기능에 패키지됨)를 설정합니다.

3. Cisco NVM App 및 TA 애드온으로 Splunk를 설정합니다.

1단계. Cisco ASA/ISE에서 Anyconnect NVM 구성

이 단계는 구성 섹션에서 자세히 다루었습니다.

NVM이 Cisco ISE/ASA에서 구성되면 클라이언트 엔드포인트에 자동 구축될 수 있습니다.

2단계. IPFIX 컬렉터 구성 요소 설정(Anyconnect NVM 컬렉터)

컬렉터 구성 요소는 엔드포인트에서 모든 IPFIX 데이터를 수집 및 변환하여 Splunk Add-On으로 전달합니다.NVM 컬렉터는 64비트 Linux에서 실행됩니다.CentOS, Ubuntu 및 Docker 구성 스크립트가 포함됩니다.CentOS 설치 스크립트 및 구성 파일은 Fedora 및 Redhat 배포에서도 사용할 수 있습니다.

일반적인 분산형 Splunk Enterprise 구축에서 컬렉터는 64비트 Linux에서 실행되는 독립형 64비트 Linux 시스템 또는 Splunk Forwarder 노드에서 실행해야 합니다.또한 Splunk 구성 요소가 없는 독립형 서버에 설치할 수도 있습니다.

> **참고:**이 솔루션은 소규모 구축 또는 데모용으로 사용할 수 있도록 NVM 컬렉터 및 Splunk Enterprise 구성 요소를 포함하는 단일 64비트 Linux 시스템에서 실행할 수도 있습니다.올인원(all-in-one)은 최대 10,000개의 엔드포인트에서 가장 쉽습니다. CESA POV 크기 조정 정보,

컬렉터를 설치하는 방법

1. /opt/splunk/etc/apps/APP_DIR/appserver/addon/(TA Add-On에 포함) 디렉토리에 있는 acnvmcollector.zipfile을 설치하려는 시스템에 복사합니다.
2. 파일 압축 해제(acnvmcollector.zip)

install.sh 스크립트를 실행하기 전에 .zip 번들에서 $PLATFORM$_README 파일을 읽는 것이 좋습니다.$PLATFORM$_README 파일은 install.sh 스크립트를 실행하기 전에 확인하고 수정해야 하는 관련 구성 설정(필요한 경우)에 대한 정보를 제공합니다.최소한 데이터를 전달하는 Splunk 인스턴스의 주소를 구성해야 합니다.시스템을 제대로 구성하지 않으면 컬렉터가 잘못 작동할 수 있습니다.

> **참고:**소스 및 목적지 주소 및 포트에 대한 UDP 트래픽을 허용하도록 네트워크 및 호스트 방화벽이 올바르게 구성되었는지 확인합니다.anyconnect 클라이언트에서 컬렉터로 들어오고 나가는 UDP 데이터가 Splunk(여기)로 들어오는 IPFIX(cflow) 트래픽

단일 NVM 컬렉터 인스턴스는 적절한 크기의 시스템에서 초당 최소 5,000개의 플로우를 처리할 수 있습니다.또는 최대 35-40k 엔드포인트.Splunk NVM 및 TA-Add on App을 사용하려면 먼저 컬렉터를 구성하고 실행해야 합니다.

기본적으로 컬렉터는 UDP 포트 2055의 AnyConnect NVM 엔드포인트에서 플로우를 수신합니다.

또한 컬렉터는 UDP 포트 20519, 20520 및 20521에서 Splunk, Per Flow Data, Endpoint Identity Data 및 Endpoint Interface Data에 대한 3개의 데이터 피드를 생성합니다.

acnvm.conf 파일을 변경하고 컬렉터 인스턴스를 다시 시작하여 수신 및 데이터 피드 포트를 변경할 수 있습니다.엔드포인트와 컬렉터 간 또는 컬렉터와 Splunk 시스템 간의 호스트/네트워크 방화벽이 구성된 UDP 포트 및 주소에 대해 열려 있는지 확인합니다.또한 AnyConnect NVM 컨피그레이션이 컬렉터 컨피그레이션과 일치하는지 확인합니다.

모든 구성 요소가 설치 및 실행되면 Splunk 응용 프로그램 내의 도움말 파일 섹션에서 사전 구성된 보고서, 데이터 모델 및 솔루션에서 생성한 정보 요소에 대한 자세한 내용을 참조하십시오.

AnyConnect 엔드포인트 중 하나를 다시 시작하고 데이터가 솔루션에 전송되고 있는지 확인할 수 있습니다.youtube를 사용하여 꾸준한 데이터 스트림을 실행합니다.

컨피그레이션 파일 - acnvm.conf에서 정보를 구성해야 합니다.

- syslog_server_ip(전달자 또는 splunk 인스턴스)가 동일한 상자에 있는 경우 127.0.0.1(LOCALHOST 사용 안 함)을 가리킬 수 있습니다.
- 컬렉터의 수신 포트(수신 IPFIX 데이터) 기본값은 ok입니다.

참고:netflow_collector_ip는 구성 파일에서 생략됩니다(기본 공용 인터페이스를 사용). 특정 로컬 IP로 재정의하도록 변경해야 합니다.

플로우 데이터 포트당, 엔드포인트 ID 데이터 포트, 엔드포인트 인터페이스 데이터 및 컬렉터 포트는 컨피그레이션 파일의 기본 설정으로 사전 구성됩니다.기본값이 아닌 포트를 사용하는 경우 이러한 값이 변경되어야 합니다.

이 정보는 구성 파일(/opt/acnvm.conf)에 추가됩니다.

DTLS 지원

(자세한 내용은 Anyconnect NVM DTLS 정보 참조)

이 작업은 컬렉터를 호스팅하는 상자에서 수행됩니다.

- 디렉토리 **/opt/acnvm/certs를 만듭니다**.
- 컬렉터에 인증서를 적용하려면 **/opt/acnvm/certs** 디렉토리의 키와 함께 **저장합니다.**
- 폴더의 소유자 및 그룹을 acnvm:acnvm**으로** 변경하려면 다음 명령을 사용합니다.**sudo chown -R acnvm:acnvm certs/**:
- acnvm**.conf에** 대한 이 섹션은 cert 및 키로 구성해야 합니다.
- config 및 cert를 배치한 후 컬렉터를 다시 시작합니다. - sudo systemctl restart acnvm**.service**
- 컬렉터 상태 확인 - **sudo systemctl status acnvm.service**

```
{ "security" :{ "dtls_enabled": true, "server_certificate":"/opt/acnvm/certs/public.cer",
"server_pkey":"/opt/acnvm/certs/private.key" },
```

컨피그레이션의 나머지는 여기 있습니다.

```
"syslog_server_ip" : "192.0.2.113", "syslog_flowdata_server_port" : 20519,
"syslog_sysdata_server_port" : 20520, "syslog_intdata_server_port" : 20521,
"netflow_collector_port" : 2055, "correlate_data": false }
```

3 .수퍼유저 권한으로 install.sh 스크립트 실행(sudo ./install.sh)

> **참고:**acnvm 서비스 계정에 대한 install.sh 및 권한을 실행하려면 sudo 권한 또는 루트가 필요합니다.

자세한 내용은 https://splunkbase.splunk.com/app/2992/#/details을 참조하십시오.

3단계. Splunk용 Cisco NVM App(CESA Dashboard) 및 TA Add-On으로 Splunk를 설정합니다.

Splunkbase에서 Cisco AnyConnect NVM App for Splunk를 사용할 수 있습니다.이 앱은 사전 정의된 보고서와 대시보드에서 사용 가능한 보고서의 엔드포인트에서 IPFIX(nvzFlow) 데이터를 사용하고 사용자 및 엔드포인트 동작의 상관관계를 분석하도록 지원합니다.

> **참고:**클라우드 구축의 경우 두 앱 모두 클라우드 인스턴스에 설치됩니다.TA만 온프레미스(전달자와 함께)에 설치됩니다. 컬렉터는 전달자와 함께 온프레미스 또는 별도의 linux/docker 상자에 설치됩니다.

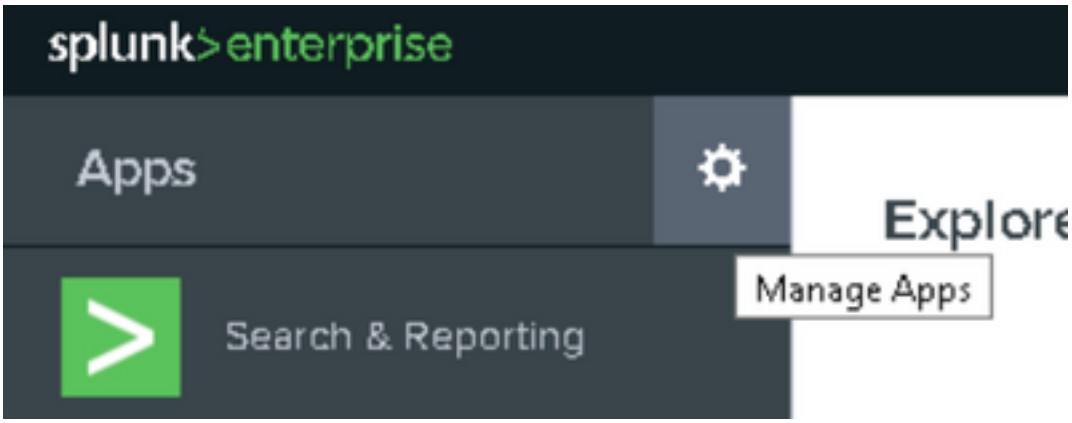
온프레미스의 경우 모든 구성 요소 및 앱을 하나의 상자(또는 별도)에 설치할 수 있습니다. 다이어그램 보기

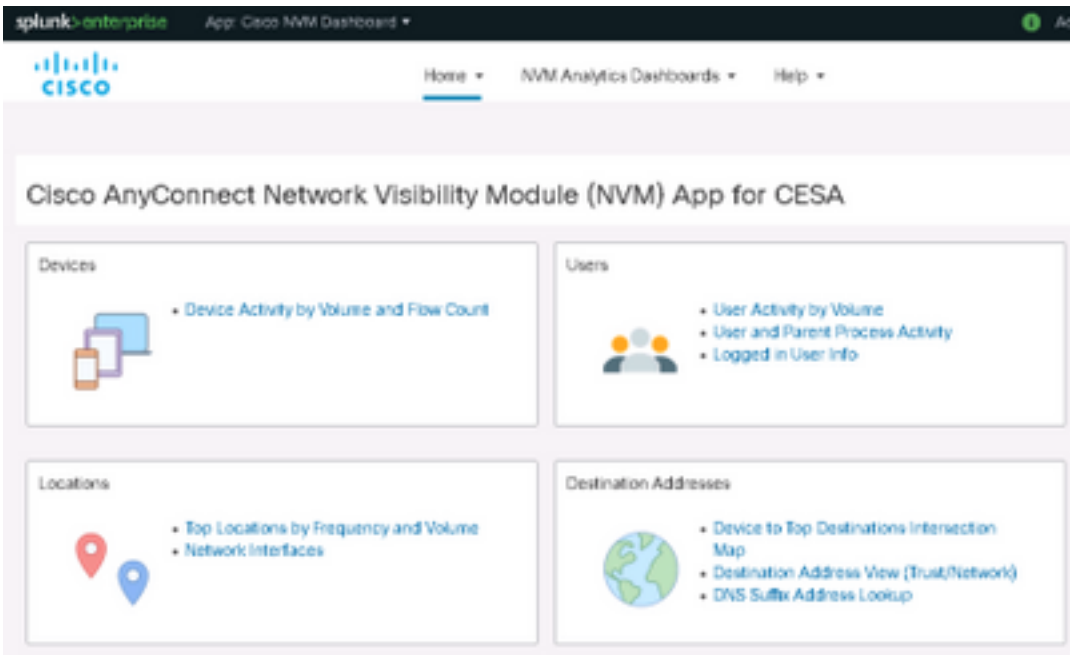
다음 파일을 다운로드합니다.

- Splunkbase에서 Splunk용 Cisco NVM 앱:https://splunkbase.splunk.com/app/2992/
- Splunkbase에서 Splunk용 Cisco NVM 추가 기능: https://splunkbase.splunk.com/app/4221/

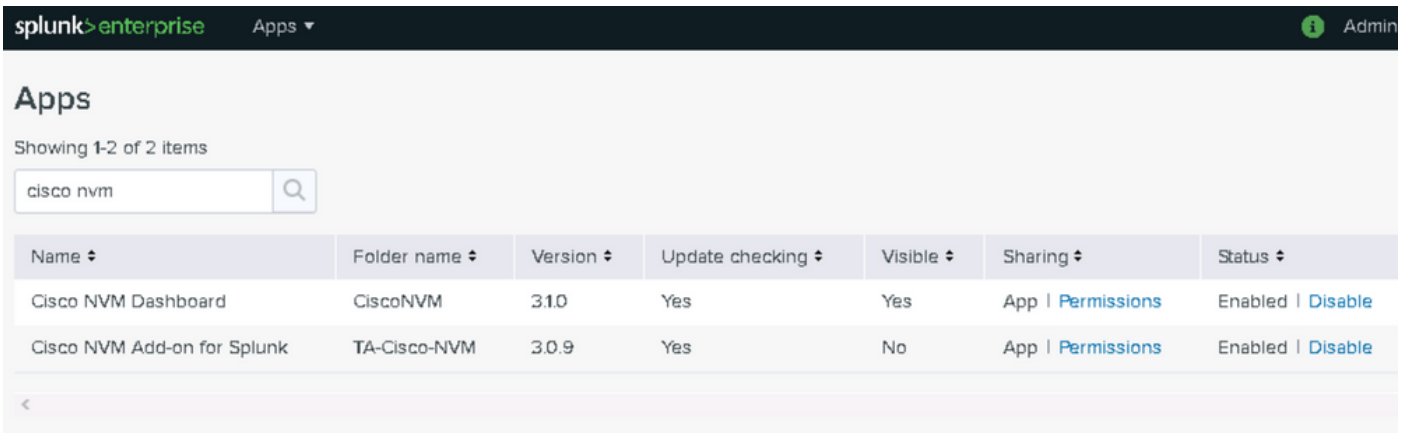
설치

1단계. Splunk > **Apps**로 이동하여 장비를 클릭하고 Splunkbase에서 다운로드한 **tar.gz** 파일을 설치하거나 Apps 섹션 내에서 검색합니다.





2단계. 그런 다음 동일한 프로세스로 **추가 기능**을 설치해야 합니다.Splunk Apps(Splunk 앱) 페이지를 보고 두 **가지** 모두 설치되었는지 확인합니다.



기본 컨피그레이션은 각각 UDP 포트 20519, 20520 및 20521에서 Splunk, Per Flow Data, Endpoint Identity Data 및 Endpoint Interface Data에 대한 3개의 데이터 피드를 수신합니다(2단계 참조).

그런 다음 추가 기능을 Splunk 소스 유형에 매핑합니다. **cisco:nvm:flowdata**, **cisco:nvm:sysdata** 및 **cisco:nvm:ifdata**.

Splunk 관리 UI를 사용하여 UDP 입력 사용

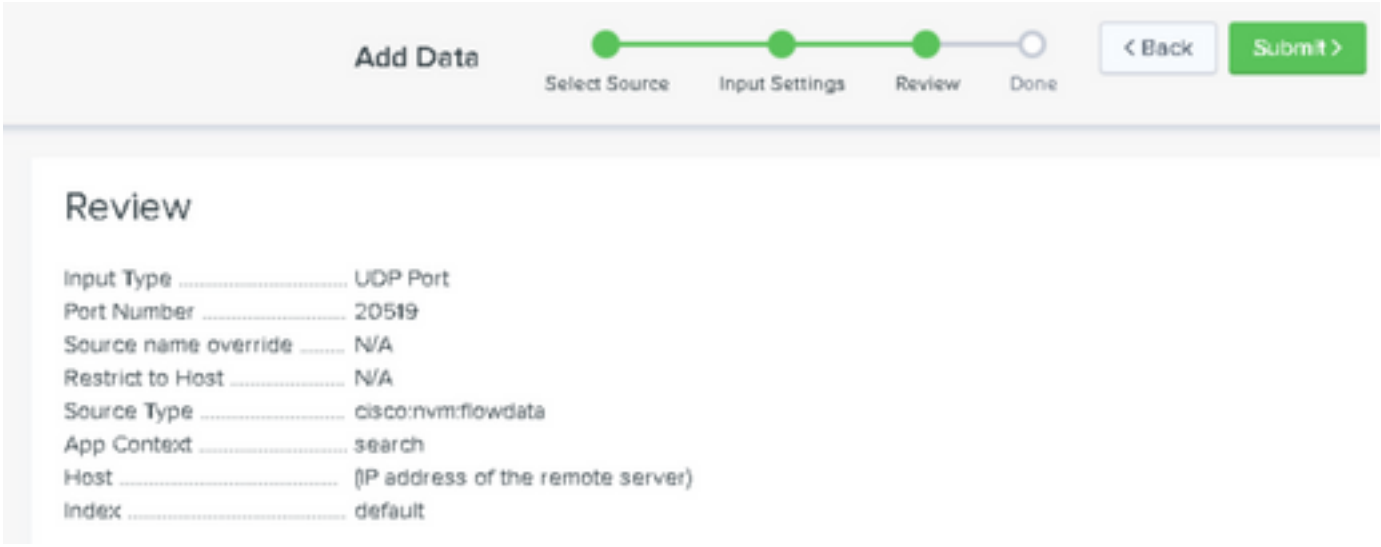
> **참고:**input.conf 파일을 사용하여 이 작업을 수행할 수도 있습니다. 이는 도움말 폴다운의 Cisco NVM 대시보드 앱 gui에서 설명합니다.

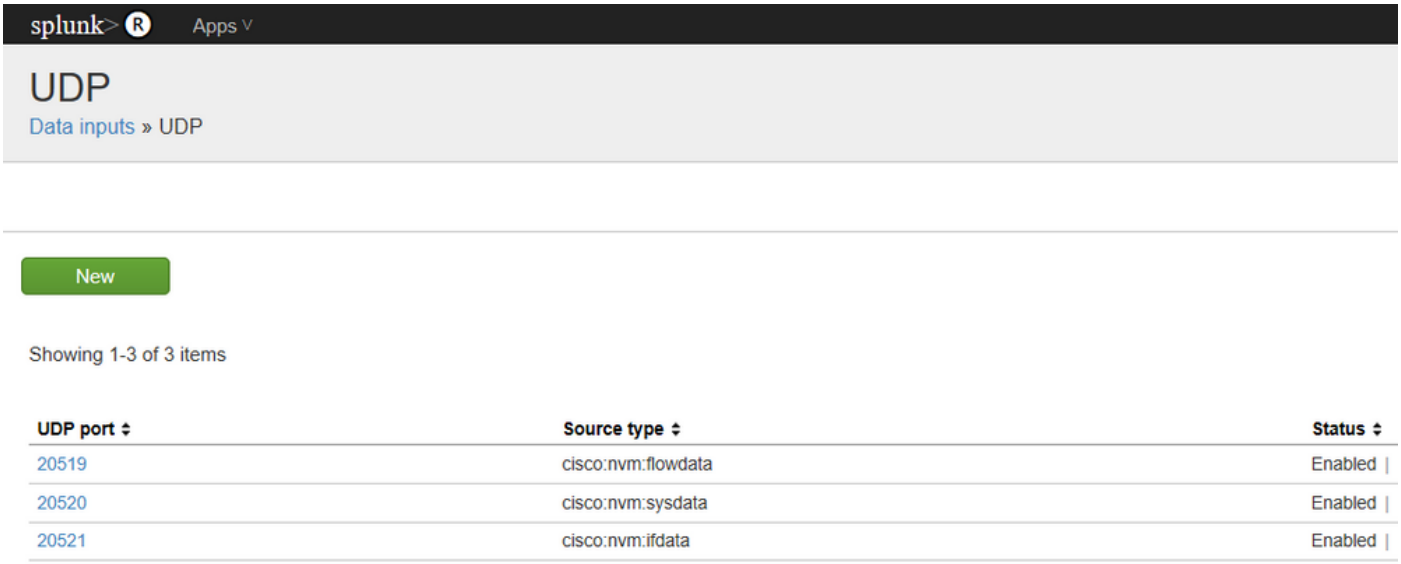
Splunk 소프트웨어를 다시 시작할 필요가 없습니다.

이미지에 표시된 대로 **Splunk > Settings > Data Input > UDP**로 이동합니다.

1. New Local UDP(새 로컬 UDP) > Enter port # missing(포트 번호 입력) > Next(다음) > Select 상응하는 소스 유형 선택 > Review(**검토)** > Submit(제출)을 클릭합니다.

2. 다른 2개 포트에 대해 반복합니다(클론 사용 시도).

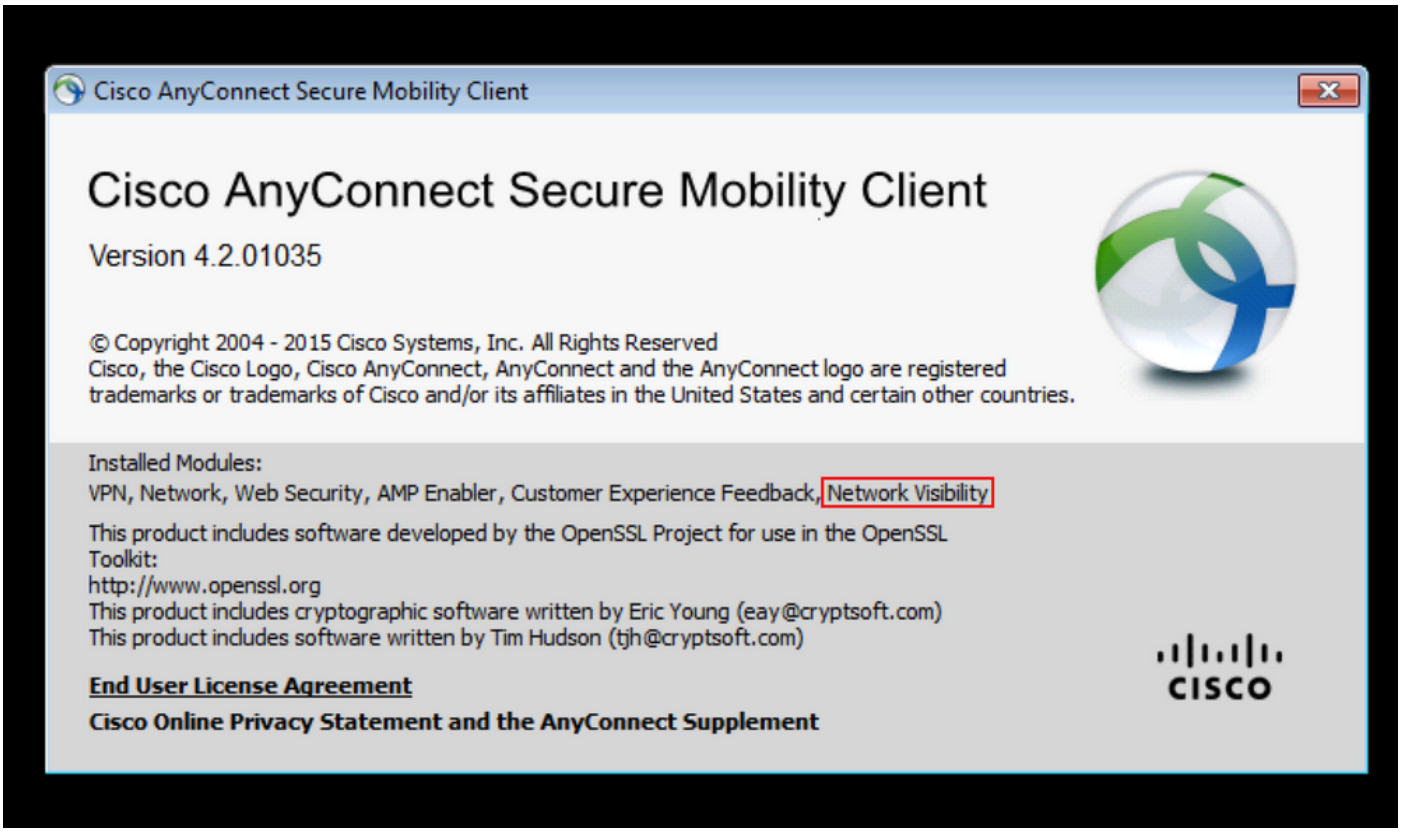




다음을 확인합니다.

AnyConnect NVM 설치 확인

설치가 완료되면 Network Visibility Module이 Anyconnect Secure Mobility Client의 **Information** 섹션 내에 **Installed Modules**에 나열되어야 합니다.



또한 nvm 서비스가 엔드포인트에서 실행 중이고 프로파일이 필수 디렉토리에 있는지 확인합니다.

컬렉터 상태를 실행 중으로 확인

컬렉터 상태가 실행 중인지 확인합니다.이렇게 하면 컬렉터가 엔드포인트에서 항상 IPFIX/cflow를 수신합니다.실행 중이 아닌 경우 파일에 대한 acnvm 계정 권한이 실행 가능하도록 허용하는지 확인합니다./opt/acnvm/bin/acnvmcollector

```
root@ubuntu-splunkcollector:~$ /etc/init.d/acnvmcollectord status
 * acnvmcollector is running
root@ubuntu-splunkcollector:~$
```

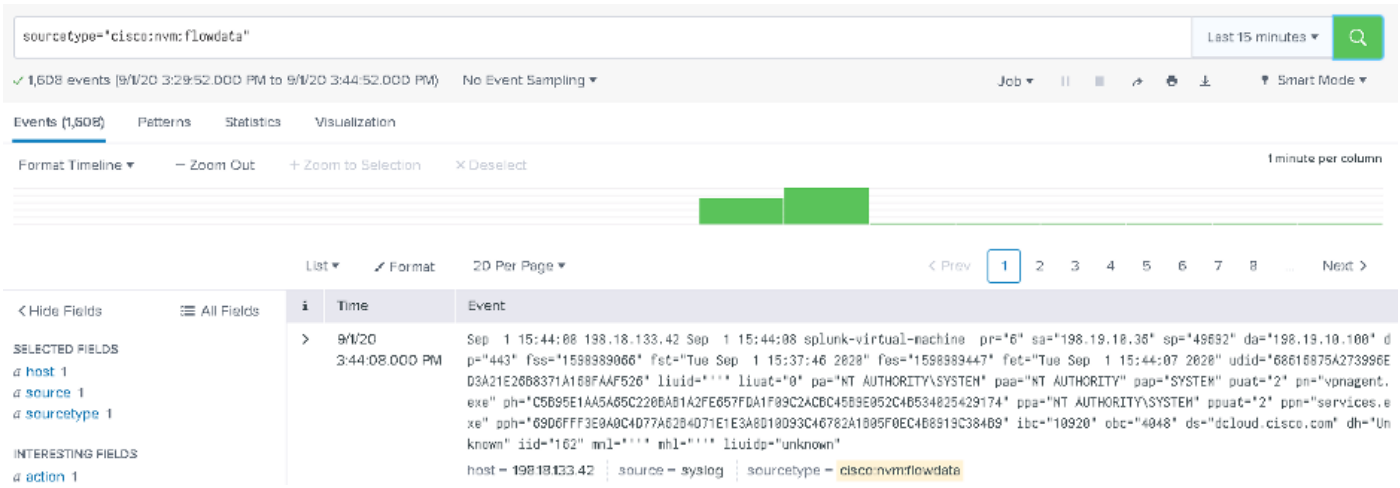
```
[splunk@splunk-virtual-machine addon]$ systemctl status acnvm.service
● acnvm.service - AC NVM Service
   Loaded: loaded (/usr/lib/systemd/system/acnvm.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2020-06-19 13:48:08 EDT; 25s ago
 Main PID: 41165 (acnvmcollector)
    Tasks: 13 (limit: 49772)
   Memory: 1.8M
   CGroup: /system.slice/acnvm.service
           ├─41165 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
           ├─41176 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
           ├─41177 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
           ├─41178 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
           └─41179 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
lines 1-12/12 (END)
```

Splunk 확인 - AnyConnect NVM CESA 대시보드

Splunk 및 관련 서비스가 실행 중인지 확인합니다.Splunk 문제 해결에 대한 자세한 내용은 해당 웹사이트를 참조하십시오.

자동화 스크립트로 인해 초기 데이터를 받은 후 5분이 경과해야 CESA의 대시보드가 업데이트되지 않습니다.수동 검색을 실행하여 즉시 검증합니다.

기본 대시보드에서 "Search & Reporting(검색 및 보고)"을 클릭합니다. 다음 화면에서 원하는 데이터를 입력한 다음 "Enter search here..."라는 메시지가 표시되는 경우 올바른 범위를 설정합니다. "sourcetype="cisco:nvm:flowdata"를 입력합니다.



Splunk Dashboard(Splunk 대시보드)를 확인하여 Go to Splunk(Splunk로 이동)를 확인하고 **Cisco NVM Dashboard(Cisco NVM 대시보드)**를 클릭하고 현재 설정을 유지하려면 Device Activity by Volume(볼륨별 **디바이스 활동) 및 Flow Count(플로우 수)를** 클릭하고 **Submit(제출)을 클릭합니다** .그래픽에 데이터가 표시됩니다.

패킷 흐름

1. IPFIX 패킷은 Anyconnect NVM 모듈에 의해 클라이언트 엔드포인트에서 생성됩니다.

2. 클라이언트 엔드포인트는 컬렉터 IP 주소로 IPFIX 패킷을 전달합니다.

3. 수집자가 정보를 수집하여 Splunk에 전달합니다.

4. 컬렉터가 세 개의 다른 스트림에서 Splunk로 트래픽을 전송합니다.플로우 데이터, 엔드포인트 데이터 및 인터페이스 데이터당

모든 트래픽은 트래픽에 대한 승인 없이 UDP입니다.

트래픽의 기본 포트:

IPFIX 데이터 2055

플로우 데이터당 20519

엔드포인트 데이터 20520

인터페이스 데이터 20521

NVM 모듈은 IPFIX 데이터를 캐시하여 신뢰할 수 있는 네트워크에 있을 때 컬렉터로 전송합니다.랩톱이 회사 네트워크(온프레미스)에 연결되거나 VPN을 통해 연결된 경우일 수 있습니다.

컨피그레이션에 따라 특정 UDP 포트에서 패킷 캡처를 실행하여 컬렉터가 NVM 모듈에서 패킷을 수신하고 있는지 확인하여 패킷이 수신되고 있는지 확인할 수 있습니다.이는 Splunk 시스템 Linux OS를 통해 수행됩니다.

플로우 템플릿

IPFIX 플로우 템플릿은 IPFIX 통신이 시작될 때 컬렉터로 전송됩니다.이러한 템플릿은 컬렉터가 IPFIX 데이터를 이해하는 데 도움이 됩니다.

또한 컬렉터는 클라이언트가 데이터를 구문 분석할 수 있도록 템플릿을 미리 로드합니다.최신 버전의 클라이언트가 프로토콜 변경 사항과 함께 릴리스되면 클라이언트에서 보낸 새 템플릿이 사용됩니다.

템플릿은 다음 조건에 따라 전송됩니다.

1. NVM 클라이언트 프로파일이 변경되었습니다.
2. 네트워크 변경 이벤트가 있습니다.
3. 클라이언트 서비스가 다시 시작됩니다.
4. 엔드포인트가 리부팅/재시작됩니다.
5. NVM 프로파일에 구성된 대로 주기적으로(기본값=24시간)

드물게 템플릿을 찾을 수 없습니다. 엔드포인트 중 하나를 다시 시작하여 쉽게 해결할 수 있습니다.

이 문제는 엔드포인트의 패킷 캡처에서 **찾을 수 없는 템플릿**을 관찰하거나 컬렉터 로그에 flowset**에 대한 템플릿**이 **없음을** 관찰하여 확인할 수 있습니다.

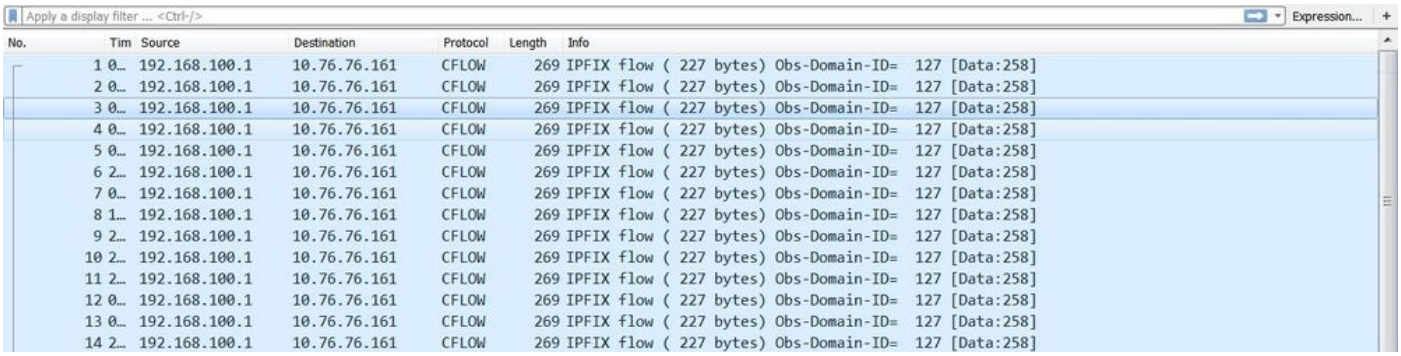
문제 해결

다음은 트러블슈팅을 위한 기본 단계입니다.

1. 클라이언트 엔드포인트와 컬렉터 간의 네트워크 연결을 확인합니다.
2. 컬렉터와 Splunk 간의 네트워크 연결을 보장합니다.
3. NVM이 클라이언트 엔드포인트에 올바르게 설치되었는지 확인합니다.
4. 엔드포인트에 캡처를 적용하여 IPFIX 트래픽이 생성되고 있는지 확인합니다.
5. 컬렉터에 캡처를 적용하여 IPFIX 트래픽을 수신하는지, 트래픽을 Splunk로 전달하는지 확인합니다.
6. Splunk에 캡처를 적용하여 트래픽을 수신하는지 확인합니다.
7. DTLS용 anyconnect 클라이언트는 컬렉터 인증서를 신뢰함NVM 프로파일이 보안 활성화됨 certs에 대해 컬렉터가 구성되어 있음

Wireshark에서 볼 수 있는 IPFIX 트래픽:

> **참고:**클라이언트와 컬렉터 간에 DTLS를 실행하는 경우 DTLS 트래픽에 대해 필터링해야 합니다.

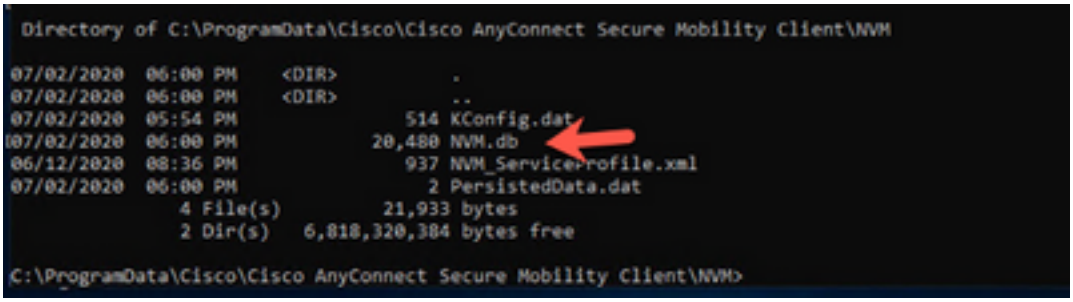


No.	Tim	Source	Destination	Protocol	Length	Info
1	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
2	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
3	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
4	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
5	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
6	2…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
7	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
8	1…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
9	2…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
10	2…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
11	2…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
12	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
13	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
14	2…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]

AnyConnect 클라이언트(NVM 모듈)

AnyConnect NVM - 컬렉터에 보고하지 않음 - CFLOW 데이터 패킷이 최종 엔드포인트를 벗어나지 않음

NVM 데이터베이스 파일이 C:\%ProgramData%\Cisco\Cisco Anyconnect Secure Mobility Client에서 증가합니까?계속 증가하면 클라이언트에서 로그를 보내지 않습니다.NVM 폴더 아래에서 SQL 데이터베이스가 증가하는 것을 볼 수 있는 경우 nvm.db는 문서화되지 않지만 NVM 가이드에서 캐시하는 방법과 캐싱에 대한 제어 방법에 대해 자세히 설명합니다.컬렉터에 데이터를 전송하지 않습니다.



```
 Directory of C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM

07/02/2020  06:00 PM    <DIR>          .
07/02/2020  06:00 PM    <DIR>          ..
07/02/2020  05:54 PM               514 KConfig.dat
07/02/2020  06:00 PM            20,480 NVM.db
06/12/2020  08:36 PM               937 NVM_ServiceProfile.xml
07/02/2020  06:00 PM                 2 PersistedData.dat
               4 File(s)         21,933 bytes
               2 Dir(s)   6,818,320,384 bytes free

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>
```

TND(Trusted Network Detection)

AnyConnect UI를 시작하고 신뢰할 수 있는 네트워크에 있는지 확인합니다.NVM은 엔드포인트가 신뢰할 수 있는 네트워크 내에 있는 경우 TND를 사용합니다.TND 컨피그레이션이 올바르지 않으면 NVM에 문제가 발생합니다.NVM에는 구성된 서버의 TLS 인증서 핑거프린트에서 작동하는 자체 TND 컨피그레이션이 있습니다.NVM 프로파일 편집기에서 구성할 수 있습니다.

NVM TND가 구성되지 않은 경우 NVM은 VPN 모듈의 TND 컨피그레이션을 사용합니다.VPN의 TND는 DHCP를 통해 받은 정보를 기반으로 작동합니다.도메인 이름 및 DNS 서버.DNS 서버 및/또는 도메인 이름이 구성된 값과 일치하면 네트워크가 신뢰된 것으로 간주됩니다.VPN은 TLS 인증서 기반 TND 탐지도 지원합니다.

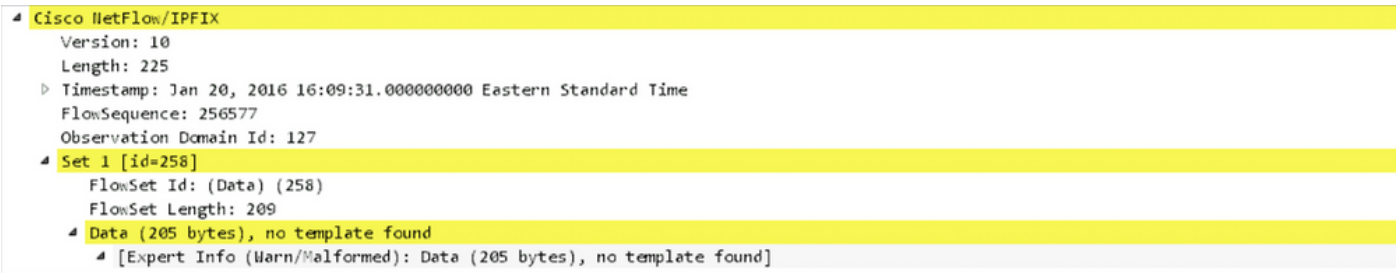
- 신뢰할 수 있는 네트워크 탐지 컨피그레이션이 올바른지 확인합니다.NVM은 신뢰할 수 있는 네트워크에서 잘못된 TND 컨피그레이션(예:3개의 DNS 서버가 있는 경우 3개의 DNS 서버가 정의되어 있어야 합니다.
- TND VPN 구성에서 트러스트된 도메인 제거

- 네트워크 문제: 스플릿 터널링(컬렉터의 IP 주소가 신뢰할 수 있는 스플릿 터널의 일부가 아니므로 데이터가 공용 인터페이스로 전송됨) 컬렉터의 IP를 항상 VPN에 대한 스플릿 포함 컨피그레이션에 포함해야 합니다.
- CollectionMode가 현재 네트워크(신뢰/신뢰 안 함)에서 수집하도록 구성되어 있는지 확인합니

다.

- VPN.xml 및 NVM_ServiceProfile.xml이 올바른 폴더에 있는지 확인하고 다시 시작합니다.
- 모든 anyconnect 서비스 시작-중지
- DNS 서버에 연결되어 있는 내부에 연결된 네트워크를 바운스합니다.

패킷 캡처:



AnyConnect 진단 및 보고 툴(DART)

AnyConnect가 NVM 구성 요소에서 실행 DART를 실행하는 문제를 해결하려면

- NVM에 필요한 모든 로그는 DART에 의해 처리되며, 로그 파일, 구성 등을 수집합니다.
- Windows 로그 - 이벤트가 한 곳에 없는 경우, AnyConnect에서 NVM용 이벤트 뷰어에 별도의 리프가 있습니다.
- macOS/linux - 네이버별로 로그 필터링

컬렉터(Linux/Docker 시스템 - 올인원 또는 독립형)

acnvmcollector를 설치하지 못했습니다.

컬렉터를 설치하고 설치 스크립트를 실행하는 동안

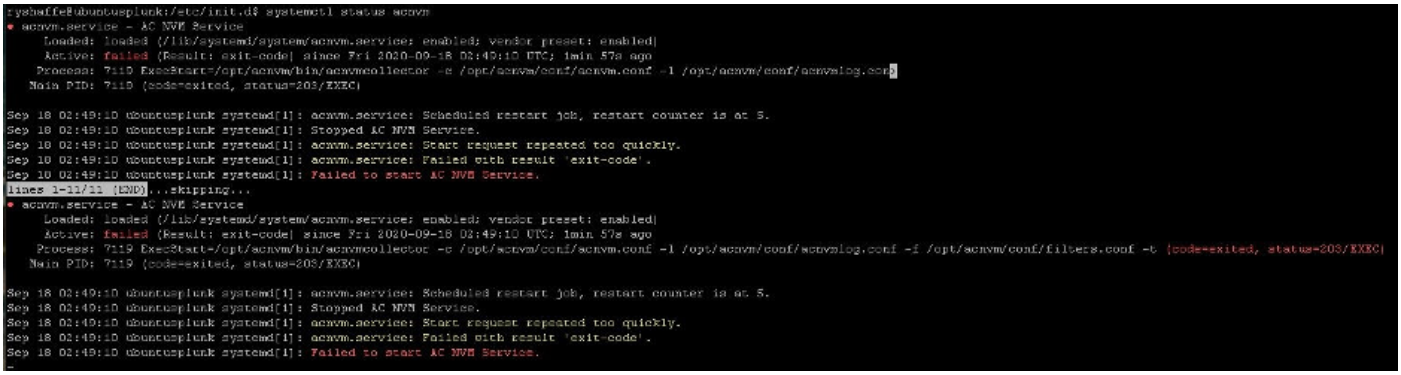
수도 ./install_ubuntu.sh

/var/log/syslog에 오류가 있습니다. "Acnvm.conf 오류:행 번호 17:쉼표가 있을 수 없는 경우, 하나 이상의 쉼표가 있기 때문입니다.

acnvmcollector를 시작하지 못했습니다.

Ubuntu에서 문제가 발생했습니다(그러나 모든 Linux에서 가능).acnvmcollector 파일에서 코드를 실행하지 못했습니다./opt/acnvm/bin/acnvmcollector

acvnm 사용자 및 그룹에 acnvmcollector에 대한 eXecute가 없습니다.



컬렉터 로그

컬렉터의 버전을 보려면 어떻게 해야 합니까?

/nvmcollector -v

디버그는 어디에서 설정할 수 있습니까?

ACMNVMLOG.conf - 컬렉터 시작 시 전송된 컨피그레이션의 일부인 로깅 레벨을 설정할 수 있습니다.변경 후 컬렉터를 다시 시작합니다.

log4cplus.rootLogger=DEBUG, STDOUT, NvmFileAppender < **ACNVMLOG**.conf 파일에 있음

```
Jan 20 12:48:54 csaxena-ubuntu-splunkcollector NVMCollector: no templates
for flowset 258 for 10.150.176.167 yet
Jan 20 12:48:55 csaxena-ubuntu-splunkcollector NVMCollector:
HandleReceivedIPFIX: exporter=10.150.176.167 bytes_recvd=234 totlength=234
Jan 20 12:48:55 csaxena-ubuntu-splunkcollector NVMCollector:
==================> flowsetid=258 flowsetlen=218
Jan 20 12:48:55 csaxena-ubuntu-splunkcollector NVMCollector: no templates
for flowset 258 for 10.150.176.167 yet
```

DTLS 문제:

- DTLS가 구성되지 않음(acnvm.conf 파일에 표시되지 않음)
- 서버 키가 잘못되었습니다(지원되지 않는 암호 키 콤보).

Splunk Console(NVM 대시보드)에서 데이터를 표시하지 않음

AnyConnect 클라이언트

- youtube를 사용하여 데이터를 생성하고 몇 개의 웹 사이트를 탐색할 수 있습니다.
- AnyConnect 클라이언트가 UDP 2055를 통해 컬렉터 서버에 정보를 보낼 수 있습니까(사이에 방화벽이 있습니까?)? 클라이언트 시스템에서 컬렉터 시스템으로 텔넷 사용
- Wireshark를 실행하여 클라이언트가 트래픽(2055 cflow) 데이터를 컬렉터로 전송하는지 확인

컬렉터 상자

- 수신 AnyConnect NVM 트래픽 확인 tcpdump를 수행합니다(그리고 25001에서 2055까지 클라이언트에서 서버로 패킷을 볼 수 있는지 확인). Sudo tcpdump -I any -c100 -nn host 10.1.110.7(클라이언트 호스트 IP에서 처음 100개의 패킷 수신)[센터에서 TCPDUMP를 사용하](#)

는 방법

- anyconnect NVM 컬렉터가 실행 중인지 확인합니다(systemctl을 사용하는 경우 상단의 정보 참조).
- 포맷, 누락된 견적, 쉼표 등에 대해서는 acnvm.conf를 확인하십시오.

- **Splunk UI** - TA - Splunk GUI 또는 input.conf를 통해 UDP 데이터 입력 및 소스 유형 설정 **UI > settings > server controls(UI > 설정 > 서버 제어)**에서 splunk를 다시 시작합니다.

공통 질문(FAQ)

1. anyconnect NVM에서 여러 대상으로 데이터를 보내려면 어떻게 해야 합니까?

이는 고가용성에 사용되거나 Splunk 및 Stealthwatch로 전송하는 데 사용됩니다.

자세한 내용은 http://cs.co/cesa-pov을 참조하십시오.

2. AnyConnect NVM DTLS용 인증서를 어디에 저장합니까?

컬렉터에 잘 알려진 인증서가 설치되어 있지 않은 랩 테스트용입니다.

- 윈도우

Windows 신뢰할 수 있는 인증서에 컬렉터 인증서 설치

- Mac OSX

루트 인증서를 설치하는 경우 이 프로세스는 표준이며 키 체인을 통해 제공되는 macOS에 대해 잘 정의되어 있습니다. Keychain 툴을 사용하여 Trusted로 가져오고 추가할 수 있습니다.

- Linux - 각 distro(Ubuntu 및 RHEL)마다 다릅니다.

RHEL 루트 CA 가져오기 단계:
1. ca **인증서를/etc/pki/ca-trust/source/anchors에 복사합니다.**
2 .**sudo update-ca-trust enable**
3. 마지막으로, **sudo update-ca-trust extract**

Ubuntu 루트 CA 가져오기 단계:

1. **.cer** 파일을 **.crt** 파일로 변환합니다.openssl x509 -inform PEM -in RootCA.cer -out rootCa.crt
2. **.crt** 파일을 **/usr/local/share/ca-certificates에 복사합니다.**
3. sudo update-**ca-certificates 명령을 실행합니다.**

XML 파일 이름

로컬 프로파일 편집기를 사용할 때핵심 VPN 모듈 XML 프로필 이름은 중요하지 않습니다. "프로필을 NVM_ServiceProfile.xml로 저장하십시오.이 정확한 이름으로 프로파일을 저장해야 합니다. 그렇지 않으면 NVM에서 데이터를 수집 및 전송하지 못합니다."

컬렉터(anyconnect NVM)

https://splunkbase.splunk.com/app/2992/#/details

- 공급업체 디렉토리를 루트 아래에 생성한 다음 다른 계정에 제공된 소유권을 생성할 수 있습니까? 설치 스크립트에 파일을 복사할 수 있는 권한이 있는 한 먼저 **/opt/acnvm을** 만들 수 있습니다.
- 파일 권한 - **install.sh**는 루트로 실행할 권한이 필요합니다.
- 서비스 계정: 사용자 **추가 -r**을 선택해야 하는 이유 및 홈 디렉토리가 없는 비대화형 계정이므로 why-s /bin/false홈 디렉토리는 필수 사항이 아니며 서비스 어카운트의 표준 관행에서 안전한 상태를 유지할 수 없습니다.모든 사용자는 홈 디렉토리를 가지고 있는지 여부에 관계없이 uid/guid를 갖습니다.
- 컬렉터 OS - CentOS, Ubuntu, Redhat에서 CentOS 스크립트를 사용할 수 있습니다.
- 설치 스크립트 - 필요한 경우 수정할 수 있습니다. acnvm이라는 새 사용자를 생성하고 모든 항목을 **/opt/acnvm** 디렉토리에 배치하므로 루트 또는 SUDO 권한**으로** 실행해야 합니다.일반 참고 사항:요구 사항에 따라 필요한 작업을 수행할 수 있도록 자체 스크립트를 만들 수도 있습니다.이 스크립트는 이미 시스템에서 실행 중인 다른 사용자를 사용할 수 있지만 이 사용자는 설치를 실행하려면 SUDO 권한이 있어야 합니다.
- -v 플래그로 실행되는 컬렉터 버전을 찾으려면 ./opt/acnvm/bin/acnvmcollector -v

권장 릴리스

Cisco는 사용 또는 업데이트 시 항상 최신 버전의 AnyConnect를 권장합니다.AnyConnect 버전을 선택하는 동안 최신 4.9.x 클라이언트 이상을 사용하십시오.이를 통해 NVM과 관련하여 최신 개선 사항이 제공됩니다.

AnyConnect 4.9.00086 새로운 기능

이 릴리스는 이러한 기능을 포함하고 업데이트를 지원하며 AnyConnect 4.9.00086에 설명된 결함을 해결하는 주 릴리스입니다.

- 새로운 NVM 컬렉터를 비롯한 플로우 및 엔드포인트 데이터를 보완하기 위한 NVM 확장은 Splunk 앱 3.x와 조율되고 플로우 정보에 대한 타임스탬프가 제공됩니다.

관련 정보

- Cisco Endpoint Security Analytics on Splunk(빠른 시작 가이드)
- Splunk용 Cisco AnyConnect NVM(Network Visibility) 앱
- Splunk Collector 설치 및 컬렉터 스크립트 설치에 대한 Splunk 문서
- Cisco AnyConnect Secure Mobility Client- 관리 설명서
- AnyConnect 4.x 릴리스 정보
- 기술 지원 및 문서 – Cisco Systems