단일 FMC에서 관리하는 FTD 간의 VPN 마이그레이션 구성

목차

소개

이 문서에서는 라우터에 대한 VPN 연결을 유지하면서 동일한 FMC에서 관리하는 사이트 대 사이트 VPN을 한 FTD에서 다른 FTD로 마이그레이션하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

마이그레이션 프로세스를 효과적으로 수행하기 위해 Cisco에서는 다음 항목에 대해 숙지할 것을 권장합니다.
· FMC에 FTD 등록: FTD(Firepower Threat Defense) 디바이스를 FMC(Firepower Management Center)에 등록하는 방법 이해
· Site-to-Site VPN 구성: FMC에서 관리하는 FTD 디바이스에서 사이트 대 사이트 VPN을 구성할 수 있는 환경

사용되는 구성 요소

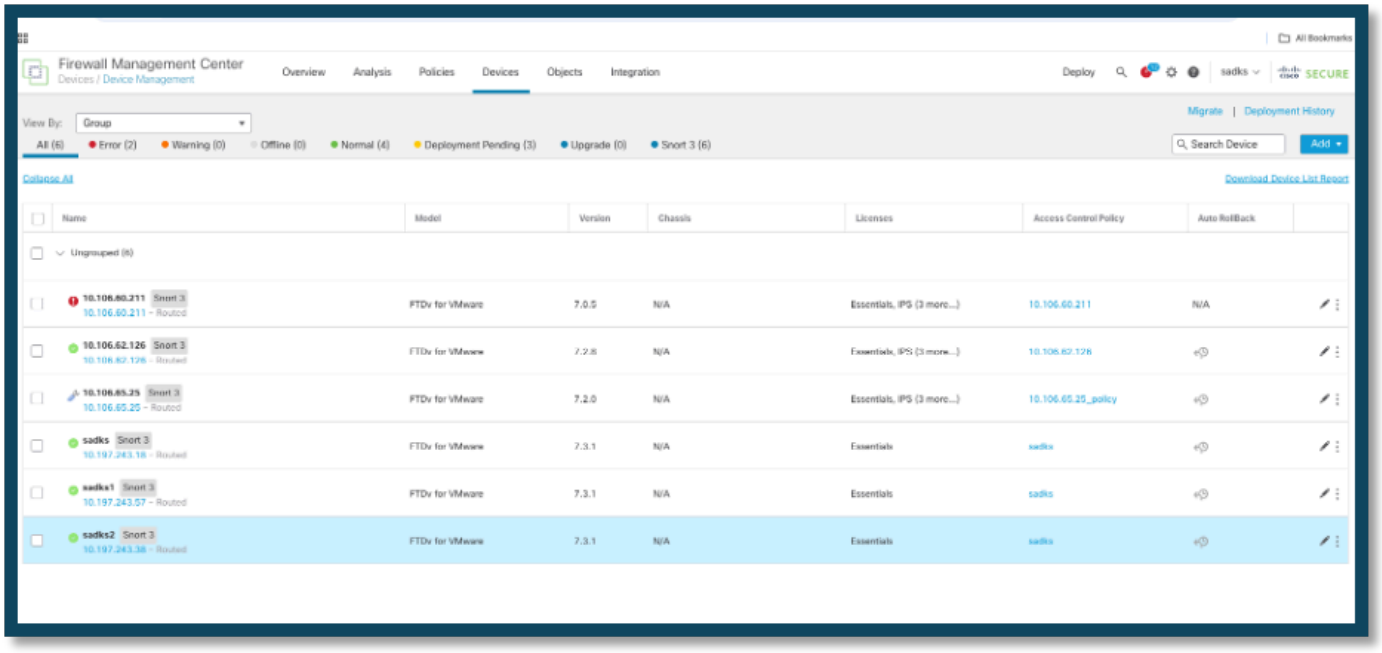
이 문서는 지정된 소프트웨어 및 하드웨어 버전을 기반으로 합니다.
· Firepower FTDv(Threat Defense Virtual): 버전 7.3.1을 실행하는 인스턴스 2개
· FMC(Firepower 관리 센터): 버전 7.4.0.

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.

구성

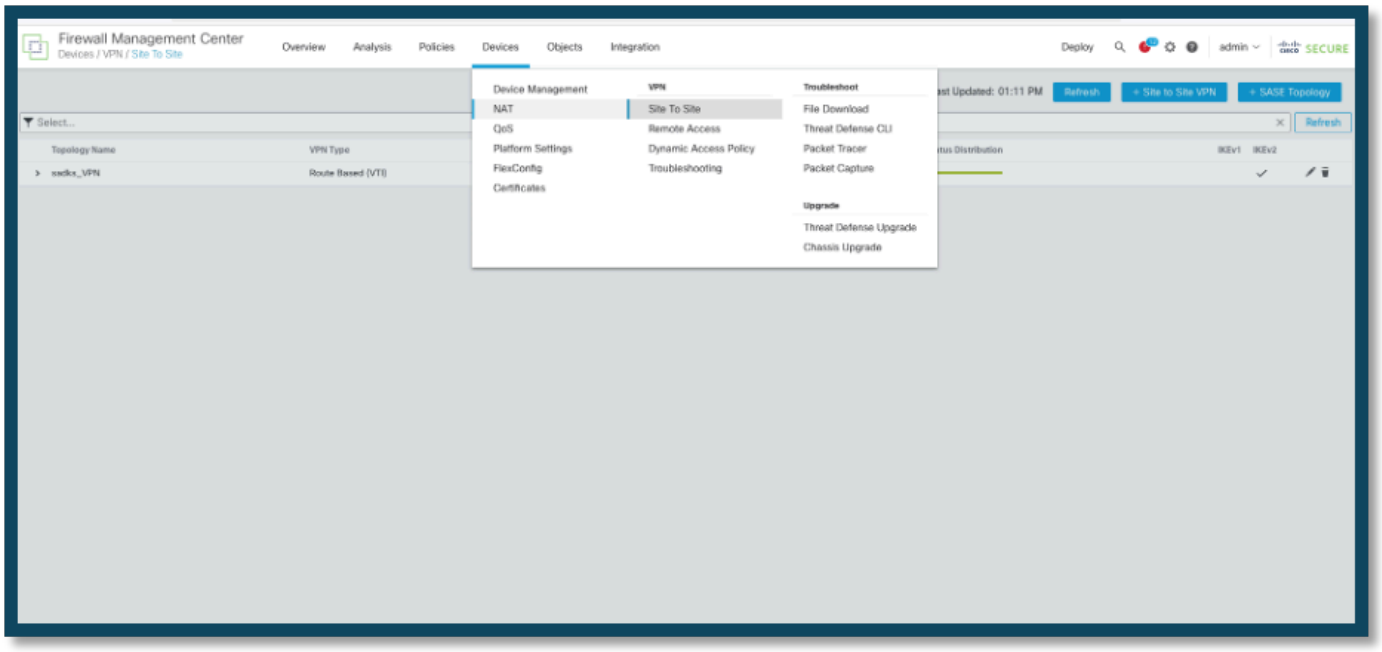
절차

1. FMC에 새 FTD 등록:
   · Devices(디바이스) > Device Management(디바이스 관리) 아래의 FMC(Firepower Management Center) 내에 새 Firepower Threat Defense(FTD) 디바이스를 등록하는 것으로 시작합니다.
   · 이 예에서 등록된 새 디바이스의 이름은 "sadks2"입니다.



새 FTD 등록

2 . Site-to-Site 터널 컨피그레이션에 액세스합니다.
   · FMC 인터페이스의 Devices(디바이스) > Site to Site(사이트 대 사이트)로 이동하여 Site-to-Site 터널 설정으로 이동합니다.

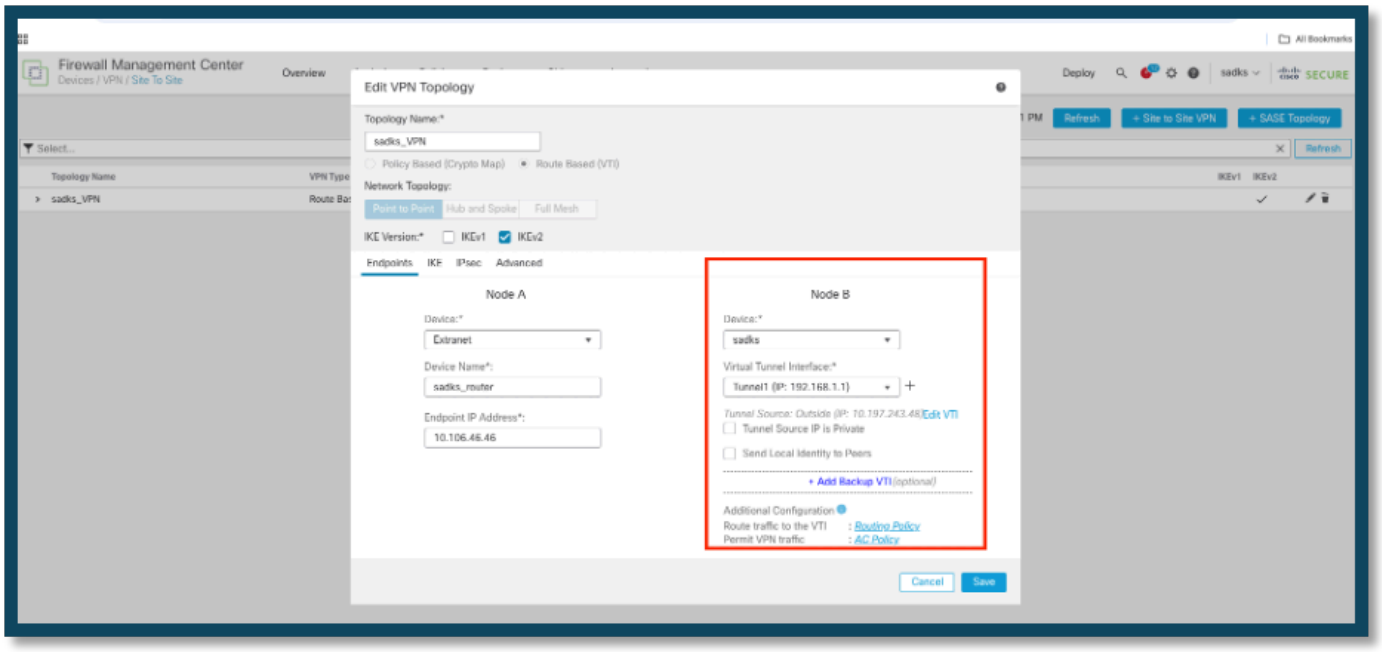


VPN Config(VPN 구성)로 이동합니다.

3. VPN 컨피그레이션을 수정합니다.

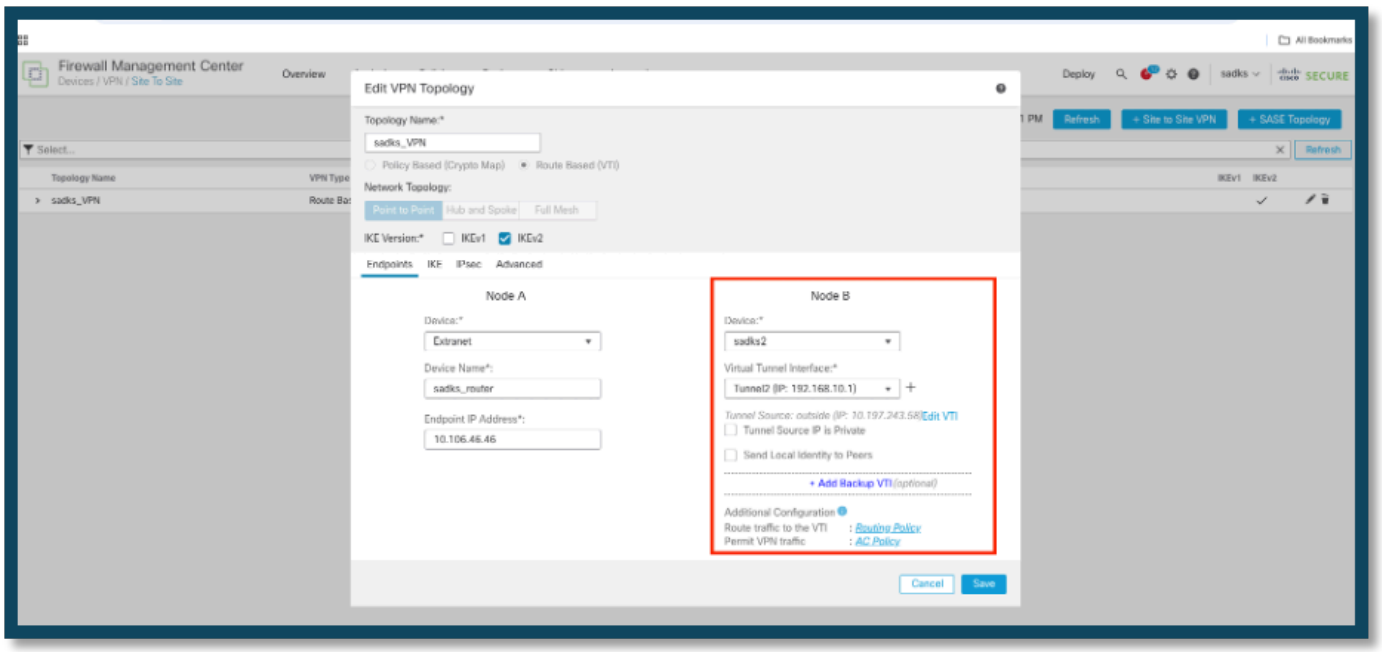
· 업데이트할 VPN 컨피그레이션을 선택합니다.

•예: 이 시나리오에서 VPN 컨피그레이션에는 FTD 디바이스 및 라우터가 포함됩니다. 여기서 Node B는 FTD 디바이스를 나타내며, 디바이스 연결을 "sadks"에서 "sadks2"로 변경하도록 컨피그레이션이 업데이트되었습니다.



기존 FTD 디바이스

수신



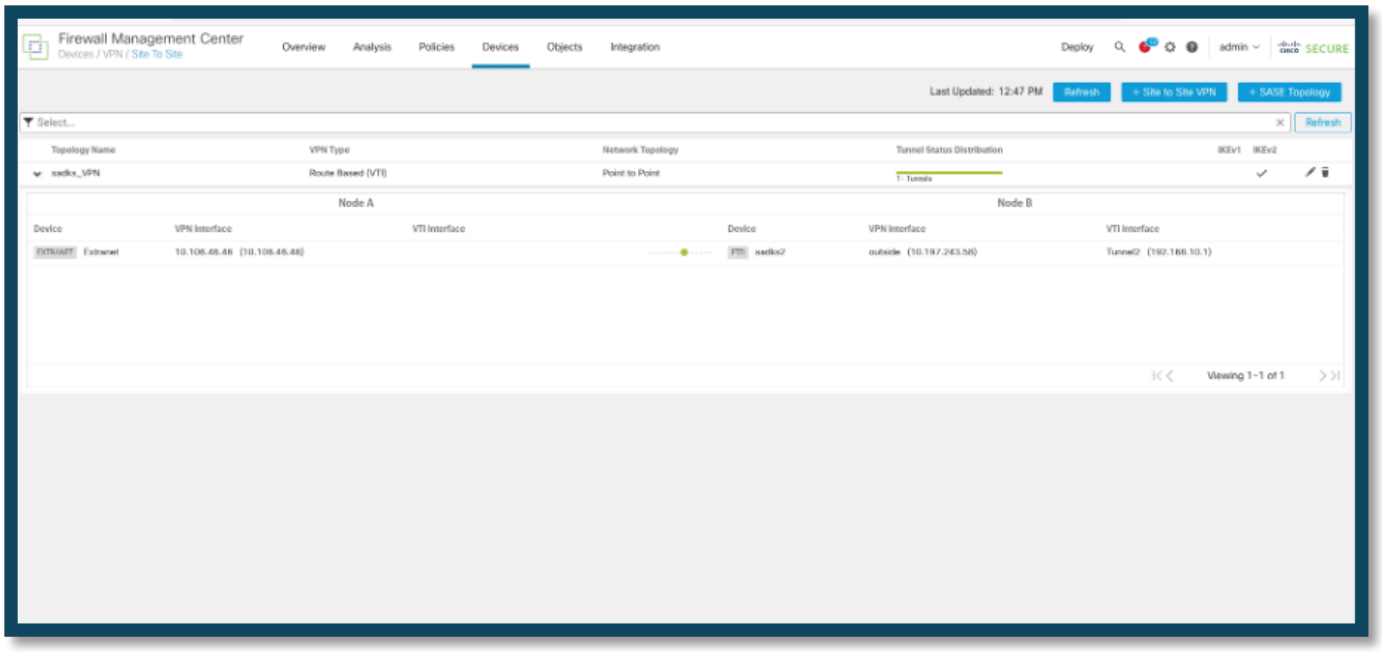
새 FTD 디바이스

4. 구성을 저장하고 배포합니다.

· 필요한 변경을 수행한 후 컨피그레이션을 저장하고 구축하여 업데이트를 활성화합니다.

다음을 확인합니다.

터널은 구축되면 가동됩니다.



터널 상태

문제 해결

초기 연결 문제

VPN을 구축할 때 양쪽이 터널을 협상합니다. 따라서 어떤 유형의 터널 오류도 트러블슈팅할 때 대화의 양쪽을 모두 확인하는 것이 좋습니다. IKEv2 터널을 디버깅하는 방법에 대한 자세한 내용은 IKEv2 VPN을 디버깅하는 방법을 참조하십시오.

터널 장애의 가장 일반적인 원인은 연결 문제입니다. 이를 결정하는 가장 좋은 방법은 디바이스에서 패킷 캡처를 수행하는 것입니다. 다음 명령을 사용하여 디바이스에서 패킷 캡처를 수행합니다.

<#root>

```
capture capout interface outside match ip host 10.106.46.46 host 10.197.243.58
```

캡처가 제자리에 있으면 VPN을 통해 트래픽을 전송하고 패킷 캡처에서 양방향 트래픽을 확인합니다.

다음 명령을 사용하여 패킷 캡처를 검토합니다.

<#root>

```
show cap capout
```

트래픽 관련 문제

일반적인 트래픽 문제는 다음과 같습니다.

- FTD 뒤에 라우팅 문제 — 내부 네트워크에서 할당된 IP 주소 및 VPN 클라이언트로 패킷을 다시 라우팅할 수 없습니다.
- 액세스 제어 목록은 트래픽을 차단합니다.
- VPN 트래픽에 대해 네트워크 주소 변환이 우회되지 않습니다.

FMC에서 관리하는 FTD의 VPN에 대한 자세한 내용은 다음 전체 컨피그레이션 가이드를 참조하십시오. FTD managed by FMC 컨피그레이션 가이드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.