정책 기반 라우팅을 통해 프라이빗 액세스를 위한 보안 방화벽 위협 방어 기능으로 보안 액세스 구성

목차

소개

이 문서에서는 IPsec을 통한 FTD를 통한 보안 액세스를 정책 기반 라우팅을 통한 보안 개인 액세스로 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

- Cisco Secure Access 지식
- Cisco Secure Access 대시보드/테넌트
- 보안 방화벽 위협 방어 및 방화벽 관리 센터 지식
- IPsec 지식
- 정책 기반 라우팅 지식

사용되는 구성 요소

- 7.7.10 코드를 실행하는 보안 방화벽
- 클라우드 기반 방화벽 관리 센터. 구성은 일반적인 가상 FMC에도 적용됩니다
- Cisco Secure Access 대시보드

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.

배경 정보

Secure Access의 네트워크 터널은 두 가지 기본 용도로 사용할 수 있습니다. 보안 인터넷 액세스 및 보안 개인 액세스

안전한 프라이빗 액세스를 위해 조직은 ZTA(Zero Trust Access) 및/또는 VPNaaS(VPN as a Service)를 활용하여 내부 애플리케이션 또는 데이터 센터와 같은 프라이빗 리소스에 사용자를 연결할 수 있습니다. IPsec 터널은 사용자와 개인 리소스 간의 네트워크 트래픽을 안전하게 암호화하여 중요한 데이터가 신뢰할 수 없는 네트워크를 통과할 때 안전하게 보호되도록 함으로써 이 아키텍처에서 중요한 역할을 합니다. IPsec 터널을 ZTA 또는 VPNaaS와 통합함으로써 조직은 내부 리소스에 대한 원활하고 안전한 액세스를 제공하는 동시에 강력한 보안 제어 및 가시성을 유지할 수 있습니다.

이 문서에서는 IPsec for Secure Private Access를 통해 FTD(Secure Firewall Threat Defense)로 보안 액세스를 구성하는 방법에 대해 설명합니다.
또한 이 가이드에서는 정책 기반 라우팅을 구성하는 단계를 제공합니다.

이 문서에서는 Secure Private Access를 위한 IPsec 터널의 컨피그레이션을 다루지만, 프라이빗 애플리케이션에 액세스하기 위한 ZTA(Zero Trust Access) 또는 VPNaaS(VPN as a Service)의 설정은 이 가이드의 범위에 속하지 않습니다.

구성

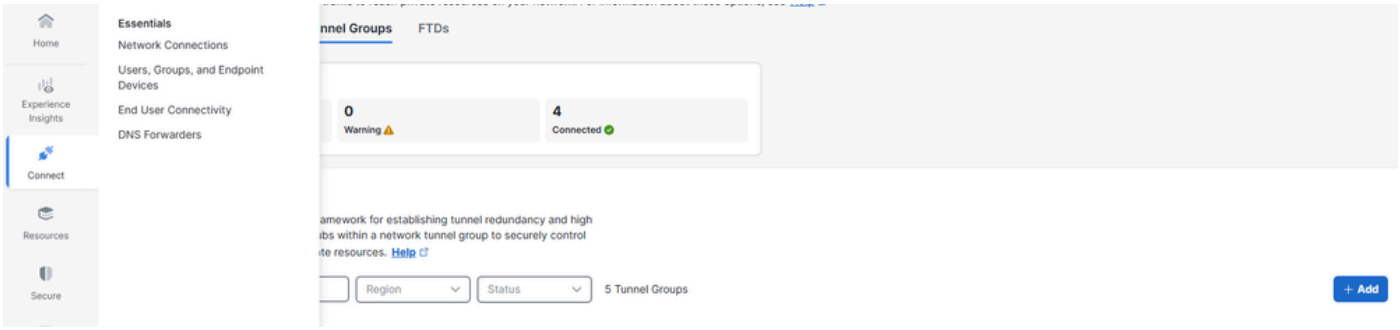
보안 액세스 컨피그레이션

네트워크 터널 그룹 컨피그레이션

1. Secure Access의 관리자 패널로 이동합니다.

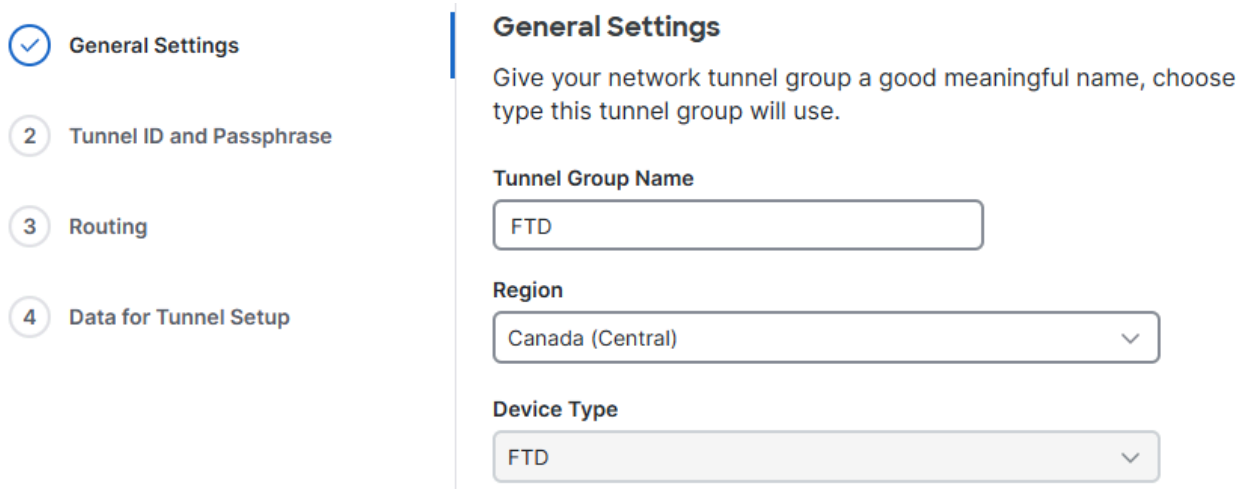
2. 네트워크 터널 그룹을 추가합니다.

- 클릭Connect> Network Connections
  - 아래에서Network Tunnel Groups>를 클릭합니다. Add



3.General Settings구성

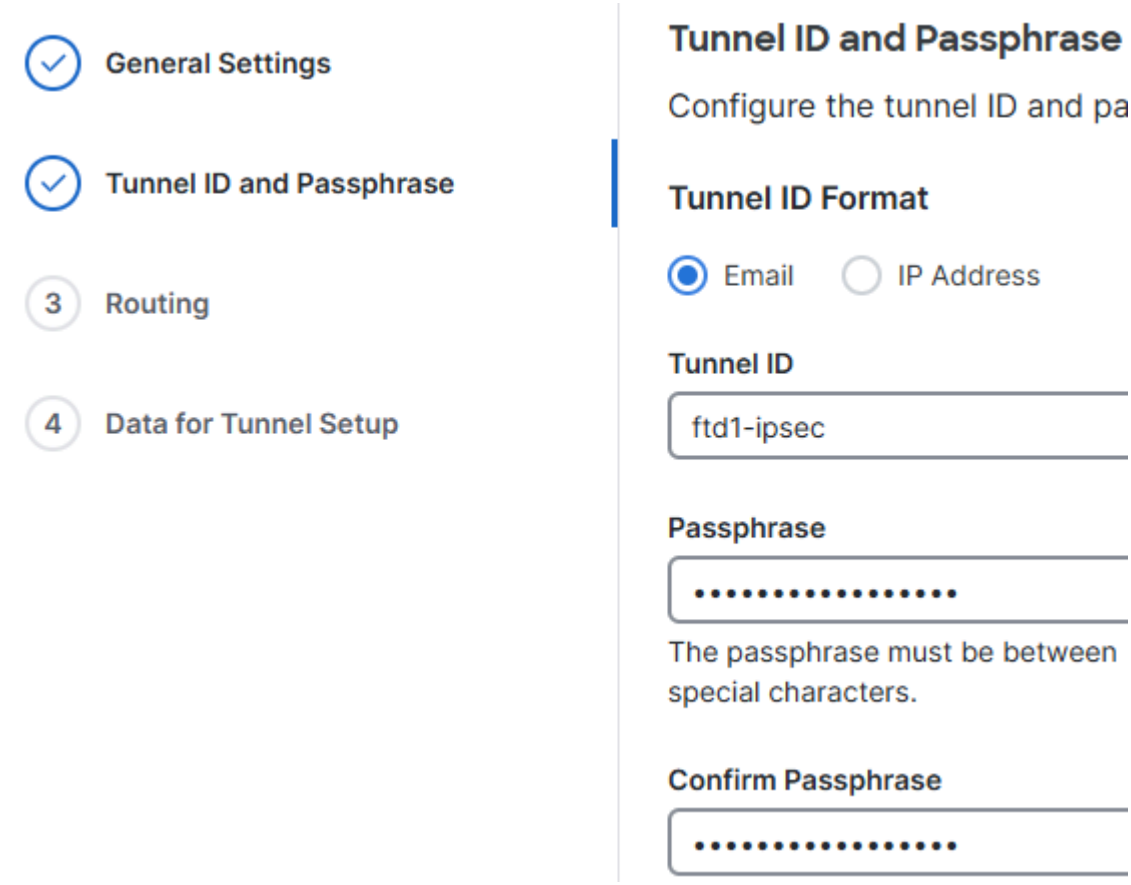
- 를Tunnel Group Name **Region** 구성하고 Device Type
  - 클릭 Next



일반 설정

4. 구성Tunnel ID및Passphrase.

- 및 **Tunnel ID**Passphrase을 구성합니다. 이 ID는 FTD 구성에 필요하므로 중요합니다
- 클릭 Next



ID 및 PSK

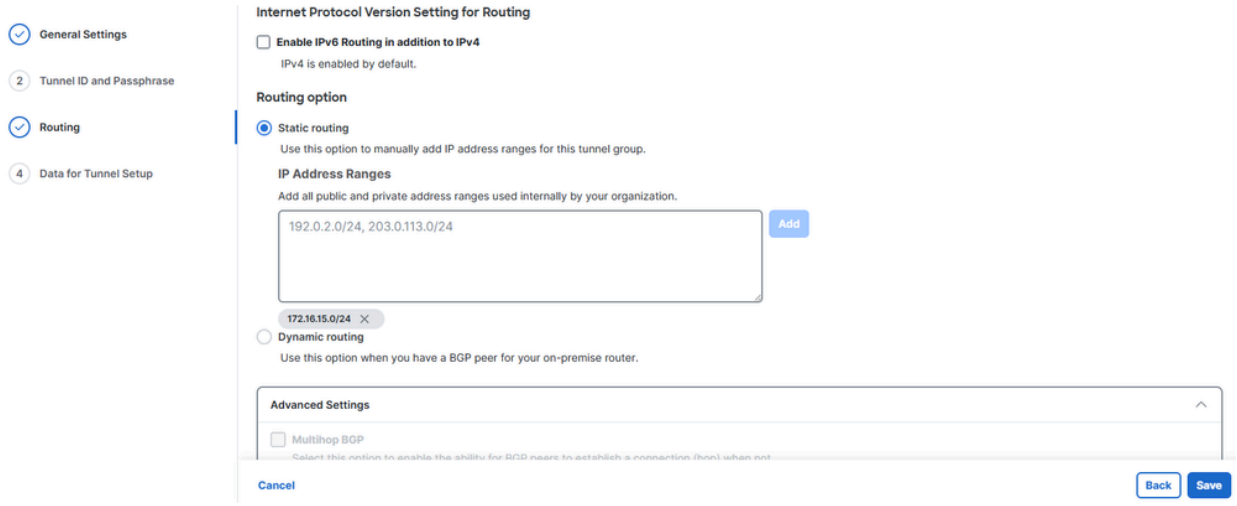
5. 고정 라우팅을 구성합니다.

보안 액세스 라우팅

정책 기반 라우팅

원격 사용자가 ZTA 및/또는 VPNaaS를 통해 액세스하려는 FTD로 보호되는 네트워크를 추가하고 Save(저장)를 클릭합니다.

- 클릭Routing> **Static routing**
  - 네트워크에서 구성했고 Secure Access를 통해 트래픽을 전달하려는 IP 주소 범위 또는 호스트를 추가하고Add
  - 클릭Save

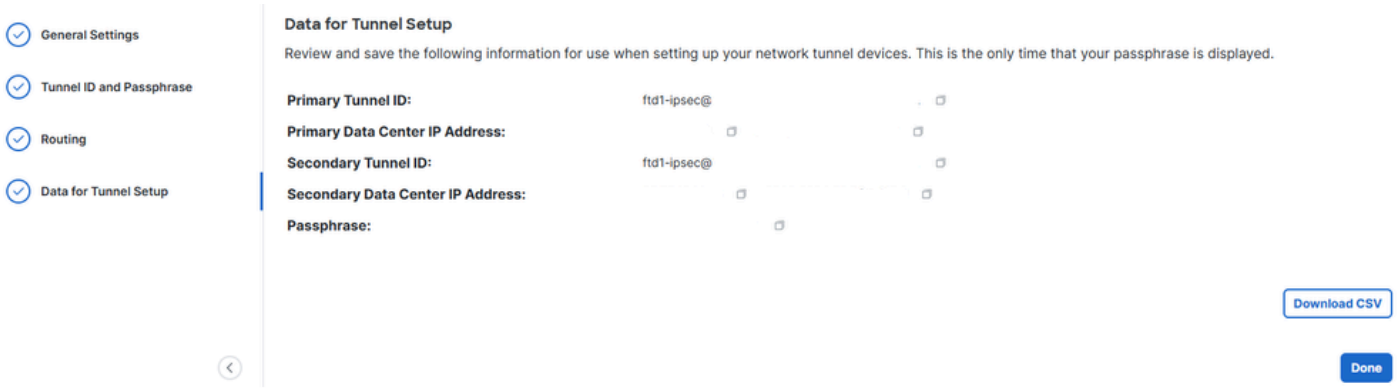


CSA 정적 라우팅

네트워크 터널 그룹 컨피그레이션 저장

FTD 컨피그레이션에 필요한 터널 설정 데이터를 다운로드하여 저장합니다.

- 클릭 Download CSV
- 클릭 Done



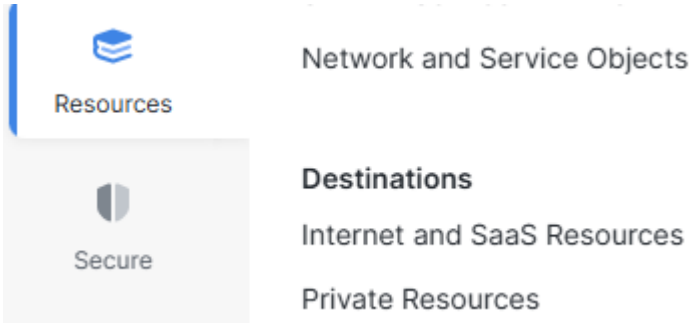
NTG 데이터

프라이빗 리소스 생성

프라이빗 리소스는 데이터 센터 또는 프라이빗 클라우드 환경에서 호스팅되는 내부 애플리케이션, 네트워크 또는 서브넷입니다. 이러한 리소스는 공개적으로 액세스할 수 없으며 조직의 인프라 뒤에서 보호됩니다.

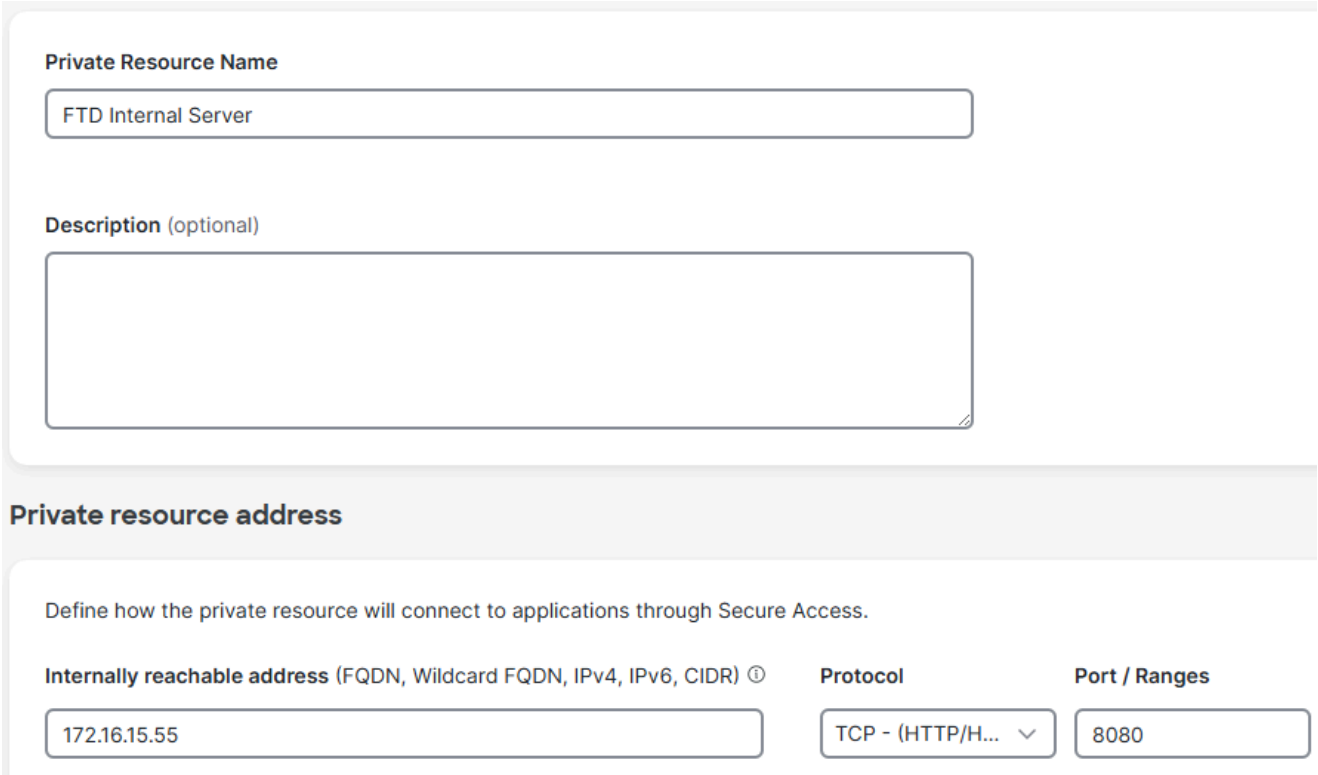
Secure Access에서 Private Resources로 정의하면 ZTA(Zero Trust Access) 또는 VPNaaS(VPN as a Service) 같은 솔루션을 통해 제어된 액세스를 활성화할 수 있습니다. 이를 통해 사용자는 리소스를 인터넷에 직접 노출하지 않고도 ID, 디바이스 상태 및 액세스 정책을 기반으로 내부 시스템에 안전하게 연결할 수 있습니다.

탐색 **Resources > Private Resources>** 클릭Add합니다.



홍보

- ,, **Private Resource Name**Internally reachable address,Protocol을 지정합니다Port/Ranges. 포트 및 프로토콜을 지정하고 필요에 따라 개인 리소스를 추가합니다.
- 요구 사항에 따라 원하는Connection Method연결(예: 제로 트러스트 연결 및/또는 VPN 연결)을 선택합니다
- 클릭 Save



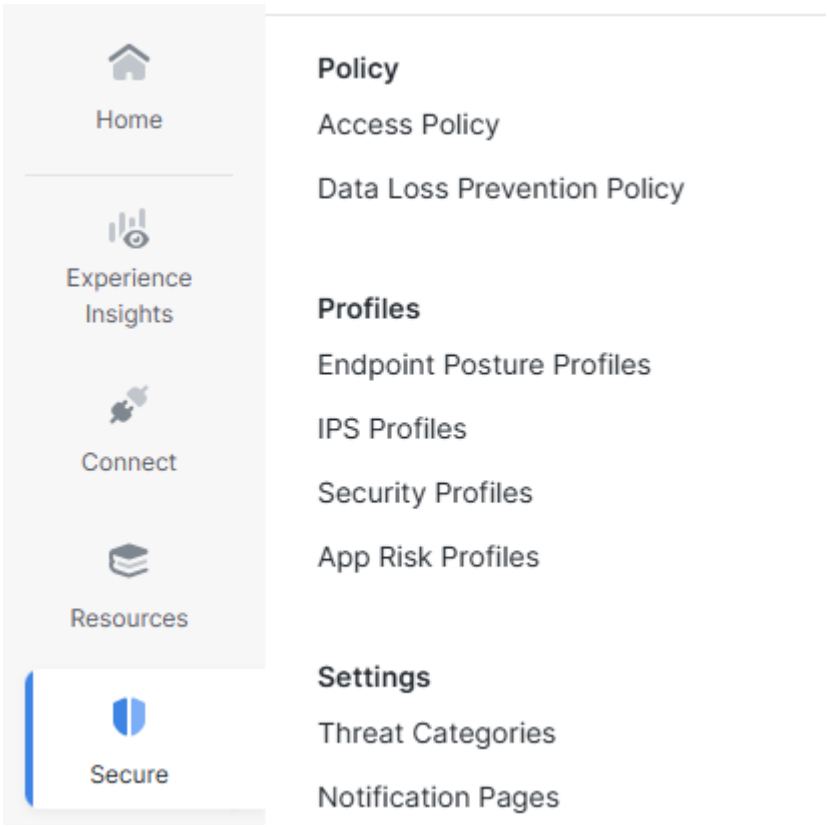
프라이빗 리소스

액세스 정책 규칙 생성

비공개 액세스 규칙은 사용자가 공개적으로 액세스할 수 없는 내부 리소스 및 애플리케이션에 안전하게 연결하는 방법을 정의합니다.

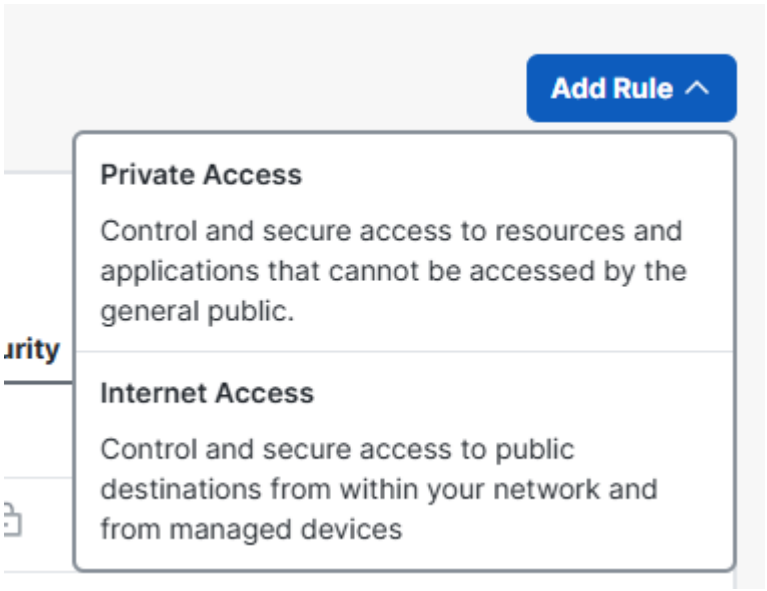
이러한 규칙은 사용자 ID, 그룹 멤버십, 디바이스 상태, 위치 또는 기타 정책 조건과 같은 요소를 기반으로 특정 프라이빗 리소스에 액세스할 수 있는 사용자를 제어하여 보안을 강화합니다. 이렇게 하면 민감한 내부 시스템이 일반 공용 액세스로부터 보호되는 동시에 ZTA 또는 VPNaaS를 통해 인증된 사용자가 안전하게 사용할 수 있습니다.

로 이동합니다 Secure>Access Policy



ACP

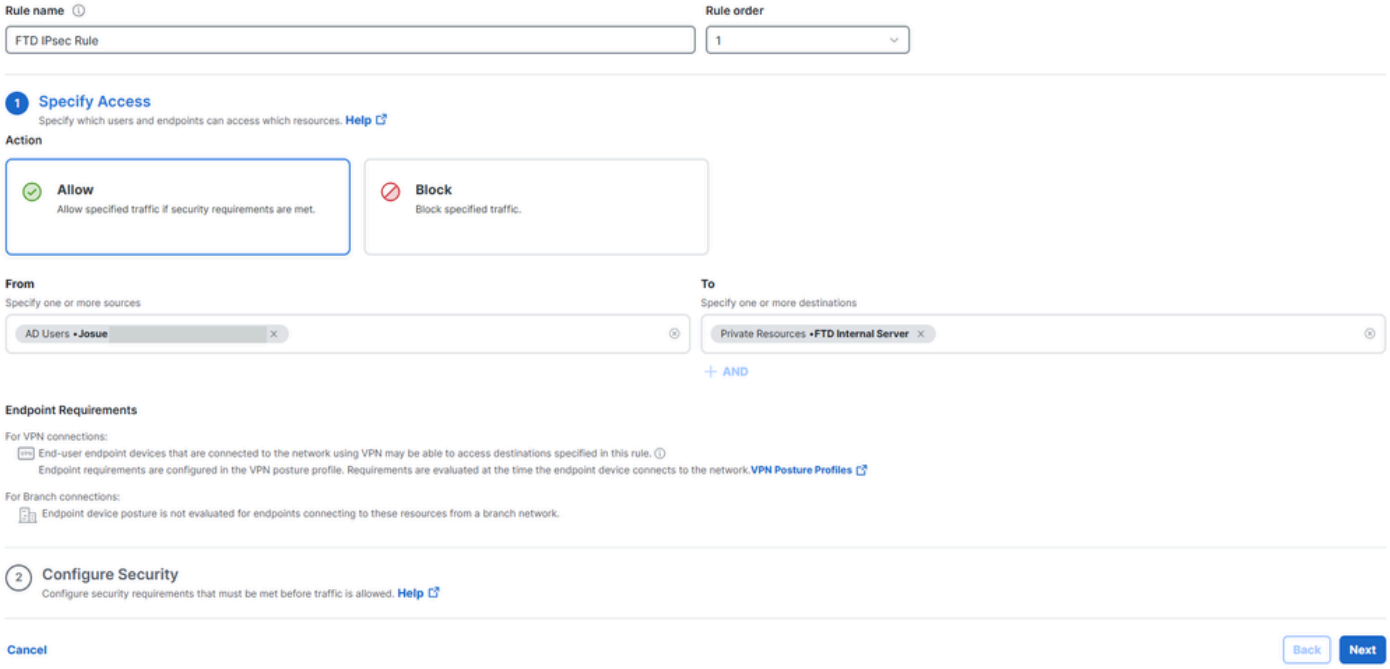
- 클릭 Add Rule
  - 클릭 Private Access



ACP 추가

- 클릭하여Rule Name이름을 지정합니다.
- 이 트래픽Action을 허용하려면Allow을 클릭합니다.
- On(From켜기)을 클릭하고 통합 권한이 있는 사용자를 지정합니다

- 을 클릭하고To이 규칙을 기반으로 해당 사용자가 갖는 액세스 권한을 지정합니다
- 을Next클릭한 다음Save페이지에서



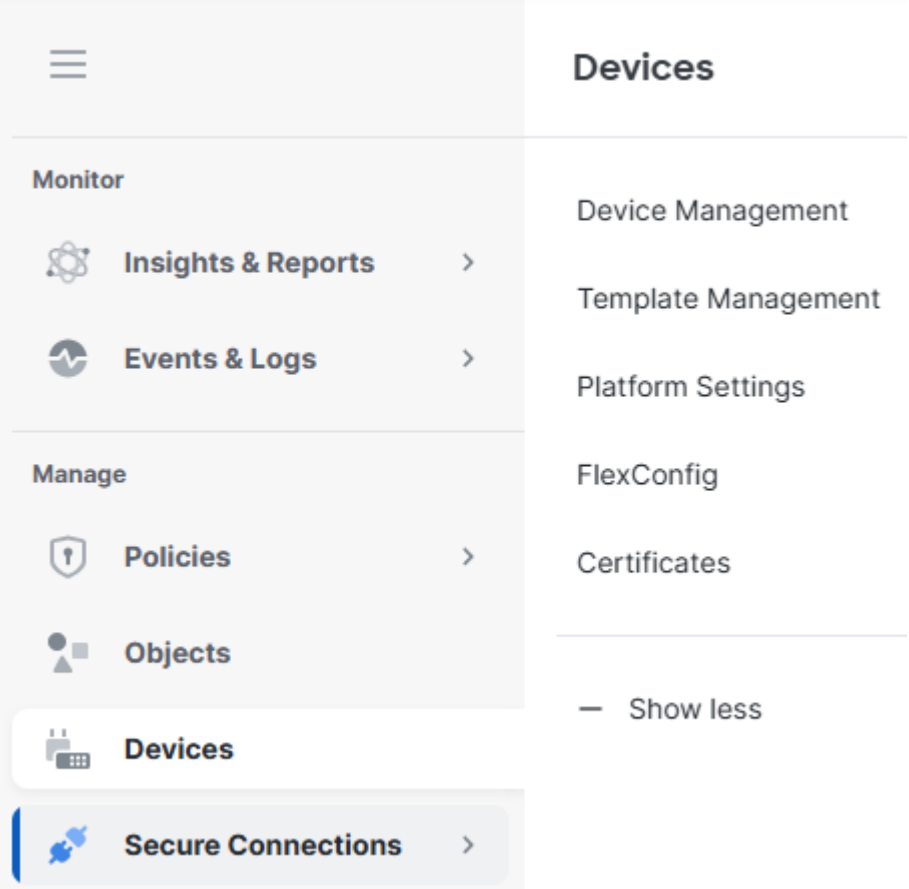
ACP 구성

FTD(Secure Firewall Threat Defense) 구성

가상 터널 인터페이스 컨피그레이션

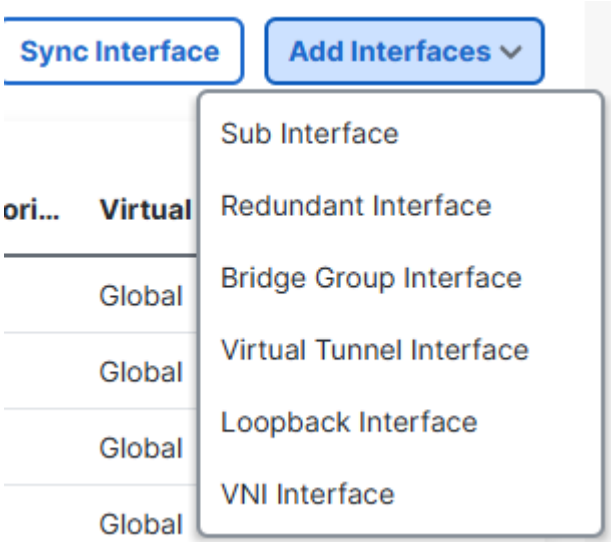
FTD의 VTI(Virtual Tunnel Interface)는 경로 기반 IPsec VPN 터널을 구성하는 데 사용되는 논리적 레이어 3 인터페이스입니다.

1.Devices>(으)로 이동합니다Device Management.



FTD 디바이스

- FTD Device(FTD 디바이스)를 클릭하고 Interfaces
  - 클릭 Add Interfaces
  - 클릭 Virtual Tunnel Interface
  - 기본 Secure Access Hub와 보조 Secure Access Hub용 가상 터널 인터페이스 2개 생성

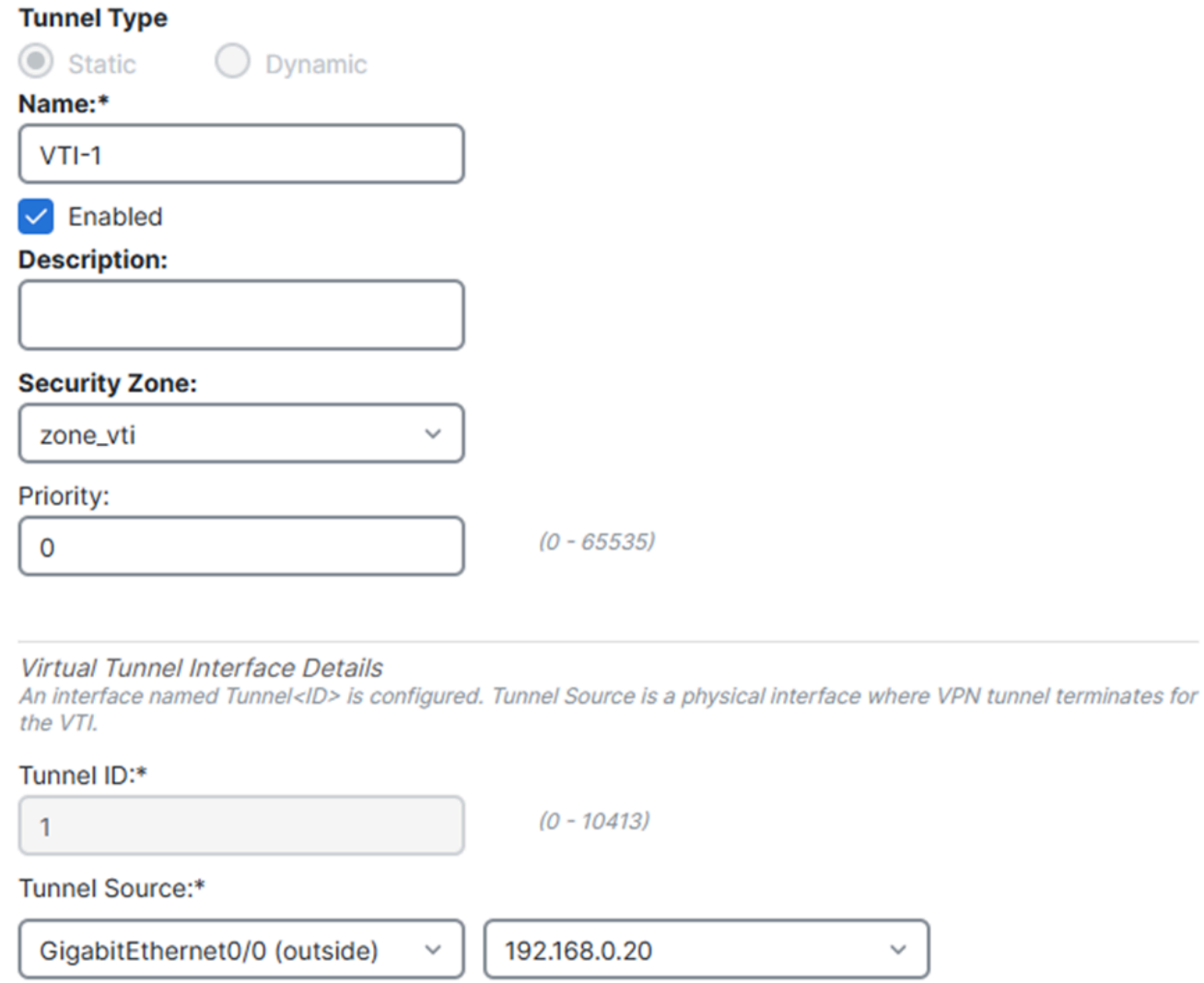


VTI 추가

가상 터널 인터페이스 1:

- 이름을 지정하고 Enable
- 선택 또는 만들기 Security Zone

- 클릭하여Tunnel ID값을 지정합니다.
- 를 클릭하고Tunnel Source터널이 설정될 WAN 인터페이스를 지정합니다
- 클릭IPsec Tunnel Mode, 선택IPv4
- 를 클릭하고IP AddressVTI의 IP 주소를 구성합니다
- 클릭OK

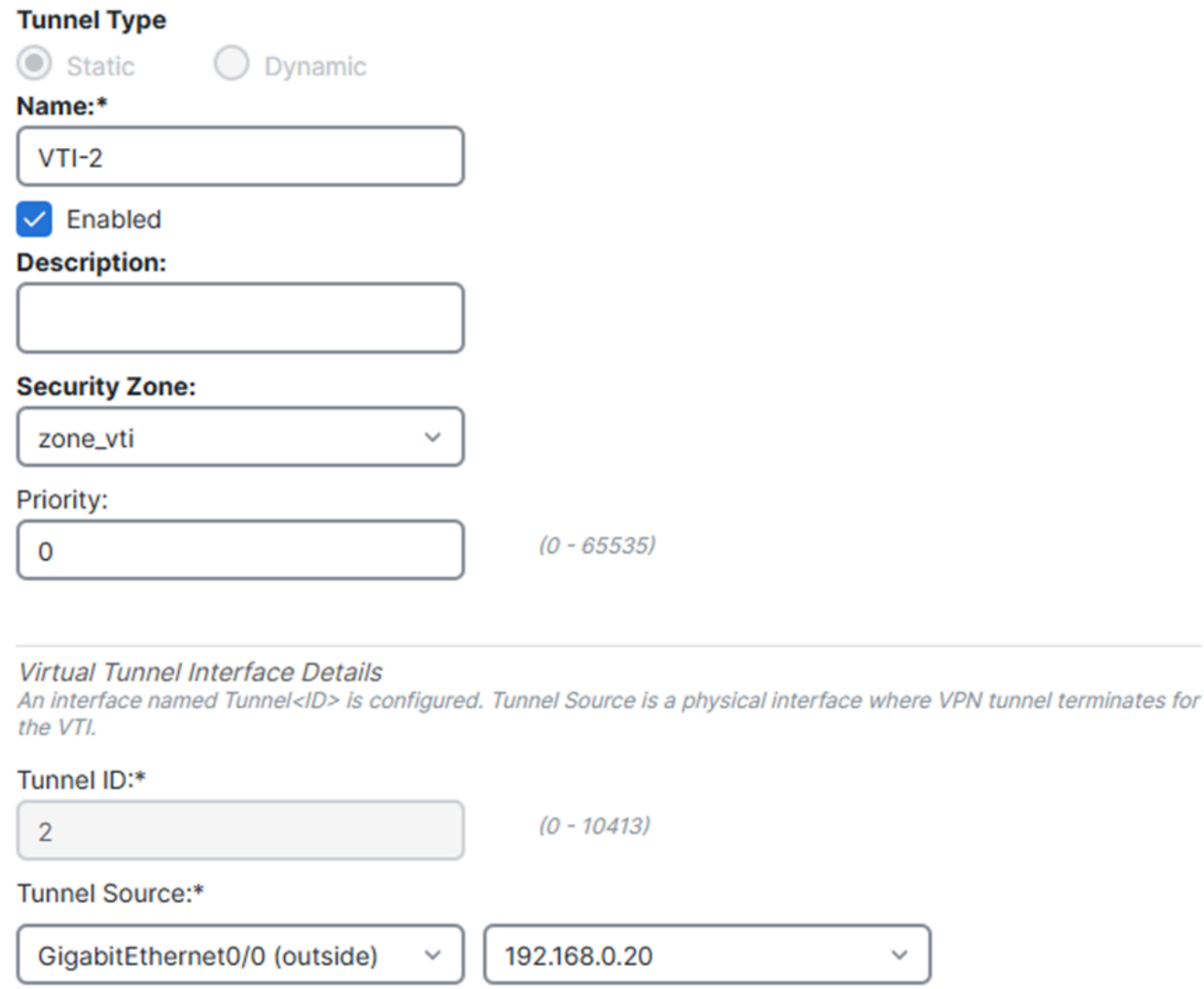


VTI1.1

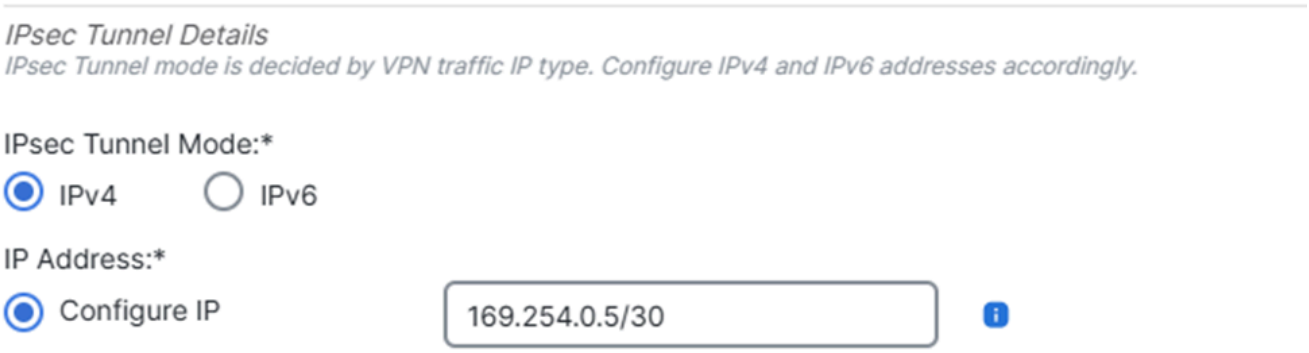
VTI1.2

가상 터널 인터페이스 2:

- 이름을 지정하고 Enable
- 선택 또는 만들기 Security Zone
- 클릭하여Tunnel ID값을 지정합니다.
- 를 클릭하고Tunnel Source터널이 설정될 WAN 인터페이스를 지정합니다
- 클릭IPsec Tunnel Mode, 선택IPv4
- 를 클릭하고IP AddressVTI의 IP 주소를 구성합니다
- 클릭OK

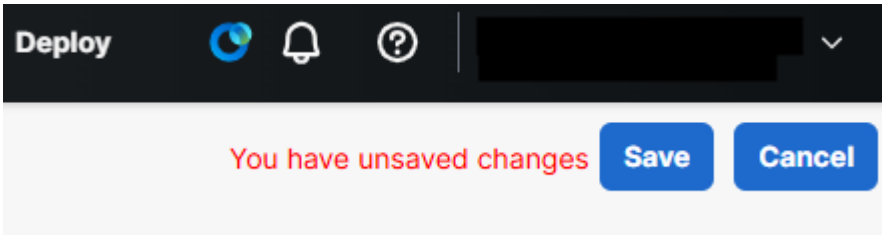


VTI2.1



VTI2.2

- Save(저장)를 클릭합니다.

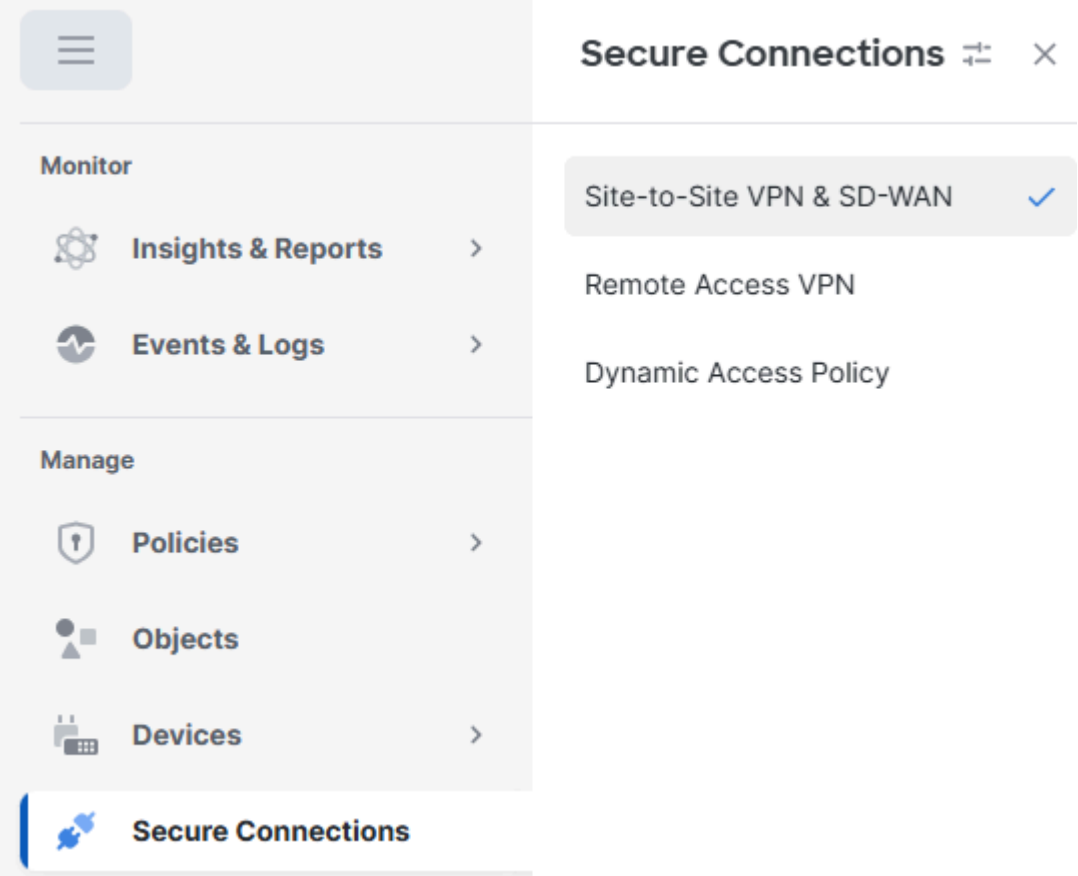


VTI 변경 사항 저장

IPsec 터널 컨피그레이션

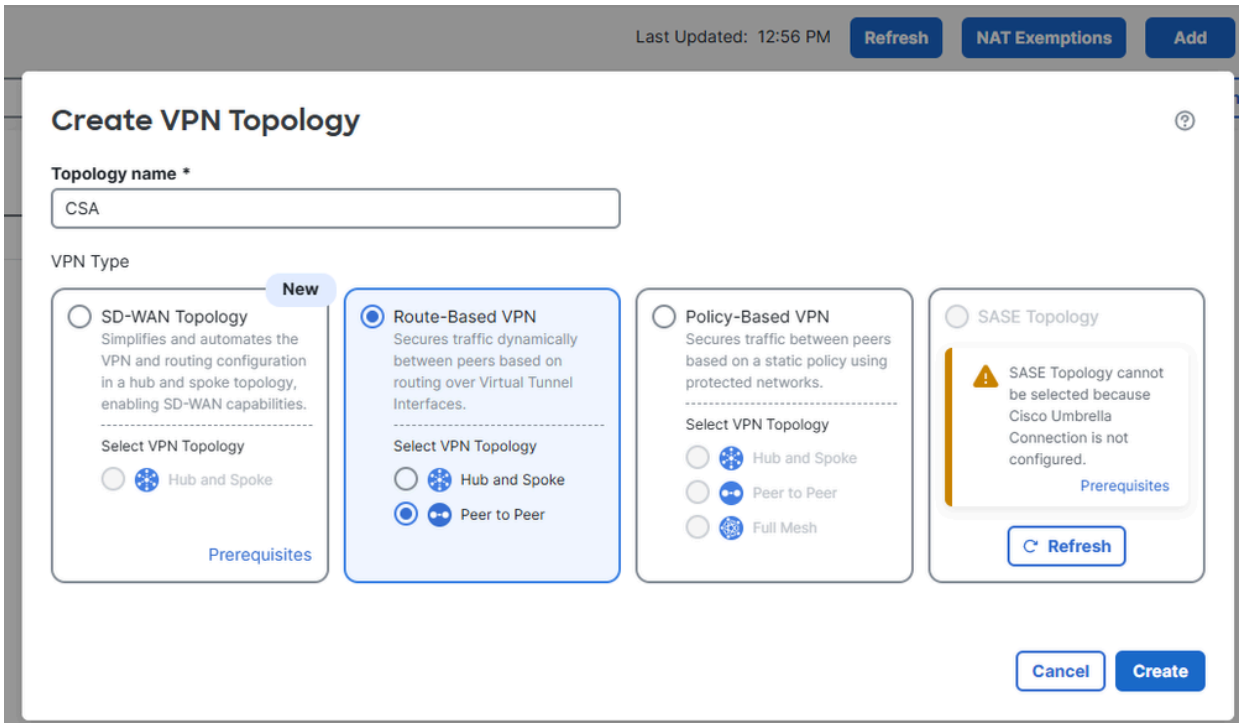
cdFMC 대시보드로 이동합니다.

- 클릭Secure Connection> Site-to-Site VPN & SD-WAN



S2

- 클릭Add
  - 클릭 Route-Based VPN
  - 클릭 Peer to Peer

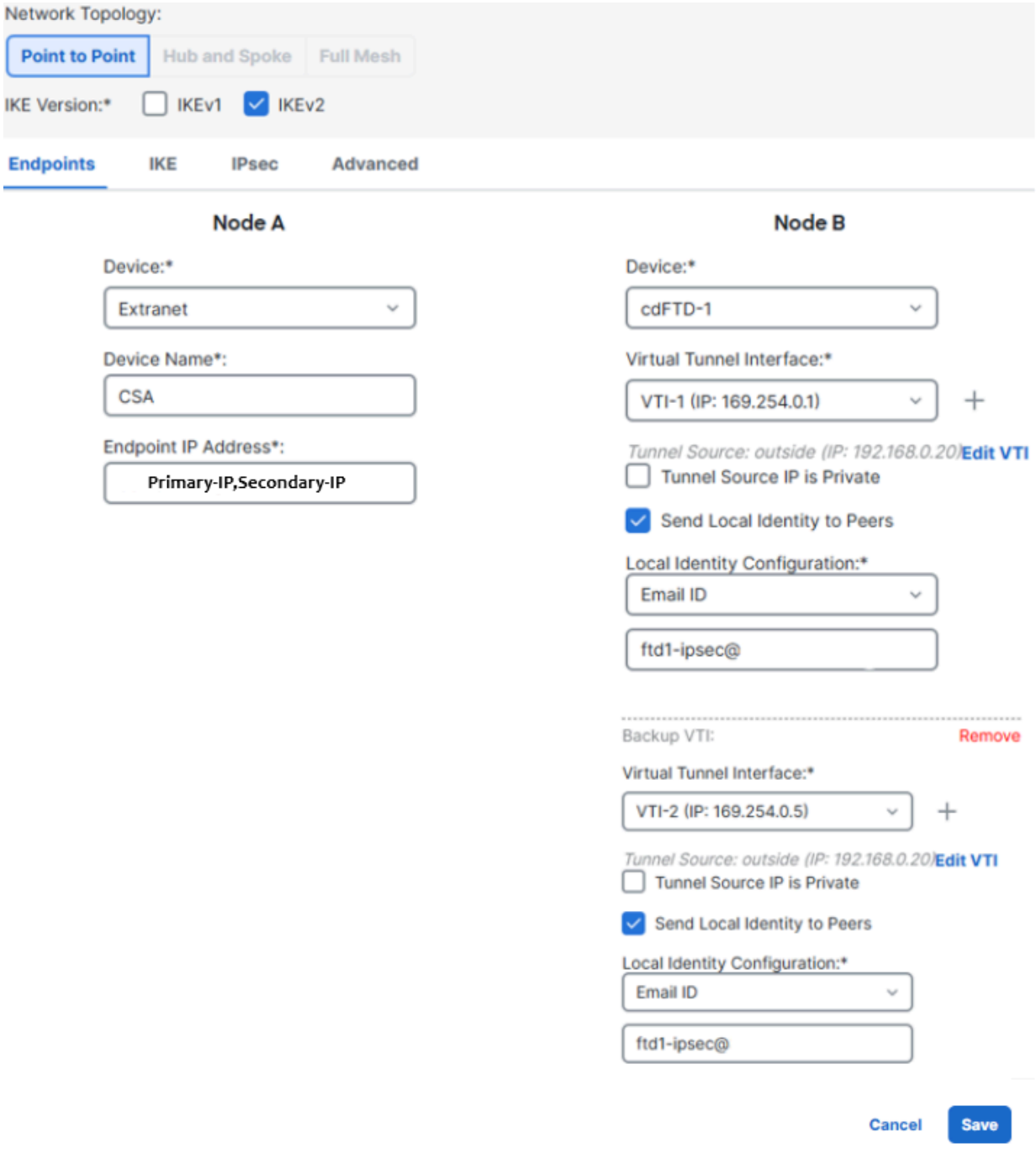


VPN 추가

- Secure Access 컨피그레이션의 5단계에서 기본 및 보조 데이터 센터의 터널 ID 및 IP 주소를

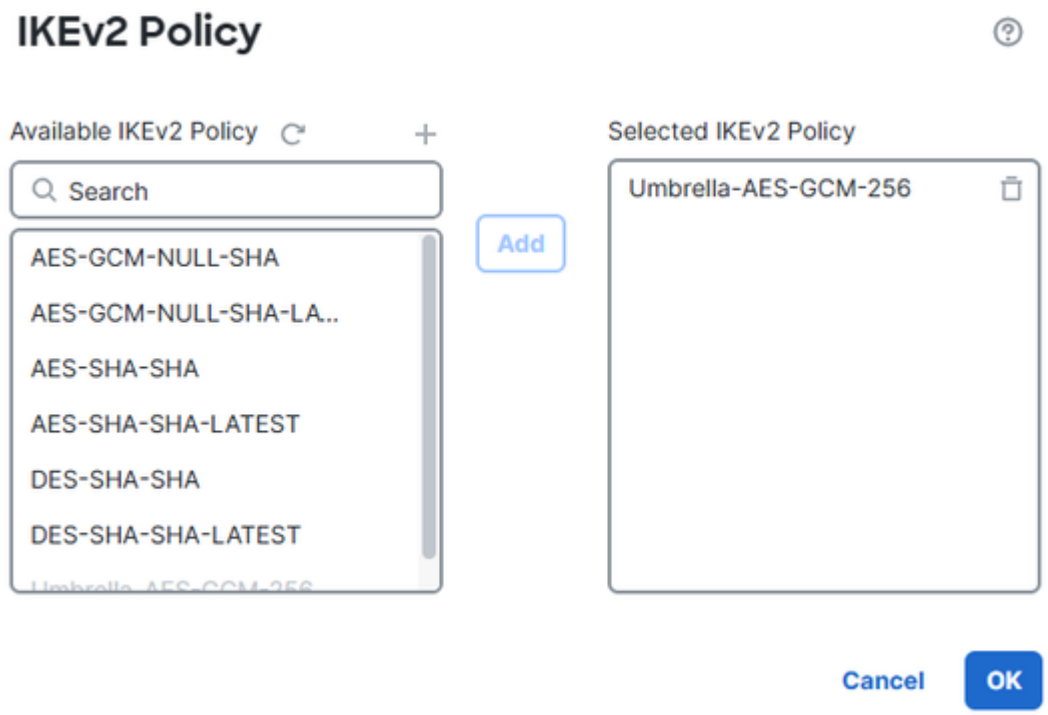
가져옵니다

- 클릭Endpoints
  - 아래에서Node ADeviceonand(켜기)를 클릭하고 Extranet
  - 클릭하여 이름Device Name을 지정합니다
  - 를 클릭하고Enpoint IP AddressesSecure Access(보안 액세스) 아래의 Save Network Tunnel Group Configuration(네트워크 터널 그룹 컨피그레이션 저장)에서 쉼표로 구분된 Secure Access Primary and Secondary IP Addresses(보안 액세스 기본 및 보조 IP 주소)를 입력합니다
    설정)
  - 아래에서Node B를 클릭하고DeviceFTD 디바이스를 선택합니다
  - 을 클릭하고Virtual Tunnel Interface이전 단계에서 생성한 첫 번째 VTI 인터페이스를 선택합니다
  - 옵션을Send Local Identity to PeersEmail ID클릭하고 기본 터널 ID를 선택합니다(Secure Access Configuration(보안 액세스 컨피그레이션) 아래의 "Save Network Tunnel Group Configuration(네트워크 터널 그룹 컨피그레이션 저장)"에서)
  - 클릭 Add Backup VTI
  - 를 클릭하고Virtual Tunnel Interface이전 단계에서 생성한 두 번째 VTI 인터페이스를 선택합니다
  - onoptionSend Local Identity to Peers을 클릭하고Email ID, 보조 터널 ID를 선택합니다(Secure Access Configuration 아래의 "Save Network Tunnel Group Configuration"에서).
  - Save(저장)를 클릭합니다.



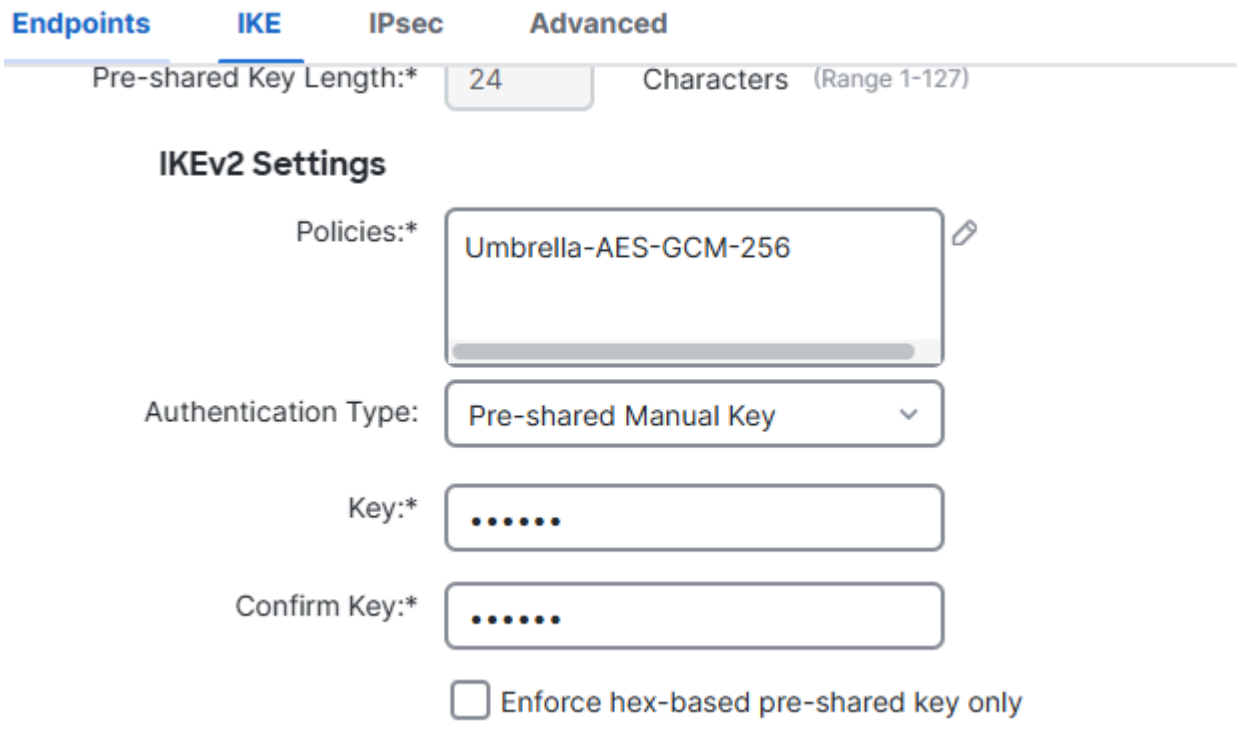
FTD VTI 컨피그레이션

- 클릭IKE
  - 클릭 **IKEv2 Settings >** Policies
  - Umbrella-AES-GCM-256옵션 선택
  - 클릭 OK



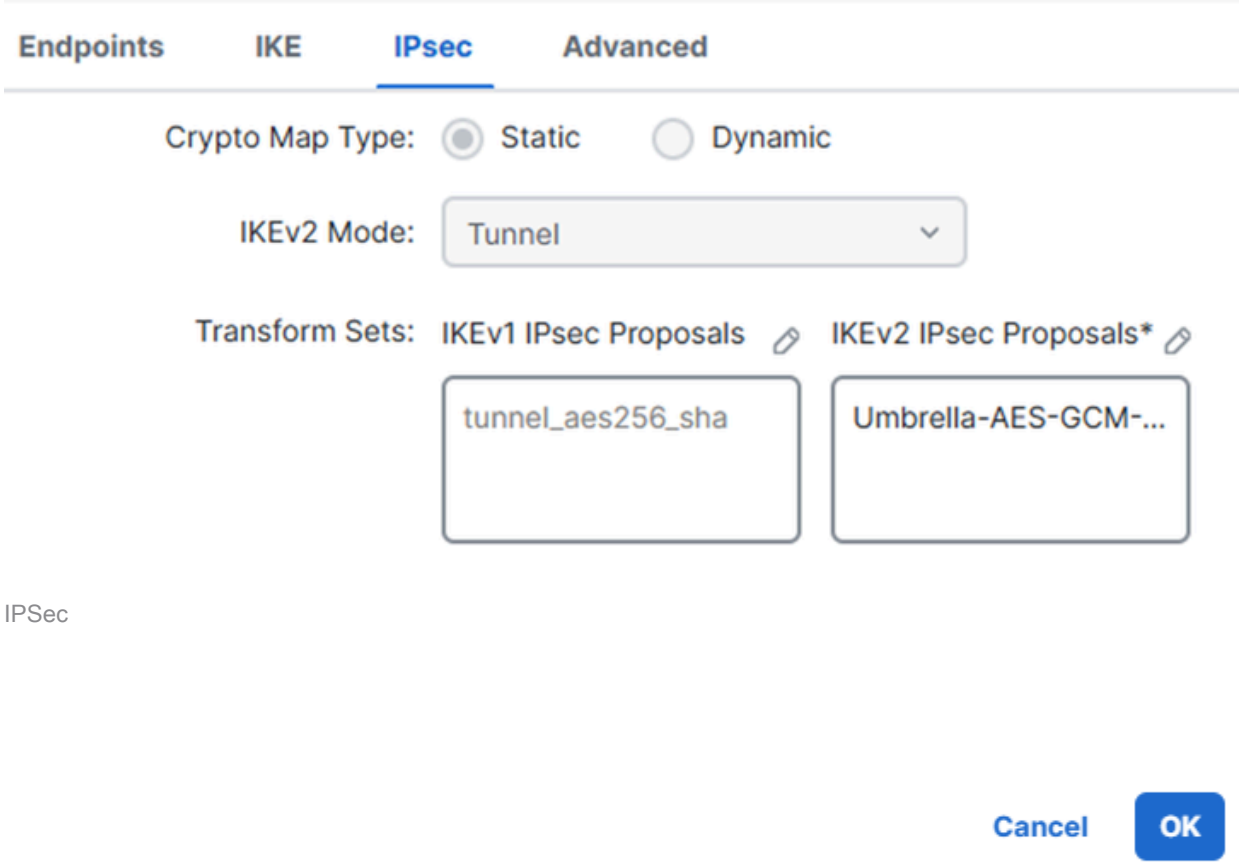
IKEv2 정책

- 을 클릭하고Authentication Type선택한Pre Shared Manual Key다음 Secure Access(보안 액세스)에 구성된 PSK(암호)를 입력합니다.



IKE

- 클릭 IPSEC
  - 클릭 IKEv2 Proposals
  - 선택 Umbrella-AES-GCM-256
  - 클릭 OK



IPSec

IKEv2 제안서 저장

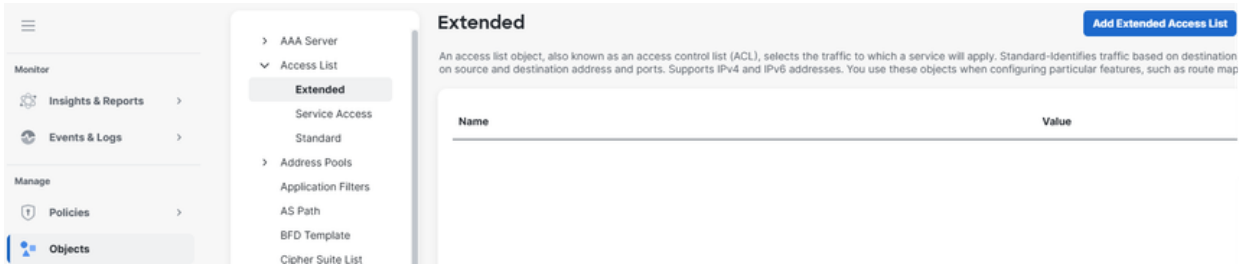
FTD 라우팅 컨피그레이션

PBR(Policy-Based Routing)을 사용하면 대상 IP 주소뿐 아니라 기준을 기반으로 트래픽 포워딩을 제어할 수 있습니다. PBR은 라우팅 테이블에만 의존하는 대신 소스, 애플리케이션, 프로토콜, 포트 또는 기타 정의된 정책을 기반으로 트래픽을 라우팅할 수 있습니다.

이를 통해 조직은 특정 트래픽 또는 우선 순위가 높은 트래픽을 기본 링크(예: 고대역폭 또는 직접 인터넷 링크)를 통해 조정하고, 성능을 최적화하며, VPN 터널을 통해 모든 트래픽을 전송하지 않고 선택한 애플리케이션을 안전하게 분리할 수 있습니다.

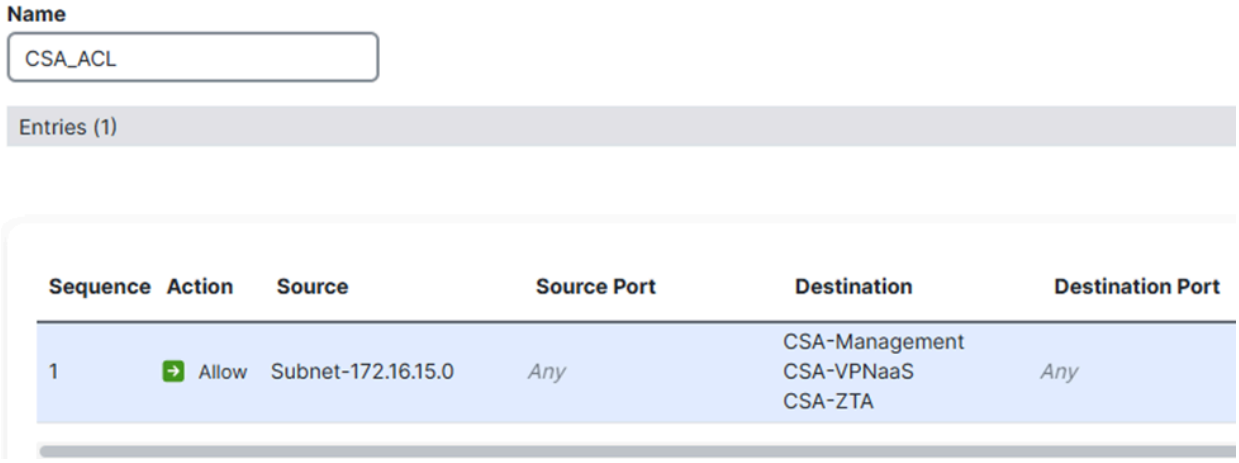
정책 기반 라우팅

- 로 이동합니다Objects
  - 클릭 Access List
  - 클릭 Extended
  - 클릭Add Extended Access List



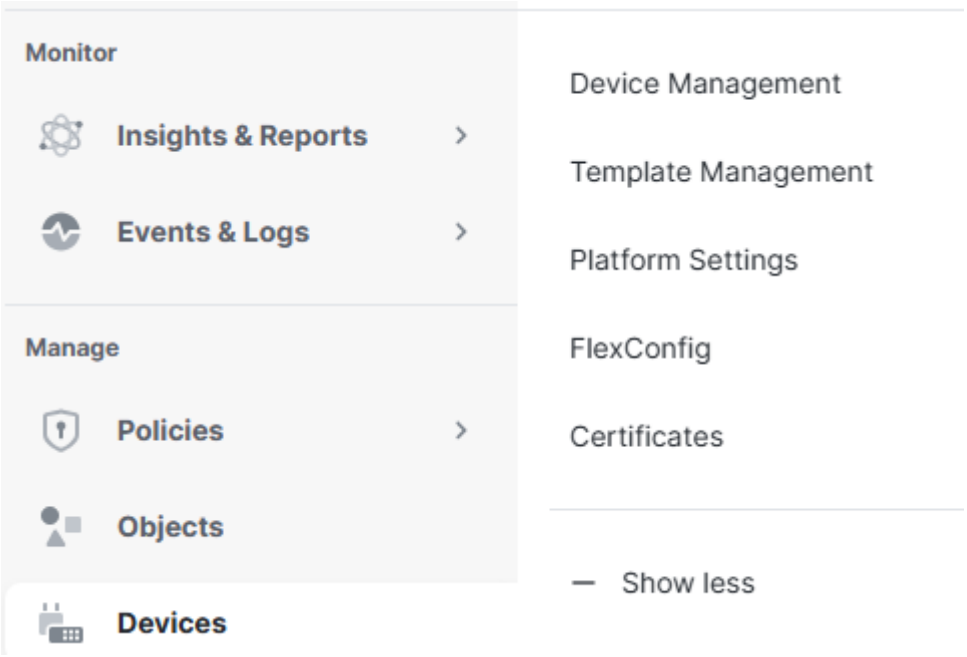
ACL 추가

터널을 통해 전송할 FTD(예: 172.16.15.0/24)로 보호되는 소스 네트워크와 일치하는 확장 ACL(Access Control List)을 생성합니다. 대상의 경우 ZTA에서 사용하는 네트워크(CGNAT 범위)와 VPNaaS에서 사용하는 네트워크를 추가합니다(Virtual Private Network IP Pool 확인).



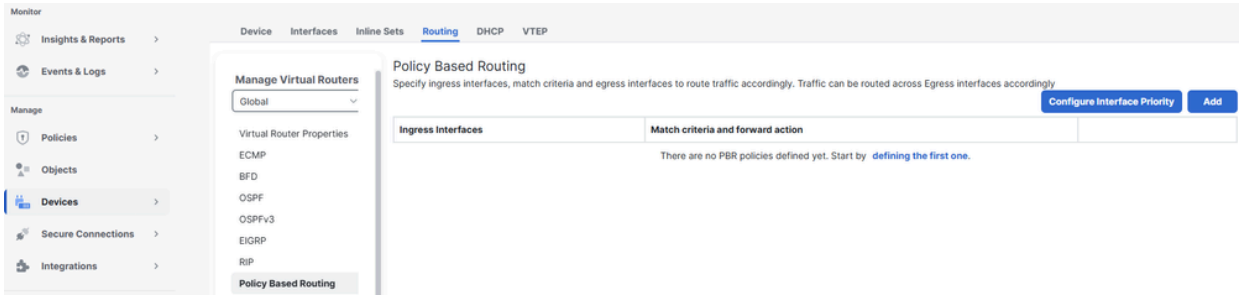
ACL

- 클릭Devices> Device Management



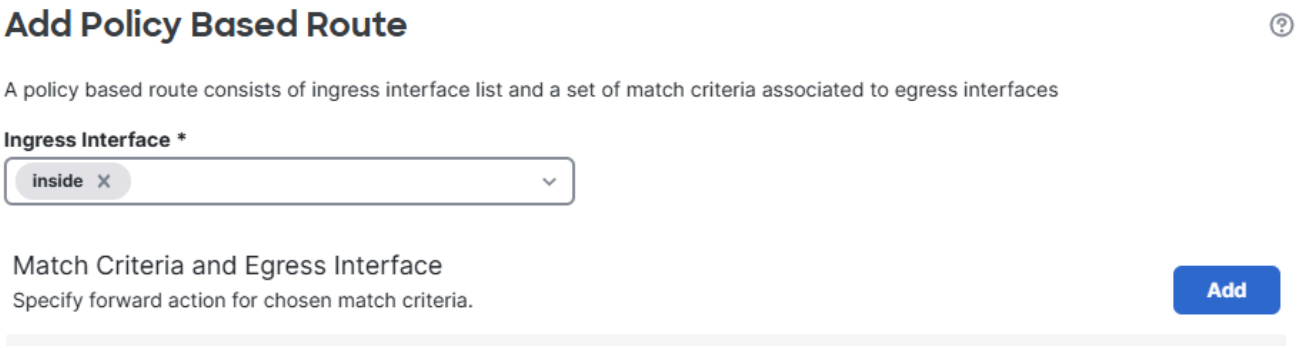
디바이스

- FTD를 클릭합니다
  - 클릭Routing
  - 클릭 Policy Based Routing
  - 클릭 Add



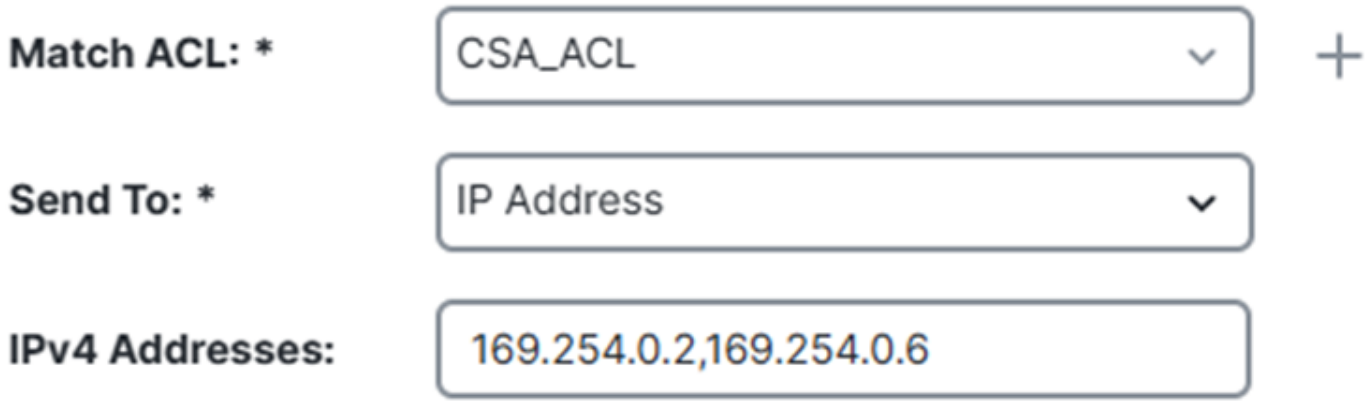
PBR 추가

- 를 클릭하고Ingress Interface내부 네트워크의 트래픽이 들어오는 인그레스 인터페이스를 선택합니다
- Match Criteria and Egress Interface(일치 기준 및 이그레스 인터페이스)에서 Add



인그레스 인터페이스

- 를 클릭하고Match ACL이전에 생성한 확장 ACL을 선택합니다.
- 클릭 Send To and select IP Address
- 를 클릭하고IPv4 AddressesFTD에서 이전에 구성된 VTI 인터페이스 서브넷(169.254.0.2 및 169.254.0.6) 내에서 IP 주소를 다음 홉으로 설정합니다
- 클릭 Save



정책 기반 컨피그레이션

PBR 저장

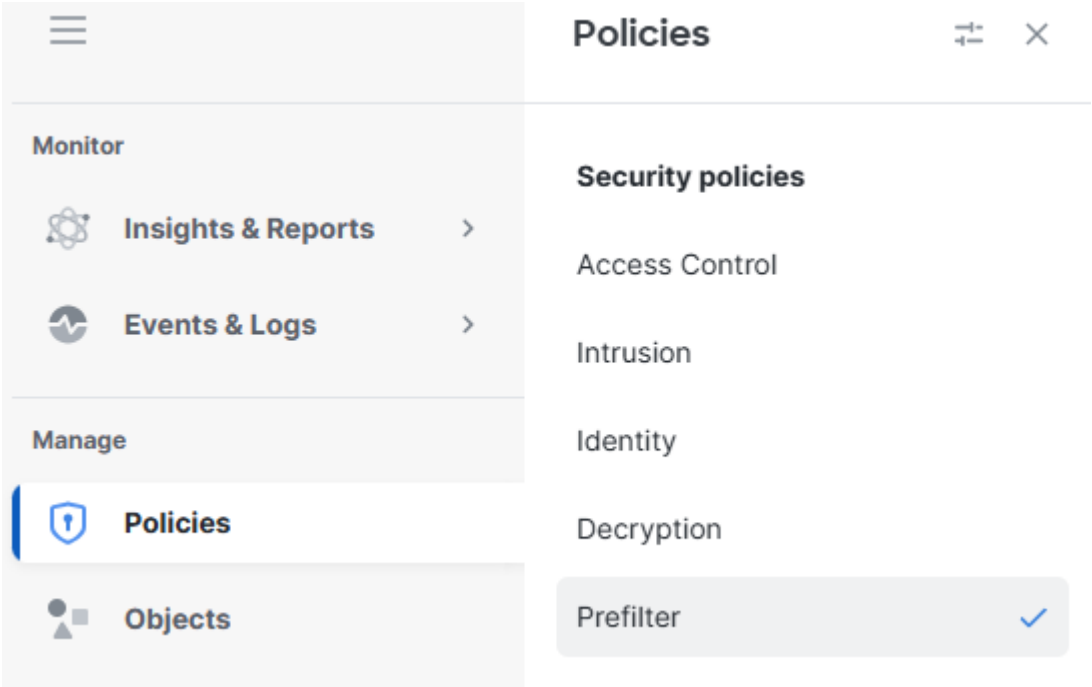
옵션이 아닌Send To >IP Address옵션을 선택해야 합니다Egress Interface.

액세스 정책 컨피그레이션

Cisco FTD(Firepower Threat Defense)에서 트래픽을 허용하고 프라이빗 리소스에 대한 액세스를 활성화하려면 트래픽이 먼저 Prefiltering이라고 하는 액세스 제어의 초기 단계를 통과해야 합니다.

사전 필터링은 심층 검사가 발생하기 전에 처리되며 간단하고 빠르게 설계되었습니다. 기본 외부 헤더 기준(예: 소스 및 목적지 IP 주소 및 포트)을 사용하여 트래픽을 신속하게 허용, 차단 또는 우회하도록 트래픽을 평가합니다. 이 단계에서 트래픽이 허용되면 심층 패킷 검사 또는 침입 정책과 같은 리소스 집약적인 검사를 건너뛰어 성능을 향상하는 동시에 보안 제어를 유지할 수 있습니다.

- 탐색Policies> Prefilter

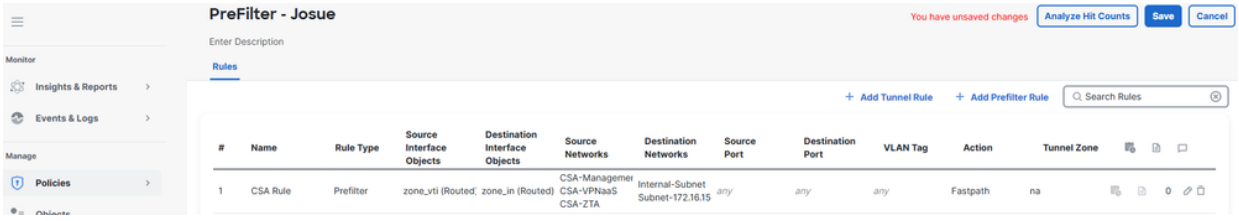


사전 필터

- Edit the Prefilter policy being used by your Access Policy(액세스 정책에서 사용 중인 사전 필터 정책 수정)를 클릭합니다

사전 필터 클릭

- 클릭 Add Tunnel Rule
  - VPNaaS 네트워크 및/또는 ZTA 서브넷에서 프라이빗 리소스로 트래픽을 추가하고 허용합니다.
  - 클릭Save



규칙 저장

이때 FTD의 컨피그레이션이 완료되고 확인되면 구축을 계속할 수 있습니다. 구축 후에는 IPsec 터널이 정상적으로 작동하여 프라이빗 리소스에 대한 보안 연결이 설정되었음을 확인합니다.

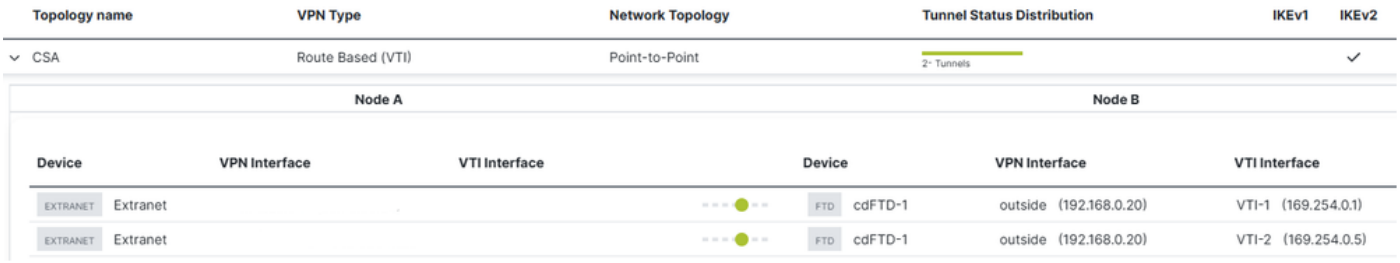
다음을 확인합니다.

FTD에서 확인

FTD의 터널 상태

작동 또는 중단 여부를 포함하여 터널의 현재 상태를 볼 수 있습니다. 이렇게 하면 IPsec 터널이 올바르게 설정되었는지 확인할 수 있습니다.

- Secure Connections(보안 연결)를 클릭합니다.
- Site-to-Site VPN & SD-WAN을 클릭합니다.
- Topology Name(토폴로지 이름)을 클릭합니다.



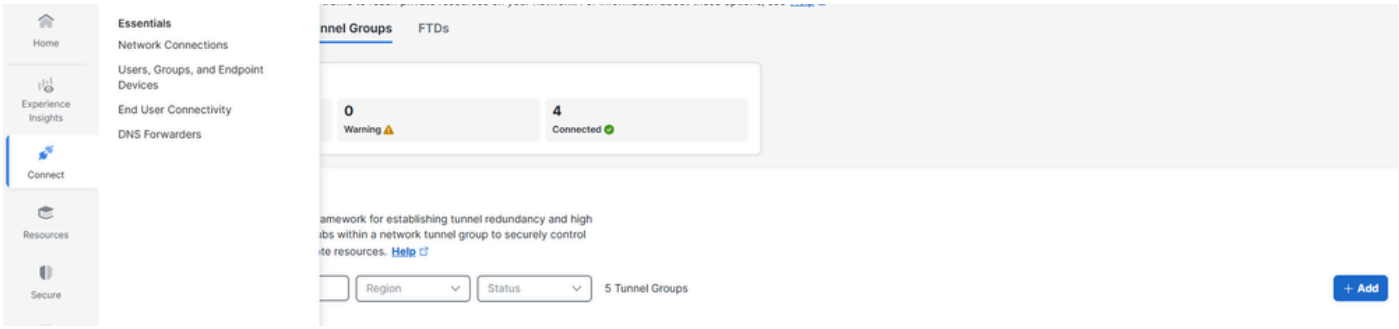
FTD 터널 상태

보안 액세스에서 확인

보안 액세스의 터널 상태

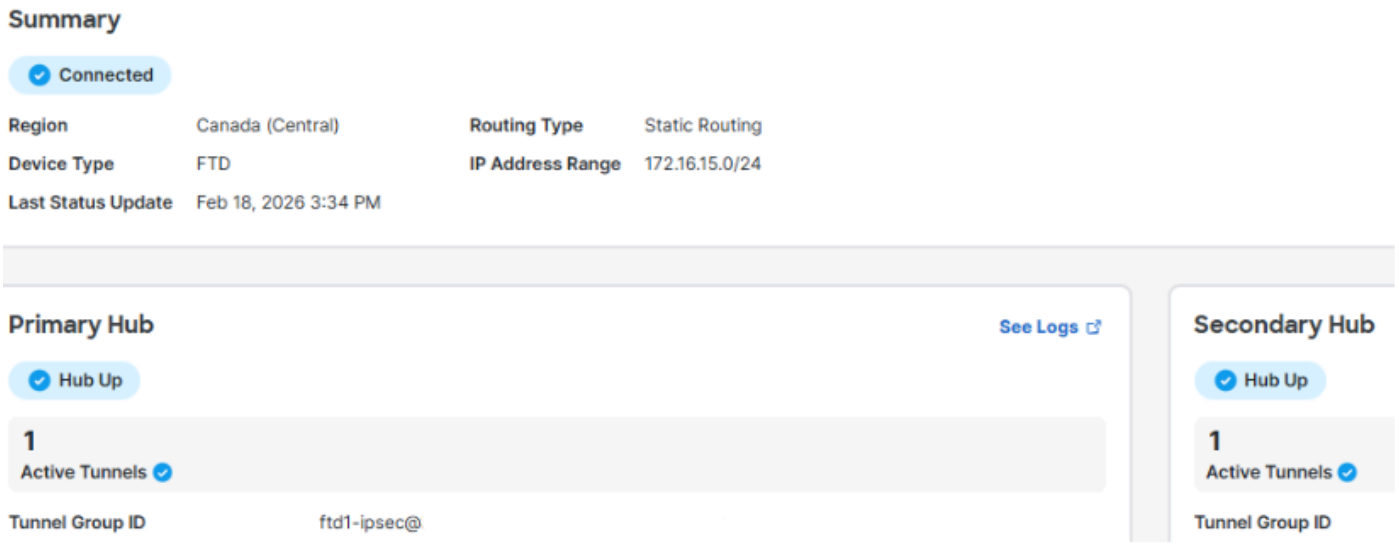
터널의 현재 상태(연결 끊김, 경고 또는 연결됨)를 볼 수 있습니다. 이렇게 하면 IPsec 터널이 올바르게 설정되었는지 확인할 수 있습니다.

- Connect(연결) > Network Connections(네트워크 연결)를 클릭합니다.
- Network Tunnel Groups(네트워크 터널 그룹)를 클릭합니다.



NTG 확인

- Network Tunnel Group(네트워크 터널 그룹)을 클릭합니다

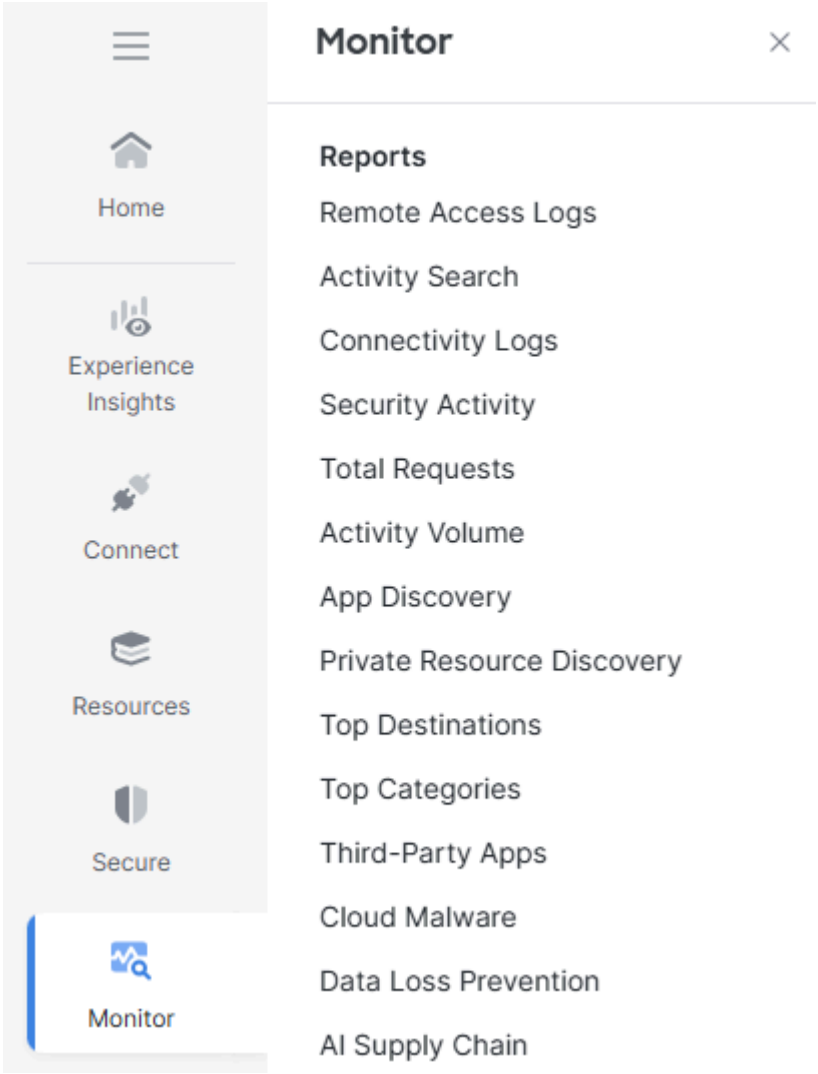


CSA 터널 상태

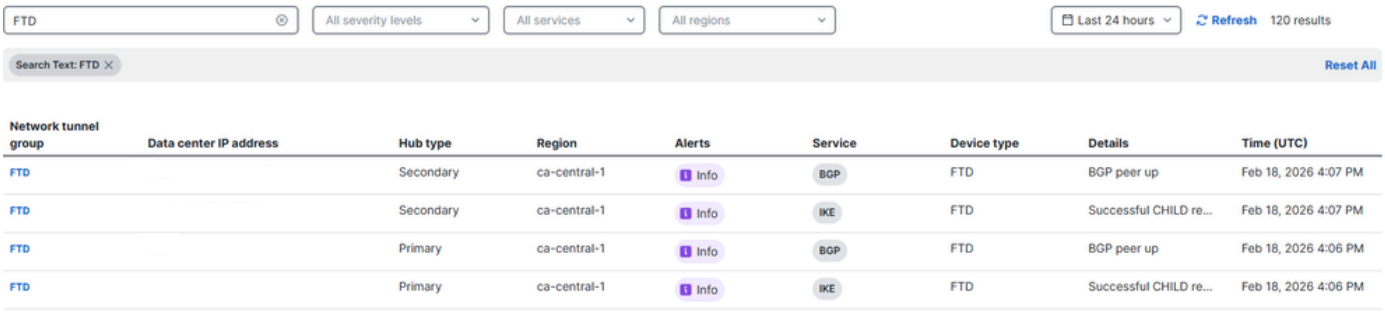
Secure Access의 이벤트

터널 이벤트를 보고 IPsec 터널의 상태가 작동 및 안정적인지 확인할 수 있습니다.

Monitor(모니터) > Network Connectivity(네트워크 연결)를 클릭합니다.

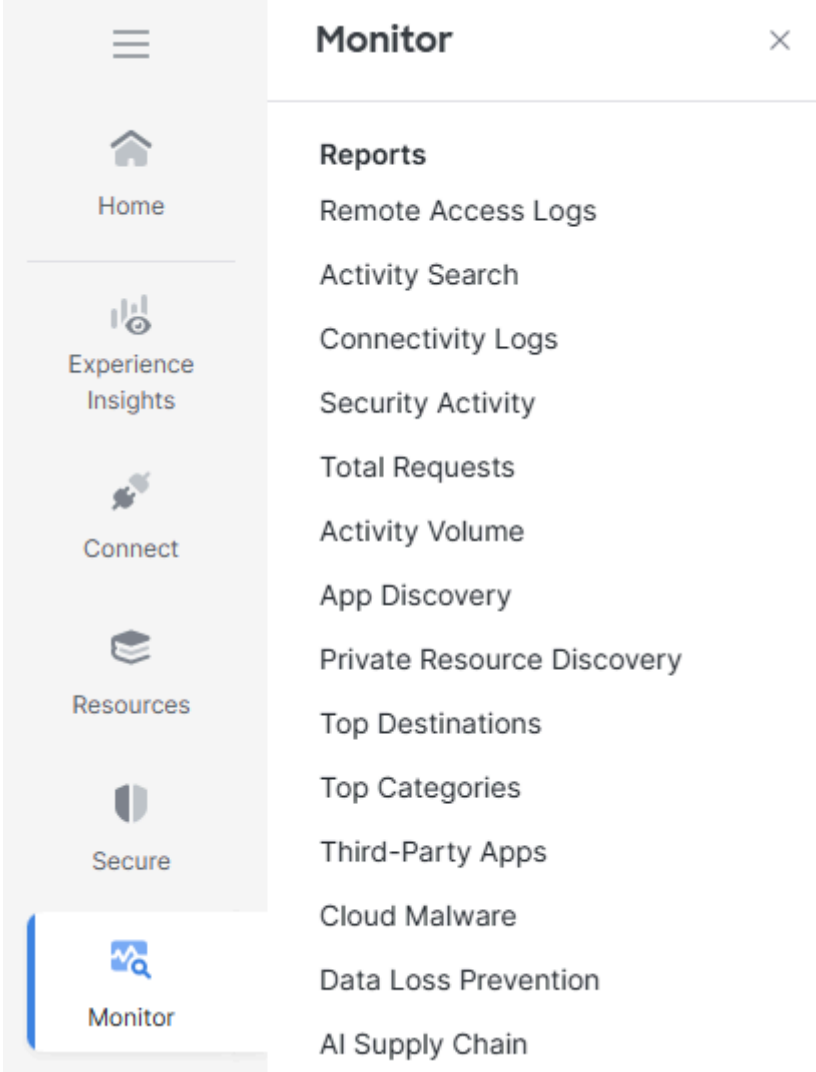


연결 로그 모니터링



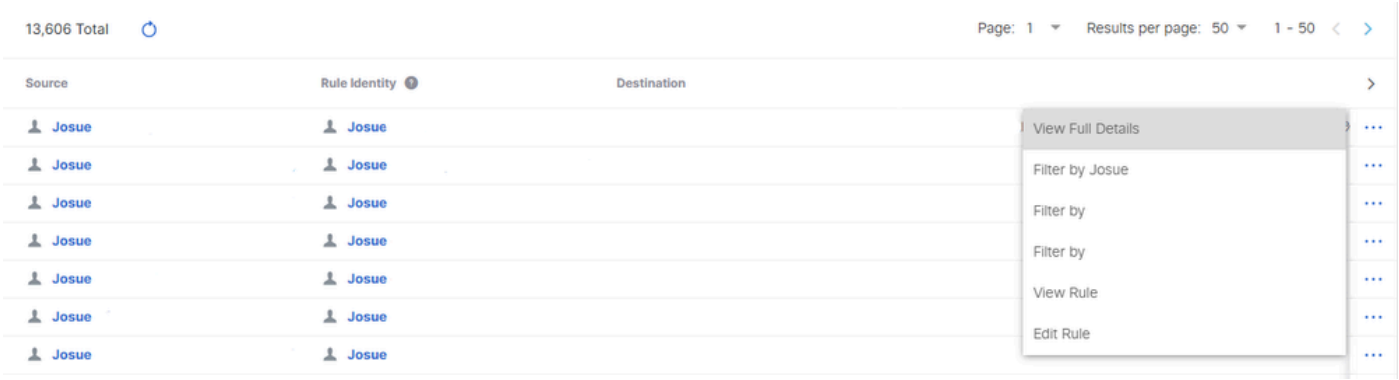
연결 로그

Monitor > Activity Search에서 이동합니다.

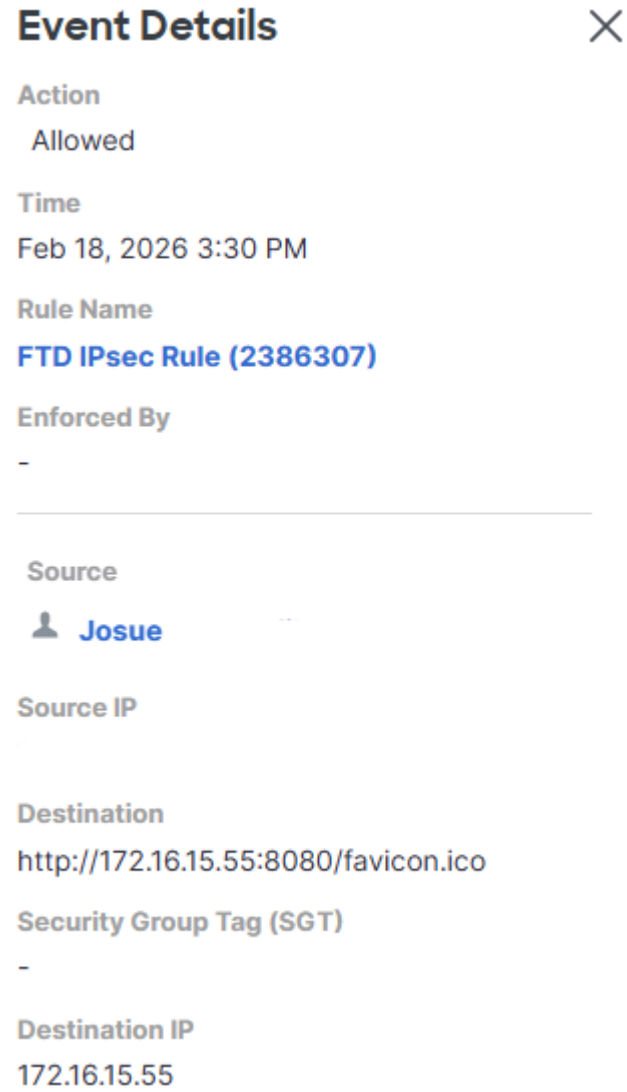


연결 로그 모니터링

관련 이벤트에서 View Full Details(전체 세부사항 보기)를 클릭합니다.



전체 세부사항



활동 검색

관련 정보

- Cisco 기술 지원 및 다운로드
- Cisco Secure Firewall Management Center Device Configuration Guide, 7.7

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.