

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

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[보안 액세스 컨피그레이션](#)

[네트워크 터널 그룹 컨피그레이션](#)

[보안 액세스 라우팅](#)

[BGP\(Dynamic Routing\)](#)

[네트워크 터널 그룹 컨피그레이션 저장](#)

[프라이빗 리소스 생성](#)

[액세스 정책 규칙 생성](#)

[FTD\(Secure Firewall Threat Defense\) 구성](#)

[가상 터널 인터페이스 컨피그레이션](#)

[IPsec 터널 컨피그레이션](#)

[FTD 라우팅 컨피그레이션](#)

[BGP\(Dynamic Routing\)](#)

[액세스 정책 컨피그레이션](#)

[다음을 확인합니다.](#)

[FTD에서 확인](#)

[FTD의 터널 상태](#)

[보안 액세스의 터널 상태](#)

[Secure Access의 이벤트](#)

[관련 정보](#)

소개

이 문서에서는 IPsec을 통한 FTD로 Secure Access를 구성하여 동적 라우팅을 통한 Secure Private Access를 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
- 동적 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 BGP를 통한 동적 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

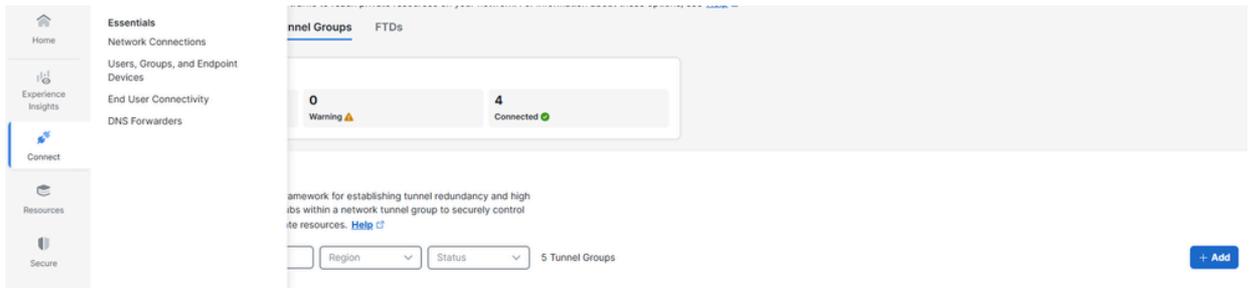
1. [Secure Access](#)의 관리자 패널로 [이동합니다](#).



CSA 대시보드

2. 네트워크 터널 그룹을 추가합니다.

- 클릭 **Connect > Network Connections**
 - 아래에서 **Network Tunnel Groups >**를 클릭합니다. Add



NTG 확인

3. General Settings 구성

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

- General Settings
- Tunnel ID and Passphrase
- Routing
- Data for Tunnel Setup

General Settings

Give your network tunnel group a good meaningful name, choose type this tunnel group will use.

Tunnel Group Name

FTD

Region

Canada (Central)

Device Type

FTD

일반 설정

4. Tunnel ID 및 Passphrase. 이 ID는 FTD 구성에 필요하므로 중요합니다

- [클릭](#) Next

- ✓ General Settings
- ✓ Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

Tunnel ID and Passphrase

Configure the tunnel ID and pa

Tunnel ID Format

Email IP Address

Tunnel ID

ftd1-ipsec

Passphrase

.....

The passphrase must be between special characters.

Confirm Passphrase

.....

ID 및 PSK

5. 동적 라우팅을 구성합니다.

보안 액세스 라우팅

BGP(Dynamic Routing)

- Secure Access에서 BGP 피어를 구성할 때 FTD의 BGP AS(Autonomous System) 번호를 지정합니다.
- [클릭](#) Routing > Dynamic routing
 - [클릭](#) 하고 Device AS Number FTDs BGP ASN을 추가합니다
 - [확인란](#)을 Block default route advertisement 선택합니다
 - [클릭](#) Save

Dynamic routing

Use this option when you have a BGP peer for your on-premise router.

Device AS Number

64513

Advanced Settings

Multihop BGP

Select this option to enable the ability for BGP peers to establish a connection (hop) when not directly connected.

Multi-region backhaul

Use Secure Access as the network backbone and prioritize regions based on origin.

Block default route advertisement

Select to block the advertisement of the default route.

CSA BGP 컨피그레이션



참고: Secure Access에서 광고하는 경로는 원래 AS 경로 앞에 다음을 포함합니다. 기본 터널의 경우 1, 보조 터널의 경우 2. 다중 영역 백홀 시나리오가 지원됩니다. 자세한 내용을 보려면 를 클릭하십시오.

네트워크 터널 그룹 컨피그레이션 저장

FTD 컨피그레이션에 필요한 터널 설정 데이터를 다운로드하여 저장합니다.

- [클릭](#) Download CSV
- [클릭](#) Done

Data for Tunnel Setup
Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID: ftd1-ipsec@

Primary Data Center IP Address:

Secondary Tunnel ID: ftd1-ipsec@

Secondary Data Center IP Address:

Passphrase:

[Download CSV](#)

[Done](#)

NTG 데이터

Summary

✖ Disconnected

Region	Canada (Central)	Routing Type	Dynamic Routing (BGP)
Device Type	FTD	Device BGP AS	64513
Last Status Update	Feb 18, 2026 3:58 PM	Peer (Secure Access) BGP AS	64512
		BGP Peer (Secure Access) IP Addresses	169.254.0.9, 169.254.0.5, 2a04:e4c4:b:c723::b67:0000/120
		Multihop BGP Addresses	—
		Multihop TTL	—

BGP 설정



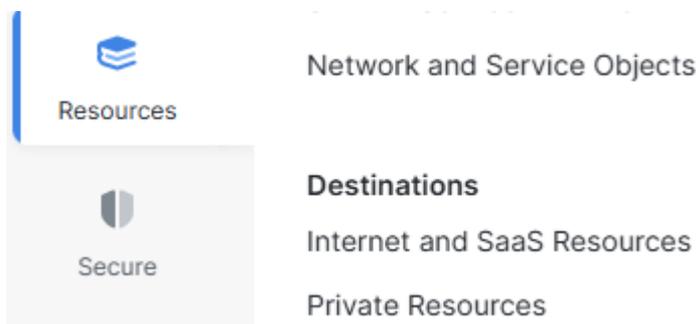
참고: BGP AS 번호 및 BGP 피어 IP 주소를 보려면 Network Tunnel Group(네트워크 터널 그룹)을 클릭합니다. BGP 피어 IP 주소는 나중에 FTD 측에서 구성됩니다.

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

Private Resource Name

FTD Internal Server

Description (optional)

Private resource address

Define how the private resource will connect to applications through Secure Access.

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ

172.16.15.55

Protocol

TCP - (HTTP/H... ▾

Port / Ranges

8080

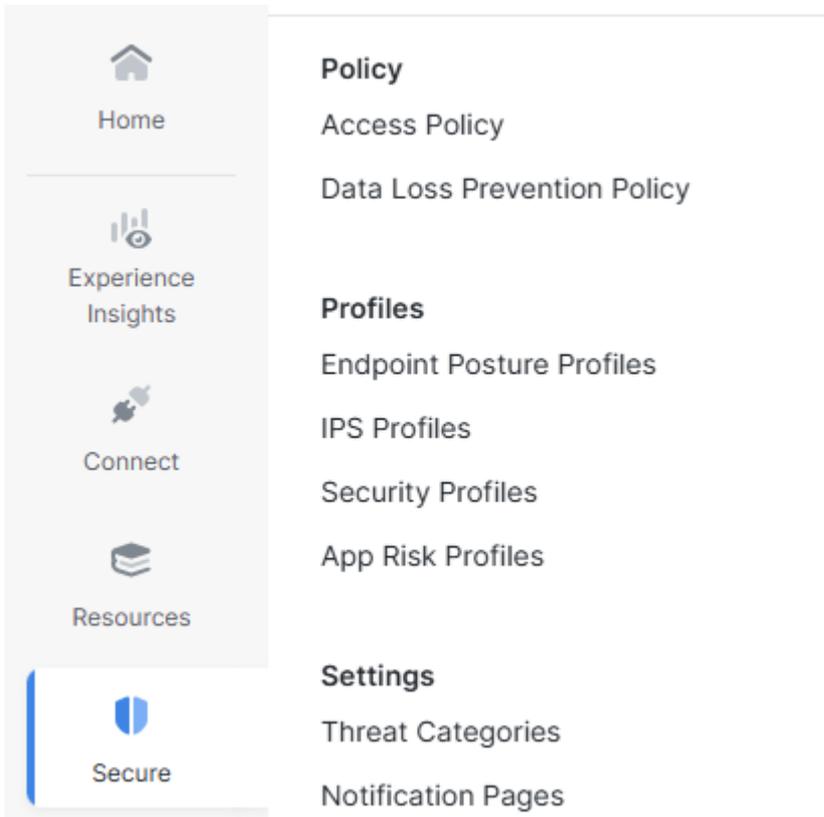
프라이빗 리소스

액세스 정책 규칙 생성

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

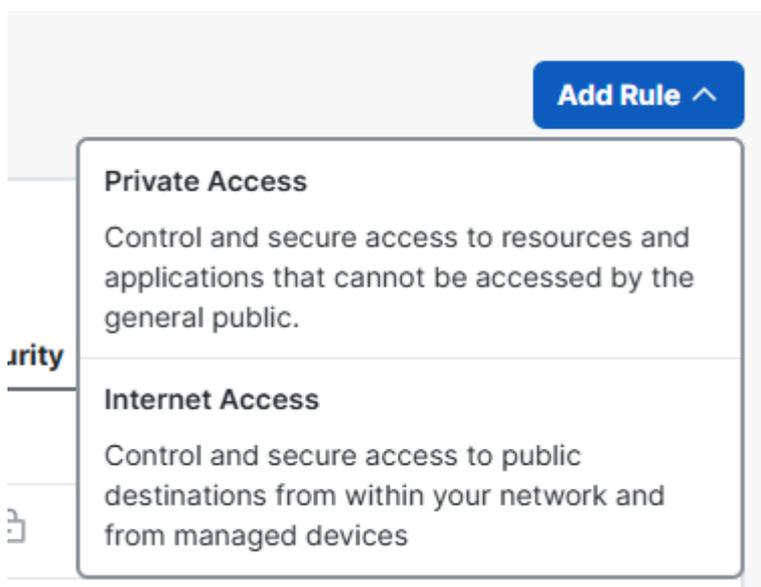
이러한 규칙은 사용자 ID, 그룹 멤버십, 디바이스 상태, 위치 또는 기타 정책 조건과 같은 요소를 기반으로 특정 프라이빗 리소스에 액세스할 수 있는 사용자를 제어하여 보안을 강화합니다. 이렇게 하면 민감한 내부 시스템이 일반 공용 액세스로부터 보호되는 동시에 ZTA 또는 VPNaaS를 통해 인증된 사용자가 안전하게 사용할 수 있습니다.

로 이동합니다 [Secure>Access Policy](#)



ACP

- **클릭** Add Rule
 - **클릭** Private Access



ACP 추가

- **클릭**하여 Rule Name 이름을 지정합니다.
- 이 트래픽 Action을 허용하려면 Allow을 **클릭**합니다.
- On(From 켜기)을 **클릭**하고 통합 권한이 있는 사용자를 지정합니다
- 을 **클릭**하고 To이 규칙을 기반으로 해당 사용자가 갖는 액세스 권한을 지정합니다
- 을 Next **클릭**한 다음 Save 페이지에서

Rule name ⓘ Rule order

1 Specify Access
Specify which users and endpoints can access which resources. [Help](#) 🔗

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From
Specify one or more sources

To
Specify one or more destinations

+ AND

Endpoint Requirements

For VPN connections:

End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. ⓘ
Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#) 🔗

For Branch connections:

Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

2 Configure Security
Configure security requirements that must be met before traffic is allowed. [Help](#) 🔗

[Cancel](#) [Back](#) [Next](#)

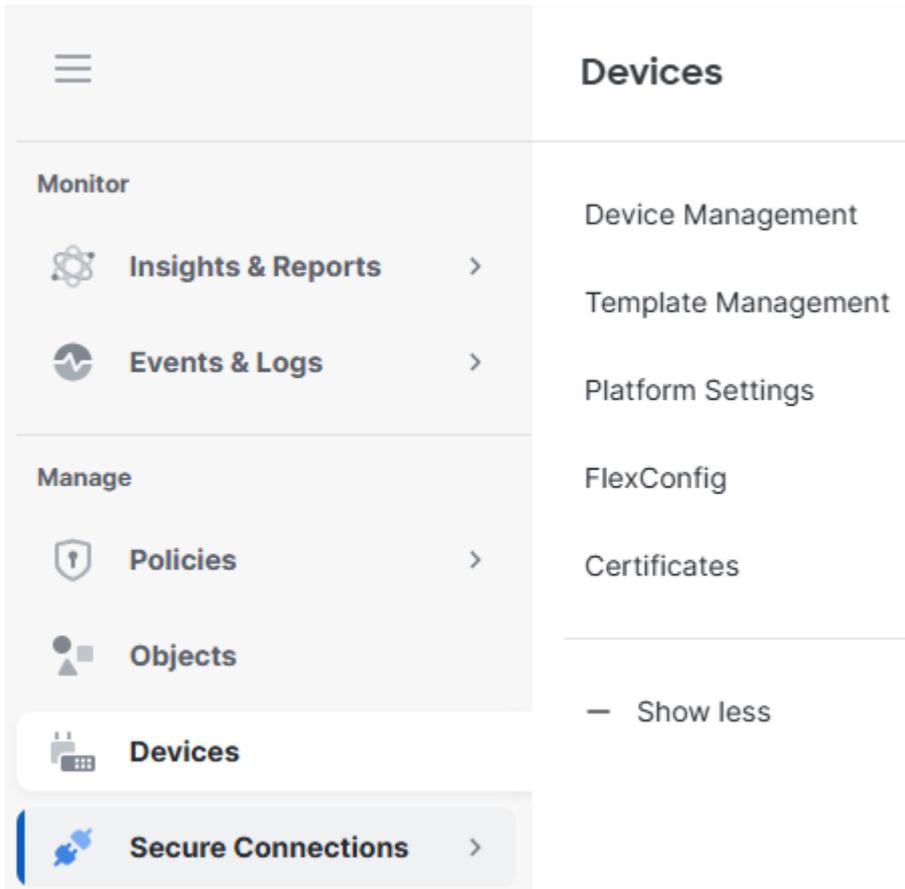
ACP 구성

FTD(Secure Firewall Threat Defense) 구성

가상 터널 인터페이스 컨피그레이션

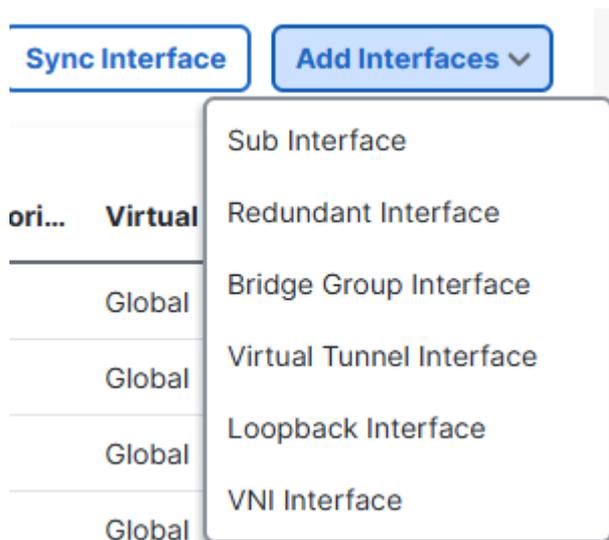
FTD의 VTI(Virtual Tunnel Interface)는 경로 기반 IPsec VPN 터널을 구성하는 데 사용되는 논리적 레이어 3 인터페이스입니다.

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
- 클릭하여 Tunnel ID 값을 지정합니다.
- 를 클릭하고 Tunnel Source 터널이 설정될 WAN 인터페이스를 지정합니다
- 클릭 IPsec Tunnel Mode, 선택 IPv4
- 를 클릭하고 IP Address VTI의 IP 주소를 구성합니다

클릭 OK

Tunnel Type

Static Dynamic

Name:*

VTI-1

Enabled

Description:

Security Zone:

zone_vti

Priority:

0

(0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

1

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (outside)

192.168.0.20

VTI1.1

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

IPv4 IPv6

IP Address:*

Configure IP

169.254.0.1/30



VTI1.2

가상 터널 인터페이스 2:

- 이름을 지정하고 Enable
- 선택 또는 만들기 Security Zone
- 클릭하여 Tunnel ID 값을 지정합니다.
- 를 클릭하고 Tunnel Source 터널이 설정될 WAN 인터페이스를 지정합니다
- 클릭 IPsec Tunnel Mode, 선택 IPv4
- 를 클릭하고 IP Address VTI의 IP 주소를 구성합니다
- 클릭 OK

Tunnel Type

Static Dynamic

Name:*

VTI-2

Enabled

Description:

Security Zone:

zone_vti

Priority:

0

(0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

2

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (outside)

192.168.0.20

VTI2.1

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

IPv4 IPv6

IP Address:*

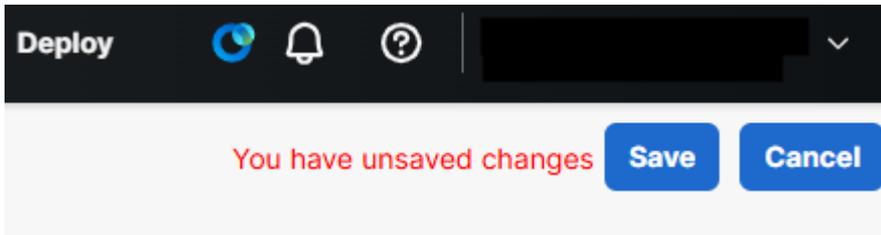
Configure IP

169.254.0.5/30



VTI2.2

Save(저장)를 클릭합니다.

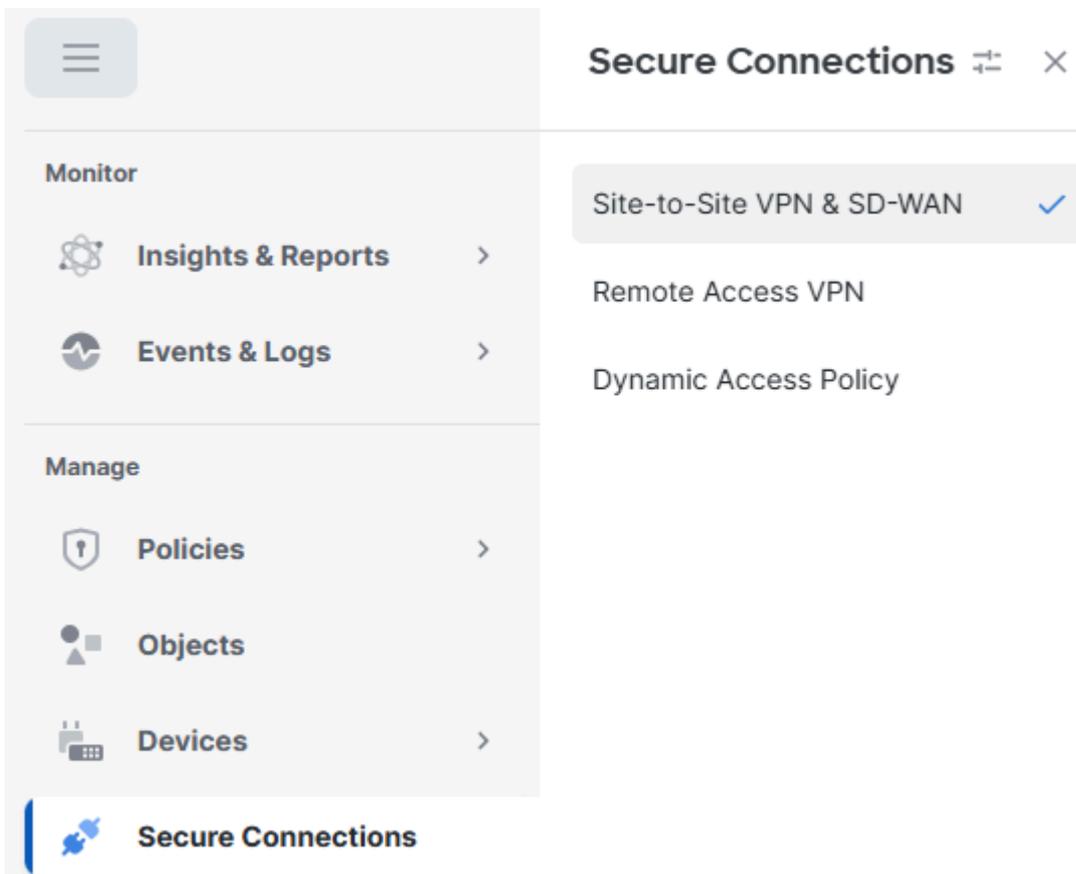


VTI 변경 사항 저장

IPsec 터널 컨피그레이션

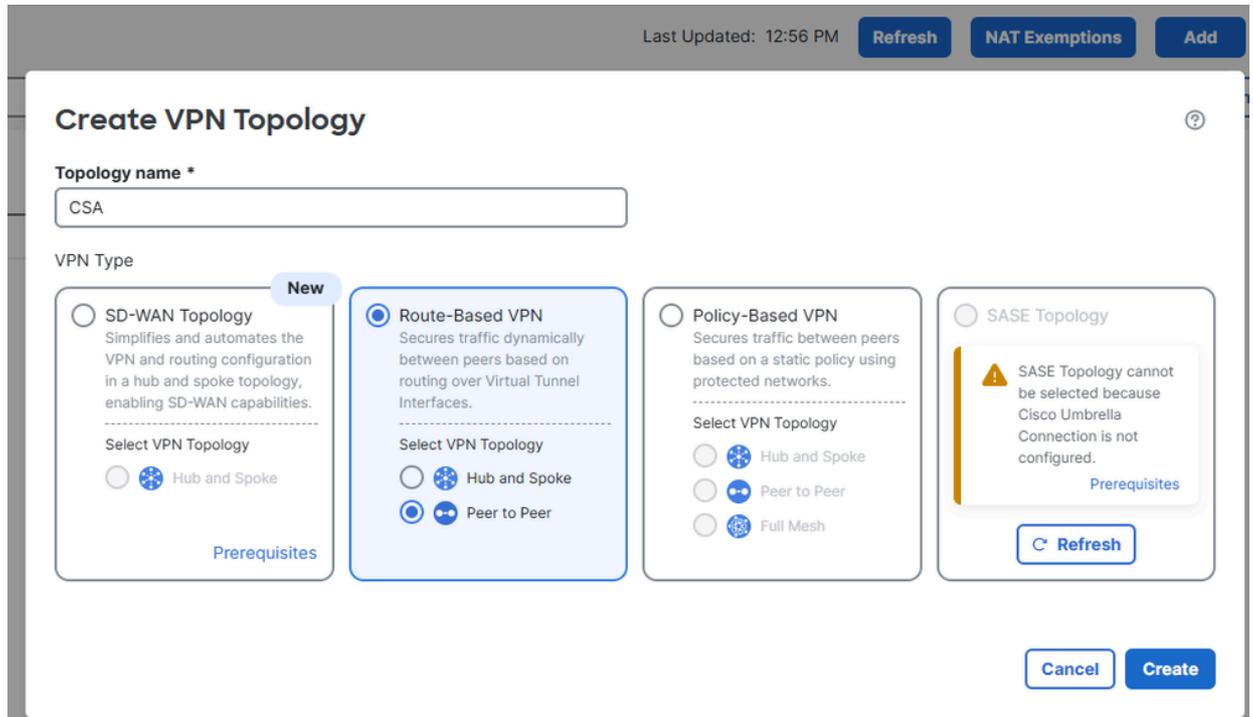
cdFMC 대시보드로 이동합니다.

- **클릭** Secure Connection > Site-to-Site VPN & SD-WAN



S2

- **클릭** Add
 - **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
- 클릭 Endpoints
 - 아래에서 Node A Device on and (켜기)를 클릭하고 Extranet
 - 클릭하여 이름 Device Name 을 지정합니다
 - 를 클릭하고 Endpoint IP Addresses Secure Access(보안 액세스) 아래의 Save Network Tunnel Group Configuration(네트워크 터널 그룹 컨피그레이션 저장)에서 심표로 구분된 Secure Access Primary and Secondary IP Addresses(보안 액세스 기본 및 보조 IP 주소)를 입력합니다
 - 설정)
 - 아래에서 Node B 를 클릭하고 Device FTD 디바이스를 선택합니다
 - 을 클릭하고 Virtual Tunnel Interface 이전 단계에서 생성한 첫 번째 VTI 인터페이스를 선택합니다
 - 옵션을 Send Local Identity to Peers Email ID 클릭하고 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 클릭하고 Virtual Tunnel Interface 이전 단계에서 생성한 두 번째 VTI 인터페이스를 선택합니다
 - on option Send Local Identity to Peers 을 클릭하고 Email ID, 보조 터널 ID를 선택합니다(Secure Access Configuration 아래의 "Save Network Tunnel Group Configuration"에서).
 - Save(저장)를 클릭합니다.

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

IKEv1

IKEv2

Endpoints

IKE

IPsec

Advanced

Node A

Device:*

Extranet

Device Name:*

CSA

Endpoint IP Address:*

Primary-IP,Secondary-IP

Node B

Device:*

cdFTD-1

Virtual Tunnel Interface:*

VTI-1 (IP: 169.254.0.1)



Tunnel Source: outside (IP: 192.168.0.20) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID

ftd1-ipsec@

Backup VTI:

[Remove](#)

Virtual Tunnel Interface:*

VTI-2 (IP: 169.254.0.5)



Tunnel Source: outside (IP: 192.168.0.20) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID

ftd1-ipsec@

Cancel

Save

FTD VTI 컨피그레이션

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

클릭 OK

IKEv2 Policy



Available IKEv2 Policy ↻ +

- AES-GCM-NULL-SHA
- AES-GCM-NULL-SHA-LA...
- AES-SHA-SHA
- AES-SHA-SHA-LATEST
- DES-SHA-SHA
- DES-SHA-SHA-LATEST
- Umbrella-AES-GCM-256

Add

Selected IKEv2 Policy

Umbrella-AES-GCM-256 ✕

Cancel OK

IKEv2 정책

- 을 클릭하고 Authentication Type 선택한 Pre Shared Manual Key 다음 Secure Access(보안 액세스)에 구성된 PSK(암호)를 입력합니다.

Endpoints **IKE** IPsec Advanced

Pre-shared Key Length:* Characters (Range 1-127)

IKEv2 Settings

Policies:* ✎

Authentication Type: ▾

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

IKE

- 클릭 IPSEC

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

Endpoints
IKE
IPsec
Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel v

Transform Sets: IKEv1 IPsec Proposals ✎ IKEv2 IPsec Proposals* ✎

tunnel_aes256_sha

Umbrella-AES-GCM-...

Cancel
OK

IPSec

IKEv2 제안서 저장

FTD 라우팅 컨피그레이션

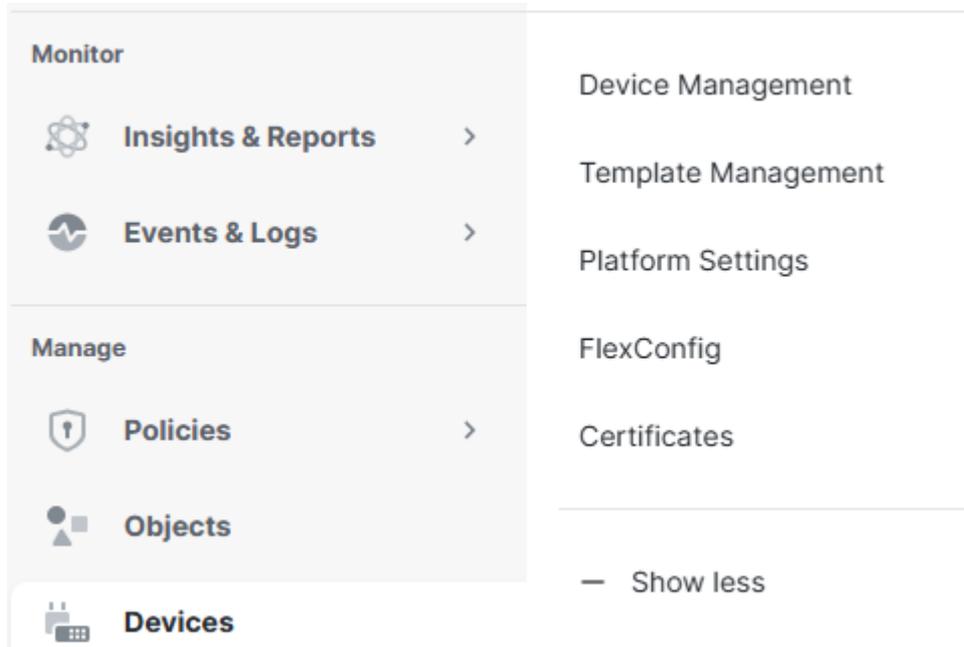
BGP(Dynamic Routing)

BGP(Border Gateway Protocol)는 AS(Autonomous System) 간 라우팅 정보 교환을 자동화하는 동적 라우팅 프로토콜입니다. 고정 경로에 의존하지 않고 특성 및 정책을 기반으로 데이터 트래픽에 사용 가능한 최상의 경로를 결정합니다.

BGP는 동적으로 경로를 학습하고 업데이트하여 확장성을 개선하고 경로 선택을 최적화하며 링크 또는 네트워크 변경 시 자동 장애 조치를 제공합니다.

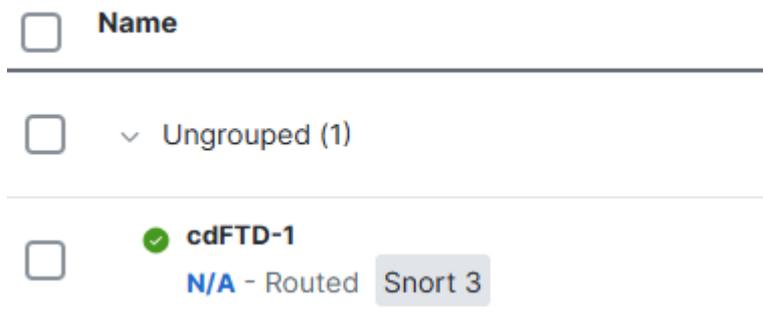
cdFMC 대시보드로 이동합니다.

- 클릭 Devices > Device Management



디바이스

- FTD를 클릭합니다



FTD 디바이스

- 클릭 **Routing** > **BGP** > **IPv4** > **Enable IPv4**
- 을 **Neighbor** 클릭하고 **Secure Access**에 대한 **BGP AS(Autonomous System)** 번호와 인접 IP 주소를 지정합니다
이 프로세스에 대한 모든 관련 컨피그레이션 세부사항이 제공되는 **Secure Access Configuration** 아래의 참고 사항을 참조하십시오.
- 클릭 **Save**

cdFTD-1 You have unsaved changes [Save](#) [Cancel](#)

Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Enable IPv4: AS Number 64513

General **Neighbor** Add Aggregate Address Filtering Networks Redistribution Route Injection

Manage Virtual Routers: Global

Virtual Router Properties: ECMP, BFD, OSPF, OSPFv3, EIGRP, RIP, Policy Based Routing, BGP, **IPv4**

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
169.254.0.2	64512	Enabled		Edit Delete
169.254.0.6	64512	Enabled		Edit Delete

BGP 네이버



참고: 2025년 11월부터 새로 생성된 모든 Secure Access 조직은 네트워크 터널 그룹의 BGP 피어링32644 대해 기본적으로 공용 ASN 인터페이스를 사용합니다. 2025년 11월 이전에 설립된 기존 조직에서는 이전에 Secure Access BGP 64512을 위해 예약한 프라이빗 ASN Service를 계속 사용합니다.

- 을 Networks 클릭하고 Secure Access에 광고할 네트워크를 추가합니다
- 클릭 Save

cdFTD-1 You have unsaved changes [Save](#) [Cancel](#)

Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Enable IPv4: AS Number 64513

General Neighbor Add Aggregate Address Filtering **Networks** Redistribution Route Injection

Manage Virtual Routers: Global

Virtual Router Properties: ECMP, BFD, OSPF, OSPFv3, EIGRP, RIP, Policy Based Routing, BGP, IPv4

Network	RouteMap
Subnet-172.16.15.0	Edit Delete

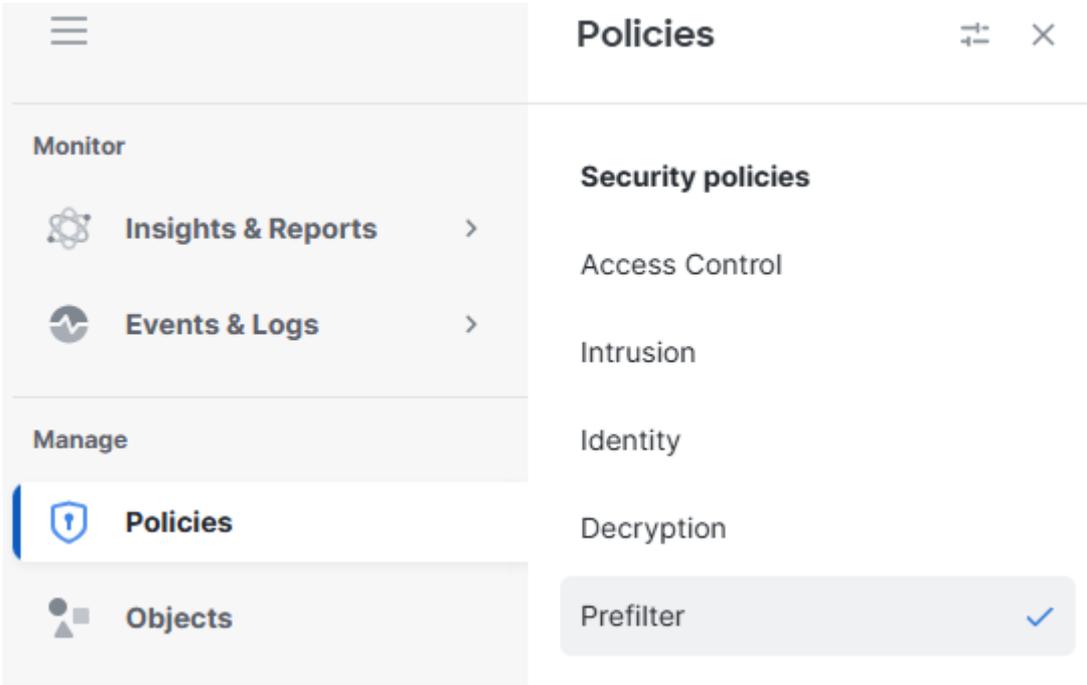
네트워크 추가

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

Prefilter Policy	Domain	Last Modified	
Default Prefilter Policy Default Prefilter Policy with default action to allow all tunnels	Global	2025-07-24 08:27:51 Modified by "admin"	🗑️ ✎️
Prefilter - Josue	Global	2026-02-18 15:26:37 Modified by	🗑️ ✎️

사전 필터 클릭

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

#	Name	Rule Type	Source Interface Objects	Destination Interface Objects	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone	
1	CSA Rule	Prefilter	zone_vr1 (Routed)	zone_in (Routed)	CSA-Manager CSA-VPNaaS CSA-ZTA	Internal-Subnet Subnet-172.16.15	any	any	any	Fastpath	na	🗑️ ✎️ 0 🗑️

규칙 저장

이때 FTD의 컨피그레이션이 완료되고 확인되면 구축을 계속할 수 있습니다. 구축 후 IPsec 터널 및 BGP 네이버 세션이 모두 정상적으로 작동하므로 연결 및 동적 라우팅이 정상적으로 작동하고 있음을 확인할 수 있습니다.

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-WAN 클릭
- Topology Name(토폴로지 이름)을 클릭합니다.

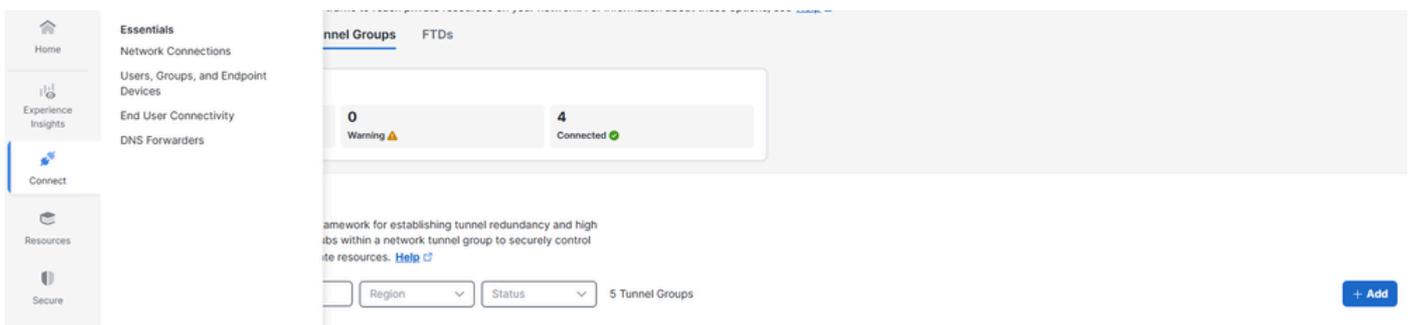
Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
CSA	Route Based (VTI)	Point-to-Point	2-Tunnels		✓
Node A			Node B		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-1 (169.254.0.1)
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-2 (169.254.0.5)

FTD 터널 상태

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

Summary

Connected

Region	Canada (Central)	Routing Type	Static Routing
Device Type	FTD	IP Address Range	172.16.15.0/24
Last Status Update	Feb 18, 2026 3:34 PM		

Primary Hub

[See Logs](#)

Hub Up

1

Active Tunnels

Tunnel Group ID ftd1-ipsec@

Secondary Hub

Hub Up

1

Active Tunnels

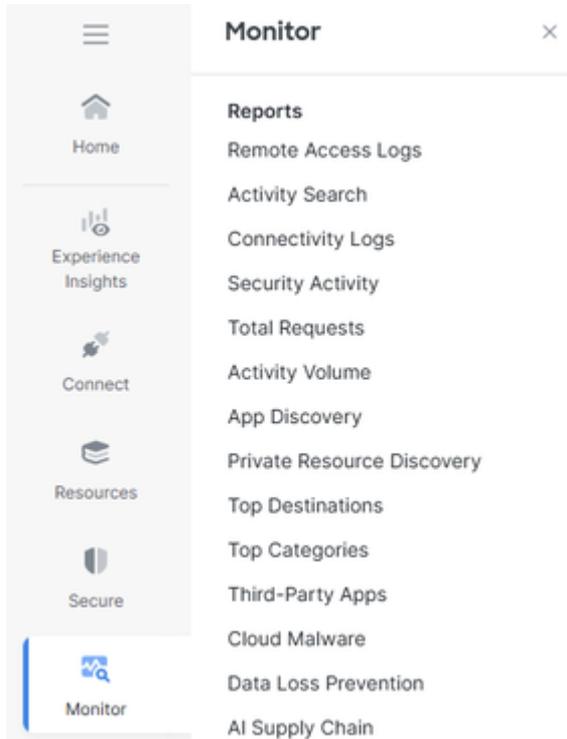
Tunnel Group ID

CSA 터널 상태

Secure Access의 이벤트

터널 및 BGP 이벤트를 보고 IPsec 터널의 상태가 작동 및 안정적인지, BGP 세션이 설정되었는지 확인할 수 있습니다.

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



연결 로그 모니터링

Network tunnel group	Data center IP address	Hub type	Region	Alerts	Service	Device type	Details	Time (UTC)
FTD		Secondary	ca-central-1	Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:07 PM
FTD		Secondary	ca-central-1	Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:07 PM
FTD		Primary	ca-central-1	Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:06 PM
FTD		Primary	ca-central-1	Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:06 PM

NTG 로그

Monitor(모니터) > Activity Search(활동 검색)로 이동합니다.

Monitor

- Home
- Experience Insights
- Connect
- Resources
- Secure
- Monitor**

Reports

- Remote Access Logs
- Activity Search
- Connectivity Logs
- Security Activity
- Total Requests
- Activity Volume
- App Discovery
- Private Resource Discovery
- Top Destinations
- Top Categories
- Third-Party Apps
- Cloud Malware
- Data Loss Prevention
- AI Supply Chain

연결 로그 모니터링

관련 이벤트에서 를 클릭합니다 View Full Details.

13,606 Total 🔄 Page: 1 Results per page: 50 1 - 50 < >

Source	Rule Identity	Destination	
Josue	Josue		View Full Details
Josue	Josue		Filter by Josue
Josue	Josue		Filter by
Josue	Josue		Filter by
Josue	Josue		View Rule
Josue	Josue		Edit Rule

전체 세부사항

Event Details



Action

Allowed

Time

Feb 18, 2026 3:30 PM

Rule Name

FTD IPsec Rule (2386307)

Enforced By

-

Source

 **Josue**

Source IP

Destination

http://172.16.15.55:8080/favicon.ico

Security Group Tag (SGT)

-

Destination IP

172.16.15.55

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.