

고가용성을 갖춘 보안 방화벽으로 보안 액세스 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[네트워크 다이어그램](#)

[구성](#)

[보안 액세스에서 VPN 구성](#)

[터널 설정 데이터](#)

[보안 방화벽에서 터널 구성](#)

[터널 인터페이스 구성](#)

[보조 인터페이스에 대한 고정 경로 구성](#)

[VTI 모드에서 보안 액세스를 위한 VPN 구성](#)

[엔드포인트 컨피그레이션](#)

[IKE 컨피그레이션](#)

[IPSEC 컨피그레이션](#)

[고급 컨피그레이션](#)

[액세스 정책 컨피그레이션 시나리오](#)

[인터넷 액세스 시나리오](#)

[RA-VPN Escenario](#)

[클랩-밥 ZTNA 에스케나리오](#)

[정책 기반 라우팅 구성](#)

[보안 액세스에 대한 인터넷 액세스 정책 구성](#)

[ZTNA 및 RA-VPN에 대한 프라이빗 리소스 액세스 구성](#)

[문제 해결](#)

[1단계\(IKEv2\) 확인](#)

[2단계\(IPSEC\) 확인](#)

[고가용성 기능](#)

[보안 액세스에 대한 트래픽 라우팅 확인](#)

[관련 정보](#)

소개

이 문서에서는 고가용성의 보안 방화벽을 사용하여 보안 액세스를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

- [사용자 프로비저닝 구성](#)
- [ZTNA SSO 인증 컨피그레이션](#)
- [원격 액세스 VPN 보안 액세스 구성](#)

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower Management Center 7.2
- Firepower 위협 방어 7.2
- 보안 액세스
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- 클라이언트리스 ZTNA

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

- Firepower Management Center 7.2
- Firepower 위협 방어 7.2
- 보안 액세스
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

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



CISCO

Secure

Access

Secure Firewall

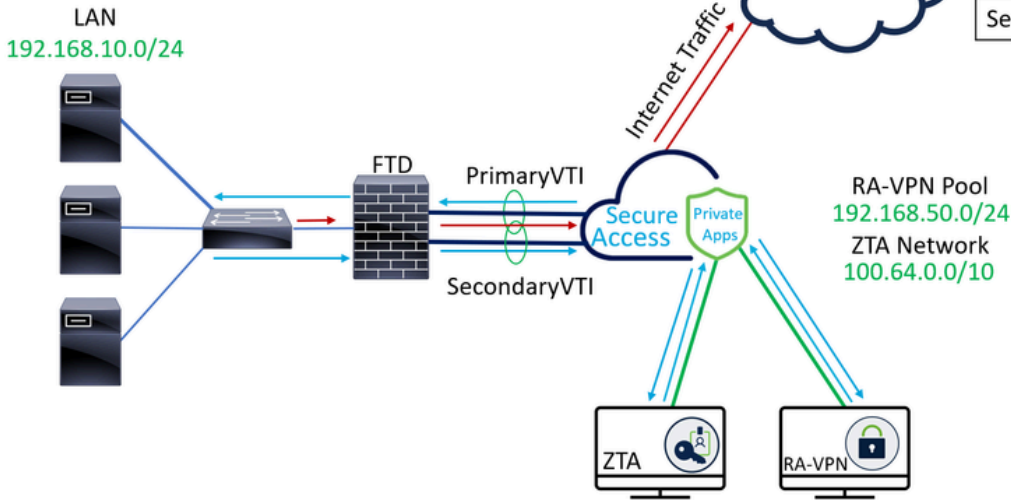
FTD

Cisco는 온프레미스 및 클라우드 기반 프라이빗 애플리케이션을 보호하고 액세스를 제공하도록 Secure Access를 설계했습니다. 또한 네트워크에서 인터넷으로의 연결도 보호합니다. 이는 여러 보안 방법 및 레이어의 구현을 통해 달성되며, 모두 클라우드를 통해 정보에 액세스할 때 정보를 보존하는 데 목적이 있습니다.

네트워크 다이어그램

Internet Access Traffic —
Private Apps Traffic —

INTERFACE	IP
PrimaryWAN	192.168.30.5
PrimaryVTI	169.254.2.1
SecondaryWAN	192.168.0.202
SecondaryVTI	169.254.3.1



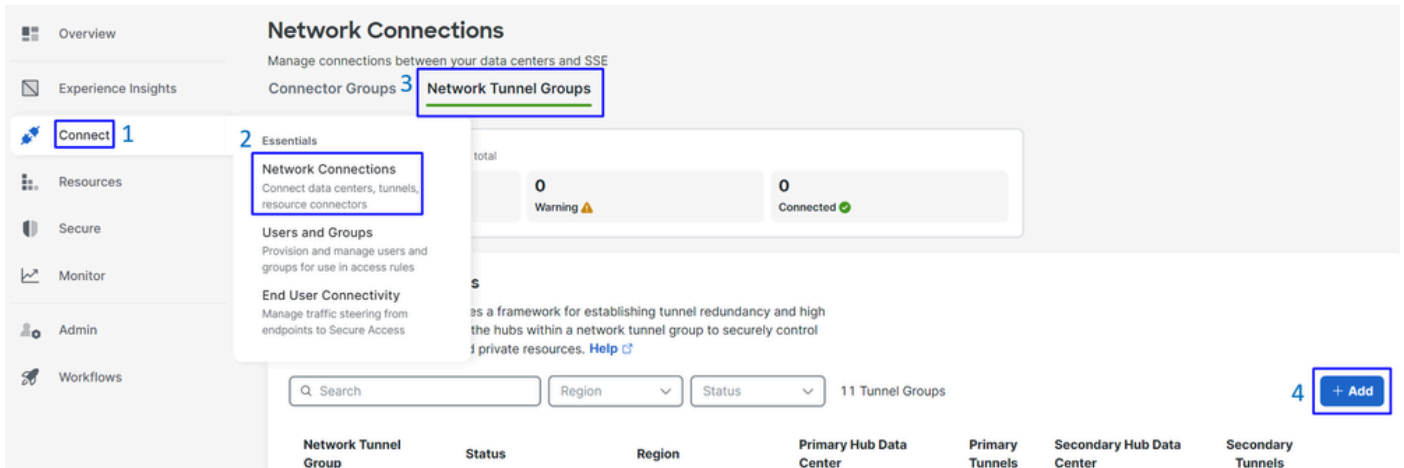
구성

보안 액세스에서 VPN 구성

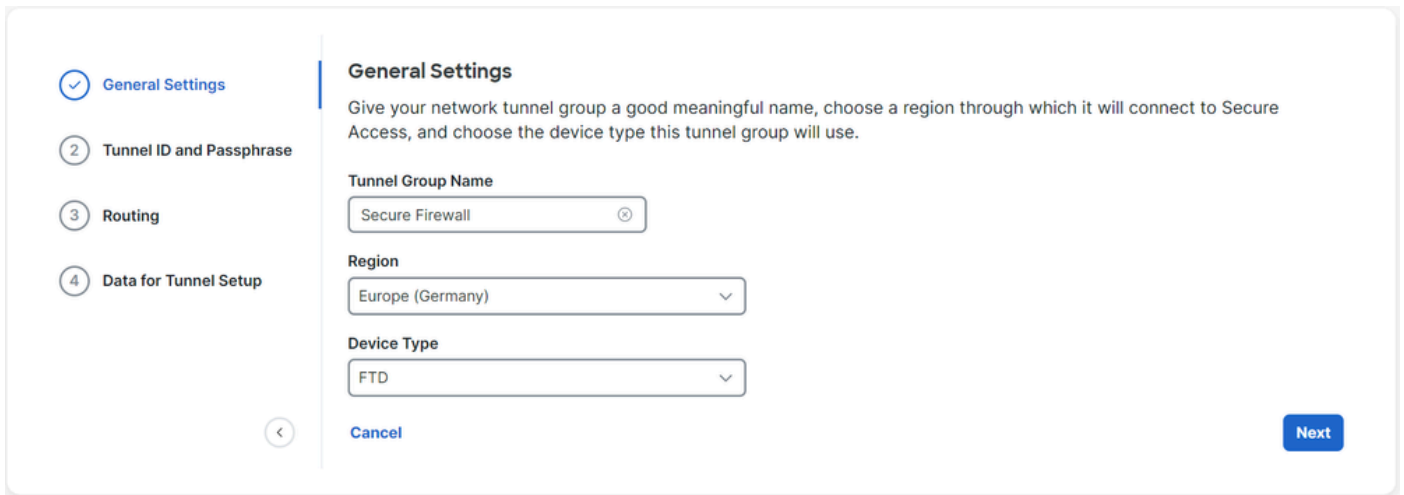
의 관리 패널로 이동합니다. [보안 액세스](#).



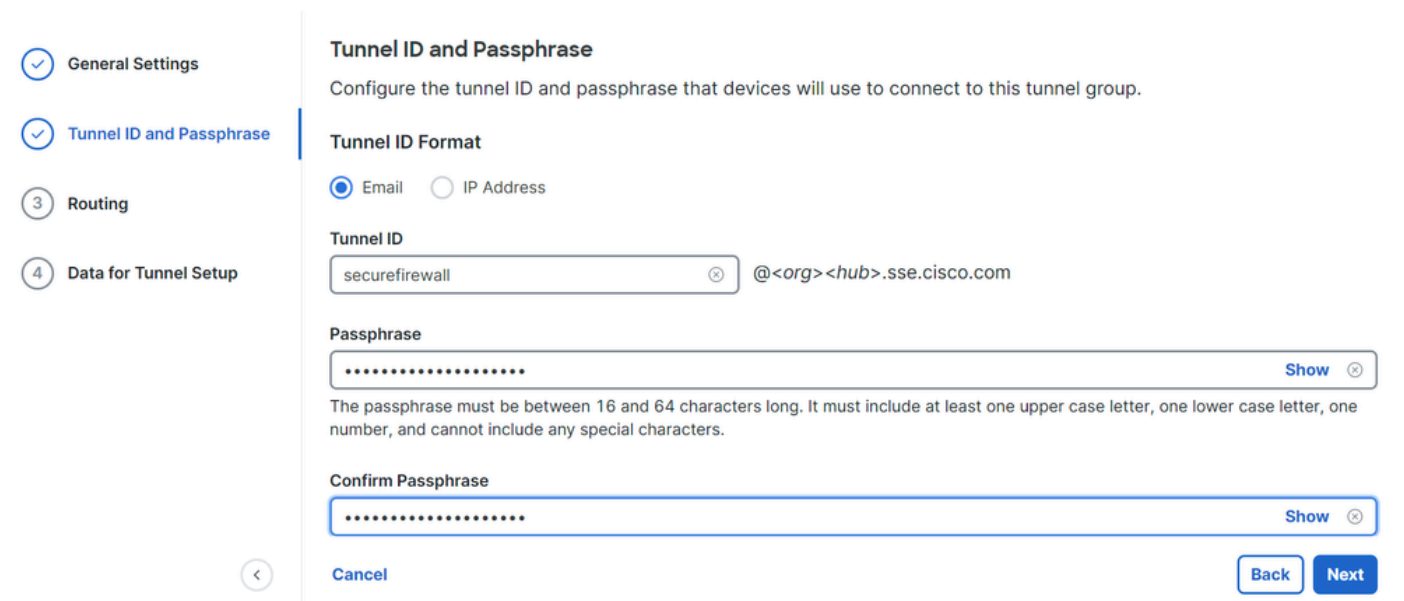
- 클릭 Connect > Network Connections
- 에서 Network Tunnel Groups 클릭 + Add



- 구성 Tunnel Group Name, Region 및 Device Type
- 을 클릭합니다 Next



- 및 를 Tunnel ID Format 구성합니다 Passphrase
- 을 클릭합니다 Next



- 네트워크에서 구성했으며 Secure Access를 통해 트래픽을 전달하려는 IP 주소 범위 또는 호

스트를 구성합니다

- 을 클릭합니다 Save

Routing option

Static routing

Use this option to manually add IP address ranges for this tunnel group.

IP Address Ranges

Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.

128.66.0.0/16, 192.0.2.0/24 Add

192.168.0.0/24 X 192.168.10.0/24 X

Dynamic routing

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

Cancel

Back

Save

터널에 대한 정보가 표시되면 Save 다음 단계를 위해 해당 정보를 저장하십시오. Configure the tunnel on Secure Firewall.

터널 설정 데이터

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

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: securefirewall@[redacted]-sse.cisco.com

Primary Data Center IP Address: 18.156.145.74

Secondary Tunnel ID: securefirewall@[redacted]-sse.cisco.com

Secondary Data Center IP Address: 3.120.45.23

Passphrase: [redacted]

Download CSV

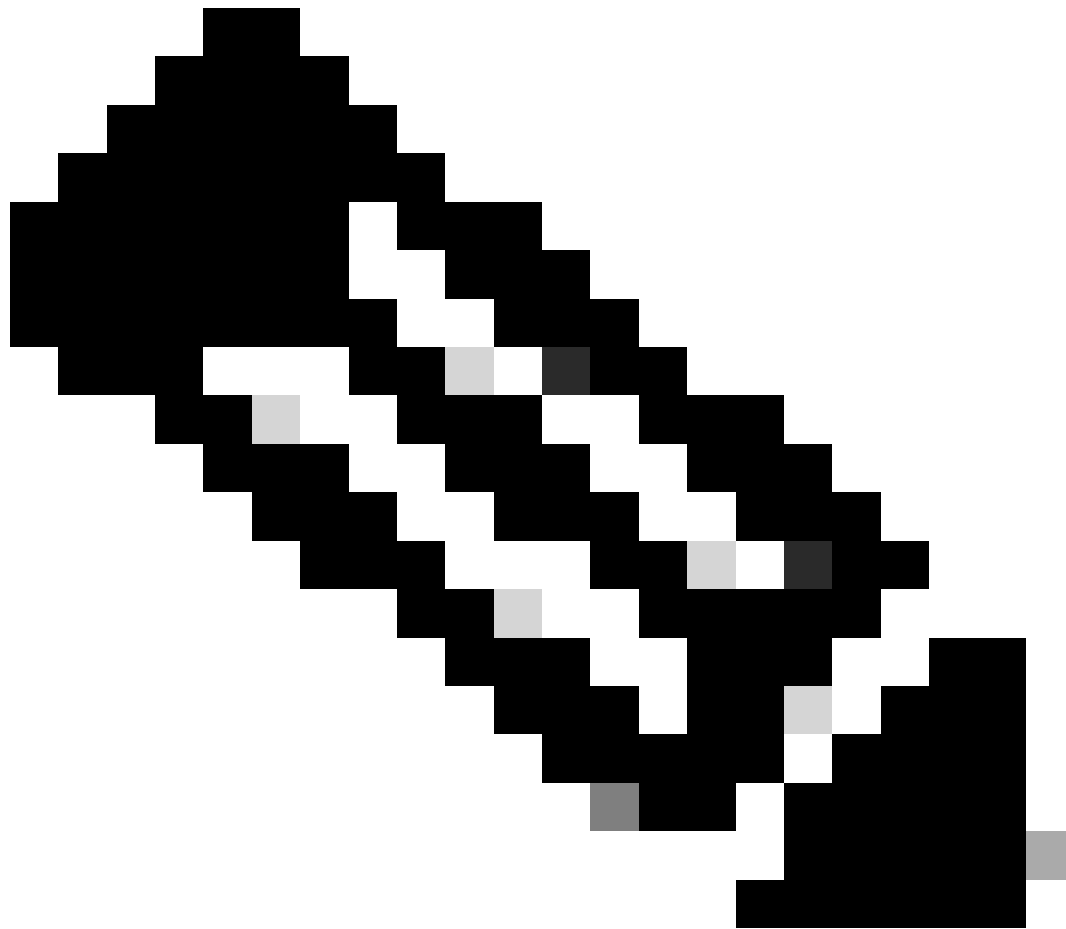
Done

보안 방화벽에서 터널 구성

터널 인터페이스 구성

이 시나리오에서는 보안 방화벽에서 VTI(Virtual Tunnel Interface) 컨피그레이션을 사용하여 이 목표를 달성합니다. 이 경우 이중 ISP가 있으며 ISP 중 하나에서 장애가 발생할 경우 HA가 필요합니다.

인터페이스	역할
기본WAN	주요 인터넷 WAN
보조WAN	보조 인터넷 WAN
기본 VTI	트래픽을 통해 Secure Access로 보내기 Principal Internet WAN 위해 연결됨
보조VTI	트래픽을 통해 Secure Access로 보내기 Secondary Internet WAN 위해 연결됨



참고: 1. 두 터널을 모두 가동하려면 고정 경로를 Primary or Secondary Datacenter IP 또는 에 할당해야 합니다.

참고: 2. 인터페이스 간에 ECMP를 구성한 경우, 두 터널을 모두 활성화하기 위해에 대한 고정 경로 Primary or Secondary Datacenter IP를 생성할 필요가 없습니다.

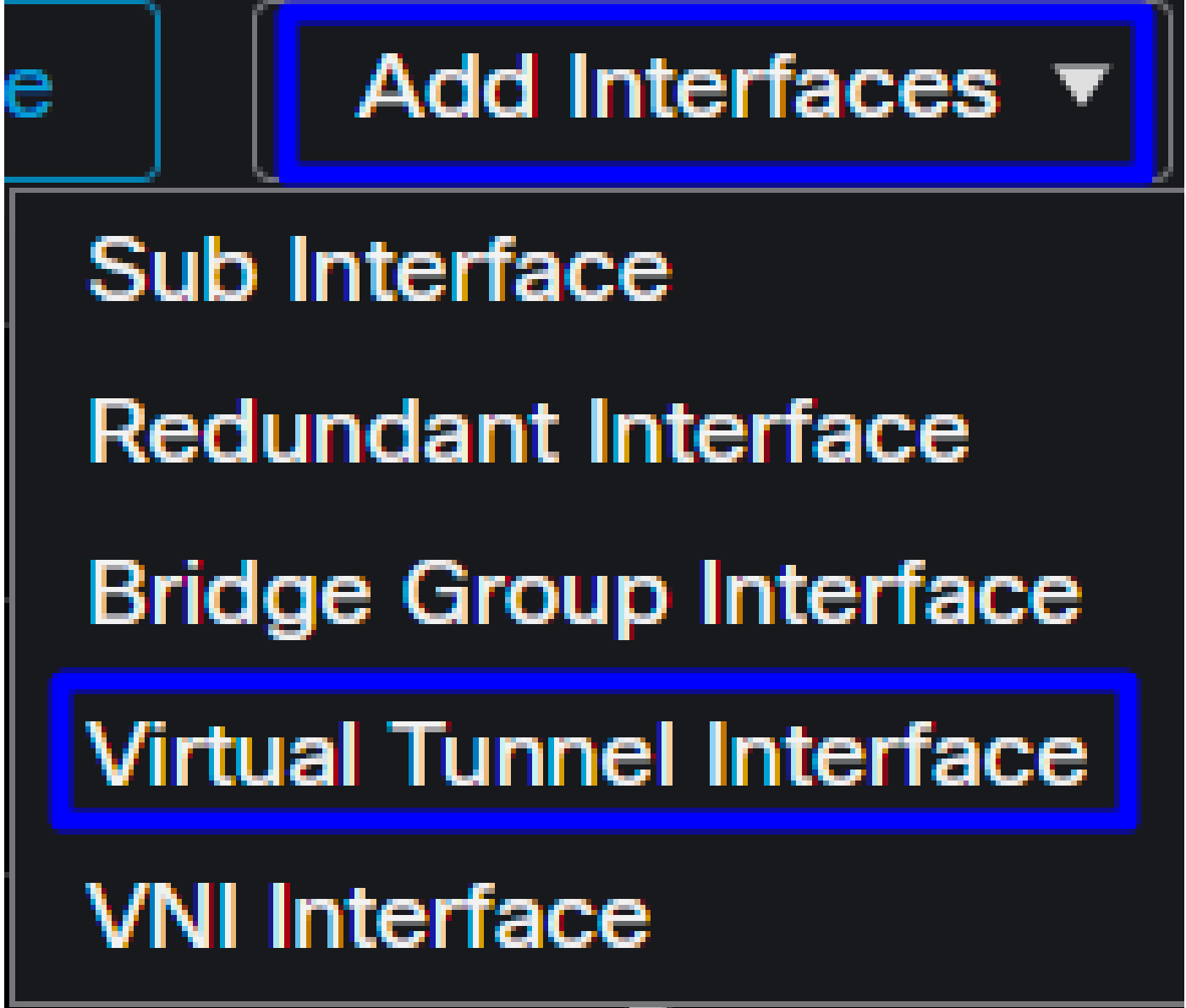
시나리오에 따라 VTI 인터페이스 PrimaryWAN를 SecondaryWAN 생성하기 위해 사용해야 하는 및 이 있습니다.

로 이동합니다 Firepower Management Center > Devices.

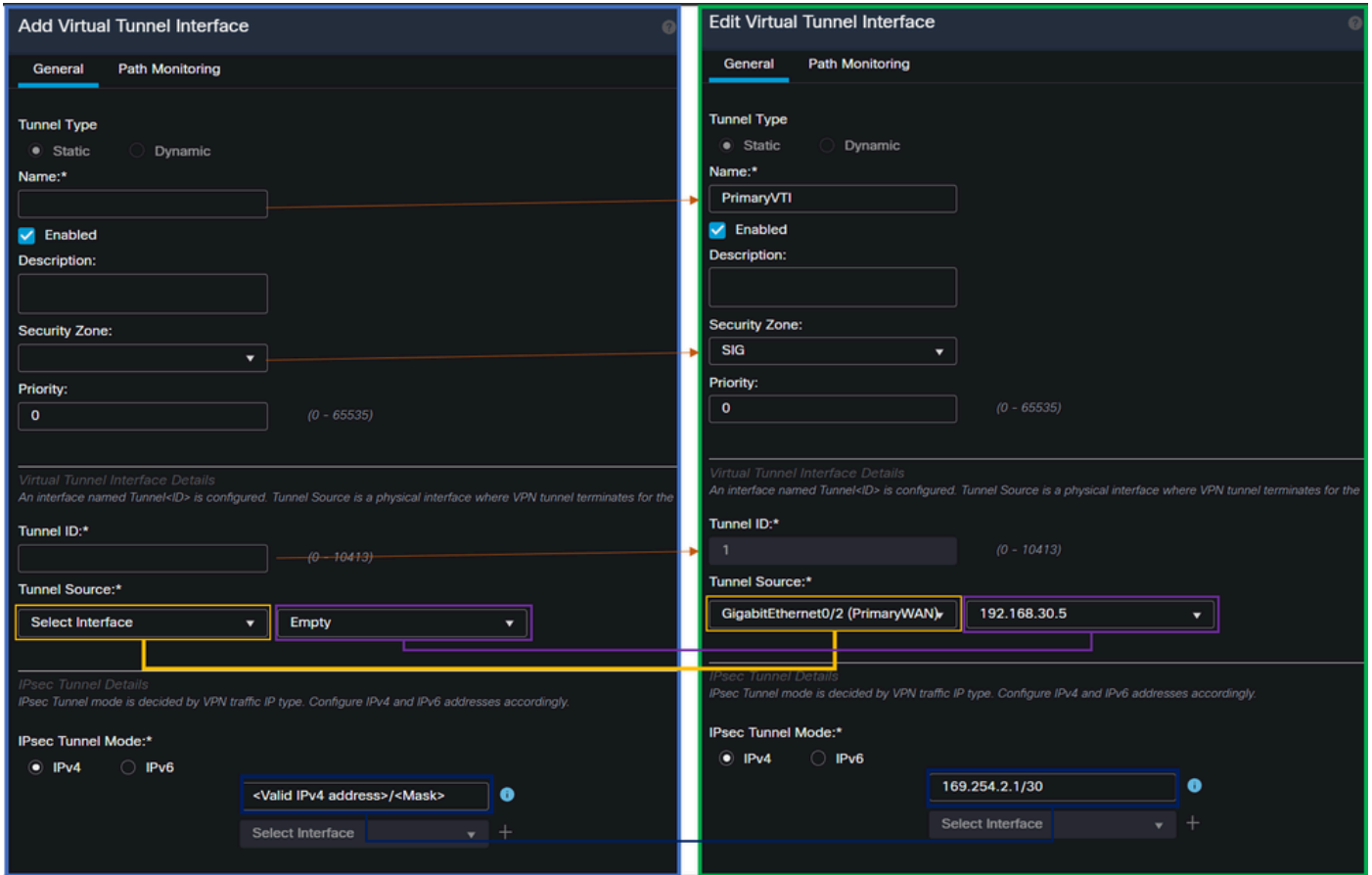
- FTD 선택
- 선택 Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)

- 클릭 Add Interfaces > Virtual Tunnel Interface



- 다음 정보를 기반으로 인터페이스를 구성합니다



- Name : 를 참조하는 이름 구성 PrimaryWAN interface
- Security Zone : 다른 것을 재사용할 수 Security Zone 있지만 Secure Access 트래픽을 위해 새 것을 만드는 것이 더 좋습니다
- Tunnel ID : 터널 ID의 번호 추가
- Tunnel Source : 를 PrimaryWAN interface 선택하고 인터페이스의 프라이빗 또는 퍼블릭 IP를 선택합니다
- IPsec Tunnel Mode : 네트워크에서 라우팅 불가 IP를 선택 IPv4 및 구성합니다(마스크 30)



참고: VTI 인터페이스의 경우 라우팅 불가 IP를 사용해야 합니다. 예를 들어, VTI 인터페이스가 2개인 경우에는 169.254.2.1/30을 사용하고 에는 PrimaryVTI 169.254.3.1/30을 사용할 수 SecondaryVTI 있습니다.

그 후에는 에도 동일한 작업을 수행해야 하며, VTI 고가용성에 대해 모든 것이 설정되어 SecondaryWAN interface 있기 때문에 다음 결과가 나타납니다.

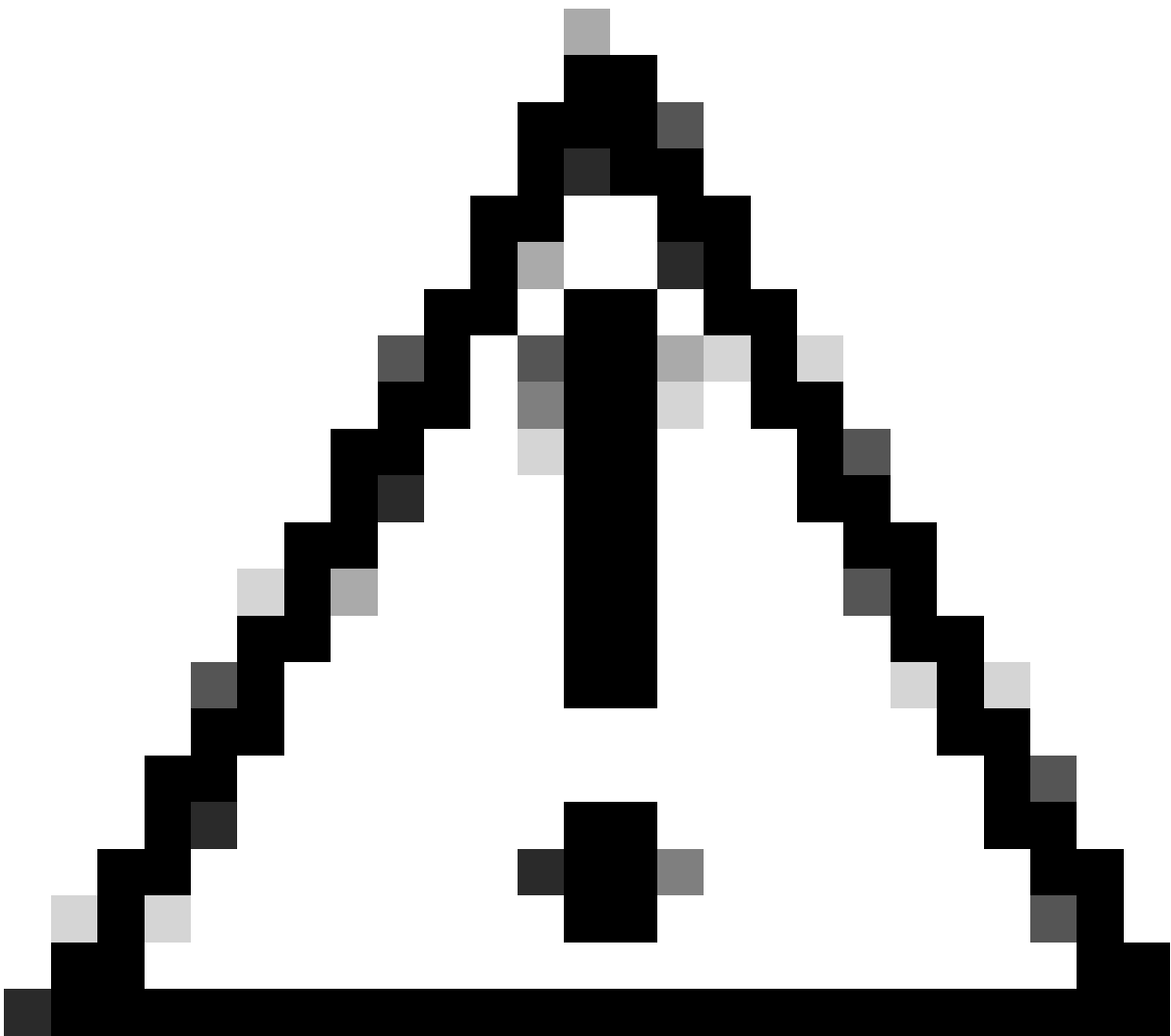
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)
Tunnel1	PrimaryVTI	VTI	SIG		169.254.2.1/30(Static)

이 시나리오에서 사용되는 IP는 다음과 같습니다.

VTI IP 컨피그레이션		
논리적 이름	IP	범위
기본 VTI	169.254.2.1/30	169.254.2.1-169.254.2.2
보조VTI	169.254.3.1/30	169.254.3.1-169.254.3.2

보조 인터페이스에 대한 고정 경로 구성

의 트래픽이 **SecondaryWAN interface** 에 도달할 수 있게 하려면 **Secondary Datacenter IP Address** 데이터센터 IP에 대한 고정 경로를 구성해야 합니다. 라우팅 테이블 위에 오도록 1의 메트릭을 사용하여 구성할 수 있습니다. 또한 IP를 호스트로 지정합니다.



주의: 이는 WAN 채널 간에 ECMP 설정이 없는 경우에만 필요합니다. ecmp를 구성한 경우

다음 단계로 건너뛸 수 있습니다.

로 이동합니다 **Device > Device Management**

- **FTD 디바이스를 클릭합니다.**
- **클릭 Routing**
- **선택 Static Route > + Add Route**

Edit Static Route Configuration


Type: IPv4 IPv6

Interface*

SecondaryWAN

Choose the SecondaryWAN interface

(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Search

Add

Selected Network

SecureAccessTunnel

Choose the Secondary Datacenter IP

192.168.0.150

192.168.10.153

any-ipv4

ASA_GW

CSA_Primary

GWWT1

Ensure that egress virtualrouter has route to that destination

Gateway

Outside_GW

Choose the SecondaryWAN Gateway

Metric:

1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

Cancel

OK

- Interface: SecondaryWAN Interface를 선택합니다
- Gateway: SecondaryWAN Gateway를 선택합니다
- Selected Network: 보조 데이터 센터 IP를 호스트로 추가합니다. 보안 액세스 단계에서 터널을 구성할 때 제공된 정보에 대한 정보, 터널 설정을 위한 데이터를 찾을 수 있습니다
- Metric: 1개 사용

- OKAnd(Save저장)를 클릭하여 정보를 저장한 다음 구축합니다.

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
SecureAccessTunnel	SecondaryWAN	Global	Outside_GW	false	1	
any-ipv4	PrimaryWAN	Global	ASA_GW	false	1	
▼ IPv6 Routes						

VTI 모드에서 보안 액세스를 위한 VPN 구성

VPN을 구성하려면 방화벽으로 이동합니다.

- 클릭 **Devices > Site to Site**
- 클릭 **+ Site to Site VPN**

엔드포인트 컨피그레이션

Endpoints(엔드포인트) 단계를 구성하려면 Data for Tunnel Setup(터널 설정용 데이터) 단계에서 제공된 정보를 사용해야 합니다.

Create New VPN Topology

Topology Name:*

Policy Based (Crypto Map)
 Route Based (VTI)

Network Topology:

IKE Version:* IKEv1 IKEv2

Node A

Device:*

Virtual Tunnel Interface:*
 +

Tunnel Source: PrimaryWAN (IP: 192.168.30.5) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Node B

Device:*

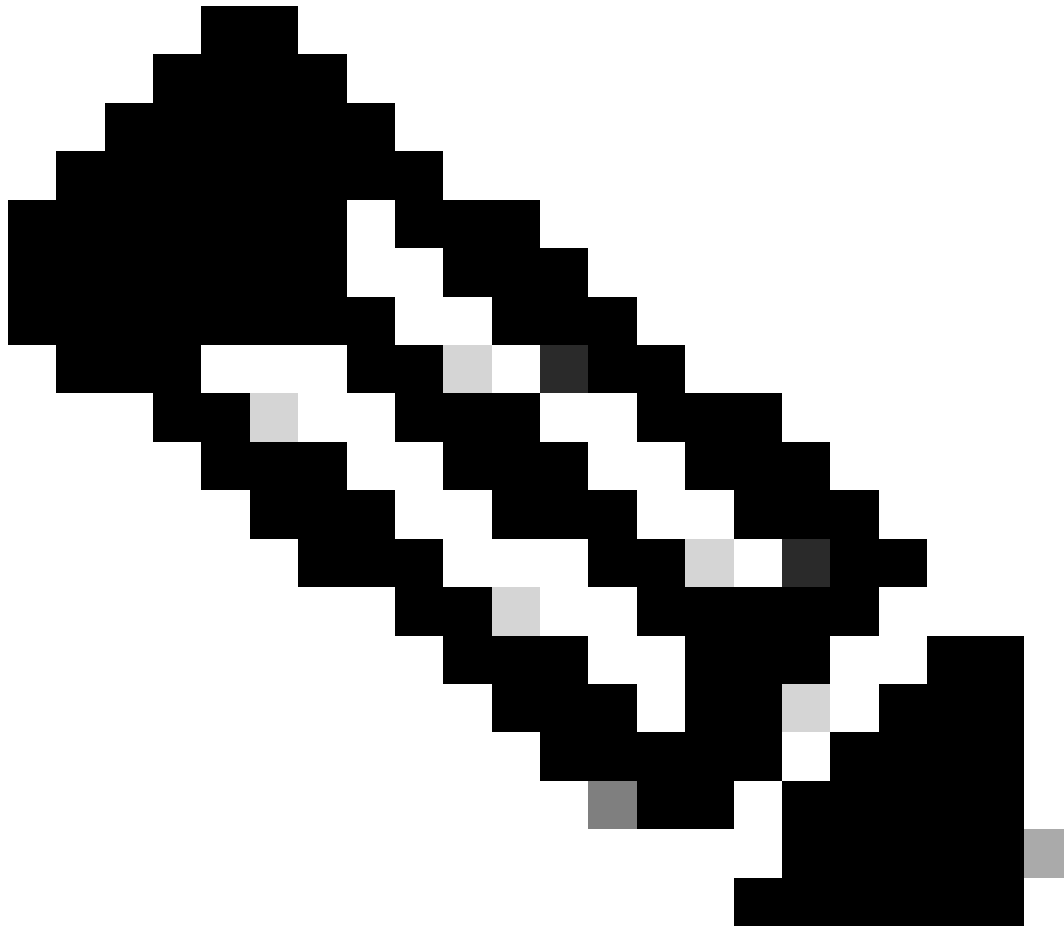
Device Name*:

Endpoint IP Address*:

Backup VTI: [Remove](#)

- 토폴로지 이름: Secure Access 통합과 관련된 이름 만들기
- 선택 **Routed Based (VTI)**
- 선택 **Point to Point**

- IKE Version: IKEv2 선택
-



참고: IKEv1은 Secure Access와의 통합에 지원되지 않습니다.

에서 Node A 다음 매개변수를 구성해야 합니다.

Node A

Device:*

FTD_HOME

Virtual Tunnel Interface:*

PrimaryVTI (IP: 169.254.2.1)



Tunnel Source: PrimaryWAN (IP: 192.168.30.5) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID

jairohome@

[+ Add Backup VTI \(optional\)](#)

- Device: FTD 장치 선택
- Virtual Tunnel Interface: 와 관련된 VTI를 PrimaryWAN Interface 선택합니다.
- 확인란을 선택합니다. Send Local Identity to Peers
- Local Identity Configuration: Email ID(이메일 ID)를 선택하고, 컨피그레이션에 Primary Tunnel ID 제공된 정보를 기반으로 Data for [Tunnel Setup\(터널 설정용 데이터\) 단계에 정보를 입력합니다](#)

를 클릭할 때 정보를 구성한 후 다음을 PrimaryVTI 클릭합니다+ Add Backup VTI.

Backup VTI:

Remove

Virtual Tunnel Interface:*

SecondaryVTI (IP: 169.254.3.1) ▼

+

Tunnel Source: SecondaryWAN (IP: 192.168.0.202) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID ▼

jairohome@

- Virtual Tunnel Interface: 와 관련된 VTI를 PrimaryWAN Interface선택합니다.
- 확인란을 선택합니다. Send Local Identity to Peers
- Local Identity Configuration: Email ID(이메일 ID)를 선택하고, 컨피그레이션에 Secondary Tunnel ID 제공된 정보를 기반으로 Data for [Tunnel Setup](#)(터널 설정용 데이터) 단계에 정보를 입력합니다

에서 Node B다음 매개변수를 구성해야 합니다.

Node B

Device:*

Extranet

Device Name*:

SecureAccess

Endpoint IP Address*:

18.156.145.74, 3.120.45.23

- Device: 엑스트라넷
- Device Name: Secure Access를 대상으로 인식하려면 Name(이름)을 선택합니다.
- Endpoint IP Address: 기본 및 보조에 대한 컨피그레이션은 기본이어야 Datacenter IP, Secondary Datacenter IP입니다. 해당 정보는 터널 설정에 대한 데이터 단계에서 찾을 수 있습니다

그런 다음 의 컨피그레이션Endpoints이 완료되고 이제 IKE Configuration(IKE 컨피그레이션) 단계로 이동할 수 있습니다.

IKE 컨피그레이션

IKE 매개변수를 구성하려면 를 IKE클릭합니다.

Endpoints

IKE

IPsec

Advanced

아래에서 IKE, 다음 매개변수를 구성해야 합니다.

Endpoints **IKE** IPsec Advanced

IKEv2 Settings

Policies:* Umbrella-AES-GCM-256

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

- Policies: 기본 Umbrella 컨피그레이션을 사용하거나 Umbrella-AES-GCM-256 를 기반으로 다른 매개 변수를 구성할 수 있습니다. [Supported IKEv2 and IPSEC Parameters](#)
- Authentication Type: 사전 공유 수동 키
- Key 및 Confirm Key [터널 설정을 위한](#) Passphrase 데이터 단계에서 정보를 찾을 수 [있습니다](#)

그런 다음 의 컨피그레이션 IKE이 완료되고 이제 IPSEC 컨피그레이션 단계로 이동할 수 있습니다.

IPSEC 컨피그레이션

IPSEC 매개변수를 구성하려면 IPSEC을 클릭합니다.

Endpoints

IKE



IPsec

Advanced

아래에서 IPSEC, 다음 매개변수를 구성해야 합니다.

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

tunnel_aes256_sha	Umbrella-AES-GCM-256
-------------------	-----------------------------

Enable Security Association (SA) Strength Enforcement

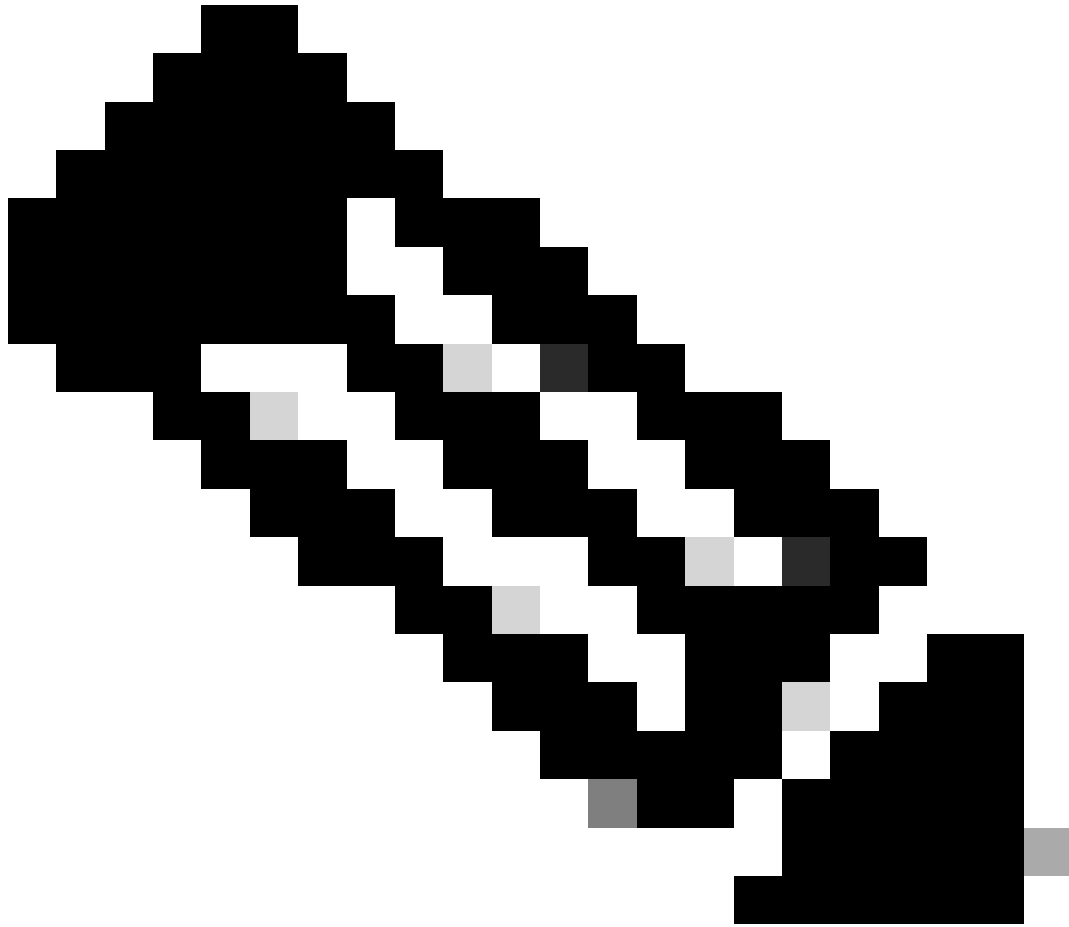
Enable Perfect Forward Secrecy

Modulus Group: 14

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

- Policies: 기본 Umbrella 컨피그레이션을 사용하거나 Umbrella-AES-GCM-256 를 기반으로 다른 매개변수를 구성할 수 있습니다. [Supported IKEv2 and IPSEC Parameters](#)

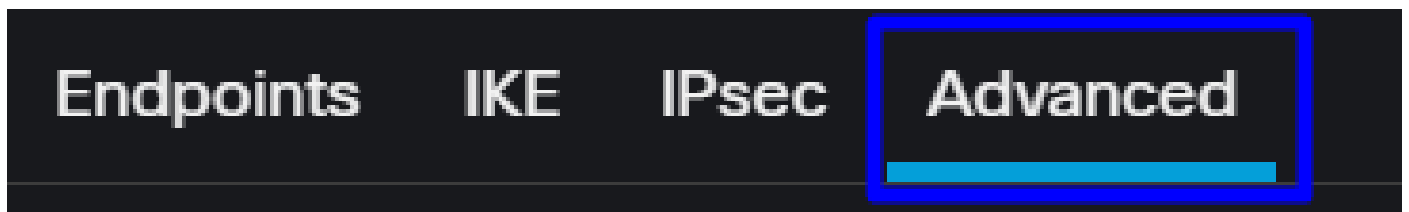


참고: IPSEC에는 다른 작업이 필요하지 않습니다.

그런 다음 의 컨피그레이션IPSEC이 완료되고 이제 고급 컨피그레이션 단계로 이동할 수 있습니다.

고급 컨피그레이션

고급 매개변수를 구성하려면 Advanced(고급)를 클릭합니다.



아래에서 **Advanced**, 다음 매개변수를 구성해야 합니다.

ISAKMP Settings

IKE Keepalive: Enable

Threshold: 10 Seconds (Range 10 - 3600)

Retry Interval: 2 Seconds (Range 2 - 10)

Identity Sent to Peers: autoOrDN

Peer Identity Validation: Do not check

Enable Aggressive Mode

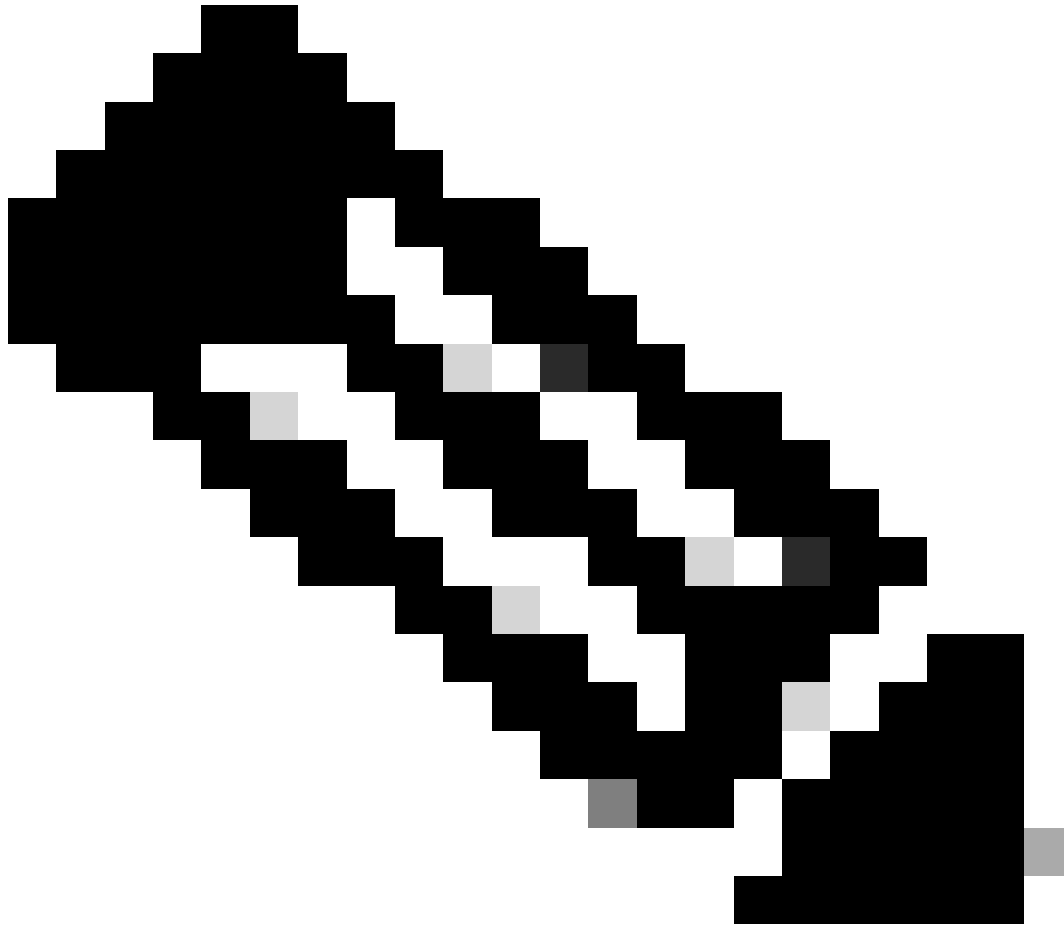
Enable Notification on Tunnel Disconnect

IKEv2 Security Association (SA) Settings

Cookie Challenge: custom

- IKE Keepalive: Enable
- Threshold: 10
- Retry Interval: 2
- Identity Sent to Peers: autoOrDN
- Peer Identity Validation: 확인 안 함

그런 다음 을 클릭하면 Save 됩니다 Deploy.



참고: 몇 분 후에 두 노드에 대해 설정된 VPN을 볼 수 있습니다.

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
SecureAccess	Route Based (VTI)	Point to Point	2 - Tunnels	✓	✗
Node A			Node B		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET Extranet	3.120.4... (3.120.45.23)●.....	FTD FTD_HOME	Secon... (192.168.0.202)	Seconda... (169.254.3.1)
EXTRANET Extranet	18.15... (18.156.145.74)●.....	FTD FTD_HOME	Primary... (192.168.30.5)	PrimaryVTI (169.254.2.1)

그런 다음 의 컨피그레이션 VPN to Secure Access in VTI Mode이 완료되고 이제 단계로 이동할 수 있습니다
Configure Policy Base Routing.



경고: Secure Access에 대한 트래픽은 두 터널이 모두 설정된 경우 기본 터널로만 전달됩니다. 기본 터널이 다운되면 보안 액세스에서 보조 터널을 통해 트래픽을 전달할 수 있습니다.

참고: Secure Access 사이트의 장애 조치는 지원되는 IPsec 값에 대한 [사용](#) 설명서에 설명된 DPD [값](#)을 기반으로 합니다.

액세스 정책 컨피그레이션 시나리오

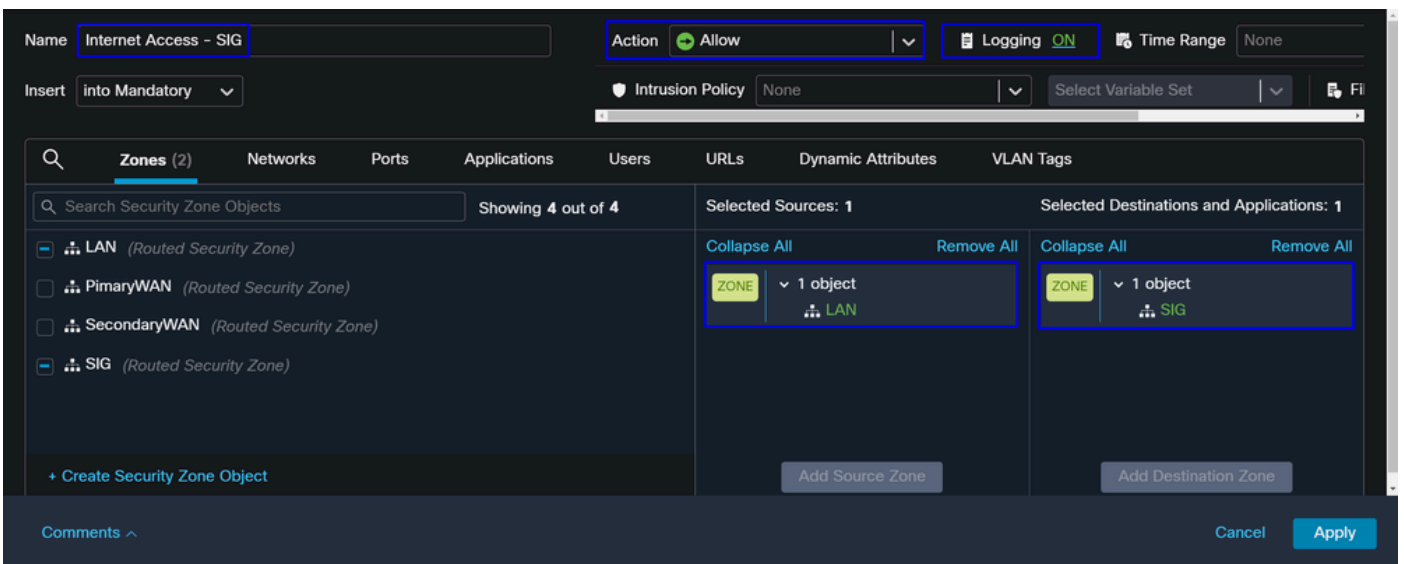
정의된 액세스 정책 규칙은 다음을 기반으로 합니다.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
● GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
● Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
● GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
● GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)
● Tunnel1	PrimaryVTI	VTI	SIG		169.254.2.1/30(Static)

인터페이스	영역
기본 VTI	시그니처
보조 VTI	시그니처
LAN	LAN

인터넷 액세스 시나리오

Policy Base Routing에서 구성하는 모든 리소스에 대한 인터넷 액세스를 제공하려면 보안 액세스에서 일부 액세스 규칙과 일부 정책을 구성해야 합니다. 이 시나리오에서 이를 달성하는 방법을 설명하겠습니다.



이 규칙은 인터넷에 LAN 대한 액세스를 제공하며, 이 경우 인터넷은 SIG입니다.

RA-VPN Escenario

RA-VPN 사용자의 액세스를 제공하려면 RA-VPN 풀에 할당한 범위를 기반으로 구성해야 합니다.

참고: RA-VPNaaS 정책을 구성하려면 Manage [Virtual Private Networks\(가상 사설 네트워크 관리\)](#)를 통해

VPNaaS의 IP 풀을 어떻게 확인합니까?

[Secure Access Dashboard\(보안 액세스 대시보드\)](#)로 이동

- 클릭 **Connect > End User Connectivity**
- 클릭 **Virtual Private Network**
- 아래에서 **Manage IP Pools**을 클릭합니다. Manage

End User Connectivity

↓ Cisco Secure Client

Manage DNS Servers (2)

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. [Help](#)

Zero Trust **Virtual Private Network** Internet Security

Global FQDN

fb57.vpn.sse.cisco.com [Copy](#)

Manage IP Pools

2 Regions mapped

Manage

- 아래에 수영장이 보입니다 Endpoint IP Pools

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House

- SIG에서 이 범위를 허용해야 하지만 PBR에서 구성한 ACL에서도 이 범위를 추가해야 합니다

액세스 규칙 컨피그레이션

프라이빗 애플리케이션 리소스에 액세스하는 기능과 함께 사용하도록 보안 액세스만 구성하는 경우 액세스 규칙은 다음과 같을 수 있습니다.

Name: Private APP | Action: Allow | Logging: ON | Time Range: None

Insert: into Mandatory | Intrusion Policy: None | Select Variable Set: [] | FI

Search Network and Geolocation Objects | Showing 27 out of 27

Networks	Geolocations
<input type="checkbox"/> 192.168.0.150 (Host Object)	192.168.0.150
<input type="checkbox"/> 192.168.10.153 (Host Object)	192.168.10.153
<input type="checkbox"/> any (Network Group)	0.0.0.0::/0
<input type="checkbox"/> any-ipv4 (Network Object)	0.0.0.0/0
<input type="checkbox"/> any-ipv6 (Host Object)	::/0

+ Create Network Object | Manually Enter IP: []

Selected Sources: 2

- ZONE 1 object: SIG
- NET 1 object: 192.168.50.0/24

Selected Destinations and Applications: 1

- ZONE 1 object: LAN

Buttons: Add Source Network, Add Destination Network, Cancel, Apply

이 규칙은 RA-VPN 풀 192.168.50.0/24에서 LAN으로의 트래픽을 허용합니다. 필요한 경우 더 많은 항목을 지정할 수 있습니다.

ACL 컨피그레이션

정책 기반 라우팅 구성

보안 액세스를 통해 내부 리소스 및 인터넷에 대한 액세스를 제공하려면 소스에서 대상으로의 트래픽 라우팅을 용이하게 하는 PBR(Policy Base Routing)을 통해 경로를 생성해야 합니다.

- 로 이동합니다 **Devices > Device Management**
- 경로를 생성할 FTD 디바이스를 선택합니다

<input type="checkbox"/>	Name	Model	Version
<input type="checkbox"/>	Ungrouped (1)		
<input checked="" type="checkbox"/>	FTD_HOME Snort 3 192.168.0.201 - Routed	FTDv for VMware	7.2.5

- 클릭 **Routing**
- 선택 **Policy Base Routing**
- 을 클릭합니다 **Add**

Policy Based Routing
Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across egress interfaces accordingly.

[Configure Interface Priority](#) [Add](#)

이 시나리오에서는 트래픽을 Secure Access로 라우팅하거나 RA-VPN 또는 클라이언트 기반 또는 브라우저 기반 ZTA 액세스를 사용하여 네트워크 내부 리소스에 대한 사용자 인증을 Secure Access에 제공하기 위해 소스로 사용하는 모든 인터페이스를 선택합니다.

- Ingress Interface(인그레스 인터페이스)에서 Secure Access를 통해 트래픽을 전송하는 모든 인터페이스를 선택합니다.

Edit Policy Based Route

A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*

LAN

- Match Criteria and Egress Interface(일치 기준 및 이그레스 인터페이스)에서 다음을 클릭한 후 다음 매개변수를 정의합니다 **Add**.

Match Criteria and Egress Interface
Specify forward action for chosen match criteria.

[Add](#)

Add Forwarding Actions

Match ACL:* Select... +

Send To:* IP Address

IPv4 Addresses: For example, 192.168.0.1, 10.10.1.2

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1

Don't Fragment: None

Internal Sources

Match ACL:* ACL

Send To:* IP Address

IPv4 Addresses: 169.254.2.2, 169.254.3.2

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1

Don't Fragment: None

- **Match ACL:** 이 ACL의 경우 보안 액세스에 라우팅하는 모든 항목을 구성합니다.

Traffic to the destination 208.67.222.222 or 208.67.220.220 over DNS using TCP or UDP will not be routed to Secure Access

✗ REJECT

Name: SSPT_FTD_ACL

Entries (2)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	Block	Any	Any	208.67.222.222 208.67.220.220	Any
2	Allow	192.168.10.0/24	Any	Any	Any

Traffic from the source 192.168.10.0/24 will be routed to Secure Access

Depends how you play with the ACL, you can define how the traffic must be routed to Secure Access

✓ ACCEPT

- **Send To:** IP 주소 선택
- **IPv4 Addresses:** 두 VTI에 모두 구성된 마스크 30에서 다음 IP를 사용해야 합니다. 이 단계에서 VTI [인터페이스](#) 컨피그레이션을 확인할 수 [있습니다](#)

인터페이스	IP	GW
기본 VTI	169.254.2.1/30	169.254.2.2
보조 VTI	169.254.3.1/30	169.254.3.2

IPv4 Addresses: For example, 192.168.0.1, 10.10.1.2 → 169.254.2.2, 169.254.3.2

이렇게 구성하면 다음 결과가 나타나고 **Save** 다음 클릭을 진행할 수 있습니다.

Match ACL:* **ACL** +

Send To:* **IP Address**

IPv4 Addresses: **169.254.2.2,169.254.3.2**

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1:

Don't Fragment: **None**

Default Interface

IPv4 settings IPv6 settings

Recursive: For example, 192.168.0.1

Default: For example, 192.168.0.1, 10.10.10.1

Peer Address

Verify Availability +

Cancel Save

그런 다음 다시 Save 구성해야 하며 다음 방법으로 구성됩니다.

A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*
LAN

Match Criteria and Egress Interface
 Specify forward action for chosen match criteria. Add

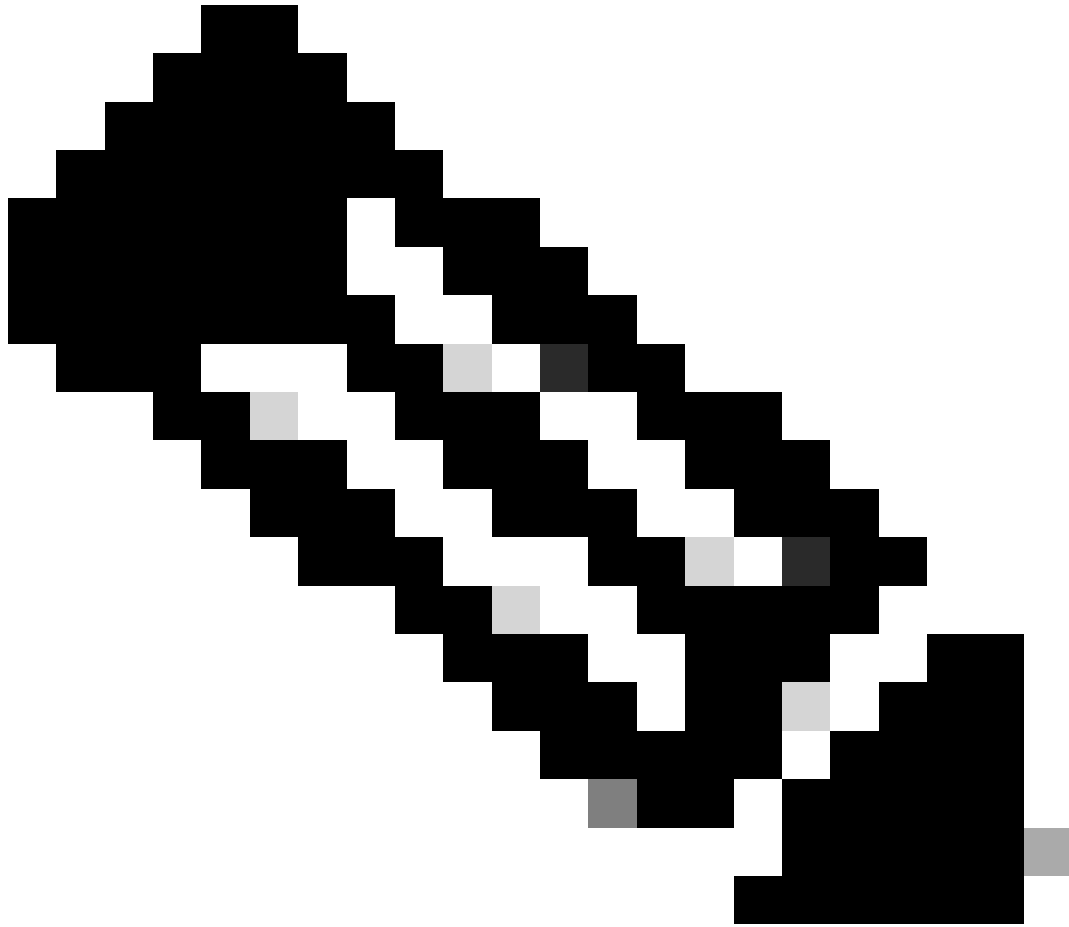
Match ACL	Forwarding Action	
ACL	Send through <div style="display: flex; align-items: center;"> <div style="border: 1px solid #0070c0; padding: 2px; margin-right: 5px;">169.254.2.2</div> <div style="border: 1px solid #0070c0; padding: 2px; margin-right: 5px;">169.254.3.2</div> <div style="margin-left: 10px;">→ Send the traffic to the PrimaryVTI</div> </div>	✎ 🗑️

↓
 If PrimaryVTI fail it will send the traffic to the SecondaryVTI

Cancel Save

그런 다음 Deploy(구축)를 수행할 수 있으며, ACL에서 Secure Access(보안 액세스)로 트래픽을 라우팅하도록 구성된 시스템의 트래픽을 볼 수 있습니다.

FMC의 **Conexion Events** 에서:



참고: 기본적으로 기본 보안 액세스 정책은 인터넷으로 향하는 트래픽을 허용합니다. 프라이빗 애플리케이션에 대한 액세스를 제공하려면 프라이빗 리소스를 생성하고 이를 프라이빗 리소스 액세스를 위한 액세스 정책에 추가해야 합니다.

보안 액세스에 대한 인터넷 액세스 정책 구성

인터넷 액세스에 대한 액세스를 구성하려면 [Secure Access](#) Dashboard(보안 액세스 대시보드)에 정책을 [생성해야 합니다](#).

- 클릭 `Secure > Access Policy`



Secure



Monitor



Admin



Workflows

Policy

Access Policy

Create rules to control and secure access to private and internet destinations

Data Loss Prevention Policy

Prevent data loss/leakage with policy rules

- 클릭 Add Rule > Internet Access

Add Rule ^

Private Access

Control and secure access to resources and applications that cannot be accessed by the general public.

Internet Access

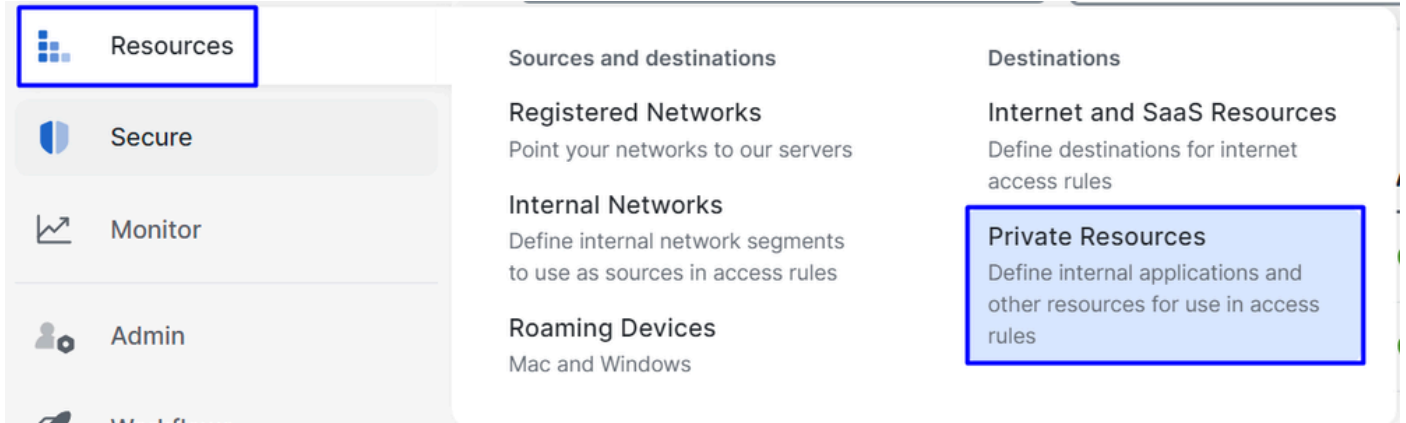
Control and secure access to public destinations from within your network and from managed devices

여기서 소스를 터널로 지정할 수 있으며, 정책에서 구성하려는 대상에 따라 대상에 대해 any를 선택할 수 있습니다. [Secure Access 사용 설명서를 확인하십시오.](#)

ZTNA 및 RA-VPN에 대한 프라이빗 리소스 액세스 구성

프라이빗 리소스에 대한 액세스를 구성하려면 먼저 [Secure Access Dashboard](#)(보안 액세스 대시보드)에서 리소스를 [생성해야 합니다](#).

클릭 **Resources > Private Resources**



- 그런 다음 ADD

컨피그레이션에서 구성할 다음 섹션을 찾습니다. **General, Communication with Secure Access Cloud and Endpoint Connection Methods.**

일반

General

Private Resource Name

Description (optional)

- Private Resource Name : 네트워크에 대한 보안 액세스를 통해 액세스를 제공하는 리소스의 이름을 만듭니다.

엔드포인트 연결 방법

Zero-trust connections
 Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

Client-based connection
 Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address) ⓘ

[+ FQDN or IP Address](#)

Browser-based connection
 Allow browser-based connections from endpoints that do not have the Secure Client installed. Enable this option when devices that your organization does not manage must connect to this resource. Fewer endpoint security checks are possible.

Public URL for this resource ⓘ
 https:// -8195126.ztna.sse.cisco.io

Protocol Server Name Indication (SNI) (optional) ⓘ

Validate Application Certificate ⓘ

- **Zero Trust Connections:** 확인란을 선택합니다.
- **Client-based connection:** 이를 활성화할 경우 Secure Client - Zero Trust Module을 사용하여 클라이언트 기반 모드를 통한 액세스를 활성화할 수 있습니다.
- **Remote Reachable Address (FQDN, Wildcard FQDN, IP Address) :** 리소스 IP 또는 FQDN을 구성합니다. fqdn을 구성하는 경우 이름을 확인하기 위해 DNS를 추가해야 합니다.
- **Browser-based connection:** 이 옵션을 활성화하면 브라우저를 통해 리소스에 액세스할 수 있습니다 (HTTP 또는 HTTPS 통신만 있는 리소스를 추가하십시오).
- **Public URL for this resource:** 브라우저를 통해 사용하는 공용 URL을 구성합니다. Secure Access는 이 리소스를 보호합니다.
- **Protocol:** 프로토콜(HTTP 또는 HTTPS)을 선택합니다

VPN connections
 Allow endpoints to connect to this resource when connected to the network using VPN.

VPN Connection: RA-VPNaaS를 통한 액세스를 활성화하려면 확인란을 선택합니다.

그런 다음 을 Save 클릭하면 해당 리소스에 추가할 수 있습니다Access Policy.

액세스 정책 구성

리소스를 생성할 때 보안 액세스 정책 중 하나에 할당해야 합니다.

- 클릭 Secure > Access Policy



Secure



Monitor



Admin



Workflows

Policy

Access Policy

Create rules to control and secure access to private and internet destinations

Data Loss Prevention Policy

Prevent data loss/leakage with policy rules

- 을 클릭합니다 Add > Private Resource

Add Rule ^

Private Access

Control and secure access to resources and applications that cannot be accessed by the general public.

Internet Access

Control and secure access to public destinations from within your network and from managed devices

이 Private Access 규칙의 경우 리소스에 대한 액세스를 제공하도록 기본값을 구성합니다. 정책 컨피그레이션에 대해 자세히 알아보려면 [User Guide\(사용 설명서\)](#)를 참조하십시오.

1 Specify Access

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

Action

<input checked="" type="radio"/> Allow Allow specified traffic if security requirements are met.	<input type="radio"/> Block Block specified traffic.
------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------

From

Specify one or more sources.

Information about sources, including selecting multiple sources. [Help](#)

To

Specify one or more destinations.

Information about destinations, including selecting multiple destinations. [Help](#)

- **Action** : 리소스에 대한 액세스를 제공하려면 Allow(허용)를 선택합니다.
- **From** : 리소스에 로그인하는 데 사용할 수 있는 사용자를 지정합니다.
- **To** : Secure Access를 통해 액세스하려는 리소스를 선택합니다.

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

<input type="checkbox"/> Zero-Trust Client-based Posture Profile Rule Defaults Requirements for end-user devices on which the Cisco Secure Client is installed. <input type="text" value="System provided (Client-based)"/>
Private Resources: SplunkFTD
<input type="checkbox"/> Zero Trust Browser-based Posture Profile Rule Defaults Requirements for end-user devices on which the Cisco Secure Client is NOT installed. <input type="text" value="System provided (Browser-based)"/>
Private Resources: SplunkFTD

- **Zero-Trust Client-based Posture Profile**: 클라이언트 기반 액세스를 위한 기본 프로필을 선택합니다
- **Zero-Trust Browser-based Posture Profile**: 기본 프로파일 브라우저 기본 액세스를 선택합니다.



참고: 상태 정책에 대해 자세히 알아보려면 Secure Access [사용 설명서](#)를 확인하십시오.

그런 다음 **Next** 및 **컨피그레이션Save** 을 클릭하고 RA-VPN 및 Client Base ZTNA 또는 Browser Base ZTNA를 통해 리소스에 액세스할 수 있습니다.

문제 해결

Secure Firewall과 Secure Access 간의 통신을 기반으로 문제를 해결하려면 Phase1(IKEv2) 및 Phase2(IPSEC)가 장치 간에 문제 없이 설정되었는지 확인할 수 있습니다.

1단계(IKEv2) 확인

1단계를 확인하려면 FTD의 CLI에서 다음 명령을 실행해야 합니다.

```
show crypto isakmp sa
```

이 경우 원하는 출력은 Secure Access의 데이터 센터 IP에 설정된 두 IKEv2 SAs 개이며 원하는 상태는 다음과 READY같습니다.

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
52346451 192.168.0.202/4500 3.120.45.23/4500
Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/4009 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0xfb34754c/0xc27fd2ba
```

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
52442403 192.168.30.5/4500 18.156.145.74/4500
Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3891 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0x4af761fd/0xfbca3343
```

2단계(IPSEC) 확인

2단계를 확인하려면 FTD의 CLI에서 다음 명령을 실행해야 합니다.

```
interface: PrimaryVTI
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.5

Protected vrf (ivrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 18.156.145.74

#pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965
#pkts decaps: 91325, #pkts decrypt: 91325, #pkts verify: 91325
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 71965, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.30.5/4500, remote crypto endpt.: 18.156.145.74/4500
path mtu 1500, ipsec overhead 63(44), media mtu 1500
```

PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: FBCA3343
current inbound spi : 4AF761FD

inbound esp sas:

spi: 0x4AF761FD (1257726461)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 2, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (3916242/27571)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0xFFFFFFFF 0xFFFFFFFF

outbound esp sas:

spi: 0xFBCA3343 (4224332611)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 2, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4239174/27571)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

interface: SecondaryVTI

Crypto map tag: __vti-crypto-map-Tunnel2-0-2, seq num: 65280, local addr: 192.168.0.202

Protected vrf (ivrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 3.120.45.23

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.0.202/4500, remote crypto endpt.: 3.120.45.23/4500
path mtu 1500, ipsec overhead 63(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: C27FD2BA
current inbound spi : FB34754C

inbound esp sas:

spi: 0xFB34754C (4214519116)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 20, crypto-map: __vti-crypto-map-Tunnel2-0-2
sa timing: remaining key lifetime (kB/sec): (4101120/27412)
IV size: 8 bytes

```

replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
outbound esp sas:
spi: 0xC27FD2BA (3263156922)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 20, crypto-map: __vti-crypto-map-Tunnel2-0-2
sa timing: remaining key lifetime (kB/sec): (4239360/27412)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

```

마지막 출력에서 두 터널이 모두 설정된 것을 볼 수 있습니다. 원하지 않는 것은 패킷encaps 및decaps 아래의 다음 출력입니다.

```

#pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965 → Packets forwarded to Secure Access
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0 → No packets forwarded from Secure Access to your firewall
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 71965, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

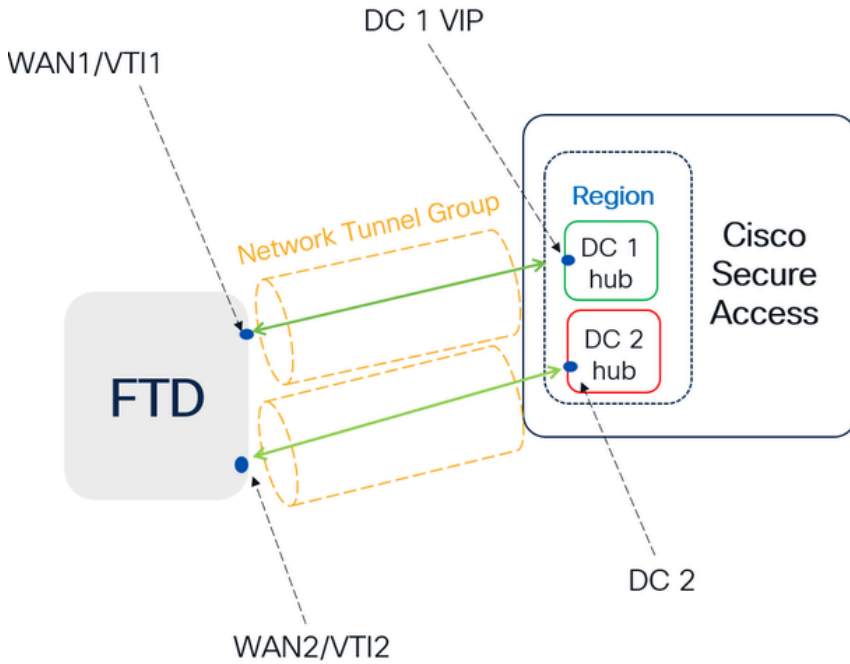
```

이 시나리오가 있는 경우 TAC에서 케이스를 여십시오.

고가용성 기능

클라우드의 데이터센터와 통신하는 Secure Access를 사용하는 터널의 기능은 액티브/패시브 방식입니다. 즉, 트래픽을 수신하기 위해 DC 1의 문만 열립니다. 1번 터널이 내려갈 때까지 dc 2 문이 닫힙니다.

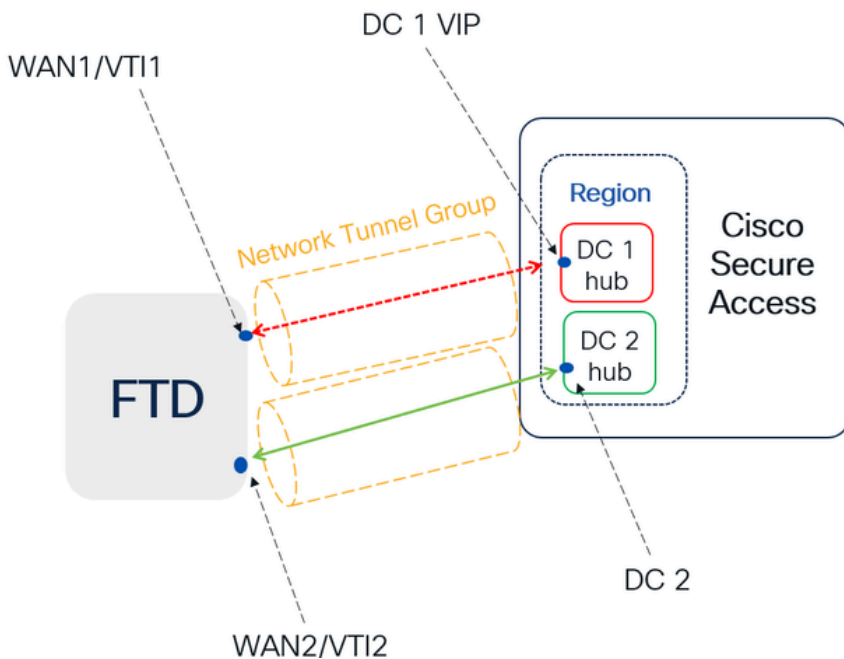
Normal Behavior



Secure Access default behavior

- DC2 is **passive** when DC1 is **active**
- Data Centers operating in High Availability (HA) mode ensure that only one tunnel receives traffic at a time. The other tunnel remains on standby and will drop any packets sent through it while in standby mode.

HA Behavior



Secure Access HA Behavior

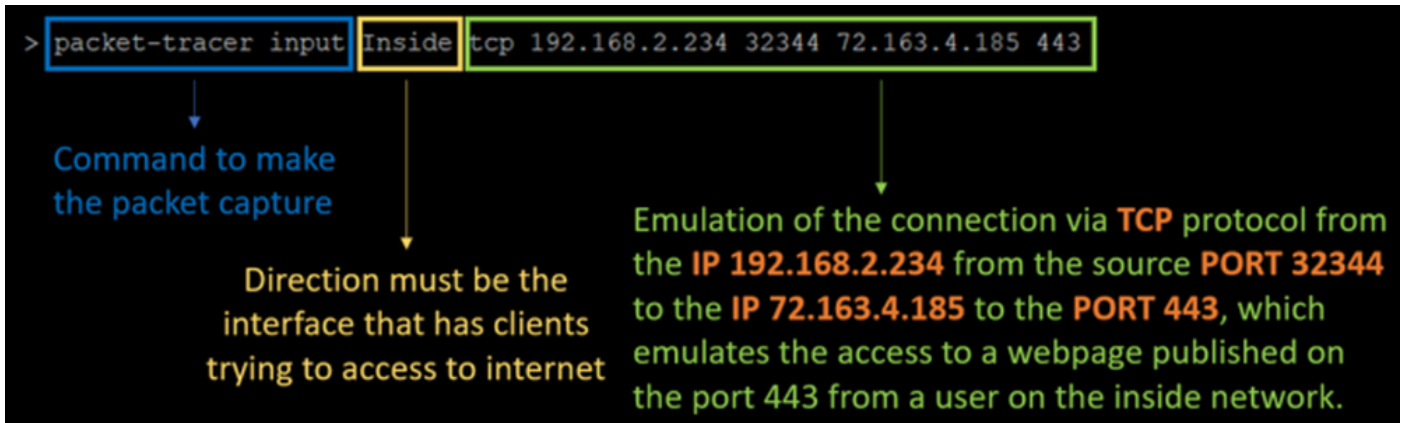
- DC2 is **Active** when DC1 or WAN1 peer is **Down**
- High availability is implemented to address failures in the WAN1 channel on the Firewall, ensuring operational continuity in the **region** and mitigating potential issues in DC1

보안 액세스에 대한 트래픽 라우팅 확인

이 예에서는 소스를 방화벽 네트워크의 시스템으로 사용합니다.

- 출처: 192.168.10.40
- 대상: 146.112.255.40(Secure Access Monitoring IP)

예:



명령을 사용합니다:

```
packet-tracer input LAN tcp 192.168.10.40 3422 146.112.255.40 80
```

성과:

```
Phase: 1  
Type: ACCESS-LIST  
Subtype:  
Result: ALLOW  
Elapsed time: 14010 ns  
Config:  
Implicit Rule  
Additional Information:  
MAC Access list
```

```
Phase: 2  
Type: PBR-LOOKUP  
Subtype: policy-route  
Result: ALLOW  
Elapsed time: 21482 ns  
Config:  
route-map FMC_GENERATED_PBR_1707686032813 permit 5  
  match ip address ACL  
  set ip next-hop 169.254.2.2 169.254.3.2  
Additional Information:  
  Matched route-map FMC_GENERATED_PBR_1707686032813, sequence 5, permit  
  Found next-hop 169.254.2.2 using egress ifc PrimaryVTI
```

```
Phase: 3  
Type: OBJECT_GROUP_SEARCH  
Subtype:  
Result: ALLOW  
Elapsed time: 0 ns  
Config:  
Additional Information:  
  Source Object Group Match Count: 0  
  Destination Object Group Match Count: 0
```

Object Group Search: 0

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Elapsed time: 233 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any ifc PrimaryVTI any rule-id 268434435
access-list CSM_FW_ACL_ remark rule-id 268434435: ACCESS POLICY: HOUSE - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434435: L7 RULE: New-Rule-#3-ALLOW
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Elapsed time: 233 ns
Config:
class-map class_map_Any
match access-list Any
policy-map policy_map_LAN
class class_map_Any
set connection decrement-ttl
service-policy policy_map_LAN interface LAN
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 233 ns
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 233 ns
Config:
Additional Information:

Phase: 8
Type: VPN
Subtype: encrypt
Result: ALLOW
Elapsed time: 18680 ns
Config:
Additional Information:

Phase: 9
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Elapsed time: 25218 ns
Config:
Additional Information:

Phase: 10

Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 14944 ns
Config:
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 0 ns
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 19614 ns
Config:
Additional Information:
New flow created with id 23811, packet dispatched to next module

Phase: 13
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 27086 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 14
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 28820 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Phase: 15
Type: SNORT
Subtype: firewall
Result: ALLOW
Elapsed time: 450193 ns
Config:
Network 0, Inspection 0, Detection 0, Rule ID 268434435
Additional Information:
Starting rule matching, zone 1 -> 3, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt: 0,
Matched rule ids 268434435 - Allow

Result:
input-interface: LAN(vrfid:0)
input-status: up
input-line-status: up
output-interface: PrimaryVTI(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 620979 ns

여기에는 통신에 대한 컨텍스트를 제시하고 트래픽을 Secure Access로 올바르게 라우팅하기 위해 PBR 컨피그레이션에서 모든 것이 올바르게 되어 있는지 알 수 있는 여러 가지 기능이 있습니다.

```
Phase: 2
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 21482 ns
Config:
route-map FMC_GENERATED_PBR_1707686032813 permit 5
  match ip address ACL
  set ip next-hop 169.254.2.2 169.254.3.2
Additional Information:
  Matched route-map FMC_GENERATED_PBR_1707686032813, sequence 5, permit
  Found next-hop 169.254.2.2 using egress ifc PrimaryVTI
```

2단계는 트래픽이 인터페이스로 전달되고 있음을 나타냅니다. 이 시나리오의 컨피그레이션에 PrimaryVTI 따르면 인터넷 트래픽은 VTI를 통해 Secure Access로 전달되어야 하므로 올바른 것입니다.

Phase: 8

Type: VPN

Subtype: encrypt

Result: ALLOW

Elapsed time: 18680 ns

Config:

Additional Information:

Phase: 9

Type: VPN

Subtype: ipsec-tunnel-flow

Result: ALLOW

Elapsed time: 25218 ns

Config:

Additional Information:

연결의 암호화 단계에 해당하며, 이 단계에서 트래픽은 암호화를 위해 평가되고 인증되므로 데이터를 안전하게 전송할 수 있습니다. 반면, 9단계에서는 VPN IPSec 터널 내 트래픽 흐름의 특정 관리에 중점을 두어, 암호화된 트래픽이 적절하게 라우팅되고 설정된 터널을 통해 허용됨을 확인합니다

Result:

```
input-interface: LAN(vrfid:0)
```

```
input-status: up
```

```
input-line-status: up
```

```
output-interface: PrimaryVTI(vrfid:0)
```

```
output-status: up
```

```
output-line-status: up
```

```
Action: allow
```

```
Time Taken: 620979 ns
```

마무리를 위해 플로우 결과가 끝날 때에서 Secure Access로 트래픽을 전달하는 LAN 트래픽 PrimaryVTI을 볼 수 있습니다. 이 작업은 allow 트래픽이 문제 없이 라우팅됨을 확인합니다.

관련 정보

- [Cisco 기술 지원 및 다운로드](#)
- [Cisco Secure Access Help Center](#)
- [Virtual Trusted Platform 모듈 개요](#)
- [제로 트러스트 액세스 모듈](#)
- [보안 액세스 오류 트러블슈팅 "등록 서비스가 응답하지 않습니다. IT 헬프 데스크에 문의"](#)

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.