

NAT를 통한 프라이빗 액세스를 위해 보안 FTD 및 ASA를 통한 보안 액세스 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[네트워크 다이어그램](#)

[구성](#)

[보안 액세스 및 보안 방화벽 스택드 방어 - PBR을 사용하는 BGP\(Dynamic\) 경로 기반 VPN](#)

[FTD 정책 기반 라우팅](#)

[FTD에서 BGP 구성](#)

[터널 상태 확인](#)

[PBR로 ASA\(Adaptive Security Appliance\)에서 고정 경로 기반 IPsec VPN 구성](#)

[보안 액세스에 대한 VPN 구성](#)

[ASA의 VPN 컨피그레이션](#)

[정책 기반 라우팅](#)

[다음을 확인합니다.](#)

소개

이 문서에서는 NAT(Network Address Translation)를 사용하여 보안 액세스 네트워크 터널 그룹을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco 방화벽 관리 센터
- Cisco Secure Firewall 위협 방어
- Cisco 보안 액세스
- Cisco Adaptive Security Appliance

- 네트워크 주소 변환
- 정책 기반 라우팅
- 방화벽의 패킷 캡처

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

- Cisco Firewall Management Center 7.10
- Cisco Secure Firewall Threat Defense 7.10
- Cisco 보안 액세스
- Cisco ASA 9.22
- Cisco 라우터

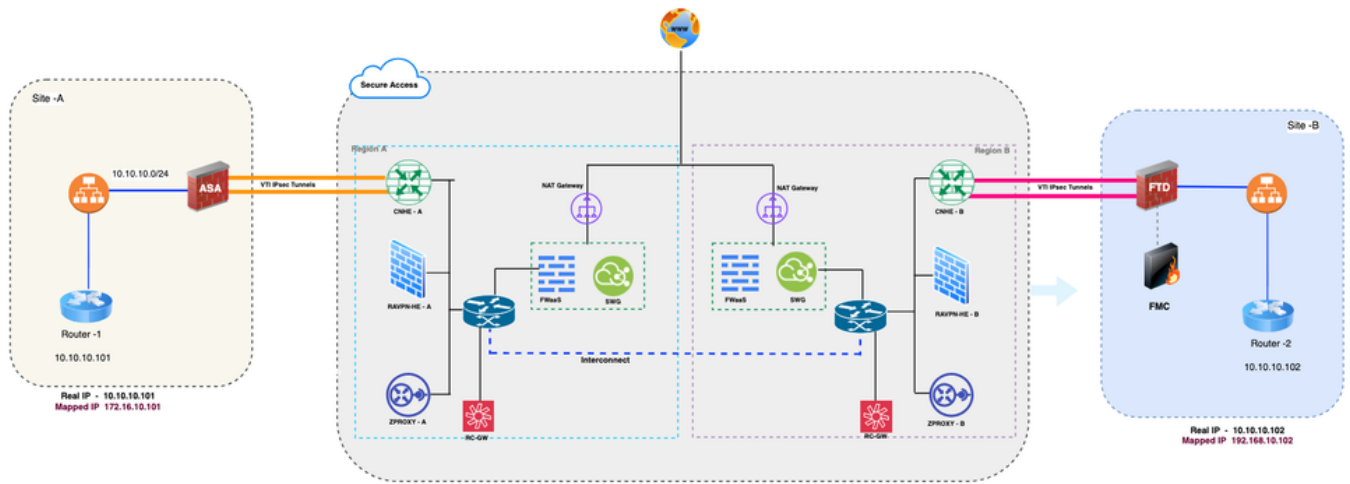
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Cisco Secure Access는 SIA(Secure Internet Access) 및 SPA(Secure Private Access)를 비롯한 클라우드 네이티브 Secure Service Edge 기능을 제공합니다. 데이터 센터를 통해 모든 트래픽을 백홀하지 않고 프라이빗 애플리케이션 액세스를 원격 사용자에게 확장하는 조직의 경우, Secure Access는 IPsec NTG(Network Tunnel Group)를 사용하여 Cisco FTD(Firewall Threat Defense), ASA(Adaptive Security Appliance), Cisco Secure Access 클라우드 PoP(Points-of-Presence)와 같은 온프레미스 네트워크 디바이스 간에 암호화된 터널을 생성합니다.

이 문서에서는 Cisco FTD, ASA와 Cisco Secure Access 간에 IKEv2를 사용하여 경로 기반 IPsec 터널을 설정하여 보안 액세스에 NAT(Network Address Translation)를 활성화하고 FTD 및 ASA의 PBR(Policy-Based Routing)에서 프라이빗 액세스 바인딩 트래픽만 터널로 이동하는 방법에 대해 자세히 설명합니다.

네트워크 다이어그램



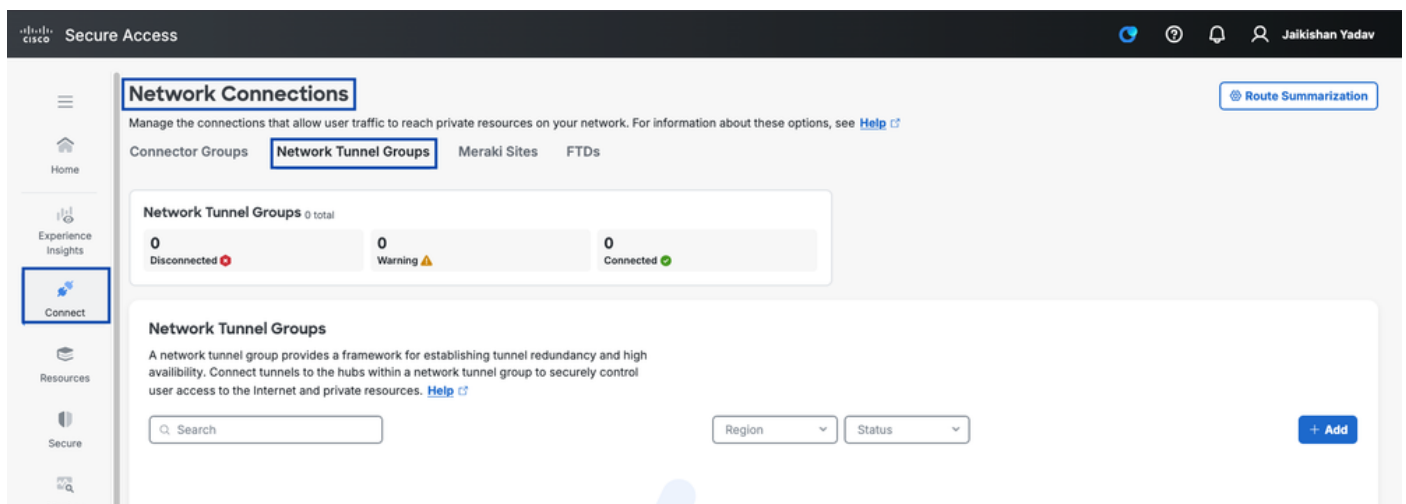
네트워크 토폴로지

구성

보안 액세스 및 보안 방화벽 스택드 방어 - PBR을 사용하는 BGP(Dynamic) 경로 기반 VPN

보안 액세스에서 네트워크 터널 그룹 구성

1. Secure Access 대시보드에 로그인 [Secure Access](#)
2. Connect(연결) > Network Connections(네트워크 연결) > Network Tunnel Groups(네트워크 터널 그룹)로 이동하고 +Add(추가)를 클릭하여 네트워크 터널 그룹을 구성합니다



보안 액세스 - 네트워크 터널 그룹

3. 네트워크 터널 그룹 구성 - 일반 설정

- 터널 그룹 이름, 영역 및 디바이스 유형 구성
- Next(다음)를 클릭합니다.

The screenshot shows the 'Add a Network Tunnel Group' configuration page. The left sidebar has four tabs: 'General Settings' (selected), 'Tunnel ID and Passphrase', 'Routing', and 'Data for Tunnel Setup'. The main content area is titled 'General Settings' and contains the following fields: 'Tunnel Group Name' (text input with 'FTD-BGP'), 'Region' (dropdown menu with 'US (Pacific Northwest)'), and 'Device Type' (dropdown menu with 'FTD'). At the bottom right is a 'Next' button.

보안 액세스 - 네트워크 터널 그룹 일반 설정

4. 터널 ID 및 암호를 구성합니다.

- 터널 ID 및 암호를 구성합니다.
- Next(다음)를 클릭합니다

The screenshot shows the 'Add a Network Tunnel Group' configuration page, specifically the 'Tunnel ID and Passphrase' tab. The left sidebar has four tabs: 'General Settings', 'Tunnel ID and Passphrase' (selected), 'Routing', and 'Data for Tunnel Setup'. The main content area is titled 'Tunnel ID and Passphrase' and contains the following fields: 'Tunnel ID Format' (radio buttons for 'Email' and 'IP Address', with 'Email' selected), 'Tunnel ID' (text input with 'ftdbgpvpn' and a placeholder '@<org><hub>.sse.cisco.com'), 'Passphrase' (password input with a 'Show' button), and 'Confirm Passphrase' (password input with a 'Show' button'). At the bottom right are 'Back' and 'Next' buttons.

5. 라우팅 구성

- 디바이스 AS 번호 구성
- Save(저장)를 클릭합니다.

The screenshot displays the 'Routing' configuration page. On the left, a sidebar shows three steps: 'Tunnel ID and Passphrase', 'Routing' (selected), and 'Data for Tunnel Setup'. The main content area is titled 'Internet Protocol Version Setting for Routing'. It includes a checkbox for 'Enable IPv6 Routing in addition to IPv4' (unchecked) with a note 'IPv4 is enabled by default.' Below this is the 'Routing option' section with two radio buttons: 'Static routing' (unchecked) and 'Dynamic routing' (checked). A description for 'Dynamic routing' states: 'Use this option when you have a BGP peer for your on-premise router.' Underneath is the 'Device AS Number' field, which contains the value '65010'. At the bottom, there is an 'Advanced Settings' section with three checkboxes: 'Multihop BGP' (unchecked), 'Override BGP route summarization' (unchecked), and 'Block default route advertisement' (unchecked). Navigation buttons at the bottom include a back arrow, 'Cancel', 'Back', and 'Save'.

6. 네트워크 터널 그룹 컨피그레이션 저장

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

- ✓ 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:	ftdbgpvpn@		
Primary Data Center IP Address:	44.228.138.150	2603:5004:13:20e::110:1	
Secondary Tunnel ID:	ftdbgpvpn@		
Secondary Data Center IP Address:	52.35.201.56	2603:5004:13:20c::110:1	
Passphrase:			

Download CSV

Done

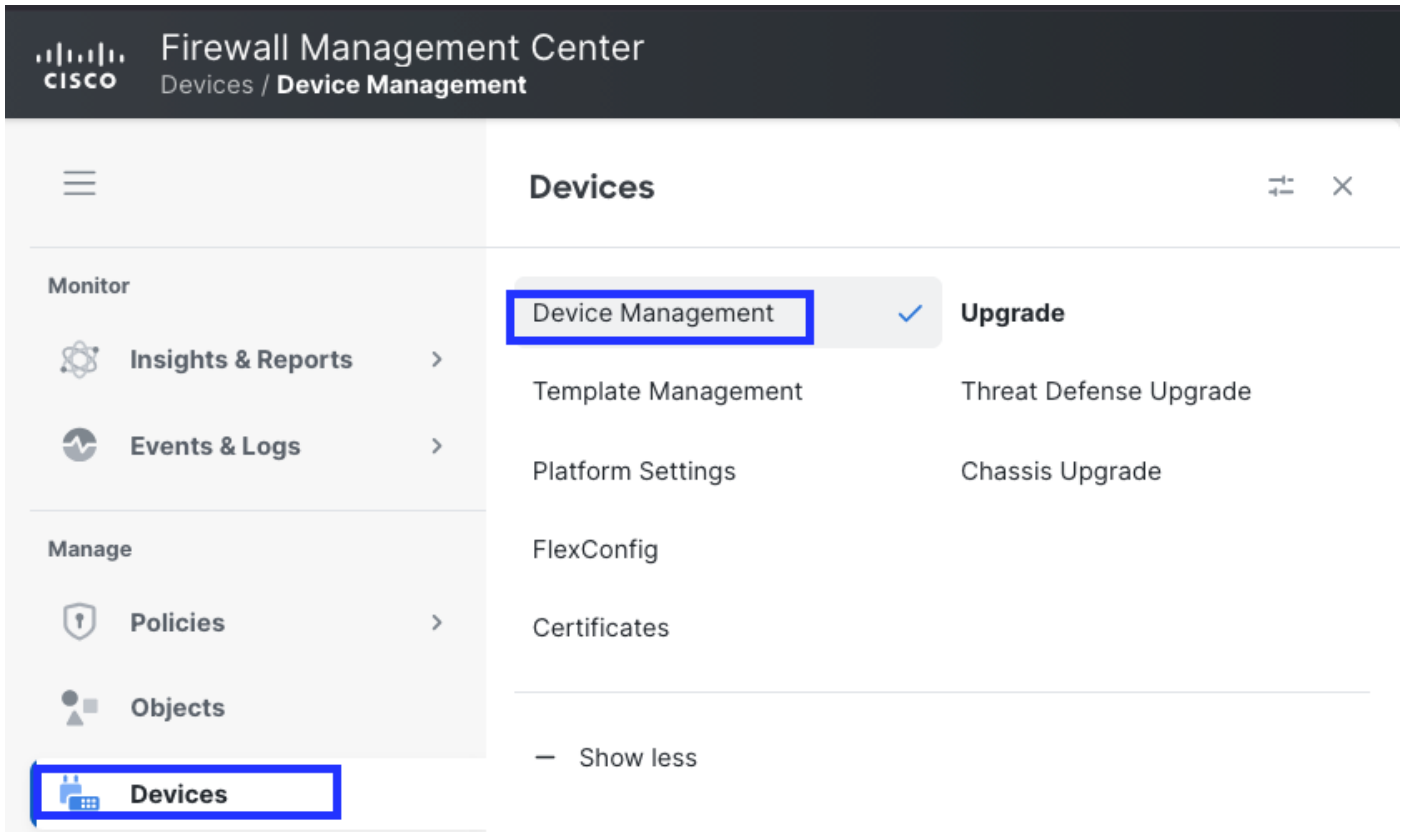
보안 액세스 - 네트워크 터널 그룹

PBR로 FTD(Secure Firewall Threat Defense)에서 동적 경로 기반 IPsec VPN 구성

1. FMC(Firewall Management Center)에 로그인

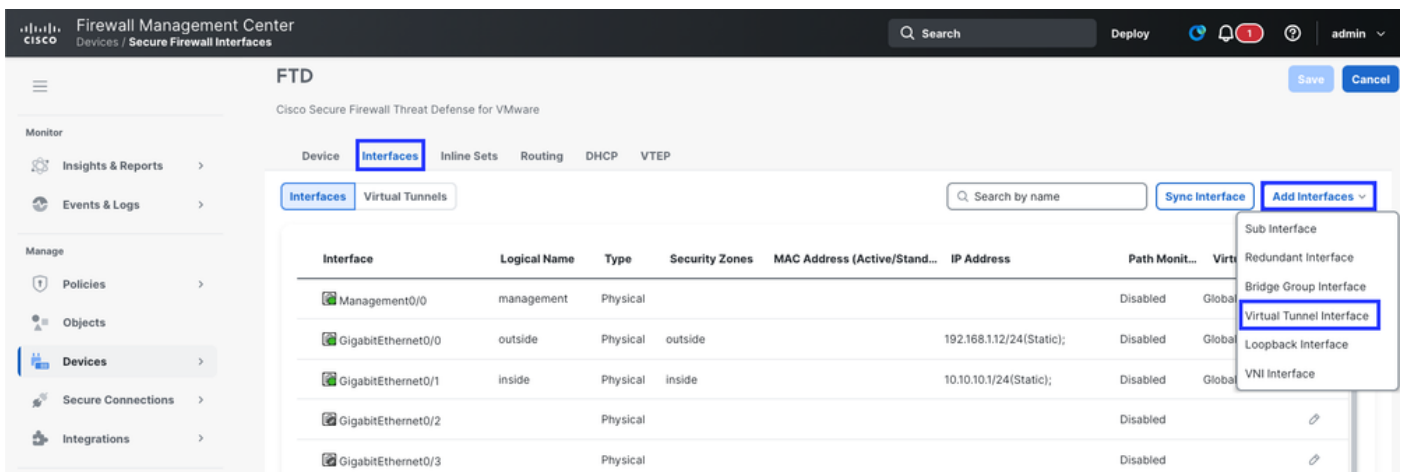
2. 가상 터널 인터페이스 VTI [구성](#)

- Devices(디바이스) > Device Management(디바이스 관리)로 이동합니다



보안 방화벽 관리 - 대시보드

- 디바이스 옆의 연필 아이콘을 클릭하고 Interface(인터페이스) 섹션으로 이동합니다
- Add interfaces(인터페이스 추가)를 클릭하고 Virtual Tunnel Interface(가상 터널 인터페이스)를 선택합니다



보안 방화벽 관리 - FTD VTI 컨피그레이션

- VTI 구성

Add Virtual Tunnel Interface



General

Path Monitoring

Tunnel Type

☒ Static ☐ Dynamic

Name:*

VTI-1

☒ Enabled

Description:

Virtual Tunnel interface for
Primary VTI VPN

Security Zone:

vti

Priority:

0

(0 - 65535)

Propagate Security Group Tag: ☒

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)

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:*

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (outside) ▾

192.168.1.12 ▾

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

☐ Borrow IP (IP unnumbered)

▾

+

Cancel

OK

보안 방화벽 관리 - FTD VTI 컨피그레이션

- 보안 액세스를 통해 보조 IPsec VPN에 대해서도 VTI-2를 구성합니다.

FTD

Cisco Secure Firewall Threat Defense for VMware

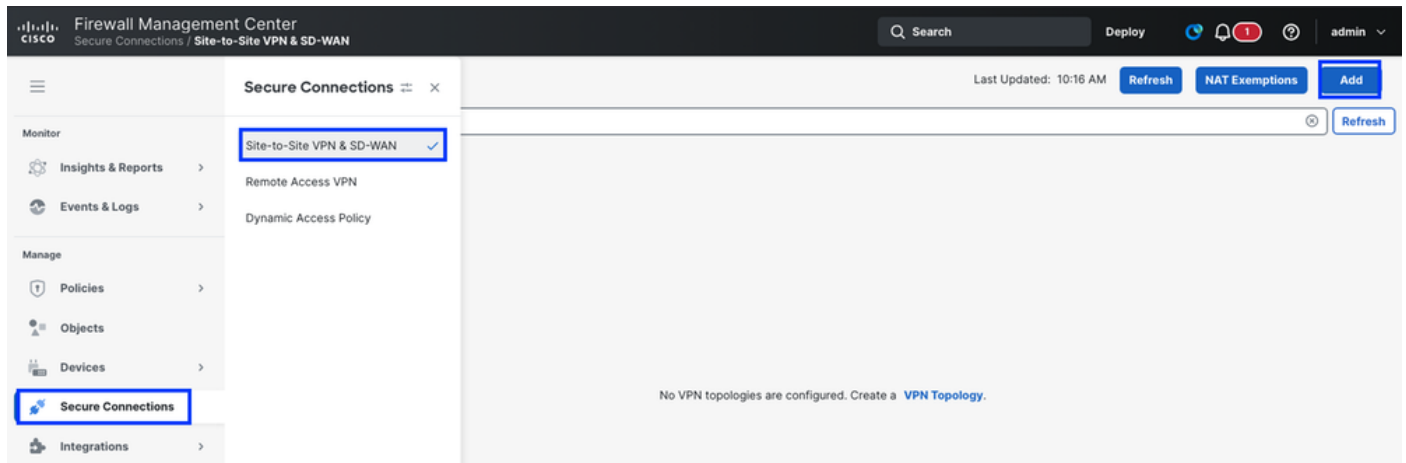
Device Interfaces Inline Sets Routing DHCP VTEP

Interfaces Virtual Tunnels

Search by name Sync Interface Add Interfaces ▾

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Stand...	IP Address	Path Monit...	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	outside	Physical	outside		192.168.1.12(Static);	Disabled	Global
Tunnel1	VTI-1	VTI	vti		169.254.2.1/30(Static);	Disabled	Global
Tunnel2	VTI-2	VTI	vti		169.254.2.5/30(Static);	Disabled	Global
GigabitEthernet0/1	inside	Physical	inside		10.10.10.1/24(Static);	Disabled	Global

3. Secure Connections(보안 연결) > Site-to-Site VPN & SD-WAN(사이트 대 사이트 VPN 및 SD-WAN)으로 이동하고 Add(추가)를 클릭하여 VPN을 구성합니다



보안 방화벽 관리 - FTD VPN 구성

- VPN 토폴로지 생성

Create VPN Topology

Topology Name *

SecureAccess-VPN-Primary

VPN Type

☐ SD-WAN Topology

Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.

Select VPN Topology

☐ Hub and Spoke

Prerequisites

☒ Route-Based VPN

Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.

Select VPN Topology

☐ Hub and Spoke

☒ Peer to Peer

☐ Policy-Based VPN

Secures traffic between peers based on a static policy using protected networks.

Select VPN Topology

☐ Hub and Spoke

☐ Peer to Peer

☐ Full Mesh

☐ SASE Topology

Warning: SASE Topology cannot be selected because Cisco Umbrella Connection is not configured.

Prerequisites

Refresh

Cancel

Create

보안 방화벽 관리 - FTD VPN 구성

- Configure Network Tunnel Group on Secure Access(보안 액세스에 네트워크 터널 그룹 구성

)의 6단계에서 기본 및 보조 데이터 센터의 터널 ID 및 IP 주소를 가져옵니다.

- Endpoints(엔드포인트) 클릭
- Node A(노드 A) 아래에서 Device(디바이스)를 클릭하고 FTD 디바이스를 선택합니다
- Virtual Tunnel Interface(가상 터널 인터페이스)를 클릭하고 이전 단계에서 생성한 첫 번째 VTI 인터페이스를 선택합니다
- Send Local Identity to Peers(피어에 로컬 ID 보내기) 옵션을 클릭하고 Email ID(이메일 ID)를 선택하고 Configure Network Tunnel Group on Secure Access(보안 액세스에서 네트워크 터널 그룹 구성) 아래의 "Save Network Tunnel Group Configuration(네트워크 터널 그룹 컨피그레이션 저장)"에서 기본 터널 ID를 입력합니다
- Node B(노드 B) 아래에서 Device(디바이스)를 클릭하고 Extranet(엑스트라넷)을 선택합니다
- Device Name(디바이스 이름)을 클릭하고 이름을 지정합니다.
- 엔드포인트 IP 주소를 클릭하고 쉼표로 구분된 보안 액세스 기본 및 보조 IP 주소를 입력합니다("Configure Network Tunnel Group Configuration(네트워크 터널 그룹 컨피그레이션 저장)" 아래의 Configure Network Tunnel Group(보안 액세스에서 네트워크 터널 그룹 구성))
- Add Backup VTI(백업 VTI 추가)를 클릭합니다
- Virtual Tunnel Interface(가상 터널 인터페이스)를 클릭하고 이전 단계에서 생성한 두 번째 VTI 인터페이스를 선택합니다
- Send Local Identity to Peers(피어에 로컬 ID 보내기) 옵션을 클릭하고 Email ID(이메일 ID)를 선택하고 Configure Network Tunnel Group on Secure Access(보안 액세스에서 네트워크 터널 그룹 구성) 아래의 "Save Network Tunnel Group Configuration(네트워크 터널 그룹 컨피그레이션 저장)"에서 보조 터널 ID를 입력합니다
- Save(저장)를 클릭합니다

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map)

☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*



IKEv1



IKEv2

Endpoints

IKE

IPsec

Advanced

Node A

Device:*

FTD

Virtual Tunnel Interface:*

VTI-1 (IP: 169.254.2.1)



Tunnel Source: outside (IP: 192.168.1.12) [Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration:*

Email ID

ftdbgpvpn(

Node B

Device:*

Extranet

Device Name:*

Secure Access

Endpoint IP Address:*

44.228.138.150,52.35.201.56

Cancel

Save

보안 FTD - VPN 엔드포인트 컨피그레이션

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map)

☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐ IKEv1

☒ IKEv2

Endpoints

IKE

IPsec

Advanced

Backup VTI:

[Remove](#)

Virtual Tunnel Interface:*

VTI-2 (IP: 169.254.2.5)



Tunnel Source: outside (IP: 192.168.1.12) [Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration:*

Email ID

tdbgpvpn@

22-

Additional
Configuration



Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [AC Policy](#)

Cancel

Save

보안 FTD - VPN 엔드포인트 컨피그레이션

- 지원되는 IPsec 매개변수에 따라 IKEv2 [설정 구성](#)
 - Policies as Umbrella-AES-GCM-256(정책을 Umbrella-AES-GCM-256으로 선택)
 - 사전 공유 수동 키로 인증 유형 선택

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*



IKEv1



IKEv2

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

Cancel

Save

보안 FTD - VPN IKE 설정

- IPsec 설정 구성
 - IKEv2 IPsec Proposals as Umbrella-AES-GCM-256(Umbrella-AES-GCM-256으로 IKEv2 IPsec 제안 선택)
 - PFS를 Modulus Group(모듈러스 그룹)을 20으로 선택합니다.

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map)

☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐ IKEv1

☒ IKEv2

Endpoints

IKE

IPsec

Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha

Umbrella-AES-GCM-...

☐ Enable Security Association (SA) Strength Enforcement

☒ Enable Perfect Forward Secrecy

Modulus Group:

20

Cancel

Save

보안 FTD - VPN IPsec 설정

- 고급 설정
- Save(저장)를 클릭합니다.

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

☒ Point to Point ☐ Hub and Spoke ☐ Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec **Advanced**

IPsec

Tunnel

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

Cancel

Save

보안 FTD - VPN 고급 설정

FTD 정책 기반 라우팅

기존 라우팅에서는 패킷이 대상 IP 주소를 기반으로 라우팅됩니다. 목적지 기반 라우팅 시스템에서 특정 트래픽의 라우팅을 변경하는 것은 어렵습니다. PBR(Policy Based Routing)은 라우팅 프로토콜에서 제공하는 메커니즘을 확장 및 보완하여 더 효과적으로 라우팅을 제어합니다.

PBR을 사용하면 IP 우선 순위를 설정할 수 있습니다. 또한 특정 트래픽에 대한 경로(예: 고비용 링크의 우선순위 트래픽)를 지정할 수도 있습니다. PBR을 사용하면 소스 포트, 대상 주소, 대상 포트, 프로토콜, 애플리케이션 또는 이러한 객체의 조합과 같은 대상 네트워크 이외의 기준을 기반으로 하는 라우팅을 정의할 수 있습니다. 자세한 내용은 [정책 기반 라우팅을 참조하십시오](#)

1. 액세스 목록 구성

- Objects(개체) > Access List(액세스 목록) > Extended(확장)로 이동합니다.

- Add Extended Access List(확장 액세스 목록 추가)를 클릭합니다.



- 액세스 목록 이름 지정
- 작업 정의
 - 허용. - 정의된 트래픽이 IPsec 터널로 전송됩니다.
 - 차단 - 트래픽이 IPsec 터널에서 우회됨
 - 규칙은 시퀀스 번호를 기준으로 일치합니다(아래부터 위로).
 - Add를 클릭합니다.
 - Save(저장)를 클릭합니다.

Add Extended Access List Entry ?

Action:
Allow

Logging:
Default

Log Level:
Informational

Log Interval:
300 Sec.

Network Port Application Users Security Group Tag

Available Networks +

10.10.10.
obj_10.10.10.0

Add to Source
Add to Destination

Source Networks (1)

obj_10.10.10.0

Destination Networks (0)

any

Cancel Add

New Extended Access List Object



Name
PBR

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Allow	obj_10.10.10.0	Any	Any	Any	Any	Any	

Displaying 1 - 1 of 1 rows < < Page 1 of 1 > >

☐ Allow Overrides

Cancel Save

보안 FTD - 확장 액세스 목록

2. 정책 기반 라우팅 구성

- Devices(디바이스) > Device Management(디바이스 관리) > FTD > Routing(라우팅)으로 이동합니다.

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The left sidebar contains a navigation menu with 'Devices' highlighted. The main content area is titled 'FTD' and 'Cisco Secure Firewall Threat Defense for VMware'. The 'Routing' tab is selected, showing 'Virtual Router Properties'. The 'Manage Virtual Routers' section has a dropdown set to 'Global'. The 'Virtual Router Properties' section includes fields for 'VRF Name' (Global), 'Description' (This is a Global Virtual Router), and 'Select Interface'. The 'Available Interfaces' list includes 'outside', 'inside', 'management', 'VTI-1', and 'VTI-2'. The 'Selected Interfaces' list includes 'outside', 'VTI-1', 'inside', 'management', and 'VTI-2'. The 'Add' button is visible between the two lists.

보안 FTD - 정책 기반 라우팅

- Add(추가)를 클릭합니다
- 액세스 목록에 정의된 서브넷에 대한 Ingress Interface - Ingress 인터페이스를 선택합니다.

Add Policy Based Route



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

Ingress Interface *

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

There are no forward-actions defined yet. Start by [defining the first one](#).

Cancel

Save

보안 FTD - 정책 기반 라우팅

- 일치 기준 및 이그레스 인터페이스 정의
 - Add를 클릭합니다.
 - Match ACL(ACL 일치)을 선택합니다.
 - Send to as IP address를 선택합니다.
 - Next hop IP 주소를 추가합니다. - VTI 인터페이스 IP 주소는 입니다. 169.254.2.130 및 169.254.2.5/30. 따라서 VTI -1 및 VTI-2의 다음 홉 IP 주소는 169.254.2.2 및 입니다. 각각 169.254.2.6
 - Save(저장)를 클릭합니다.

Add Forwarding Actions

Match ACL: * +

Send To: *

IPv4 Addresses:

IPv6 Addresses:

Don't Fragment:

☐ Default Interface

IPv4 settings

IPv6 settings

Recursive:

Default:

☐ Peer Address

Cancel

Save

보안 FTD - 정책 기반 라우팅

FTD

Cisco Secure Firewall Threat Defense for VMware

You have unsaved changes

Save

Cancel

Device Interfaces Inline Sets **Routing** DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

✓ BGP

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

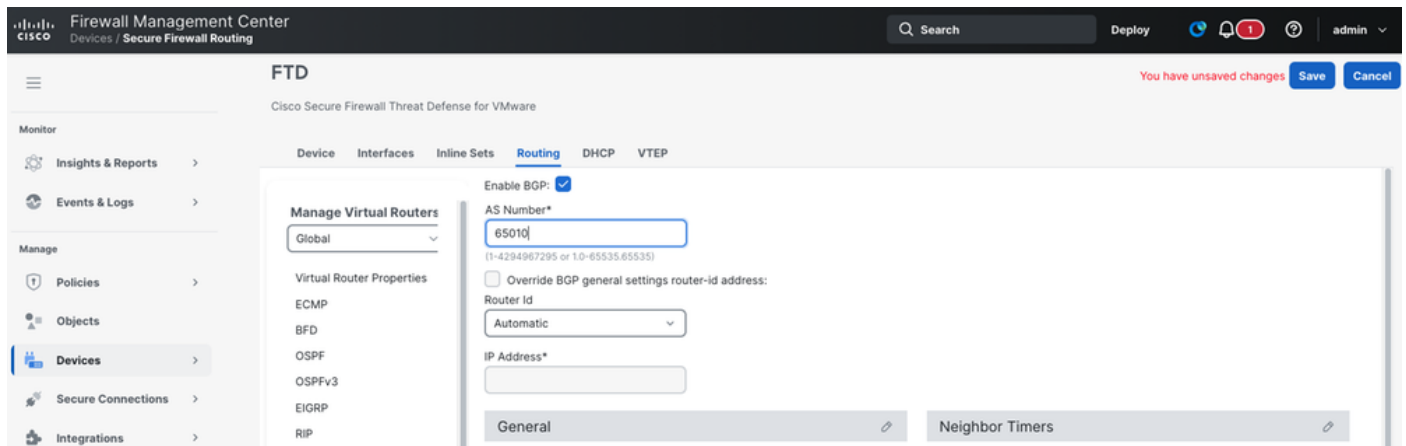
Ingress Interfaces	Match criteria and forward action		
inside	If traffic matches the Access List PBR	Send through 169.254.2.2 169.254.2.6	 

보안 FTD - 정책 기반 라우팅

FTD에서 BGP 구성

1. BGP 활성화

- Devices(디바이스) > Device Management(디바이스 관리) > FTD > Routing(라우팅) > General Settings(일반 설정) > BGP로 이동합니다
- BGP를 활성화하고 AS 번호(FTD 로컬 AS 번호)를 추가합니다.
- Save(저장)를 클릭합니다.



보안 FTD - BGP 라우팅

- BGP > IPv4로 이동합니다.

2. BGP 네이버 추가 - 보안 액세스 BGP 피어는 169.254.0.5 이상입니다. 169.254.0.9

Add Neighbor



IP Address*

169.254.0.5

Remote AS*

64512

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☐ Allow connections with neighbor that is not directly connected

☒ Limited number of TTL hops to neighbor

TTL Hops

254

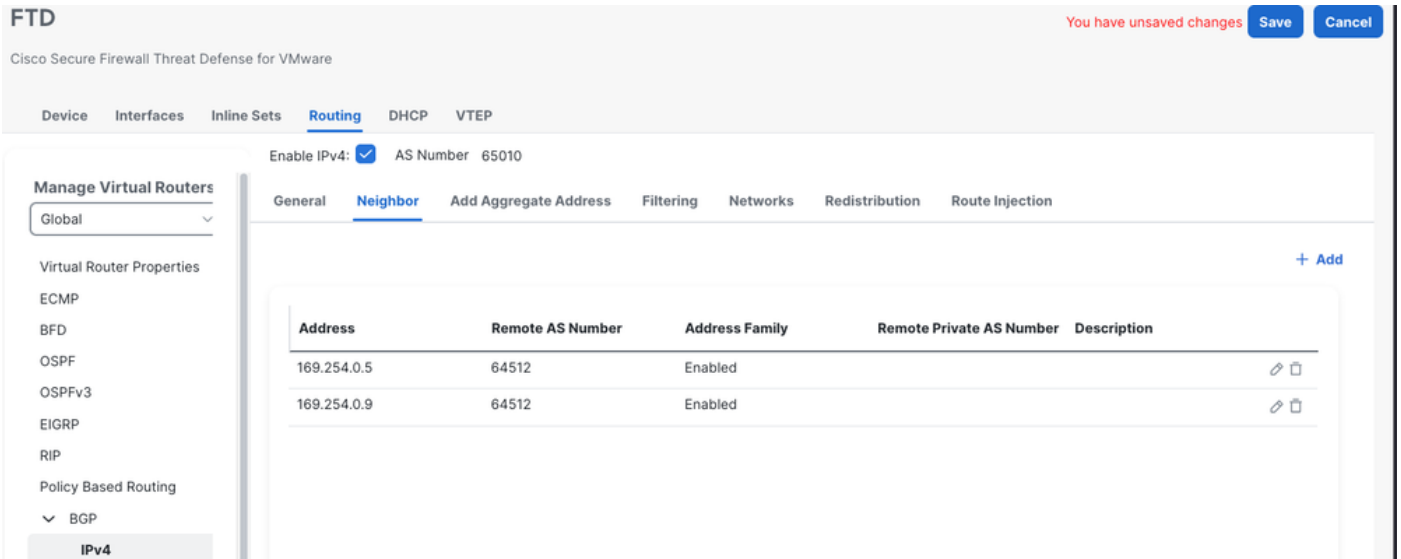
(1-254)

☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

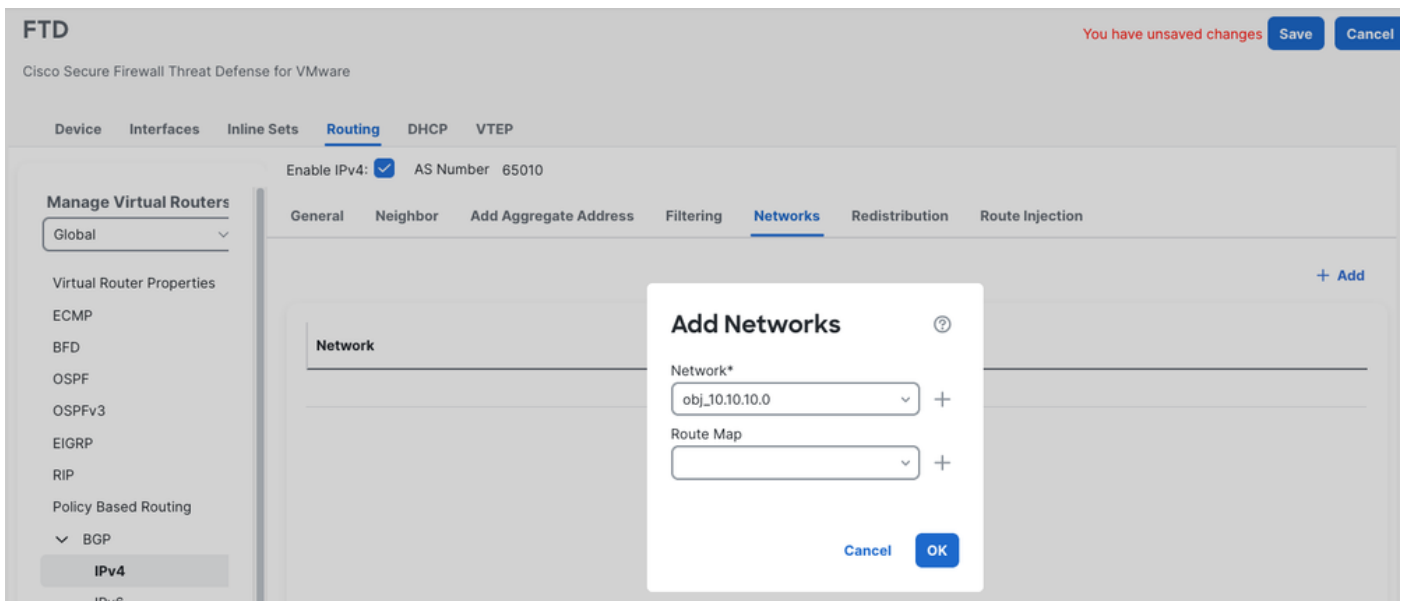
OK



보안 FTD - BGP 라우팅

3. 네트워크 추가 - 보안 액세스를 위해 광고해야 하는 네트워크

- OK(확인)를 클릭합니다.



보안 FTD - BGP 라우팅

- 변경 사항 저장 및 배포

터널 상태 확인

보안 액세스에서

The screenshot shows the Cisco Secure Access interface. The main section is titled "FTD-BGP" and shows a "Summary" of the Auto VPN tunnels. The status is "Connected". The configuration details include:

Region	US (Pacific Northwest)	Routing Type	Dynamic Routing (BGP)
Device Type	FTD	Device BGP AS	65010
Last Status Update	Jun 08, 2026 3:53 AM	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	—

Below the summary, there are two sections for "Primary Tunnel Hub" and "Secondary Tunnel Hub", both showing "Hub Up" status and "1 Active Tunnels".

보안 FTD - IPsec 터널 상태

FMC에서

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The main section is titled "SecureAccess-VPN" and shows a "Topology Name" of "SecureAccess-VPN", "VPN Type" of "Route Based (VTI)", and "Network Topology" of "Point-to-Point". The "Tunnel Status Distribution" shows "2 Tunnels".

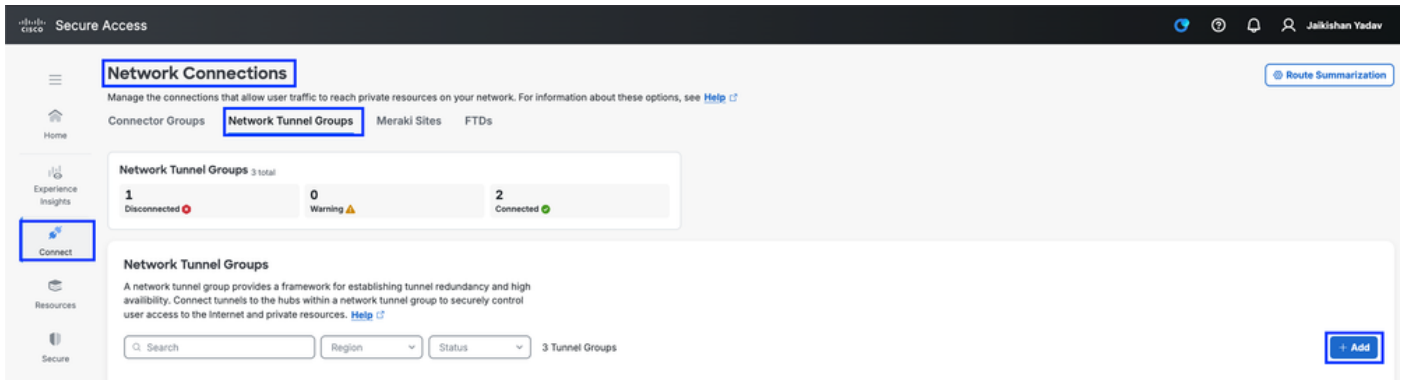
Node A	Node B																		
<table border="1"><thead><tr><th>Device</th><th>VPN Interface</th><th>VTI Interface</th></tr></thead><tbody><tr><td>EXTRANET Extranet</td><td>44.228.138.150 (44.228...</td><td>FTD FTD</td></tr><tr><td>EXTRANET Extranet</td><td>52.35.201.56 (52.35.20...</td><td>FTD FTD</td></tr></tbody></table>	Device	VPN Interface	VTI Interface	EXTRANET Extranet	44.228.138.150 (44.228...	FTD FTD	EXTRANET Extranet	52.35.201.56 (52.35.20...	FTD FTD	<table border="1"><thead><tr><th>Device</th><th>VPN Interface</th><th>VTI Interface</th></tr></thead><tbody><tr><td>FTD FTD</td><td>outside (192.168.1.12)</td><td>VTI-1 (169.254.2.1)</td></tr><tr><td>FTD FTD</td><td>outside (192.168.1.12)</td><td>VTI-2 (169.254.2.5)</td></tr></tbody></table>	Device	VPN Interface	VTI Interface	FTD FTD	outside (192.168.1.12)	VTI-1 (169.254.2.1)	FTD FTD	outside (192.168.1.12)	VTI-2 (169.254.2.5)
Device	VPN Interface	VTI Interface																	
EXTRANET Extranet	44.228.138.150 (44.228...	FTD FTD																	
EXTRANET Extranet	52.35.201.56 (52.35.20...	FTD FTD																	
Device	VPN Interface	VTI Interface																	
FTD FTD	outside (192.168.1.12)	VTI-1 (169.254.2.1)																	
FTD FTD	outside (192.168.1.12)	VTI-2 (169.254.2.5)																	

보안 FMC - IPsec 터널 상태

PBR로 ASA(Adaptive Security Appliance)에서 고정 경로 기반 IPsec VPN 구성

보안 액세스에 대한 VPN 구성

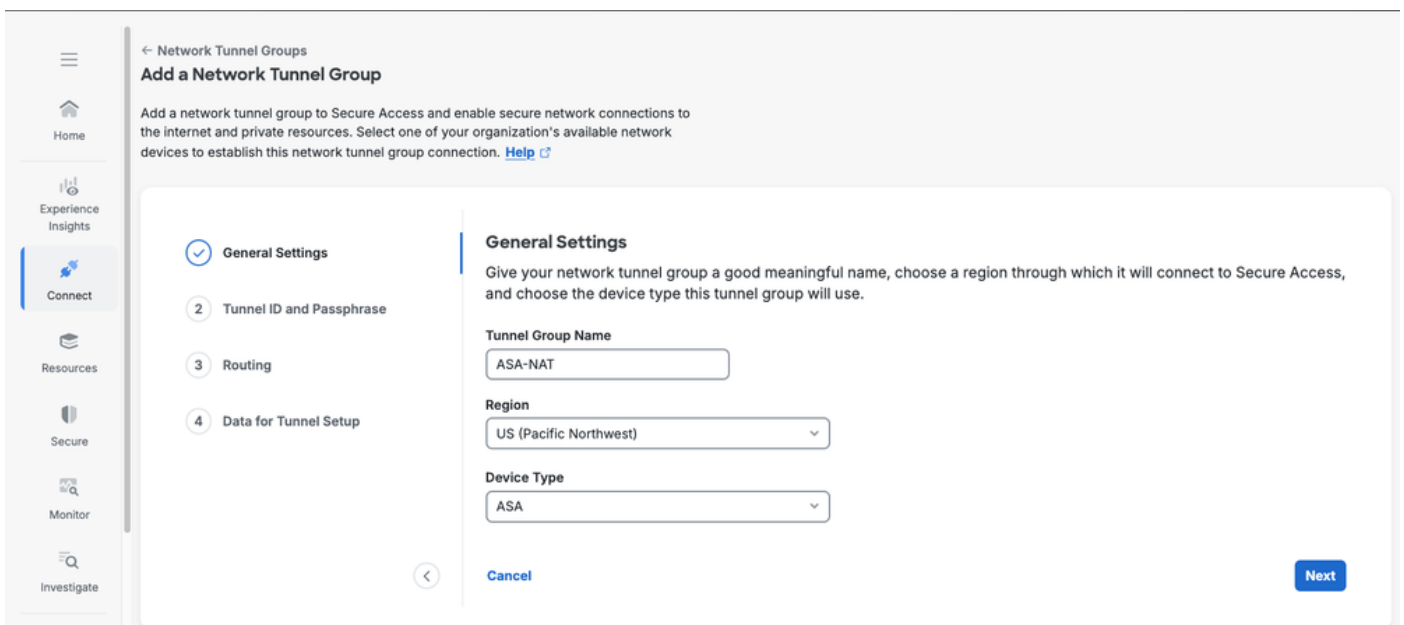
1. Secure Access 대시보드에 로그인 [Secure Access](#)
2. Connect(연결) > Network Connections(네트워크 연결) > Network Tunnel Groups(네트워크 터널 그룹)로 이동하고 +Add(추가)를 클릭하여 네트워크 터널 그룹을 구성합니다



보안 액세스 - 네트워크 터널 그룹

3. 네트워크 터널 그룹 구성 - 일반 설정

- 터널 그룹 이름, 영역 및 디바이스 유형 구성
- Next(다음)를 클릭합니다.



보안 액세스 - 네트워크 터널 그룹 일반 설정

4. 터널 ID 및 암호를 구성합니다.

- 터널 ID 및 암호를 구성합니다.
- Next(다음)를 클릭합니다

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

Tunnel ID and Passphrase

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

Tunnel ID Format

☒ Email ☐ IP Address

Tunnel ID

asahomevpn @<org><hub>.sse.cisco.com

Passphrase

..... [Show](#)

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

..... [Show](#)

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

보안 액세스 - 네트워크 터널 그룹

5. NAT(Network Address Translation) 활성화

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

☒ **Network Address Translation (NAT)**

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site → Secure Access

Source NAT

All source IP addresses translate to range:

100.96.0.0/16

☐ Translate to Secure Access NAT subnet

Secure Access → Site

Source NAT

Add a destination mapping to enable this rule

Destination NAT Mappings

Name	Direction	Original CIDR	Translated CIDR	...
+ Add Mappings Configure full bi-directional granular control over destination IP address translation.				

Internet Protocol Version Setting for Routing

☐ Enable IPv6 Routing in addition to IPv4

[Cancel](#) [Back](#) [Save](#)

보안 액세스 - 네트워크 터널 그룹 NAT 설정

6. 대상 NAT 매핑 추가

플로 1 - 라우터 1에서 라우터 2(Site-to-Secure Access)

폴로 2 - 라우터 2에서 라우터 1로(사이트에 대한 보안 액세스)

Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

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

Routing options and network overlaps

Configure routing options for this tunnel group.

☒ **Network Address Translation (NAT)**

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site to Secure Access

Source NAT

All source IP addresses translate to range:

100.96.0.0/16

☒ Translate to Secure Access NAT subnet

Secure Access to Site

Source NAT

Add a destination mapping to enable this rule

Destination NAT Mappings

Name	Direction	Original CIDR	Translated CIDR	
ASA-To-FTD	Site to Secure Access	10.10.10.102/32	192.168.10.102/32	☒ x

Rows per page: 30 < 1 >

[+ Add Mappings](#)

Internet Protocol Version Setting for Routing

☒ Enable IPv6 Routing in addition to IPv4

보안 액세스 - 네트워크 터널 그룹 NAT 설정



주의: NAT가 활성화된 경우 BGP를 수행할 수 없습니다. 또한 고객 에지 디바이스에서도 고정 VPN을 구성합니다



팁: 변환된 IP에 ping을 실행해야 합니다.
변환된 IP는 변환된 CIDR에, 실제 IP는 원래 CIDR에 배치됩니다.

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

4 Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

☒ Network Address Translation (NAT)

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site → Secure Access ⓘ

Source NAT

All source IP addresses translate to range:

100.96.0.0/16

☐ Translate to Secure Access NAT subnet

Secure Access → Site ⓘ

Source NAT

All source IP addresses translate to range:

100.103.255.0/24

☐ Translate to Secure Access NAT subnet

Destination NAT Mappings

Name	Direction ⓘ	Original CIDR	Translated CIDR	...
> ASA-To-FTD	Site → Secure Access	10.10.10.102/32	→ 192.168.10.102/32	ⓘ ⌵
> FTD-To-ASA	Secure Access → Site	10.10.10.101/32	→ 172.16.10.101/32	ⓘ ⌵

Rows per page 30 < 1 >

[+ Add Mappings](#)

Internet Protocol Version Setting for Routing

Cancel

Back Save

보안 액세스 - 네트워크 터널 그룹 NAT 설정

클릭 저장



팁: '사이트 A'에서 '사이트 B'로 이동하는 트래픽의 경우 CNHE-1의 POV 방향은 'Site-> SecureAccess'입니다.

'사이트 B'에서 '사이트 A'로 이동하는 트래픽의 경우 CNHE-1의 POV 방향은 'SecureAccess -> Site'입니다.

ASA의 VPN 컨피그레이션

1. ASA CLI에 로그인하여 활성화 모드를 시작하고 인터넷에 대한 기본 IP 연결을 확인합니다

ASA# sh ip

시스템 IP 주소:

인터페이스 이름 IP 주소 서브넷 마스크 방법

GigabitEthernet0/0 외부 192.168.1.40 255.255.255.0 설명서

GigabitEthernet0/1 inside 10.10.1 255.255.255.0 매뉴얼

현재 IP 주소:

인터페이스 이름 IP 주소 서브넷 마스크 방법

GigabitEthernet0/0 외부 192.168.1.40 255.255.255.0 설명서

GigabitEthernet0/1 inside 10.10.1 255.255.255.0 매뉴얼

ASA# ping 8.8.8.8

중단할 이스케이프 시퀀스를 입력합니다.

5, 100바이트 ICMP 에코를 8.8.8.8로 보내는 경우 시간 초과는 2초입니다.

!!!!

성공률은 100%(5/5), 왕복 최소/평균/최대 = 20/28/30ms

ASA 번호

2. IKEv2 정책을 구성하고 외부 인터페이스에서 IKEv2를 활성화합니다

crypto ikev2 정책 10

암호화 aes-gcm-256

무결성 null

그룹 19

수명 초 86400

crypto ikev2 enable outside(외부 암호화 ikev2 활성화)

3. IPSec 제안 구성

암호화 ipsec ikev2 ipsec-proposal Ipsec-Proposal-Primary

프로토콜 esp 암호화 aes-gcm-256

4. IPsec 프로파일 구성

암호화 ipsec 프로파일 csa-profile-primary

ikev2 ipsec-proposal Ipsec-Proposal-primary 설정

ikev2 local-identity email-id <primary tunnel-id> 설정

5. 그룹 정책을 구성하고 특성 아래에서 IKEv2 프로토콜을 활성화합니다.

group-policy csa-policy-primary 내부

group-policy csa-policy-primary 특성

vpn-tunnel-protocol ikev2

6. 터널 그룹을 구성합니다.

tunnel-group 44.228.138.150 type ipsec-l2l

터널 그룹 44.228.138.150 일반 특성

default-group-policy csa-policy-primary

터널 그룹 44.228.138.150 ipsec 특성

ikev2 원격 인증 사전 공유 키 <사전 공유 키>

ikev2 local-authentication pre-shared-key <pre-shared-key>

7. VTI(가상 터널 인터페이스) 구성

- Nameif는 원하는 경우
- VTI에 할당된 IP 주소는 ASA의 다른 인터페이스와 중복되어서는 안 됩니다
- 터널 소스방화벽의 외부 인터페이스여야 함
- 터널 대상은 데이터 센터 IP 주소여야 합니다.

인터페이스 터널 1

nameif VTI-1

ip 주소 169.254.2.1 255.255.255.252

터널 소스 인터페이스 외부

터널 대상 44.228.138.150

터널 모드 ipsec ipv4

터널 보호 ipsec 프로파일 csa-profile-primary

8. 매핑된 IP 주소 또는 서브넷에 대한 트래픽이 VTI 인터페이스 내부에서 라우팅되도록 라우팅을 구성합니다. 다음 홉은 VTI 범위 내에서 IP별로 필요합니다.

route VTI-1 0.0.0.0 0.0.0 169.254.2.2 5. (인터넷 기반, RAVPN 풀 또는 CGNAT 트래픽의 경우)

또는

route VTI-1 172.16.10.101 255.255.255 169.254.2.2 5

정책 기반 라우팅

1. 액세스 목록

access-list PBR extended permit ip 10.10.10.0 255.255.255.0 any

2. 노선도

route-map RM-CSA permit 10

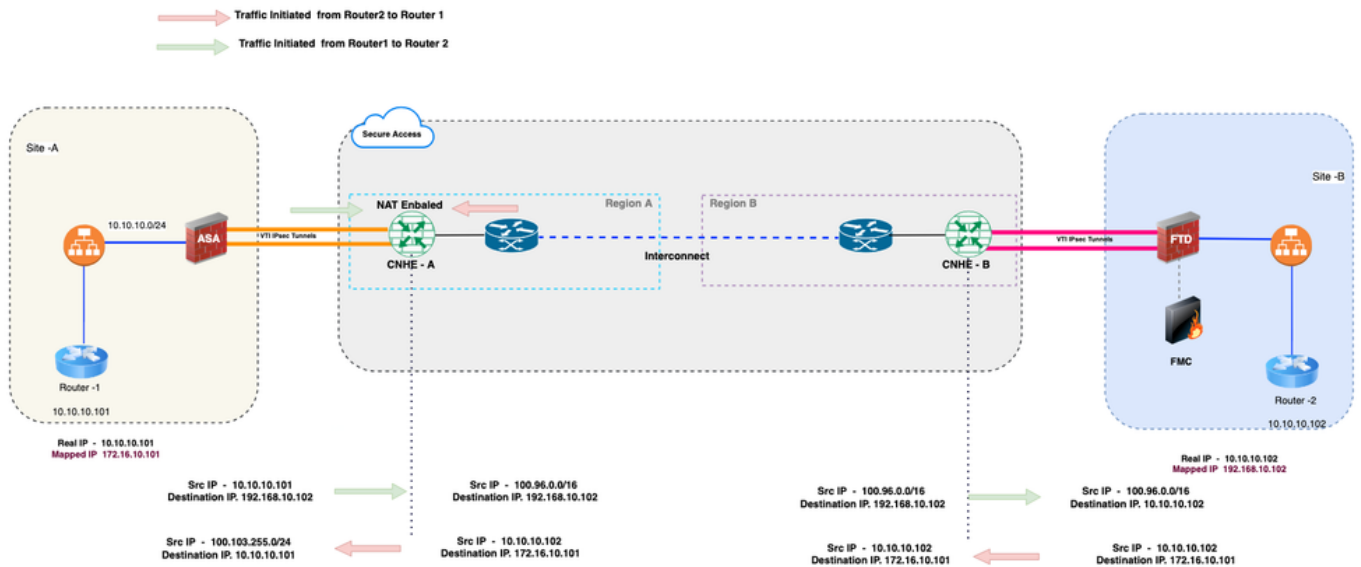
ip 주소 PBR 일치

ip next-hop 169.254.2.2 169.254.2.6 설정

3. 인그레스 인터페이스에 Route-map 적용

```
interface GigabitEthernet 0/1
nameif 내부
보안 수준 100
ip address 10.10.10.1 255.255.255.0
policy-route route-map RM-CSA
```

다음을 확인합니다.



라우터 인터페이스 및 GW 연결 상태

```
Router1#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
GigabitEthernet1 192.168.1.101 YES NVRAM down      down
GigabitEthernet2 10.10.10.101 YES NVRAM up        up
GigabitEthernet3 unassigned YES NVRAM administratively down down
GigabitEthernet9 unassigned YES unset administratively down down
Router1#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

테스트 1- Router2 → Router1. - Ping 테스트

```

Router1#ping 192.168.10.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.102, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 207/211/223 ms
Router1#

```

ASA의 패킷 캡처(로컬 FW)

```

ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA#
ASA#
ASA# ter pag 20
ASA# sh cap capin

10 packets captured

  1: 10:56:45.024244      10.10.10.101 > 192.168.10.102 icmp: echo request
  2: 10:56:45.231143      192.168.10.102 > 10.10.10.101 icmp: echo reply
  3: 10:56:45.232470      10.10.10.101 > 192.168.10.102 icmp: echo request
  4: 10:56:45.441856      192.168.10.102 > 10.10.10.101 icmp: echo reply
  5: 10:56:45.443122      10.10.10.101 > 192.168.10.102 icmp: echo request
  6: 10:56:45.652477      192.168.10.102 > 10.10.10.101 icmp: echo reply
  7: 10:56:45.653423      10.10.10.101 > 192.168.10.102 icmp: echo request
  8: 10:56:45.875397      192.168.10.102 > 10.10.10.101 icmp: echo reply
  9: 10:56:45.876450      10.10.10.101 > 192.168.10.102 icmp: echo request
 10: 10:56:46.082301      192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

  1: 10:56:45.024458      10.10.10.101 > 192.168.10.102 icmp: echo request
  2: 10:56:45.230914      192.168.10.102 > 10.10.10.101 icmp: echo reply
  3: 10:56:45.232516      10.10.10.101 > 192.168.10.102 icmp: echo request
  4: 10:56:45.441795      192.168.10.102 > 10.10.10.101 icmp: echo reply
  5: 10:56:45.443153      10.10.10.101 > 192.168.10.102 icmp: echo request
  6: 10:56:45.652432      192.168.10.102 > 10.10.10.101 icmp: echo reply
  7: 10:56:45.653454      10.10.10.101 > 192.168.10.102 icmp: echo request
  8: 10:56:45.875351      192.168.10.102 > 10.10.10.101 icmp: echo reply
  9: 10:56:45.876480      10.10.10.101 > 192.168.10.102 icmp: echo request
 10: 10:56:46.082240      192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown

```

FTD(원격 FW)의 패킷 캡처

```

ftd# sh cap
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd# sh cap vti

```

10 packets captured

```

 1: 16:06:41.122292      100.96.2.0 > 10.10.10.102 icmp: echo request
 2: 16:06:41.124856      10.10.10.102 > 100.96.2.0 icmp: echo reply
 3: 16:06:41.329557      100.96.2.0 > 10.10.10.102 icmp: echo request
 4: 16:06:41.330442      10.10.10.102 > 100.96.2.0 icmp: echo reply
 5: 16:06:41.546327      100.96.2.0 > 10.10.10.102 icmp: echo request
 6: 16:06:41.547106      10.10.10.102 > 100.96.2.0 icmp: echo reply
 7: 16:06:41.752036      100.96.2.0 > 10.10.10.102 icmp: echo request
 8: 16:06:41.752814      10.10.10.102 > 100.96.2.0 icmp: echo reply
 9: 16:06:41.967891      100.96.2.0 > 10.10.10.102 icmp: echo request
10: 16:06:41.968501      10.10.10.102 > 100.96.2.0 icmp: echo reply

```

10 packets shown

```
ftd# sh cap capin
```

10 packets captured

```

 1: 16:06:41.123299      100.96.2.0 > 10.10.10.102 icmp: echo request
 2: 16:06:41.124825      10.10.10.102 > 100.96.2.0 icmp: echo reply
 3: 16:06:41.330000      100.96.2.0 > 10.10.10.102 icmp: echo request
 4: 16:06:41.330396      10.10.10.102 > 100.96.2.0 icmp: echo reply
 5: 16:06:41.546800      100.96.2.0 > 10.10.10.102 icmp: echo request
 6: 16:06:41.547090      10.10.10.102 > 100.96.2.0 icmp: echo reply
 7: 16:06:41.752448      100.96.2.0 > 10.10.10.102 icmp: echo request
 8: 16:06:41.752783      10.10.10.102 > 100.96.2.0 icmp: echo reply
 9: 16:06:41.968242      100.96.2.0 > 10.10.10.102 icmp: echo request
10: 16:06:41.968486      10.10.10.102 > 100.96.2.0 icmp: echo reply

```

10 packets shown

테스트 2. - 라우터 2 → 라우터 1 ping 테스트

```

Router2#sh ip int br
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet1   unassigned      YES NVRAM    administratively down down
GigabitEthernet2   10.10.10.102   YES NVRAM    up          up
GigabitEthernet3   unassigned      YES NVRAM    administratively down down
Router2#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

```

FTD 패킷 캡처(로컬 FW)

```

ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd#
ftd#
ftd#
ftd# sh cap vti

10 packets captured

  1: 16:11:45.622450      10.10.10.102 > 172.16.10.101 icmp: echo request
  2: 16:11:45.823825      172.16.10.101 > 10.10.10.102 icmp: echo reply
  3: 16:11:45.825762      10.10.10.102 > 172.16.10.101 icmp: echo request
  4: 16:11:46.045667      172.16.10.101 > 10.10.10.102 icmp: echo reply
  5: 16:11:46.046857      10.10.10.102 > 172.16.10.101 icmp: echo request
  6: 16:11:46.252321      172.16.10.101 > 10.10.10.102 icmp: echo reply
  7: 16:11:46.253572      10.10.10.102 > 172.16.10.101 icmp: echo request
  8: 16:11:46.453803      172.16.10.101 > 10.10.10.102 icmp: echo reply
  9: 16:11:46.454764      10.10.10.102 > 172.16.10.101 icmp: echo request
 10: 16:11:46.664119      172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

  1: 16:11:45.622083      10.10.10.102 > 172.16.10.101 icmp: echo request
  2: 16:11:45.823886      172.16.10.101 > 10.10.10.102 icmp: echo reply
  3: 16:11:45.825442      10.10.10.102 > 172.16.10.101 icmp: echo request
  4: 16:11:46.045697      172.16.10.101 > 10.10.10.102 icmp: echo reply
  5: 16:11:46.046582      10.10.10.102 > 172.16.10.101 icmp: echo request
  6: 16:11:46.252352      172.16.10.101 > 10.10.10.102 icmp: echo reply
  7: 16:11:46.253313      10.10.10.102 > 172.16.10.101 icmp: echo request
  8: 16:11:46.453849      172.16.10.101 > 10.10.10.102 icmp: echo reply
  9: 16:11:46.454596      10.10.10.102 > 172.16.10.101 icmp: echo request
 10: 16:11:46.664150      172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown

```

ASA 패킷 캡처(원격 FW)

```

ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA# sh cap capin

10 packets captured

  1: 11:08:30.288391      100.103.255.195 > 10.10.10.101 icmp: echo request
  2: 11:08:30.289123      10.10.10.101 > 100.103.255.195 icmp: echo reply
  3: 11:08:30.504566      100.103.255.195 > 10.10.10.101 icmp: echo request
  4: 11:08:30.504963      10.10.10.101 > 100.103.255.195 icmp: echo reply
  5: 11:08:30.710992      100.103.255.195 > 10.10.10.101 icmp: echo request
  6: 11:08:30.711404      10.10.10.101 > 100.103.255.195 icmp: echo reply
  7: 11:08:30.917112      100.103.255.195 > 10.10.10.101 icmp: echo request
  8: 11:08:30.917402      10.10.10.101 > 100.103.255.195 icmp: echo reply
  9: 11:08:31.128243      100.103.255.195 > 10.10.10.101 icmp: echo request
 10: 11:08:31.128640      10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

  1: 11:08:30.287964      100.103.255.195 > 10.10.10.101 icmp: echo request
  2: 11:08:30.289322      10.10.10.101 > 100.103.255.195 icmp: echo reply
  3: 11:08:30.504505      100.103.255.195 > 10.10.10.101 icmp: echo request
  4: 11:08:30.505009      10.10.10.101 > 100.103.255.195 icmp: echo reply
  5: 11:08:30.710961      100.103.255.195 > 10.10.10.101 icmp: echo request
  6: 11:08:30.711434      10.10.10.101 > 100.103.255.195 icmp: echo reply
  7: 11:08:30.917066      100.103.255.195 > 10.10.10.101 icmp: echo request
  8: 11:08:30.917417      10.10.10.101 > 100.103.255.195 icmp: echo reply
  9: 11:08:31.128197      100.103.255.195 > 10.10.10.101 icmp: echo request
 10: 11:08:31.128685      10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown

```

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.