

# IPSec 터널을 통해 액세스 서버에 AnyConnect를 구성합니다.

## 목차

---

[소개:](#)

[사전 요구 사항:](#)

[기본 요구 사항](#)

[사용되는 구성 요소](#)

[네트워크 다이어그램](#)

[FMC의 컨피그레이션](#)

[FMC에서 관리하는 FTD의 RAVPN 컨피그레이션](#)

[FMC에서 관리하는 FTD의 IKEv2 VPN:](#)

[다음을 확인합니다.](#)

[문제 해결](#)

---

## 소개:

이 문서에서는 FMC에서 관리하는 FTD에 RAVPN 설정을 구축하고 FTD 간에 사이트 대 사이트 터널을 구축하는 절차에 대해 설명합니다.

## 사전 요구 사항:

### 기본 요구 사항

- 사이트 대 사이트 VPN 및 RAVPN에 대한 기본적인 이해는 도움이 됩니다.
- Cisco Firepower 플랫폼에서 IKEv2 정책 기반 터널을 구성하는 기본 사항에 대한 이해가 필수적입니다.

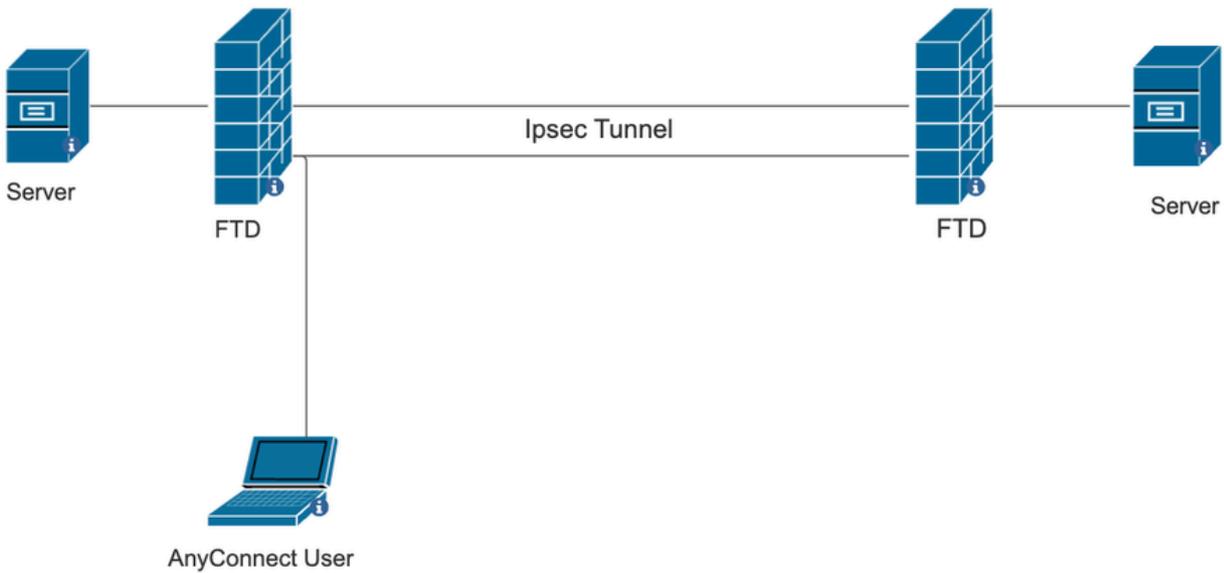
이 절차는 AnyConnect 사용자가 다른 FTD 피어 뒤에 있는 서버에 액세스할 수 있는 FTD 간의 Site-to-Site 터널 및 FMC에서 관리하는 FTD에 RAVPN 설정을 구축하기 위한 것입니다.

### 사용되는 구성 요소

- Cisco Firepower Threat Defense for VMware: 버전 7.0.0
- Firepower Management Center: 버전 7.2.4(빌드 169)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 가동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

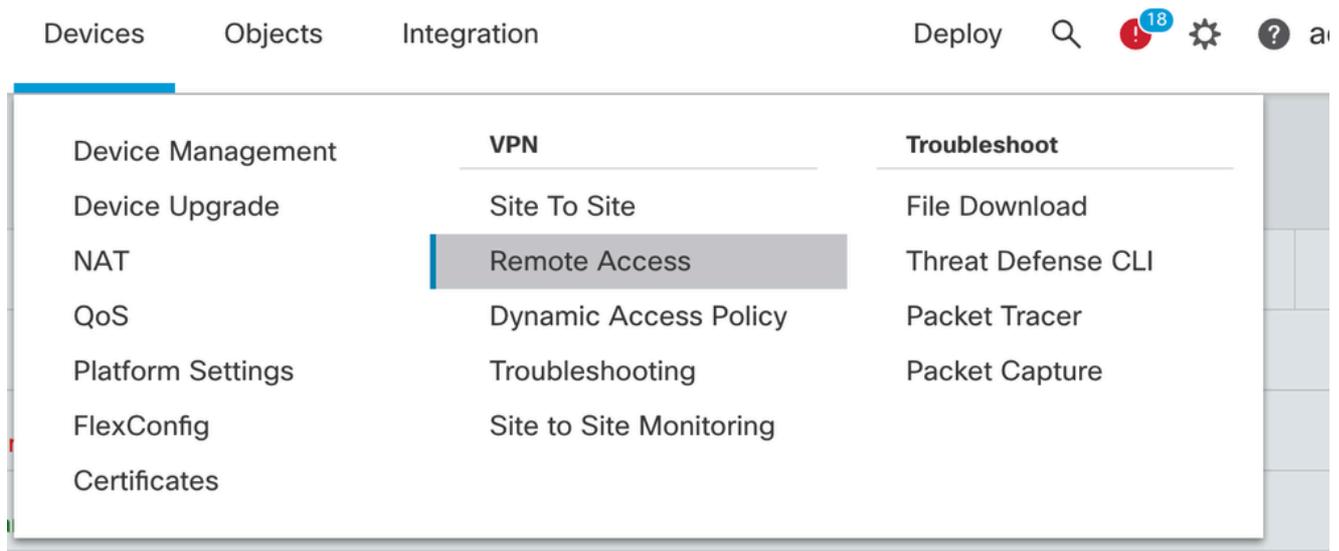
# 네트워크 다이어그램



## FMC의 컨피그레이션

### FMC에서 관리하는 FTD의 RAVPN 컨피그레이션

1. Devices(디바이스) > Remote Access(원격 액세스)로 이동합니다.



2. Add(추가)를 클릭합니다.
3. 이름을 구성하고 사용 가능한 디바이스에서 FTD를 선택하고 Next(다음)를 클릭합니다.

## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

### Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:\*

Description:

VPN Protocols:

- SSL
- IPsec-IKEv2

Targeted Devices:

Available Devices

- 10.106.50.55
- 10.88.146.35
- New\_FTD

Selected Devices

- 10.106.50.55

### Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

#### Authentication Server

Configure [LOCAL](#) or [Realm](#) or [RADIUS Server Group](#) or [SSO](#) to authenticate VPN clients.

#### AnyConnect Client Package

Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

#### Device Interface

Interfaces should be already configured on targeted [devices](#) so that they can be used as a security zone or interface group to enable VPN access.

## 4. 연결 프로파일 이름을 구성하고 인증 방법을 선택합니다.

참고: 이 컨피그레이션 샘플에서는 AAA만 사용하고 로컬 인증을 사용합니다. 그러나 요구 사항에 따라 구성합니다.

## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

### Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:\*

**!** This name is configured as a connection alias, it can be used to connect to the VPN gateway

### Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:

Authentication Server:\*

(LOCAL or Realm or RADIUS)

Local Realm:\*

Authorization Server:

(Realm or RADIUS)

Accounting Server:

(RADIUS)

## 5. AnyConnect의 IP 주소 할당에 사용되는 VPN 풀을 구성합니다.

(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ●

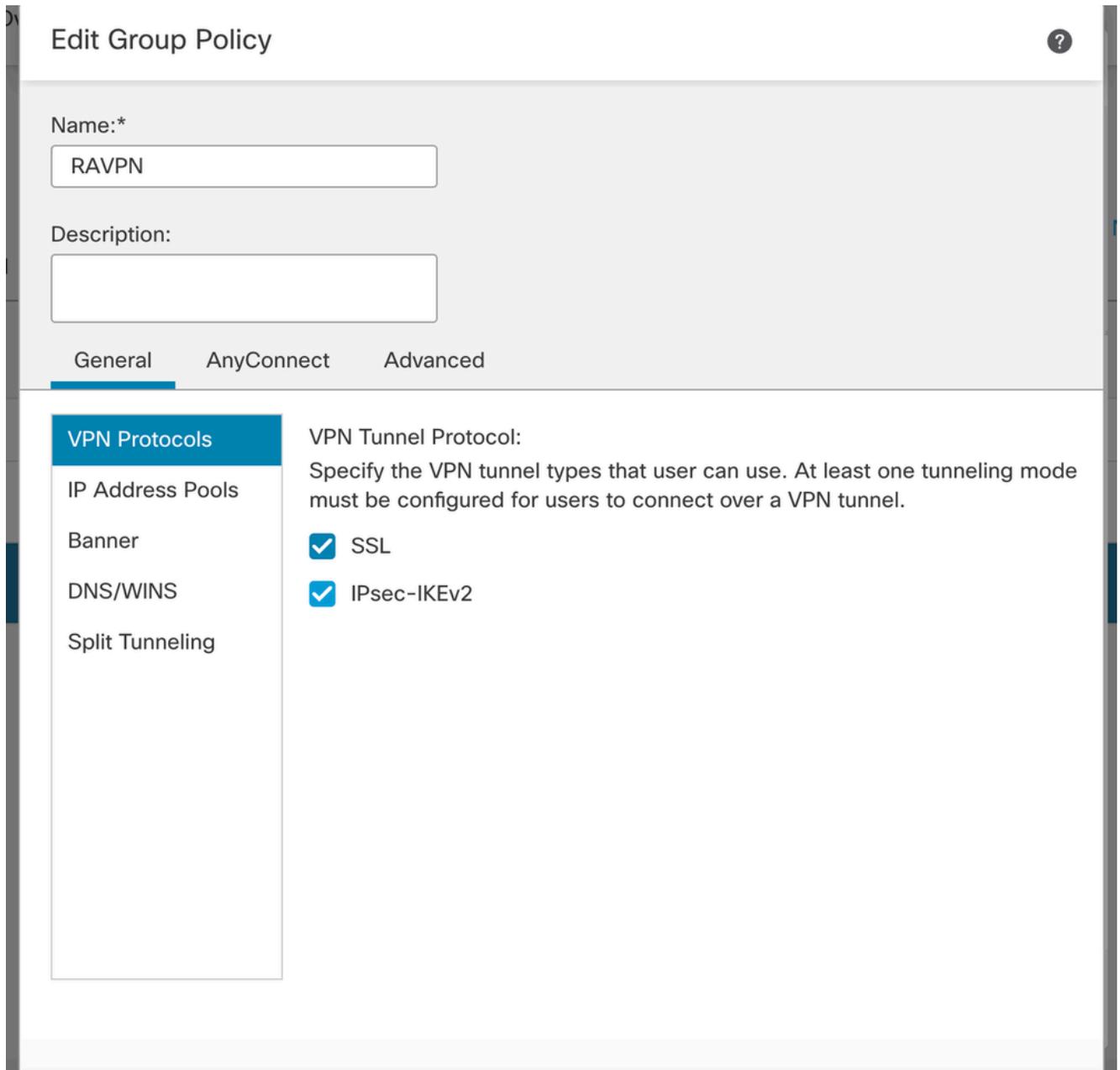
Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:  

IPv6 Address Pools:  

6. 그룹 정책을 생성합니다. 그룹 정책을 생성하려면 +를 클릭합니다. 그룹 정책의 이름을 추가합니다.



Edit Group Policy ?

Name:\*

Description:

General AnyConnect Advanced

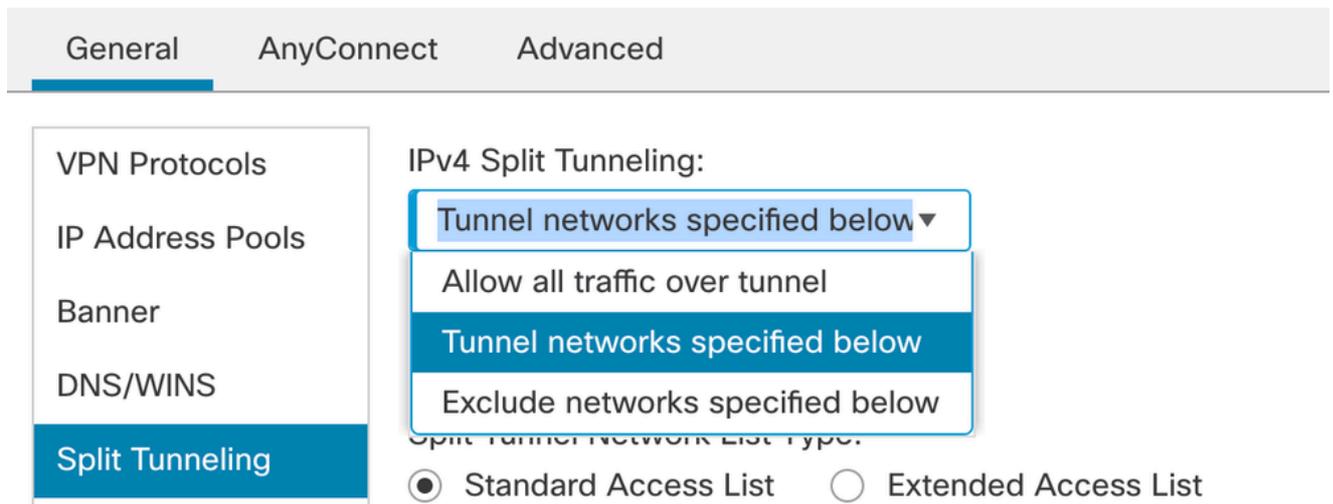
**VPN Protocols**

- IP Address Pools
- Banner
- DNS/WINS
- Split Tunneling

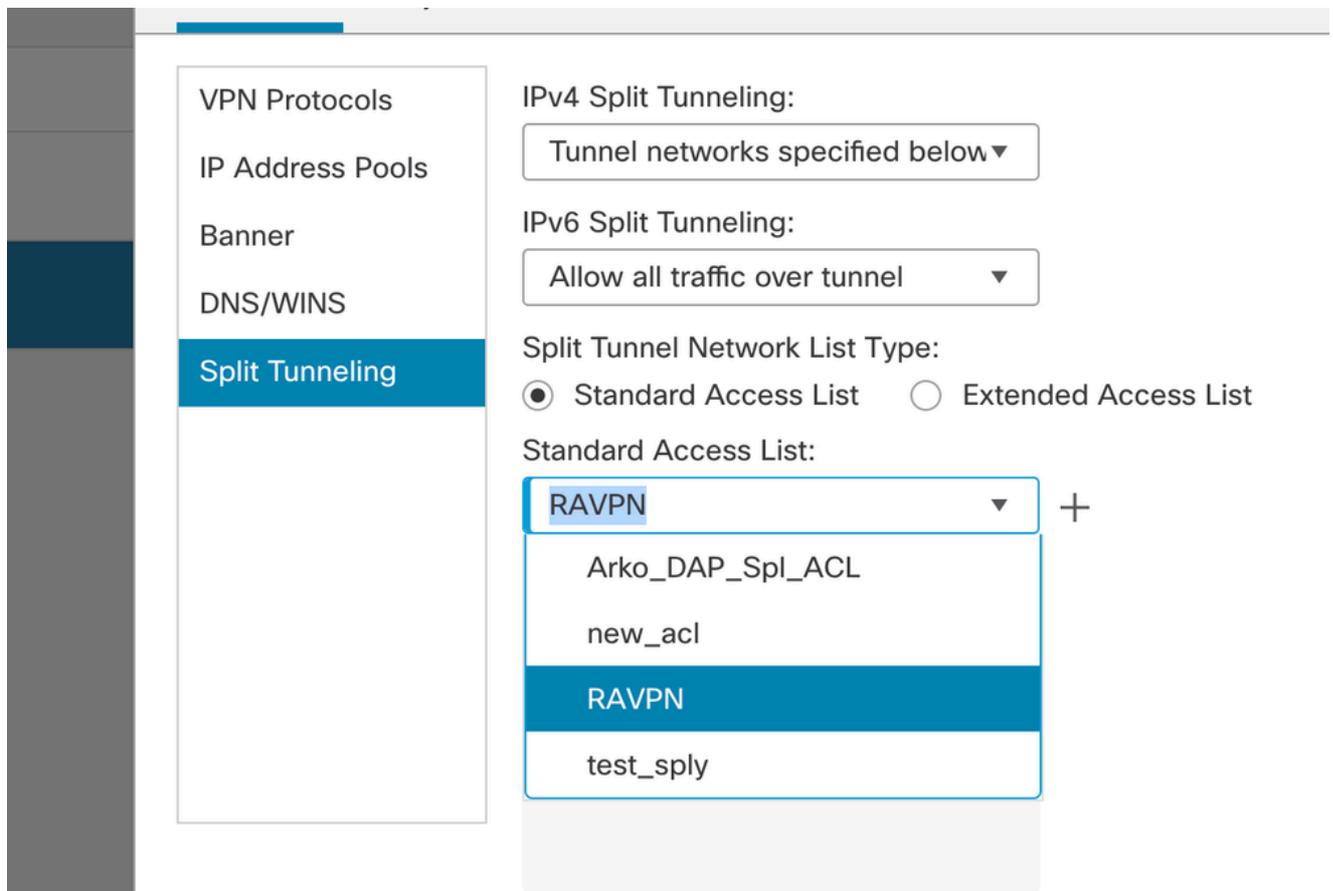
VPN Tunnel Protocol:  
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

- SSL
- IPsec-IKEv2

7. 스플릿 터널링으로 이동합니다. 여기에 지정된 터널 네트워크를 선택합니다.



8. 드롭다운 목록에서 올바른 액세스 목록을 선택합니다. ACL이 아직 구성되지 않은 경우: + 아이콘을 클릭하여 표준 액세스 목록을 추가하고 새 액세스 목록을 생성합니다. 저장을 클릭합니다.



9. 추가된 그룹 정책을 선택하고 Next(다음)를 클릭합니다.

### Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:\*  +

[Edit Group Policy](#)

## 10. AnyConnect 이미지를 선택합니다.

### AnyConnect Client Image

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

[Show Re-order buttons](#) +

<input type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input type="checkbox"/>	anyconnect	anyconnect410.pkg	Windows
<input checked="" type="checkbox"/>	anyconnect-win-4.10.07073-we...	anyconnect-win-4.10.07073-webdeploy-k9...	Windows
<input type="checkbox"/>	secure_client_5-1-2	cisco-secure-client-win-5_1_2_42-webde...	Windows

## 11. AnyConnect 연결을 활성화해야 하는 인터페이스를 선택하고 인증서를 추가한 다음 해독된 트래픽에 대한 Bypass Access Control(액세스 제어 우회) 정책을 선택하고 Next(다음)를 클릭합니다.

## Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:\*  +  
 Enable DTLS on member interfaces

**▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.**

## Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:\*  +

## Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)  
*This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.*

12. 컨피그레이션을 검토하고 Finish(마침)를 클릭합니다.

**Remote Access VPN Policy Configuration**

Firepower Management Center will configure an RA VPN Policy with the following settings

Name:	RAVPN
Device Targets:	10.106.50.55
Connection Profile:	RAVPN
Connection Alias:	RAVPN
AAA:	
Authentication Method:	AAA Only
Authentication Server:	sid_tes_local (Local)
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
AnyConnect Images:	anyconnect-win-4.10.07073-webdeploy-k9.pkg
Interface Objects:	sid_outside
Device Certificates:	cert1_1

**Additional Configuration Requirements**

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**  
An **Access Control** rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**  
If NAT is enabled on the targeted devices, you must define a **NAT Policy** to exempt VPN traffic.
- DNS Configuration**  
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using **FlexConfig Policy** on the targeted devices.
- Port Configuration**  
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in **NAT Policy** or other services before deploying the configuration.

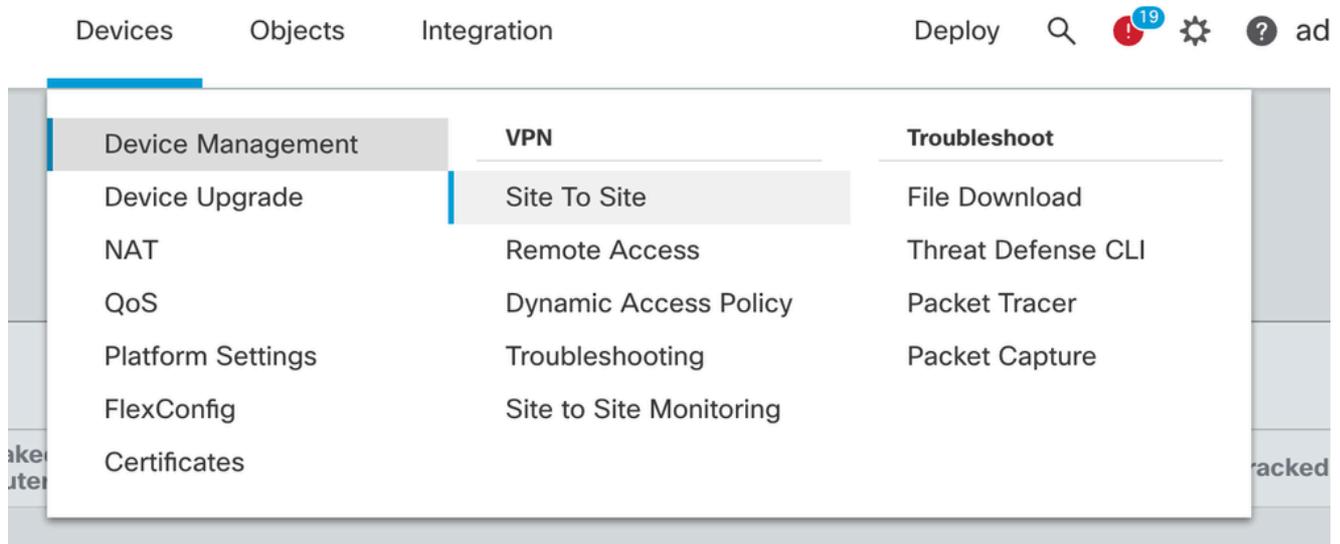
Cancel Back **Finish**

13. 저장 및 배포를 클릭합니다.

RAVPN		You have unsaved changes <span>Save</span> <span>Cancel</span>	
Enter Description		Policy Assignments (1)	
Connection Profile   Access Interfaces   Advanced		Local Realm: New_Realm   Dynamic Access Policy: None	
Name	AAA	Group Policy	
DefaultWEBVPGGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy	
RAVPN	Authentication: LOCAL Authorization: None Accounting: None	RAVPN	

## FMC에서 관리하는 FTD의 IKEv2 VPN:

1. Devices(디바이스) > Site To Site(사이트 대 사이트)로 이동합니다.



2. Add(추가)를 클릭합니다.
3. 노드 A에 대해 +를 클릭합니다.

Center

## Create New VPN Topology

Topology Name:\*

Policy Based (Crypto Map)
  Route Based (VTI)

Network Topology:

IKE Version:\*  IKEv1  IKEv2

Node A: +

Device Name	VPN Interface	Protected Networks	

Node B: +

Device Name	VPN Interface	Protected Networks	

- 디바이스에서 FTD를 선택하고 인터페이스를 선택한 다음 IPsec 터널을 통해 암호화해야 하는 로컬 서브넷(이 경우 VPN 풀 주소도 포함)을 추가하고 OK를 클릭합니다.

## Edit Endpoint



Device:\*

Interface:\*

IP Address:\*

This IP is Private

Connection Type:

Certificate Map:

 +

Protected Networks:\*

Subnet / IP Address (Network)  Access List (Extended)

FTD-Lan	
VPN_Pool_Subnet	

+

5. 노드 B에 대해 + 클릭:

> 디바이스에서 엑스트라넷을 선택하고 피어 디바이스의 이름을 지정합니다.

> 피어 세부 정보를 구성하고 VPN 터널을 통해 액세스해야 하는 원격 서브넷을 추가한 다음 OK(확인)를 클릭합니다.

## Edit Endpoint ?

Device:\*

Device Name:\*

IP Address:\*  
 Static  Dynamic

Certificate Map:  
 +

Protected Networks:\*  
 Subnet / IP Address (Network)  Access List (Extended)

Remote-Lan2 +

Remote-Lan +

6. IKE 탭을 클릭합니다. 요구 사항에 따라 IKEv2 설정을 구성합니다

## Edit VPN Topology



Topology Name:\*

FTD-S2S-FTD

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:\*

FTD-ASA

Authentication Type:

Pre-shared Manual Key

Key:\*

.....

Confirm Key:\*

.....

Enforce hex-based pre-shared key only

Cancel

Save

7. IPsec 탭: 요구 사항에 따라 IPsec 설정을 구성합니다.

Topology Name:\*

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

IKE Version:\*  IKEv1  IKEv2

Endpoints **IKE** IPsec Advanced

Crypto Map Type:  Static  Dynamic

IKEv2 Mode:

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals\*

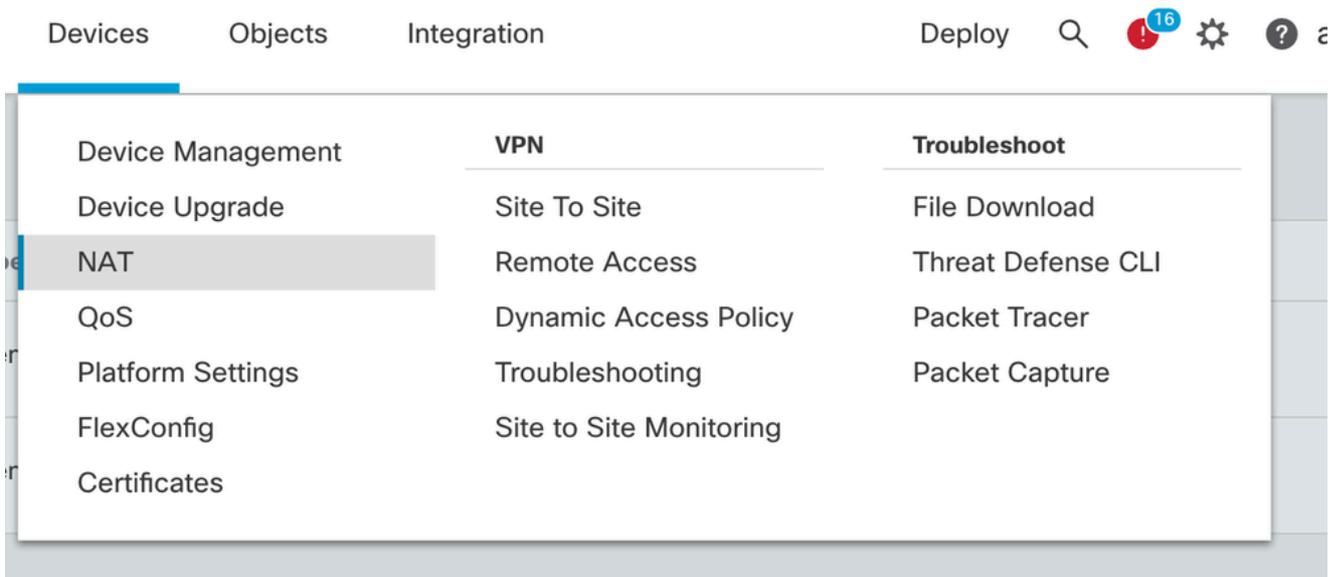
Enable Security Association (SA) Strength Enforcement  
 Enable Reverse Route Injection  
 Enable Perfect Forward Secrecy

Modulus Group:

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

Lifetime Size:  Kbytes (Range 10-2147483647)

8. 관심 트래픽에 대한 Nat-Exempt 구성(선택 사항)  
 Devices(디바이스) > NAT를 클릭합니다.



9. 여기서 구성된 NAT를 사용하면 RAVPN 및 내부 사용자가 S2S IPsec 터널을 통해 서버에 액세스할 수 있습니다.

☐	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options	
						Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services		
<input type="checkbox"/>	3	↔	Static	sid_outside	sid_outside	VPN_Pool_Subnet	Remote-Lan		VPN_Pool_Subnet	Remote-Lan		Dns:route-lookup no-proxy-arp	
<input type="checkbox"/>	4	↔	Static	sid_inside	sid_outside	FTD-Lan	Remote-Lan2		FTD-Lan	Remote-Lan2		Dns:false route-lookup no-proxy-arp	
<input type="checkbox"/>	5	↔	Static	sid_inside	sid_outside	FTD-Lan	Remote-Lan		FTD-Lan	Remote-Lan		Dns:false route-lookup no-proxy-arp	

10. 마찬가지로 S2S 터널이 가동될 다른 피어 엔드에서도 컨피그레이션을 수행합니다.

참고: 암호화 ACL 또는 관심 트래픽 서브넷은 양쪽 피어에서 서로의 미리 복사본이어야 합니다.

## 다음을 확인합니다.

### 1. RAVPN 연결을 확인하려면

```
<#root>
```

```
firepower# show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Username : test
```

```
Index : 5869
```

```
Assigned IP : 2.2.2.1 Public IP : 10.106.50.179
```

```
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License : AnyConnect Premium
```

```
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
```

```
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
```

```
Bytes Tx : 15470 Bytes Rx : 2147
```

```
Group Policy : RAVPN Tunnel Group : RAVPN
```

```
Login Time : 03:04:27 UTC Fri Jun 28 2024
```

```
Duration : 0h:14m:08s
```

```
Inactivity : 0h:00m:00s
```

```
VLAN Mapping : N/A VLAN : none
```

```
Audt Sess ID : 0a6a3468016ed000667e283b
```

```
Security Grp : none Tunnel Zone : 0
```

## 2. IKEv2 연결을 확인하려면

<#root>

```
firepower# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:2443, Status:UP-ACTIVE

, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote Status Role  
3363898555
```

```
10.106.52.104/500 10.106.52.127/500 READY INITIATOR
```

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/259 sec

Child sa: local selector 2.2.2.0/0 - 2.2.2.255/65535

remote selector 10.106.54.0/0 - 10.106.54.255/65535

ESP spi in/out: 0x4588dc5b/0x284a685

## 3. IPSec 연결을 확인하려면

<#root>

```
firepower# show crypto ipsec sa peer 10.106.52.127  
peer address: 10.106.52.127
```

Crypto map tag: CSM\_outside1\_map

,

seq num: 2, local addr: 10.106.52.104

```
access-list CSM_IPSEC_ACL_1 extended permit ip 2.2.2.0 255.255.255.0 10.106.54.0 255.255.255.0
```

```
local ident (addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.106.54.0/255.255.255.0/0/0)
```

current\_peer: 10.106.52.127

#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 3, #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.: 10.106.52.104/500, remote crypto endpt.: 10.106.52.127/500

path mtu 1500, ipsec overhead 94(44), media mtu 1500

PMTU time remaining (sec): 0, DF policy: copy-df

ICMP error validation: disabled, TFC packets: disabled

current outbound spi: 0284A685

current inbound spi : 4588DC5B

i

nbound esp sas:

spi: 0x4588DC5B (1166597211)

SA State: active

transform: esp-aes-256 esp-sha-512-hmac no compression

in use settings ={L2L, Tunnel, IKEv2, }

slot: 0, conn\_id: 5882, crypto-map: CSM\_outside1\_map

sa timing: remaining key lifetime (kB/sec): (3962879/28734)

IV size: 16 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x0000000F

outbound esp sas:

spi: 0x0284A685 (42247813)

SA State: active

```
transform: esp-aes-256 esp-sha-512-hmac no compression
```

```
in use settings ={L2L, Tunnel, IKEv2, }  
slot: 0, conn_id: 5882, crypto-map: CSM_outside1_map  
sa timing: remaining key lifetime (kB/sec): (4285439/28734)  
IV size: 16 bytes  
replay detection support: Y  
Anti replay bitmap:  
0x00000000 0x00000001
```

## 문제 해결

1. AnyConnect 연결 문제를 해결하려면 dart 번들을 수집하거나 AnyConnect 디버그를 활성화합니다.
2. IKEv2 터널의 문제를 해결하려면 다음 디버그를 사용합니다.

```
debug crypto condition peer <peer IP address>  
debug crypto ikev2 platform 255  
debug crypto ikev2 protocol 255  
debug crypto ipsec 255
```

3. FTD의 트래픽 문제를 해결하려면 패킷 캡처를 수행하고 구성을 확인합니다.

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.