

# FMC에서 관리하는 FTD의 사이트 대 사이트 VPN 구성

## 목차

---

### [소개](#)

#### [사전 요구 사항](#)

##### [요구 사항](#)

##### [사용되는 구성 요소](#)

### [설정](#)

#### [1단계. VPN 토폴로지를 정의합니다.](#)

#### [2단계. IKE 매개변수를 구성합니다.](#)

#### [3단계. IPsec 매개변수를 구성합니다.](#)

#### [4단계. 액세스 제어 우회.](#)

#### [5단계. 액세스 제어 정책을 생성합니다.](#)

#### [6단계. NAT 제외를 구성합니다.](#)

#### [7단계. ASA를 구성합니다.](#)

### [다음을 확인합니다.](#)

### [문제 해결 및 디버그](#)

#### [초기 연결 문제](#)

#### [트래픽 관련 문제](#)

---

## 소개

이 문서에서는 FMC에서 관리하는 FTD(Firepower Threat Defense)에서 사이트 대 사이트 VPN을 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 항목에 대한 지식이 있어야 합니다.

- VPN에 대한 기본 이해
- firepower Management Center 경험
- ASA 명령줄 경험

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD 6.5

- ASA 9.10(1)32
- IKEv2

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.

## 설정

firepower Management Center를 사용하여 FTD의 컨피그레이션부터 시작합니다.

1단계. VPN 토폴로지를 정의합니다.

1. Devices(디바이스) > VPN > Site To Site(사이트 대 사이트)로 이동합니다. 이 이미지에 표시된 대로 Add VPN(VPN 추가) 아래에서 Firepower Threat Defense Device(위협 방어 디바이스)를 클릭합니다.



2. Create New VPN Topology(새 VPN 토폴로지 생성) 상자가 나타납니다. 쉽게 식별할 수 있는 이름을 VPN에 지정합니다.

네트워크 토폴로지: 포인트 투 포인트

IKE 버전: IKEv2

이 예에서 엔드포인트를 선택하면 노드 A는 FTD이고 노드 B는 ASA입니다. 이 이미지에 표시된 대로 녹색 더하기 버튼을 클릭하여 토폴로지에 디바이스를 추가합니다.

**Create New VPN Topology** ? X

Topology Name:\*

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:\*  IKEv1  **IKEv2**

**Endpoints** IKE IPsec Advanced

Node A: +

Device Name	VPN Interface	Protected Networks

Node B: +

Device Name	VPN Interface	Protected Networks

**i** Ensure the protected networks are allowed by access control policy of each device.

Save Cancel

3. FTD를 첫 번째 엔드포인트로 추가합니다.

암호화 맵이 배치되는 인터페이스를 선택합니다. IP 주소는 디바이스 컨피그레이션에서 자동으로 채워져야 합니다.

이 이미지에 표시된 대로 Protected Networks(보호된 네트워크) 아래의 녹색 더하기 기호를 클릭하여 이 VPN에서 암호화해야 할 서브넷을 선택합니다.

## Add Endpoint



Device:\*

FTD

Interface:\*

outside

IP Address:\*

172.16.100.20

This IP is Private

Connection Type:

Bidirectional

Certificate Map:



Protected Networks:\*

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



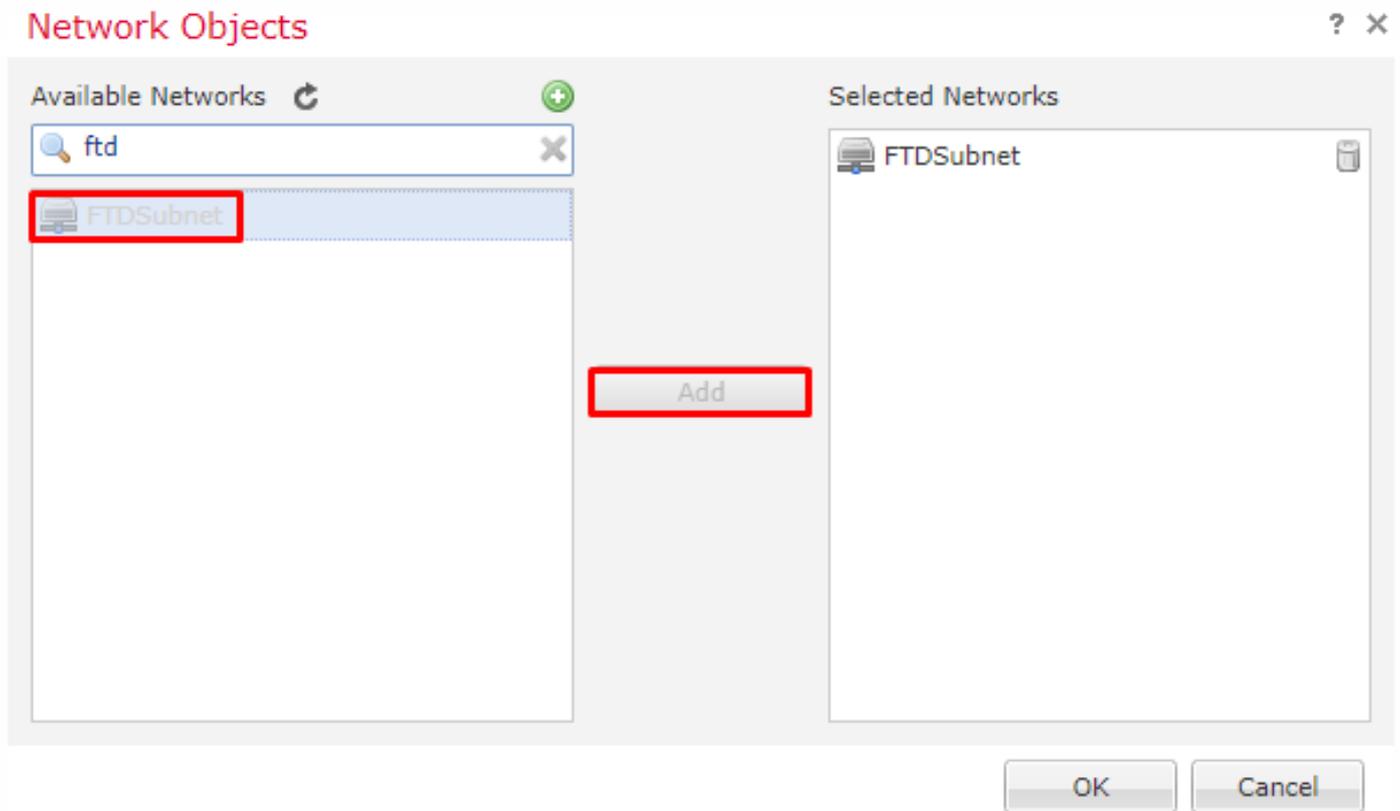
OK

Cancel

4. 녹색 더하기 기호를 클릭하면 네트워크 개체가 여기에 생성됩니다.

5. 암호화해야 하는 FTD에 모든 로컬 서브넷을 추가합니다. Add(추가)를 클릭하여 선택한 네트워크로 이동합니다. 이제 이 이미지에 표시된 대로 OK를 클릭합니다.

FTDSubnet = 10.10.113.0/24



노드 A: (FTD) 엔드포인트가 완료되었습니다. 이미지에 표시된 대로 노드 B의 녹색 더하기 기호를 클릭합니다.

### Create New VPN Topology

Topology Name: RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:  IKEv1  IKEv2

**Endpoints** IKE IPsec Advanced

Node A:

Device Name	VPN Interface	Protected Networks
FTD	outside/172.16.100.20	FTDSubnet

Node B:

Device Name	VPN Interface	Protected Networks

ⓘ Ensure the protected networks are allowed by access control policy of each device.

Save Cancel

노드 B는 ASA입니다. FMC에서 관리하지 않는 디바이스는 엑스트라넷으로 간주됩니다.

6. 장치 이름 및 IP 주소를 추가합니다. 그림과 같이 녹색 더하기 기호를 클릭하여 보호된 네트워크를 추가합니다.

## Edit Endpoint



Device:\*

Device Name:\*

IP Address:\*  Static  Dynamic

Certificate Map:

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

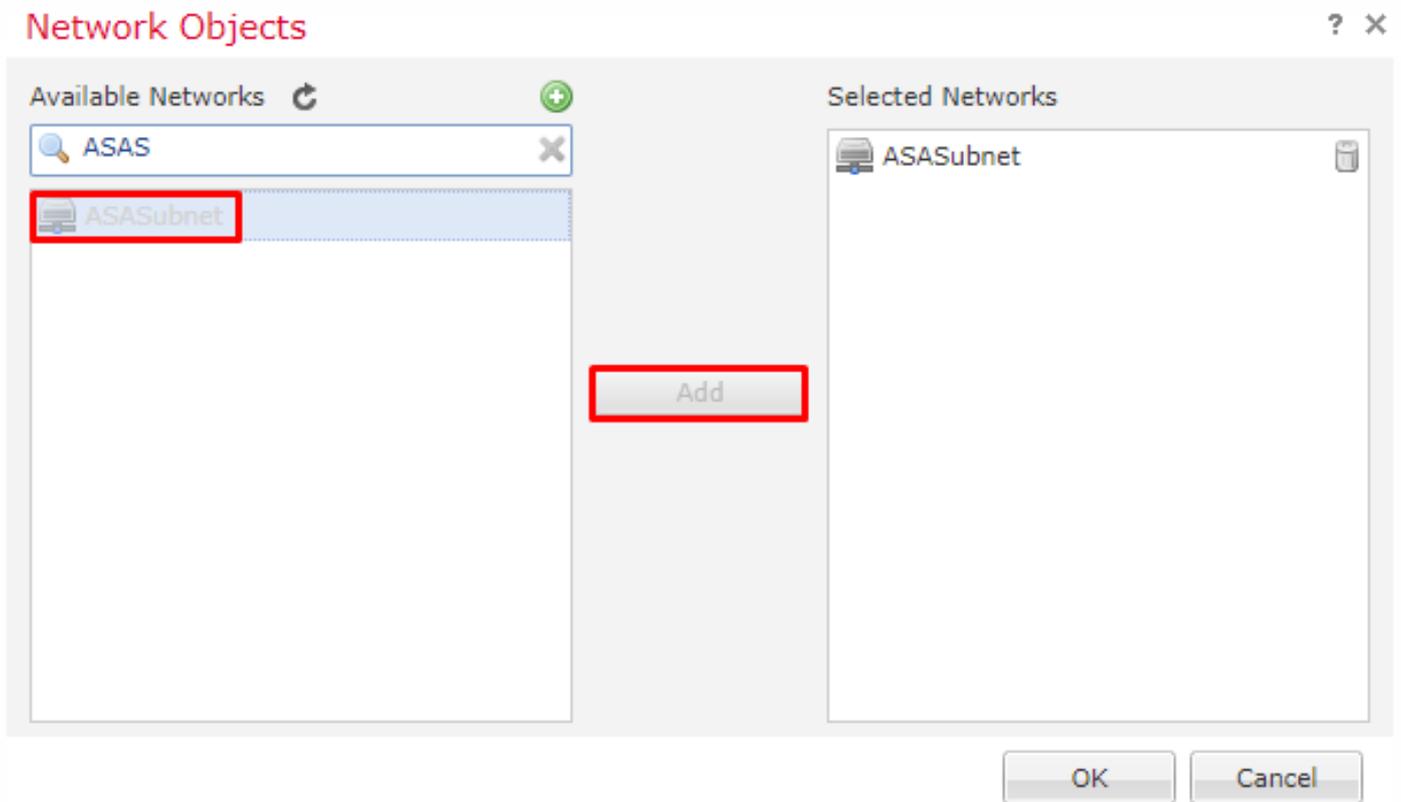


OK

Cancel

7. 이 이미지에 표시된 대로 암호화할 ASA 서브넷을 선택하고 선택한 네트워크에 추가합니다.

ASASubnet = 10.10.110.0/24



2단계. IKE 매개변수를 구성합니다.

이제 두 엔드포인트 모두 IKE/IPSEC 컨피그레이션을 통과합니다.

1. IKE 탭에서 IKEv2 초기 교환에 사용되는 매개변수를 지정합니다. 이미지에 표시된 대로 녹색 더하기 기호를 클릭하여 새 IKE 정책을 생성합니다.

## Create New VPN Topology

? X

Topology Name:\* RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:\*  IKEv1  IKEv2

Endpoints **IKE** IPsec Advanced

**IKEv1 Settings**

Policy:\* preshared\_sha\_aes256\_dh5\_5

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:\* 24 Characters (Range 1-127)

**IKEv2 Settings**

Policy:\* AES-GCM-NULL-SHA

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:\* 24 Characters (Range 1-127)

Save Cancel

2. 새 IKE 정책에서 우선 순위 번호와 연결 1단계의 수명을 지정합니다. 이 문서에서는 초기 교환에 Integrity(SHA256), Encryption(AES-256), PRF(SHA256) 및 Diffie-Hellman Group(Group 14) 매개 변수를 사용합니다

 참고: 디바이스의 모든 IKE 정책은 선택한 정책 섹션의 내용에 관계없이 원격 피어로 전송됩니다. 원격 피어와 일치하는 첫 번째 IKE 정책이 VPN 연결에 대해 선택됩니다. 우선 순위 필드를 사용하여 어떤 정책을 먼저 보낼지 선택합니다. 우선 순위 1이 먼저 전송됩니다.

# New IKEv2 Policy

Name:\*

Description:

Priority:  (1-65535)

Lifetime:  seconds (120-2147483647)

- Integrity Algorithms**
- Encryption Algorithms
- PRF Algorithms
- Diffie-Hellman Group

### Available Algorithms

- MD5
- SHA
- SHA512
- SHA256**
- SHA384
- NULL

Add

### Selected Algorithms

- SHA256

Save Cancel

# New IKEv2 Policy

Name:\*

Description:

Priority:  (1-65535)

Lifetime:  seconds (120-2147483647)

Integrity Algorithms

**Encryption Algorithms**

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- AES
- AES-256**
- DES
- 3DES
- AES-192
- AES-GCM
- AES-GCM-192
- AES-GCM-256
- NULL

Add

Selected Algorithms

- AES-256

Save Cancel

# New IKEv2 Policy



Name:\*

Description:

Priority:  (1-65535)

Lifetime:  seconds (120-2147483647)

- Integrity Algorithms
- Encryption Algorithms
- PRF Algorithms**
- Diffie-Hellman Group

- Available Algorithms
- MD5
  - SHA
  - SHA512
  - SHA256**
  - SHA384

Add

- Selected Algorithms
- SHA256

Save Cancel

## New IKEv2 Policy

? X

Name:*	<input type="text" value="ASA"/>
Description:	<input type="text"/>
Priority:	<input type="text" value="1"/> (1-65535)
Lifetime:	<input type="text" value="86400"/> seconds (120-2147483647)

Integrity Algorithms	Available Groups	Selected Groups
Encryption Algorithms		
PRF Algorithms	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21	<input type="checkbox"/> 14
<b>Diffie-Hellman Group</b>		

3. 매개변수가 추가되면 이 정책을 선택하고 인증 유형을 선택합니다.

4. 사전 공유 키 설명서를 선택합니다. 이 문서에서는 PSK cisco123이 사용됩니다.

**Create New VPN Topology** ? X

Topology Name:\*

Network Topology:  Point to Point  Hub and Spoke  Full Mesh

IKE Version:\*  IKEv1  IKEv2

Endpoints **IKE** IPsec Advanced

**IKEv1 Settings**

Policy:\*  +

Authentication Type:

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

**IKEv2 Settings**

Policy:\*  +

Authentication Type:

Key:\*

Confirm Key:\*

Enforce hex-based pre-shared key only

3단계. IPsec 매개변수를 구성합니다.

1. 이 이미지에 표시된 대로 IPsec 아래에서 연필을 클릭하여 변형 집합을 편집하고 새 IPsec 제안을 만듭니다.

## Create New VPN Topology

? X

Topology Name:\* RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:\*  IKEv1  IKEv2

Endpoints IKE **IPsec** Advanced

Crypto Map Type:  Static  Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals: tunnel\_aes256\_sha  
IKEv2 IPsec Proposals\*: AES-GCM

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

Modulus Group: 14

Lifetime Duration\*: 28800 Seconds (Range 120-2147483647)  
Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

— **ESPv3 Settings**

Save Cancel

2. 새 IKEv2 IPsec 제안을 만들려면 녹색 더하기 기호를 클릭하고 2단계 매개변수를 입력합니다.

ESP Encryption(ESP 암호화) > AES-GCM-256을 선택합니다. GCM 알고리즘을 암호화에 사용하면 해시 알고리즘이 필요 없다. GCM을 사용하면 해시 기능이 내장되어 있습니다.

### Edit IKEv2 IPsec Proposal



Name:\* ASA

Description:

ESP Hash

ESP Encryption

Available Algorithms

- AES-GCM-256
- AES-256
- AES-GCM-192
- AES-192
- AES-GCM
- AES
- 3DES
- DES
- AES-GMAC-25

Add

Selected Algorithms

- AES-GCM-256

Save Cancel

3. 새 IPsec 제안이 생성된 후 선택한 변형 집합에 추가합니다.

### IKEv2 IPsec Proposal



Available Transform Sets

Search

- AES-GCM
- AES-SHA
- ASA
- DES\_SHA-1

Add

Selected Transform Sets

- ASA

OK Cancel

이제 새로 선택한 IPsec 제안이 IKEv2 IPsec 제안 아래에 나열됩니다.

필요한 경우 여기에서 2단계 수명 및 PFS를 편집할 수 있습니다. 이 예에서는 수명이 기본값으로 설정되고 PFS가 비활성화됩니다.

The screenshot shows the 'Create New VPN Topology' dialog box with the following configuration:

- Topology Name: RTPVPN-ASA
- Network Topology: Point to Point
- IKE Version: IKEv2
- Endpoints: IKE, IPsec (selected), Advanced
- Crypto Map Type: Static
- IKEv2 Mode: Tunnel
- Transform Sets: IKEv1 IPsec Proposals (tunnel\_aes256\_sha), IKEv2 IPsec Proposals\* (ASA)
- Enable Security Association (SA) Strength Enforcement: unchecked
- Enable Reverse Route Injection: checked
- Enable Perfect Forward Secrecy: unchecked
- Modulus Group: 14
- Lifetime Duration: 28800 Seconds
- Lifetime Size: 4608000 Kbytes
- ESPv3 Settings: collapsed

선택 사항 - Bypass Access Control(액세스 제어 우회) 또는 Create an Access Control Policy(액세스 제어 정책 생성) 옵션을 완료해야 합니다.

4단계. 액세스 제어 우회.

선택적으로, Advanced(고급) > Tunnel(터널)에서 sysopt permit-vpn을 활성화할 수 있습니다.

이렇게 하면 액세스 제어 정책을 사용하여 사용자로부터 들어오는 트래픽을 검사할 가능성이 사라집니다. VPN 필터 또는 다운로드 가능한 ACL을 사용하여 사용자 트래픽을 필터링할 수 있습니다. 이 명령은 전역 명령이며 이 확인란이 활성화된 경우 모든 VPN에 적용됩니다.

**Create New VPN Topology** ? x

Topology Name: \*

Network Topology:  Point to Point  Hub and Spoke  Full Mesh

IKE Version: \*  IKEv1  IKEv2

Endpoints | IKE | IPsec | **Advanced**

IKE  
IPsec  
**Tunnel**

**NAT Settings**

Keepalive Messages Traversal  
Interval:  Seconds (Range 10 - 3600)

**Access Control for VPN Traffic**

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

**Certificate Map Settings**

Use the certificate map configured in the Endpoints to determine the tunnel

Use the certificate OU field to determine the tunnel

Use the IKE identity to determine the tunnel

Use the peer IP address to determine the tunnel

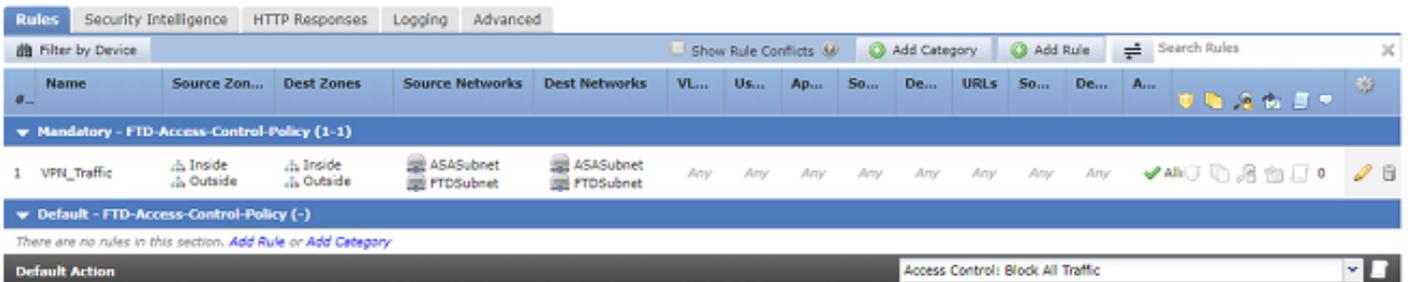
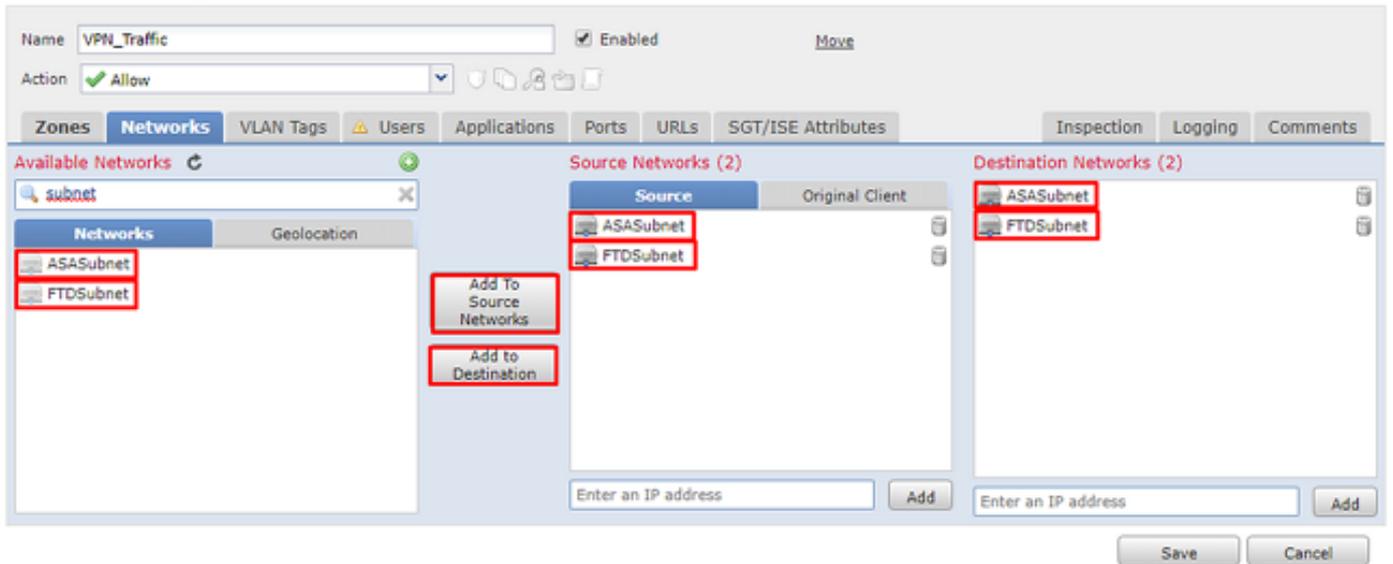
sysopt permit-vpn이 활성화되지 않은 경우 FTD 디바이스를 통한 VPN 트래픽을 허용하도록 액세스 제어 정책을 생성해야 합니다. sysopt permit-vpn이 활성화된 경우 액세스 제어 정책 생성을 건너뛴니다.

5단계. 액세스 제어 정책을 생성합니다.

Access Control Policies(액세스 제어 정책)에서 Policies(정책) > Access Control(액세스 제어) > Access Control(액세스 제어)로 이동하고 FTD 디바이스를 대상으로 하는 정책을 선택합니다. 규칙을 추가하려면 여기 이미지에 표시된 대로 Add Rule(규칙 추가)을 클릭합니다.

내부 네트워크에서 외부 네트워크로, 외부 네트워크에서 내부 네트워크로 트래픽을 허용해야 합니다. 둘 다 수행할 하나의 규칙을 만들거나 두 개의 규칙을 만들어 서로 분리하십시오. 이 예에서는 둘 다 수행할 수 있도록 하나의 규칙이 생성됩니다.

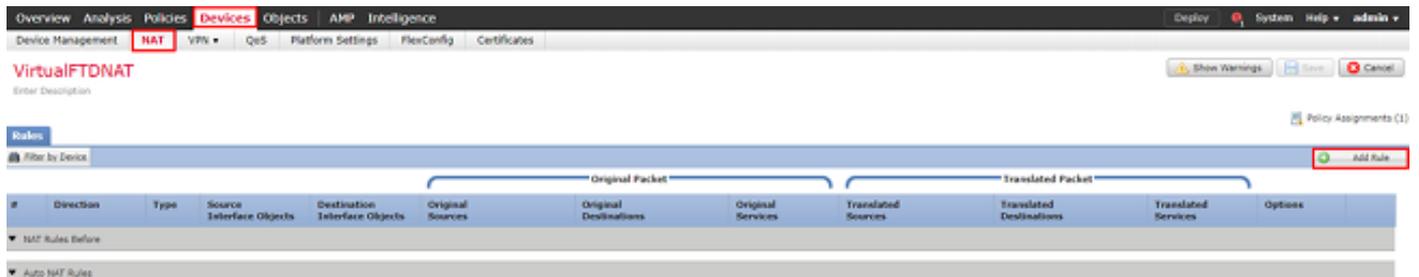
## Editing Rule - VPN\_Traffic



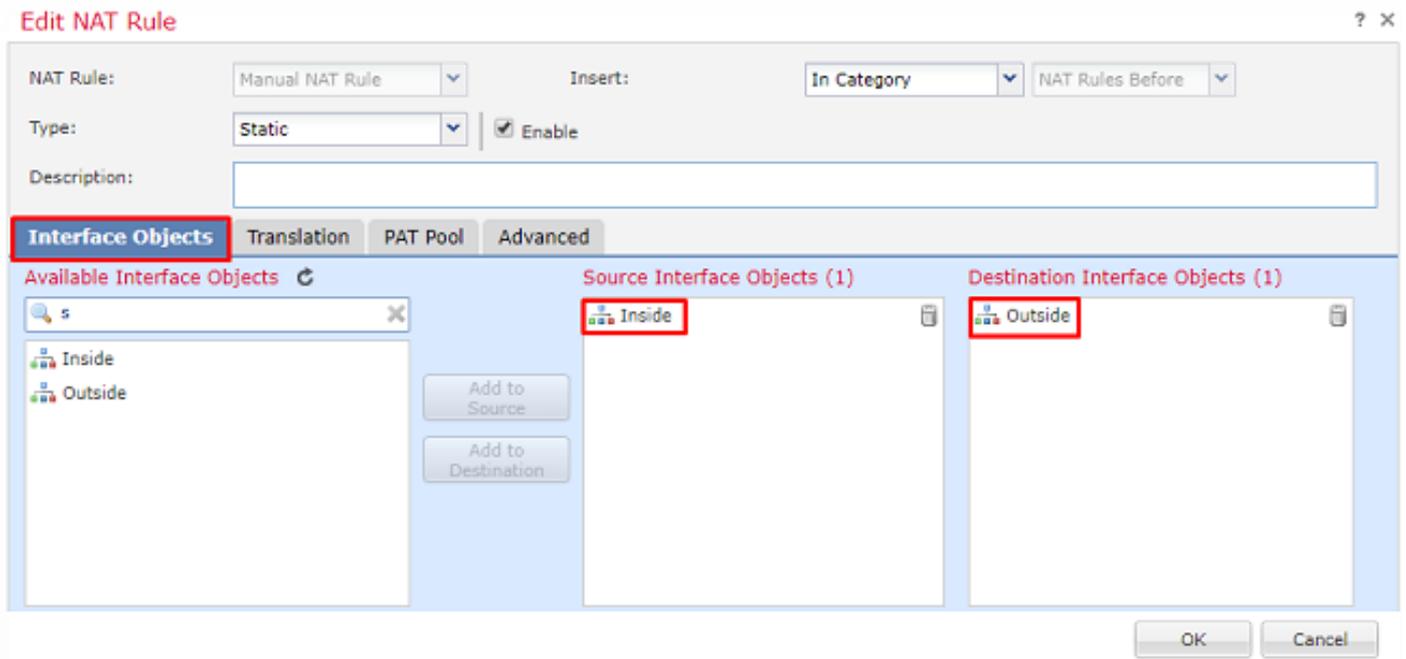
6단계. NAT 제외를 구성합니다.

VPN 트래픽에 대한 NAT 예외 문을 구성합니다. VPN 트래픽이 다른 NAT 문에 도달하여 VPN 트래픽을 잘못 변환하지 않도록 하려면 NAT 제외가 있어야 합니다.

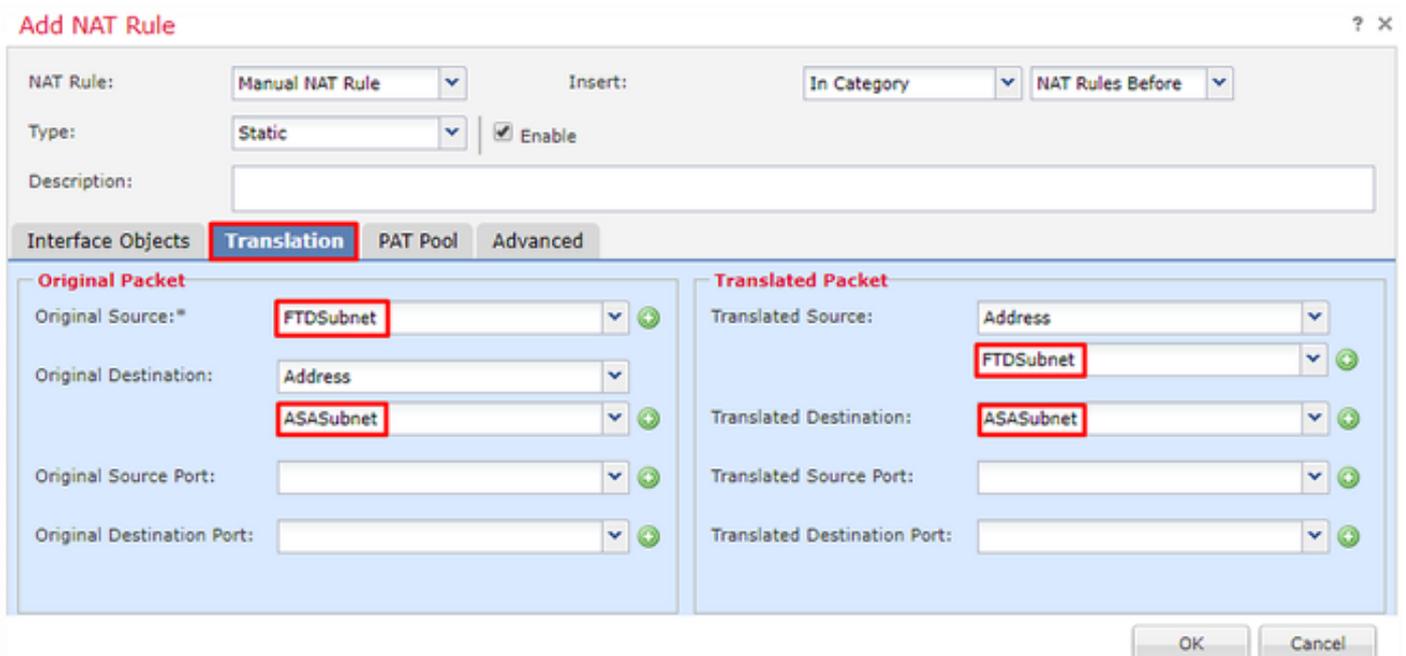
1. Devices(디바이스) > NAT로 이동하여 FTD를 대상으로 하는 NAT 정책을 선택합니다. Add Rule(규칙 추가) 버튼을 클릭할 때 새 규칙을 생성합니다.



2. 새 고정 수동 NAT 규칙을 만듭니다. 내부 및 외부 인터페이스를 참조합니다.



3. 변환 탭에서 소스 및 대상 서브넷을 선택합니다. NAT 예외 규칙이므로 이 이미지에 표시된 대로 원래 소스/대상 및 변환된 소스/대상을 동일하게 설정합니다.



4. 마지막으로 Advanced(고급) 탭으로 이동하여 no-proxy-arp 및 route-lookup을 사용하도록 설정합니다.

### Add NAT Rule

NAT Rule:  Insert:

Type:   Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

OK Cancel

5. 이 규칙을 저장하고 NAT 목록에서 최종 결과를 확인합니다.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates

VirtualFTDNAT Enter Description Show Warnings Save Cancel

Rules Policy Assignments

Filter by Device Add Rule

#	Direction	Type	Original Packet			Translated Packet			Options
			Source Interface...	Destination Interface...	Original Sources	Original Destinations	Original Services	Translated Sources	
▼ NAT Rules Before									
1	↔	Static	Inside	Outside	FTDSubnet	ASASubnet	FTDSubnet	ASASubnet	Dns:fail route-ik no-pro
▼ Auto NAT Rules									
#	↔	Dynamic	Inside	Outside	any-obj		Interface		Dns:fail
▼ NAT Rules After									

6. 컨피그레이션이 완료되면 컨피그레이션을 저장하고 FTD에 구축합니다.

7단계. ASA를 구성합니다.

1. ASA의 외부 인터페이스에서 IKEv2를 활성화합니다.

```
Crypto ikev2 enable outside
```

2. FTD에 구성된 것과 동일한 매개변수를 정의하는 IKEv2 정책을 생성합니다.

```
Crypto ikev2 policy 1
```

```
Encryption aes-256
Integrity sha256
Group 14
Prf sha256
Lifetime seconds 86400
```

3. ikev2 프로토콜을 허용하는 그룹 정책을 생성합니다.

```
Group-policy FTD_GP internal
Group-policy FTD_GP attributes
Vpn-tunnel-protocol ikev2
```

4. 피어 FTD 공용 IP 주소에 대한 터널 그룹을 생성합니다. 그룹 정책을 참조하고 사전 공유 키를 지정합니다.

```
Tunnel-group 172.16.100.20 type ipsec-l2l
Tunnel-group 172.16.100.20 general-attributes
Default-group-policy FTD_GP
Tunnel-group 172.16.100.20 ipsec-attributes
ikev2 local-authentication pre-shared-key cisco123
ikev2 remote-authentication pre-shared-key cisco123
```

5. 암호화할 트래픽을 정의하는 액세스 목록을 만듭니다. (FTDSubnet 10.10.113.0/24)  
(ASASubnet 10.10.110.0/24)

```
Object network FTDSUBNET
Subnet 10.10.113.0 255.255.255.0
Object network ASASUBNET
Subnet 10.10.110.0 255.255.255.0
Access-list ASAToFTD extended permit ip object ASASUBNET object FTDSUBNET
```

6. FTD에 지정된 알고리즘을 참조하여 ikev2 ipsec 제안서를 생성합니다.

```
Crypto ipsec ikev2 ipsec-proposal FTD
Protocol esp encryption aes-gcm-256
```

7. 구성을 함께 연결하는 암호화 맵 항목을 생성합니다.

```
Crypto map outside_map 10 set peer 172.16.100.20
```

```
Crypto map outside_map 10 match address ASAtoFTD
Crypto map outside_map 10 set ikev2 ipsec-proposal FTD
Crypto map outside_map 10 interface outside
```

8. 방화벽에서 VPN 트래픽을 NAT하지 못하도록 하는 NAT 예외 문을 만듭니다.

```
Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FTDSubnet FTDSubnet no-
```

다음을 확인합니다.

---

 참고: 현재로서는 FMC에서 VPN 터널 상태를 검토할 수 있는 방법이 없습니다. 이 기능 CSCvh77603에 대한 개선 요청이 [있습니다](#).

---

VPN 터널을 통해 트래픽을 시작하려고 합니다. ASA 또는 FTD의 명령줄에 액세스할 경우 packet tracer 명령을 사용하여 이 작업을 수행할 수 있습니다. packet-tracer 명령을 사용하여 VPN 터널을 가동할 때는 반드시 두 번 실행하여 터널이 가동되는지 확인해야 합니다. 명령이 처음 실행되면 VPN 터널이 중단되므로 VPN encrypt DROP(VPN 암호화 삭제)으로 packet-tracer 명령이 실패합니다. 방화벽의 내부 IP 주소는 항상 실패하므로 패킷 추적기에서 소스 IP 주소로 사용하지 마십시오.

```
firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10
```

```
Phase: 10
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:
```

```
firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10
```

```
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.100.1 using egress ifc outside
```

```
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet no-proxy-
Additional Information:
NAT divert to egress interface outside
```

Untranslate 10.10.110.10/0 to 10.10.110.10/0

Phase: 3

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip ifc Inside object-group FMC_INLINE_src_rule_268436483 ifc ou
```

```
access-list CSM_FW_ACL_ remark rule-id 268436483: ACCESS POLICY: FTD-Access-Control-Policy - Mandatory
```

```
access-list CSM_FW_ACL_ remark rule-id 268436483: L7 RULE: VPN_Traffic
```

```
object-group network FMC_INLINE_src_rule_268436483
```

```
description: Auto Generated by FMC from src of UnifiedNGFWRule# 1 (FTD-Access-Control-Policy/mandatory)
```

```
network-object object ASASubnet
```

```
network-object object FTDSubnet
```

```
object-group network FMC_INLINE_dst_rule_268436483
```

```
description: Auto Generated by FMC from dst of UnifiedNGFWRule# 1 (FTD-Access-Control-Policy/mandatory)
```

```
network-object object ASASubnet
```

```
network-object object FTDSubnet
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: NAT

Subtype:

Result: ALLOW

Config:

```
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet no-proxy-
```

Additional Information:

Static translate 10.10.113.10/0 to 10.10.113.10/0

Phase: 10

Type: VPN

Subtype: encrypt

Result: ALLOW

Config:

Additional Information:

Result:

```
input-interface: Inside
```

```
input-status: up
```

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

```
output-interface: outside
```

```
output-status: up
```

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

```
Action: allow
```

터널 상태를 모니터링하려면 FTD 또는 ASA의 CLI로 이동합니다.

FTD CLI에서 다음 명령을 사용하여 phase-1 및 phase-2를 확인합니다.

crypto ikev2 sa 표시

```
<#root>
```

```
> show crypto ikev2 sa
```

IKEV2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote
	9528731 172.16.100.20/500	192.168.200.10/500

READY

INITIATOR

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK  
Life/Active Time: 86400/118 sec

Child sa: local selector

10.10.113.0/0 - 10.10.113.255/65535

remote selector

10.10.110.0/0 - 10.10.110.255/65535

ESP spi in/out:

0x66be357d/0xb74c8753

## 문제 해결 및 디버그

### 초기 연결 문제

VPN을 구축할 때 양쪽이 터널을 협상합니다. 따라서 어떤 유형의 터널 장애도 트러블슈팅할 때 대화의 양쪽을 모두 가져오는 것이 가장 좋습니다. IKEv2 터널을 디버그하는 방법에 대한 자세한 설명서는 [How to debug IKEv2 VPNs\(IKEv2 VPN을 디버깅하는 방법\)을 참조하십시오.](#)

터널 장애의 가장 일반적인 원인은 연결 문제입니다. 이를 확인하는 가장 좋은 방법은 디바이스에서 패킷 캡처를 수행하는 것입니다. 디바이스에서 패킷 캡처를 수행하려면 다음 명령을 사용합니다

```
Capture capout interface outside match ip host 172.16.100.20 host 192.168.200.10
```

캡처가 제자리에 있으면 VPN을 통해 트래픽을 전송하고 패킷 캡처에서 양방향 트래픽을 확인합니다.

다음 명령을 사용하여 패킷 캡처를 검토합니다.

### 캡아웃 표시

```
firepower# show cap capout
```

```
4 packets captured
```

1: 11:51:12.059628	172.16.100.20.500 > 192.168.200.10.500:	udp 690
2: 11:51:12.065243	192.168.200.10.500 > 172.16.100.20.500:	udp 619
3: 11:51:12.066692	172.16.100.20.500 > 192.168.200.10.500:	udp 288
4: 11:51:12.069835	192.168.200.10.500 > 172.16.100.20.500:	udp 240

## 트래픽 관련 문제

일반적인 트래픽 문제는 다음과 같습니다.

- FTD 뒤에 라우팅 문제 — 내부 네트워크에서 할당된 IP 주소 및 VPN 클라이언트로 패킷을 다시 라우팅할 수 없습니다.
- 액세스 제어 목록은 트래픽을 차단합니다.
- VPN 트래픽에 대해 네트워크 주소 변환이 우회되지 않습니다.

FMC에서 관리하는 FTD의 VPN에 대한 자세한 내용은 [FTD managed by FMC 컨피그레이션 가이드를 참조하십시오.](#)

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.