

FMC에서 관리하는 FTD의 경로 기반 사이트 대 사이트 VPN 터널 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[제한 사항](#)

[FMC의 컨피그레이션 단계](#)

[다음을 확인합니다.](#)

[FMC GUI에서](#)

[FTD CLI에서](#)

소개

이 문서에서는 Firepower Management Center에서 관리하는 Firepower Threat Defense에서 고정 경로 기반 사이트 대 사이트 VPN 터널을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- VPN 터널의 작동 방식에 대한 기본 이해
- FMC를 탐색하는 방법을 이해합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco FMC(Firepower Management Center) 버전 6.7.0
- Cisco FTD(Firepower Threat Defense) 버전 6.7.0

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

경로 기반 VPN을 사용하면 VPN 터널을 통해 보내거나 암호화해야 하는 관심 트래픽을 결정할 수 있으며, 정책 기반 또는 암호화 맵 기반 VPN에서처럼 정책/액세스 목록 대신 트래픽 라우팅을 사용할 수 있습니다. 암호화 도메인은 IPsec 터널로 들어오는 모든 트래픽을 허용하도록 설정됩니다. IPsec 로컬 및 원격 트래픽 선택기는 0.0.0.0/0.0.0.0으로 설정됩니다. 즉, IPsec 터널로 라우팅되는 트래픽은 소스/대상 서브넷과 상관없이 암호화됩니다.

이 문서에서는 SVTI(Static Virtual Tunnel Interface) 컨피그레이션에 대해 중점적으로 설명합니다. 보안 방화벽의 DVTI(Dynamic Virtual Tunnel Interface) 컨피그레이션은 이 문서를 [참조하십시오](#).

제한 사항

FTD의 경로 기반 터널에 대한 알려진 제한 사항:

- Ipsec만 지원합니다. GRE는 지원되지 않습니다.
- IPv4 인터페이스뿐 아니라 IPv4, 보호 네트워크 또는 VPN 페이로드만 지원합니다(IPv6는 지원되지 않음).
- VPN에 대한 트래픽을 분류하는 VTI 인터페이스에는 정적 라우팅 및 BGP 동적 라우팅 프로토콜만 지원됩니다(OSPF, RIP 등의 다른 프로토콜은 지원되지 않음).
- 인터페이스당 100개의 VTI만 지원됩니다.
- VTI는 FTD 클러스터에서 지원되지 않습니다.
- VTI는 다음 정책에서 지원되지 않습니다.
 - QoS
 - NAT
 - 플랫폼 설정

새 VPN 터널의 경우 FMC/FTD 버전 6.7.0에서는 이러한 알고리즘이 더 이상 지원되지 않습니다. FMC는 FTD < 6.7을 관리하기 위해 제거된 모든 암호를 지원합니다.

- 3DES, DES 및 NULL 암호화는 IKE 정책에서 지원되지 않습니다.
- DH 그룹 1, 2, 24는 IKE 정책 및 IPsec 제안에서 지원되지 않습니다.
- MD5 무결성은 IKE 정책에서 지원되지 않습니다.
- PRF MD5는 IKE 정책에서 지원되지 않습니다.
- DES, 3DES, AES-GMAC, AES-GMAC-192 및 AES-GMAC-256 암호화 알고리즘은 IPsec 제

안서에서 지원되지 않습니다.

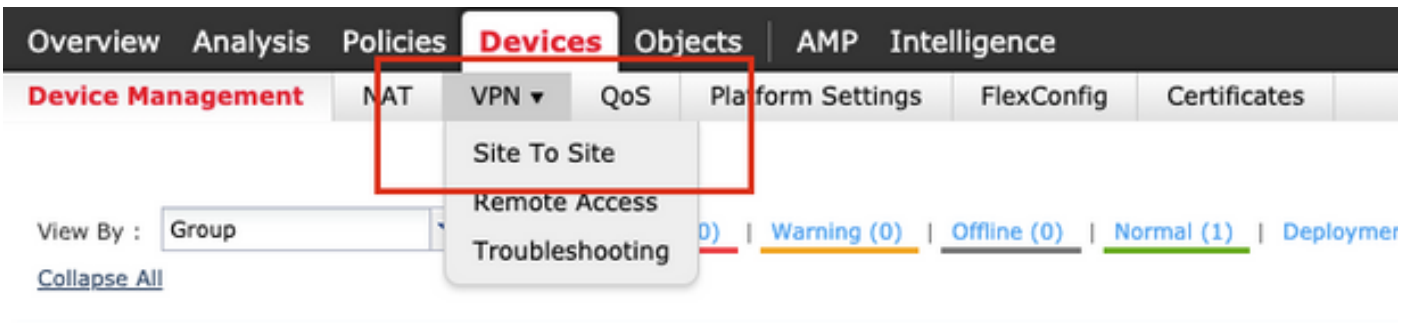
참고: 사이트 대 사이트 경로 기반은 물론 정책 기반 VPN 터널에 대해서도 마찬가지입니다. 이전 FTD를 FMC에서 6.7로 업그레이드하기 위해, 업그레이드를 차단하는 제거된 암호와 관련된 변경 사항에 대해 사용자에게 경고하는 사전 검증 확인 경고가 트리거됩니다.

FMC 6.7을 통해 관리되는 FTD 6.7	사용 가능한 구성	사이트 대 사이트 VPN 터널
신규 설치	약한 암호는 사용할 수 있지만 FTD 6.7 디바이스를 구성하는데 사용할 수 없습니다.	약한 암호는 사용할 수 있지만 FTD 6.7 디바이스를 구성하는데 사용할 수 없습니다.
업그레이드: 약한 암호로만 구성된 FTD	FMC 6.7 UI에서 업그레이드하면 사전 검증 확인에 오류가 표시됩니다. 재구성할 때까지 업그레이드가 차단됩니다.	FTD 업그레이드 후 피어가 설정을 변경하지 않았다고 가정할 경우 터널이 종료됩니다.
업그레이드: 일부 약한 암호와 일부 강한 암호로만 구성된 FTD	FMC 6.7 UI에서 업그레이드하면 사전 검증 확인에 오류가 표시됩니다. 재구성할 때까지 업그레이드가 차단됩니다.	FTD 업그레이드 후 피어에 강력한 암호가 있다고 가정하고 터널을 다시 설정합니다.
업그레이드: Class C 국가(강력한 암호화 라이선스가 없음)	DES 허용이 허용됨	DES 허용이 허용됨

참고: 추가 라이선스는 필요하지 않으며, Route Based VPN은 Licensed(라이선스) 및 Evaluation(평가) 모드에서 구성할 수 있습니다. 암호화 규정 준수(Export Controlled Features Enabled)가 없으면 DES만 암호화 알고리즘으로 사용할 수 있습니다.

FMC의 컨피그레이션 단계

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



2단계. Add VPN(VPN 추가)을 클릭하고 이미지에 표시된 대로 Firepower Threat Defense Device(위협 방어 디바이스)를 선택합니다.



Deploy

System

Help ▾

admin ▾



Add VPN ▾

Firepower Device

Firepower Threat Defense Device

3단계. Topology Name(토폴로지 이름)을 제공하고 Type of VPN(VPN 유형)을 VTI(Route Based)로 선택합니다. IKE 버전을 선택합니다.

이 데모의 목적:

토폴로지 이름: VTI-ASA

IKE 버전: IKEv2

Topology Name:*

VTI-ASA

Policy Based (Crypto Map) Route Based (VTI)

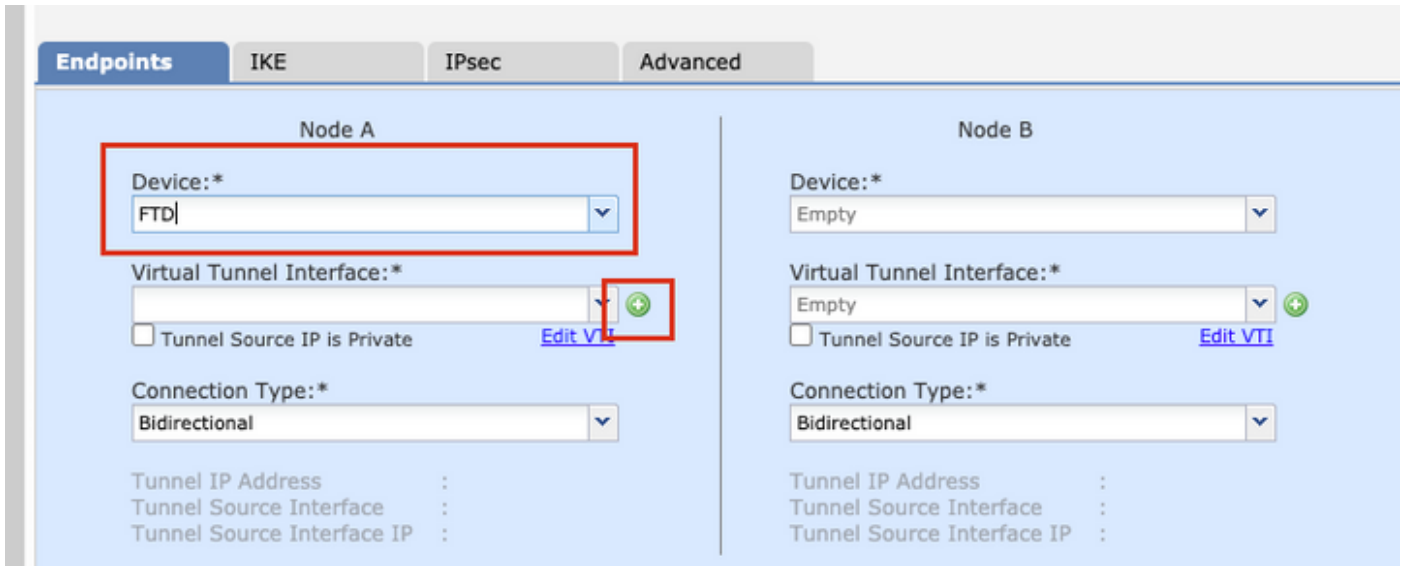
Network Topology:

Point to Point Hub and Spoke Full Mesh

IKE Version:*

IKEv1 IKEv2

4단계. 터널을 구성해야 하는 디바이스를 선택하거나, 새 가상 템플릿 인터페이스를 추가(+ 아이콘 클릭)하거나 기존 목록에서 하나를 선택할 수 있습니다.



5단계. 새 가상 터널 인터페이스의 매개변수를 정의합니다. OK(확인)를 클릭합니다.

이 데모의 목적:

이름: VTI-ASA

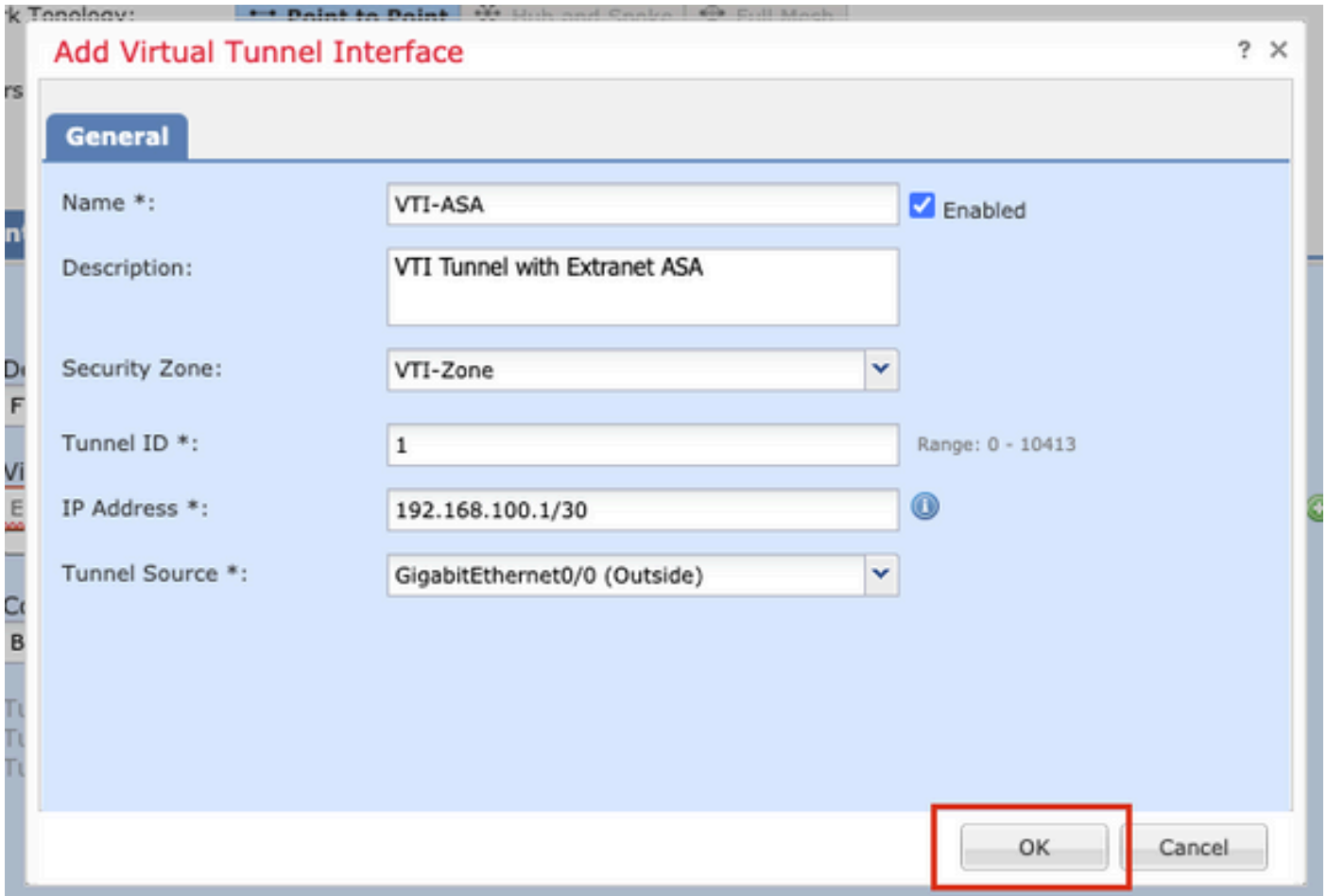
설명(선택 사항): 엑스트라넷 ASA를 사용하는 VTI 터널

보안 영역: VTI 영역

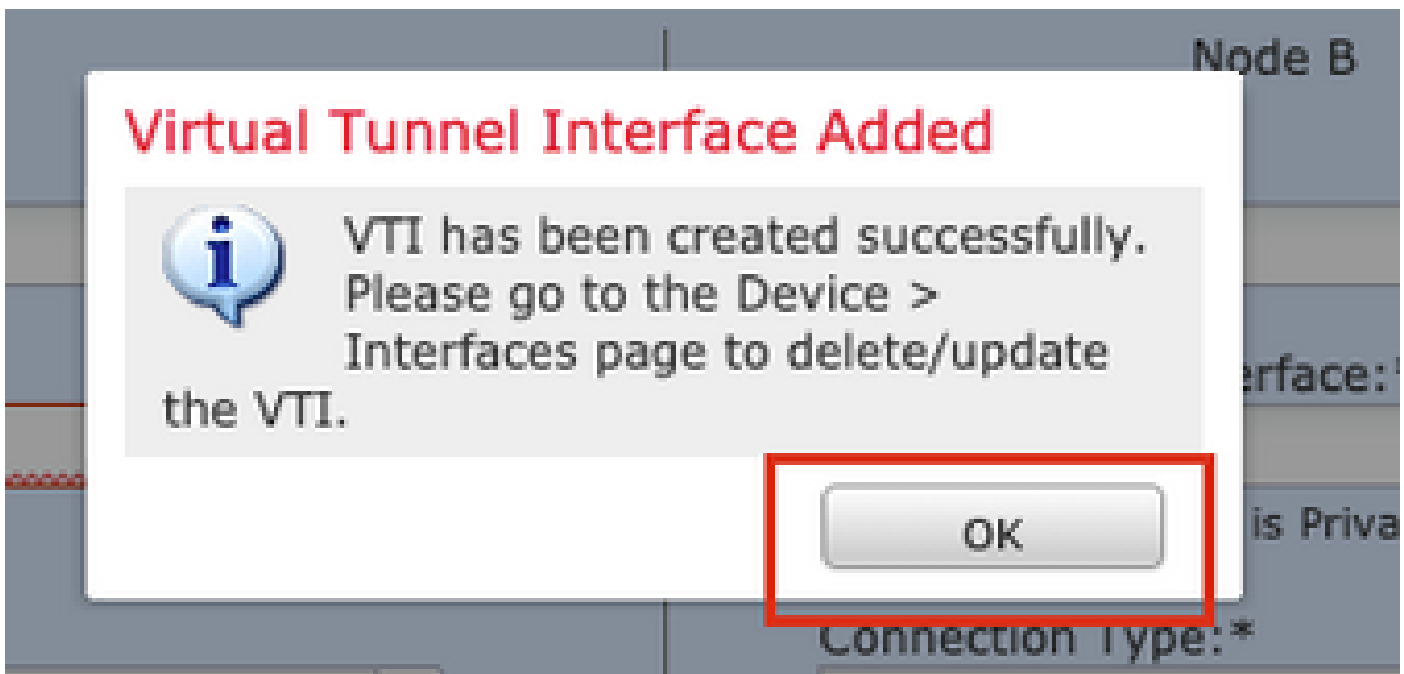
터널 ID: 1

IP 주소: 192.168.100.1/30

터널 소스: GigabitEthernet0/0(외부)



6단계. 새 VTI가 생성되었음을 알리는 팝업에서 OK를 클릭합니다.



7단계. 새로 생성된 VTI 또는 Virtual Tunnel Interface(가상 터널 인터페이스) 아래에 있는 VTI를 선택합니다. 노드 B(피어 디바이스)에 대한 정보를 제공합니다.

이 데모의 목적:

장치: 엑스트라넷

디바이스 이름: ASA-Peer

엔드포인트 IP 주소: 10.106.67.252

Create New VPN Topology

Topology Name: *

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

IKE Version: * IKEv1 IKEv2

Endpoints | IKE | IPsec | Advanced

Node A

Device: *

Virtual Tunnel Interface: *

Tunnel Source IP is Private

Connection Type: *

Tunnel IP Address : 192.168.100.1
Tunnel Source Interface : Outside
Tunnel Source Interface IP : 10.197.224.90

Additional Configuration ⓘ
Route traffic to the VTI : [Routing Policy](#)
Permit VPN traffic : [AC Policy](#)

Node B


Device: *

Device Name: *

Endpoint IP Address: *

8단계. IKE 탭으로 이동합니다. 사전 정의된 정책을 사용하도록 선택하거나 정책 탭 옆의 + 버튼을 클릭하고 새 정책을 생성할 수 있습니다.

IKEv2 Settings

Policy:* AES-GCM-NULL-SHA-LATEST 

Authentication Type: Pre-shared Automatic Key

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

9단계(새 IKEv2 정책을 생성하는 경우 선택 사항) 정책의 Name(이름)을 입력하고 정책에서 사용할 Algorithms(알고리즘)를 선택합니다. 저장을 클릭합니다.

이 데모의 목적:

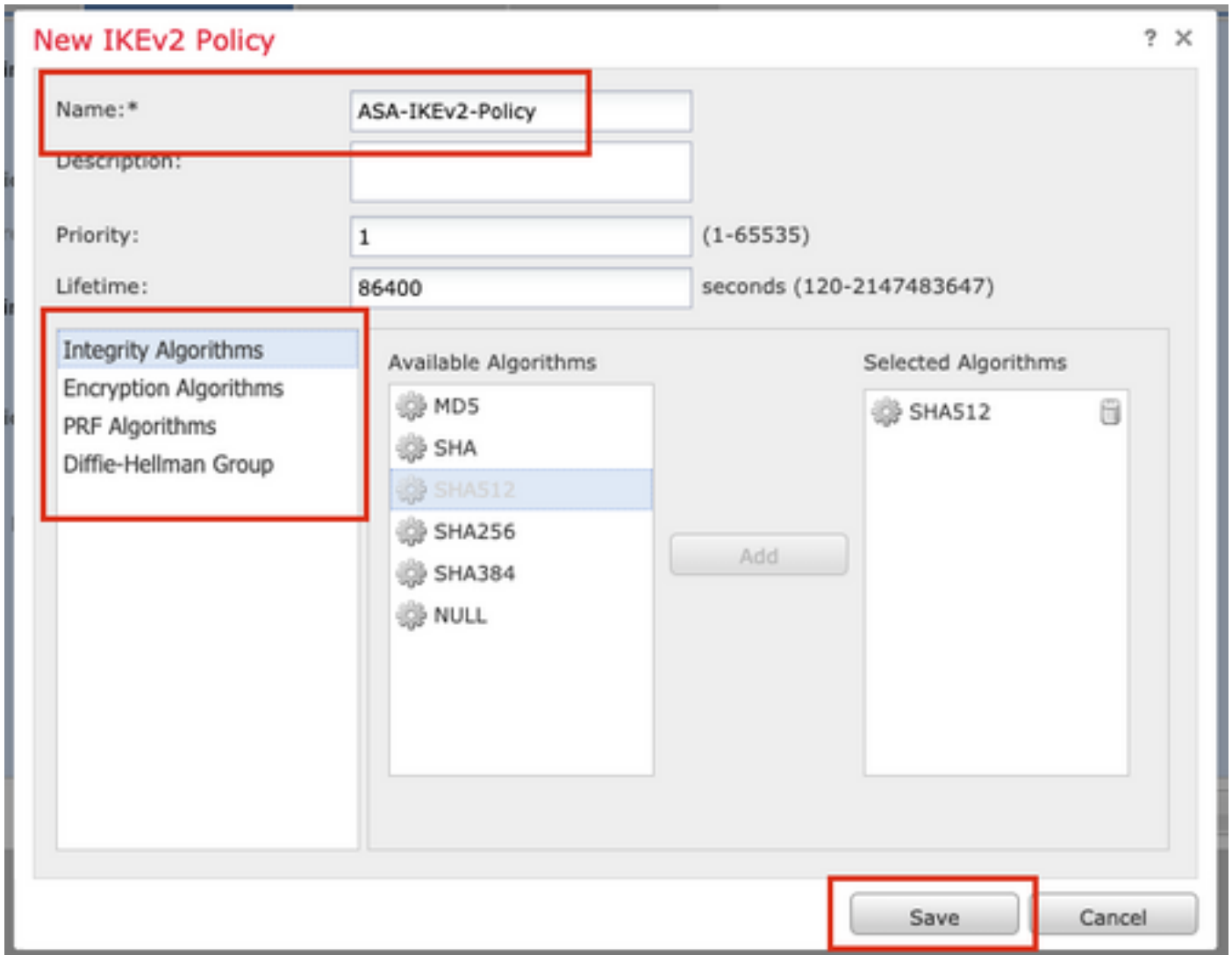
이름: ASA-IKEv2-Policy

무결성 알고리즘: SHA-512

암호화 알고리즘: AES-256

PRF 알고리즘: SHA-512

Diffie-Hellman 그룹: 21



10단계. 새로 생성한 정책 또는 존재하는 정책을 선택합니다. 인증 유형을 선택합니다. 사전 공유 수동 키를 사용하는 경우 키 및 확인 키 상자에 키를 입력합니다.

이 데모의 목적:

정책: ASA-IKEv2-Policy

인증 유형: 사전 공유 수동 키

키: cisco123

확인 키: cisco123

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh14_3 [v] [+]

Authentication Type: Pre-shared Automatic Key [v]

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

IKEv2 Settings


Policy:* ASA-IKEv2-Policy [v] [+]

Authentication Type: Pre-shared Manual Key [v]

Key:* [.....]

Confirm Key:* [.....]

Enforce hex-based pre-shared key only



 참고: 두 엔드포인트가 동일한 FMC에 등록된 경우 사전 공유 자동 키 옵션도 사용할 수 있습니다.

11단계. IPsec 탭으로 이동합니다. 사전 정의된 IKEv2 IPsec 제안을 사용하도록 선택하거나 새로 생성할 수 있습니다. IKEv2 IPsec Proposal(IKEv2 IPsec 제안) 탭 옆에 있는 Edit(편집) 버튼을 클릭합니다.

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel [v]

Transform Sets:

IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

tunnel_aes256_sha AES-GCM

Enable Security Association (SA) Strength Enforcement

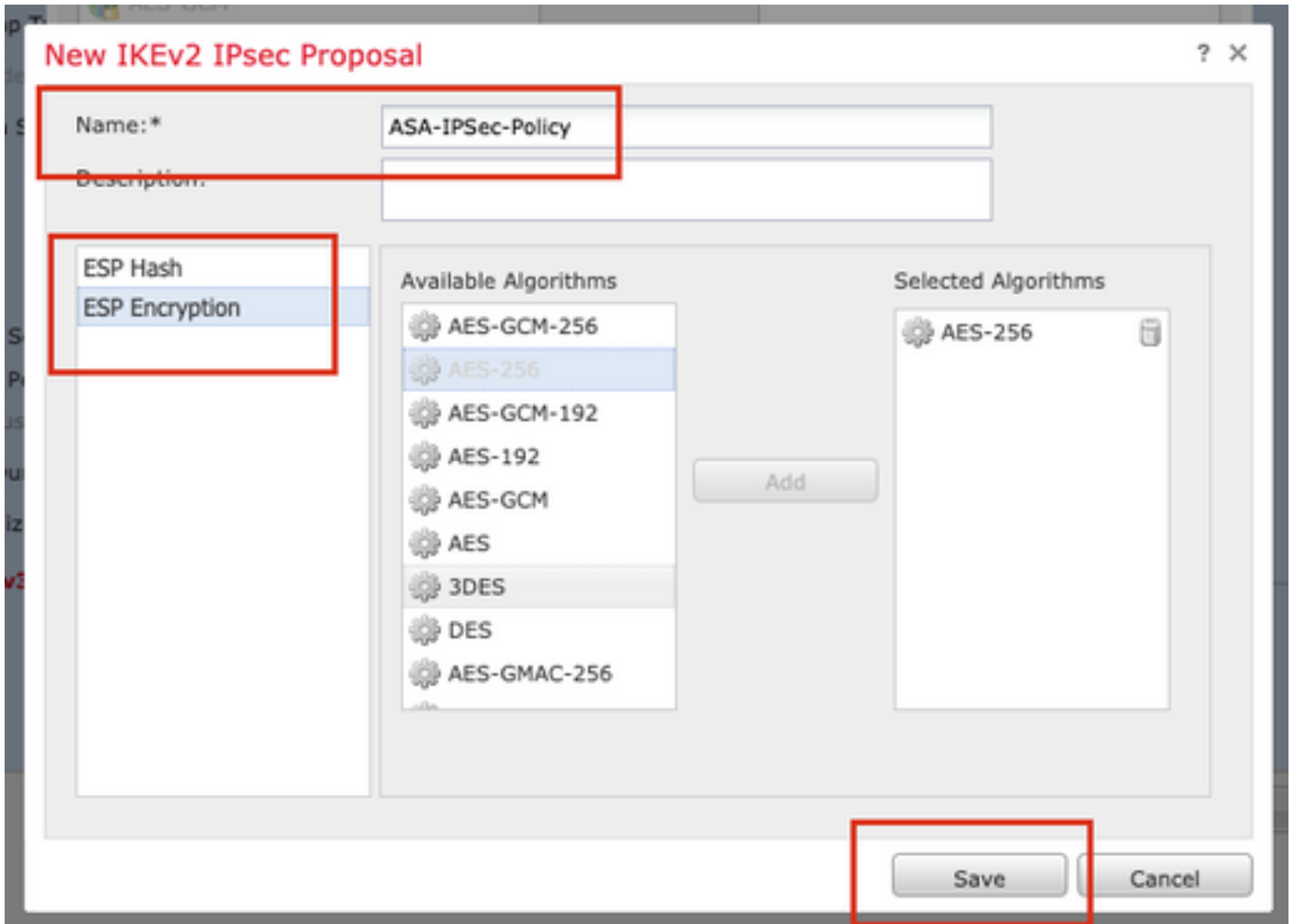
12단계(새 IKEv2 IPsec 제안을 만드는 경우 선택 사항) 제안서 이름을 입력하고 제안서에 사용할 알고리즘을 선택합니다. 저장을 클릭합니다.

이 데모의 목적:

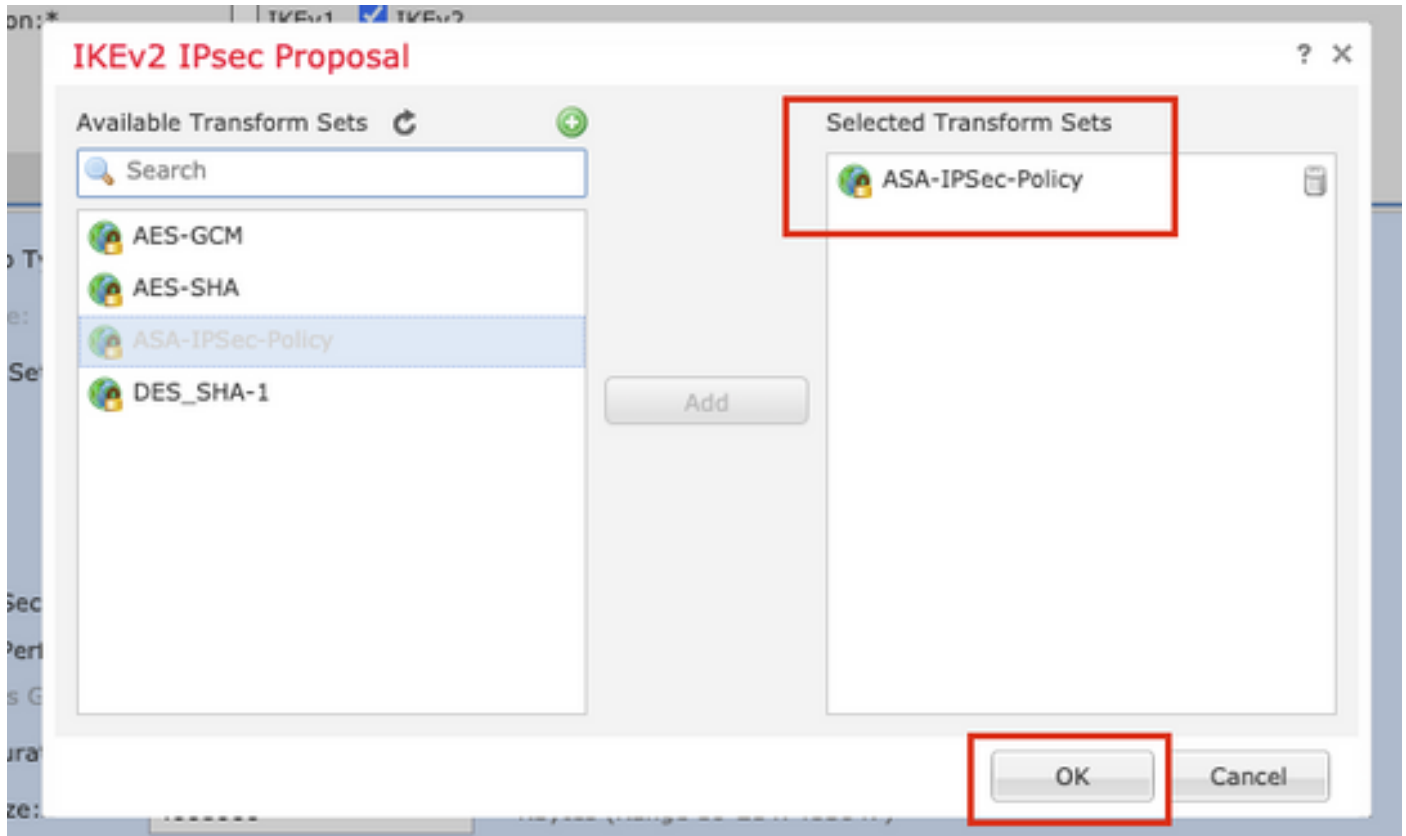
Name(이름): ASA-IPSec-Policy

ESP 해시: SHA-512

ESP 암호화: AES-256



13단계. 사용 가능한 제안의 목록에서 새로 생성한 제안서 또는 존재하는 제안을 선택합니다. OK(확인)를 클릭합니다.



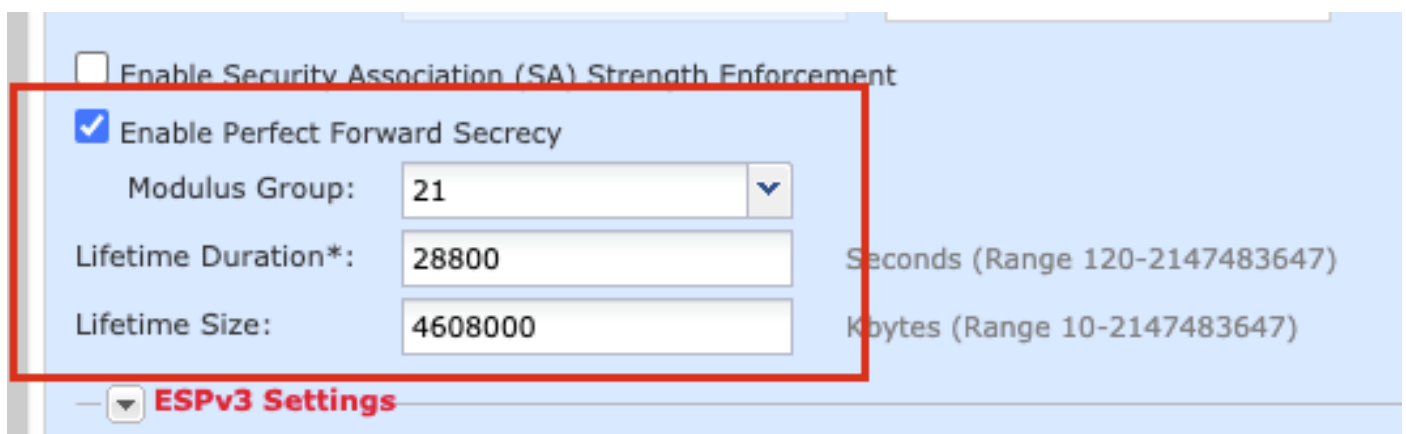
14단계. (선택 사항) Perfect Forward Secrecy 설정을 선택합니다. IPsec 수명 기간 및 수명 크기를 구성합니다.

이 데모의 목적:

PFS(Perfect Forward Secrecy): 모듈러스 그룹 21

수명 기간: 28800(기본값)

수명 크기: 4608000(기본값)



15단계. 구성된 설정을 확인합니다. 이 이미지에 표시된 대로 Save를 클릭합니다.

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 Perfect Forward Secrecy


Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

— **ESPv3 Settings** —

16단계. 액세스 제어 정책을 구성합니다. Policies(정책) > Access Control(액세스 제어) > Access Control(액세스 제어)로 이동합니다. FTD에 적용된 정책을 수정합니다.

 참고: sysopt connection permit-vpn은 경로 기반 VPN 터널에서 작동하지 않습니다. 액세스 제어 규칙은 IN-> OUT 영역과 OUT -> IN 영역에 대해 모두 구성해야 합니다.

Zones(영역) 탭에서 Source Zones(소스 영역)와 Destination Zones(대상 영역)를 제공합니다.

Networks(네트워크) 탭에서 Source Networks(소스 네트워크), Destination Networks(대상 네트워크)를 제공합니다. Add(추가)를 클릭합니다.

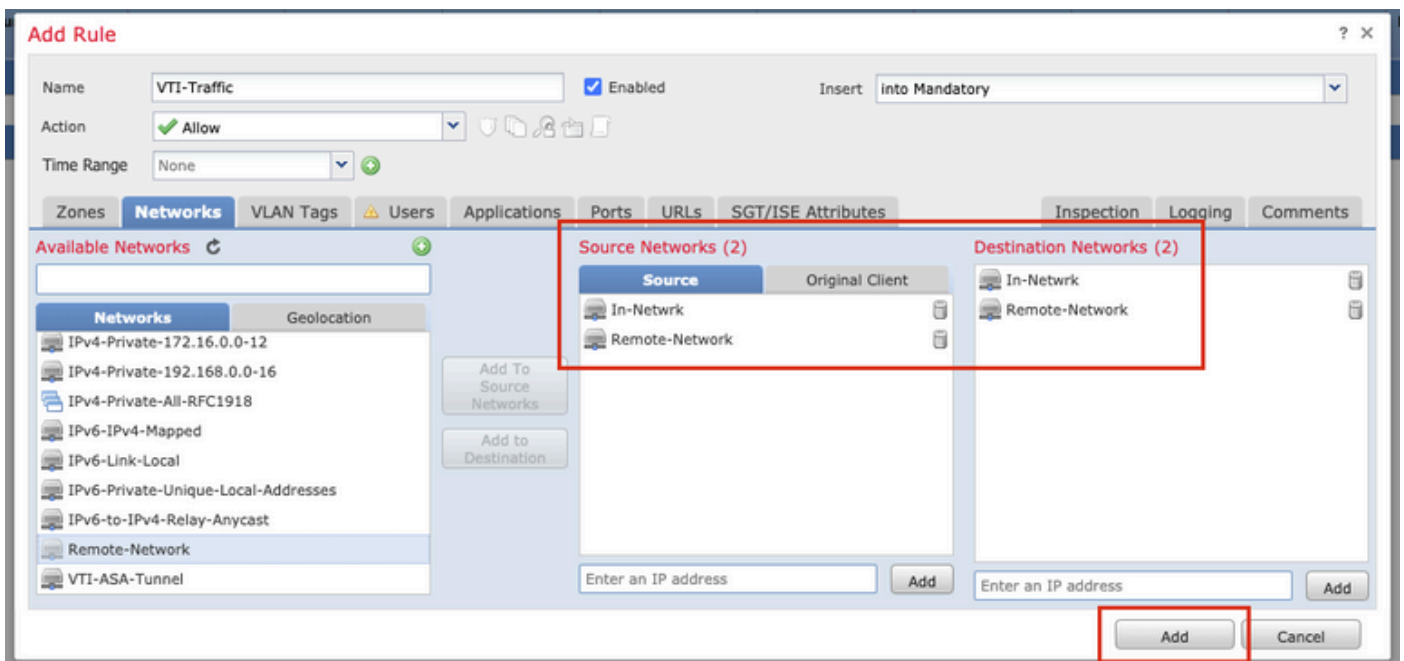
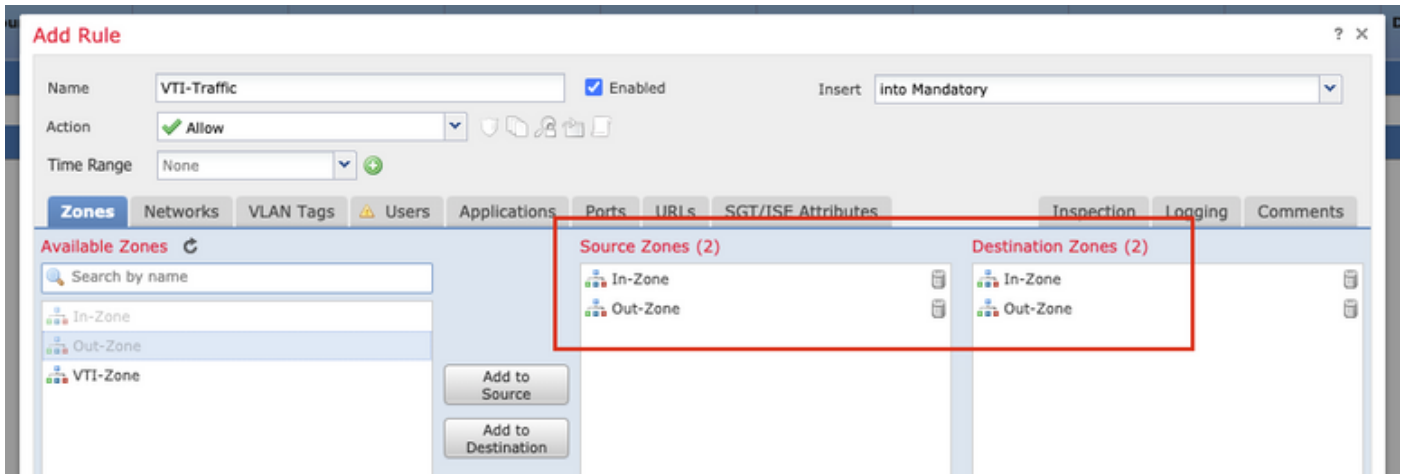
이 데모의 목적:

소스 영역: 영역 내(In-Zone) 및 영역 외(Out-Zone)

대상 영역: Out-Zone 및 In-Zone

소스 네트워크: 네트워크 내 및 원격 네트워크

대상 네트워크: 원격 네트워크 및 네트워크 내



17단계. VTI 터널을 통해 라우팅을 추가합니다. Devices(디바이스) > Device Management(디바이스 관리)로 이동합니다. VTI 터널이 구성된 디바이스를 편집합니다.

Routing(라우팅) 탭에서 Static Route(고정 경로)로 이동합니다. Add Route(경로 추가)를 클릭합니다.

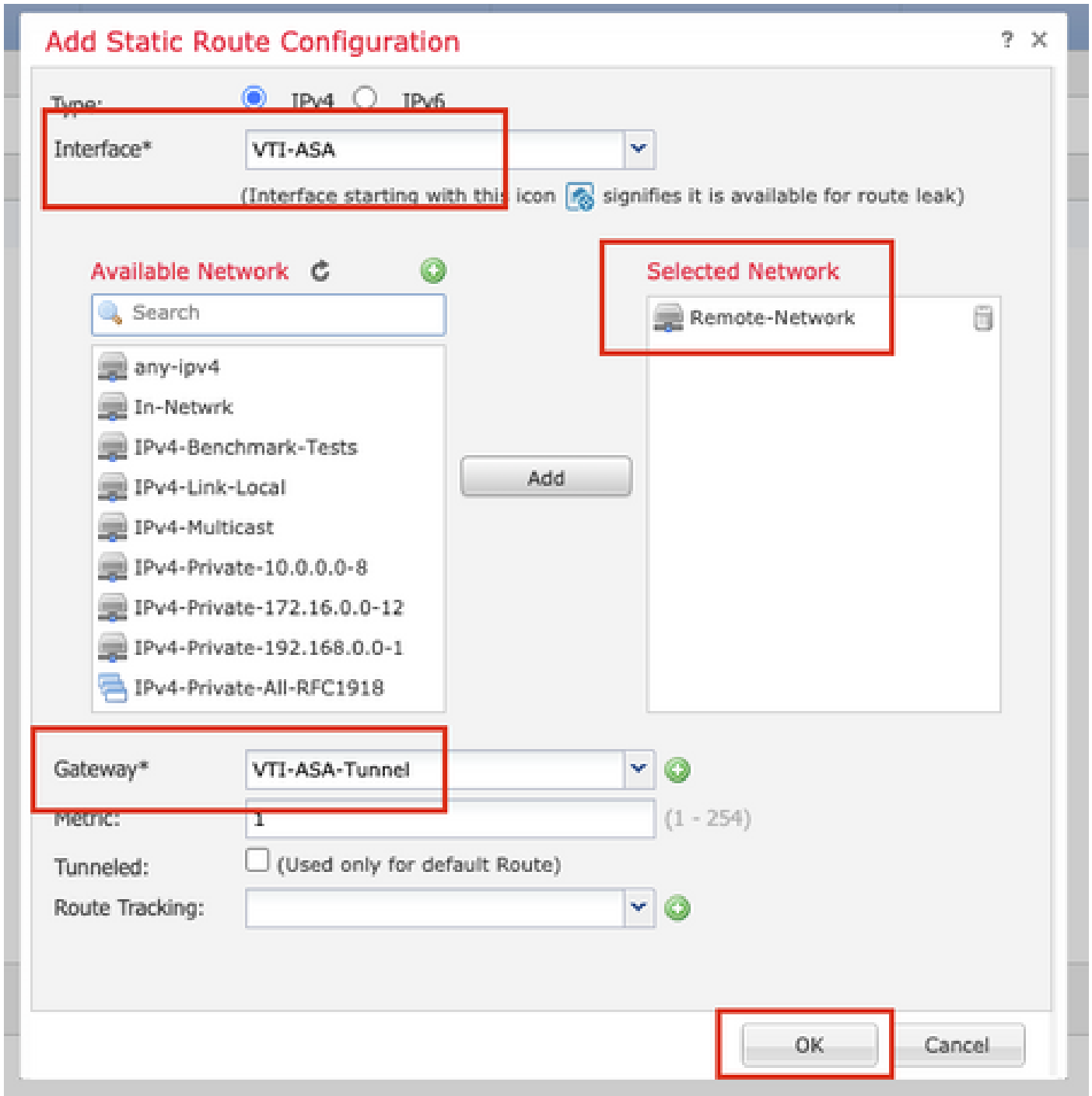
인터페이스를 제공하고, 네트워크를 선택하고, 게이트웨이를 제공합니다. OK(확인)를 클릭합니다.

이 데모의 목적:

인터페이스: VTI-ASA

네트워크: 원격 네트워크

게이트웨이: VTI-ASA-터널



18단계. Deploy(구축) > Deployment(구축)로 이동합니다. 컨피그레이션을 구축해야 하는 FTD를 선택하고 Deploy(구축)를 클릭합니다.

구축에 성공한 후 컨피그레이션이 FTD CLI에 푸시됨:

```
<#root>
```

```
crypto ikev2 policy 1
```

```
encryption aes-256
integrity sha512
group 21
prf sha512
lifetime seconds 86400
```

```
crypto ikev2 enable Outside

crypto ipsec ikev2 ipsec-proposal CSM_IP_1

protocol esp encryption aes-256
protocol esp integrity sha-512

crypto ipsec profile FMC_IPSEC_PROFILE_1

set ikev2 ipsec-proposal CSM_IP_1
set pfs group21

group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ikev1 ikev2

tunnel-group 10.106.67.252 type ipsec-l2l
tunnel-group 10.106.67.252 general-attributes
default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****

interface Tunnel1

description VTI Tunnel with Extranet ASA
nameif VTI-ASA

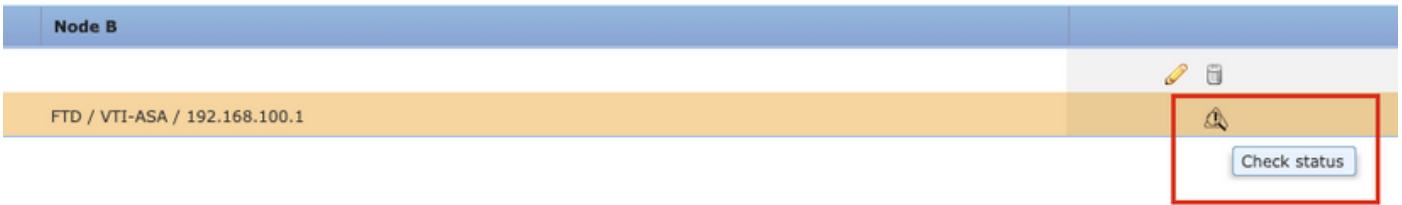
ip address 192.168.100.1 255.255.255.252
tunnel source interface Outside
tunnel destination 10.106.67.252
tunnel mode ipsec ipv4

tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

다음을 확인합니다.

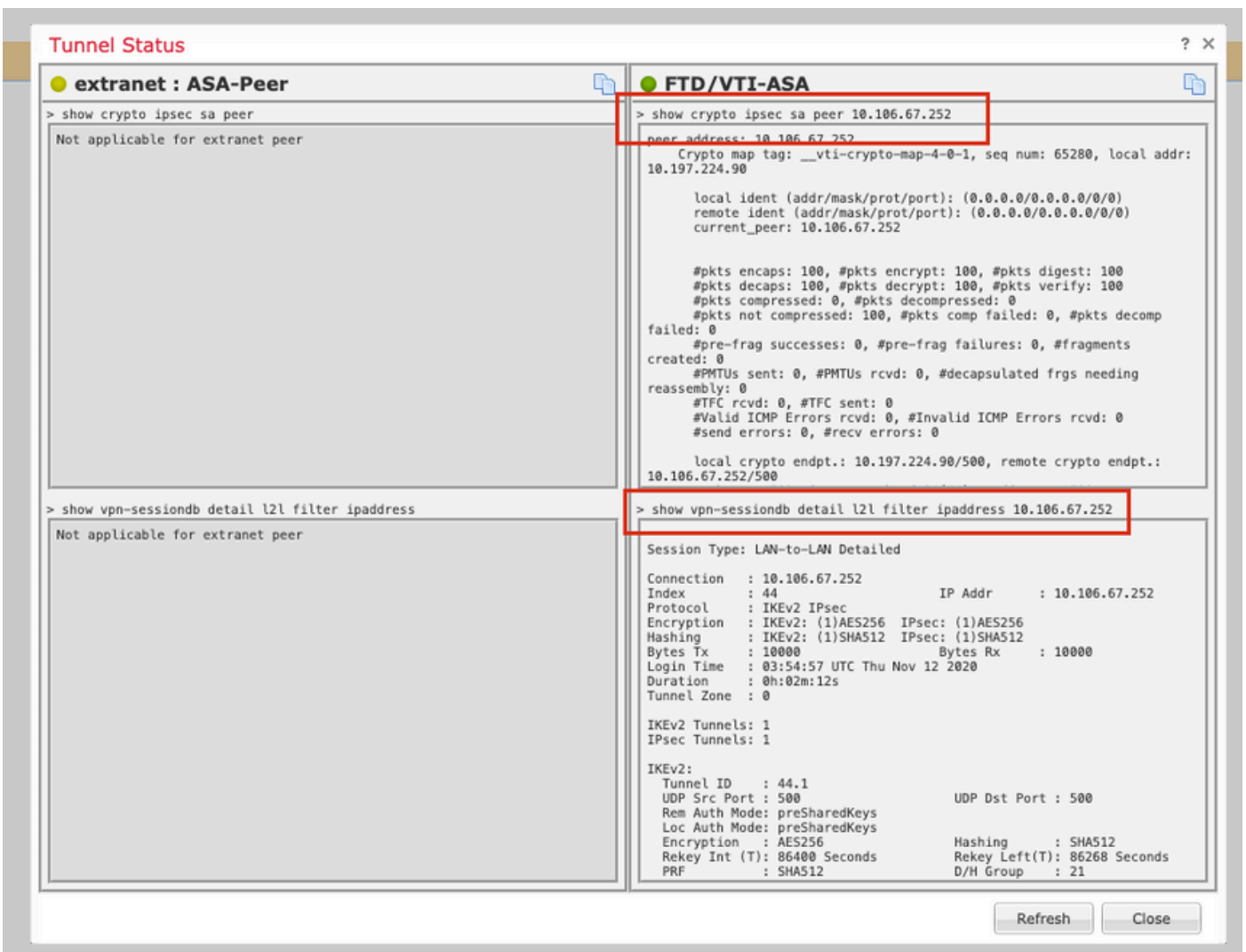
FMC GUI에서

GUI 자체에서 VPN 터널의 라이브 상태를 모니터링하려면 Check Status 옵션을 클릭합니다



여기에는 FTD CLI에서 가져온 다음 명령이 포함됩니다.

- show crypto ipsec sa peer <Peer IP Address>
- show vpn-sessiondb detail l2l filter ipaddress <Peer IP Address>



FTD CLI에서

이러한 명령은 FTD CLI에서 VPN 터널의 컨피그레이션 및 상태를 보는 데 사용할 수 있습니다.

```
show running-config crypto
show running-config nat
show running-config route
```

```
show crypto ikev1 sa detailed
show crypto ikev2 sa detailed
show crypto ipsec sa detailed
show vpn-sessiondb detail 121
```

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.