FDM에서 관리하는 FTD에서 사이트 대 사이트 VPN 구성

목차

소개

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

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- VPN에 대한 기본 이해
- FDN을 사용한 경험
- ASA(Adaptive Security Appliance) 명령행 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 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

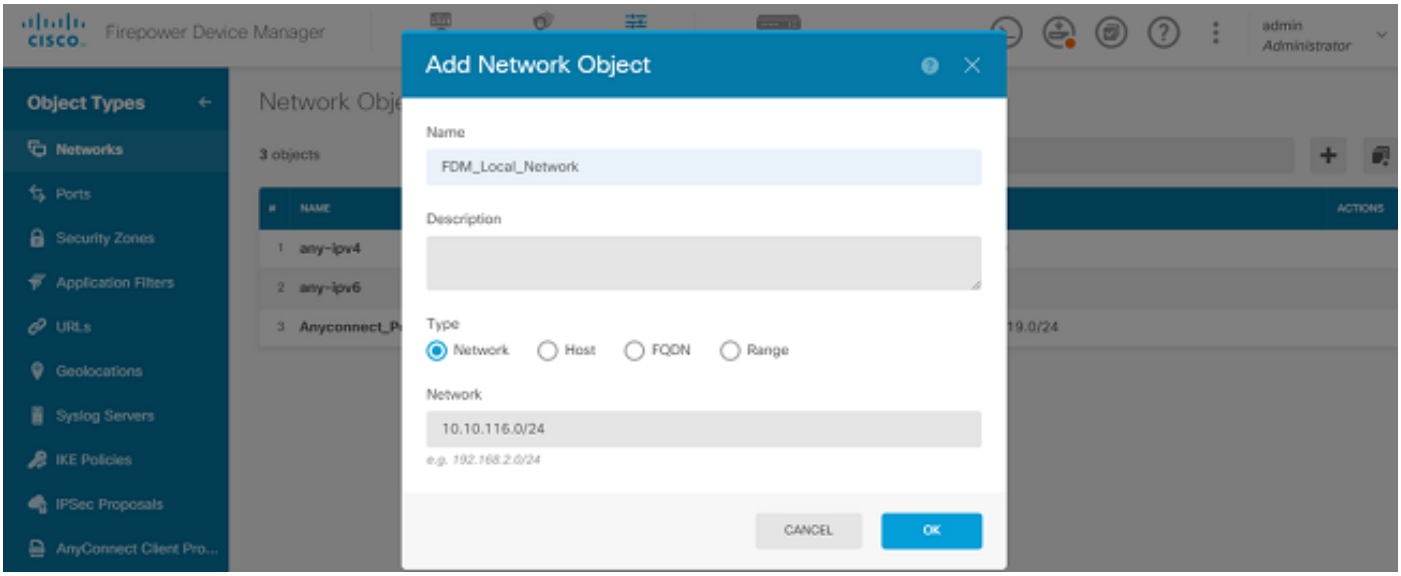
구성

FTD에서 FDM을 사용하여 컨피그레이션으로 시작합니다.

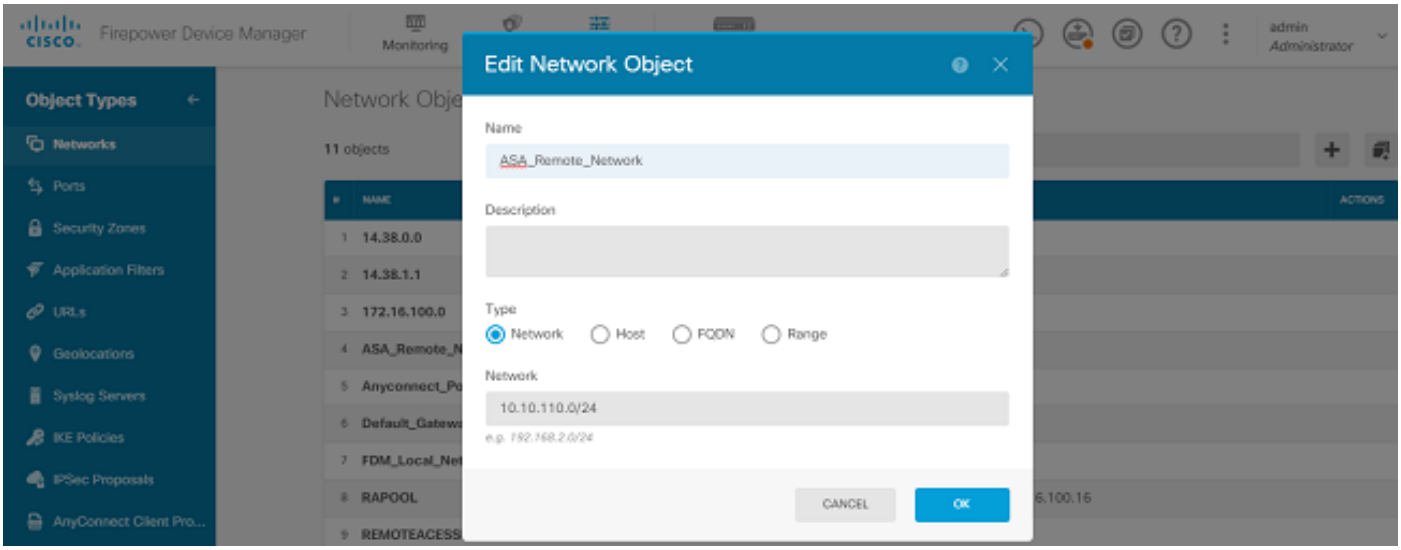
보호 네트워크 정의

Objects(개체) > Networks(네트워크) > Add New Network(새 네트워크 추가)..

FDM GUI에서 LAN 네트워크에 대한 객체를 구성합니다. 이미지에 표시된 대로 FDM 디바이스 뒤에 로컬 네트워크에 대한 객체를 생성합니다.



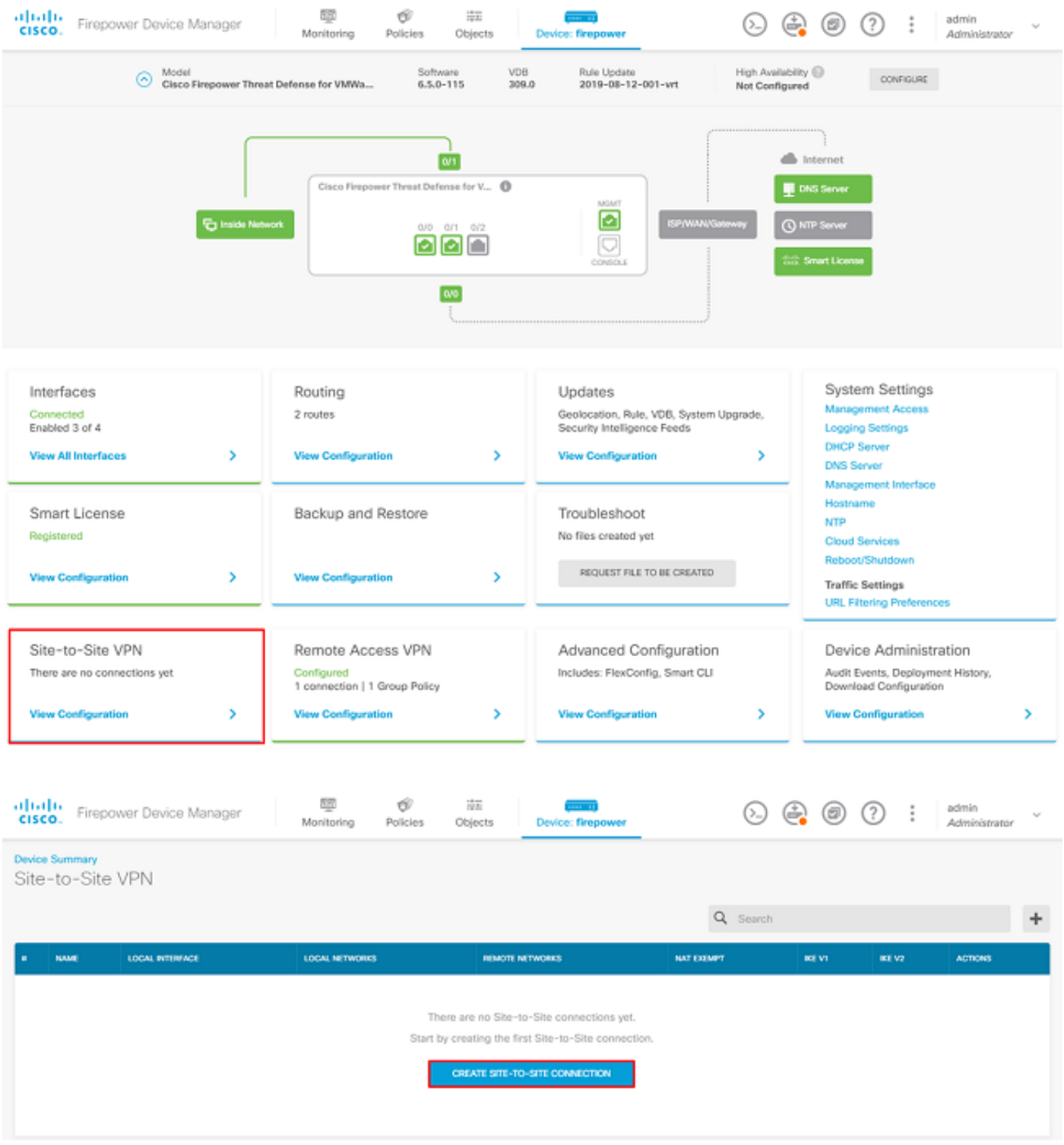
그림과 같이 ASA 디바이스 뒤에 있는 원격 네트워크에 대한 객체를 생성합니다.



Site-to-Site VPN 구성

Site-to-Site VPN(사이트 대 사이트 VPN) > Create Site-to-Site Connection(사이트 대 사이트 연결 생성)으로 이동합니다.

이미지에 표시된 대로 FDM에서 사이트 대 사이트 마법사를 진행합니다.

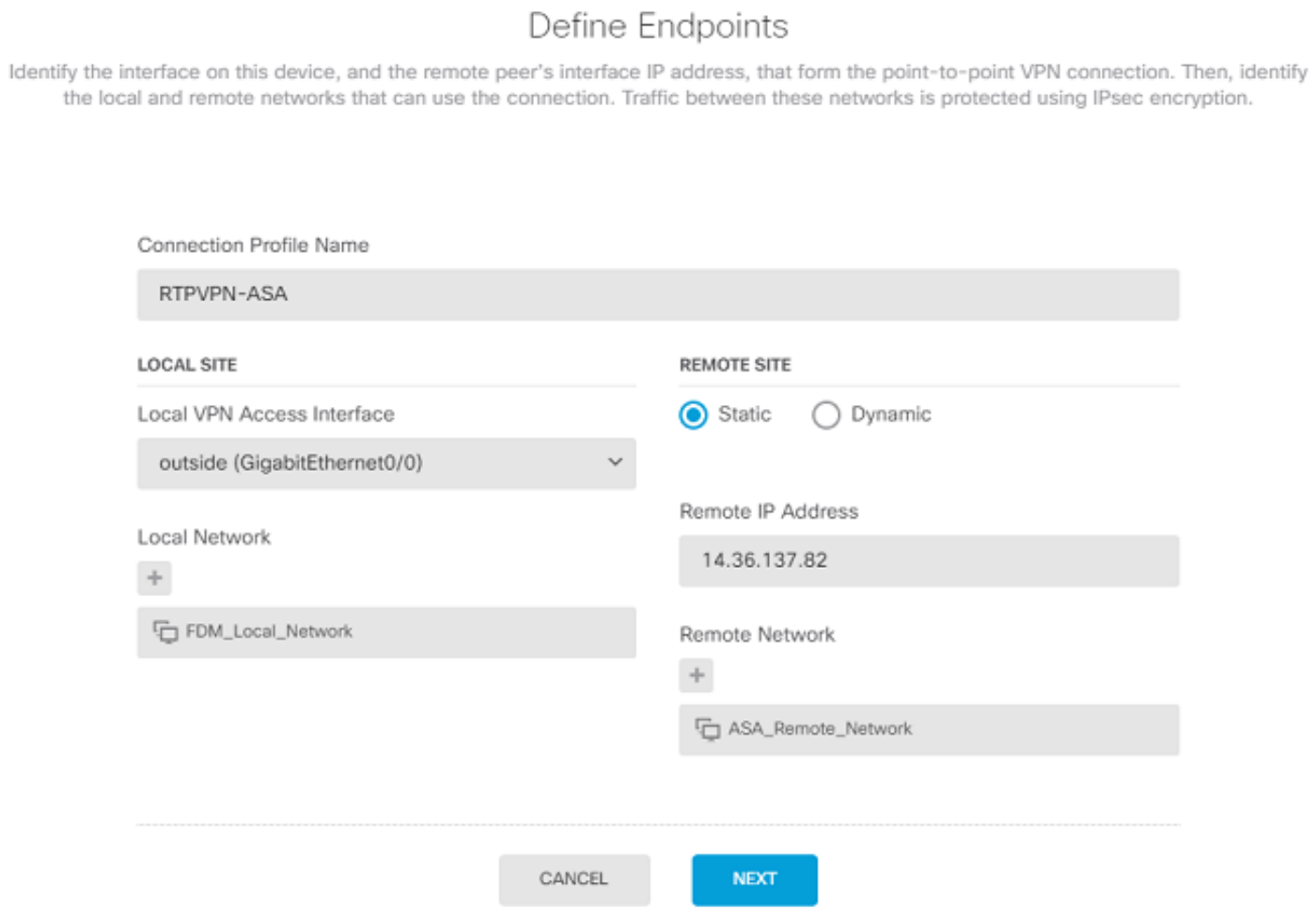


사이트 대 사이트 연결에서 쉽게 식별할 수 있는 연결 프로파일 이름을 지정합니다.

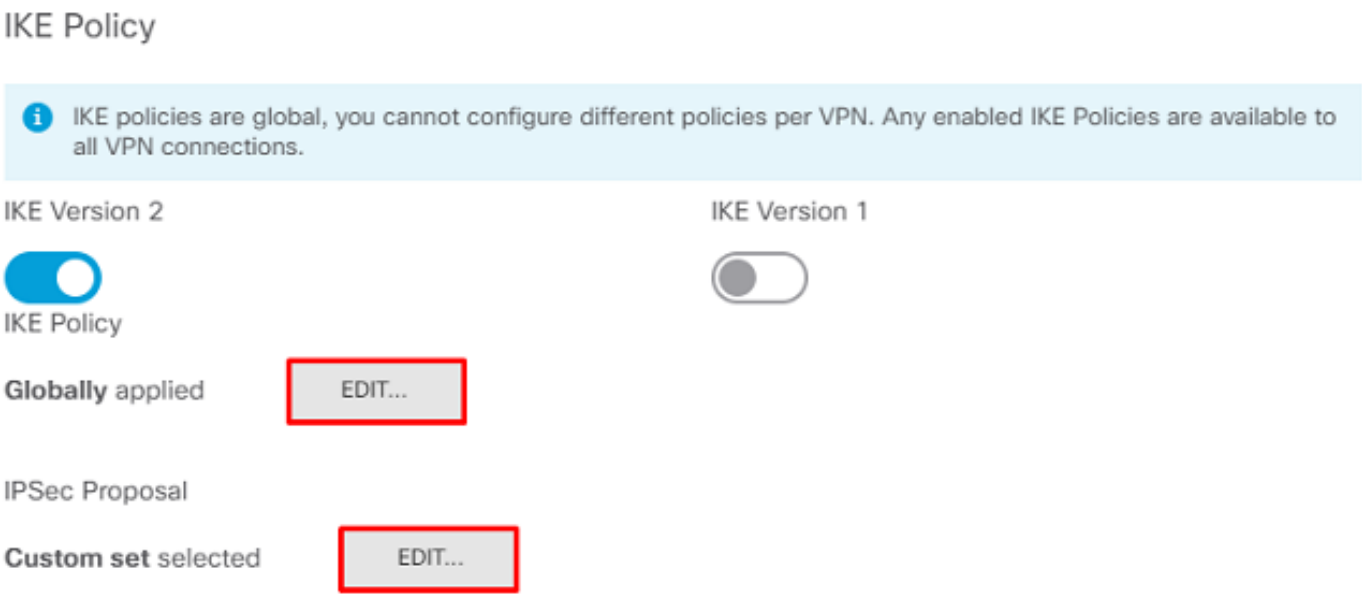
FTD에 대해 올바른 외부 인터페이스를 선택한 다음 사이트 간 VPN에서 암호화해야 하는 로컬 네

트워크를 선택합니다.

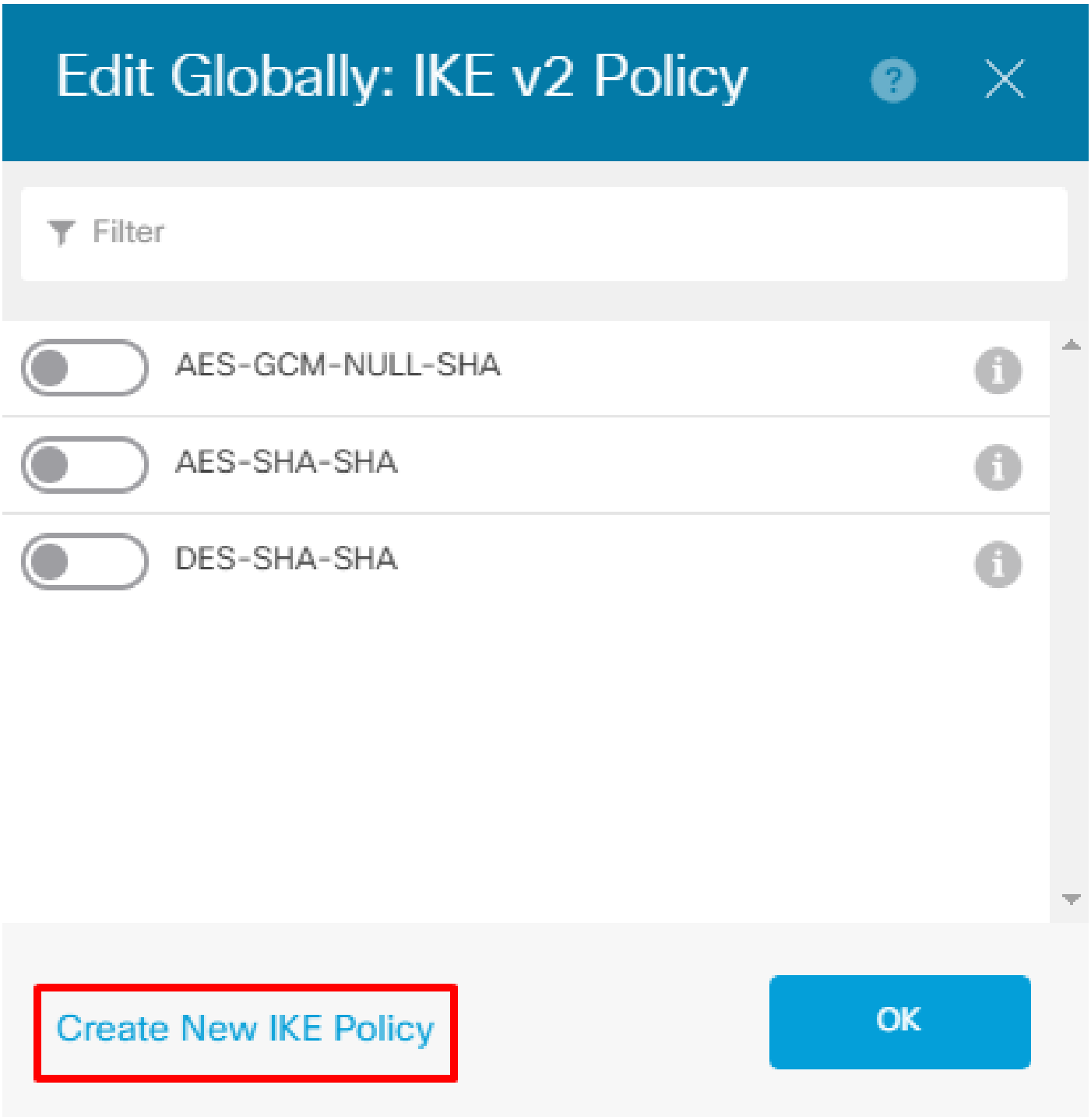
원격 피어의 공용 인터페이스를 설정합니다. 그런 다음 그림과 같이 Site-to-Site VPN 전체에서 암호화된 원격 피어의 네트워크를 선택합니다.



다음 페이지에서 Edit(편집) 버튼을 선택하여 그림과 같이 IKE(Internet Key Exchange) 매개변수를 설정합니다.

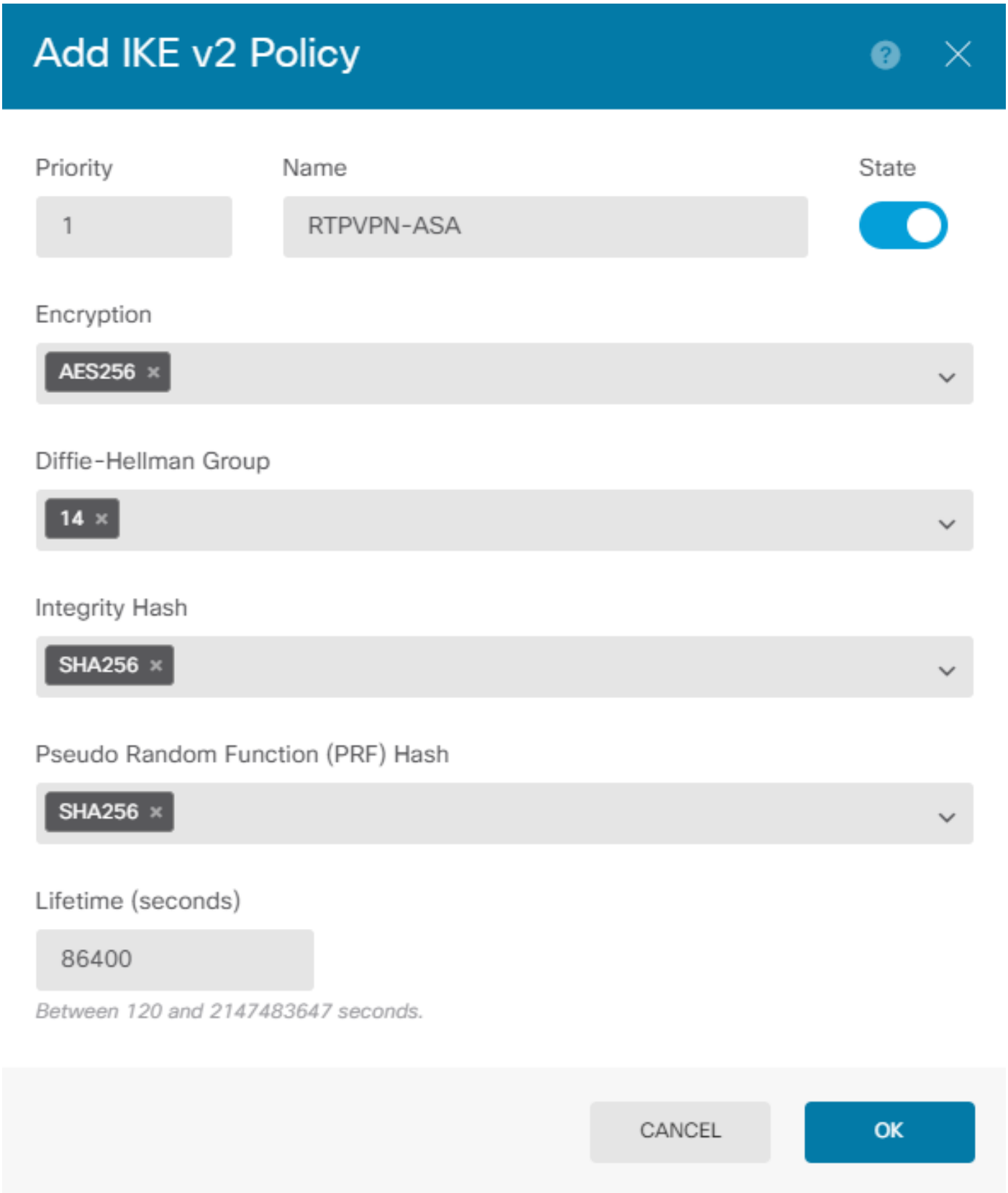


이미지에 표시된 대로 Create New IKE Policy(새 IKE 정책 생성) 버튼을 선택합니다.

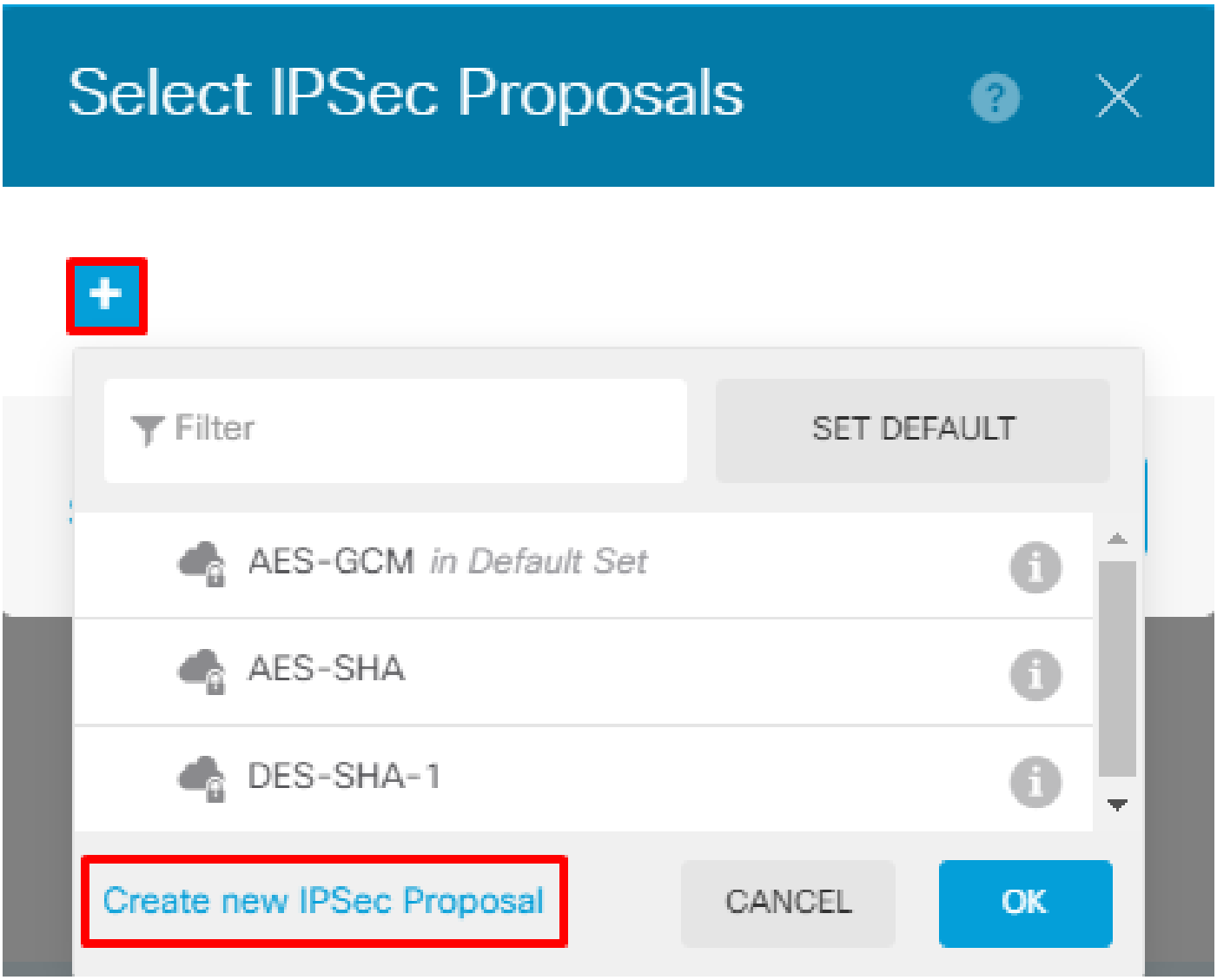


이 설명서에서는 IKEv2 초기 교환에 다음 매개변수를 사용합니다.

암호화 AES-256
무결성 SHA256
DH 그룹 14
PRF SHA256



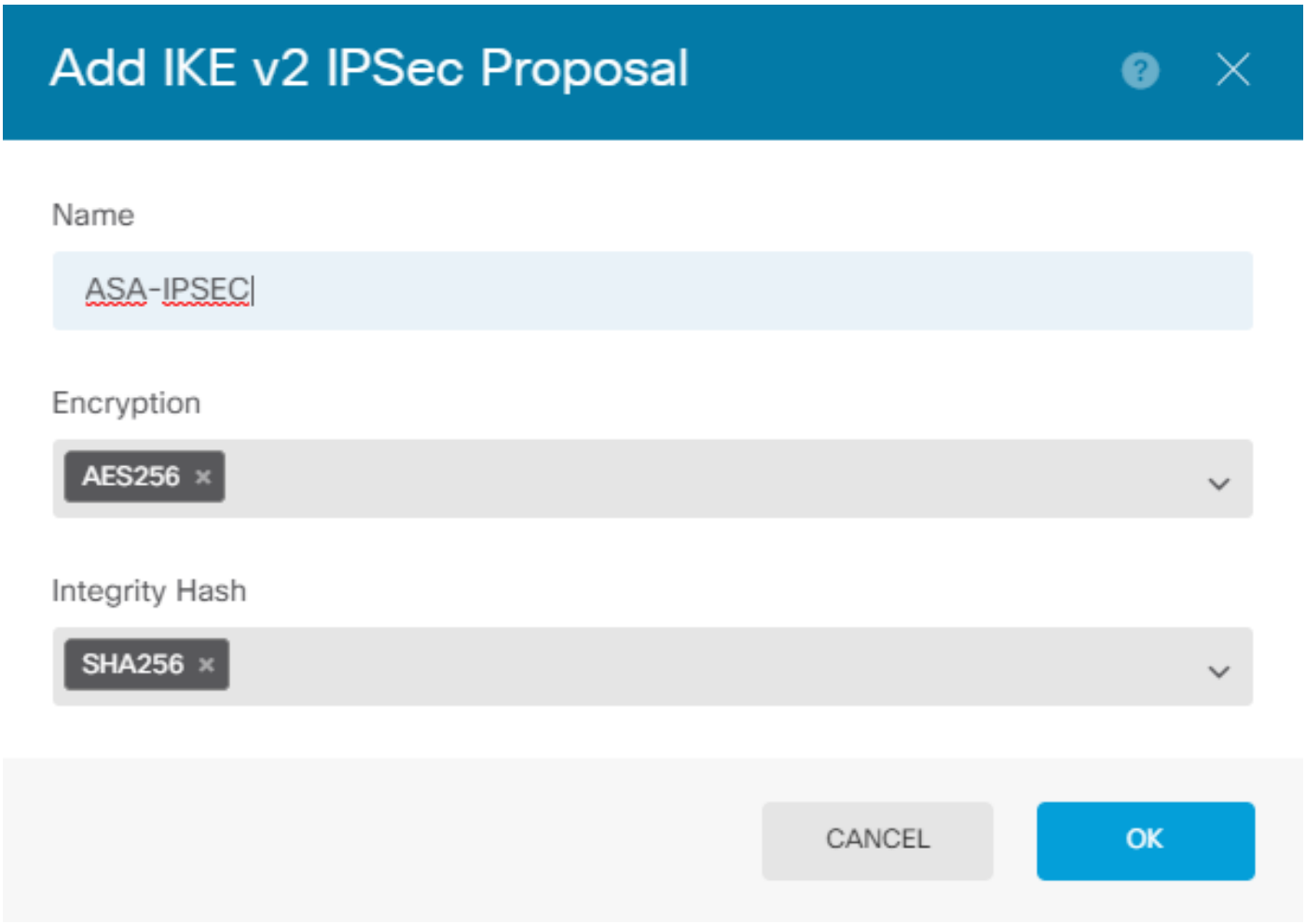
메인 페이지로 돌아간 후 IPSec Proposal에 대한 Edit(편집) 버튼을 선택합니다. 이미지에 표시된 대로 새 IPSec 제안서를 생성합니다.



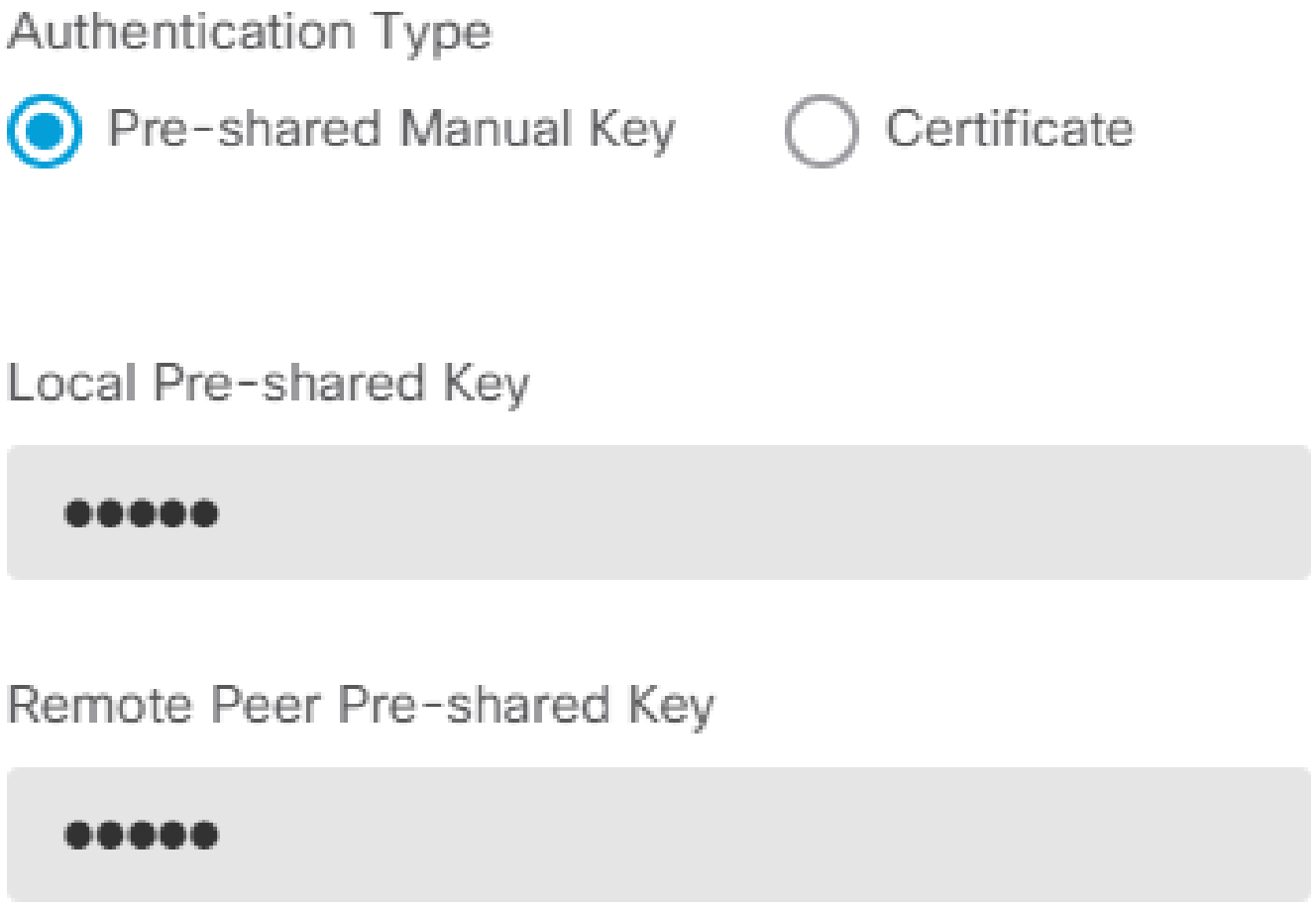
이 설명서에서는 IPSec에 다음 매개변수를 사용합니다.

암호화 AES-256

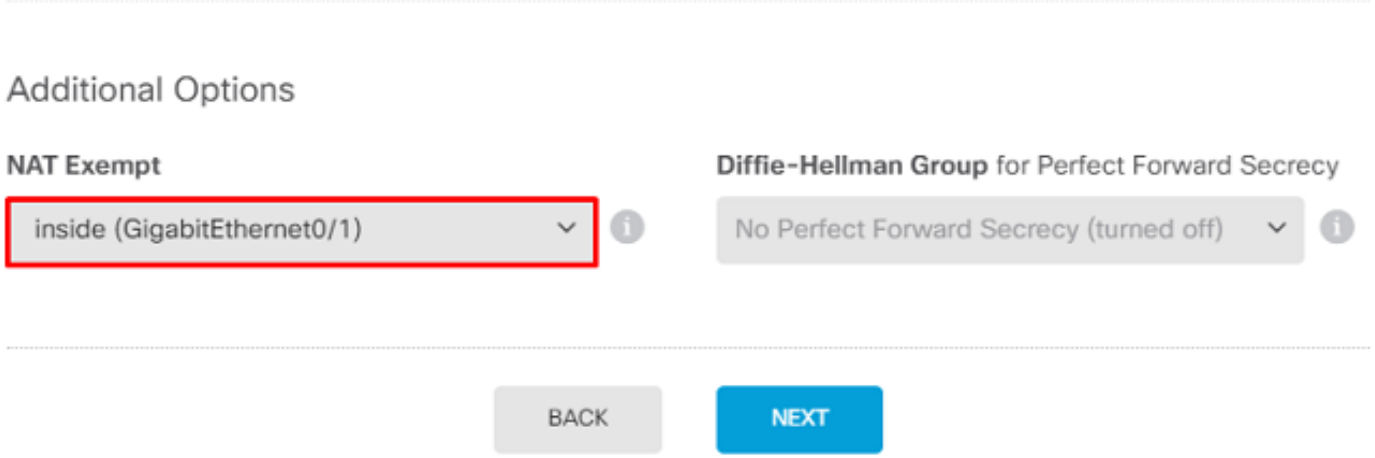
무결성 SHA256



인증을 사전 공유 키로 설정하고 양쪽 끝에서 사용되는 사전 공유 키(PSK)를 입력합니다. 이 가이드에서는 이미지에 표시된 대로 Cisco의 PSK가 사용됩니다.



내부 NAT Exempt 인터페이스를 설정합니다. 내부 인터페이스가 여러 개 사용되는 경우 Policies(정책) > NAT 아래에 수동 NAT Exempt(제외) 규칙을 생성해야 합니다.



마지막 페이지에 Site-to-Site 연결에 대한 요약이 표시됩니다. 올바른 IP 주소가 선택되었는지, 올바른 암호화 매개변수가 사용되었는지 확인하고 finish(마침) 버튼을 누릅니다. 새 Site-to-Site VPN을

구축합니다.

ASA 컨피그레이션은 CLI를 사용하여 완료됩니다.

ASA 컨피그레이션

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 FDM_GP internal
Group-policy FDM_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 172.16.100.10 type ipsec-l2l
Tunnel-group 172.16.100.10 general-attributes
 Default-group-policy FDM_GP
Tunnel-group 172.16.100.10 ipsec-attributes
 ikev2 local-authentication pre-shared-key cisco
 ikev2 remote-authentication pre-shared-key cisco
```

5. 암호화할 트래픽을 정의하는 액세스 목록을 만듭니다. (FTDSubnet 10.10.116.0/24)

(ASASubnet 10.10.110.0/24):

```
Object network FDMSubnet
 Subnet 10.10.116.0 255.255.255.0
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 참조하는 IKEv2 IPsec 제안서를 생성합니다.

```
Crypto ipsec ikev2 ipsec-proposal FDM
 Protocol esp encryption aes-256
 Protocol esp integrity sha-256
```

7. 구성을 함께 연결하는 암호화 맵 항목을 생성합니다.

```
Crypto map outside_map 20 set peer 172.16.100.10
Crypto map outside_map 20 match address ASAtoFTD
Crypto map outside_map 20 set ikev2 ipsec-proposal FTD
Crypto map outside_map 20 interface outside
```

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

```
Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FDMSubnet FDMSubnet
no-proxy-arp route-lookup
```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

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 시작할 때 터널이 시작되는지 확인하려면 해당 터널을 두 번 실행해야 합니다. 명령이 처음 실행되면 VPN 터널이 다운되므로 VPN encrypt DROP으로 packet-tracer 명령이 실패합니다. 항상 실패하므로 방화벽의 내부 IP 주소를 패킷 추적기의 소스 IP 주소로 사용하지 마십시오.

```
firepower# packet-tracer input inside icmp 10.10.116.10 8 0 10.10.110.10

Phase: 9
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:


firepower# packet-tracer input inside icmp 10.10.116.10 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 |s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAclSrcNwgV4
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 NGFW_ONBOX_ACL global
access-list NGFW_ONBOX_ACL advanced trust object-group |acSvcg-268435457 ifc inside any ifc outside any
access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule
object-group service |acSvcg-268435457
service-object ip
Additional Information:

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static |s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAclSrcNwgV4
Additional Information:
Static translate 10.10.116.10/0 to 10.10.116.10/0

Phase: 9
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 show crypto ikev2 sa 명령을 사용하여 phase-1 및 phase-2를 확인합니다.

```
> show crypto ikev2 sa

IKEv2 SAs:

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

Tunnel-id Local                                                 Remote
  3821043 172.16.100.10/500                                      192.168.200.10/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1150 sec
Child sa: local selector  10.10.116.0/0 - 10.10.116.255/65535
          remote selector 10.10.110.0/0 - 10.10.110.255/65535
          ESP spi in/out: 0x7398dcbd/0x2303b0c0
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

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 172.16.100.10 host 192.168.200.10
```

캡처가 제자리에 있으면 VPN을 통해 트래픽을 전송하고 패킷 캡처에서 양방향 트래픽을 확인합니

다.

show cap capout 명령을 사용하여 패킷 캡처를 검토합니다.

```
firepower# show cap capout

4 packets captured

   1: 01:21:06.763983       172.16.100.10.500 > 192.168.200.10.500:  udp 574
   2: 01:21:06.769415       192.168.200.10.500 > 172.16.100.10.500:  udp 619
   3: 01:21:06.770666       172.16.100.10.500 > 192.168.200.10.500:  udp 288
   4: 01:21:06.773748       192.168.200.10.500 > 172.16.100.10.500:  udp 256
```

트래픽 관련 문제

사용자가 겪는 일반적인 트래픽 문제:

- 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 NAT(Network Address Translation)가 우회되지 않습니다.

관련 정보

FDM에서 관리하는 FTD의 Site-to-Site VPN에 대한 자세한 내용은 여기에서 전체 컨피그레이션 가이드를 참조하십시오.

- FTD Managed by FDM Configuration Guide를 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.