ASA와 FTD 간에 IKEv2 IPv6 사이트 간 터널 구성

목차

소개

이 문서에서는 IKEv2(Internet Key Exchange version 2) 프로토콜을 사용하여 ASA(Adaptive Security Appliance)와 FTD(Firepower Threat Defense) 간 IPv6 사이트 대 사이트 터널을 설정하는 컨피그레이션 예를 제공합니다.설정에는 ASA와 FTD를 VPN 종료 디바이스로 사용하는 엔드 투 엔드 IPv6 네트워크 연결이 포함됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA CLI 구성에 대한 기본 지식
- IKEv2 및 IPSEC 프로토콜에 대한 기본 지식
- IPv6 주소 지정 및 라우팅 이해
- FMC를 통한 FTD 컨피그레이션에 대한 기본적인 이해

사용되는 구성 요소

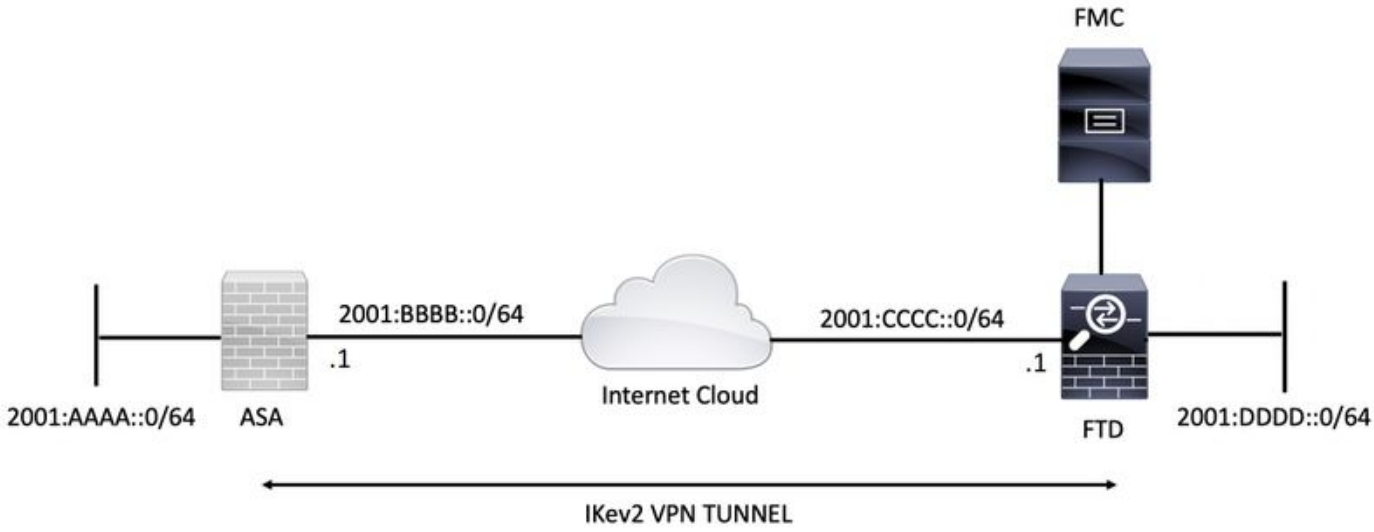
이 문서의 정보는 특정 랩 설정의 디바이스에서 생성된 가상 환경을 기반으로 합니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 프로덕션 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 9.6.(4)12를 실행하는 Cisco ASAv
- 6.5.0을 실행하는 Cisco FTDv
- 6.6.0을 실행하는 Cisco FMCv

구성

네트워크 다이어그램



ASA 컨피그레이션

이 섹션에서는 ASA에 필요한 컨피그레이션에 대해 설명합니다.

1단계. ASA 인터페이스를 구성합니다.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ipv6 address 2001:bbbb::1/64
ipv6 enable

interface GigabitEthernet0/1
nameif inside
security-level 100
ipv6 address 2001:aaaa::1/64
ipv6 enable
```

2단계. IPv6 기본 경로를 설정합니다.

```
ipv6 route outside ::/0 2001:bbbb::2
```

3단계. IKEv2 정책을 구성하고 외부 인터페이스에서 IKEv2를 활성화합니다.

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 14
prf sha256
lifetime seconds 86400

crypto ikev2 enable outside
```

4단계. 터널 그룹을 구성합니다.

```
tunnel-group 2001:cccc::1 type ipsec-l2l
tunnel-group 2001:cccc::1 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco123
ikev2 local-authentication pre-shared-key cisco123
```

5단계. 흥미로운 트래픽과 일치하도록 객체 및 ACL(Access Control List)을 생성합니다.

```
object-group network local-network
network-object 2001:aaaa::/64

object-group network remote-network
network-object 2001:dddd::/64

access-list CRYPTO_ACL extended permit ip object-group local-network object-group remote-network
```

6단계. 흥미로운 트래픽에 대한 NAT(Identity Network Address Translation) 규칙을 구성합니다.

```
nat (inside,outside) source static local-network local-network destination static remote-network
remote-network no-proxy-arp route-lookup
```

7단계. IKEv2 IPSec 제안을 구성합니다.

```
crypto ipsec ikev2 ipsec-proposal ikev2_aes256
protocol esp encryption aes-256
protocol esp integrity sha-1
```

8단계. 암호화 맵을 설정하고 외부 인터페이스에 적용합니다.

```
crypto map VPN 1 match address CRYPTO_ACL
crypto map VPN 1 set peer 2001:cccc::1
crypto map VPN 1 set ikev2 ipsec-proposal ikev2_aes256
crypto map VPN 1 set reverse-route

crypto map VPN interface outside
```

FTD 컨피그레이션

이 섹션에서는 FMC를 사용하여 FTD를 구성하는 지침을 제공합니다.

VPN 토폴로지 정의

1. **Devices > VPN > Site To Site .**

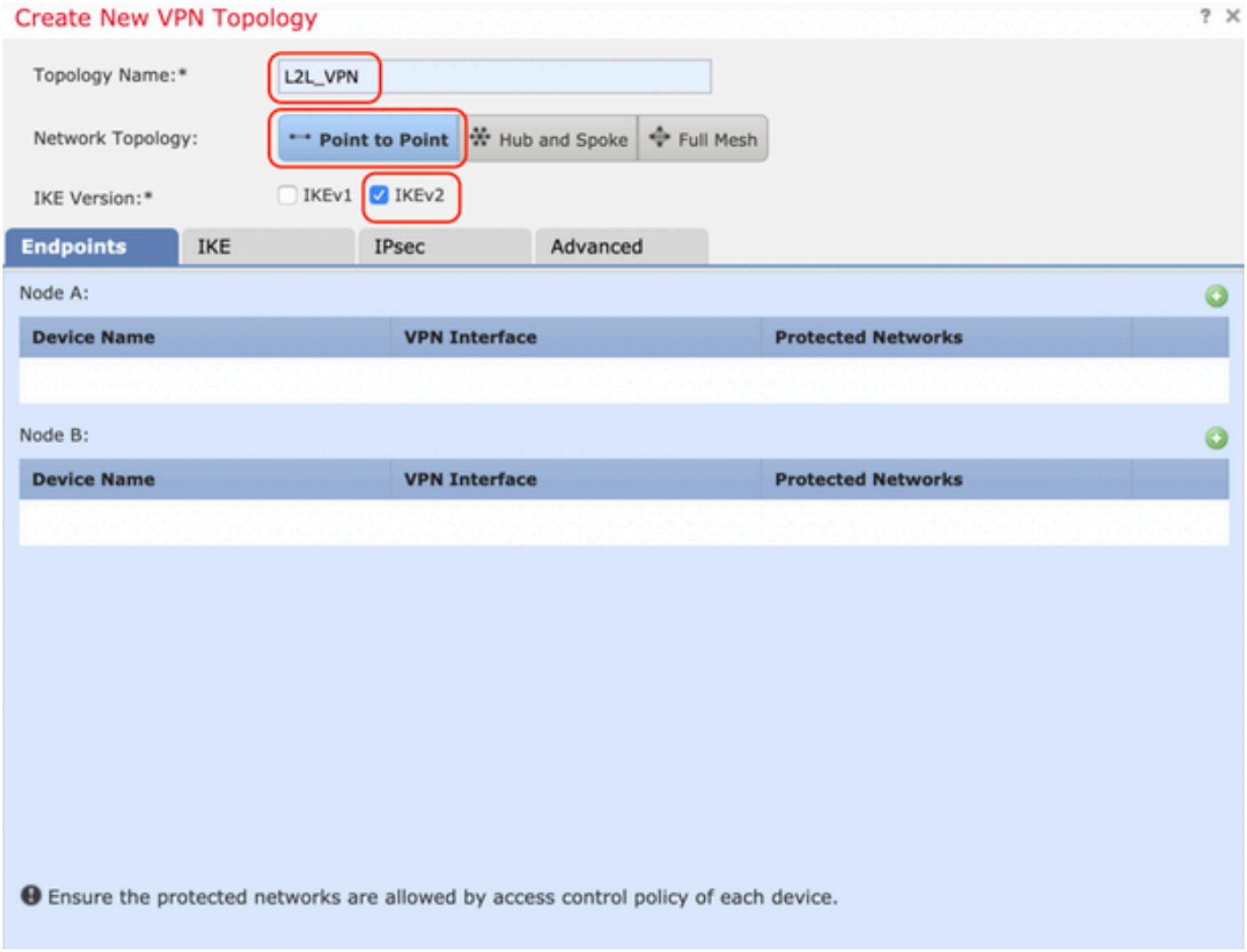
'VPN ' 'Firepower Threat Defense ' .

2단계. 'Create New VPN Topology' 상자가 나타납니다.VPN에 식별 가능한 이름을 지정합니다.

네트워크 토폴로지:포인트 투 포인트

IKE 버전:IKEv2

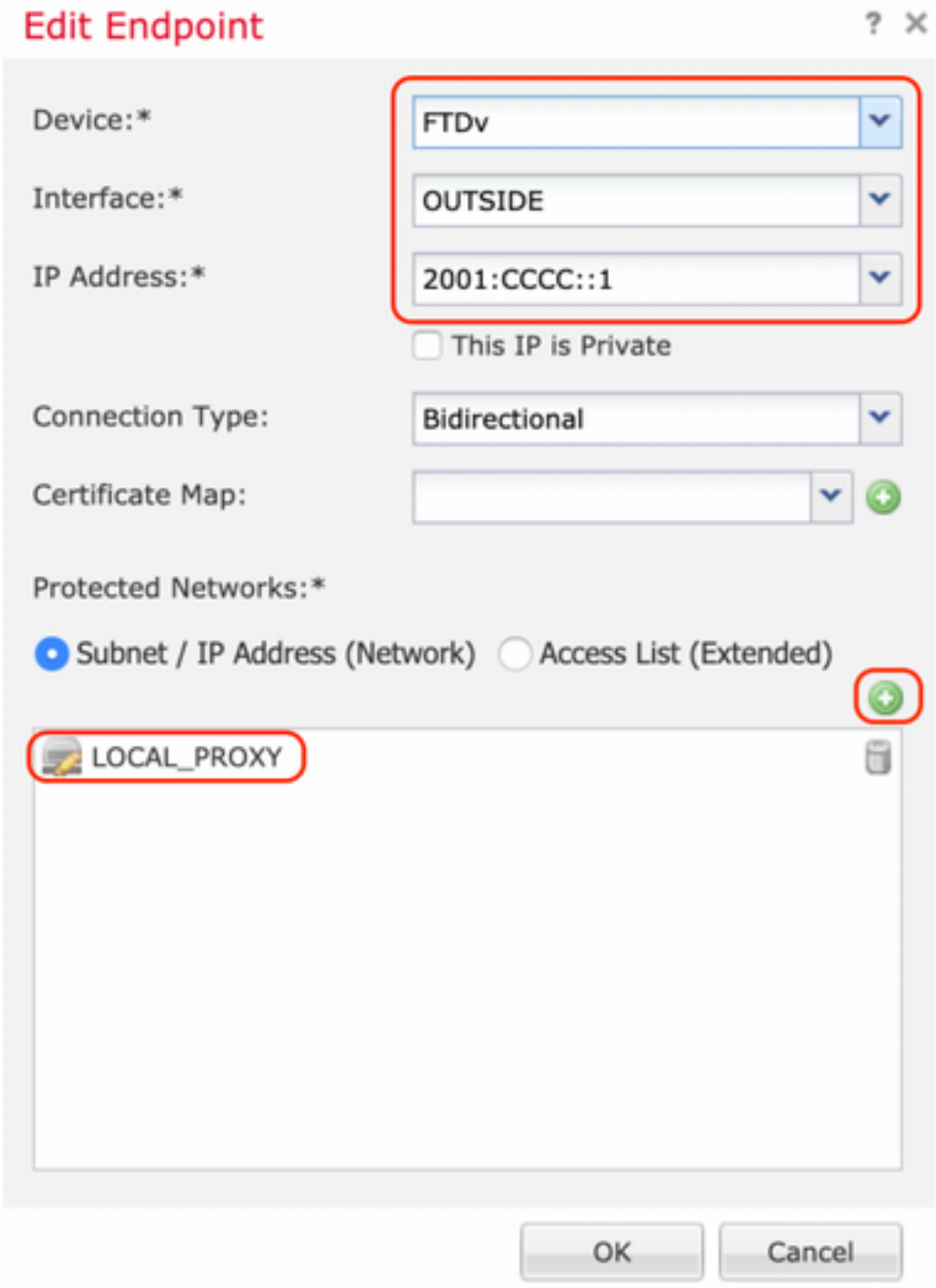
이 예에서는 엔드포인트 노드 A를 선택하면 FTD가 됩니다.노드 B는 ASA입니다.토폴로지에 디바이스를 추가하려면 녹색 + 버튼을 클릭합니다.

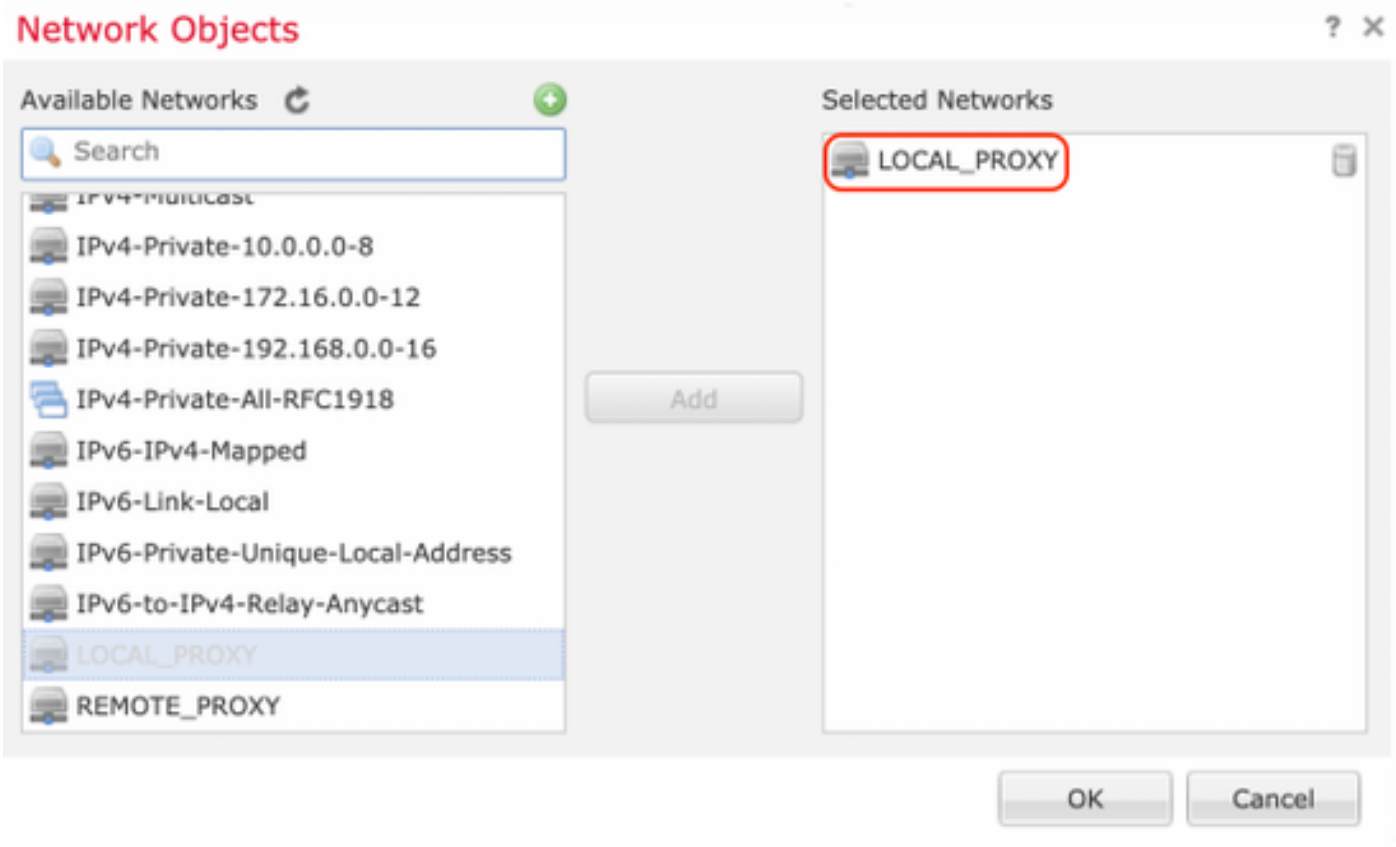


3단계. FTD를 첫 번째 엔드포인트로 추가합니다.

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

이 VPN 터널을 통해 암호화된 서브넷을 선택하려면 Protected Networks 아래에서 녹색 더하기 아이콘을 클릭합니다.이 예에서 FMC의 '로컬 프록시' 네트워크 개체는 IPv6 서브넷 '2001:DDD::/64'로 구성됩니다.

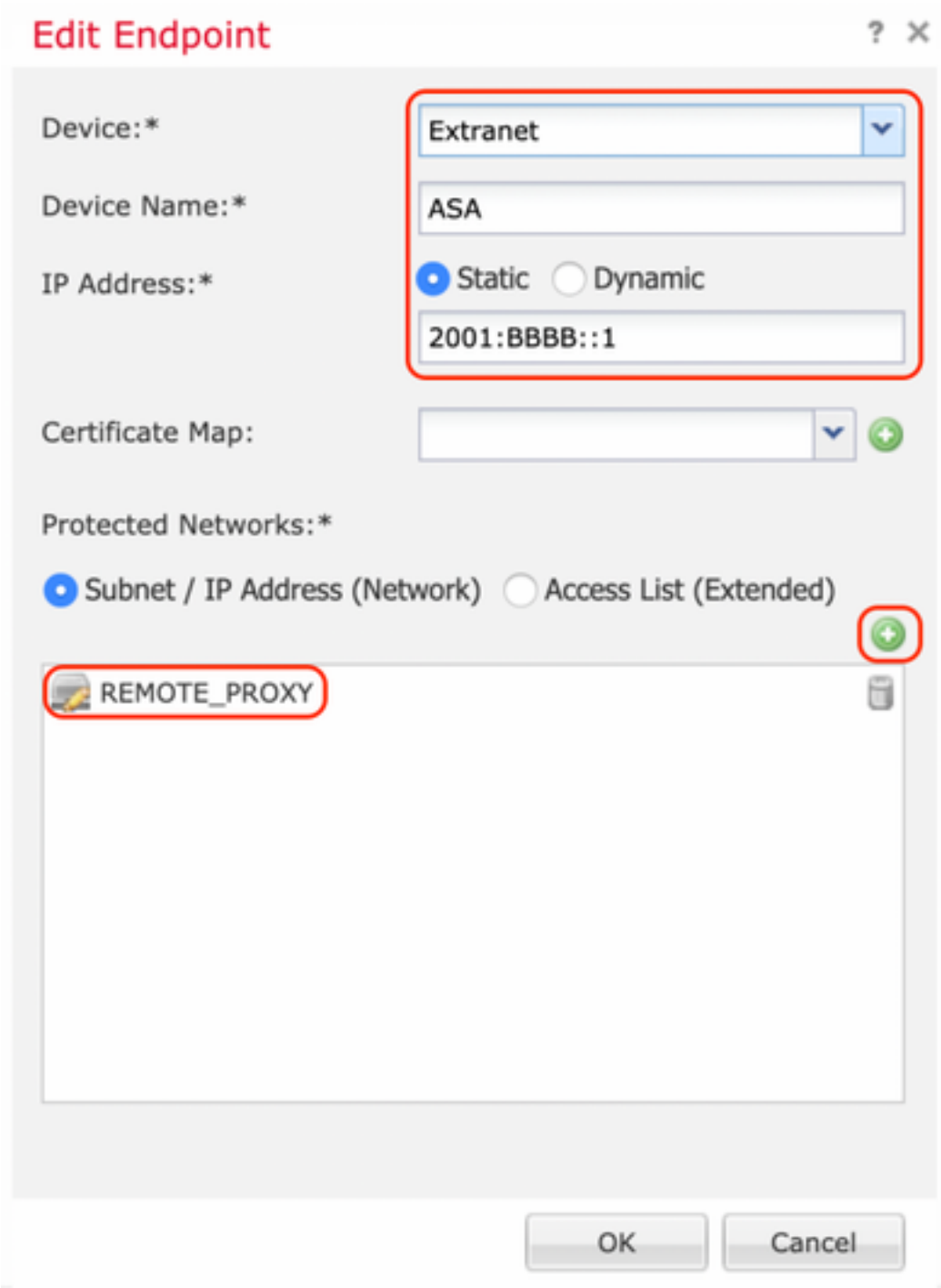

Edit Endpoint
Device:*
FTDv
Interface:*
OUTSIDE
IP Address:*
2001:CCCC::1
This IP is Private
Connection Type:
Bidirectional
Certificate Map:
Protected Networks:*
Subnet / IP Address (Network)
Access List (Extended)
LOCAL_PROXY
OK
Cancel



위 단계를 수행하면 FTD 엔드포인트 컨피그레이션이 완료됩니다.

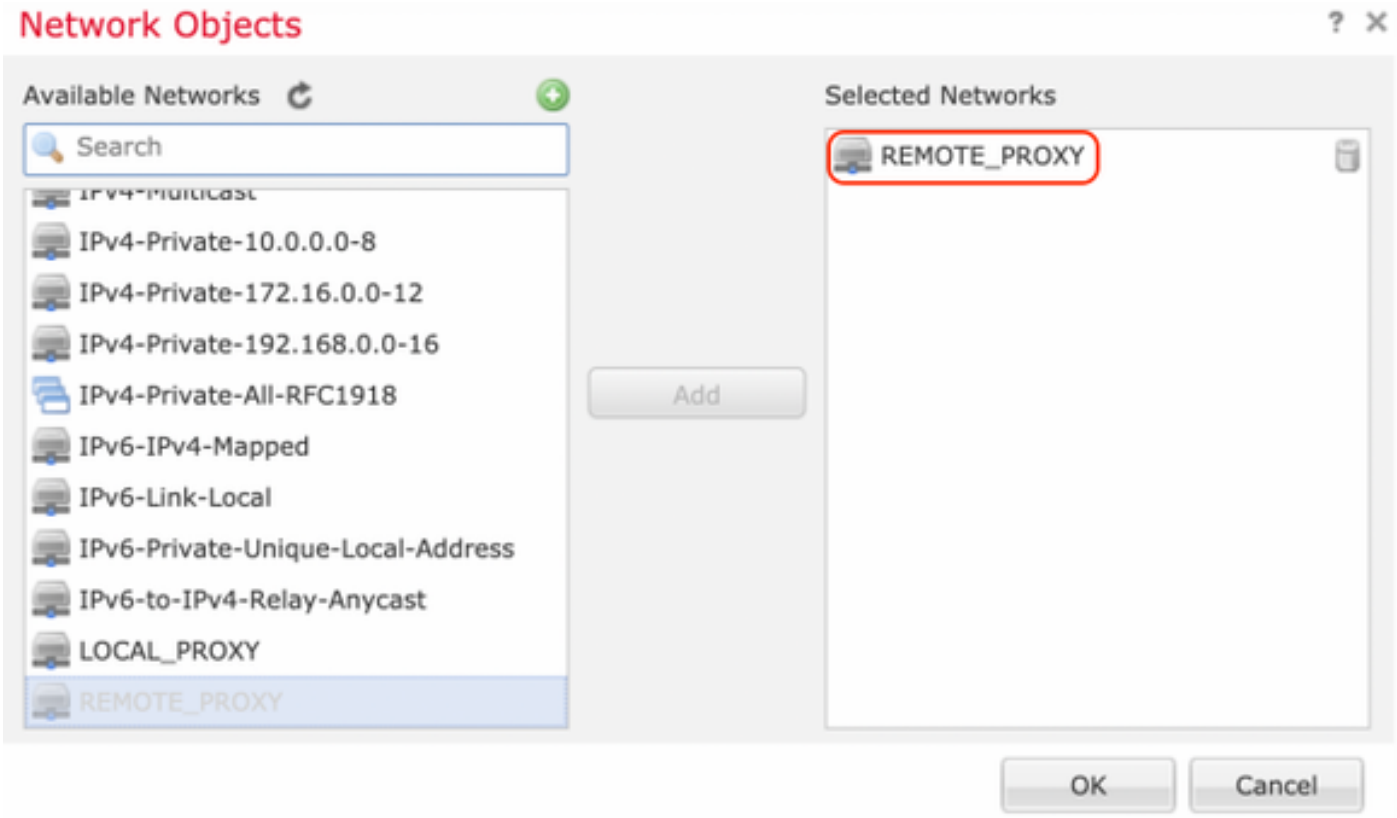
4단계. 컨피그레이션 예에서 ASA인 노드 B의 녹색 더하기 아이콘을 클릭합니다.FMC에서 관리하지 않는 디바이스는 엑스트라넷으로 간주됩니다.디바이스 이름과 IP 주소를 추가합니다.

5단계. 녹색 더하기 아이콘을 선택하여 보호된 네트워크를 추가합니다.



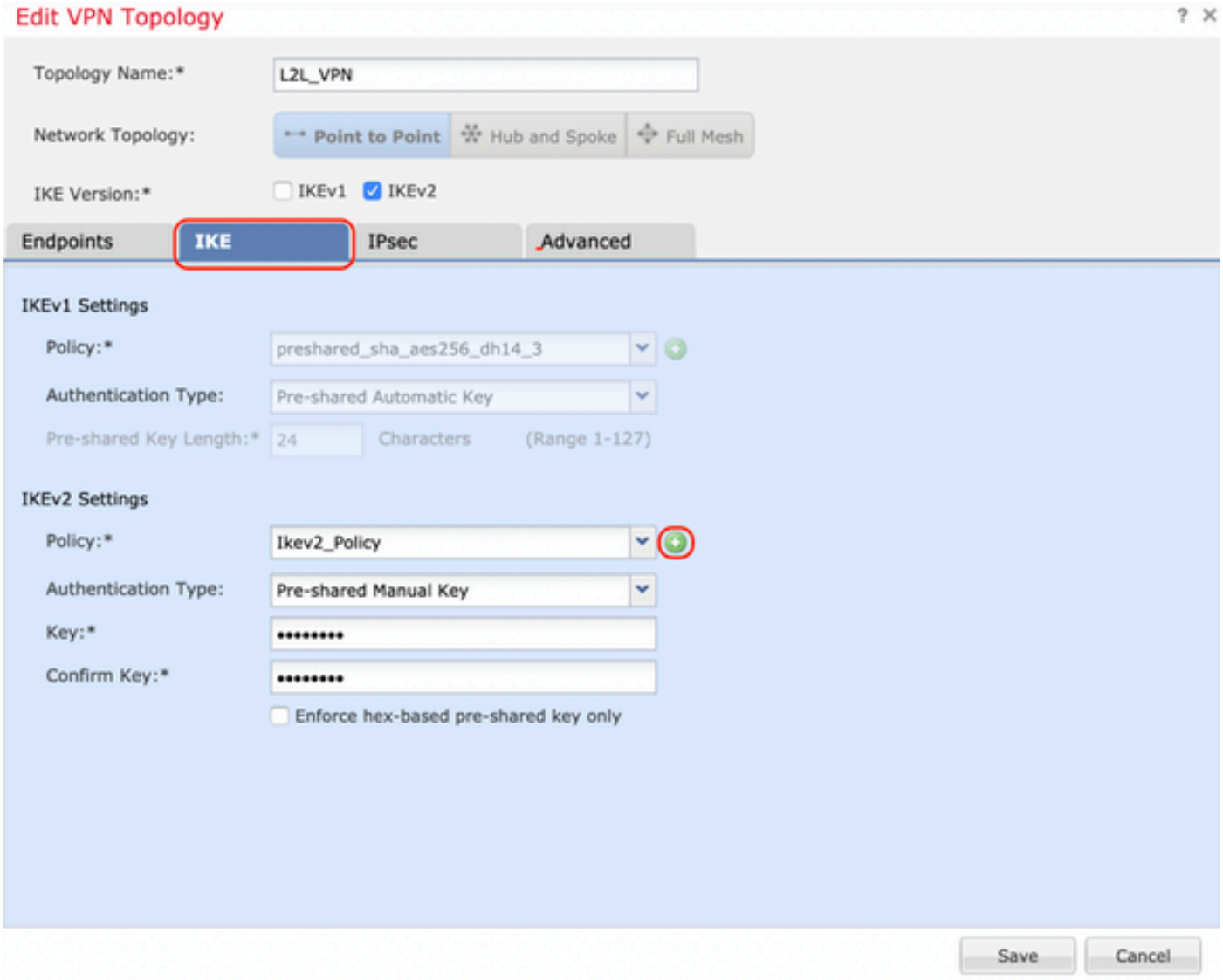
6단계. 암호화해야 하는 ASA 서브넷을 선택하고 선택한 네트워크에 추가합니다.

'Remote Proxy'는 이 예에서 ASA 서브넷 '2001:AAAA::/64'입니다.



IKE 매개변수 구성

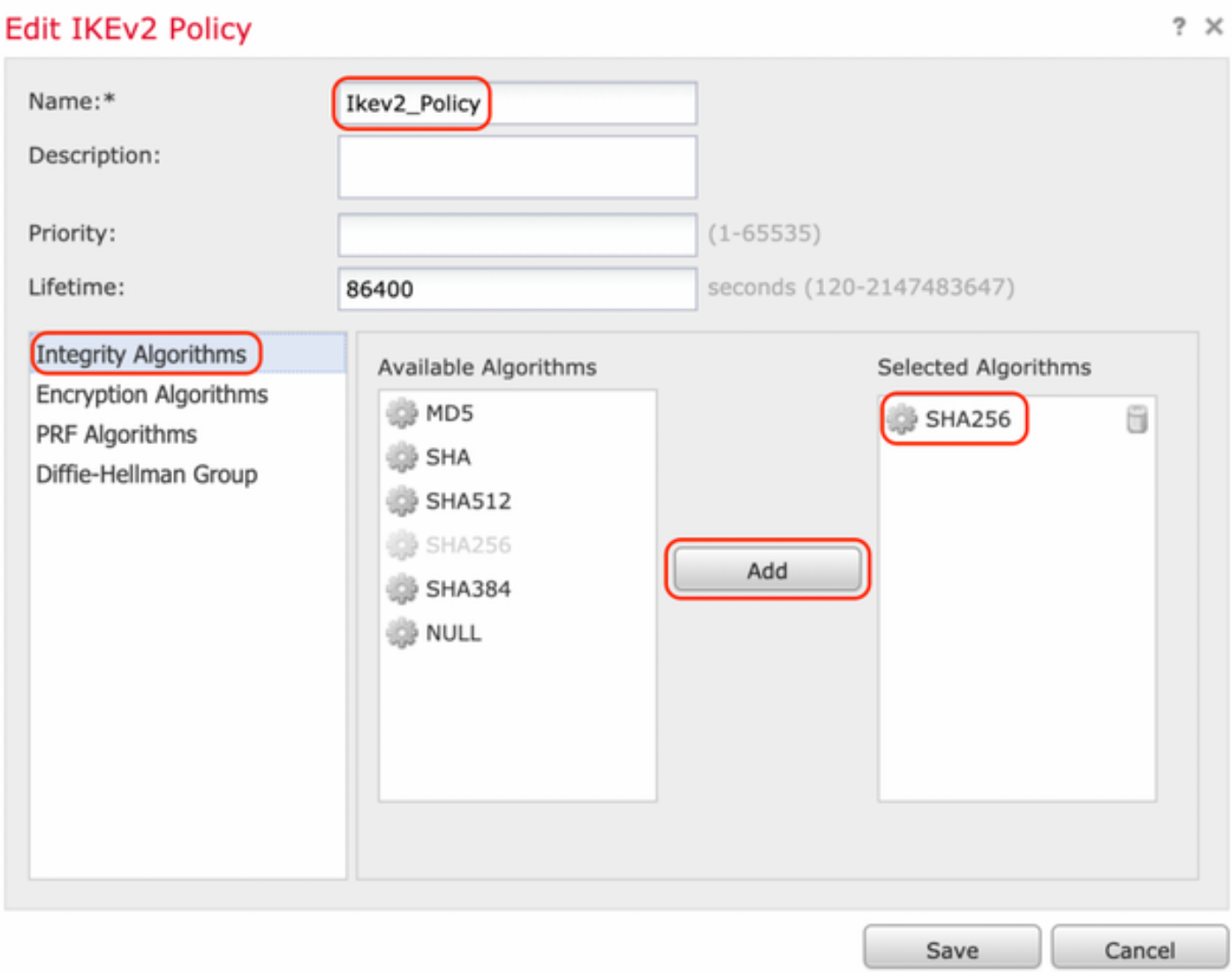
1단계. IKE 탭에서 IKEv2 초기 교환에 사용할 매개변수를 지정합니다.녹색 더하기 아이콘을 클릭하여 새 IKE 정책을 생성합니다.

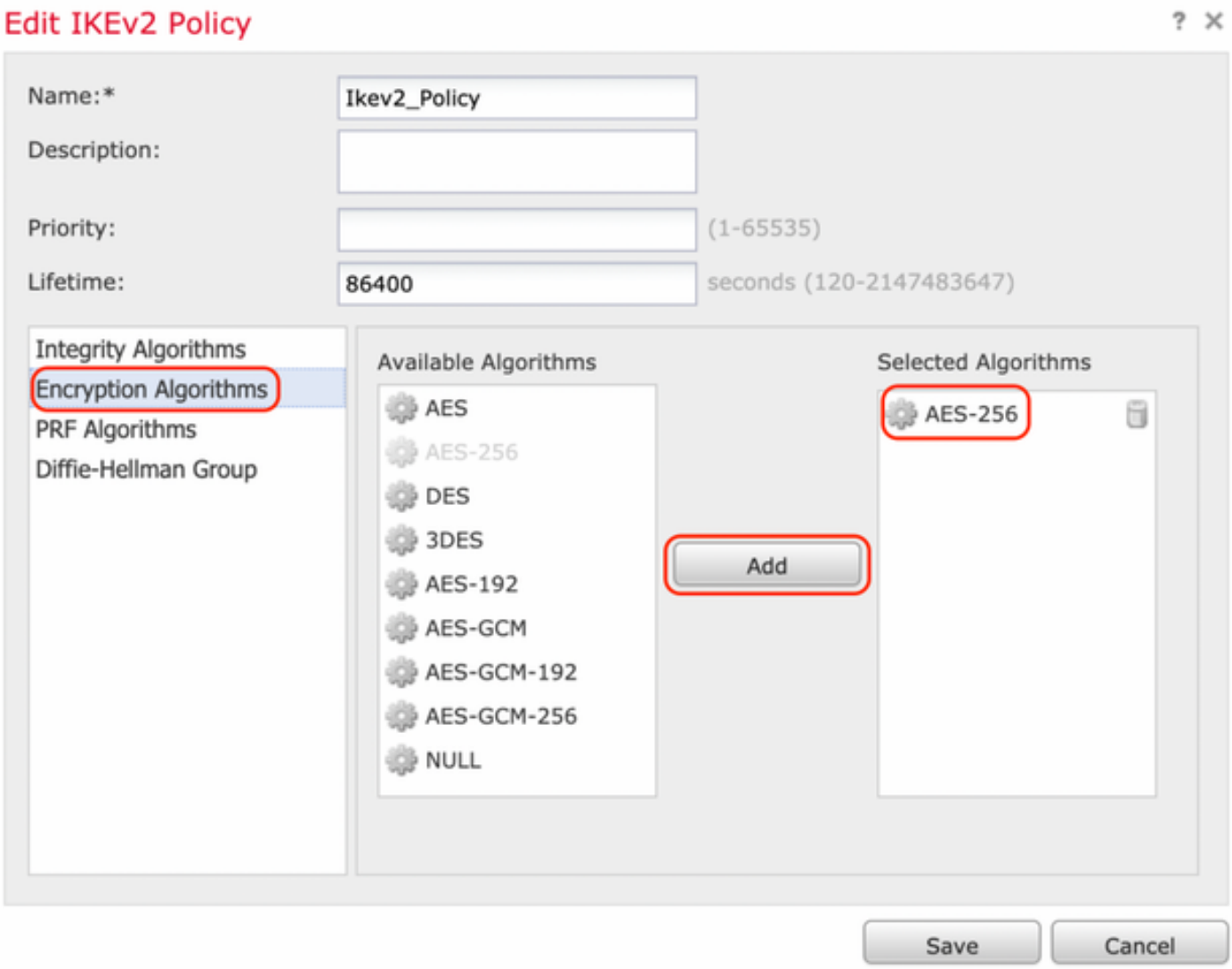


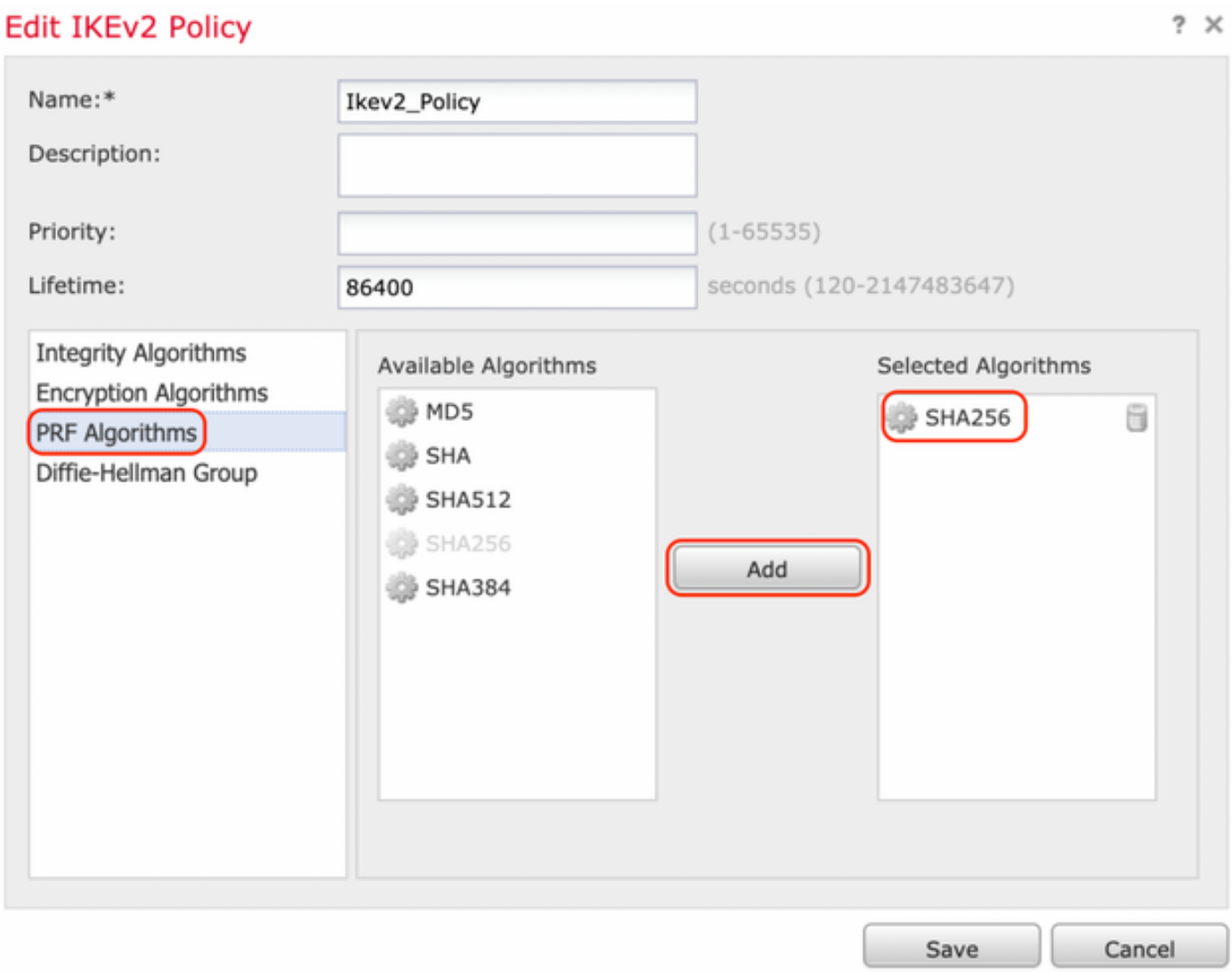
2단계. 새 IKE 정책에서 연결의 1단계 수명 및 우선순위 번호를 지정합니다.이 설명서에서는 다음과 같은 매개변수를 초기 교환에 사용합니다.
무결성(SHA256),
암호화(AES-256),
PRF(SHA256) 및
Diffie-Hellman 그룹(그룹 14).

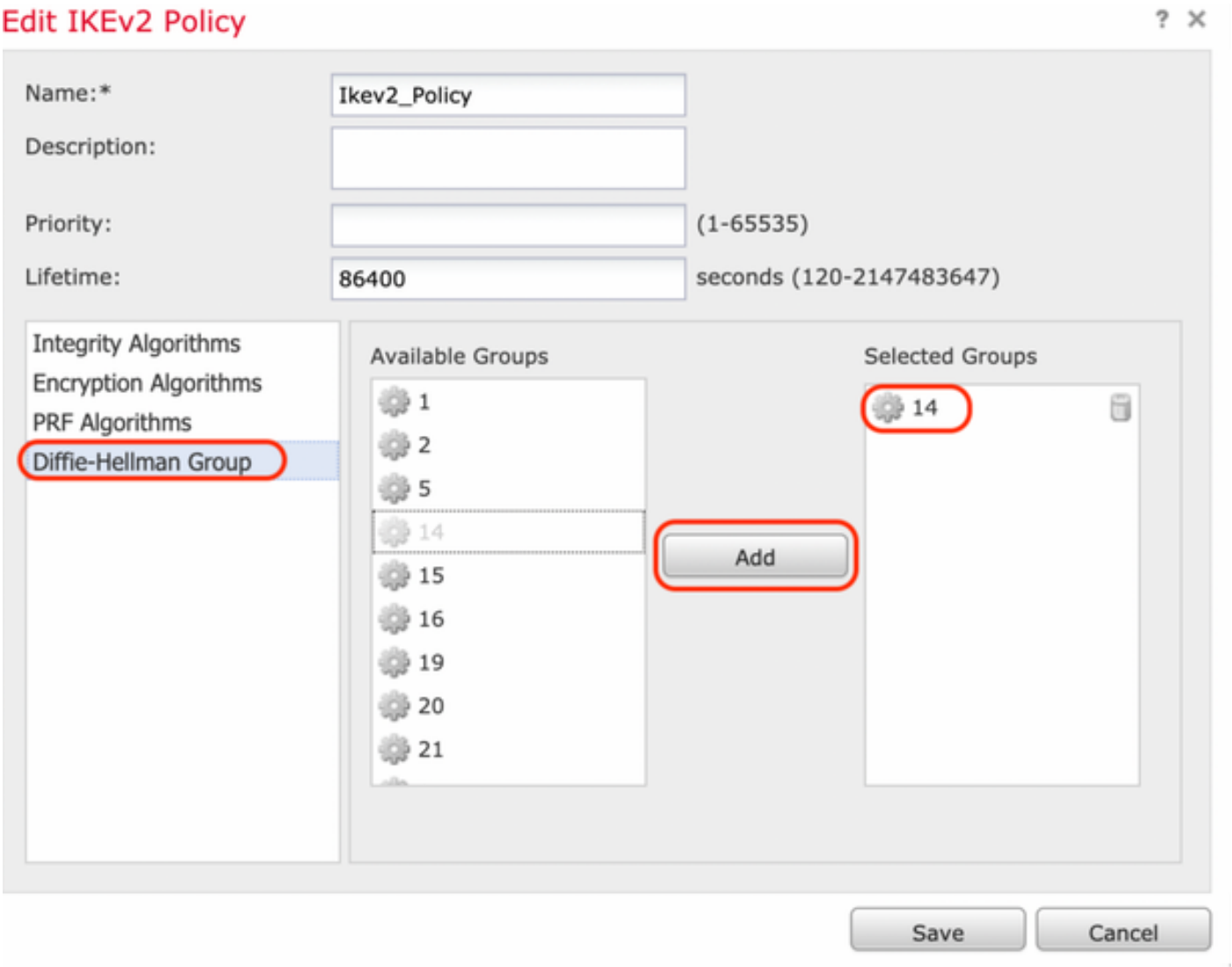
선택한 정책 섹션에 있는 내용과 상관없이 디바이스의 모든 IKE 정책이 원격 피어로 전송됩니다.원격 피어가 일치하는 첫 번째 항목이 VPN 연결에 대해 선택됩니다.

[선택 사항] 우선 순위 필드를 사용하여 어떤 정책을 먼저 전송할지 선택합니다.우선 순위 1이 먼저 전송됩니다.


Edit IKEv2 Policy
Name:*
Ikev2_Policy
Description:
Priority:
(1-65535)
Lifetime:
86400
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

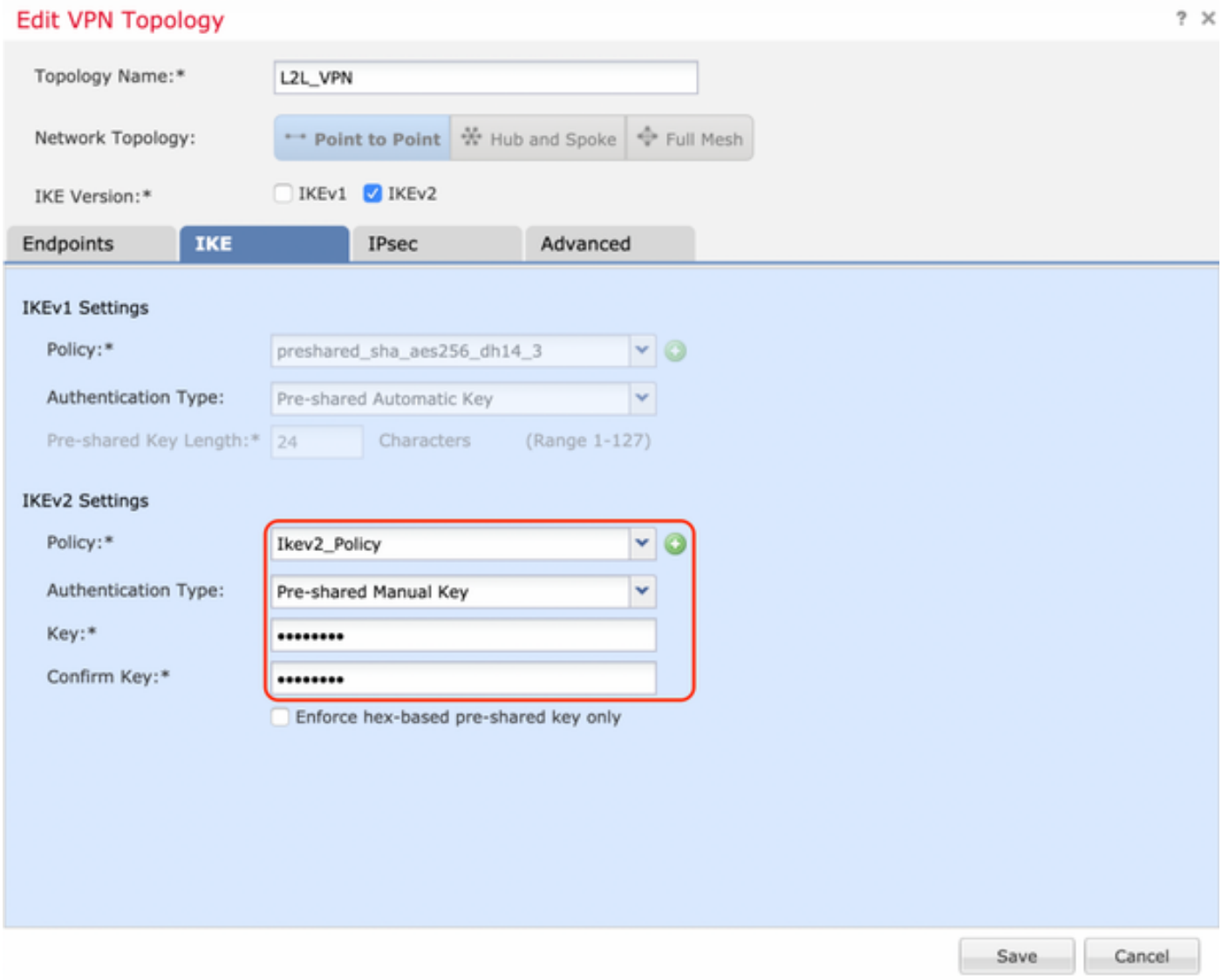

Edit IKEv2 Policy
Name:*
Ikev2_Policy
Description:
Priority:
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
AES
AES-256
DES
3DES
AES-192
AES-GCM
AES-GCM-192
AES-GCM-256
NULL
Add
Selected Algorithms
AES-256
Save
Cancel


Edit IKEv2 Policy
Name:*
Ikev2_Policy
Description:
Priority:
(1-65535)
Lifetime:
86400
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



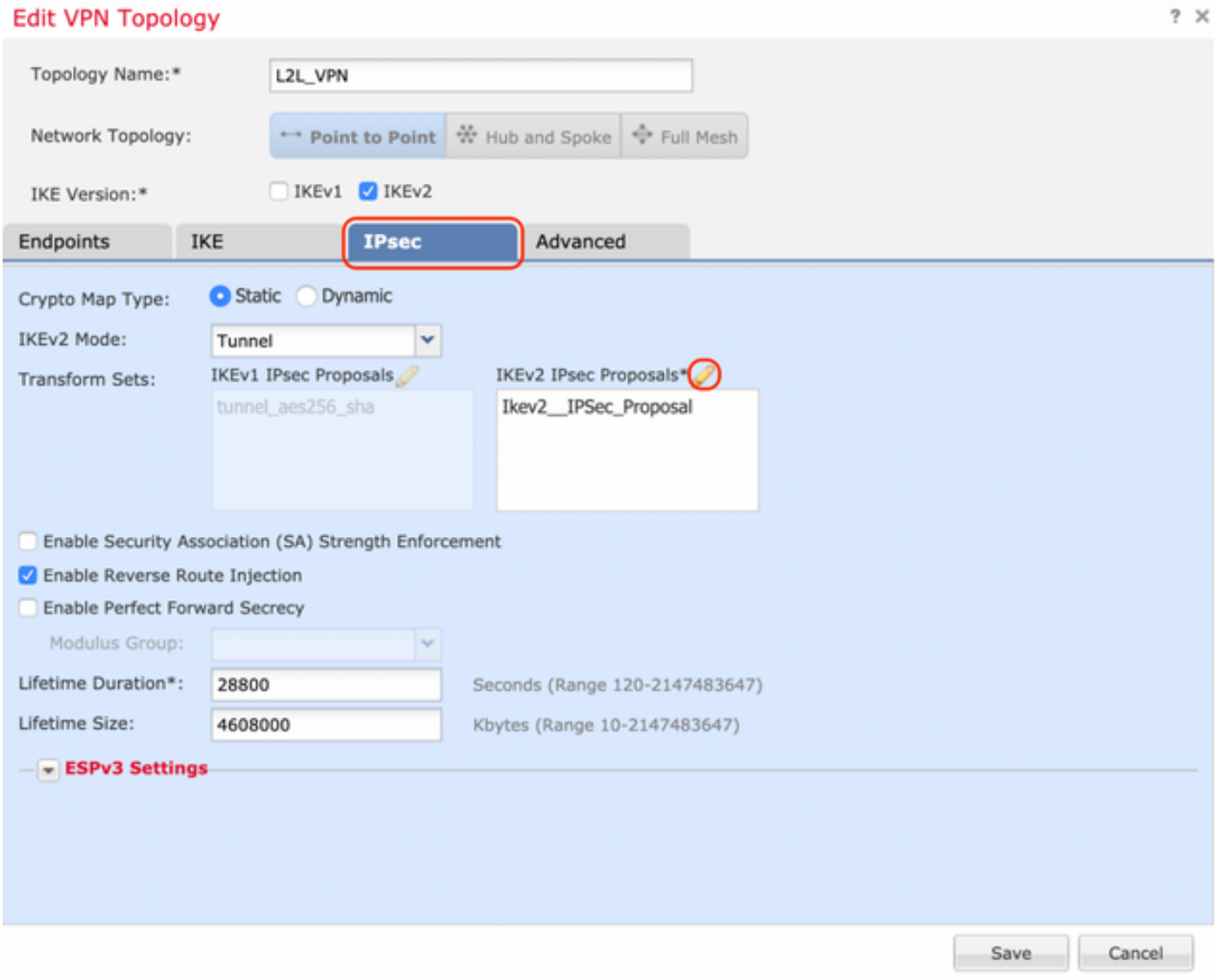
3단계. 매개변수가 추가되면 위에서 구성한 정책을 선택하고 인증 유형을 선택합니다.

사전 공유 수동 키 옵션을 선택합니다.이 가이드에서는 사전 공유 키 'cisco123'이 사용됩니다.



IPSEC 매개변수 구성

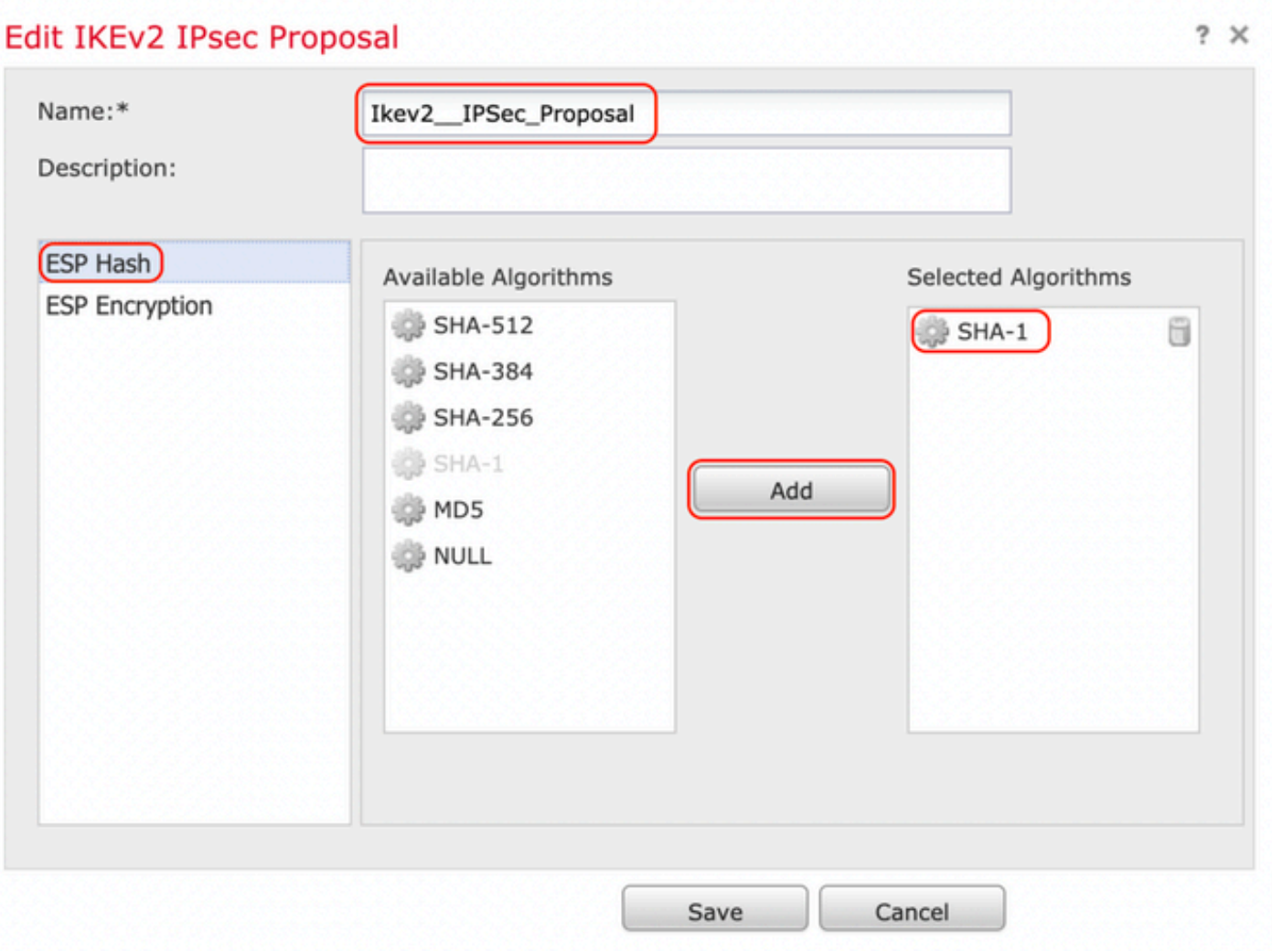
1. IPsec IPsec .

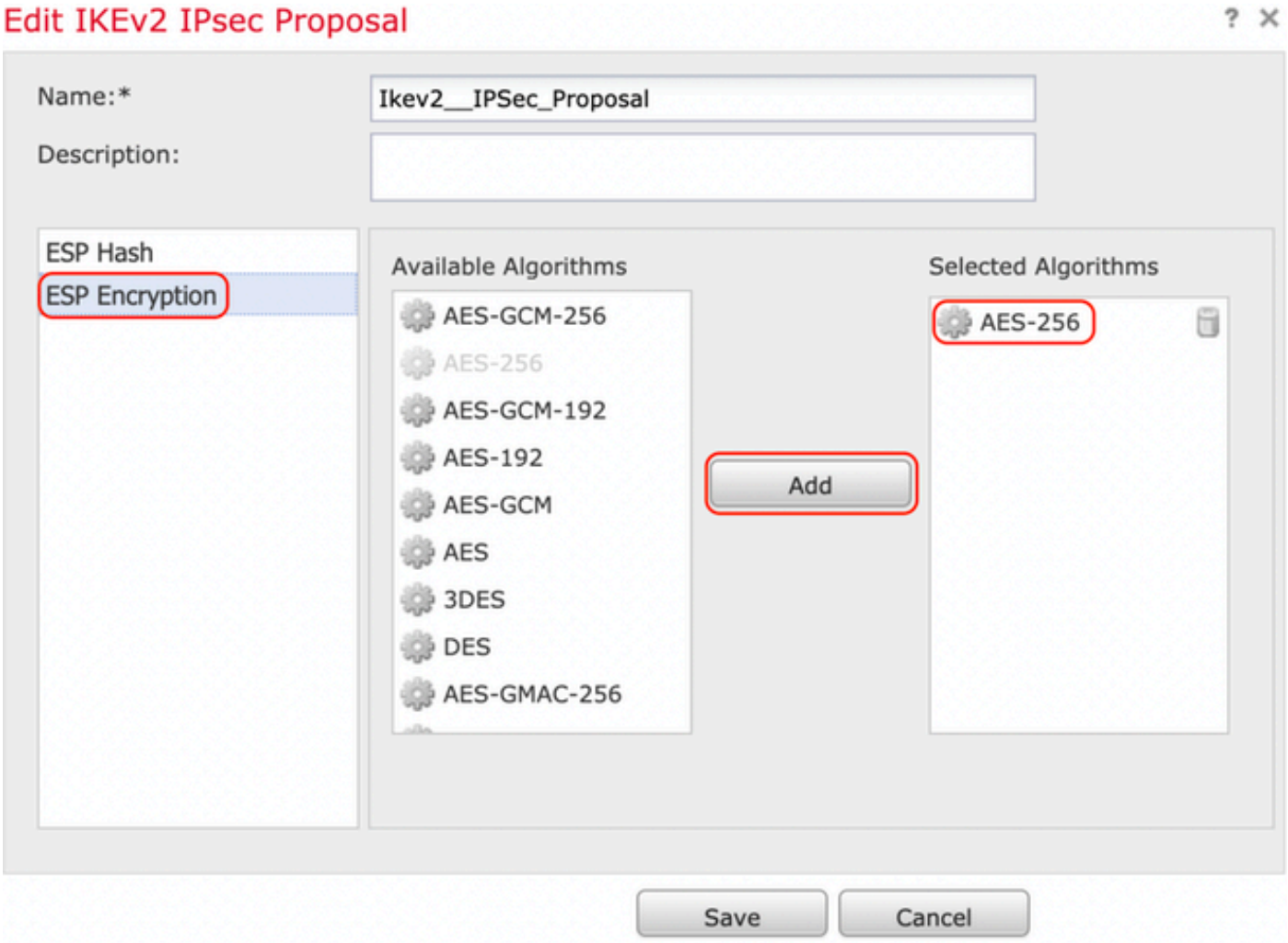


2단계. 녹색 더하기 아이콘을 선택하고 아래와 같이 2단계 매개변수를 입력하여 새 IKEv2 IPsec 제안을 생성합니다.

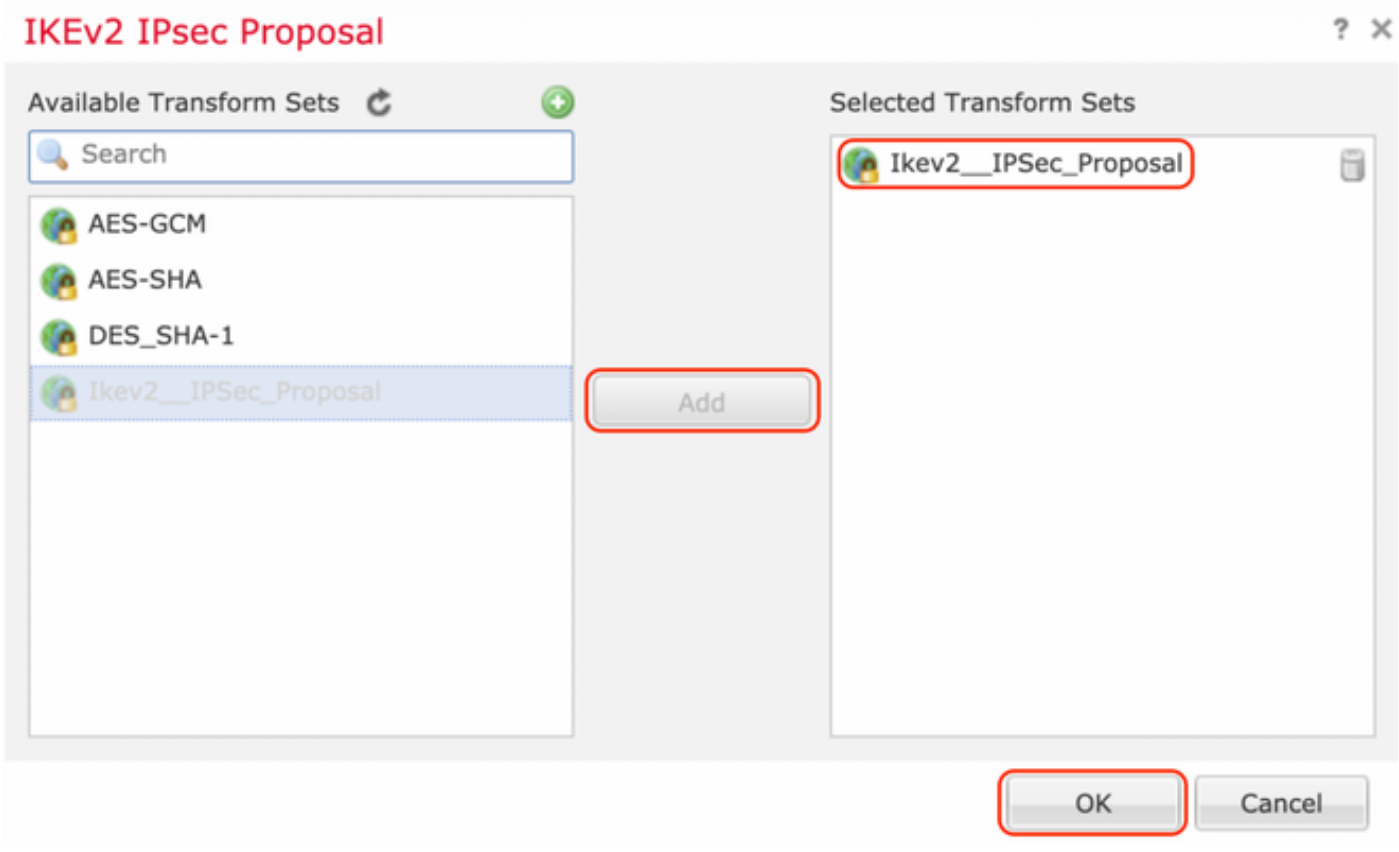
ESP 해시:SHA-1

ESP 암호화:AES-256


Edit IKEv2 IPsec Proposal
Name:*
Ikev2__IPSec_Proposal
Description:
ESP Hash
ESP Encryption
Available Algorithms
SHA-512
SHA-384
SHA-256
SHA-1
MD5
NULL
Add
Selected Algorithms
SHA-1
Save
Cancel

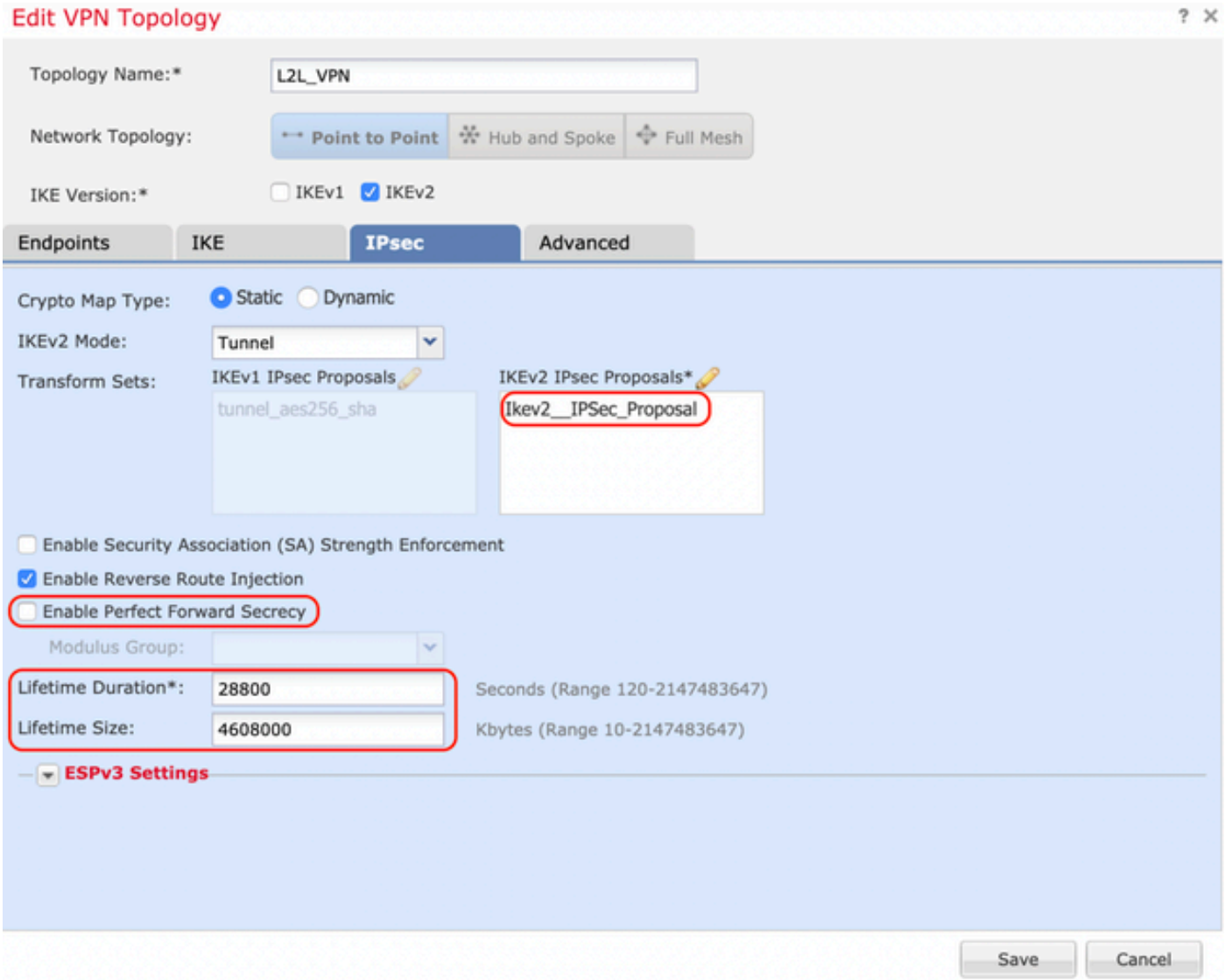


3단계. 새 IPsec 제안이 생성되면 선택한 변형 집합에 추가합니다.



4단계. 새로 선택한 IPsec 제안이 IKEv2 IPsec 제안서에 나열됩니다.

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



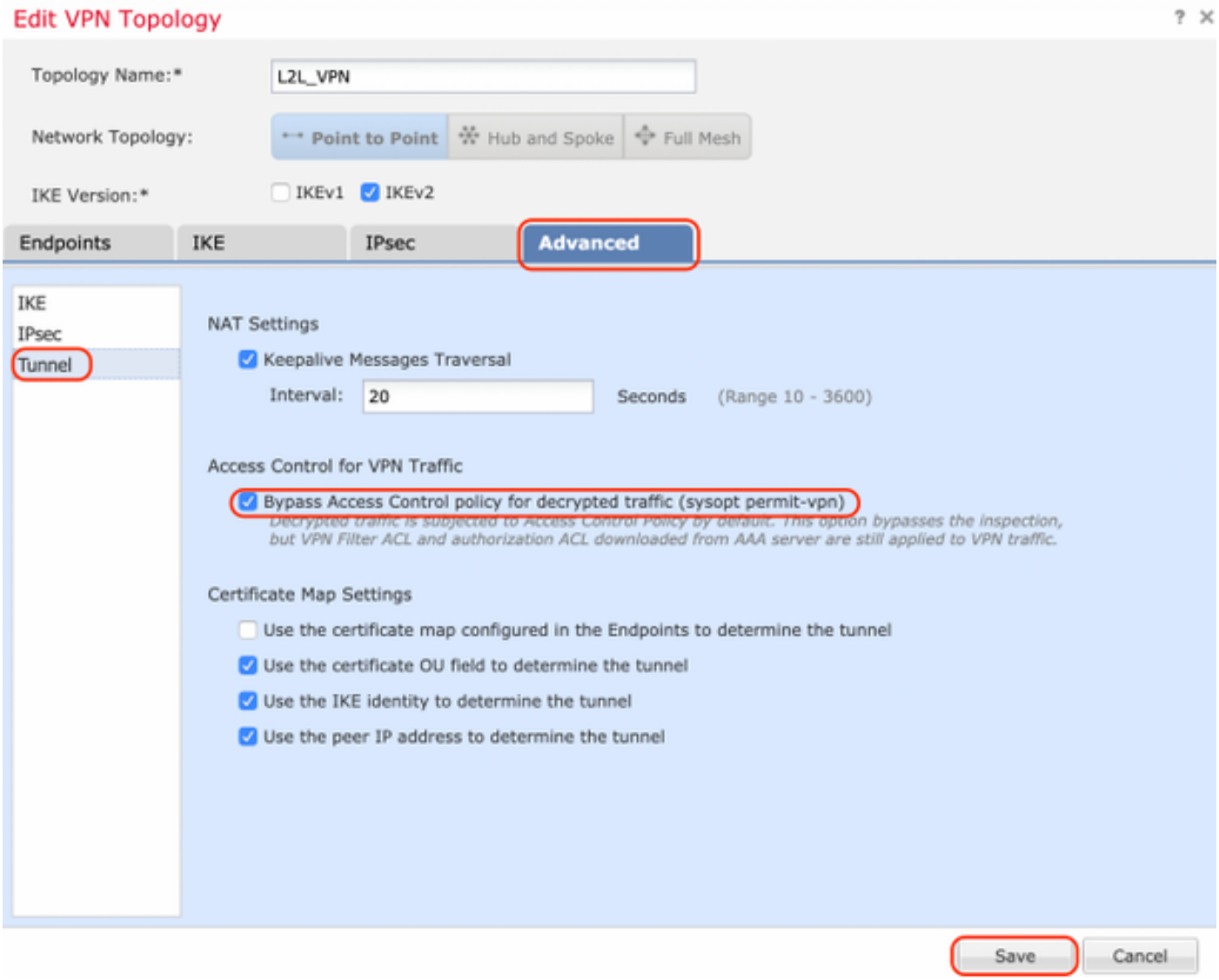
FTD를 통해 VPN 서브넷을 허용하려면 Bypass Access Control(액세스 제어 우회) 또는 Create Access Control Policy(액세스 제어 정책 생성) 규칙을 구성하려면 아래 단계를 구성해야 합니다.

액세스 제어 우회

sysopt *permit-vpn이* 활성화되지 않은 경우 FTD 디바이스를 통한 VPN 트래픽을 허용하려면 액세스 제어 정책을 생성해야 합니다.sysopt permit-vpn이 활성화된 경우 액세스 제어 정책 생성을 건너뜁니다.이 컨피그레이션 예에서는 "Bypass Access Control" 옵션을 사용합니다.

sysopt permit-*vpn* 매개변수는 *Advanced(고급)* > Tunnel(터널)에서 활성화할 수 있습니다.

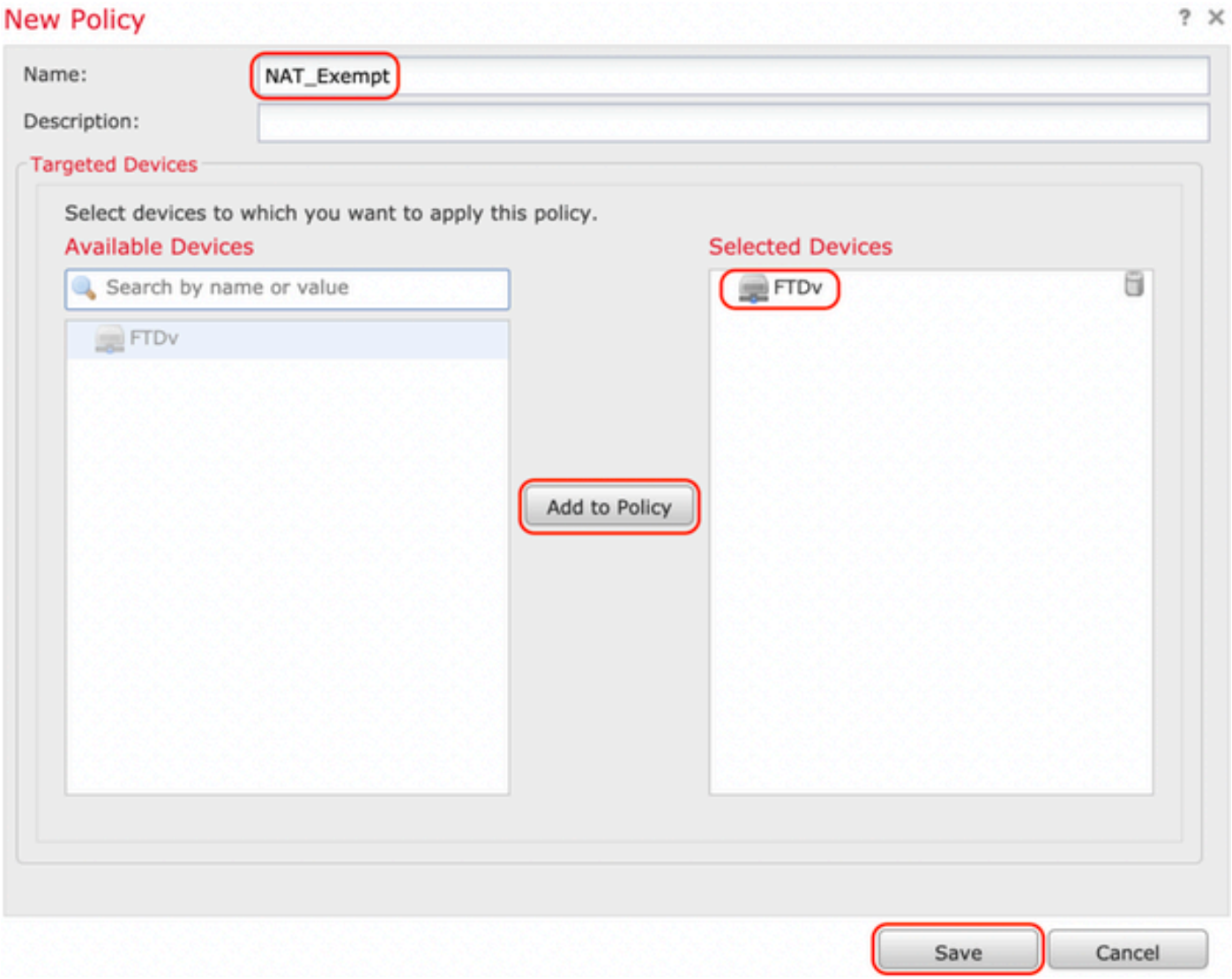
> **주의:**이 옵션은 Access Control Policy를 사용하여 사용자로부터 들어오는 트래픽을 검사할 가능성을 제거합니다.VPN 필터 또는 다운로드 가능한 ACL을 사용하여 사용자 트래픽을 필터링할 수 있습니다.이 명령은 전역 명령이며 이 확인란이 활성화된 경우 모든 VPN에 적용됩니다.



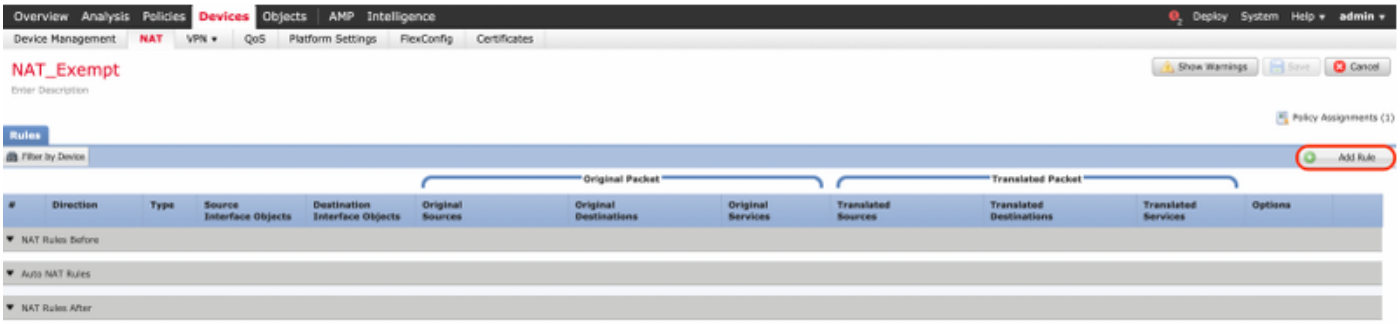
NAT 예외 구성

VPN 트래픽에 대한 NAT Exemption 문을 구성합니다.VPN 트래픽이 다른 NAT 문과 일치하고 VPN 트래픽을 잘못 변환하지 않도록 하려면 NAT 면제가 있어야 합니다.

1단계. Devices(디바이스) **> NAT** 및 c로 이동합니다.New Policy(새 정책) **> Threat Defense NAT**를 클릭하여 새 정책**을 생성합니다**.



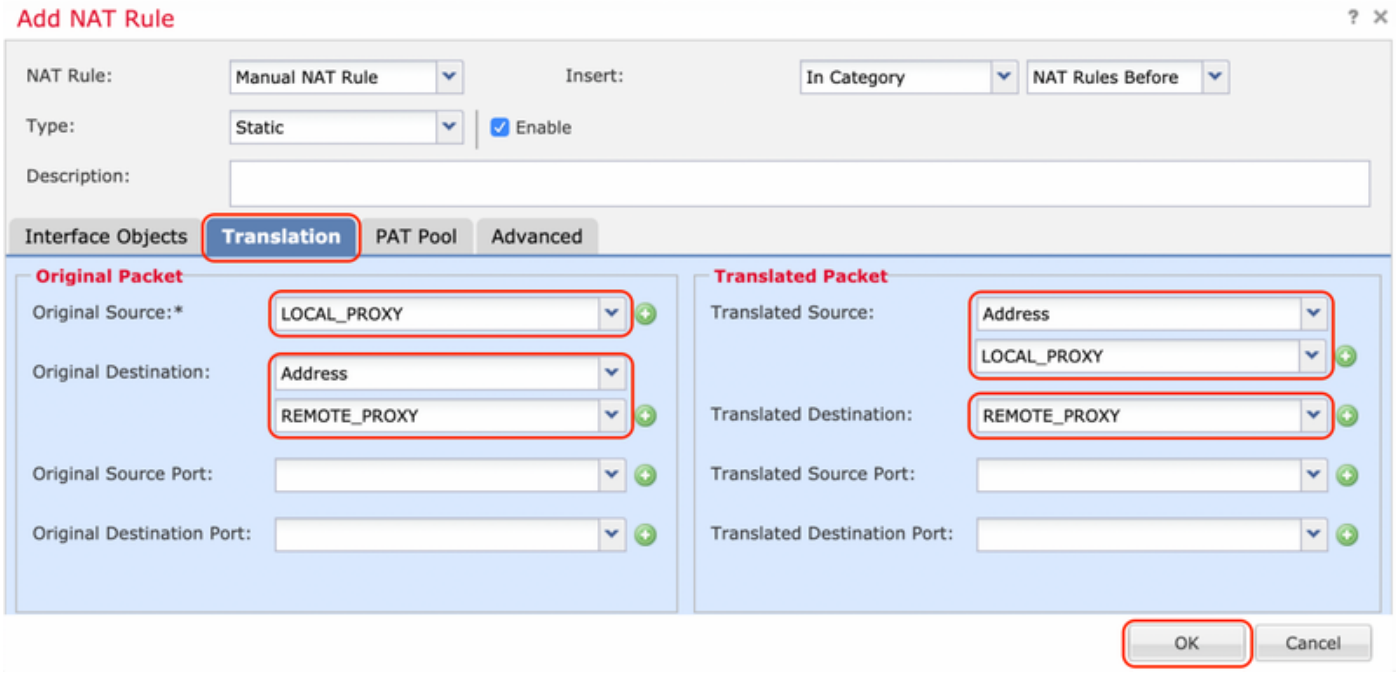
2단계. Add **Rule**(규칙 **추가)을 클릭합니다**.



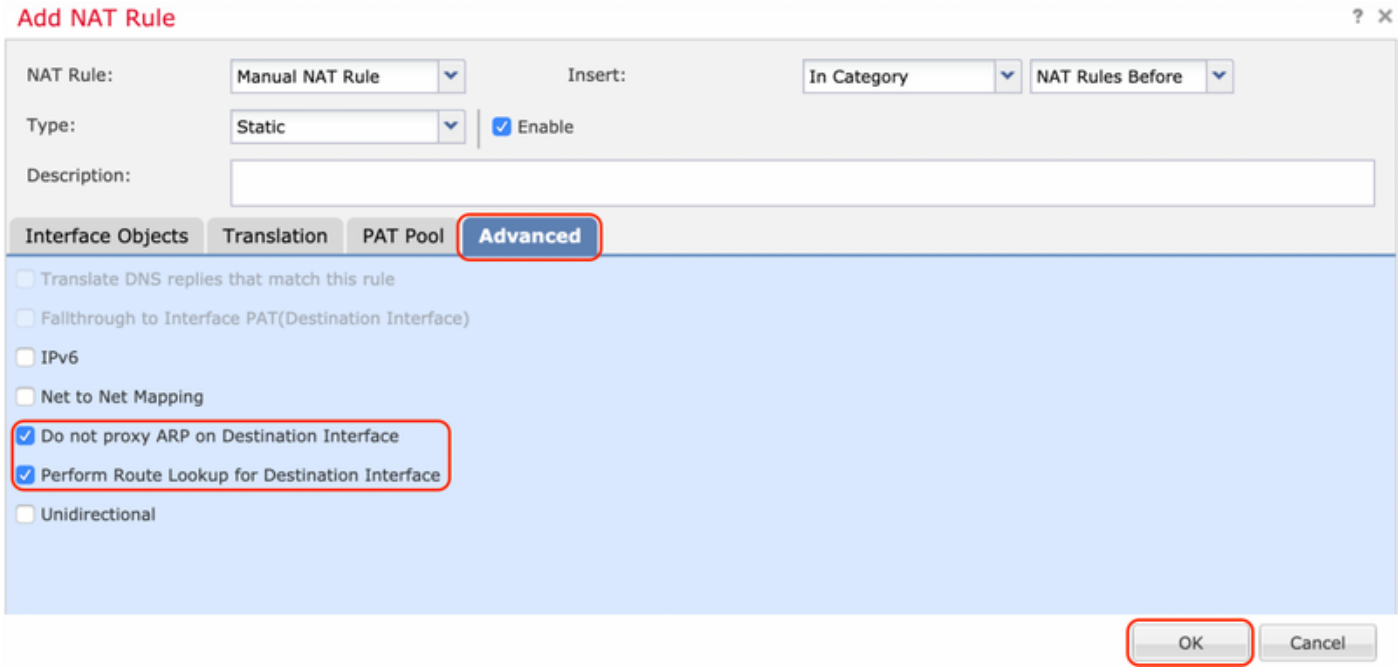
3단계. 새 고정 수동 NAT 규칙을 생성합니다.

NAT 규칙에 대한 내부 및 외부 인터페이스를 참조합니다.Interface Objects 탭에서 인터페이스를 지정하면 이러한 규칙이 다른 인터페이스의 트래픽에 영향을 주지 않습니다.

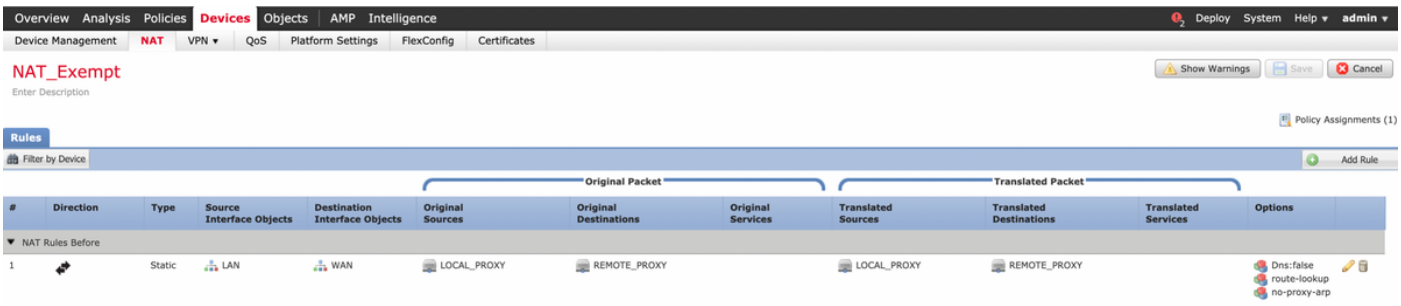
Translation(변환) 탭으로 이동하여 소스 및 대상 서브넷을 선택합니다.NAT 예외 규칙이므로 원래 소스/대상과 변환된 소스/대상이 동일한지 확인합니다.



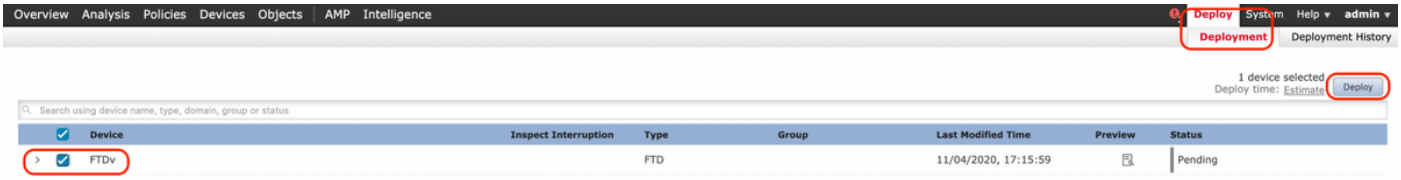
Advanced(고급) 탭을 클릭하고 no-proxy-arp 및 route-lookup을 활성화합니다.



이 규칙을 저장하고 NAT 목록에서 최종 NAT 문을 확인합니다.



4단계. 컨피그레이션이 완료되면 컨피그레이션을 저장하고 FTD에 구축합니다.



다음을 확인합니다.

LAN 시스템에서 흥미로운 트래픽을 시작하거나 ASA에서 아래의 packet-tracer 명령을 실행할 수 있습니다.

```
packet-tracer input inside icmp 2001:aaaa::23 128 0 2001:dddd::33 detail
```

참고: Here Type = 128 및 Code=0은 ICMPv6 "Echo Request"를 나타냅니다.

아래 섹션에서는 ASAv 또는 FTD LINA CLI에서 실행하여 IKEv2 터널의 상태를 확인할 수 있는 명령에 대해 설명합니다.

다음은 ASA의 출력의 예입니다.

```
ciscoasa# show crypto ikev2 sa

IKEv2 SAs:

Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 Remote
                      Status         Role
  6638313 2001:bbbb::1/500                                      2001:cccc::1/500
                      READY    INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/224 sec
Child sa: local selector  2001:aaaa::/0 - 2001:aaaa::ffff:ffff:ffff:ffff/65535
          remote selector 2001:dddd::/0 - 2001:dddd::ffff:ffff:ffff:ffff/65535
          ESP spi in/out: 0xa0fd3fe6/0xd95ecdb8


ciscoasa# show crypto ipsec sa detail
interface: outside
    Crypto map tag: VPN, seq num: 1, local addr: 2001:bbbb::1

      access-list CRYPTO_ACL extended permit ip 2001:aaaa::/64 2001:dddd::/64
      local ident (addr/mask/prot/port): (2001:aaaa::/64/0/0)
      remote ident (addr/mask/prot/port): (2001:dddd::/64/0/0)
      current_peer: 2001:cccc::1

      #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 11
      #pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 11
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #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
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
```

```
      #pkts invalid pad (rcv): 0,
      #pkts invalid ip version (rcv): 0,
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 2001:bbbb::1/500, remote crypto endpt.: 2001:cccc::1/500
      path mtu 1500, ipsec overhead 94(64), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D95ECDB8
      current inbound spi : A0FD3FE6

    inbound esp sas:
      spi: 0xA0FD3FE6 (2700951526)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 1937408, crypto-map: VP
         sa timing: remaining key lifetime (kB/sec): (4055040/28535)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0xD95ECDB8 (3646868920)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 1937408, crypto-map: VPN
         sa timing: remaining key lifetime (kB/sec): (4193280/28535)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001


ciscoasa# show vpn-sessiondb detail l2l filter name 2001:cccc::1

Session Type: LAN-to-LAN Detailed

Connection   : 2001:cccc::1
Index        : 473                    IP Addr      : 2001:cccc::1
Protocol     : IKEv2 IPsec
Encryption   : IKEv2: (1)AES256  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA256  IPsec: (1)SHA1
Bytes Tx     : 352                    Bytes Rx     : 352
Login Time   : 12:27:36 UTC Sun Apr 12 2020
Duration     : 0h:06m:40s

IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
  Tunnel ID    : 473.1
  UDP Src Port : 500                    UDP Dst Port : 500
  Rem Auth Mode: preSharedKeys
  Loc Auth Mode: preSharedKeys
  Encryption   : AES256                 Hashing      : SHA256
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86000 Seconds
  PRF          : SHA256                 D/H Group    : 14
  Filter Name  :

IPsec:
  Tunnel ID    : 473.2
```

```
Local Addr    : 2001:aaaa::/64/0/0
Remote Addr   : 2001:dddd::/64/0/0
Encryption    : AES256                  Hashing      : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds            Rekey Left(T): 28400 Seconds
Rekey Int (D): 4608000 K-Bytes          Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 30 Minutes               Idle TO Left : 23 Minutes
Bytes Tx      : 352                     Bytes Rx     : 352
Pkts Tx       : 11                      Pkts Rx      : 11
```

문제 해결

ASA 및 FTD에서 IKEv2 터널 설정 문제를 해결하려면 다음 debug 명령을 실행합니다.

디버그 암호화 조건 피어 <피어 IP>
debug crypto ikev2 protocol 255
debug crypto ikev2 platform 255

다음은 참조를 위해 작동하는 IKEv2 디버깅 샘플입니다.
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

참조

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425-configure-ipsec-00.html
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/81824-common-ipsec-trouble.html
https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/vpn/asa-95-vpn-config/vpn-site2site.html