BGP를 오버레이로 사용하여 ASA와 FTD 간의 경로 기반 Site-To-Site VPN 구성

목차

소개

firepower Firepower 이 문서에서는 BGP(Dynamic Routing Border Gateway Protocol)를 오버레이로 사용하는 FMC(Domain Management Center)에서 ASA(Adaptive Security Appliance)와 FTD(Domain Threat Defense Managed) 간의 경로 기반 Site-to-Site VPN 터널을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- IPsec Site-to-Site VPN에 대한 기본 이해
- FTD 및 ASA의 BGP 컨피그레이션
- FMC 경험

사용되는 구성 요소

- Cisco ASAv 버전 9.20(2)2
- Cisco FMC 버전 7.4.1
- Cisco FTD 버전 7.4.1

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

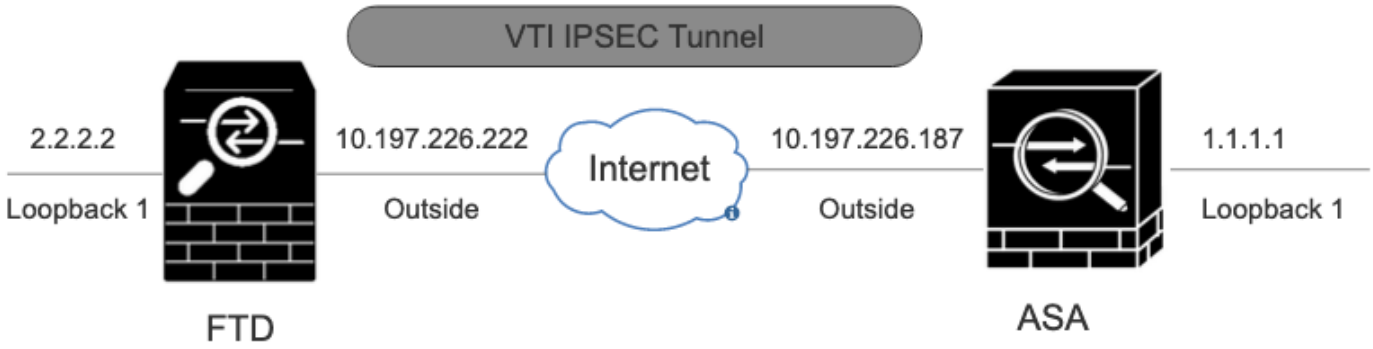
경로 기반 VPN은 VPN 터널을 통해 전송되거나 암호화되는 관심 트래픽을 결정하고 정책 기반 또는 암호화 맵 기반 VPN에서처럼 정책/액세스 목록 대신 트래픽 라우팅을 사용합니다. 암호화 도메인은 IPsec 터널로 들어오는 모든 트래픽을 허용하도록 설정됩니다. IPsec 로컬 및 원격 트래픽 선택기는 0.0.0.0/0.0.0.0으로 설정됩니다. IPsec 터널로 라우팅되는 트래픽은 소스/대상 서브넷과 상관없이 암호화됩니다.

이 문서에서는 동적 라우팅 BGP를 오버레이로 사용하는 SVTI(Static Virtual Tunnel Interface) 컨피그레이션에 대해 중점적으로 설명합니다.

구성

이 섹션에서는 SVTI IPSec 터널을 통해 BGP 네이버십을 가져오기 위해 ASA 및 FTD에서 필요한 컨피그레이션에 대해 설명합니다.

네트워크 다이어그램



네트워크 다이어그램

설정

FMC를 사용하여 FTD에서 IPSec VPN 구성

1단계. 로 Devices > VPN > Site To Site 이동합니다.

2단계. 를 클릭합니다+Site to Site VPN.

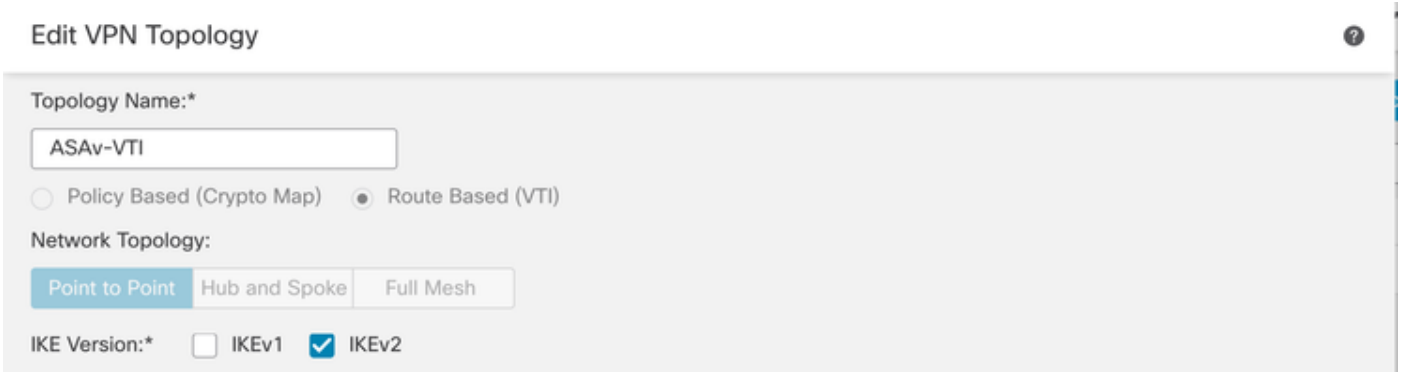
사이트 대 사이트 *VPN*

3단계. 를 Topology Name 제공하고 Type of VPN as(VPN 유형)를 Route Based (VTI) 선택합니다. 를 IKE Version 선택합니다.

이 데모의 경우:

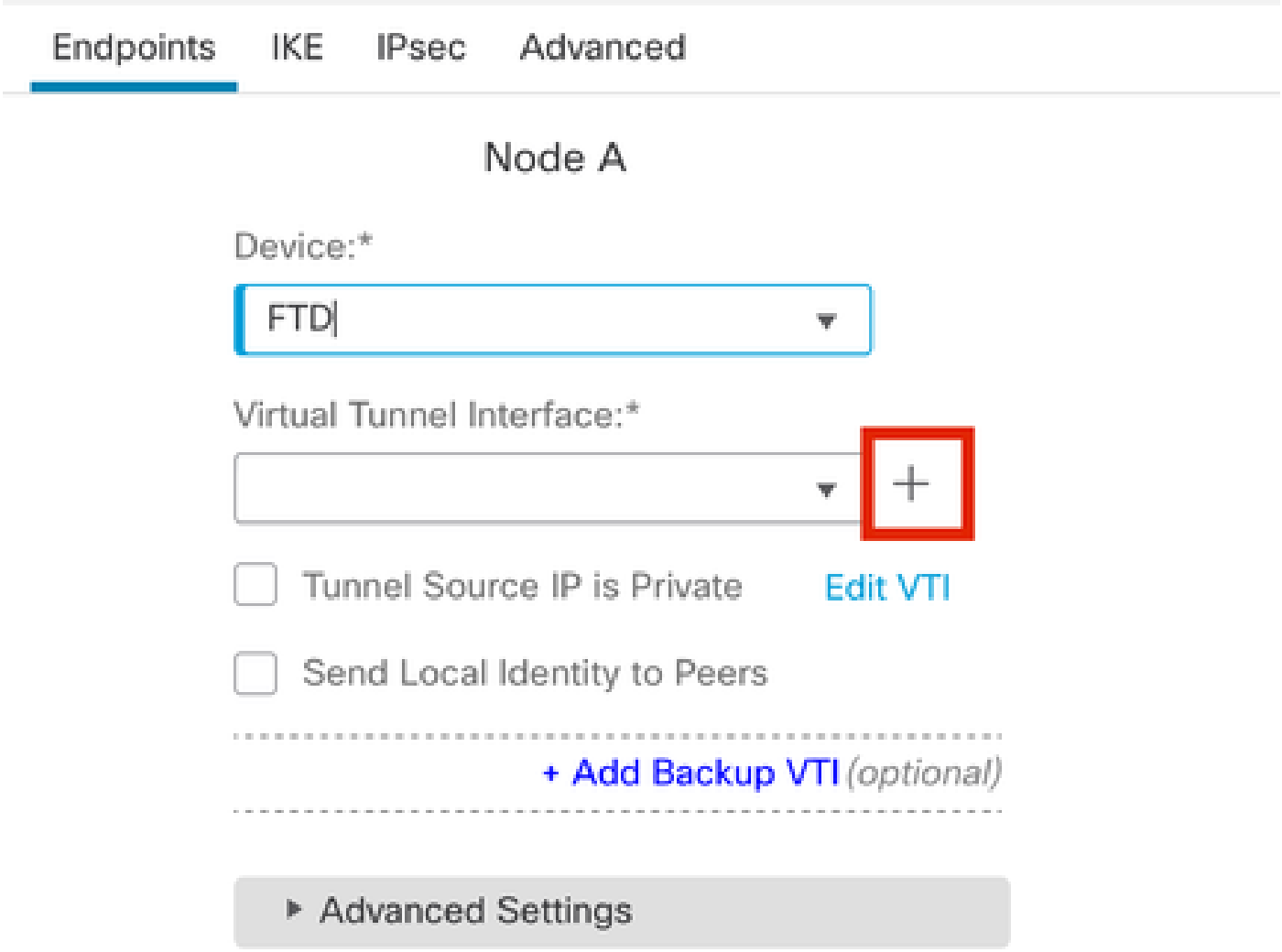
토폴로지 이름: ASAv-VTI

IKE 버전: IKEv2



VPN 토폴로지

4단계. 터널Device을 구성해야 하는 를 선택합니다. 새 가상 터널 인터페이스를 추가하거나(아이콘 클릭) 기존 목록에서 가상 터널+ 인터페이스를 선택할 수 있습니다.



엔드포인트 노드 *A*

5단계. 의 매개변수를 New Virtual Tunnel Interface 정의합니다. 를 Ok 클릭합니다.

이 데모의 경우:

이름: ASA-VTI

설명(선택 사항): 엑스트라넷 ASA를 사용하는 VTI 터널

보안 영역: VTI 영역

터널 ID: 1

IP 주소: 169.254.2.1/24

터널 소스: GigabitEthernet0/1(외부)

IPsec 터널 모드: IPv4

Add Virtual Tunnel Interface

General | Path Monitoring

Tunnel Type

(•) Static ( ) Dynamic

Name:*

ASAv-VTI

[x] Enabled

Description:

VTI Tunnel with Extranet ASA

Security Zone:

VTI-Zone

Priority:

0 (0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VT

Tunnel ID:*

3 (0 - 10413)

Tunnel Source:*

GigabitEthernet0/1 (Outside) | 10.197.226.222

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

(•) IPv4 ( ) IPv6

IP Address:*

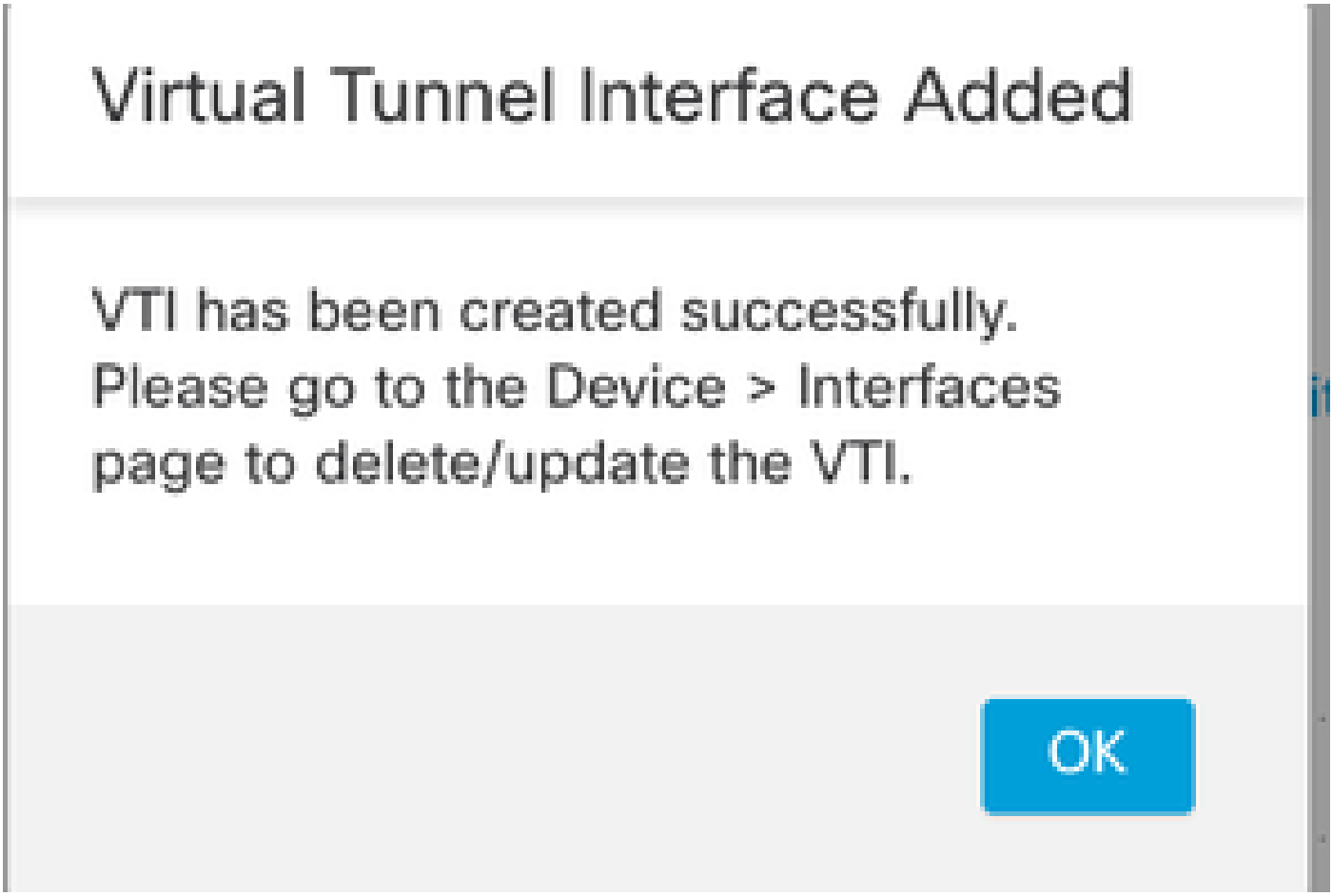
(•) Configure IP 169.254.2.1/24

( ) Borrow IP (IP unnumbered) Loopback1 (loopback)

Cancel OK

가상 터널 인터페이스

6단계. 새 VTI가 생성되었음을 알리는 팝업을 클릭합니다OK.



가상 터널 인터페이스 추가됨

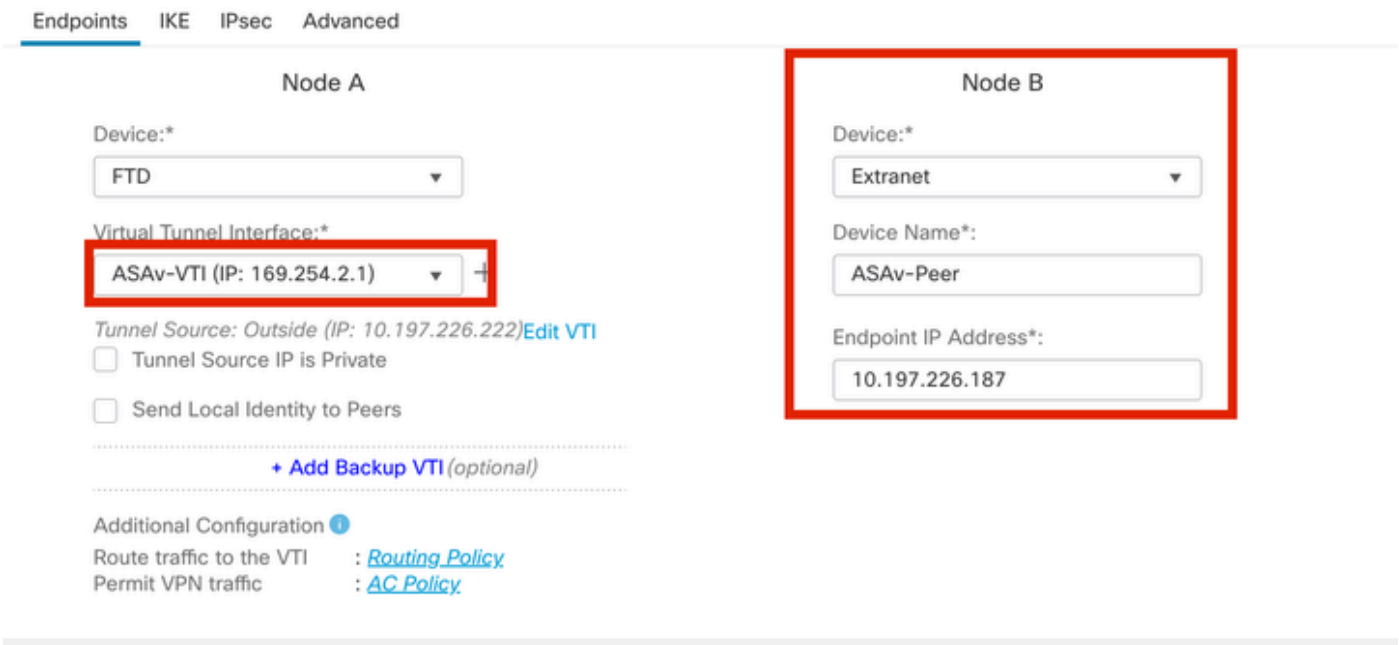
7단계. 에서 새로 생성된 VTI 또는 VTI를 Virtual Tunnel Interface 선택합니다. 노드 B(피어 디바이스)에 대한 정보를 제공합니다.

이 데모의 경우:

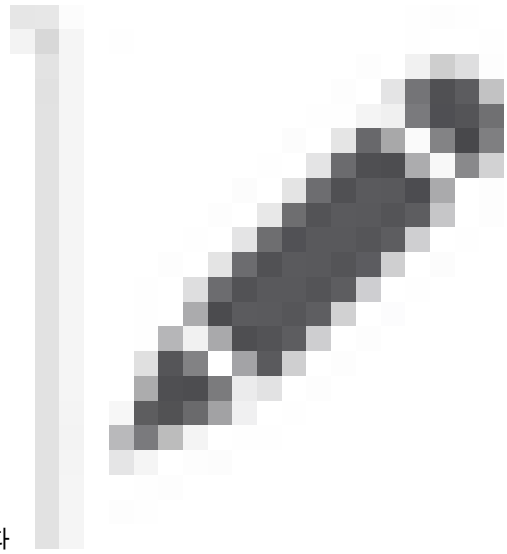
장치: 엑스트라넷

디바이스 이름: ASAv-Peer

엔드포인트 IP 주소: 10.197.226.187



엔드포인트 노드 *B*



8단계. IKE 탭으로 이동합니다. 를 클릭합니다
. 미리 정의된 Policy 항목을 사용하도록 선택하거나 탭 +옆에 있는 Policy단추를 클릭하여 새 항목을 만들 수 있습니다.

9단계(새 IKEv2 정책을 생성하는 경우 선택 사항) 정책에 Name대한 를 제공하고 정책에서Algorithms 사용할 를 선택합니다. 를 Save 클릭합니다.

이 데모의 경우:

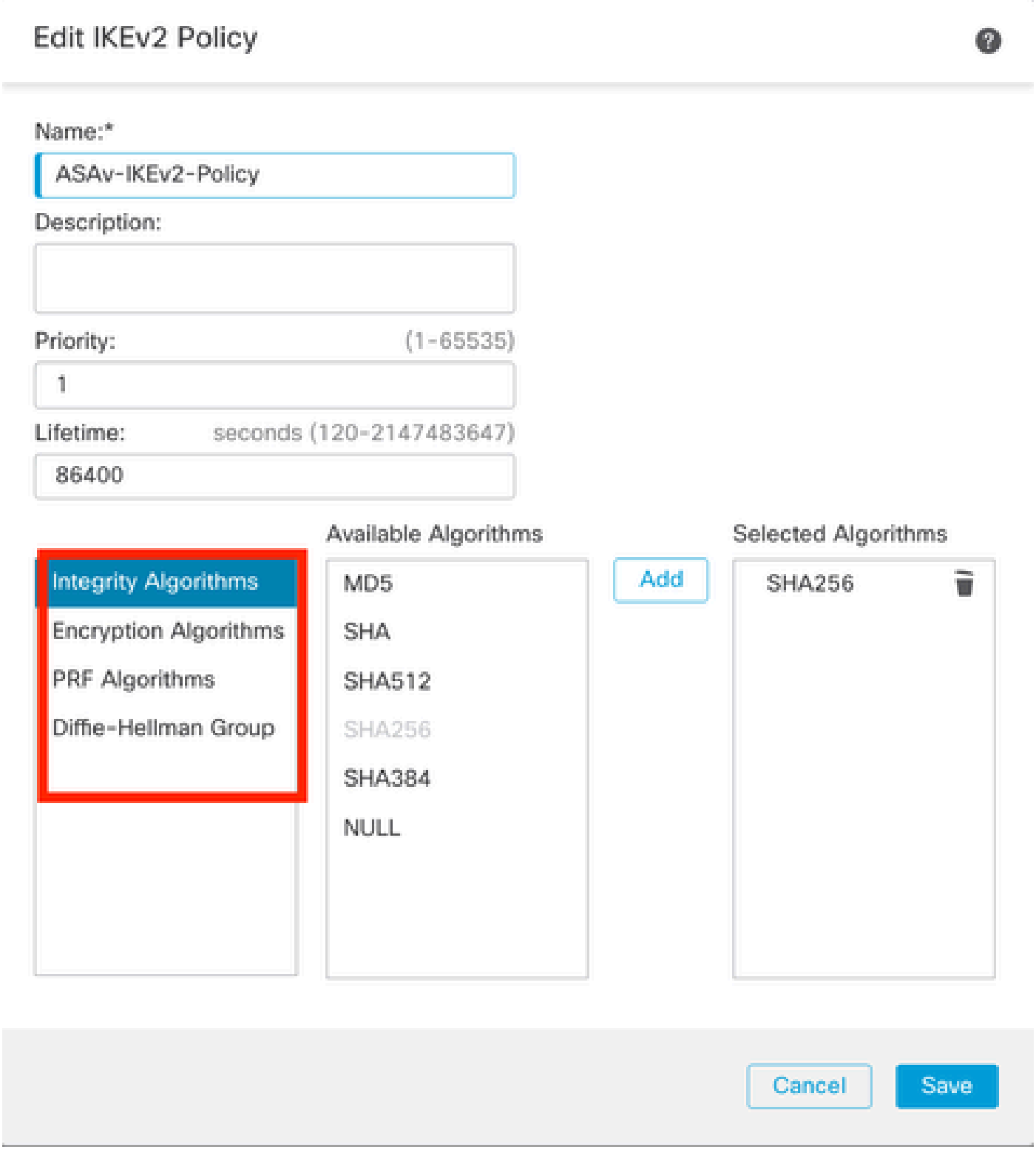
이름: ASAv-IKEv2-policy

무결성 알고리즘: SHA-256

암호화 알고리즘: AES-256

PRF 알고리즘: SHA-256

Diffie-Hellman 그룹: 14



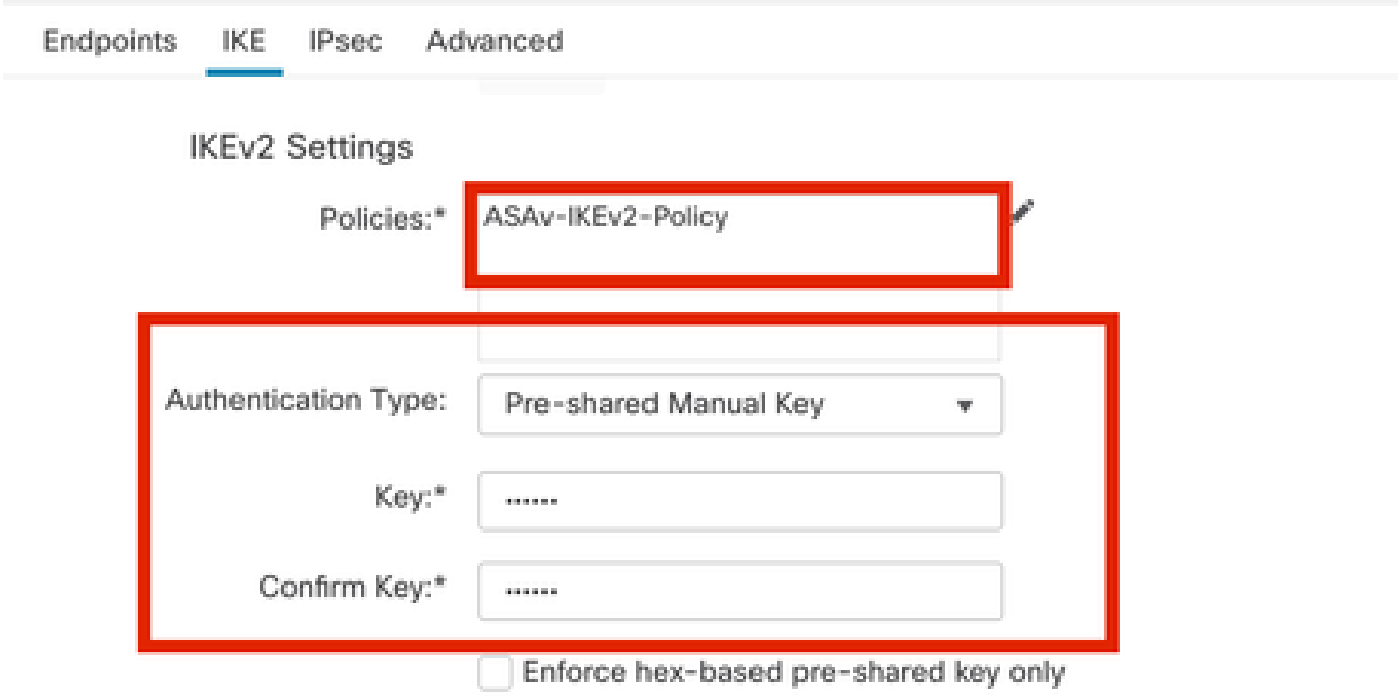
IKEv2-정책

10단계. 새로 생성된 Policy 또는 존재하는 Policy을 선택합니다. 을 Authentication Type선택합니다. 사전 공유 수동 키를 사용하는 경우 Key및 상자에 키를 Confirm Key 입력합니다.

이 데모의 경우:

정책: ASAv-IKEv2-Policy

인증 유형: 사전 공유 수동 키



인증

11단계. 탭으로 IPsec 이동합니다. 을 클릭하면 사전 정의된 IKEv2 IPsec 제안을 사용하도록 선택하거나 새로 만들 수 있습니다 . 탭 옆의 +버튼을 IKEv2 IPsec Proposal 클릭합니다.

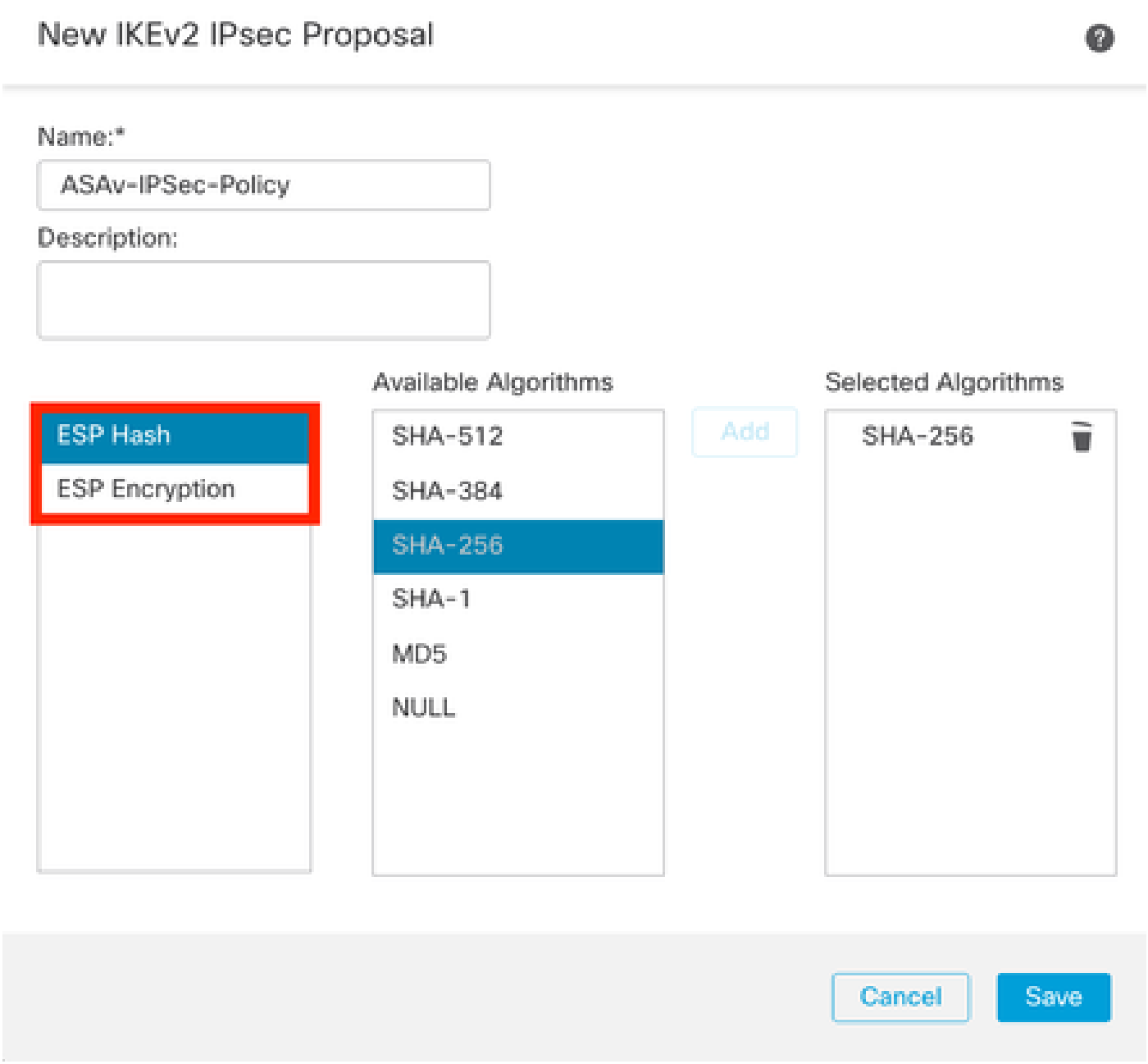
12단계(새 IKEv2 IPsec 제안을 만드는 경우 선택 사항) 제안Name에 대한 을 입력하고 제안에Algorithms 사용할 을 선택합니다. 를 Save 클릭합니다.

이 데모의 경우:

이름: ASAv-IPSec-Policy

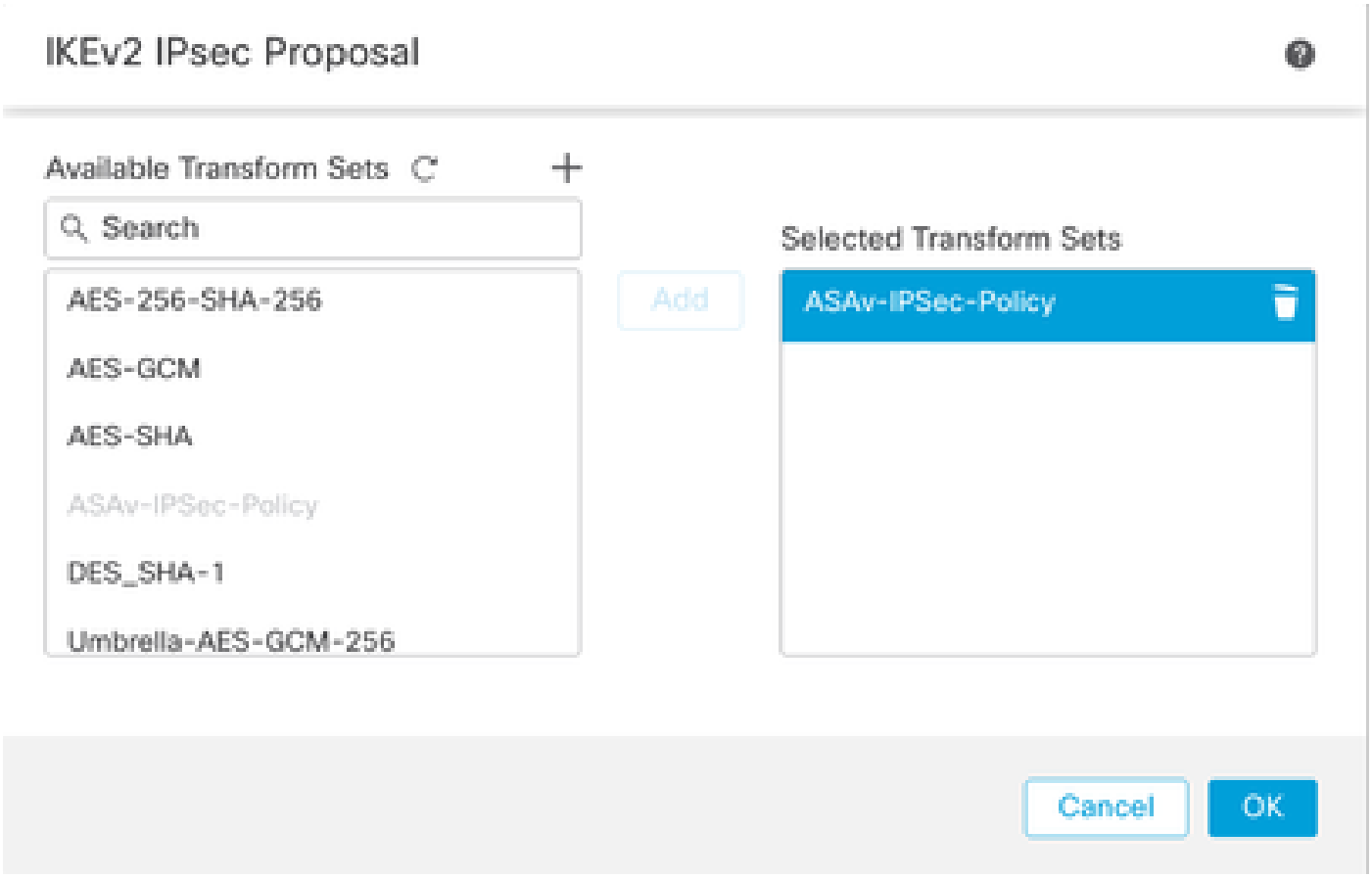
ESP 해시: SHA-256

ESP 암호화: AES-256



IKEv2-IPsec-제안

13단계. 사용 가능한 제안의 Proposal 목록에서 새로 Proposal생성했거나 존재하는 제안서를 선택합니다. 를 OK 클릭합니다.



변형 집합

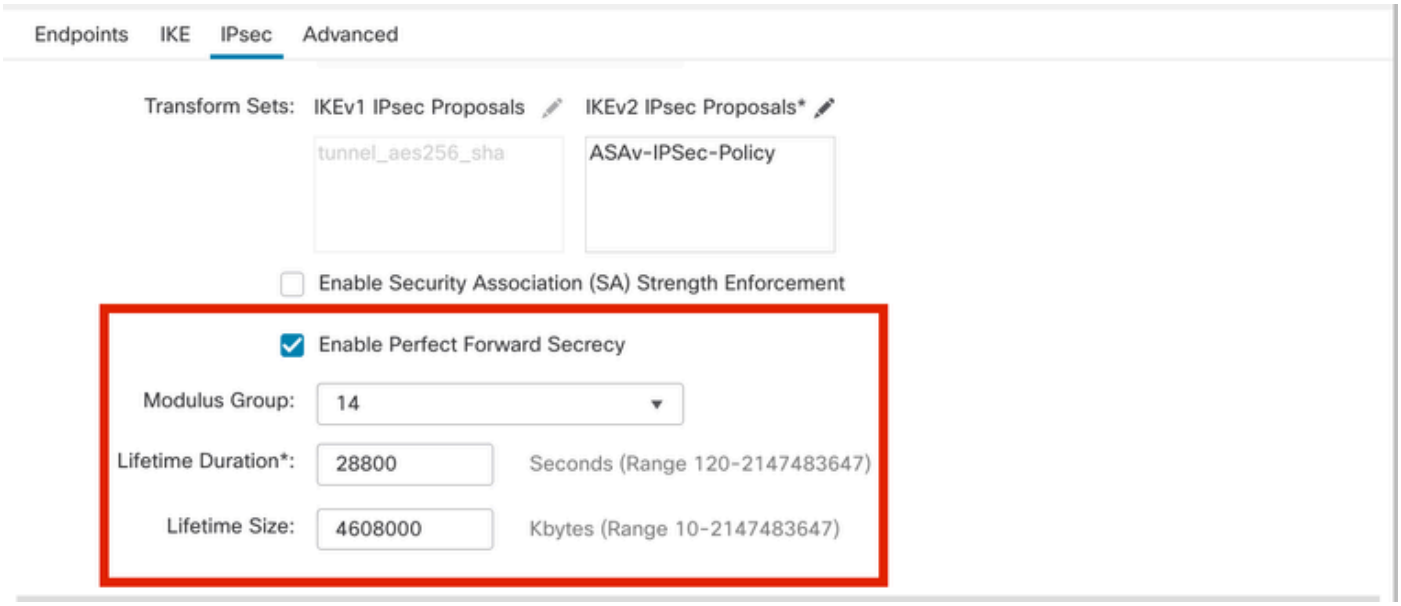
단계 14. (선택 사항) 설정을 Perfect Forward Secrecy 선택합니다. IPsec을 Lifetime Duration and Lifetime Size구성합니다.

이 데모의 경우:

PFS(Perfect Forward Secrecy): 모듈러스 그룹 14

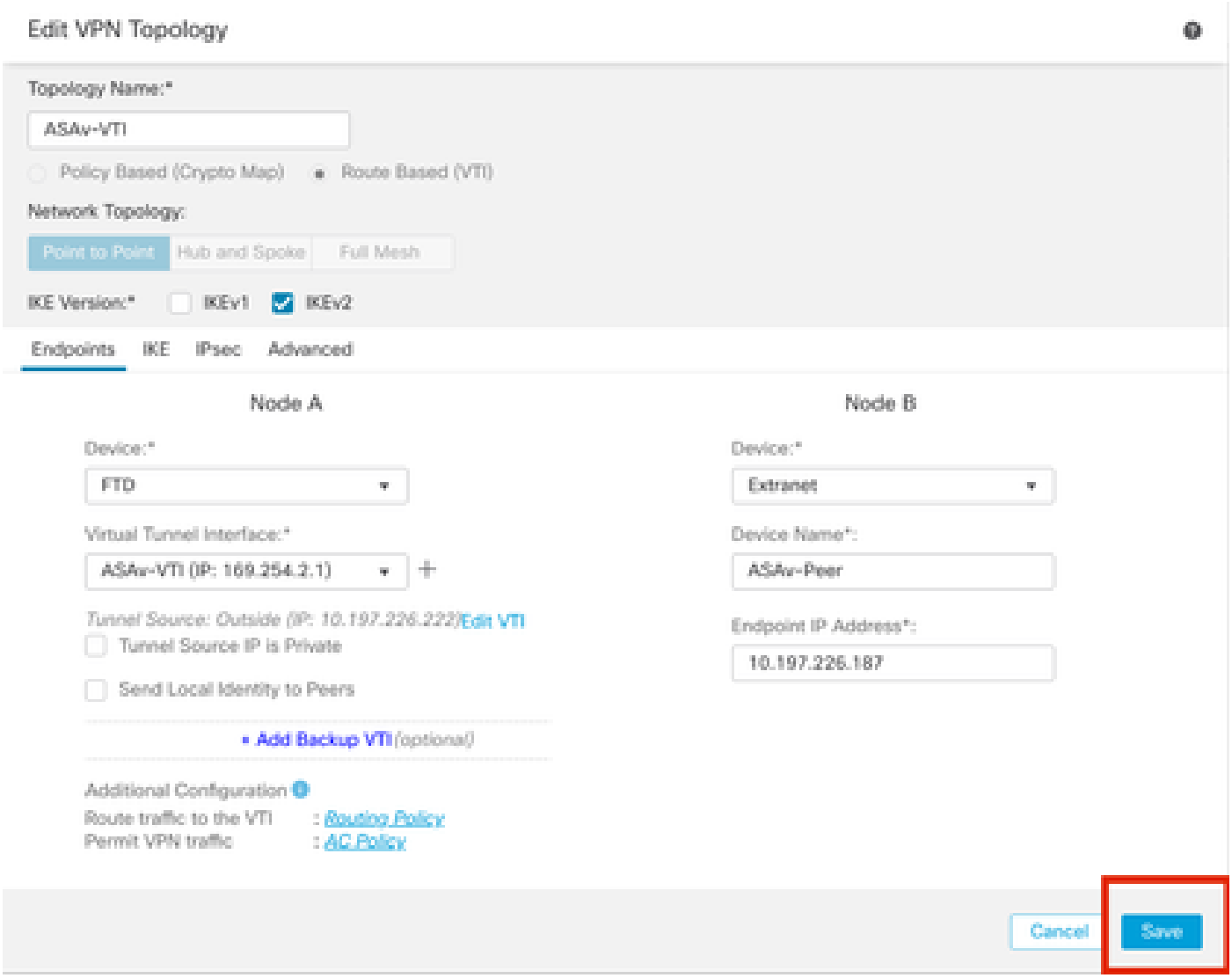
수명 기간: 28800(기본값)

수명 크기: 4608000(기본값)



PFS 구성

15단계. 구성된 설정을 확인합니다. 이 이미지에 표시된 대로 을 클릭합니다Save.



컨피그레이션 저장

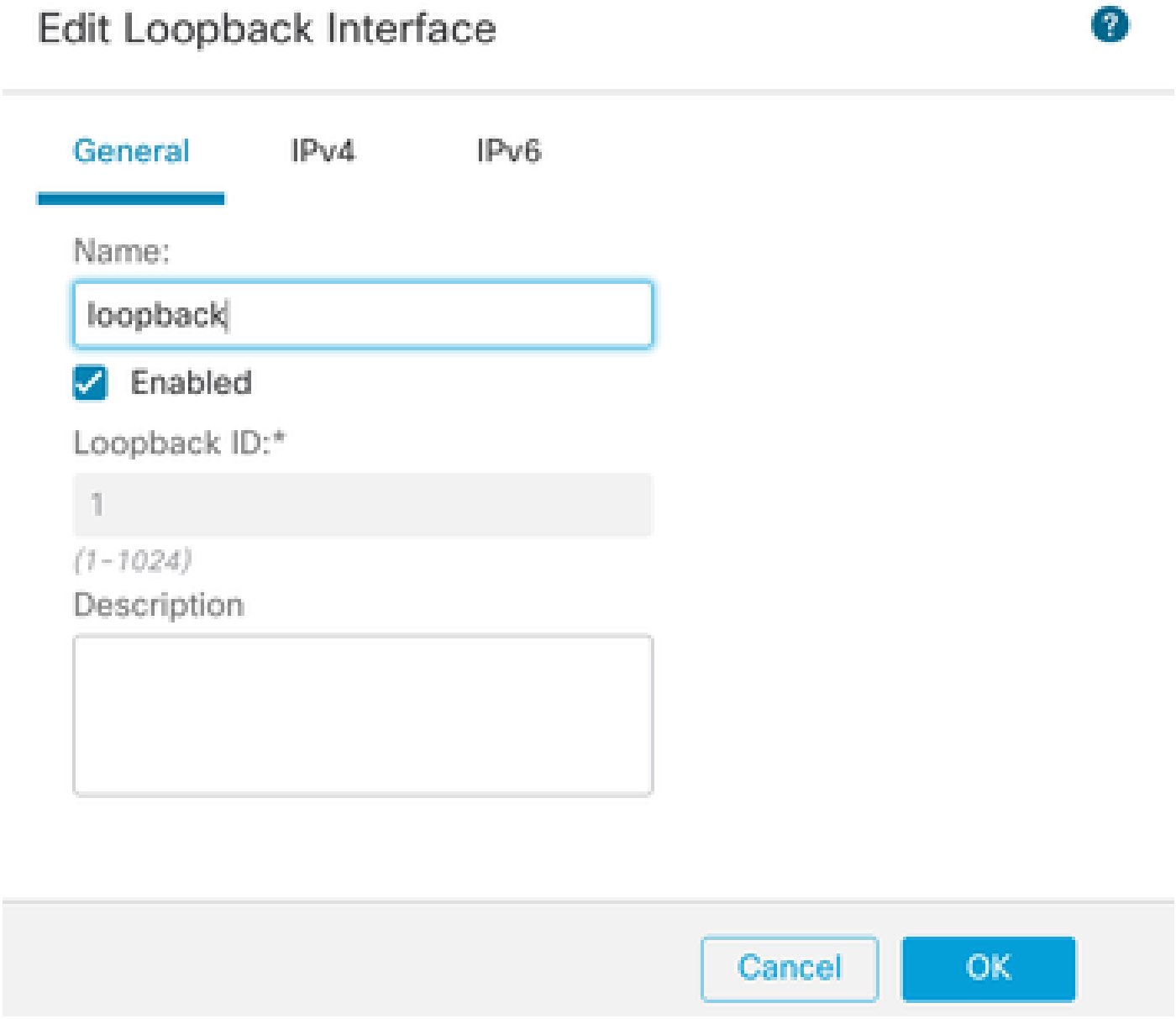
FMC를 사용하여 FTD에서 루프백 인터페이스 구성

로 Devices > Device Management 이동합니다. 루프백을 구성해야 하는 디바이스를 편집합니다.

1단계. 로 Interfaces > Add Interfaces > Loopback Interface 이동합니다.

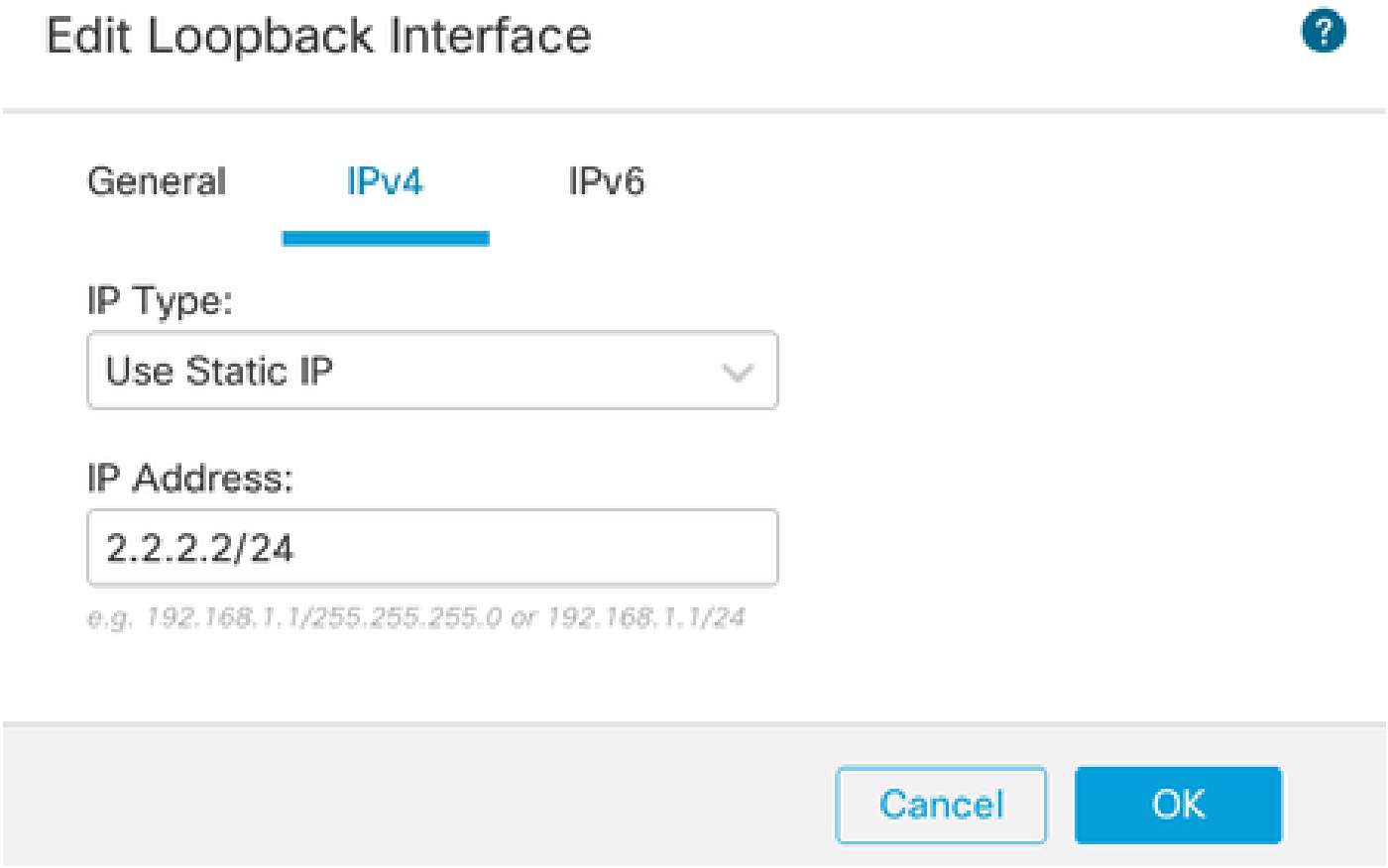
루프백 인터페이스로 이동합니다.

2단계. "루프백"이라는 이름을 입력하고 루프백 ID "1"을 입력한 다음 인터페이스를 활성화합니다.



루프백 인터페이스 활성화

3단계. 인터페이스의 IP 주소를 구성하고 을 클릭합니다OK .



루프백 인터페이스에 *IP* 주소 제공

ASA에서 IPSec VPN 구성

```
!--- Configure IKEv2 Policy ---!

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



!--- Enable IKEv2 on the outside interface ---!

crypto ikev2 enable outside



!---Configure Tunnel-Group with pre-shared-key---!

tunnel-group 10.197.226.222 type ipsec-l2l
tunnel-group 10.197.226.222 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

```
!--- Configure IPSec Policy ---!

crypto ipsec ikev2 ipsec-proposal ipsec_proposal_for_FTD
protocol esp encryption aes-256
protocol esp integrity sha-256




!--- Configure IPSec Profile ---!

crypto ipsec profile ipsec_profile_for_FTD
set ikev2 ipsec-proposal FTD-ipsec-proposal
set pfs group14




!--- Configure VTI ---!

interface Tunnel1
nameif FTD-VTI
ip address 169.254.2.2 255.255.255.0
tunnel source interface outside
tunnel destination 10.197.226.222
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec_profile_for_FTD




!--- Configure the WAN routes ---!

route outside 0.0.0.0 0.0.0.0 10.197.226.1 1
```

ASA에서 루프백 인터페이스 구성

```
interface Loopback1
nameif loopback
ip address 1.1.1.1 255.255.255.0
```

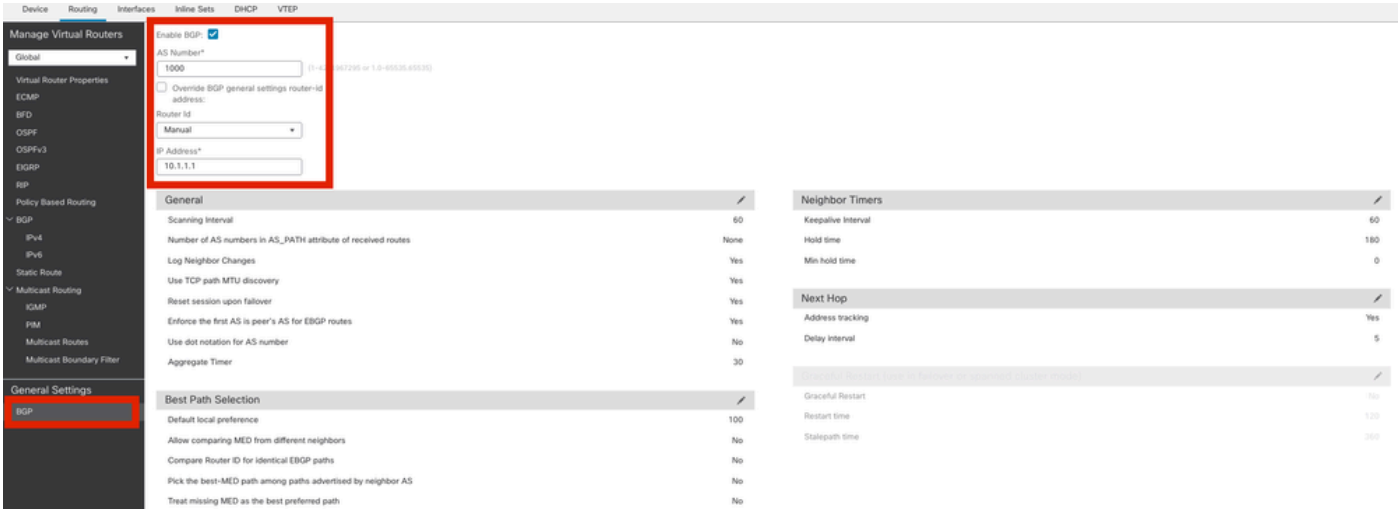
FMC를 사용하여 FTD에서 오버레이 BGP 구성

로 이동합니다Devices > Device Management.Edit VTI 터널이 구성된 디바이스로 이동한 다음 로 이동합니다Routing >General Settings > BGP.

1단계. 이 이미지에 표시된 대로 BGP를 활성화하고 AS(Autonomous System) 번호 및 라우터 ID를 구성합니다.

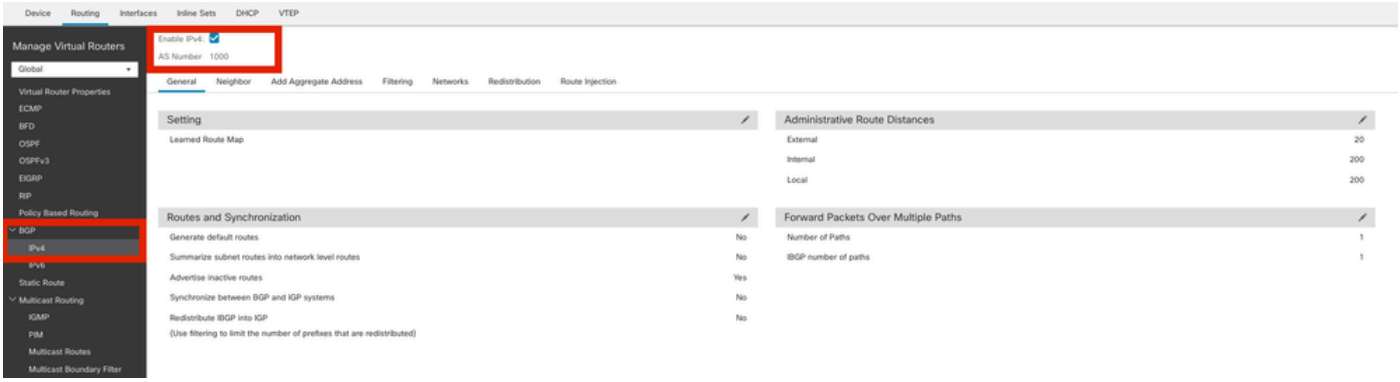
AS 번호는 두 디바이스 FTD 및 ASA에서 동일해야 합니다.

라우터 ID는 BGP에 참여하는 각 라우터를 식별하는 데 사용됩니다.



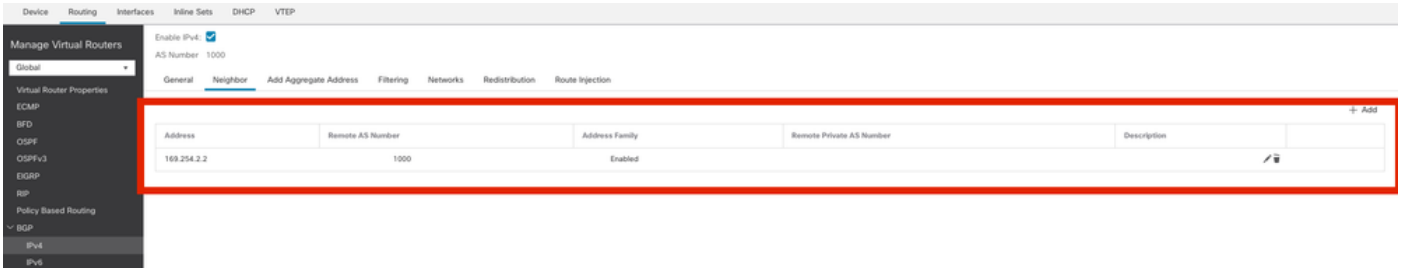
BGP 구성으로 이동합니다.

2단계. FTD에서 BGP > IPv4 BGP IPv4로 이동하여 활성화합니다.



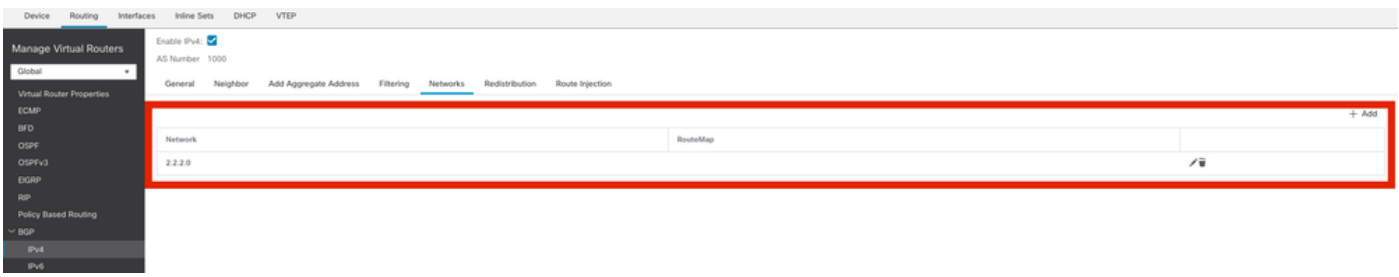
BGP 활성화

3단계. Tab(탭)에서Neighbor ASAv VTI 터널 IP 주소를 인접 디바이스로 추가하고 인접 디바이스를 활성화합니다.



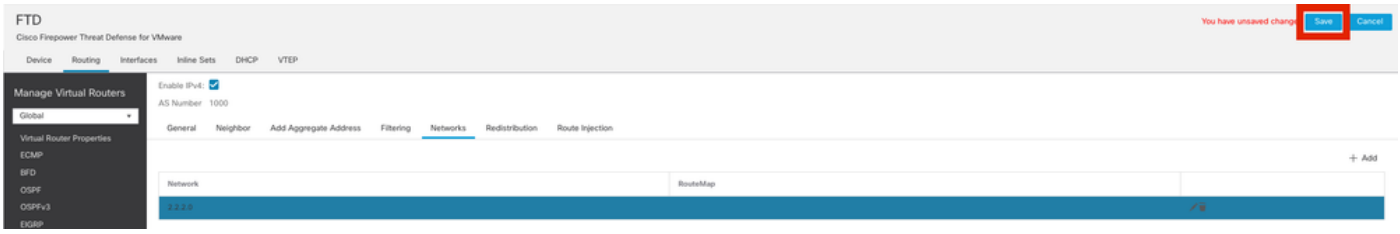
BGP 인접 디바이스 추가

4단계. 에서 Networks BGP를 통해 광고할 네트워크 중 VTI 터널을 통과해야 하는 네트워크를 추가합니다(이 경우 루프백1).



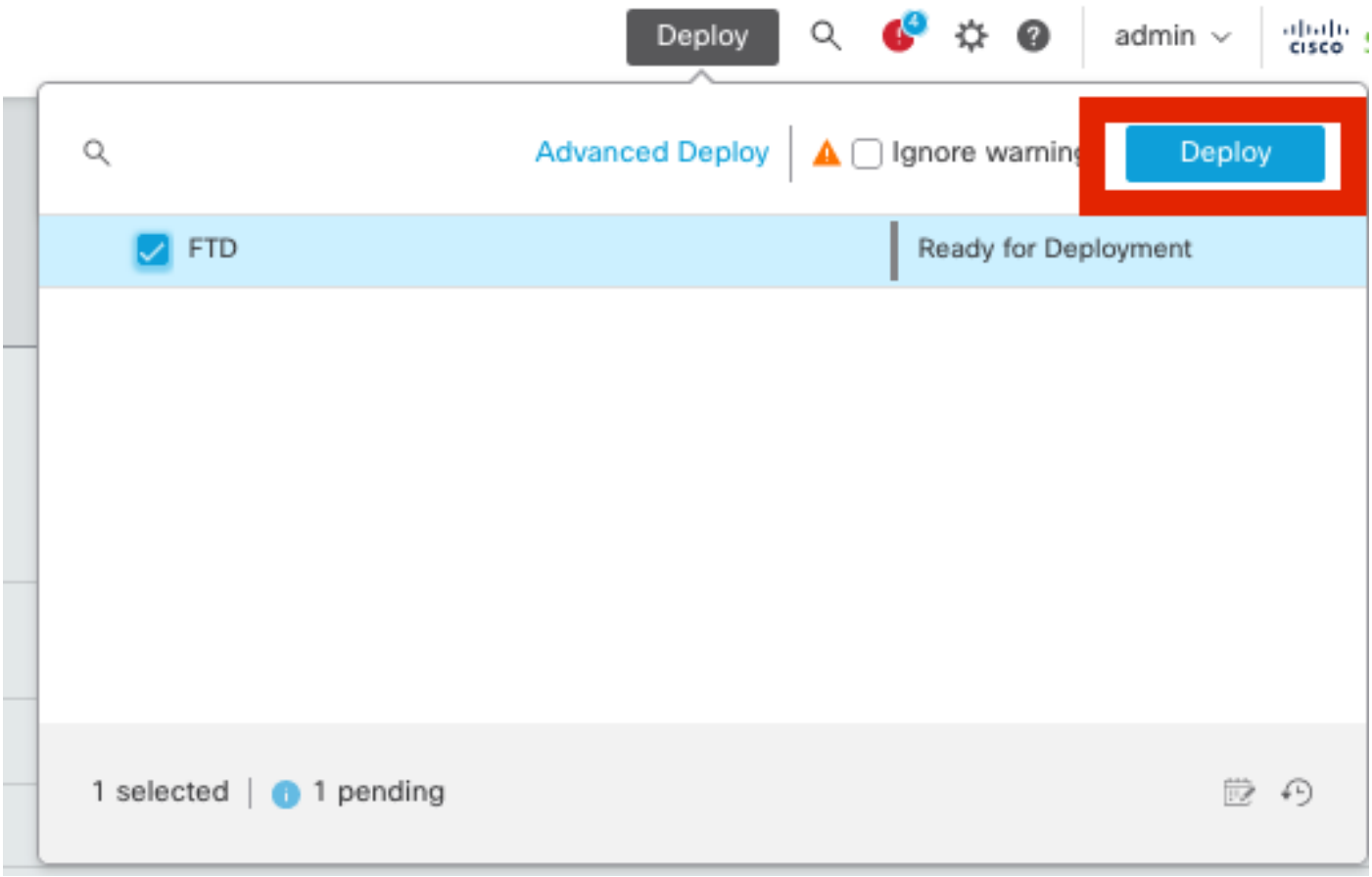
BGP 네트워크 추가

5단계. 다른 모든 BGP 설정은 선택 사항이며 환경에 따라 구성할 수 있습니다. 컨피그레이션을 확인하고 을 클릭합니다Save.



BGP 컨피그레이션 저장

6단계. 모든 컨피그레이션을 구축합니다.



구축

ASA에서 오버레이 BGP 구성

```
router bgp 1000
bgp log-neighbor-changes
bgp router-id 10.1.1.2
address-family ipv4 unicast
neighbor 169.254.2.1 remote-as 1000
neighbor 169.254.2.1 transport path-mtu-discovery disable
neighbor 169.254.2.1 activate
network 1.1.1.0 mask 255.255.255.0
no auto-summary
no synchronization
```

exit-address-family

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

FTD의 출력

<#root>

#show crypto ikev2 sa

```
IKEv2 SAs:
Session-id:20, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id         Local                  Remote                fvrf/ivrf          Status       Role
666846307      10.197.226.222/500      10.197.226.187/500    Global/Global      READY        RESPONDER
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/1201 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xa14edaf6/0x8540d49e
```

#show crypto ipsec sa

```
interface: ASAv-VTI
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 10.197.226.222

  Protected vrf (ivrf): Global
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer: 10.197.226.187

  #pkts encaps: 45, #pkts encrypt: 45, #pkts digest: 45
  #pkts decaps: 44, #pkts decrypt: 44, #pkts verify: 44
  #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
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 10.197.226.222/500, remote crypto endpt.: 10.197.226.187/500
  path mtu 1500, ipsec overhead 78(44), media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: 8540D49E
  current inbound spi : A14EDAF6

inbound esp sas:
 spi: 0xA14EDAF6 (2706299638)
  SA State: active
  transform: esp-aes-256 esp-sha-256-hmac no compression
  in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, }
  slot: 0, conn_id: 49, crypto-map: __vti-crypto-map-Tunnel1-0-1
  sa timing: remaining key lifetime (kB/sec): (4331517/27595)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
  000001FFF 0xFFFFFFFF
outbound esp sas:
 spi: 0x8540D49E (2235618462)
  SA State: active
  transform: esp-aes-256 esp-sha-256-hmac no compression
  in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, }
  slot: 0, conn_id: 49, crypto-map: __vti-crypto-map-Tunnel1-0-1
  sa timing: remaining key lifetime (kB/sec): (4101117/27595)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
  0x00000000 0x00000001
```

#show bgp summary

```
BGP router identifier 10.1.1.1, local AS number 1000
BGP table version is 5, main routing table version 5
2 network entries using 400 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 976 total bytes of memory
BGP activity 21/19 prefixes, 24/22 paths, scan interval 60 secs

Neighbor        V         AS      MsgRcvd      MsgSent       TblVer      InQ      OutQ      Up/Down
169.254.2.2     4       1000   22              22                  5            0         0
```

#show bgp neighbors

```
BGP neighbor is 169.254.2.2, vrf single_vf, remote AS 1000, internal link
   BGP version 4, remote router ID 10.1.1.2
   BGP state = Established, up for 00:19:49
   Last read 00:01:04, last write 00:00:38, hold time is 180, keepalive interval is 60 seconds
   Neighbor sessions:
      1 active, is not multisession capable (disabled)
   Neighbor capabilities:
      Route refresh: advertised and received(new)
      Four-octets ASN Capability: advertised and received
      Address family IPv4 Unicast: advertised and received
      Multisession Capability:
  Message statistics:
      InQ depth is 0
      OutQ depth is 0
                       Sent    Rcvd
Opens              1        1
Notifications:     0        0
Updates:           2        2
Keepalives:       19       19
Route Refresh: 0         0
Total:                22       22
Default minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast
   Session: 169.254.2.2
   BGP table version 5, neighbor version 5/0
   Output queue size : 0
   Index 15
  15 update-group member
                             Sent     Rcvd
Prefix activity:             ----     ----
Prefixes Current:            1          1         (Consumes 80 bytes)
Prefixes Total:              1          1
Implicit Withdraw:           0          0
Explicit Withdraw:           0          0
Used as bestpath:           n/a        1
Used as multipath:           n/a        0
                                Outbound           Inbound
Local Policy Denied Prefixes:   --------            -------
Bestpath from this peer:         1                          n/a
Invalid Path:                    1                          n/a
Total:                           2                            0
Number of NLRIs in the update sent: max 1, min 0

Address tracking is enabled, the RIB does have a route to 169.254.2.2
Connections established 7; dropped 6
Last reset 00:20:06, due to Peer closed the session of session 1
Transport(tcp) path-mtu-discovery is disabled
Graceful-Restart is disabled
```

#show route bgp

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
            D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
            N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
            E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
            i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
            ia - IS-IS inter area, * - candidate default, U - per-user static route
            o - ODR, P - periodic downloaded static route, + - replicated route
            SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.197.226.1 to network 0.0.0.0

B        1.1.1.0 255.255.255.0 [200/0] via 169.254.2.2, 00:19:55
```

ASA의 출력

<#root>

#show crypto ikev2 sa

```
IKEv2 SAs:

Session-id:7, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id    Local                    Remote                   fvrf/ivrf            Status
442126361    10.197.226.187/500       10.197.226.222/500       Global/Global         READY
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/1200 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x8540d49e/0xa14edaf6
```

#show crypto ipsec sa

```
interface: FTD-VTI
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 10.197.226.187
```

```
  Protected vrf (ivrf): Global
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
 current_peer: 10.197.226.222


 #pkts encaps: 44 #pkts encrypt: 44, #pkts digest: 44
 #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
 #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
 #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.197.226.187/500, remote crypto endpt.: 10.197.226.222/500
 path mtu 1500, ipsec overhead 78(44), media mtu 1500
 PMTU time remaining (sec): 0, DF policy: copy-df
 ICMP error validation: disabled, TFC packets: disabled
 current outbound spi: A14EDAF6
 current inbound spi : 8540D49E

inbound esp sas:
 spi: 0x8540D49E (2235618462)
     SA State: active
      transform: esp-aes-256 esp-sha-256-hmac no compression
      in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, }
     slot: 0, conn_id: 9, crypto-map: __vti-crypto-map-Tunnel1-0-1
     sa timing: remaining key lifetime (kB/sec): (4147198/27594)
     IV size: 16 bytes
     replay detection support: Y
    Anti replay bitmap:
    0x00000000 0x007FFFFF
outbound esp sas:
  spi: 0xA14EDAF6 (2706299638)
    SA State: active
    transform: esp-aes-256 esp-sha-256-hmac no compression
    in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, }
    slot: 0, conn_id: 9, crypto-map: __vti-crypto-map-Tunnel1-0-1
    sa timing: remaining key lifetime (kB/sec): (3916798/27594)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
    0x00000000 0x00000001
```

#show bgp summary

```
BGP router identifier 10.1.1.2, local AS number 1000
BGP table version is 7, main routing table version 7
2 network entries using 400 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
```

```
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 976 total bytes of memory
BGP activity 5/3 prefixes, 7/5 paths, scan interval 60 secs

Neighbor        V      AS      MsgRcvd      MsgSent     TblVer    InQ     OutQ     Up/Down     State/Pf
169.254.2.1   4     1000       22             22       7       0          0      00:19:42      1
```

#show bgp neighbors

```
BGP neighbor is 169.254.2.1, context single_vf, remote AS 1000, internal link
    BGP version 4, remote router ID 10.1.1.1
    BGP state = Established, up for 00:19:42
    Last read 00:01:04, last write 00:00:38, hold time is 180, keepalive interval is 60 seconds
    Neighbor sessions:
    1 active, is not multisession capable (disabled)
Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Multisession Capability:
Message statistics:
   InQ depth is 0
   OutQ depth is 0
                    Sent     Rcvd
Opens:              1         1
Notifications:    0         0
Updates:          2         2
Keepalives:      19       19
Route Refresh: 0         0
Total:              22       22
Default minimum time between advertisement runs is 0 seconds
For address family: IPv4 Unicast
  Session: 169.254.2.1
  BGP table version 7, neighbor version 7/0
  Output queue size : 0

  Index 5
  5 update-group member
                     Sent      Rcvd
Prefix activity:     ----   ----
Prefixes Current:    1         1 (Consumes 80 bytes)
Prefixes Total:      1         1
Implicit Withdraw:   0         0
Explicit Withdraw:   0         0
Used as bestpath:  n/a       1
Used as multipath:  n/a       0

                                  Outbound        Inbound
Local Policy Denied Prefixes:     --------        -------
Bestpath from this peer:           1              n/a
Invalid Path:                      1              n/a
Total:                             2              0
Number of NLRIs in the update sent: max 1, min 0
```

```
Address tracking is enabled, the RIB does have a route to 169.254.2.1
Connections established 5; dropped 4
Last reset 00:20:06, due to Peer closed the session of session 1
Transport(tcp) path-mtu-discovery is disabled
Graceful-Restart is disabled
```

#show route bgp

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
           D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
           i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
           ia - IS-IS inter area, * - candidate default, U - per-user static route
           o - ODR, P - periodic downloaded static route, + - replicated route
           SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.197.226.1 to network 0.0.0.0

B       2.2.2.0 255.255.255.0 [200/0] via 169.254.2.1, 00:19:55
```

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug ip bgp all

- IPv4 인터페이스뿐 아니라 IPv4, 보호 네트워크 또는 VPN 페이로드만 지원합니다(IPv6는 지원되지 않음).

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.