BGPをオーバーレイとして使用したASAとFTD間のルートベースのサイト間VPNの設定

内容

はじめに

このドキュメントでは、ダイナミックルーティングのBorder Gateway Protocol(BGP)をオーバーレイとして使用するFirepower Management Center(FMC)によって、適応型セキュリティアプライアンス(ASA)とFirepower Threat Defense managed(FTD)の間にルートベースのサイト間VPN(IPSec)トンネルを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- IPSecサイト間VPNの基本的な知識
- FTDおよびASAでのBGPの設定
- FMCの使用経験

使用するコンポーネント

- Cisco ASAvバージョン9.20(2)2
- Cisco FMCバージョン7.4.1
- Cisco FTDバージョン7.4.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

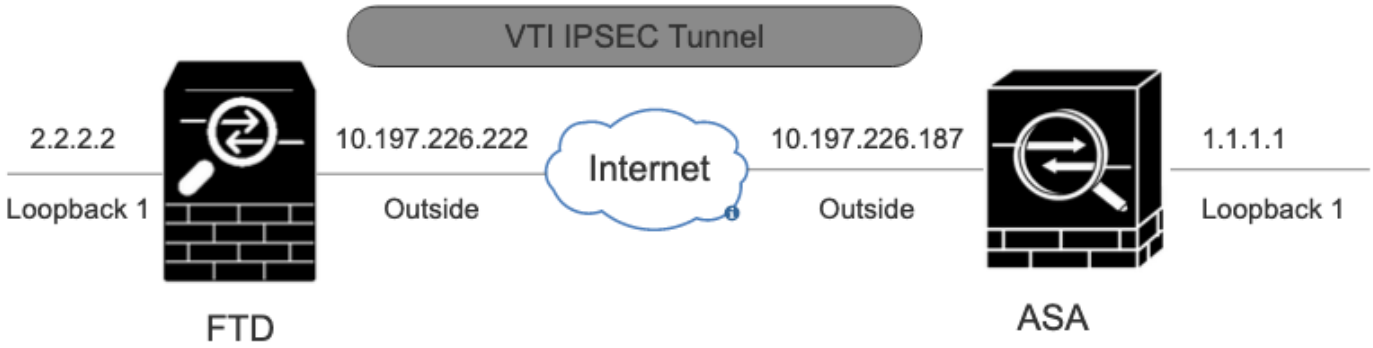
ルートベースのVPNでは、暗号化するトラフィック、またはVPNトンネルを介して送信するトラフィックを判別できます。また、ポリシーベースまたは暗号マップベースのVPNのように、ポリシー/アクセスリストの代わりにトラフィックルーティングを使用します。 暗号化ドメインは、IPsecトンネルに入るすべてのトラフィックを許可するように設定されます。IPsecローカルおよびリモートトラフィックセレクタは0.0.0.0/0.0.0.0に設定されます。IPSecトンネルにルーティングされるトラフィックは、送信元/宛先サブネットに関係なく暗号化されます。

このドキュメントでは、ダイナミックルーティングBGPをオーバーレイとして使用したスタティック仮想トンネルインターフェイス(SVTI)の設定を中心に説明します。

設定

このセクションでは、SVTI IPSecトンネルを介してBGPネイバーシップを起動するためにASAおよびFTDで必要な設定について説明します。

ネットワーク図



ネットワーク図

コンフィギュレーション

FMCを使用したFTDでのIPSec VPNの設定

ステップ 1：Devices > VPN > Site To Siteに移動します。

ステップ 2：+Site to Site VPNをクリックします。

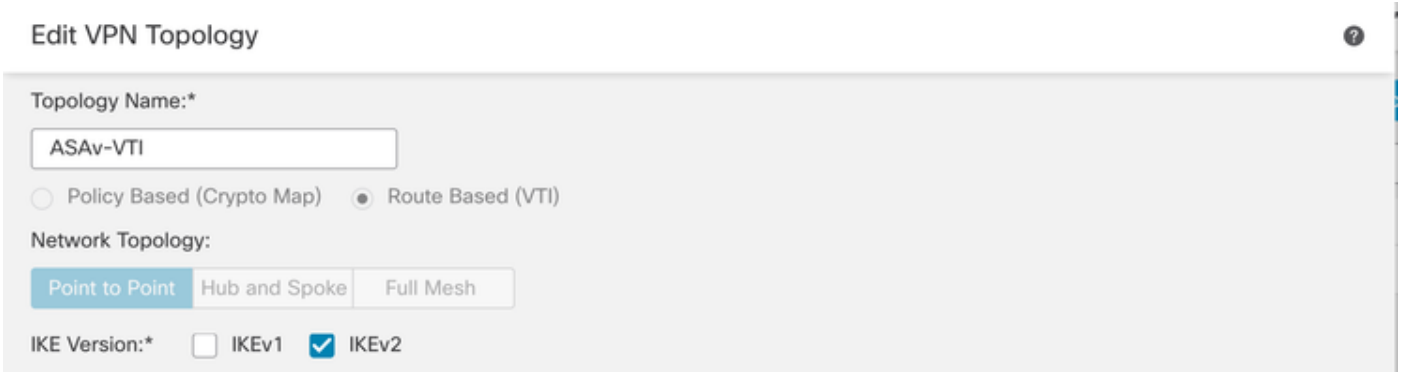
サイト間 *VPN*

ステップ 3：Topology Nameを入力し、VPNのタイプとしてRoute Based (VTI)を選択します。IKE Versionを選択します。

このデモンストレーションでは、次の操作を行います。

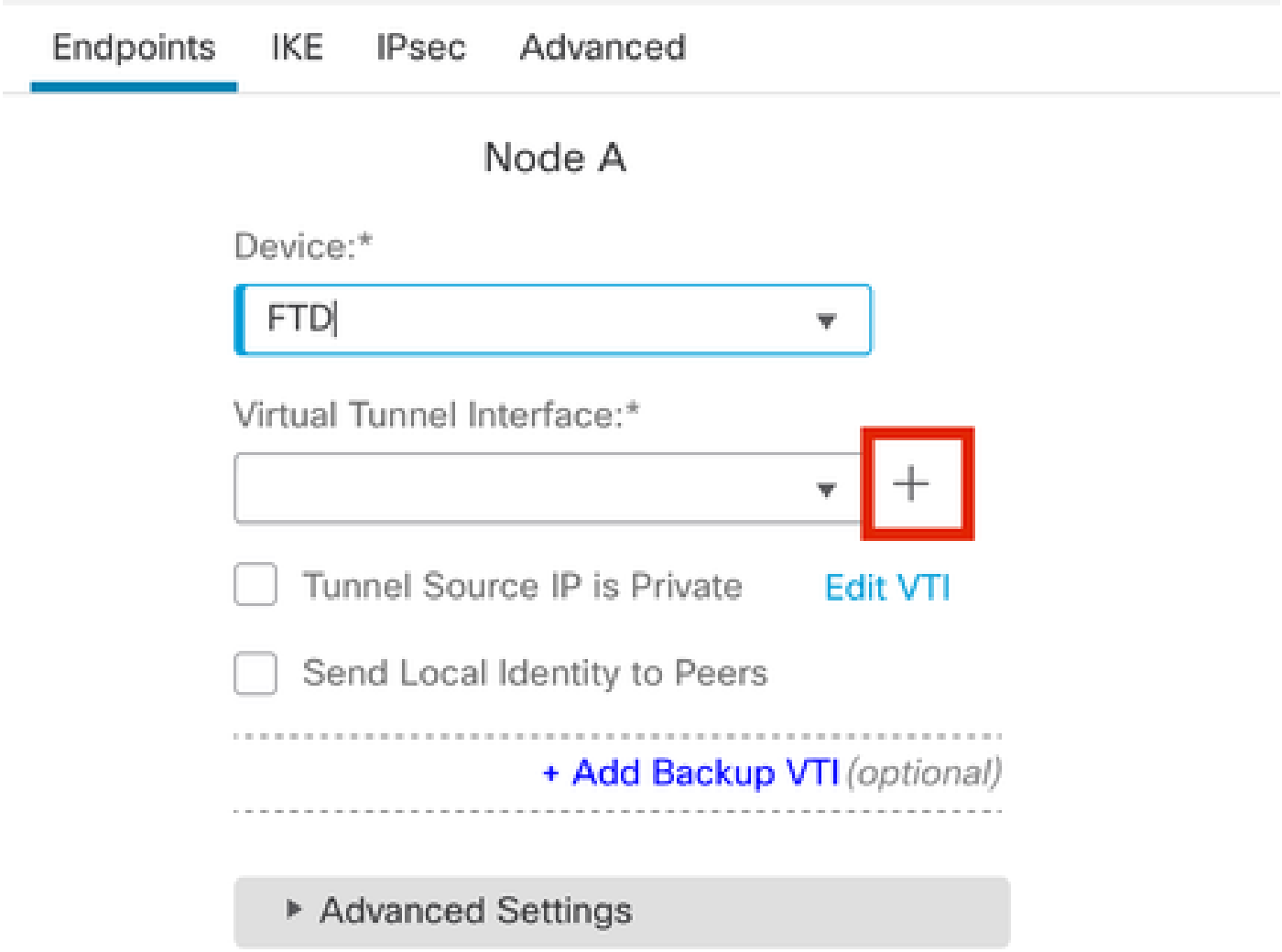
トポロジ名：ASAv-VTI

IKEバージョン：IKEv2



*VPN*トポロジ

ステップ 4：トンネルを設定する必要があるDeviceを選択します。新しい仮想トンネルインターフェイスを追加するか(+アイコンをクリック)、既存のリストから選択します。



エンドポイントノードA

ステップ 5：New Virtual Tunnel Interfaceのパラメータを定義します。をクリックします。Ok

このデモンストレーションでは、次の操作を行います。

名前：ASA-VTI

説明（オプション）：エクストラネットASAを使用したVTIトンネル

セキュリティゾーン：VTIゾーン

トンネルID:1

IPアドレス：169.254.2.1/24

トンネル送信元：GigabitEthernet0/1（外部）

IPsecトンネルモード：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:*

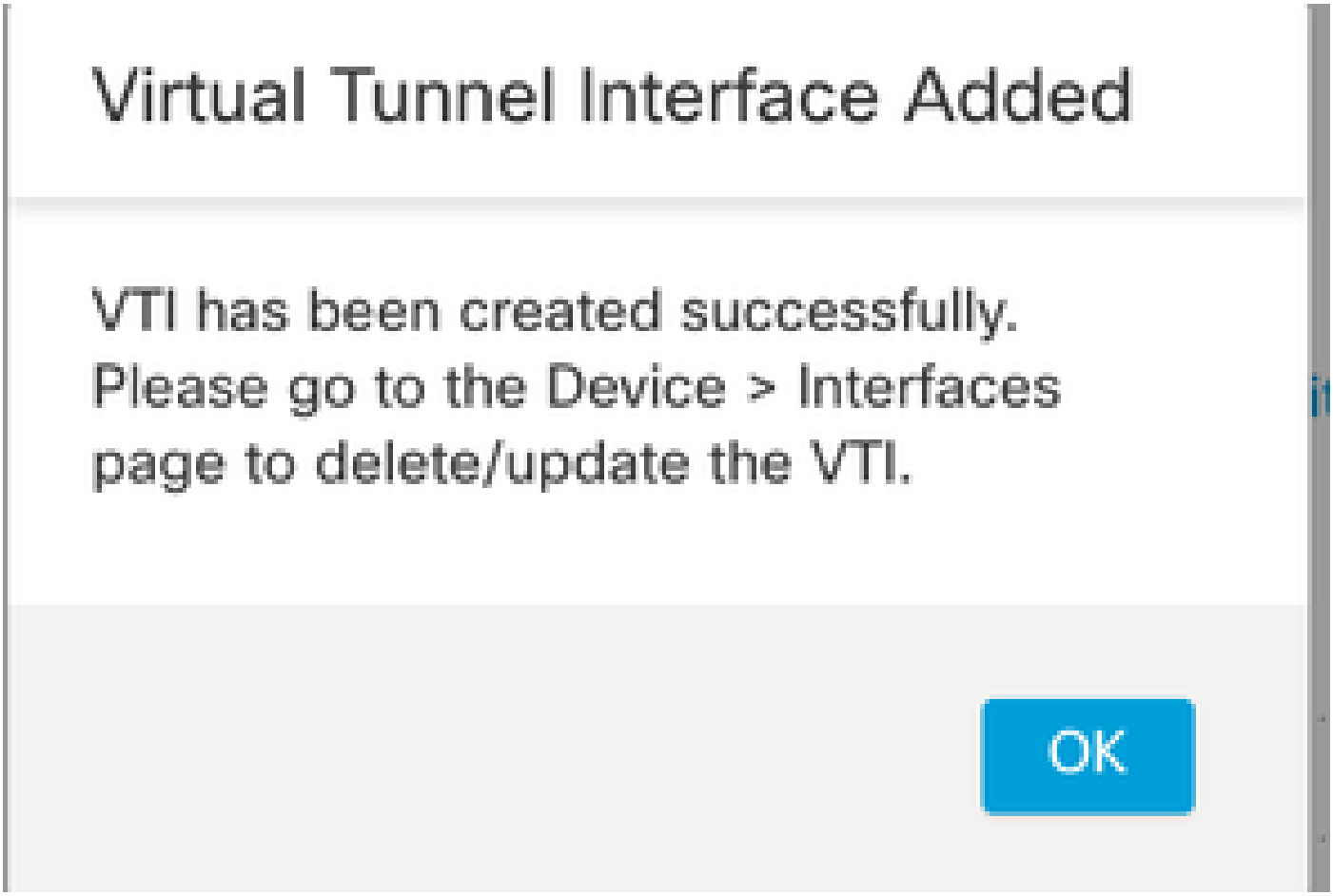
(•) Configure IP 169.254.2.1/24

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

Cancel OK

仮想トンネルインターフェイス

手順 6：新しいVTIが作成されたことを示すポップアップをクリックOK。



仮想トンネルインターフェイスの追加

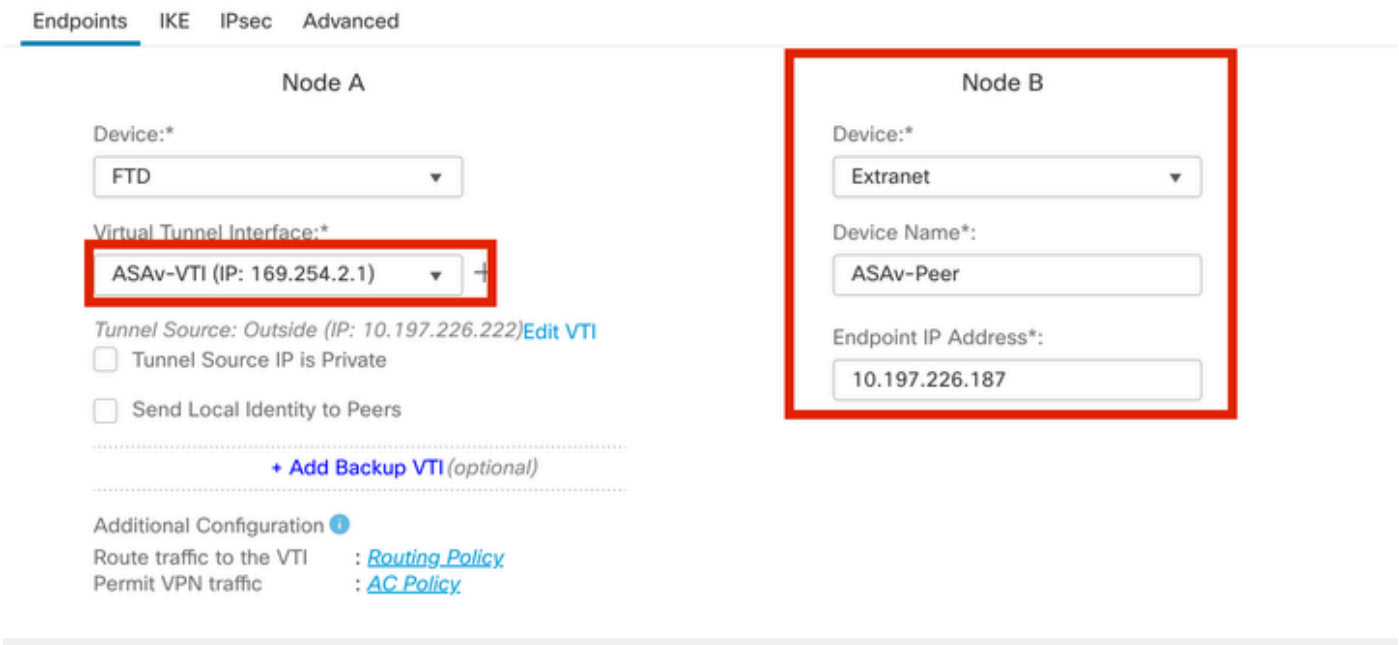
手順 7：新しく作成したVTIまたはVirtual Tunnel Interfaceの下のVTIを選択します。ノードB（ピアデバイス）の情報を入力します。

このデモンストレーションでは、次の操作を行います。

デバイス：エクストラネット

デバイス名：ASAv-Peer

エンドポイントIPアドレス：10.197.226.187



エンドポイントノード*B*

ステップ 8：**IKE**タブに移動します。

をクリックします。定義済みのPolicyを使用するか、Policyタブの横にあるボタ+ンをクリックして新しいタブを作成するかを選択できます。

ステップ9:（新しいIKEv2ポリシーを作成する場合はオプション）ポリシーにNameを指定し、ポリシーで使用するAlgorithmsを選択します。をクリックします。Save

このデモンストレーションでは、次の操作を行います。

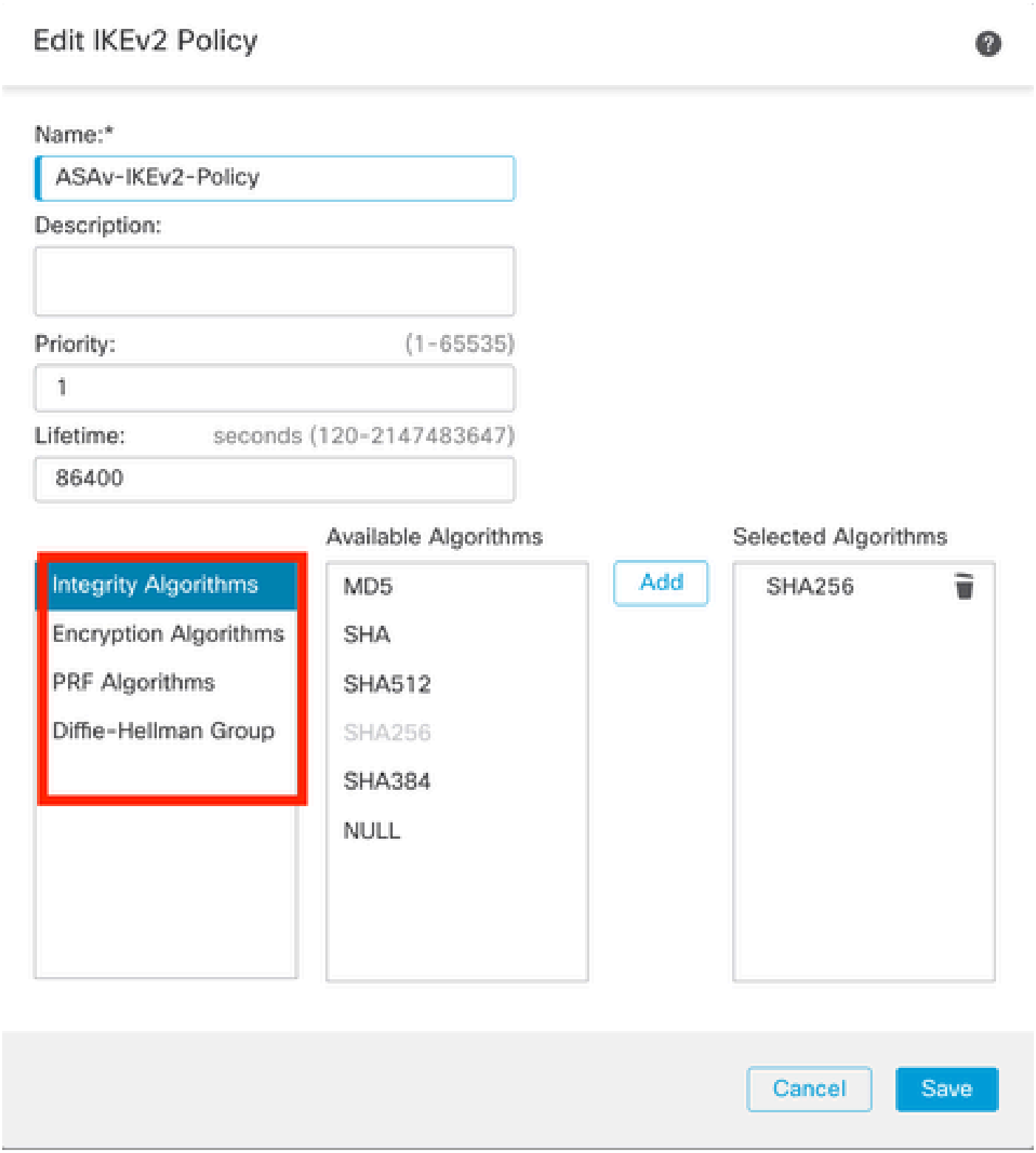
名前：ASAv-IKEv2-policy

整合性アルゴリズム：SHA-256

暗号化アルゴリズム：AES-256

PRFアルゴリズム：SHA-256

Diffie-Hellmanグループ：14



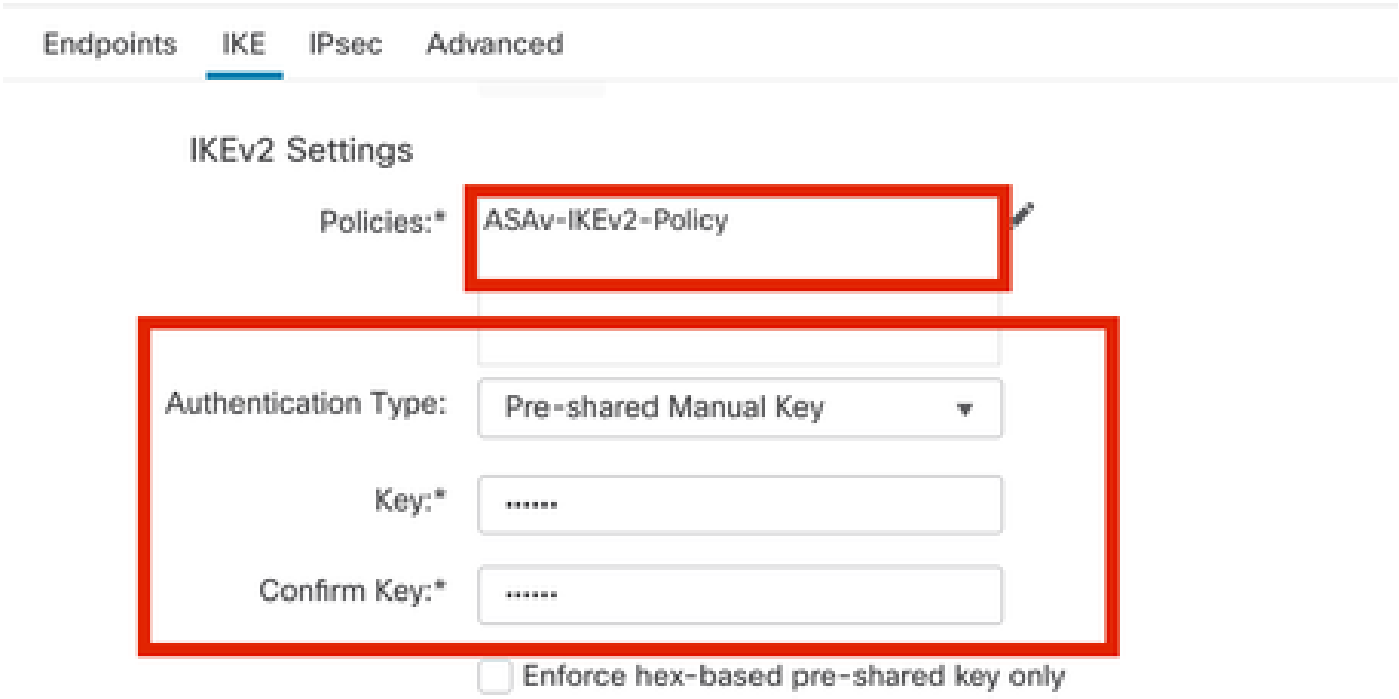
*IKEv2*ポリシー

ステップ 10：新しく作成したPolicyまたは既存のPolicyを選択します。Authentication Typeを選択します。事前共有手動キーを使用する場合は、KeyおよびConfirm Key ボックスにキーを入力します。

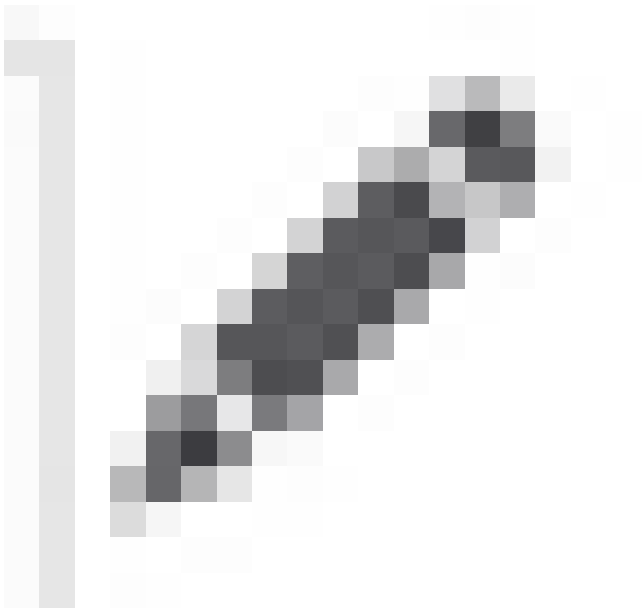
このデモンストレーションでは、次の操作を行います。

ポリシー：ASAv-IKEv2-Policy

認証タイプ：事前共有手動キー



[Authentication]



ステップ 11IPsec タブに移動します。

をクリックすると、事前定義されたIKEv2 IPsecプロポーザルを使用するか、新しいプロポーザルを作成するかを選択できます。タ IKEv2 IPsec Proposal ブの横にある+ボタンをクリックします。

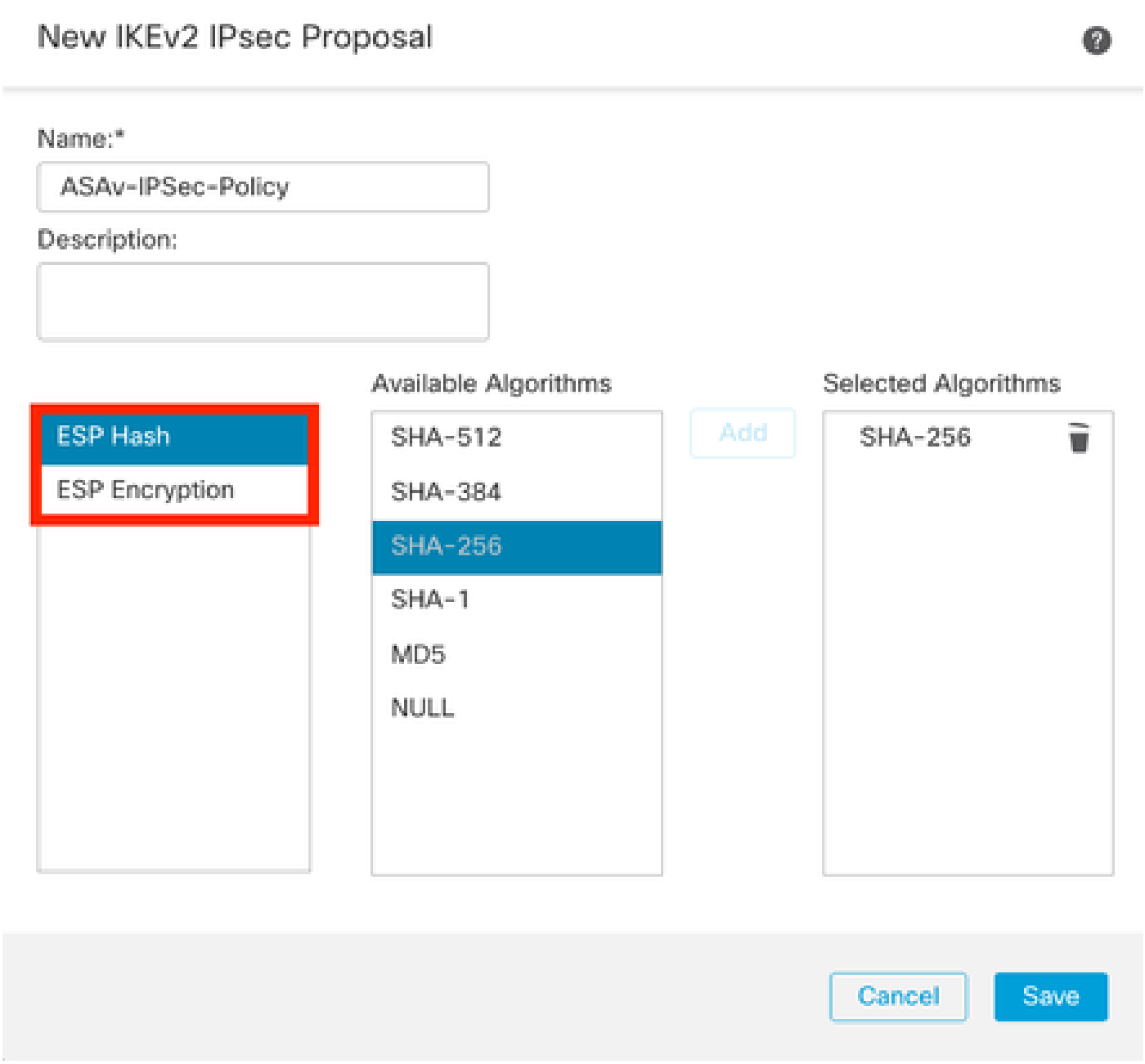
ステップ12. (新しいIKEv2 IPsecプロポーザルを作成する場合はオプション) 提案のNameを入力し、提案で使用するAlgorithmsを選択します。をクリックします。Save

このデモンストレーションでは、次の操作を行います。

名前：ASAv-IPSec-Policy

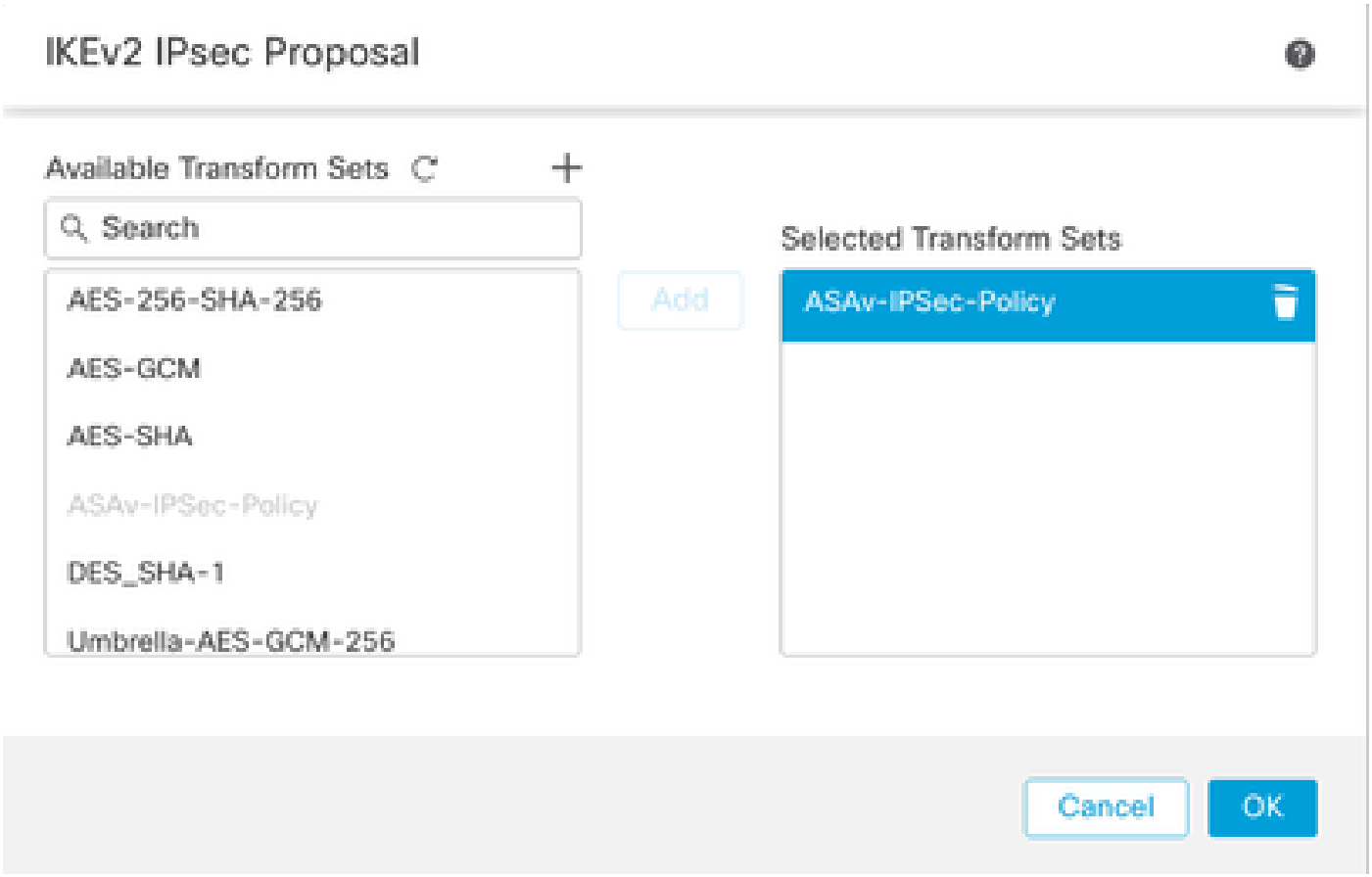
ESPハッシュ：SHA-256

ESP暗号化：AES-256



IKEv2-IPsec – プロポーザル

ステップ 13 使用可能なプロポーザルのリストから、新しく作成したProposalまたは既存のプロポーザルProposalを選択します。をクリックします。OK



変換セット

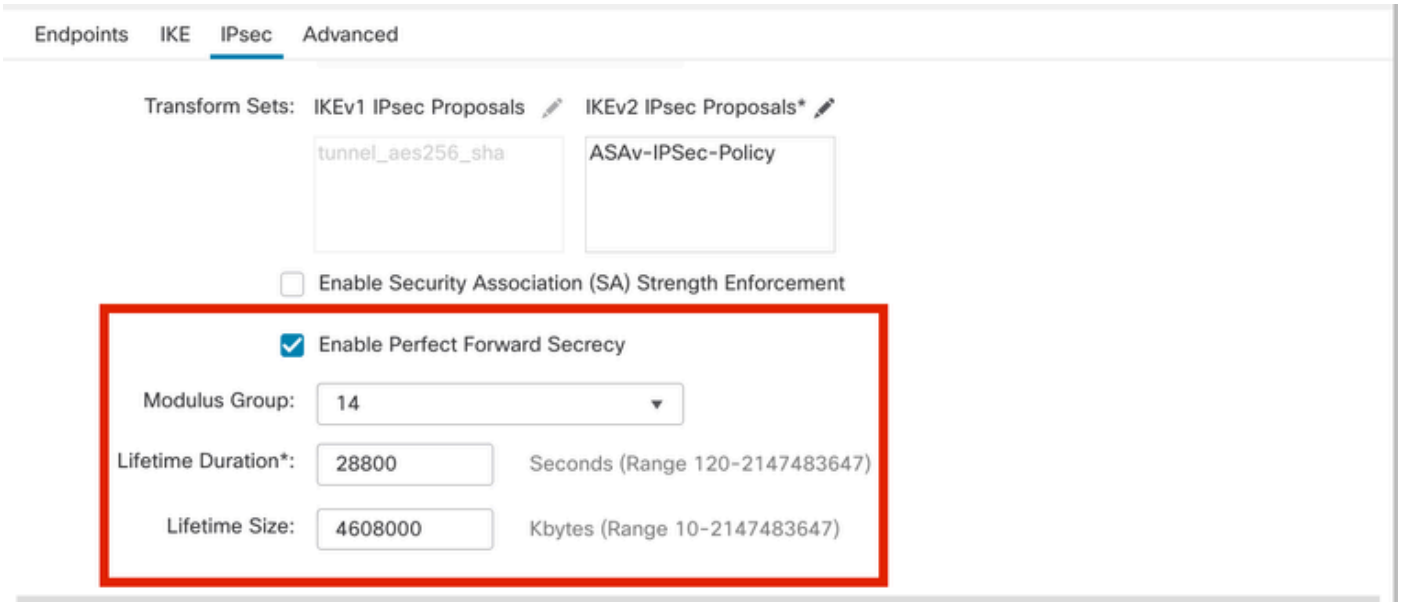
ステップ14: (オプション) Perfect Forward Secrecyの設定を選択します。IPSecの設定Lifetime Duration and Lifetime Size

このデモンストレーションでは、次の操作を行います。

完全転送秘密：モジュラスグループ14

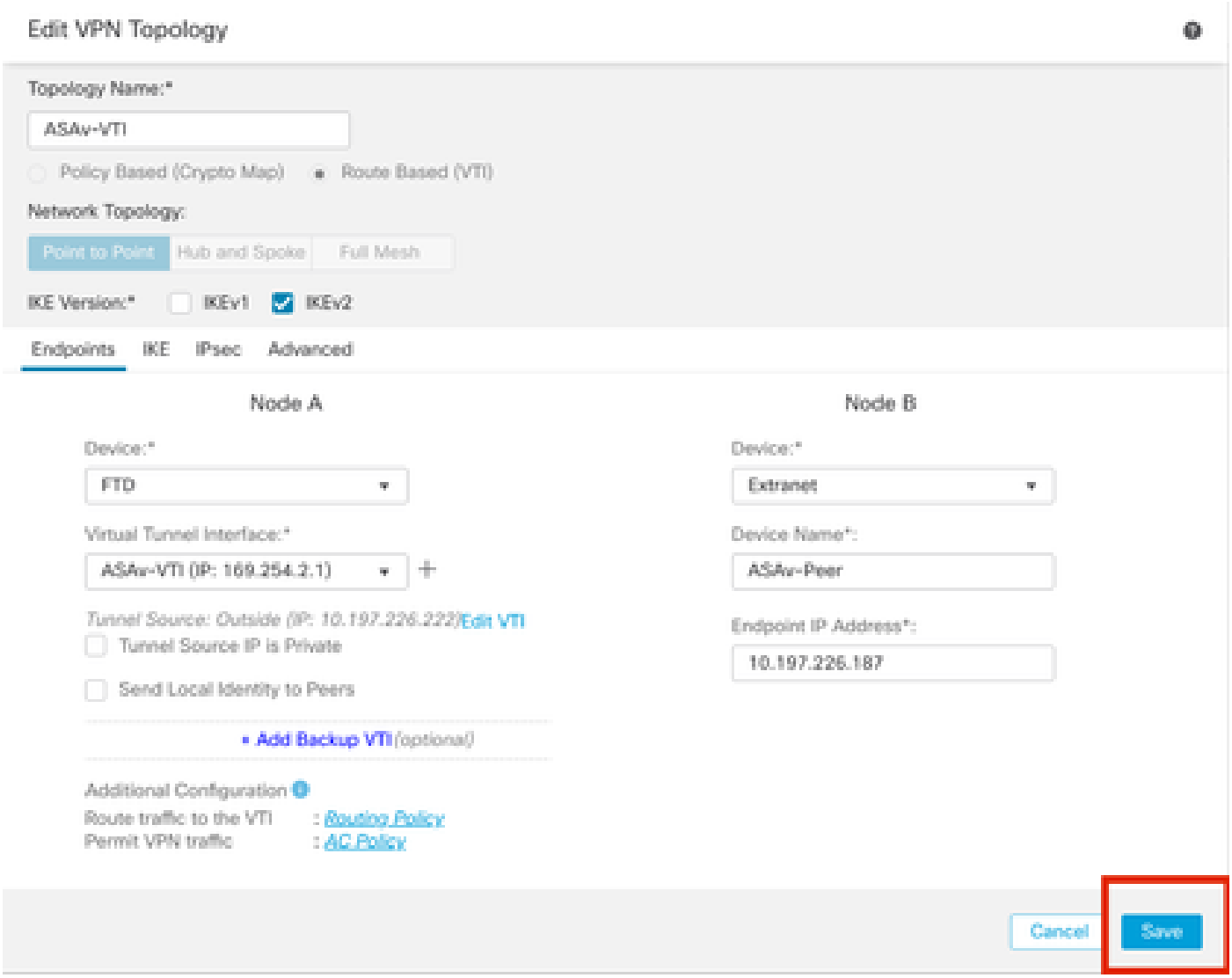
有効期間： 28800 (既定値)

Lifetime Size (ライフタイムサイズ) :4608000 (デフォルト)



*PFS*の設定

ステップ 15：設定を確認します。次の図に示すように、Saveをクリックします。



設定を保存します。

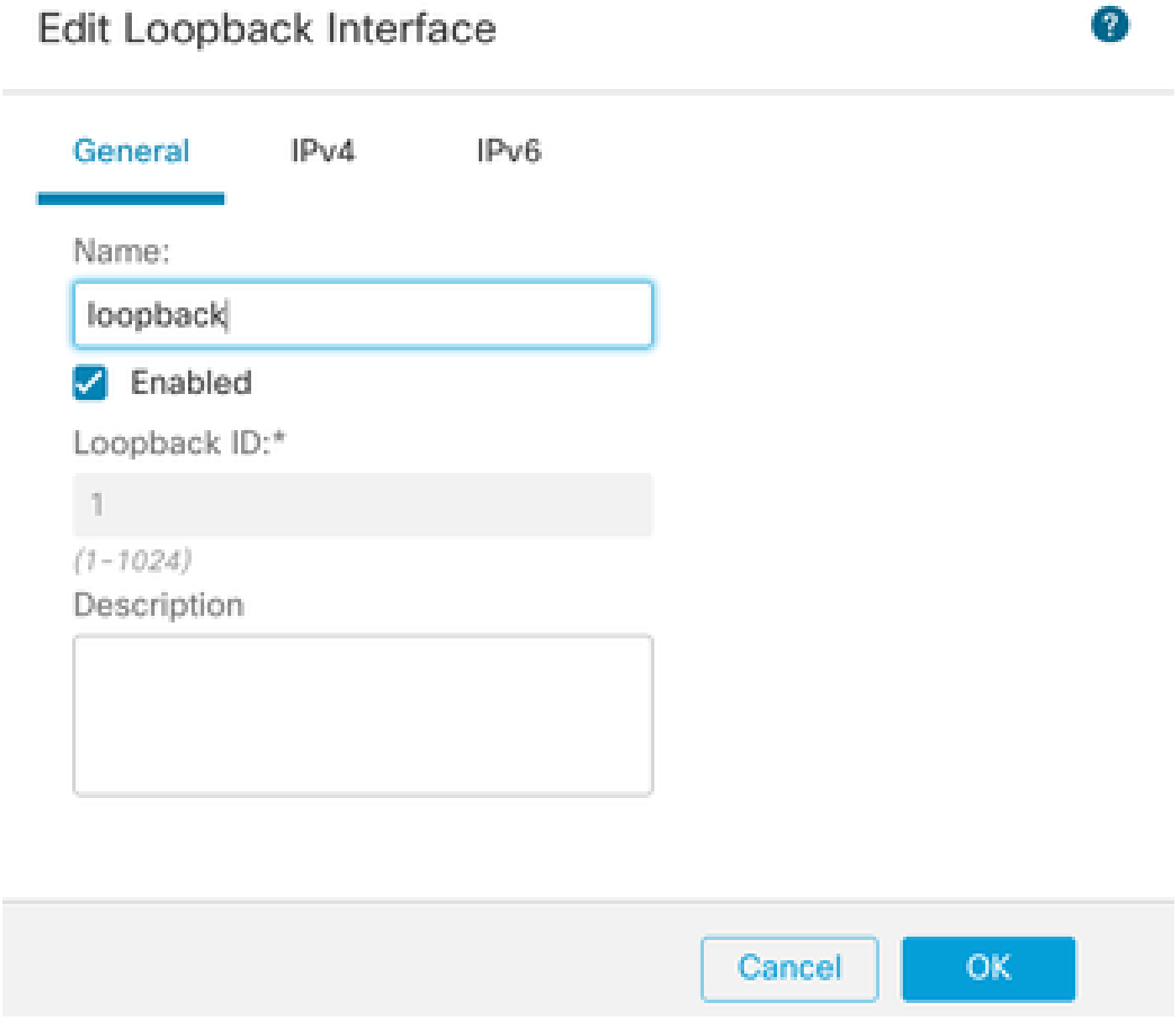
FMCを使用したFTDのループバックインターフェイスの設定

Devices > Device Managementに移動します。ループバックを設定する必要があるデバイスを編集します。

ステップ 1：次に.Interfaces > Add Interfaces > Loopback Interface

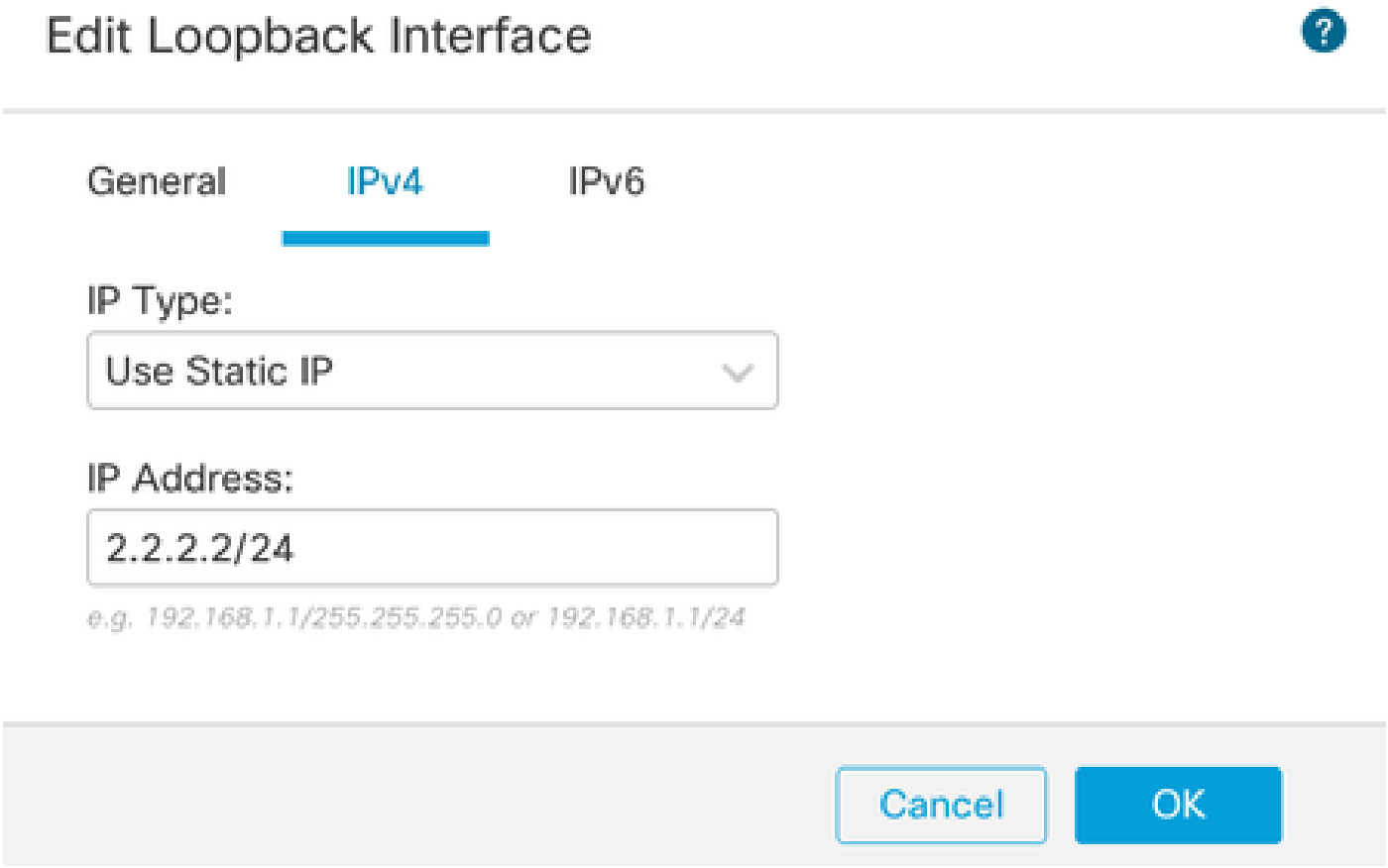
ループバックインターフェイスに移動します

ステップ 2：「loopback」という名前を入力し、ループバックID「1」を指定して、インターフェイスを有効にします。



ループバックインターフェイスの有効化

ステップ 3：インターフェイスのIPアドレスを設定し、OK をクリックします。



ループバックインターフェイスにIPアドレスを提供する

ASAでのIPSec VPNの設定

```
!--- 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
```

ASAでのループバックインターフェイスの設定

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

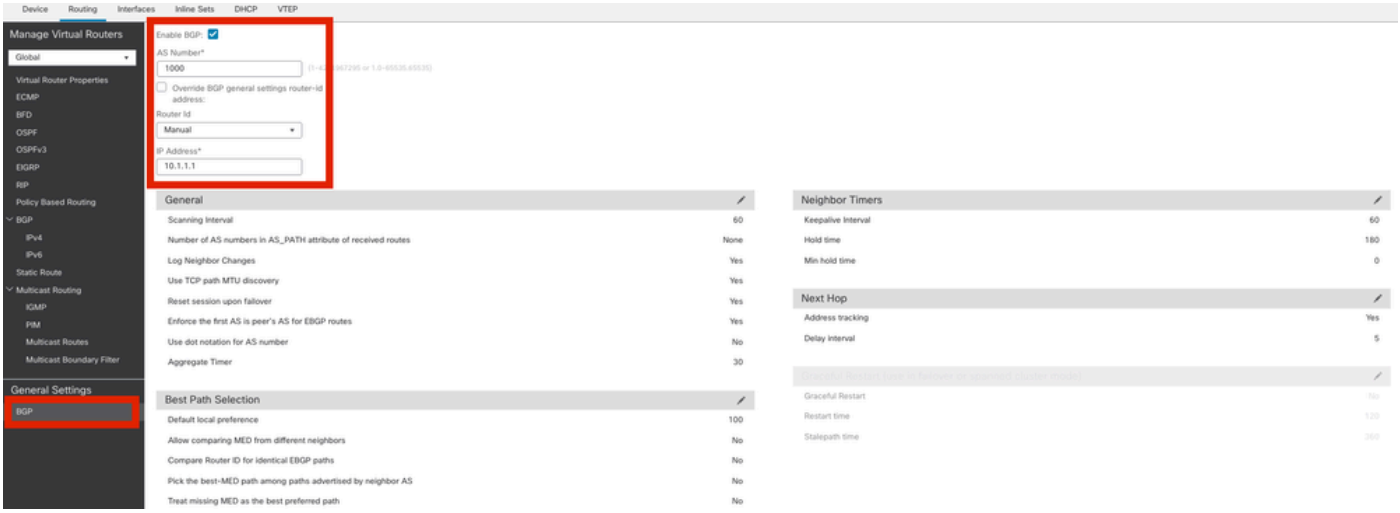
FMCを使用したFTDでのオーバーレイBGPの設定

Devices > Device Management.Edit VTIトンネルが設定されているデバイスに移動し、Routing >General Settings > BGPに移動します。

ステップ 1：BGPを有効にして、自律システム(AS)番号とルータIDを設定します（次の図を参照）。

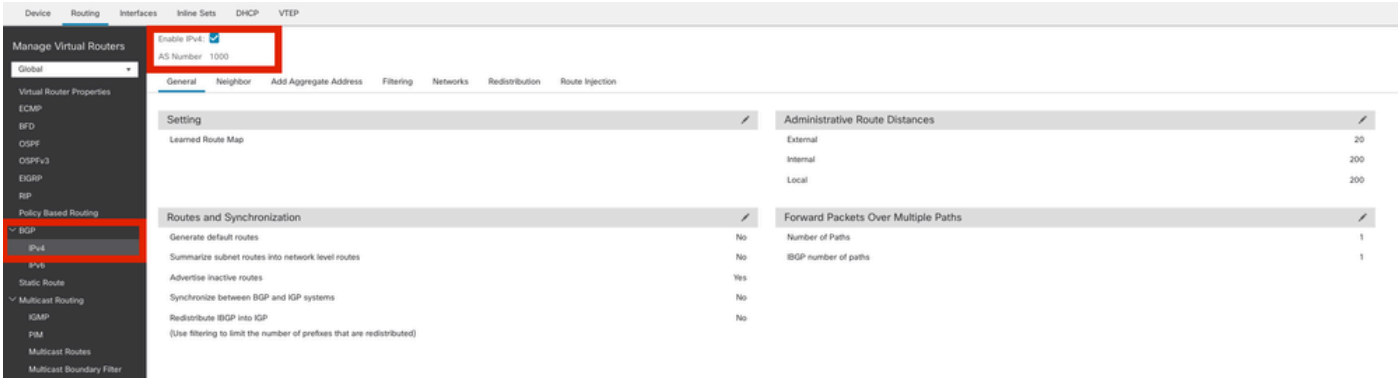
AS番号は、デバイスFTDとASAの両方で同じである必要があります。

ルータIDは、BGPに参加している各ルータを識別するために使用されます。



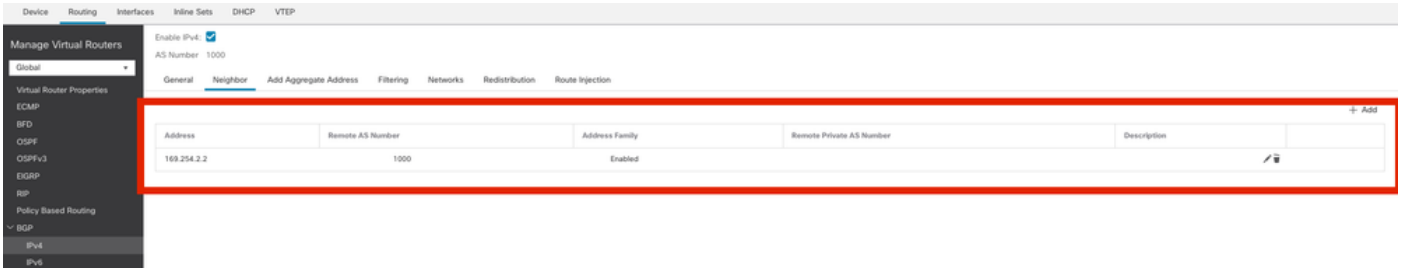
*BGP*を設定します

ステップ 2：FTDでBGP > IPv4に移動し、BGP IPv4を有効にします。



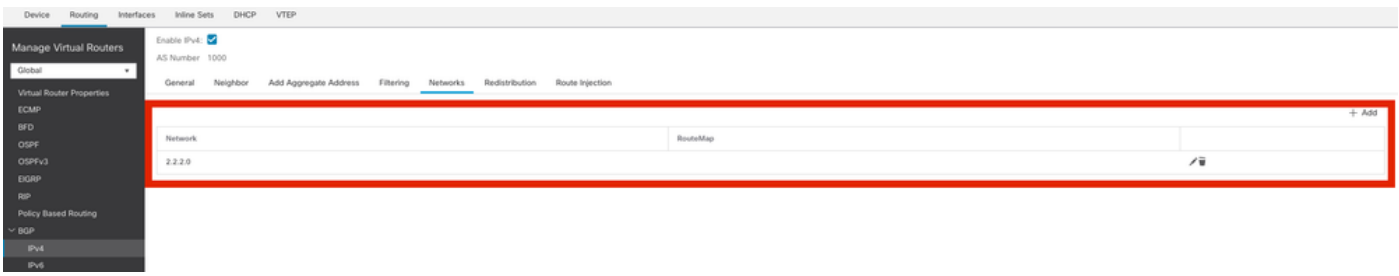
*BGP*の有効化

ステップ 3：タブでNeighbor、ASAv VTIトンネルIPアドレスをネイバーとして追加し、ネイバーを有効にします。



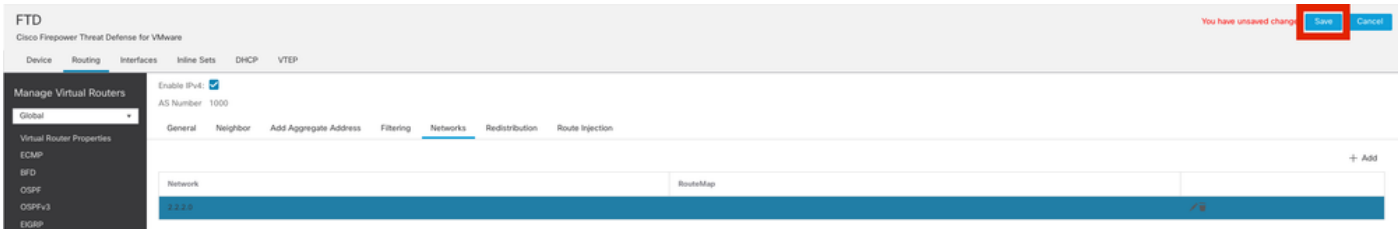
*BGP*ネイバーの追加

ステップ 4：Networksで、BGPを通じてアドバタイズするネットワークのうち、VTIトンネルを通過する必要があるネットワーク（この場合はloopback1）を追加します。



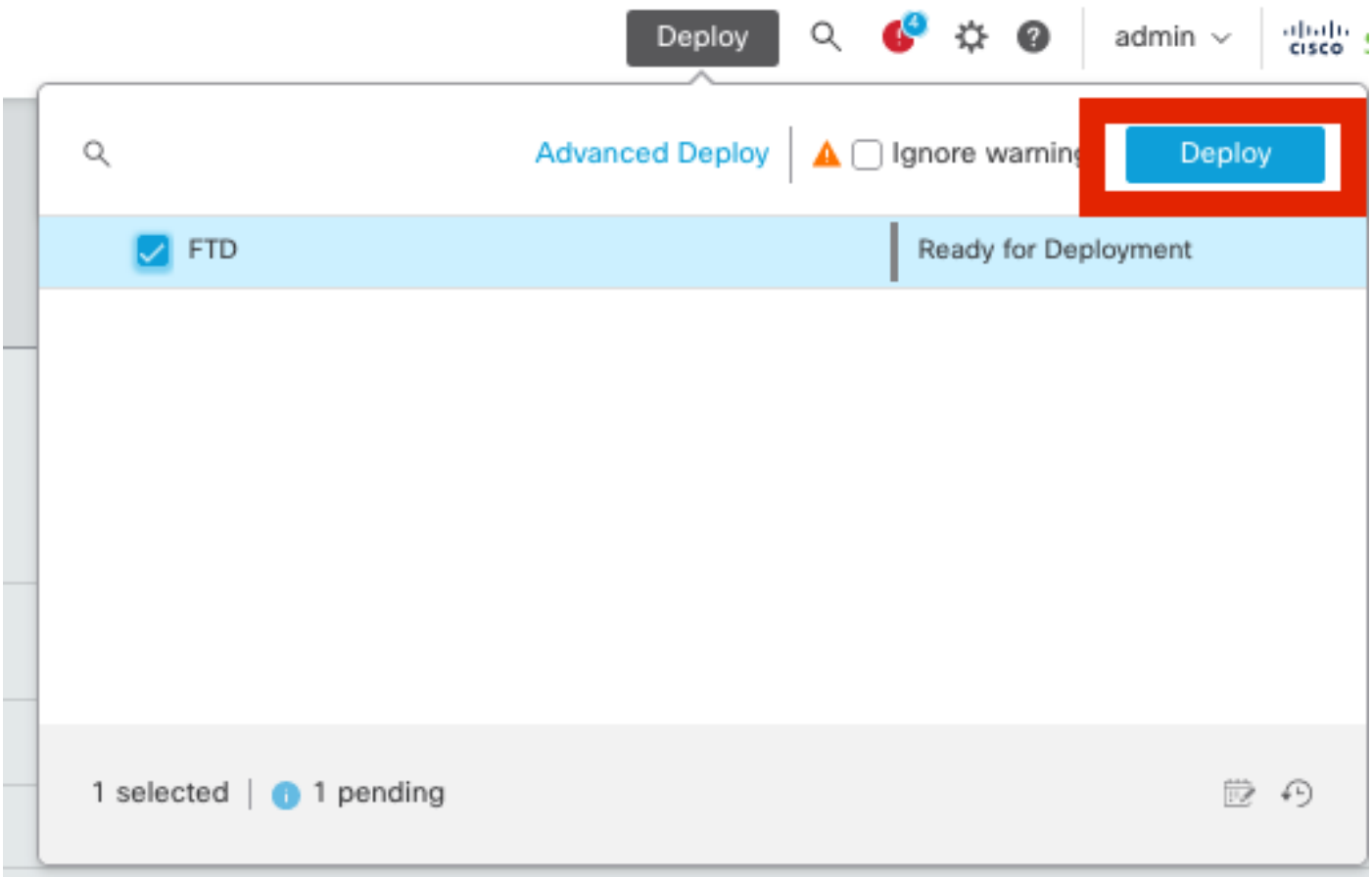
*BGP*ネットワークの追加

ステップ 5：その他すべてのBGP設定はオプションであり、環境に応じて設定できます。設定を確認して、Saveをクリックします。



*BGP*設定の保存

手順 6：すべての設定を展開します。



導入

ASAでのオーバーレイBGPの設定

```
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

確認

ここでは、設定が正常に機能しているかどうかを確認します。

FTDの出力

<#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
```

ASAでの出力

<#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
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

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

- IPv4インターフェイスとIPv4、保護されたネットワーク、またはVPNペイロードのみをサポート（IPv6はサポートされない）。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。