ASAとFTD間のIKEv2 IPv6サイト間トンネルの設定

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[設定](#)
[ネットワーク図](#)
[ASA の設定](#)
[FTD の設定](#)
[アクセスコントロールのバイパス](#)
[NAT免除の設定](#)
[確認](#)
[トラブルシュート](#)
[参考資料](#)

概要

このドキュメントでは、インターネットキーエクスチェンジバージョン2(IKEv2)プロトコルを使用して、ASA（適応型セキュリティアプライアンス）とFTD(Firepower Threat Defense)間のIPv6サイト間トンネルを設定する設定例を紹介します。セットアップには、ASAとFTDをVPN終端デバイスとして使用したエンドツーエンドのIPv6ネットワーク接続が含まれます。

前提条件

要件

次の項目に関する知識があることを推奨します。

- ASA CLI設定に関する基礎知識
- IKEv2およびIPSECプロトコルに関する基礎知識
- IPv6アドレッシングとルーティングの理解
- FMCによるFTD設定の基本的な理解

使用するコンポーネント

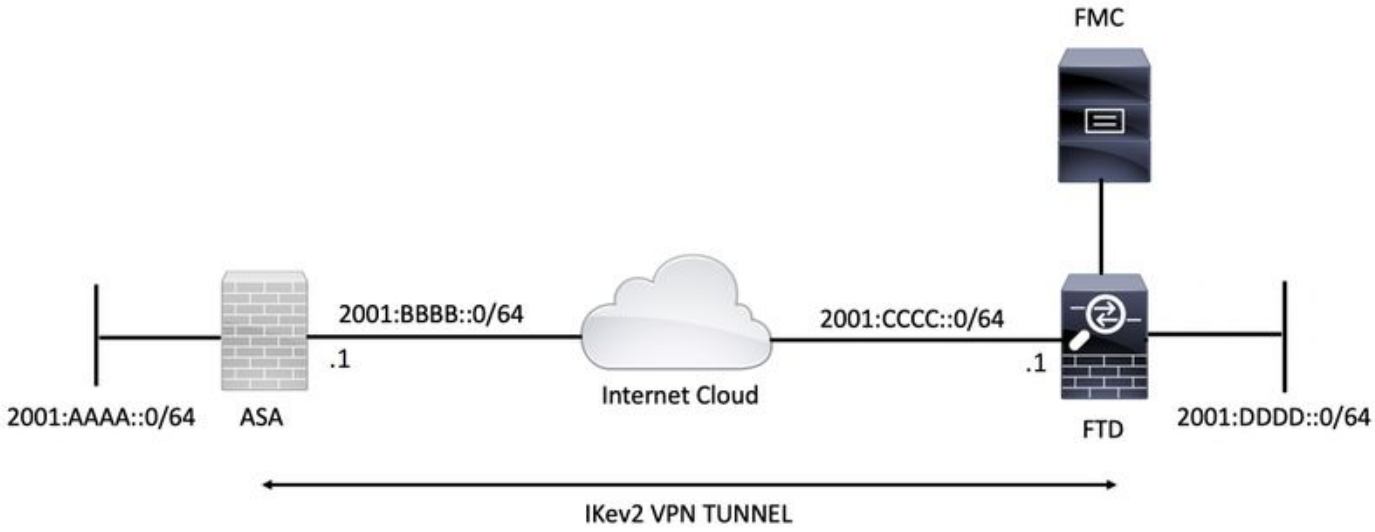
このドキュメントの情報は、特定のラボ設定のデバイスから作成された仮想環境に基づいています。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。ネットワークが稼働中である場合は、コマンドの潜在的な影響について理解しておく必要があります。

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 9.6.(4)12を実行するCisco ASAv
- 6.5.0を実行するCisco FTDv
- 6.6.0を実行するCisco FMCv

設定

ネットワーク図



ASA の設定

このセクションでは、ASAで必要な設定について説明します。

ステップ1:ASAインターフェイスを設定します。

```
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
```

ステップ2:IPv6デフォルトルートを設定します。

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

手順3:IKEv2ポリシーを設定し、外部インターフェイスでIKEv2を有効にします。

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

crypto ikev2 enable outside
```

ステップ4：トンネルグループを設定します。

```
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
```

ステップ5：対象トラフィックに一致するオブジェクトとアクセスコントロールリスト(ACL)を作成します。

```
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
```

ステップ6：対象トラフィックのIDネットワークアドレス変換(NAT)ルールを設定します。

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

ステップ7:IKEv2 IPSecプロポーザルを設定します。

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

ステップ8：暗号マップを設定し、外部インターフェイスに適用します。

```
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 の設定

このセクションでは、FMCを使用してFTDを設定する手順について説明します。

VPNトポロジの定義

1:[Devices] > [**VPN] > [Site To Site]**

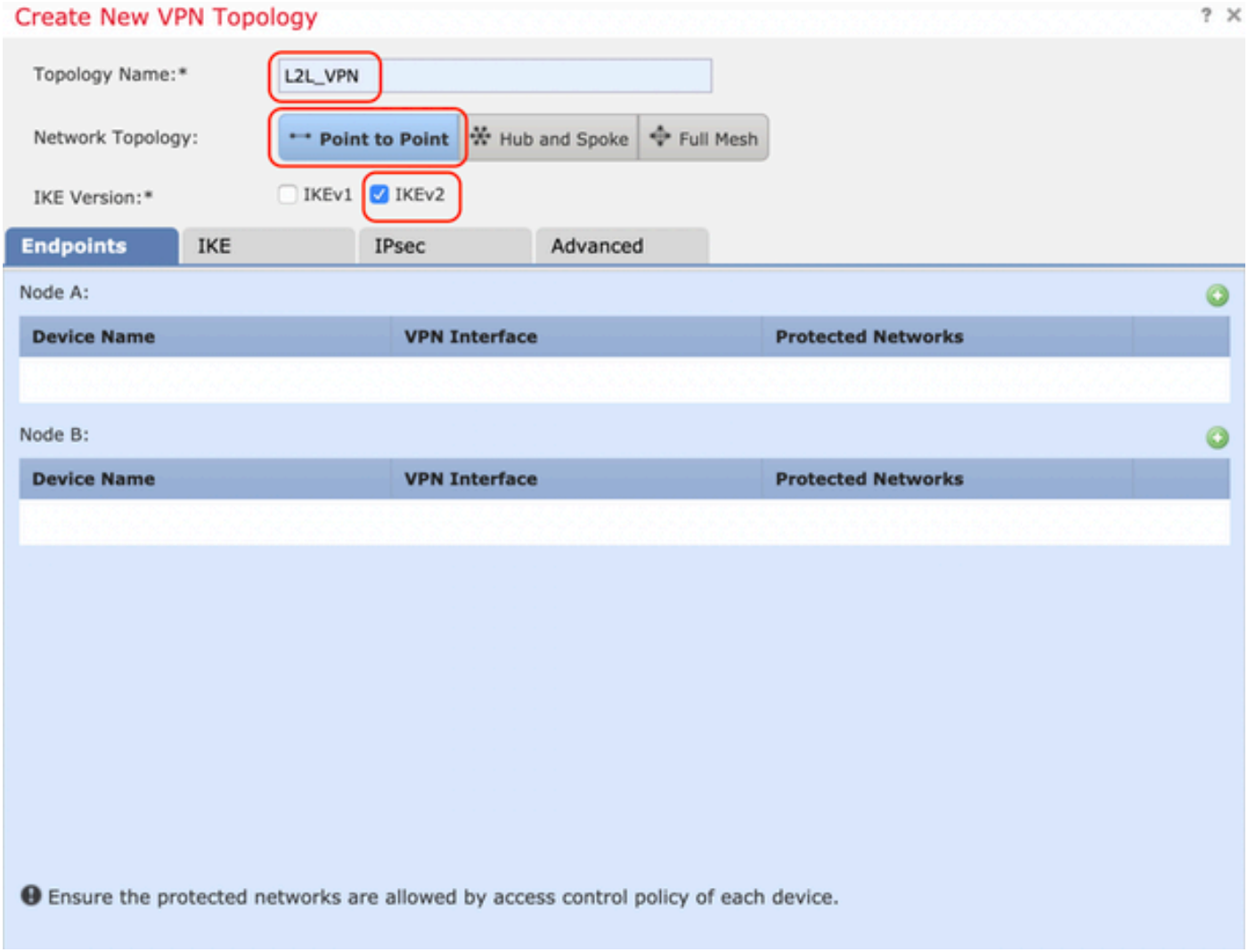
[Add VPN][Firepower Threat Defense Device]

ステップ2:[Create New VPN Topology]ボックスが表示されます。VPNに簡単に識別できる名前を付けます。

Network Topology:ポイントツーポイント

IKEバージョン：IKEv2

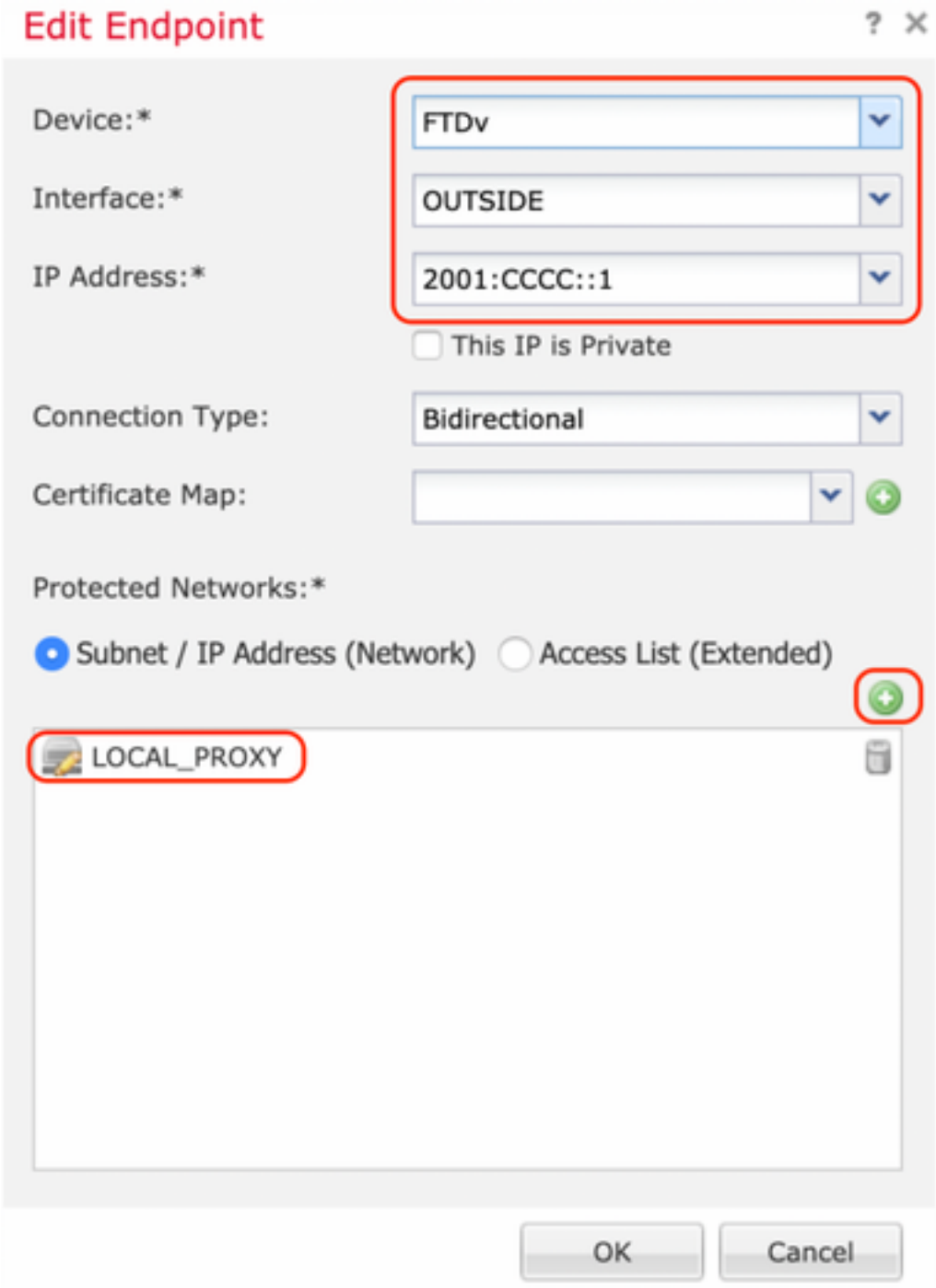
この例では、エンドポイントを選択する際に、ノードAがFTDです。ノードBはASAです。緑色のプラスボタンをクリックして、デバイスをトポロジに追加します。

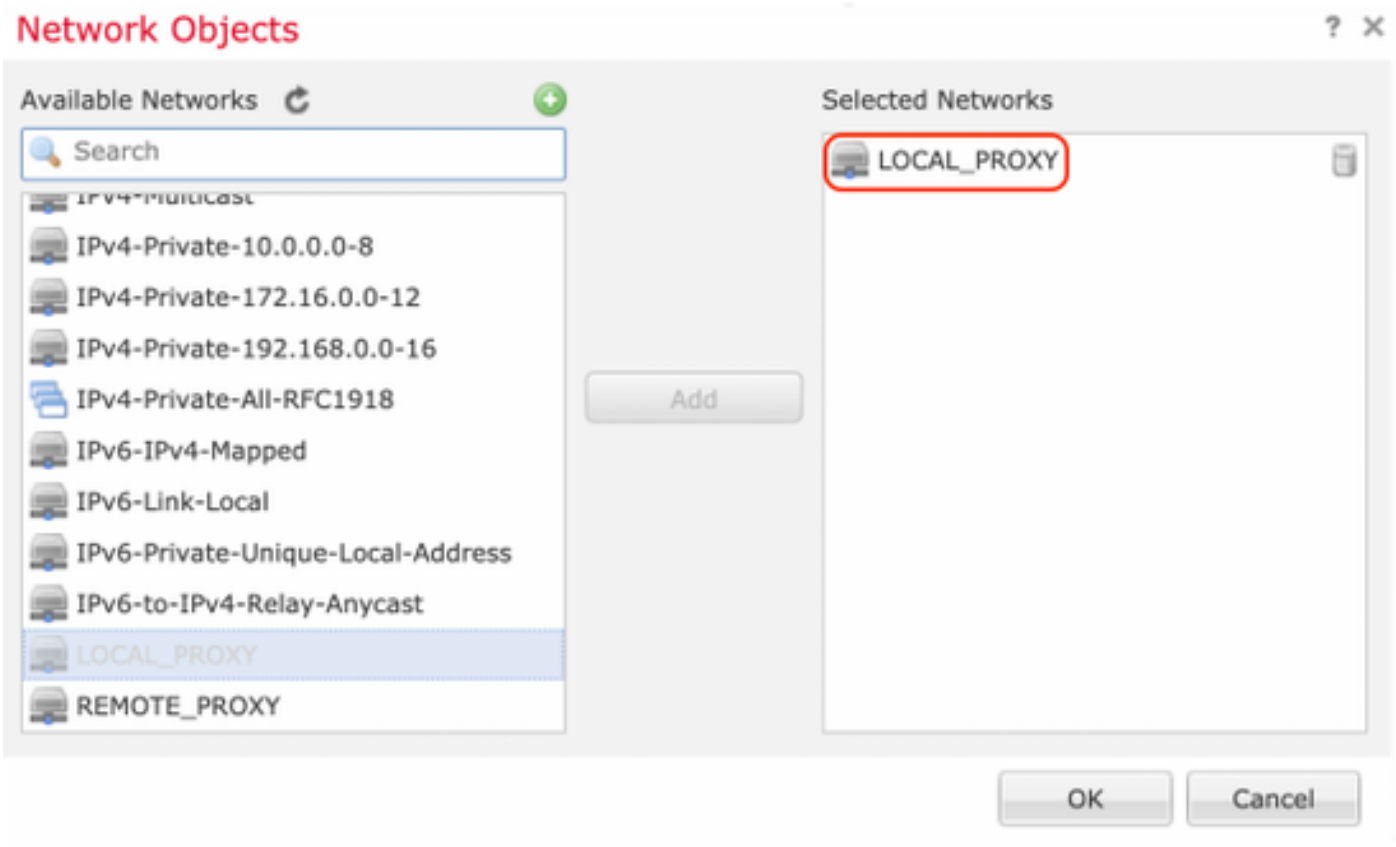


ステップ3：最初のエンドポイントとしてFTDを追加します。

暗号マップが適用されるインターフェイスを選択します。IPアドレスは、デバイス設定から自動的に入力されます。

[Protected Networks]の下の緑色のプラス記号アイコンをクリックして、このVPNトンネルを介して暗号化されるサブネットを選択します。この例では、FMCの「ローカルプロキシ」ネットワークオブジェクトは、IPv6サブネット「2001:DDDD::/64」で構成されています。

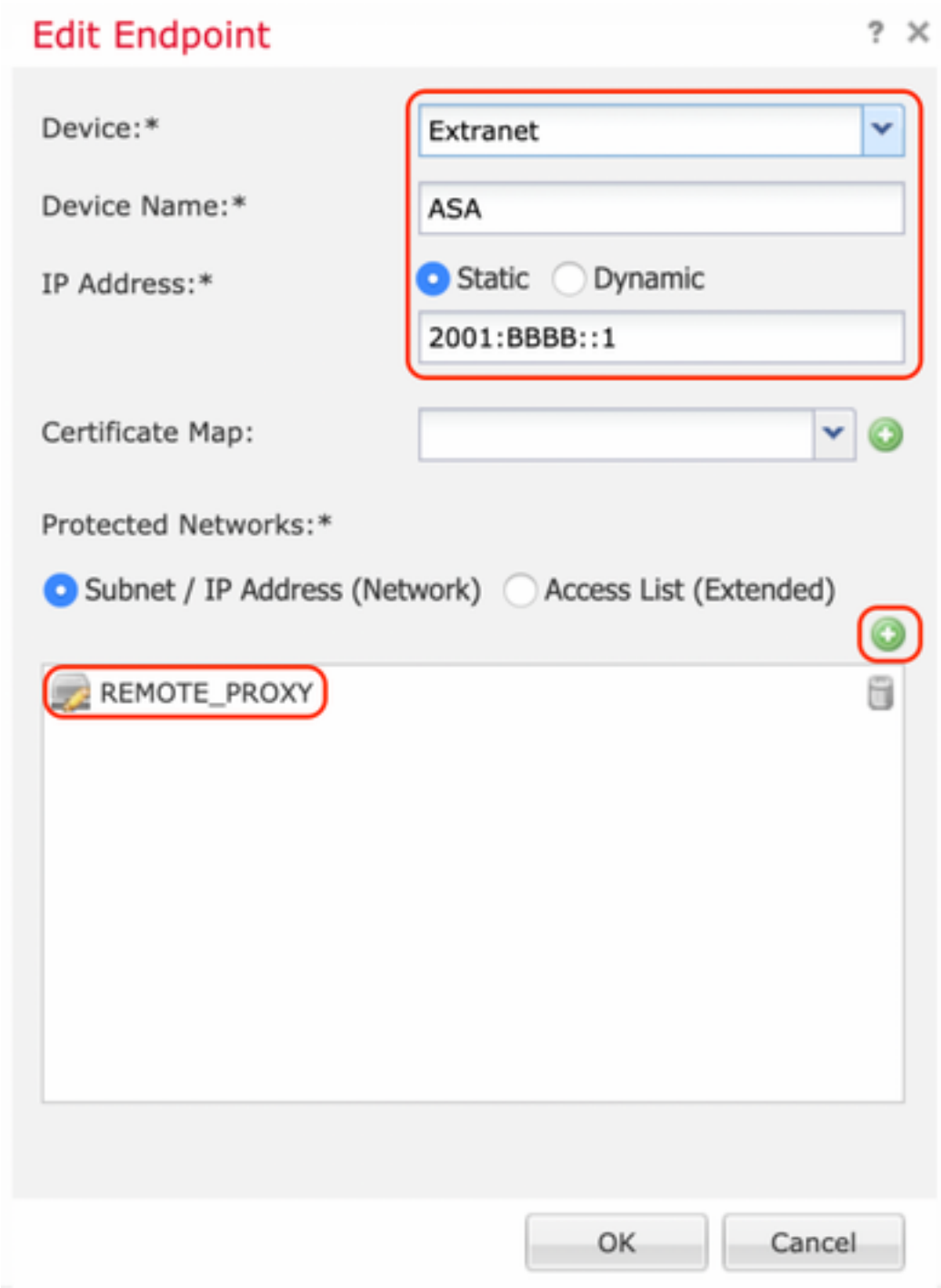

Edit Endpoint
Device:*
FTDv
Interface:*
OUTSIDE
IP Address:*
2001:CCCC::1
This IP is Private
Connection Type:
Bidirectional
Certificate Map:
Protected Networks:*
Subnet / IP Address (Network)
Access List (Extended)
LOCAL_PROXY
OK
Cancel



上記の手順では、FTDエンドポイントの設定が完了しています。

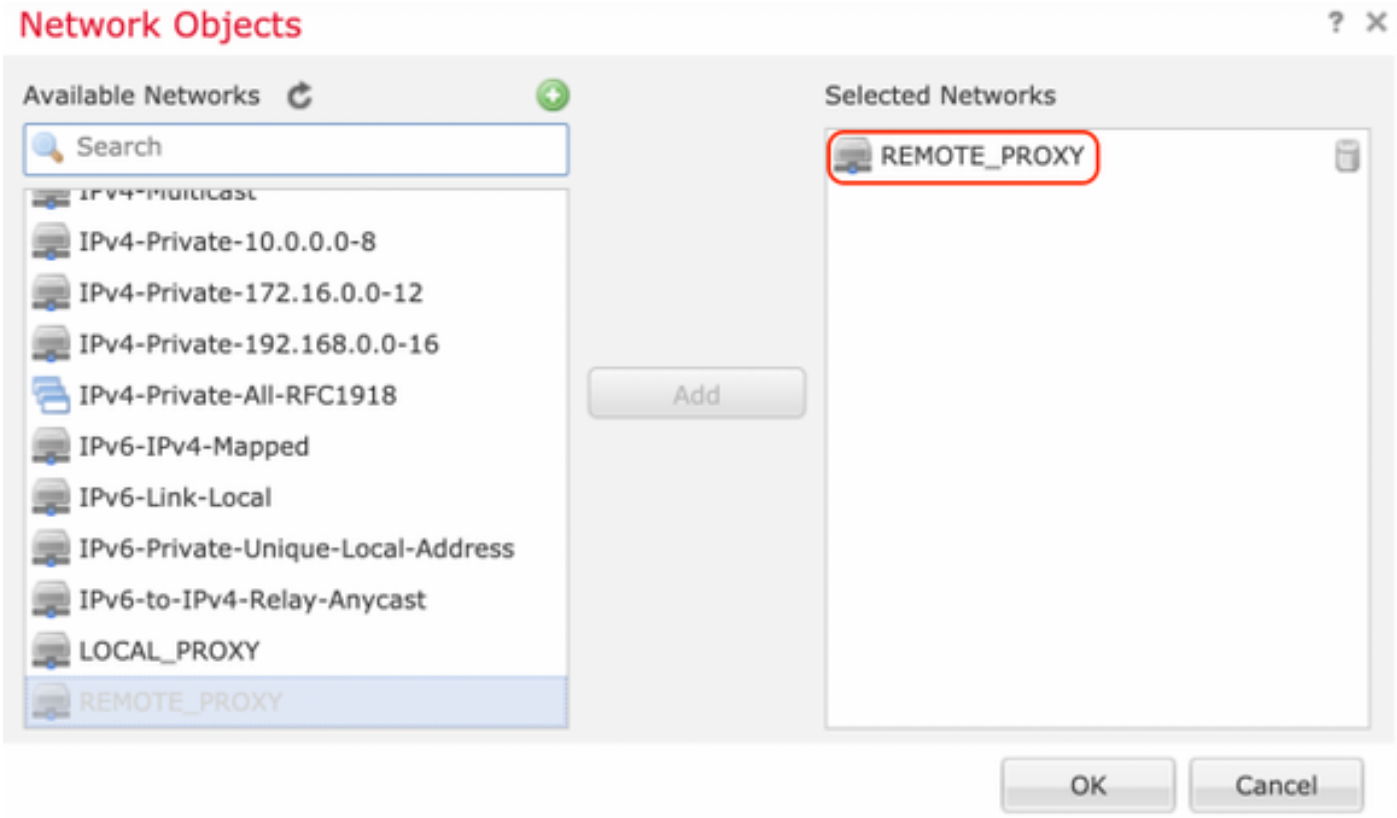
ステップ4：設定例のASAであるノードBの緑色のプラス記号アイコンをクリックします。FMCによって管理されていないデバイスは、エクストラネットと見なされます。デバイス名とIPアドレスを追加します。

ステップ5：保護されたネットワークを追加するには、緑色のプラス記号アイコンを選択します。



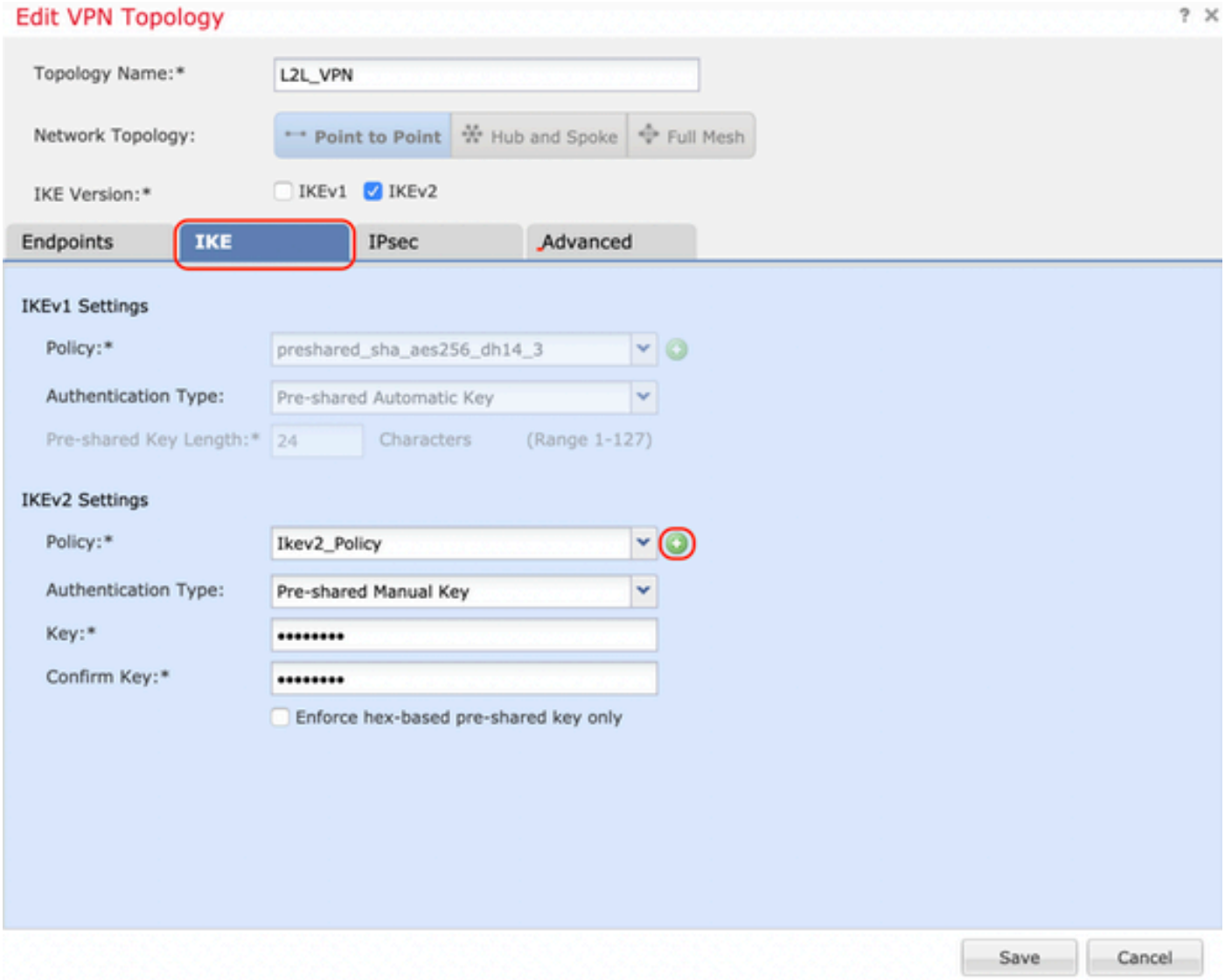
ステップ6：暗号化する必要があるASAサブネットを選択し、選択したネットワークに追加します。

この例では、「リモートプロキシ」はASAサブネット「2001:AAAA::/64」です。



IKEパラメータの設定

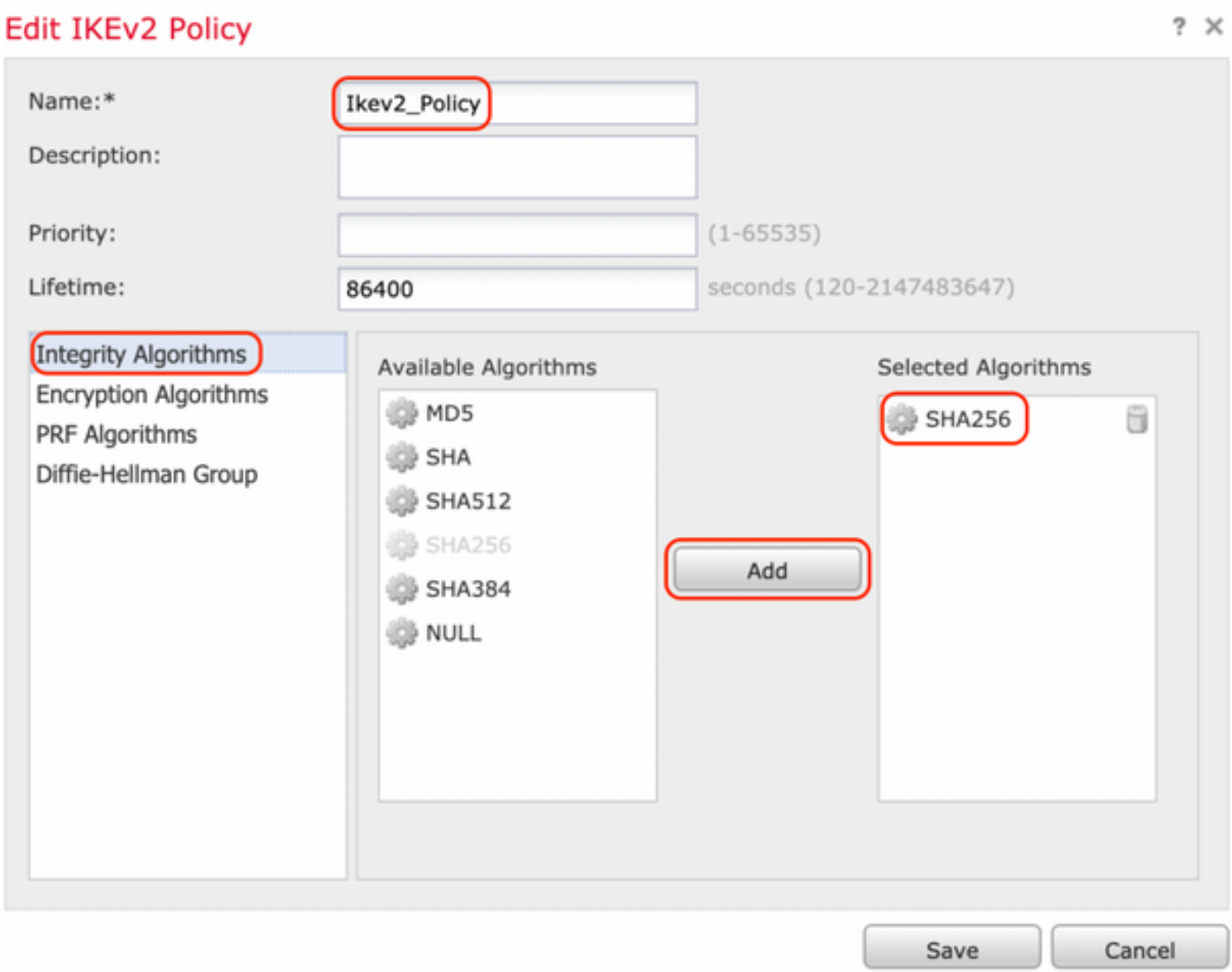
ステップ1:[IKE]タブで、IKEv2の初期交換に使用するパラメータを指定します。新しいIKEポリシーを作成するには、緑色のプラスアイコンをクリックします。

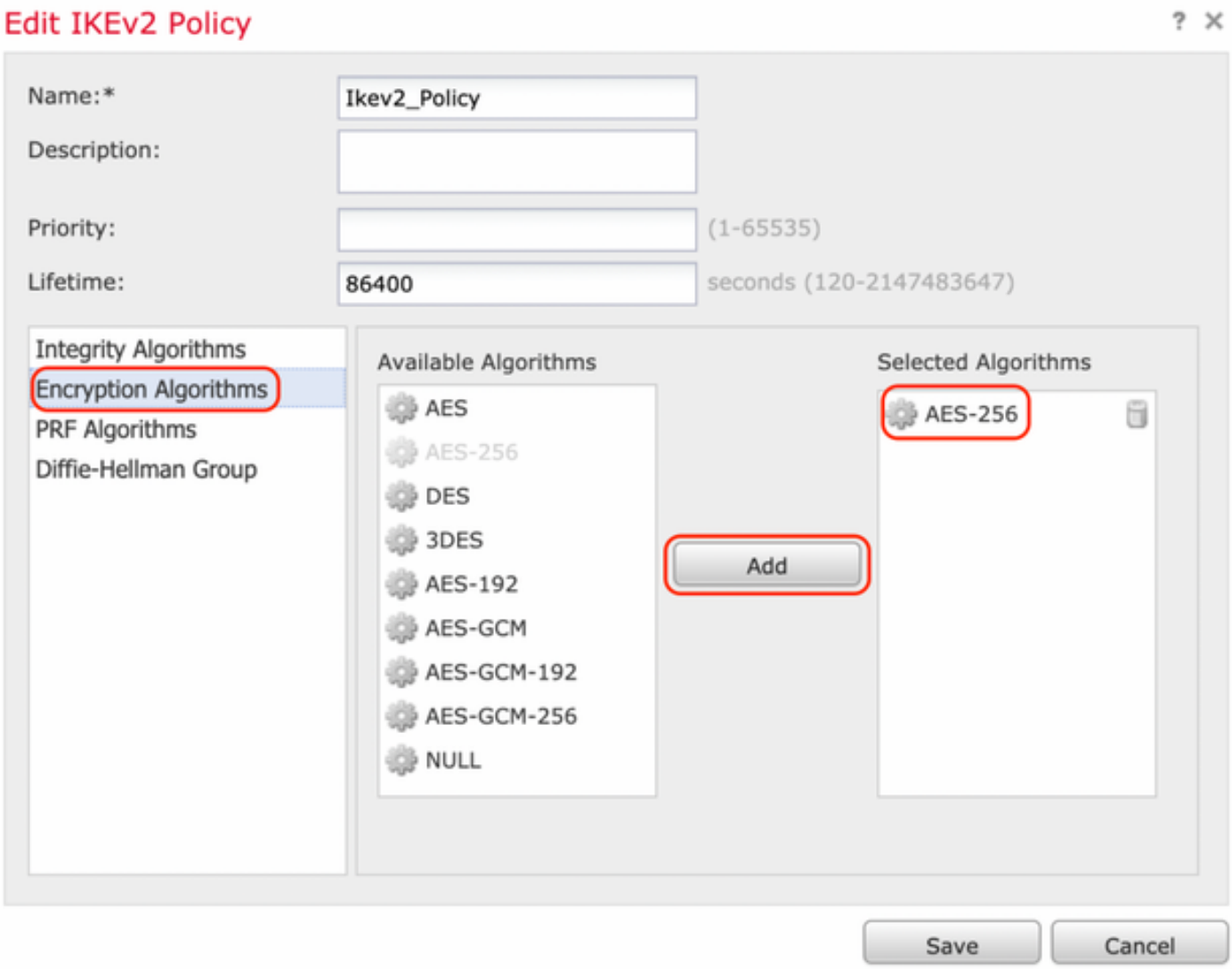


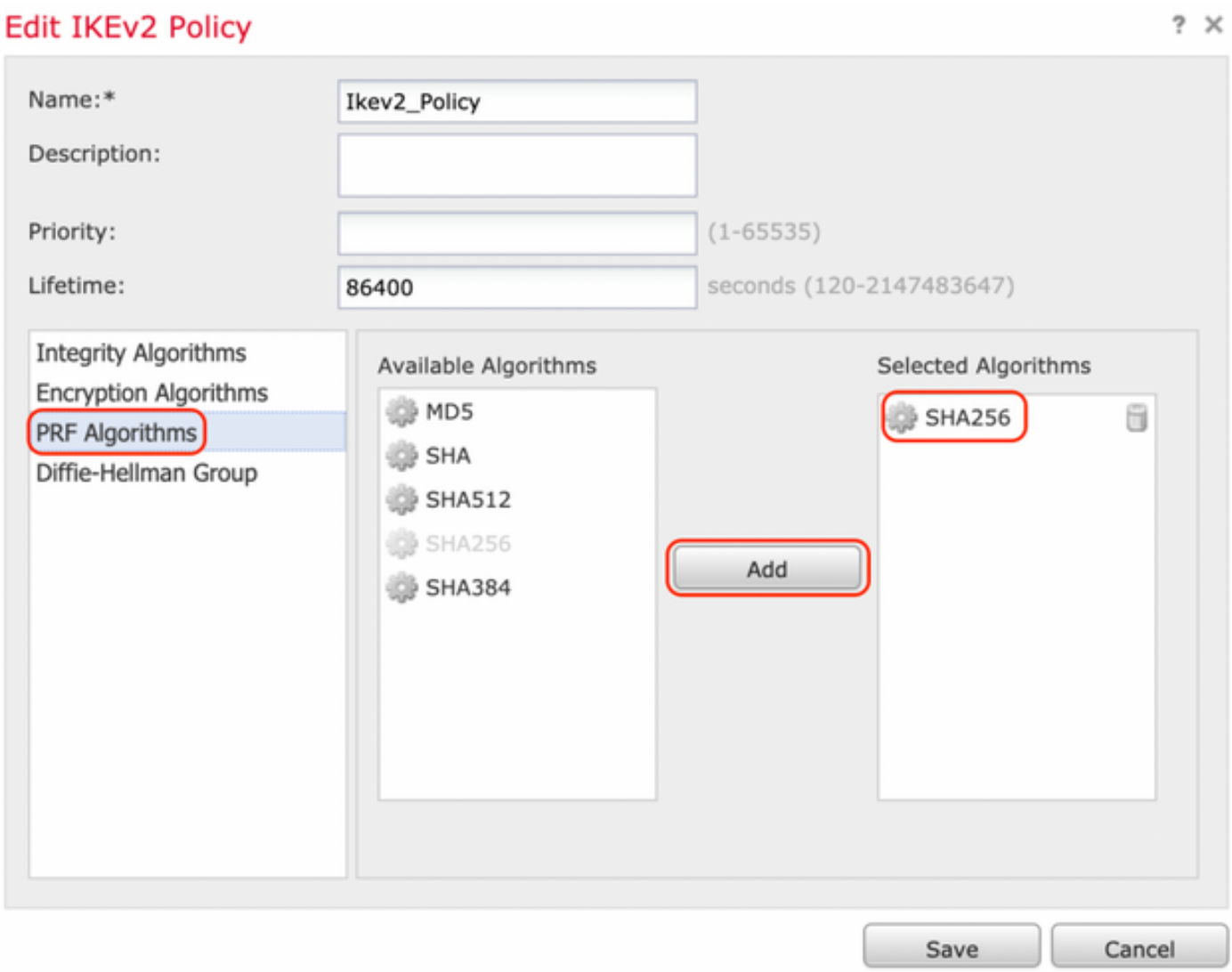
ステップ2：新しいIKEポリシーで、プライオリティ番号と接続のフェーズ1のライフタイムを指定します。このガイドでは、最初の交換に次のパラメータを使用します。
整合性(SHA256)、
暗号化(AES-256)、
PRF(SHA256)、および
Diffie-Hellmanグループ（グループ14）。

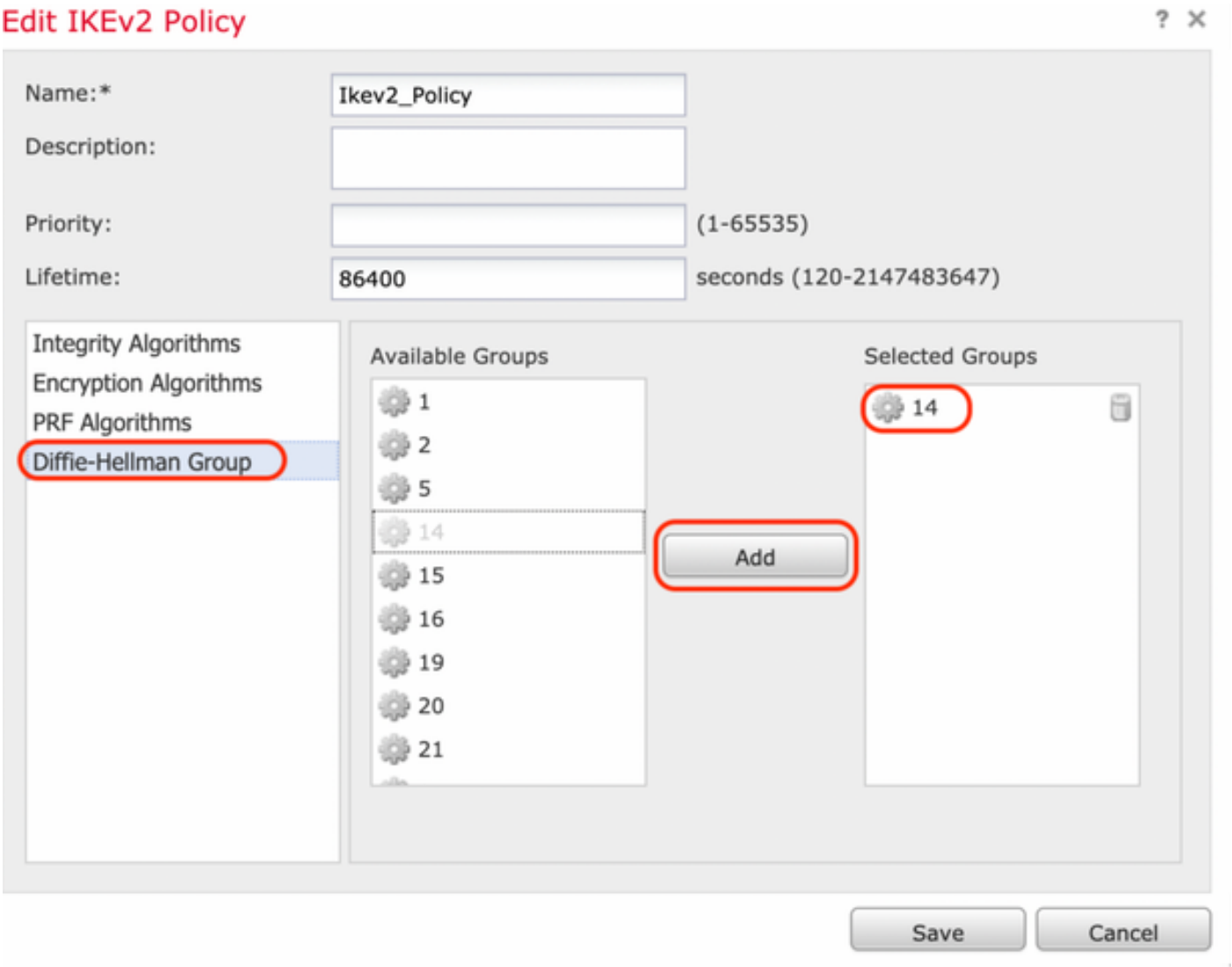
デバイス上のすべてのIKEポリシーは、選択したポリシーセクションの内容に関係なく、リモートピアに送信されます。リモートピアが一致する最初のピアがVPN接続に対して選択されます。

[オプション]優先フィールドを使用して、最初に送信するポリシーを選択します。プライオリティ1が最初に送信されます。


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

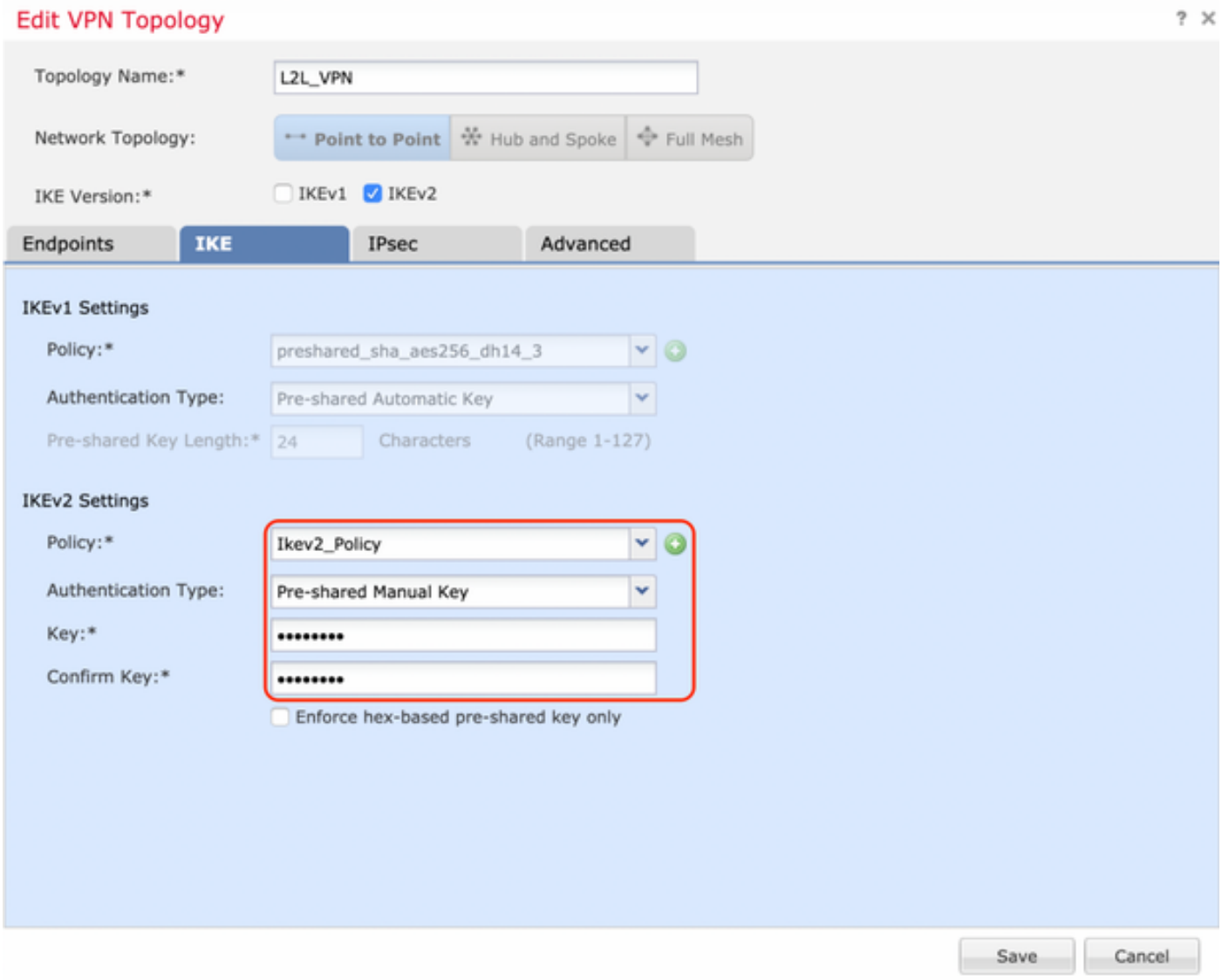

Edit IKEv2 Policy
Name:*
Ikev2_Policy
Description:
Priority:
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
AES
AES-256
DES
3DES
AES-192
AES-GCM
AES-GCM-192
AES-GCM-256
NULL
Add
Selected Algorithms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



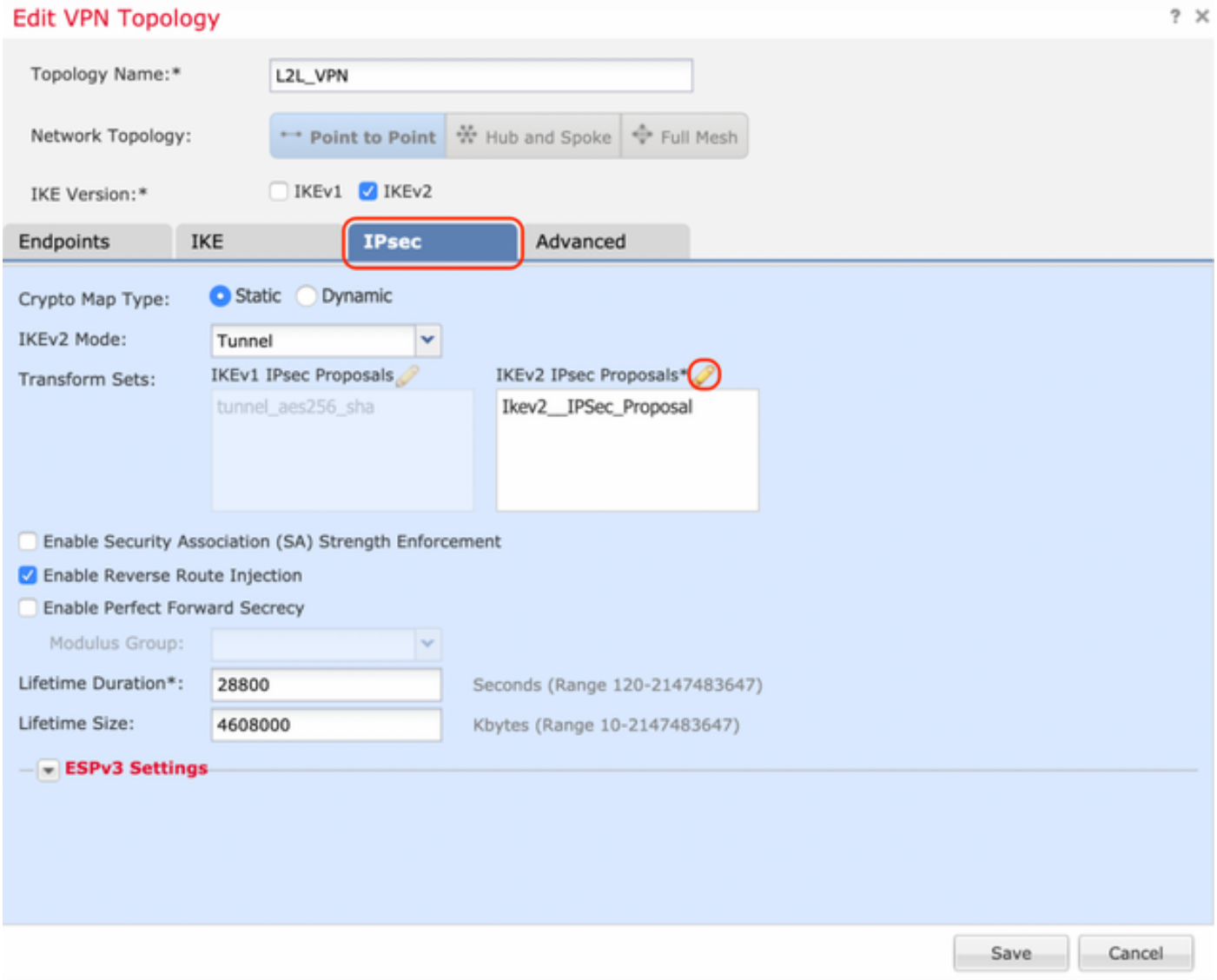
ステップ3：パラメータを追加したら、上記の設定ポリシーを選択し、認証タイプを選択します。

[Pre-shared Manual Key]オプションを選択します。このガイドでは、事前共有キー「**cisco123**」を使用します。



IPsec パラメータの設定

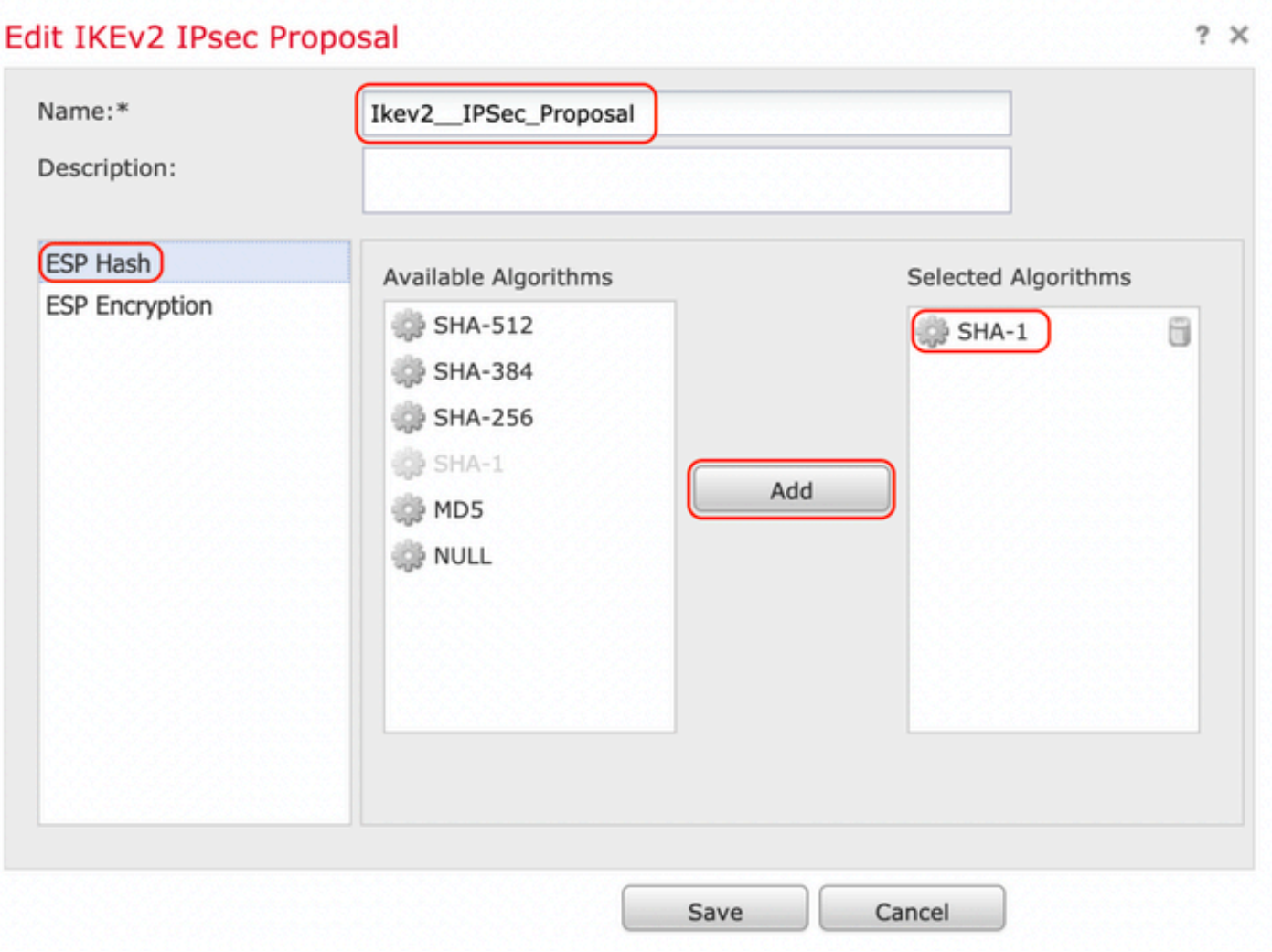
1:[IPsec]IPsec

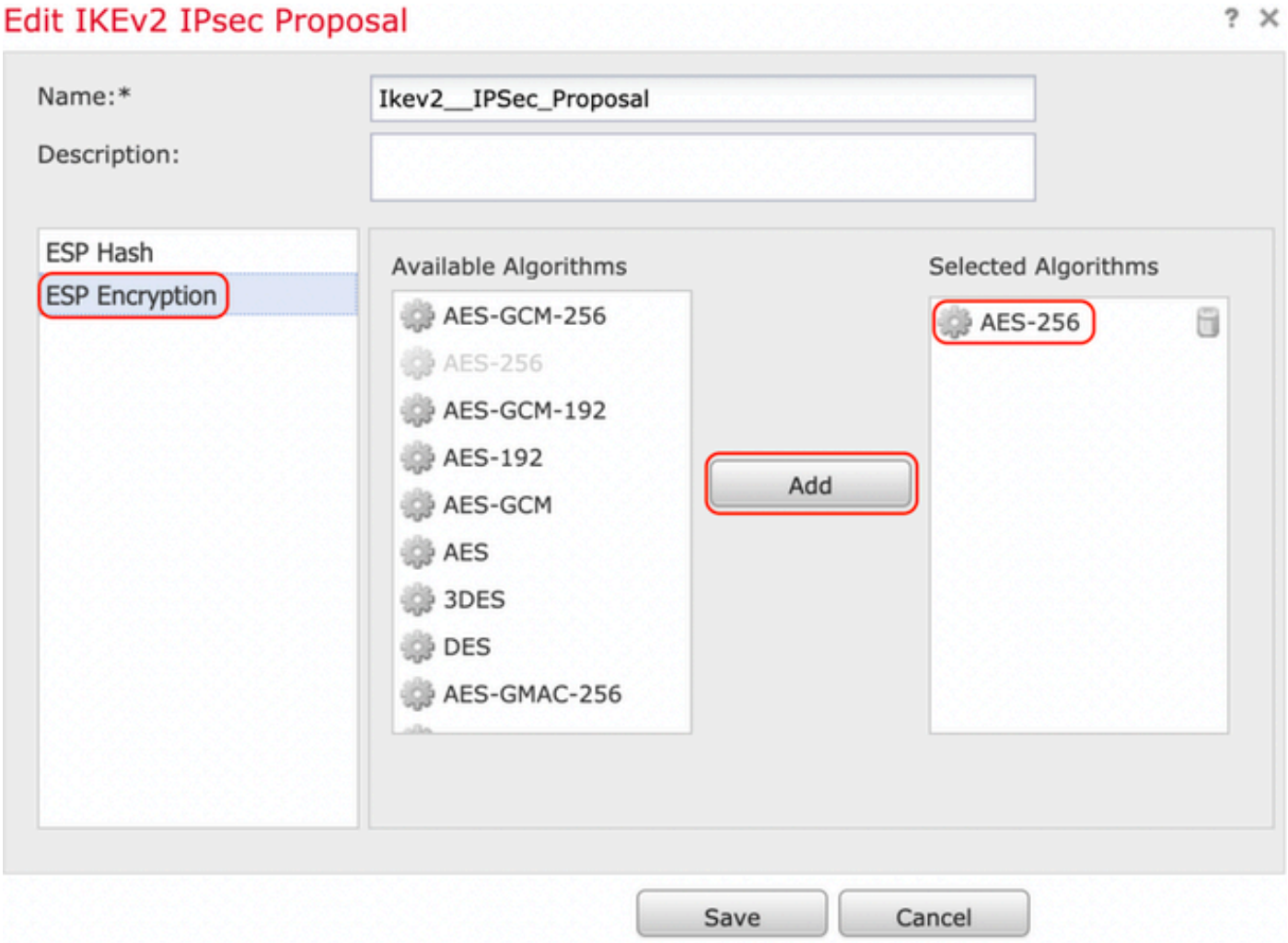


ステップ2：緑のプラス記号アイコンを選択して、次に示すようにフェーズ2パラメータを入力し、新しいIKEv2 IPsecプロポーザルを作成します。

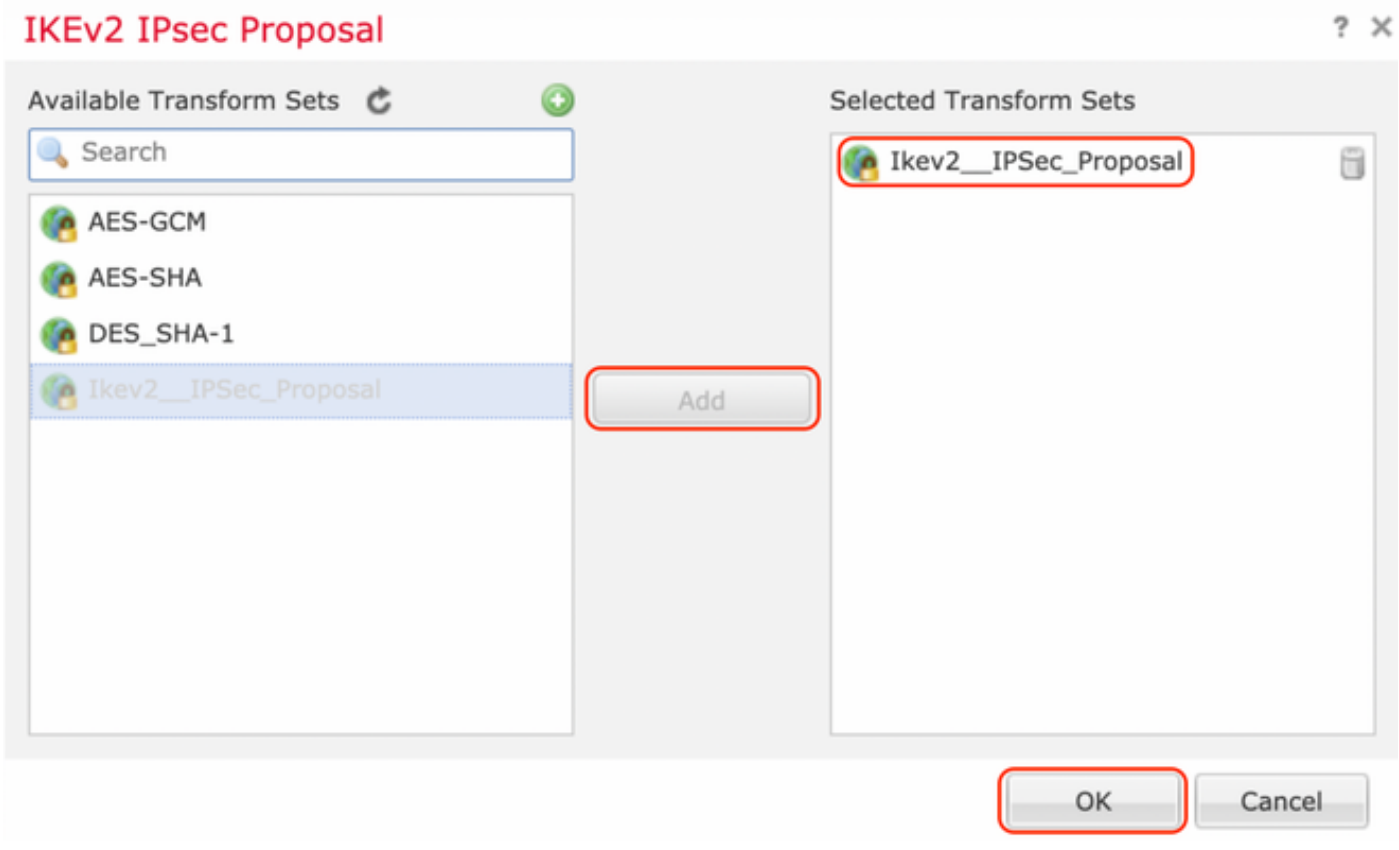
ESPハッシュ：SHA-1

ESP暗号化：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

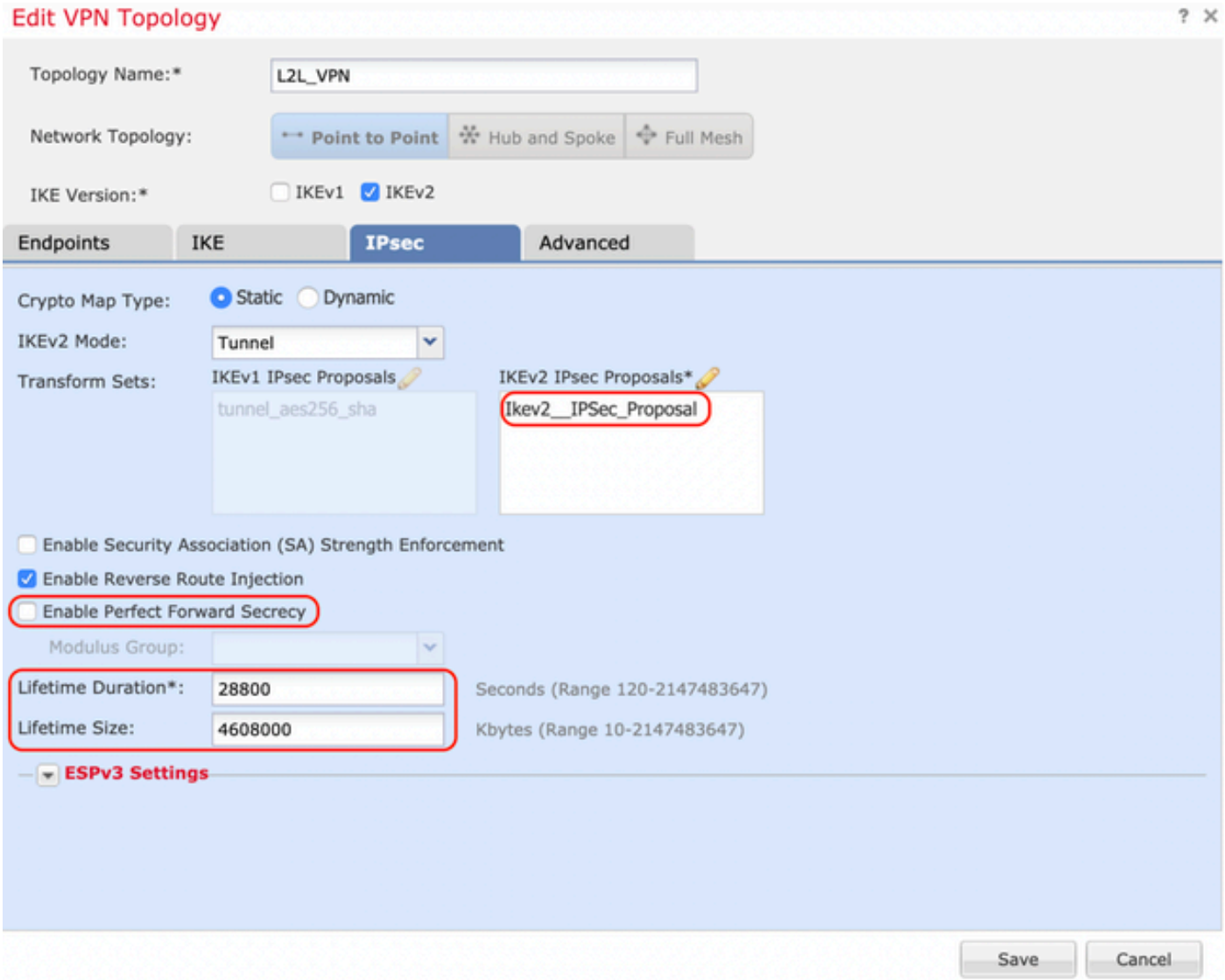


ステップ3：新しいIPsecプロポーザルが作成されたら、選択したトランスフォームセットに追加します。



ステップ4：新しく選択したIPsecプロポーザルが[IKEv2 IPsec Proposals]の下に表示されます。

必要に応じて、フェーズ2ライフタイムとPFSを編集できます。この例では、ライフタイムがデフォルトに設定され、PFSが無効になっています。



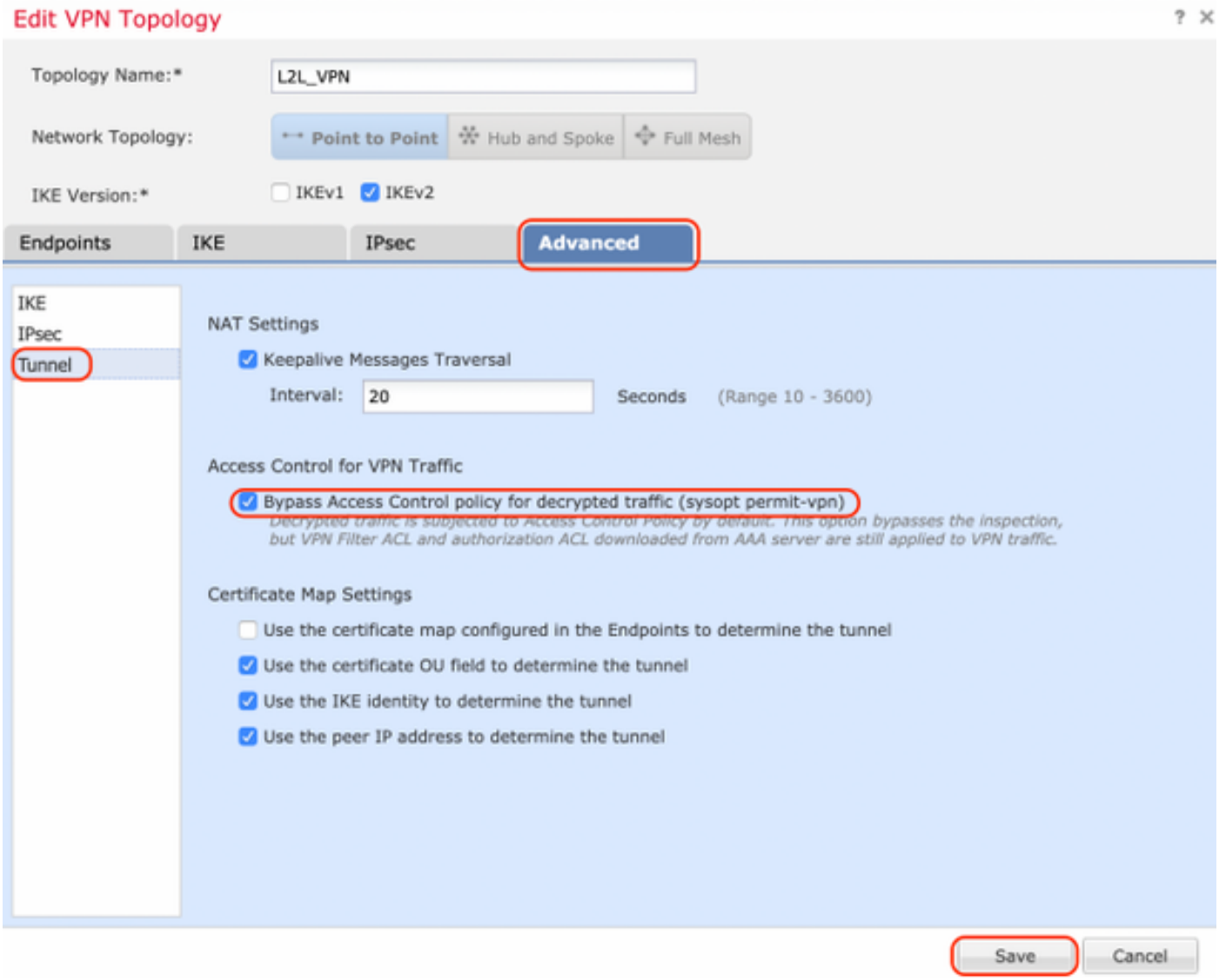
FTDを介してVPNサブネットを許可するには、次の手順をBypass Access ControlまたはCreate Access Control Policyルールに設定する必要があります。

アクセスコントロールのバイパス

sysopt permit-vpnが有効になっていない場合は、FTDデバイスを介したVPNトラフィックを許可するためにアクセスコントロールポリシーを作成する必要があります。sysopt permit-vpnが有効になっている場合は、アクセスコントロールポリシーの作成をスキップします。この設定例では、[Bypass Access Control]オプションを使用します。

パラメータsysopt permit-vpnは、[Advanced] > [Tunnel]で有効にできます。

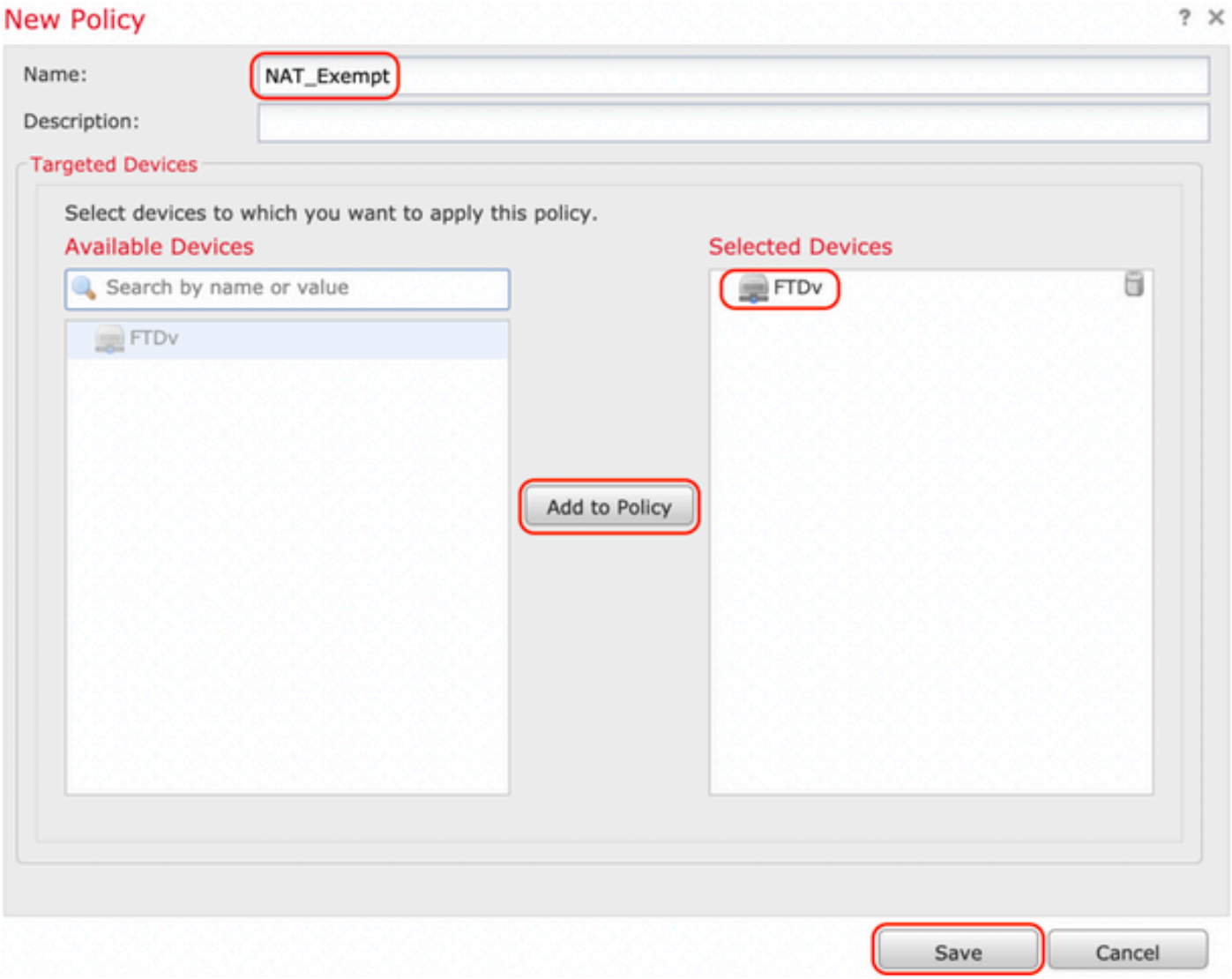
> **注意**：このオプションを使用すると、アクセスコントロールポリシーを使用してユーザからのトラフィックを検査する可能性がなくなります。VPNフィルタまたはダウンロード可能ACLは、ユーザトラフィックのフィルタリングにも使用できます。これはグローバルコマンドで、このチェックボックスが有効になっている場合はすべてのVPNに適用されます。



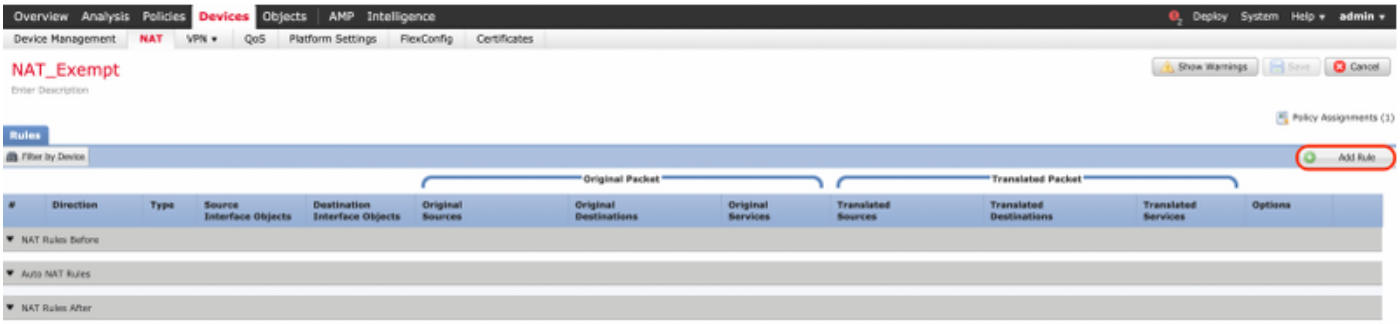
NAT免除の設定

VPNトラフィックのNAT免除ステートメントを設定します。VPNトラフィックが別のNAT文と一致せず、VPNトラフィックが誤って変換されるのを防ぐために、NAT免除を設定する必要があります。

ステップ1:[Devices] > [NAT]および[c]に移動します[New Policy] > [Threat Defense NAT]をクリックして、新しいポリシーを作成します。



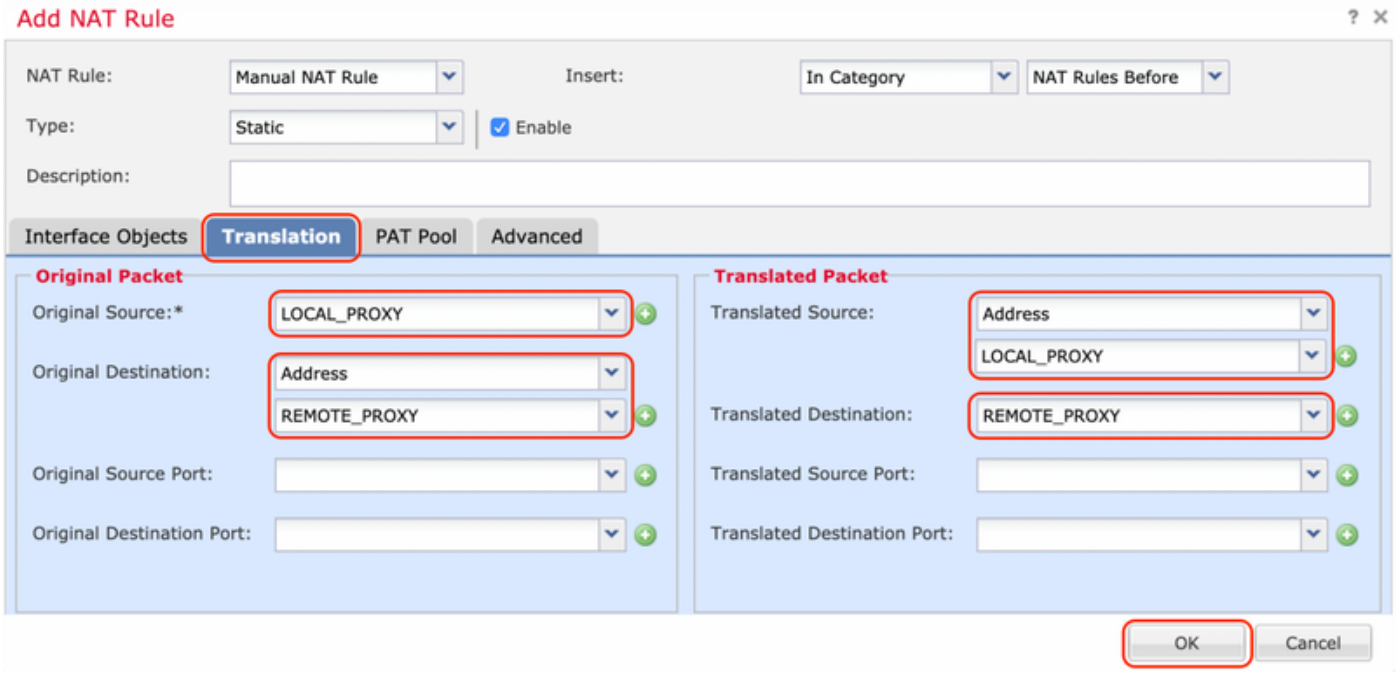
ステップ2:[Add Rule]をクリックします。



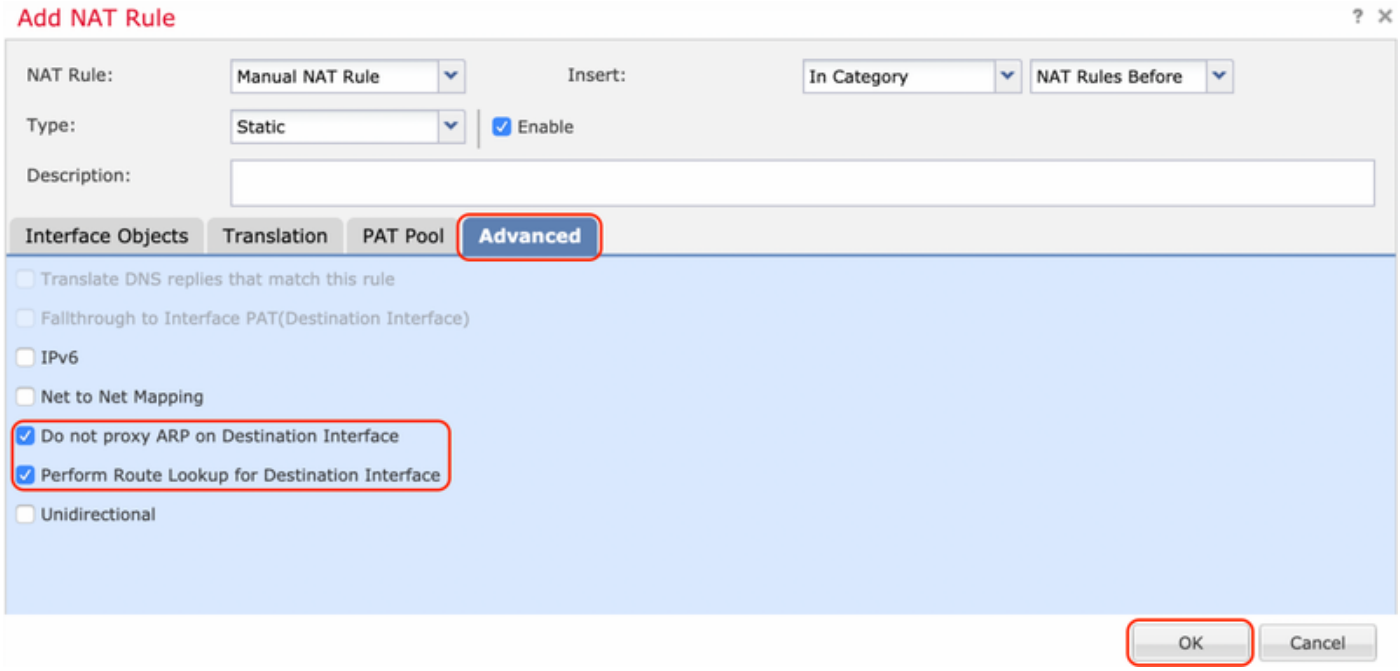
ステップ3：新しいスタティック手動NATルールを作成します。

NATルールの内部インターフェイスと外部インターフェイスを参照してください。[Interface Objects]タブでインターフェイスを指定すると、これらのルールが他のインターフェイスからのトラフィックに影響を与えなくなります。

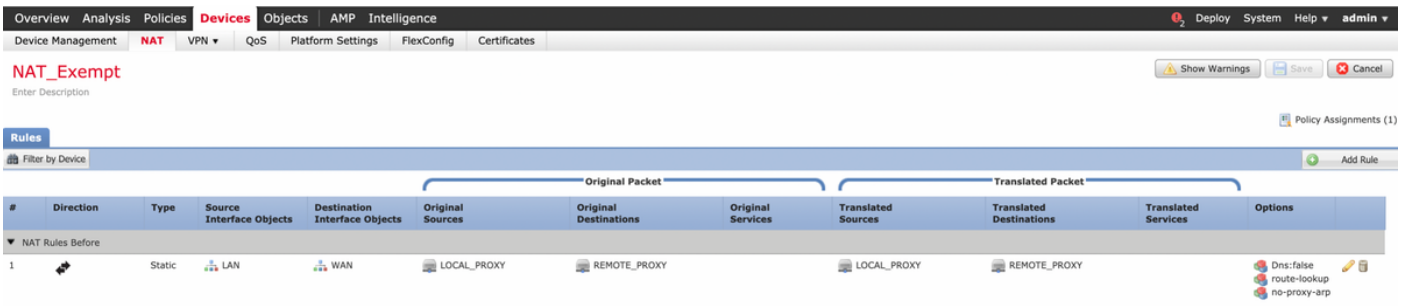
[Translation]タブに移動し、送信元と宛先のサブネットを選択します。これはNAT免除ルールであるため、元の送信元/宛先と変換された送信元/宛先が同じであることを確認します。



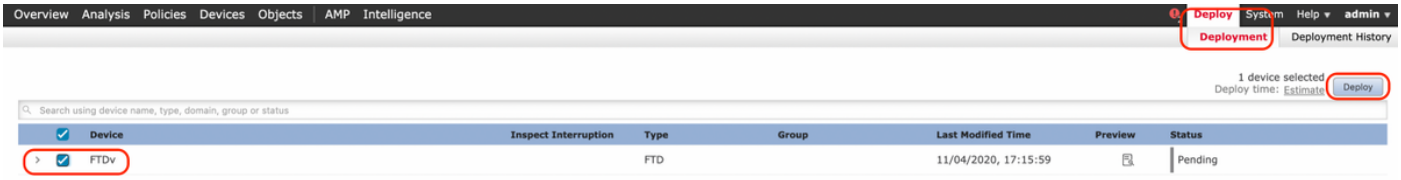
[Advanced]タブをクリックし、**no-proxy-arpとroute-lookupを有効にします。**



このルールを保存し、NATリストの最後のNATステートメントを確認します。



ステップ4：設定が完了したら、設定を保存してFTDに展開します。



確認

LANマシンから対象トラフィックを開始するか、ASAで次のpacket-tracerコマンドを実行できます。

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

注:Type = 128で、Code=0はICMPv6「エコー要求」を表します。

次のセクションでは、ASAvまたはFTD LINA CLIで実行してIKEv2トンネルのステータスを確認できるコマンドについて説明します。

ASAからの出力例を次に示します。

```
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
```

トラブルシュート

ASAおよびFTDでIKEv2トンネル確立の問題をトラブルシューティングするには、次のdebugコマンドを実行します。

debug crypto condition peer <peer IP>
debug crypto ikev2 protocol 255
debug crypto ikev2 platform 255

次に、参照用の動作中のIKEv2デバッグの例を示します。
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

参考資料

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