FDMによって管理されるFTD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、Firepower Device Manager(FDM)によって管理されるFirepower Threat Defense(FTD)でサイト間VPN(L2L)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。

- VPNの基本的な知識
- FDNの使用経験
- 適応型セキュリティアプライアンス(ASA)コマンドラインの経験

使用するコンポーネント

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。

- Cisco FTD 6.5
- ASA 9.10(1)32
- IKEv2

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。

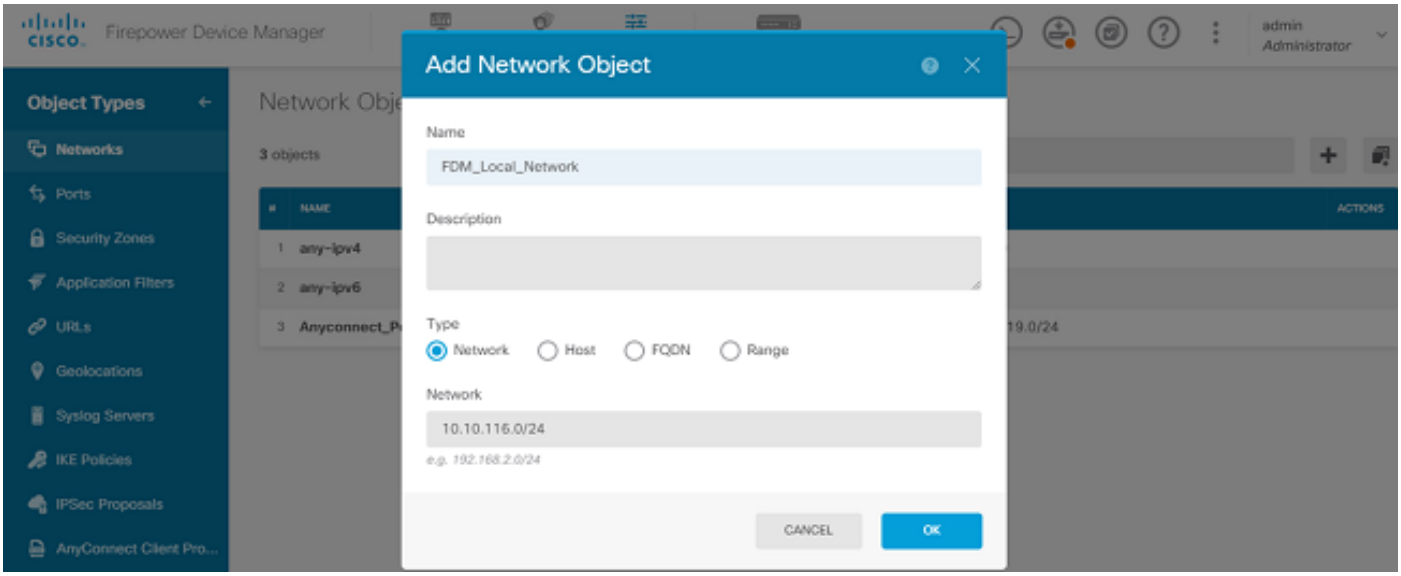
設定

FDMを使用したFTDの設定から開始します。

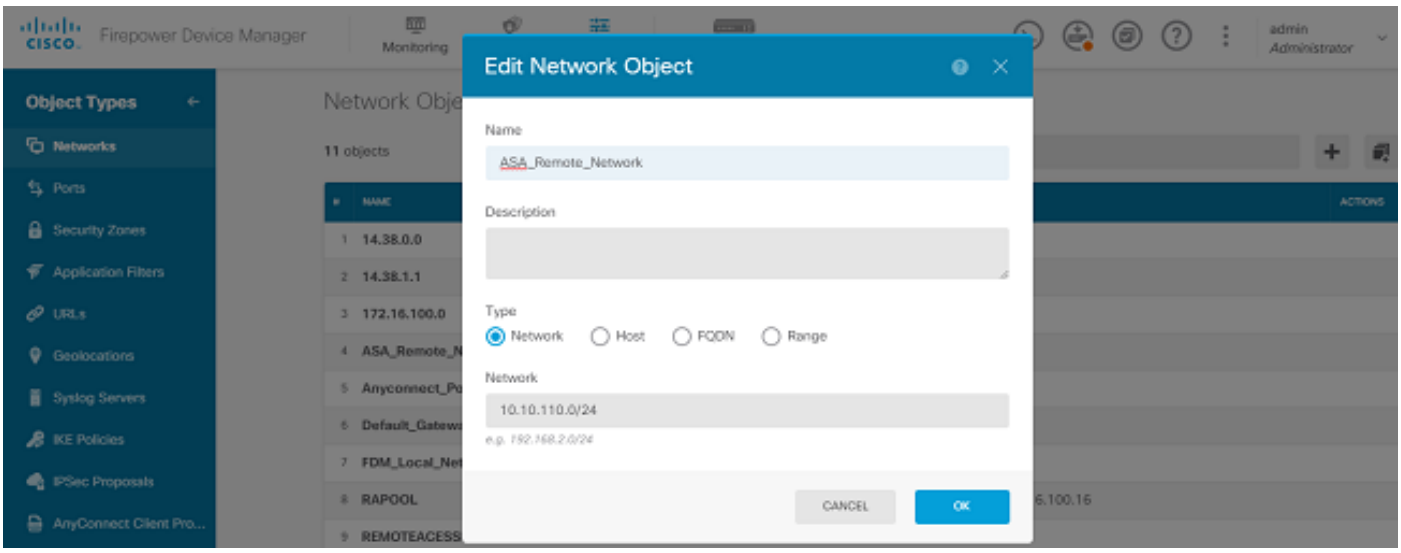
保護されたネットワークの定義

Objects > Networks > Add New Networkの順に移動します。

FDM GUIからLANネットワークのオブジェクトを構成します。図に示すように、FDMデバイスの背後にあるローカル・ネットワークのオブジェクトを作成します。



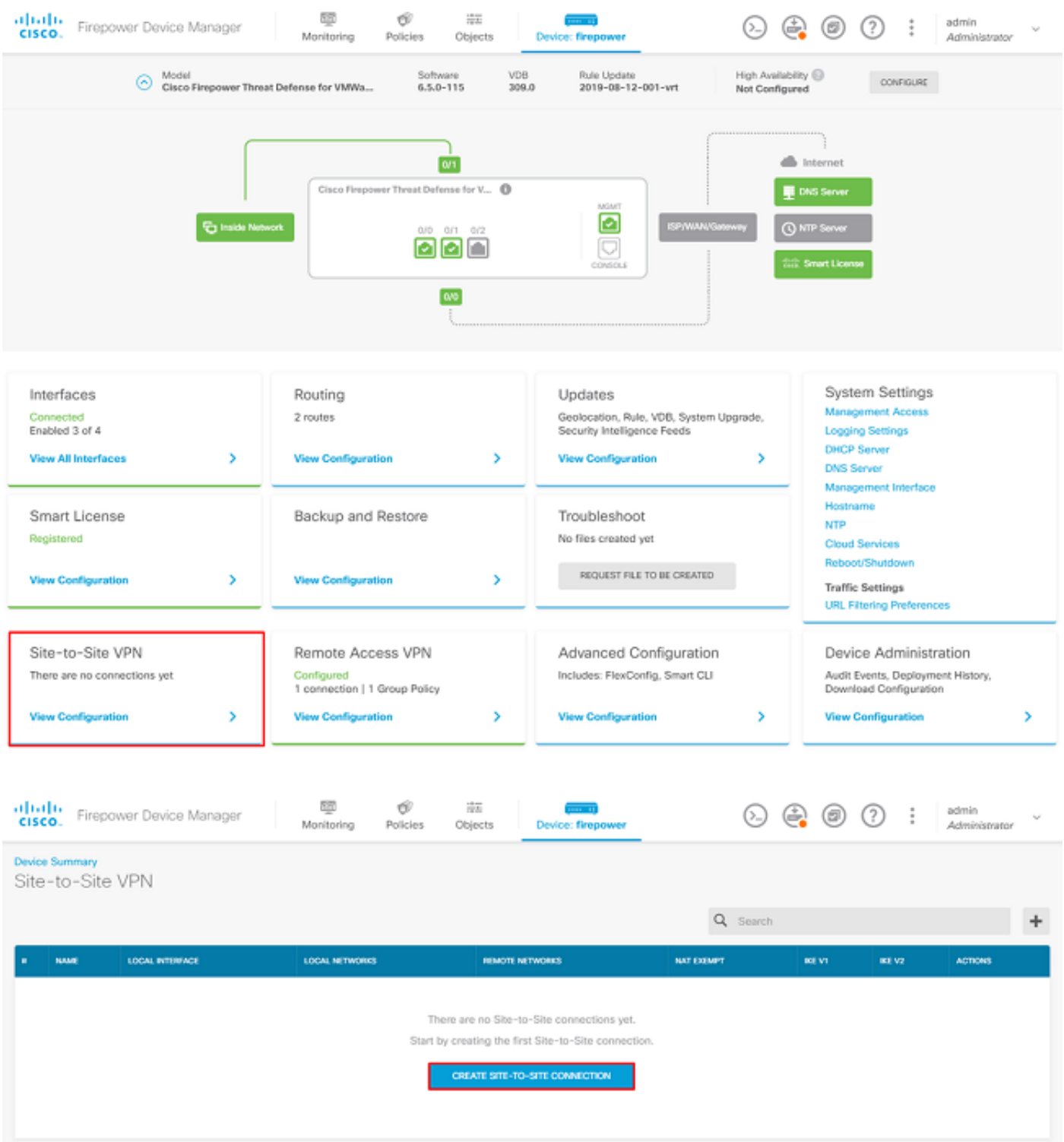
図に示すように、ASAデバイスの背後にあるリモートネットワークのオブジェクトを作成します。



サイト間VPNの設定

Site-to-Site VPN > Create Site-to-Site Connectionの順に移動します。

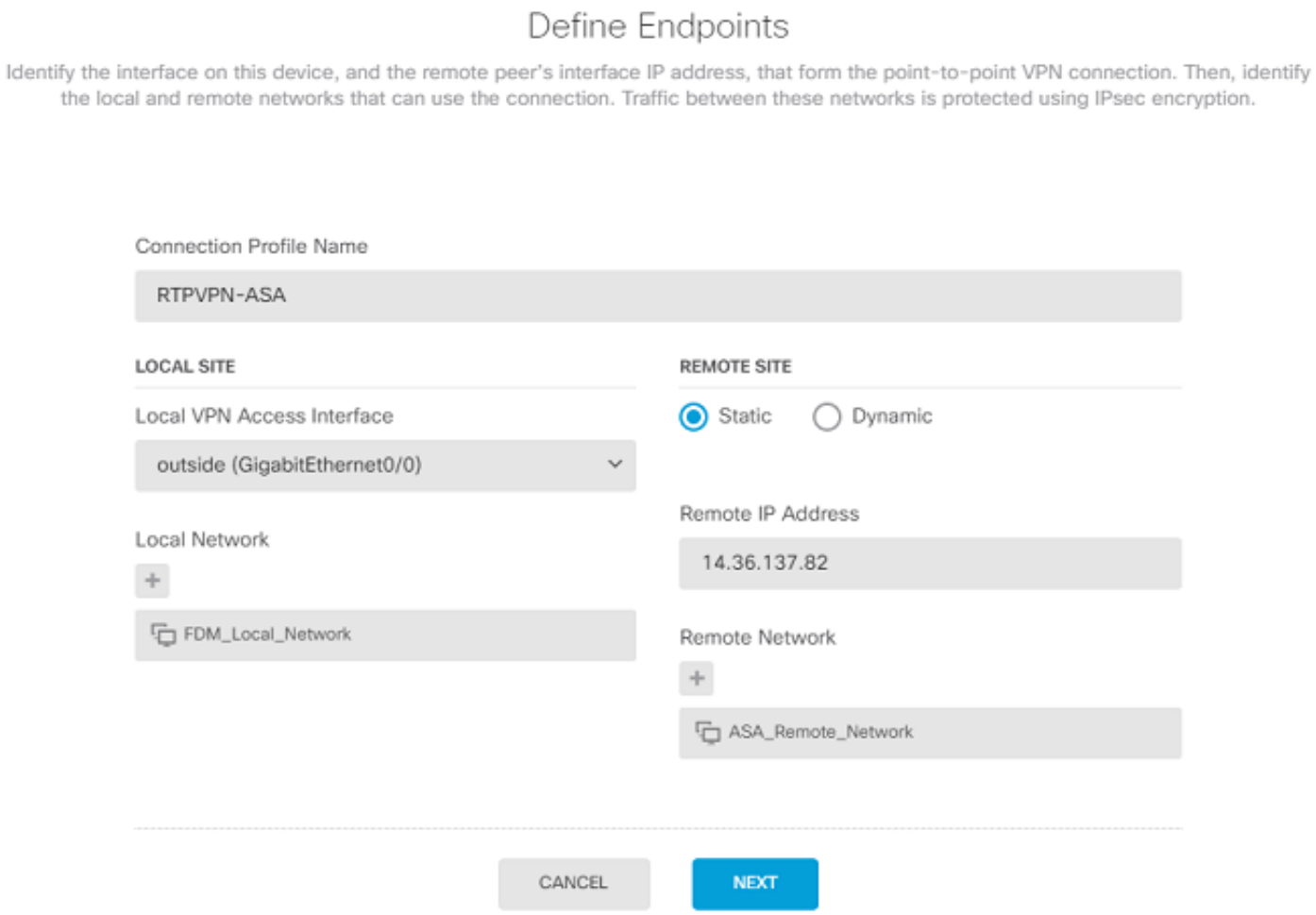
図に示すように、FDMでサイト間ウィザードを実行します。



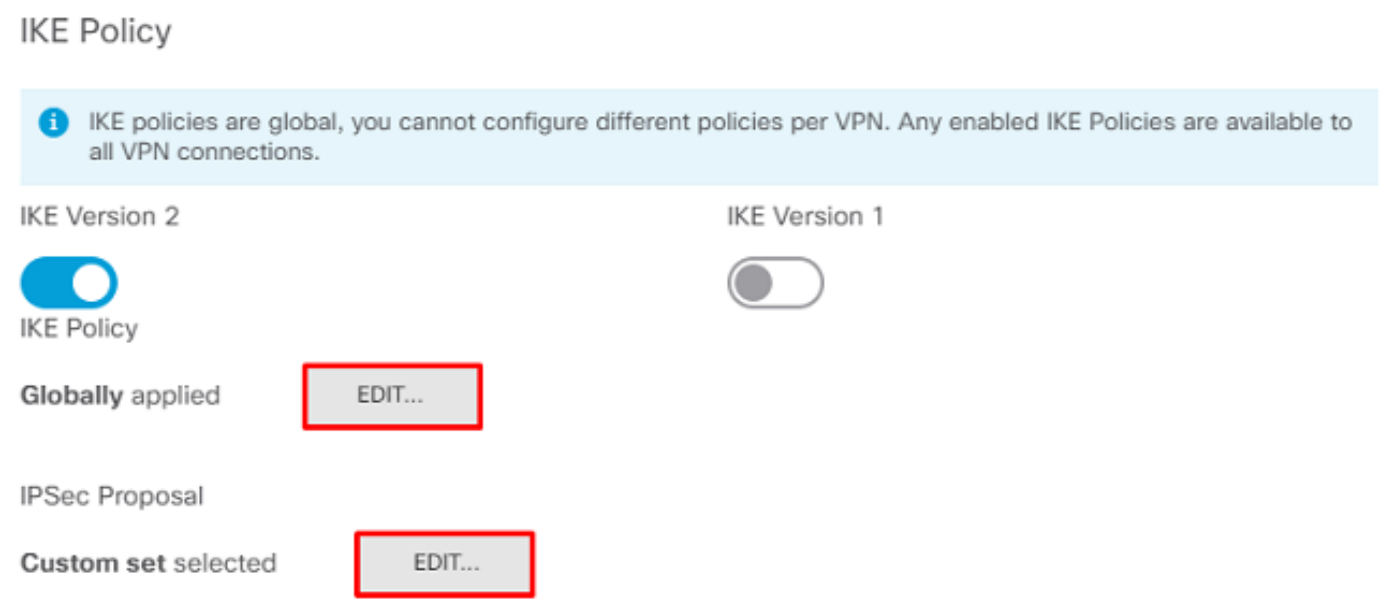
サイト間接続に、簡単に識別できる接続プロファイル名を指定します。

FTDの正しい外部インターフェイスを選択し、サイト間VPNで暗号化する必要があるローカルネットワークを選択します。

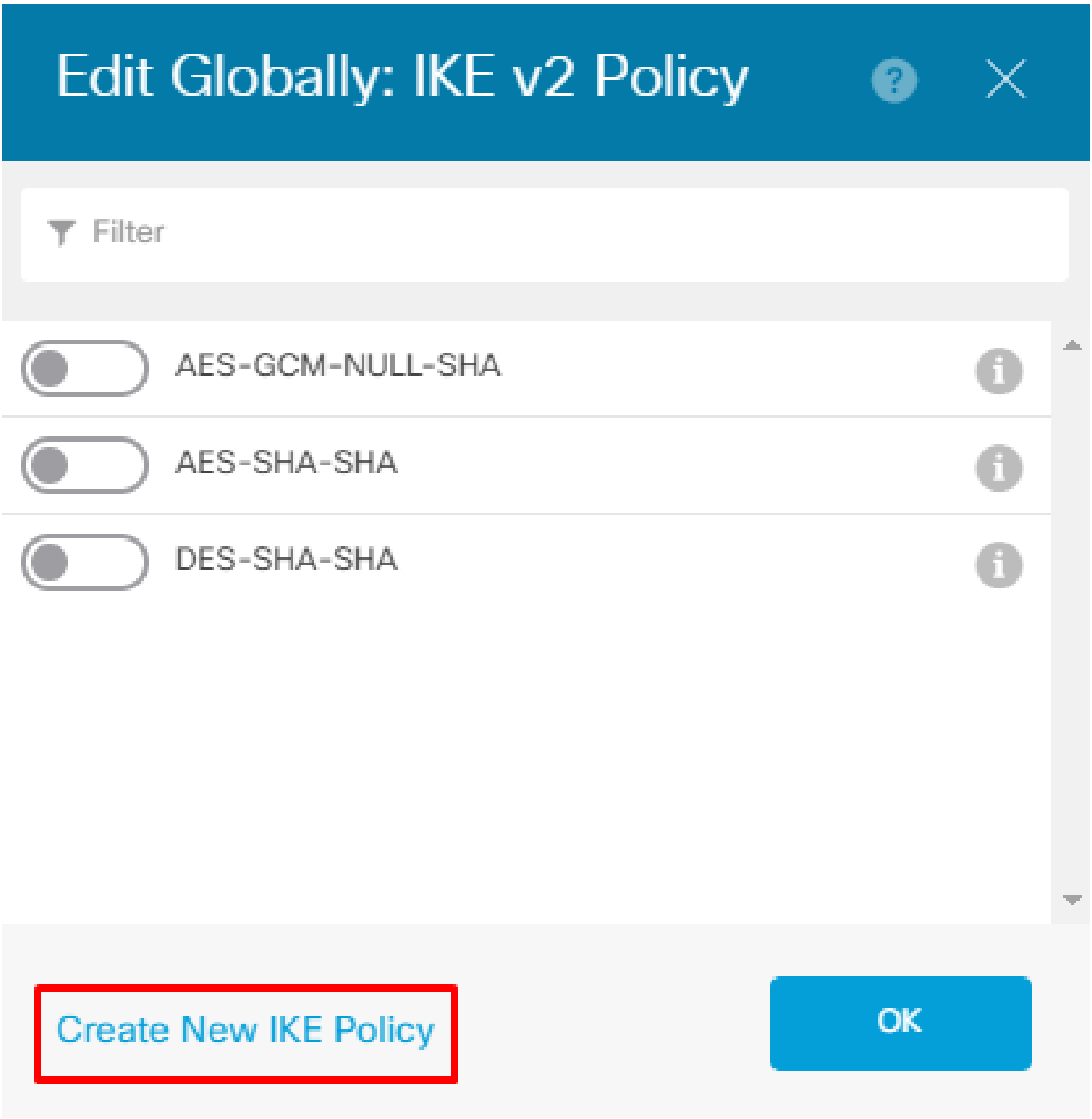
リモートピアのパブリックインターフェイスを設定します。次に、図に示すように、サイト間VPNで暗号化されているリモートピアのネットワークを選択します。



次のページでEditボタンを選択し、図に示すようにInternet Key Exchange（IKE；インターネット鍵交換）パラメータを設定します。

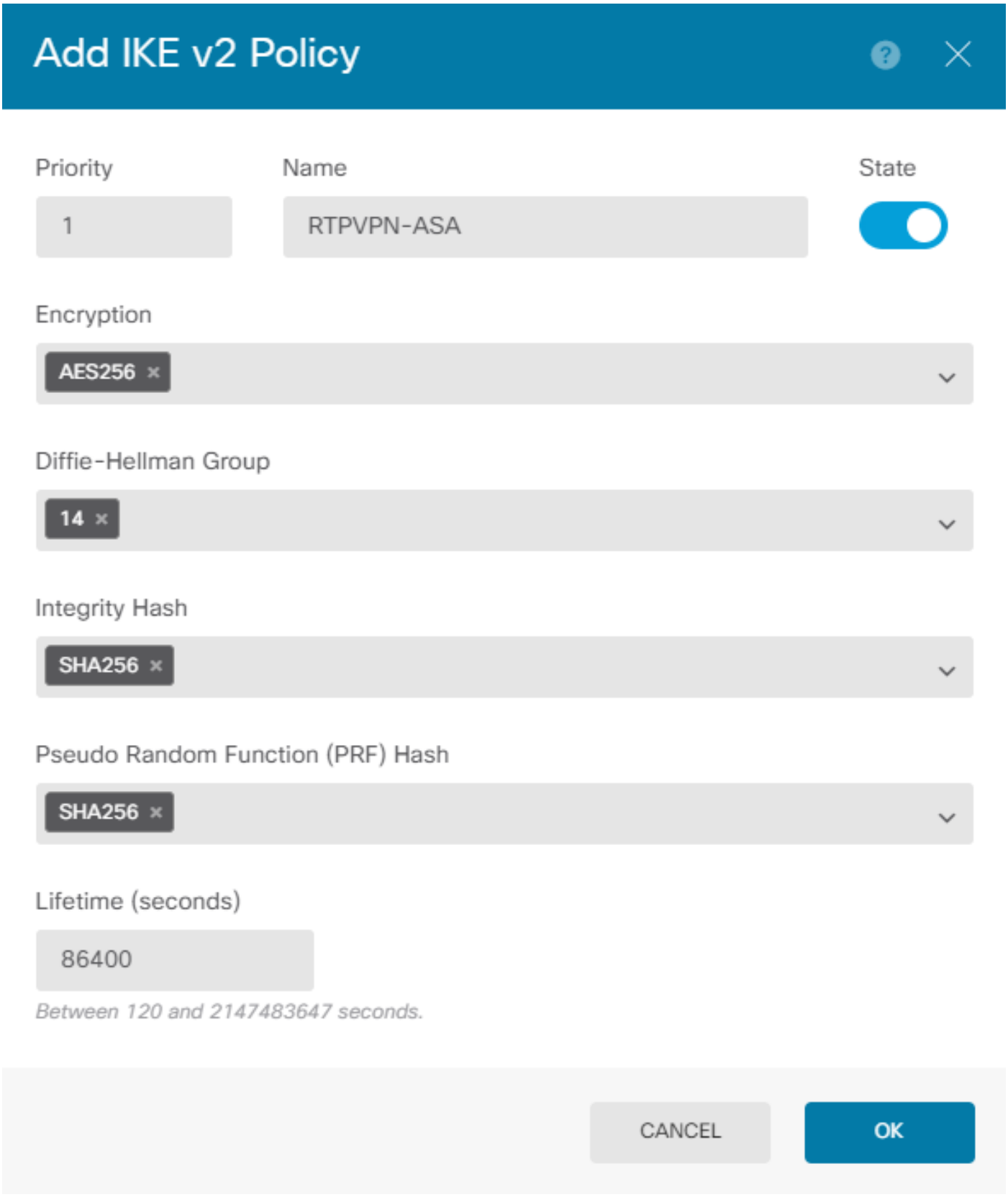


図に示すように、Create New IKE Policyボタンを選択します。

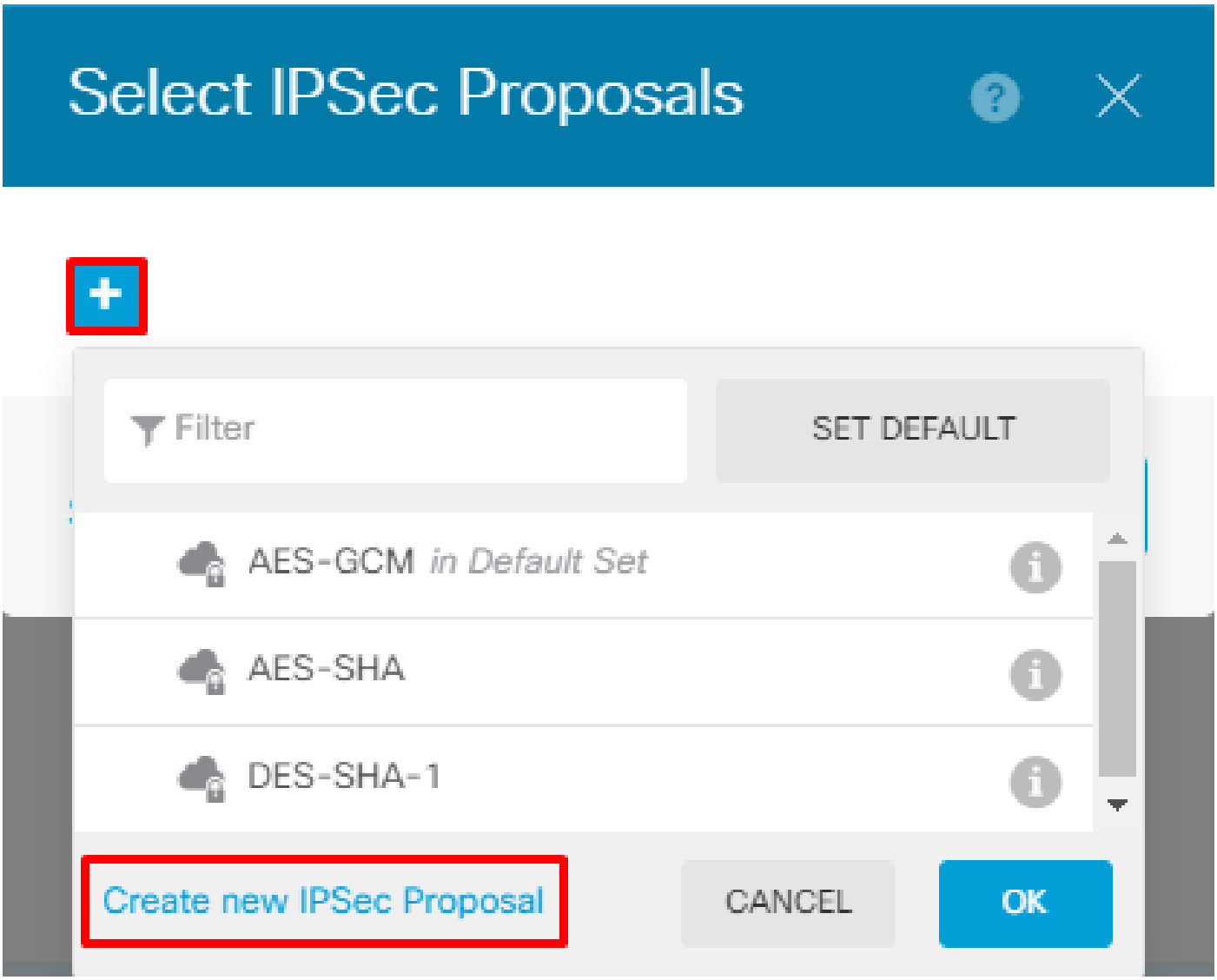


このガイドでは、IKEv2の初期交換に次のパラメータを使用します。

暗号化AES-256
整合性SHA256
DHグループ14
PRF SHA256



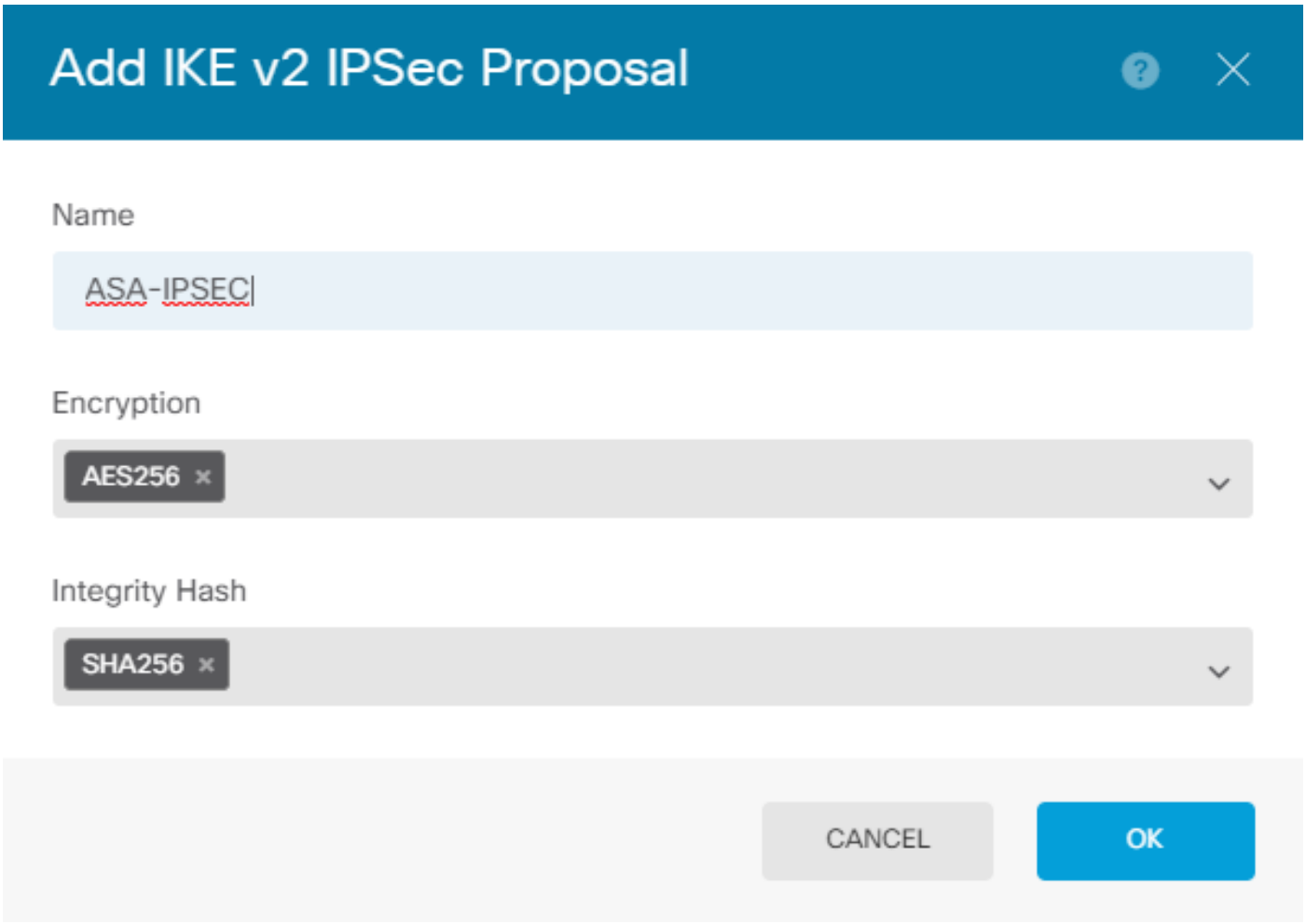
メインページに戻ったら、IPSecプロポーザルのEditボタンを選択します。図に示すように、新しいIPSecプロポーザルを作成します。



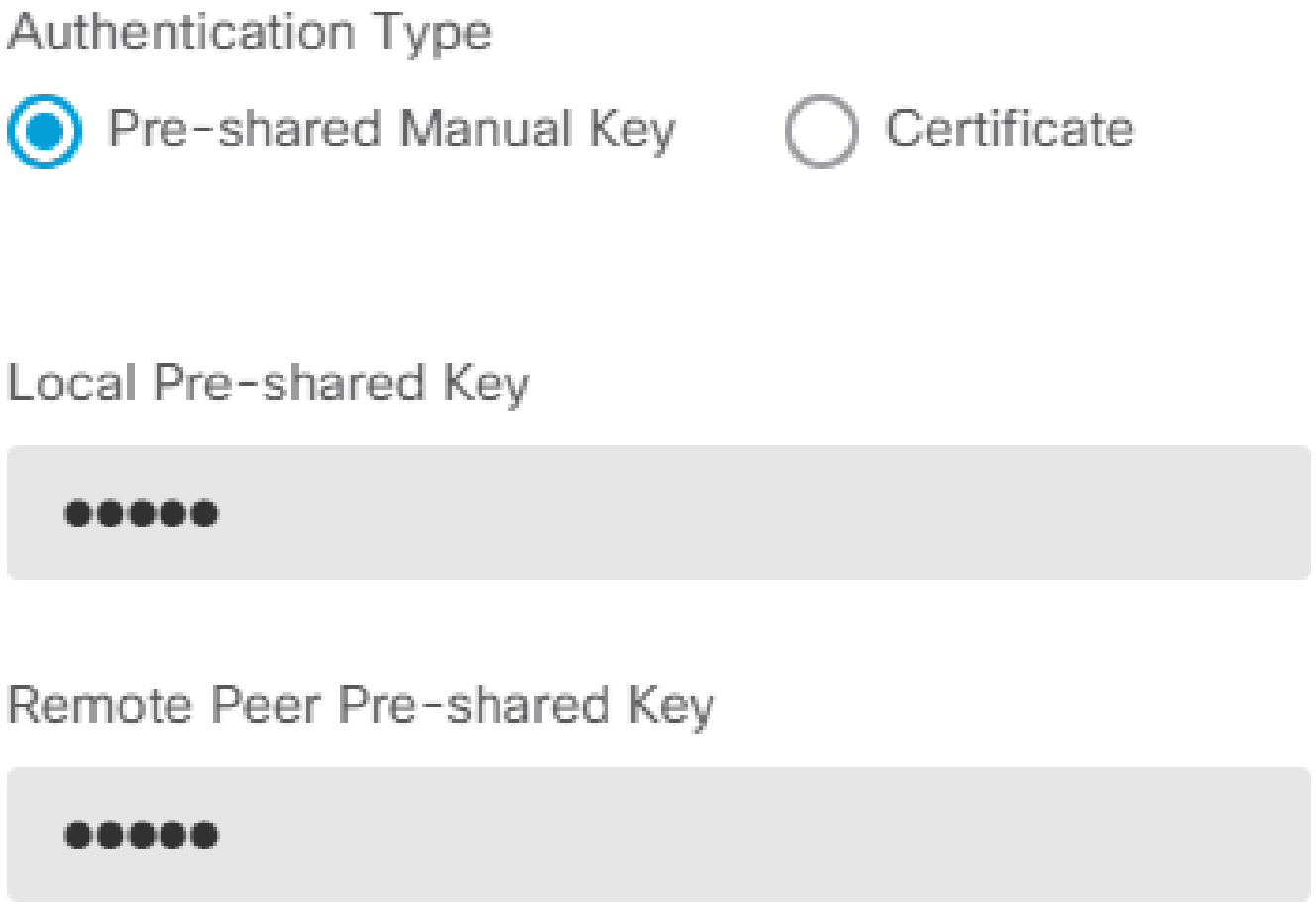
このガイドでは、IPSecに次のパラメータを使用します。

暗号化AES-256

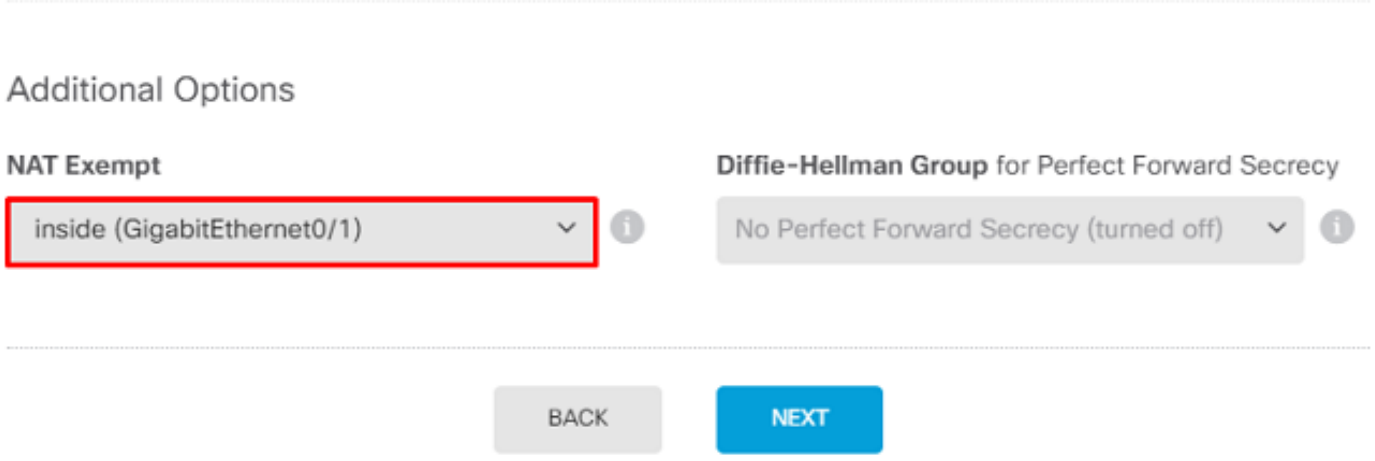
整合性SHA256



認証を事前共有キー(PSK)に設定し、両端で使用される事前共有キー(PSK)を入力します。このガイドでは、図に示すようにCiscoのPSKを使用します。



内部NAT免除インターフェイスを設定します。複数の内部インターフェイスが使用されている場合は、Policies > NATの下に手動のNAT免除ルールを作成する必要があります。



最後のページには、サイト間接続の概要が表示されます。正しいIPアドレスが選択されていることと、適切な暗号化パラメータが使用されていることを確認し、[完了]ボタンをクリックします。

新しいサイト間VPNを導入します。

ASAの設定は、CLIを使用して完了します。

ASA の設定

1. ASAの外部インターフェイスでIKEv2を有効にします。

```
Crypto ikev2 enable outside
```

2. FTDで設定されているのと同じパラメータを定義するIKEv2ポリシーを作成します。

```
Crypto ikev2 policy 1
 Encryption aes-256
 Integrity sha256
 Group 14
 Prf sha256
 Lifetime seconds 86400
```

3. IKEv2プロトコルを許可するグループポリシーを作成します。

```
Group-policy FDM_GP internal
Group-policy FDM_GP attributes
Vpn-tunnel-protocol ikev2
```

4.ピアFTDパブリックIPアドレスのトンネルグループを作成します。グループポリシーを参照し、事前共有キーを指定します。

```
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.暗号化するトラフィックを定義するアクセスリストを作成します(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. FTDで指定されたアルゴリズムを参照するIKEv2 IPsecプロポーザルを作成します。

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

7.設定を結び付けるクリプトマップエントリを作成します。

```
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. VPNトラフィックがファイアウォールによってNAT処理されないようにするNAT免除ステートメントを作成します。

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

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。

VPNトンネル経由でトラフィックを開始してみます。ASAまたはFTDのコマンドラインにアクセスするには、packet tracerコマンドを使用します。packet-tracerコマンドを使用してVPNトンネルを起動する場合、トンネルが起動するかどうかを確認するために、2回実行する必要があります。このコマンドを初めて発行すると、VPNトンネルがダウンするため、packet-tracerコマンドは

VPN encrypt DROPで失敗します。ファイアウォールの内部IPアドレスをパケットトレーサの送信元IPアドレスとして使用しないでください。これは常に失敗します。

```
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
```

トンネルのステータスを監視するには、FTDまたはASAのCLIに移動します。

FTD CLIから、show crypto ikev2 saコマンドを使用してフェーズ1とフェーズ2を確認します。

```
> 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
```

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。

初期接続の問題

VPNを構築する際、トンネルをネゴシエートしている2つの側があります。したがって、あらゆるタイプのトンネル障害をトラブルシューティングする場合は、会話の両側を取得するのが最善です。 IKEv2トンネルのデバッグ方法の詳細については、『IKEv2 VPNのデバッグ方法』を参照してください。

トンネル障害の最も一般的な原因は、接続の問題です。これを判断する最善の方法は、デバイスでパケットキャプチャを取得することです。

デバイスでパケットキャプチャを取得するには、次のコマンドを使用します。

```
Capture capout interface outside match ip host 172.16.100.10 host 192.168.200.10
```

キャプチャが実行されたら、VPN経由でトラフィックを送信し、パケットキャプチャに双方向トラフィックが含まれていないかを確認します。

show cap capoutコマンドを使用して、パケットキャプチャを確認します。

```
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
```

トラフィック固有の問題

ユーザが経験する一般的なトラフィックの問題は次のとおりです。

- FTDのルーティングの問題：内部ネットワークが、割り当てられたIPアドレスとVPNクライアントにパケットをルーティングして戻すことができません。
- トラフィックをブロックするアクセスコントロールリスト。
- ネットワークアドレス変換(NAT)がVPNトラフィックにバイパスされていない。

関連情報

FDMによって管理されるFTD上のサイト間VPNの詳細については、ここから完全な設定ガイドを参照してください。

- FDMで管理されるFTD構成ガイド』を参照してください。

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。