在FDM管理的FTD上配置站點到站點VPN

目錄

簡介

本文檔介紹如何在由FirePower裝置管理器(FDM)管理的Firepower威脅防禦(FTD)上配置站點到站點VPN。

必要條件

需求

思科建議您瞭解以下主題：

- 對VPN有基礎認識
- 使用FDN的經驗
- 使用自適應安全裝置(ASA)命令列體驗

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科FTD 6.5
- ASA 9.10(1)32
- IKEv2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

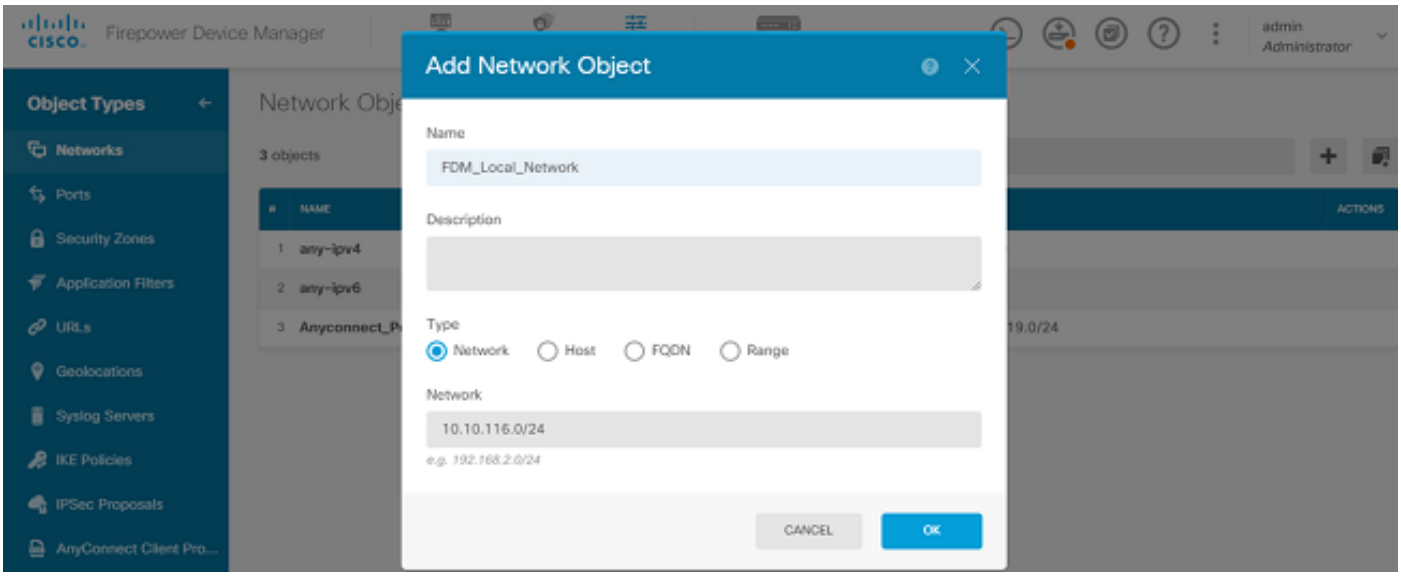
設定

從使用FDM的FTD上的配置開始。

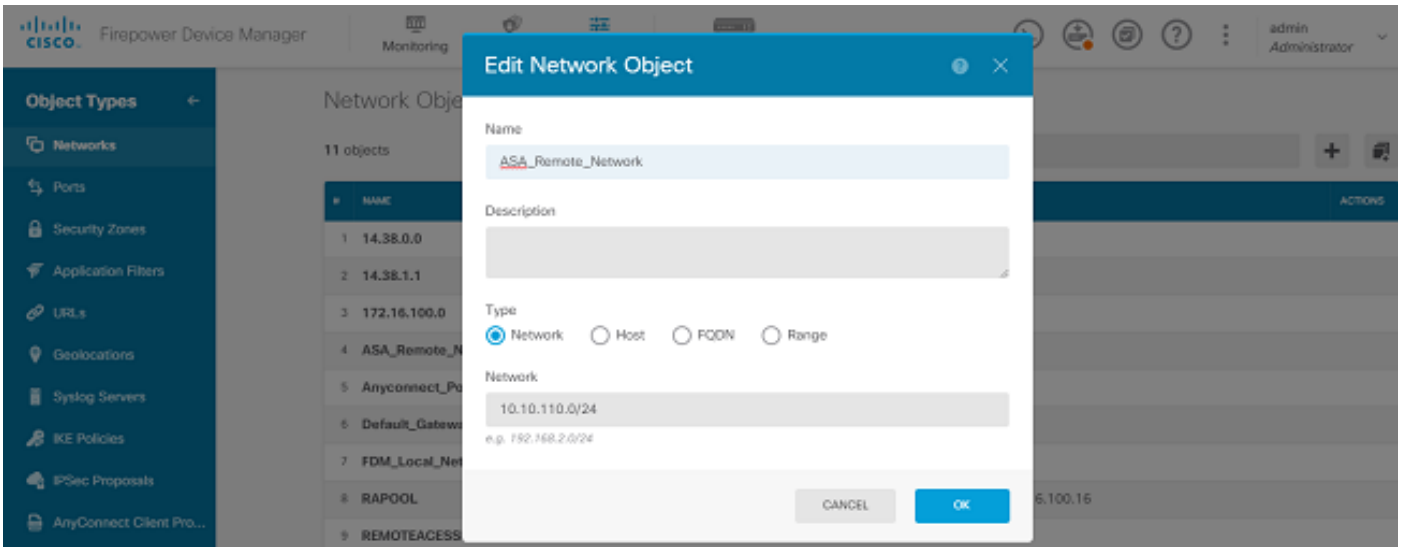
定義受保護的網路

導航到對象>網路>新增新網路。

通過FDM GUI為LAN網路配置對象。在FDM裝置後面為本地網路建立對象，如下圖所示。



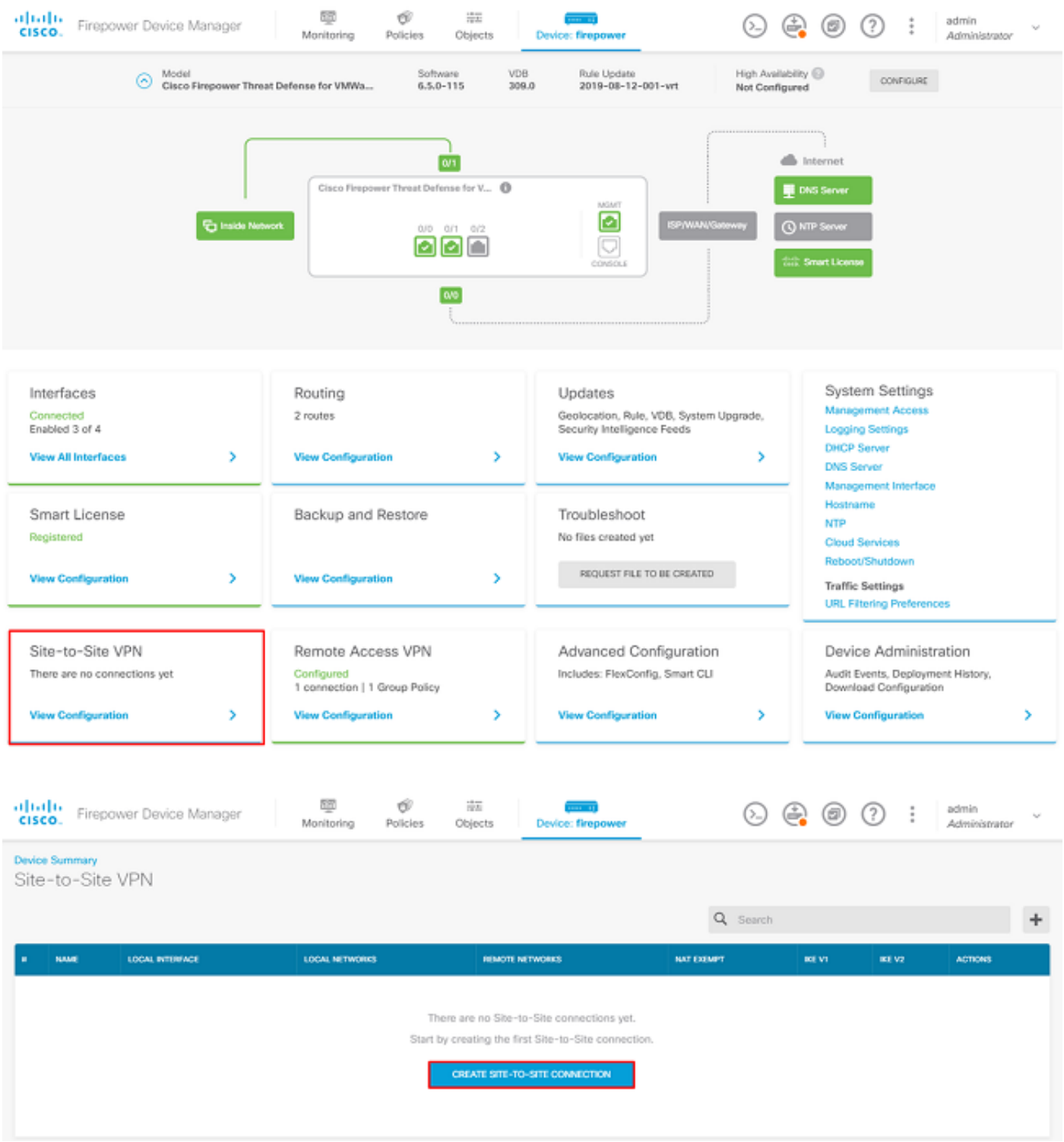
在ASA裝置後面為遠端網路建立一個對象，如下圖所示。



配置站點到站點VPN

導航到站點到站點VPN >建立站點到站點連線。

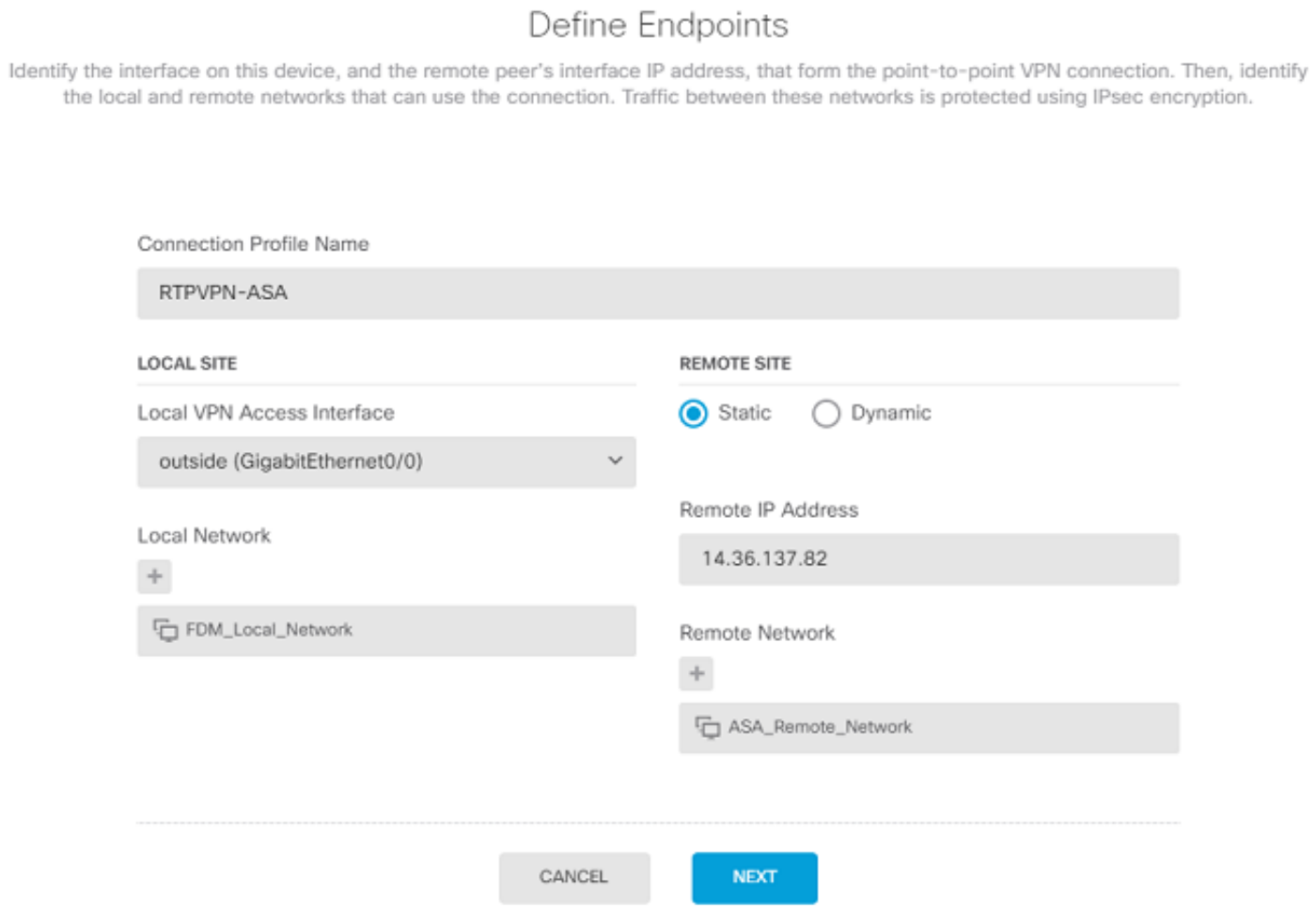
通過FDM上的「站點到站點」嚮導，如下圖所示。



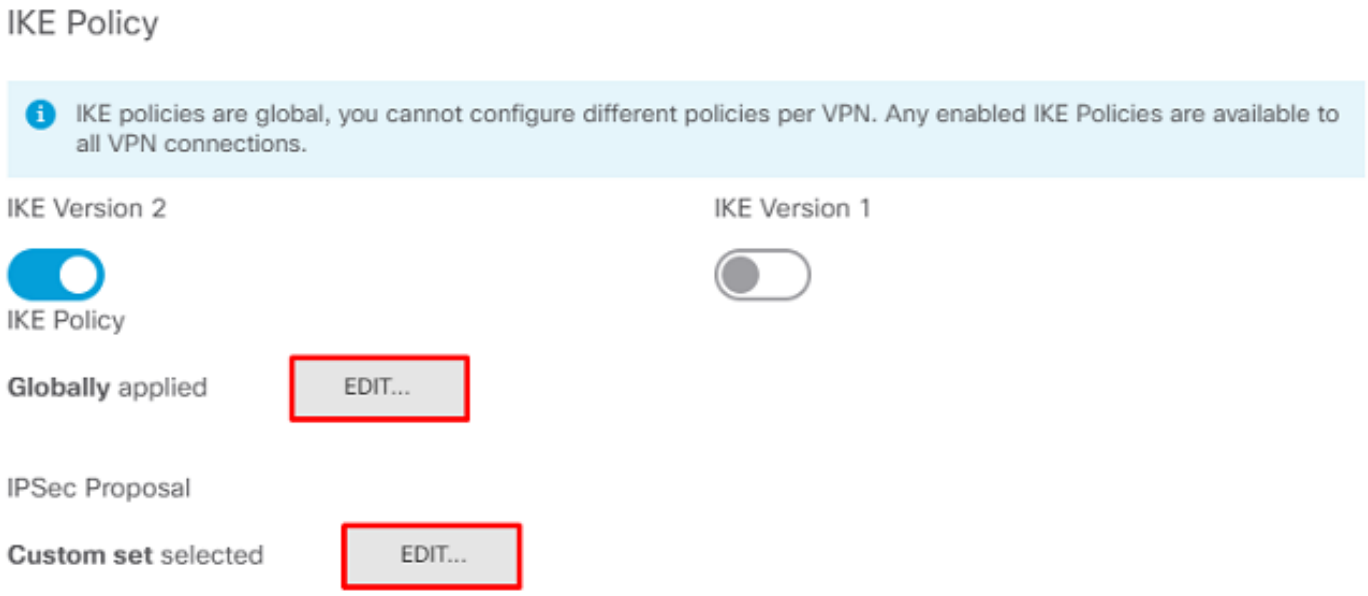
為站點到站點連線提供一個易於識別的連線配置檔名稱。

為FTD選擇正確的外部介面，然後選擇Local network that needs be encrypted through the site to site VPN。

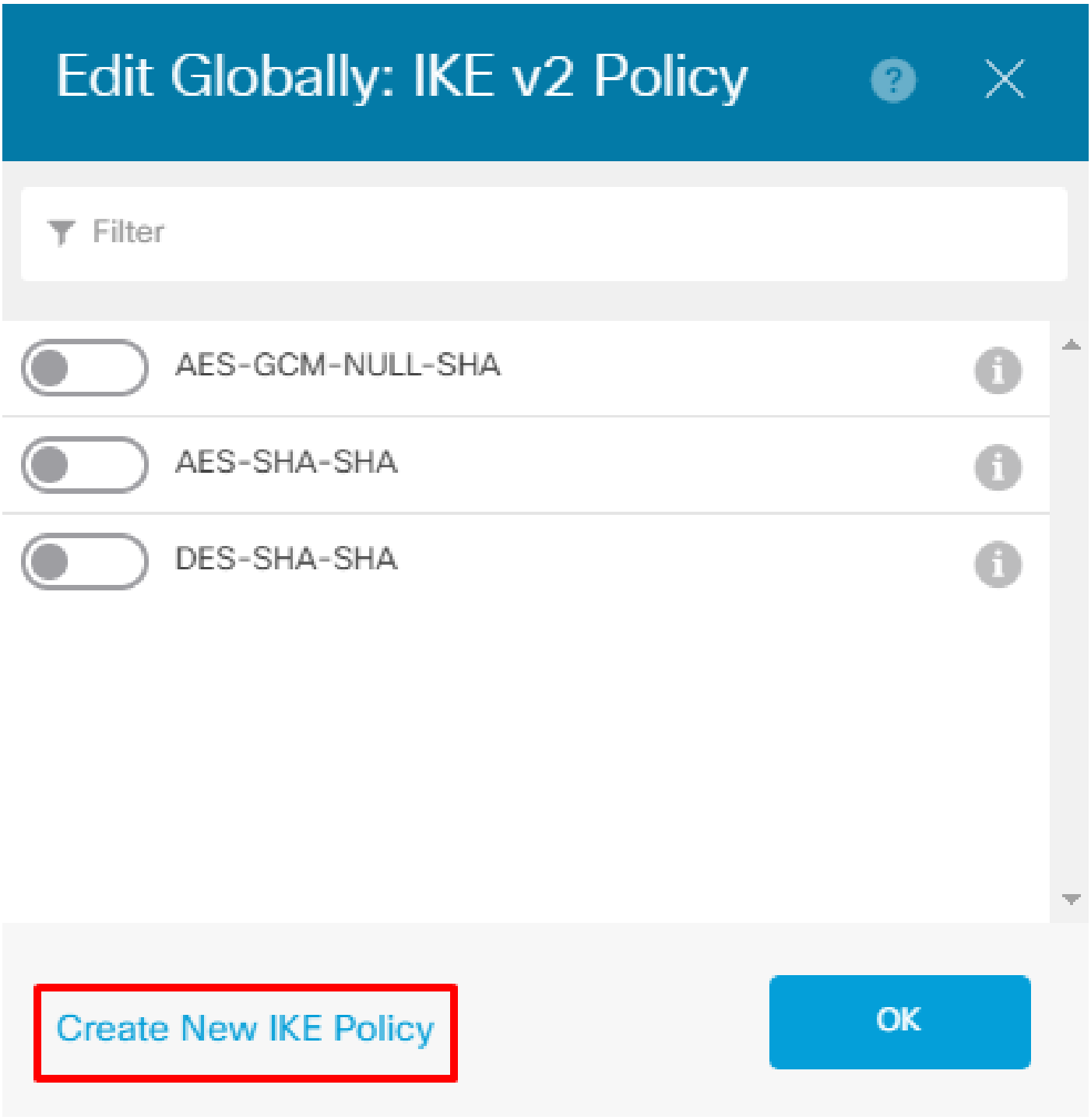
設定遠端對等體的公共介面。然後選擇通過站點到站點VPN加密的遠端對等體的網路，如下圖所示。



在下一頁上，選擇Edit按鈕以設定Internet金鑰交換(IKE)引數，如下圖所示。

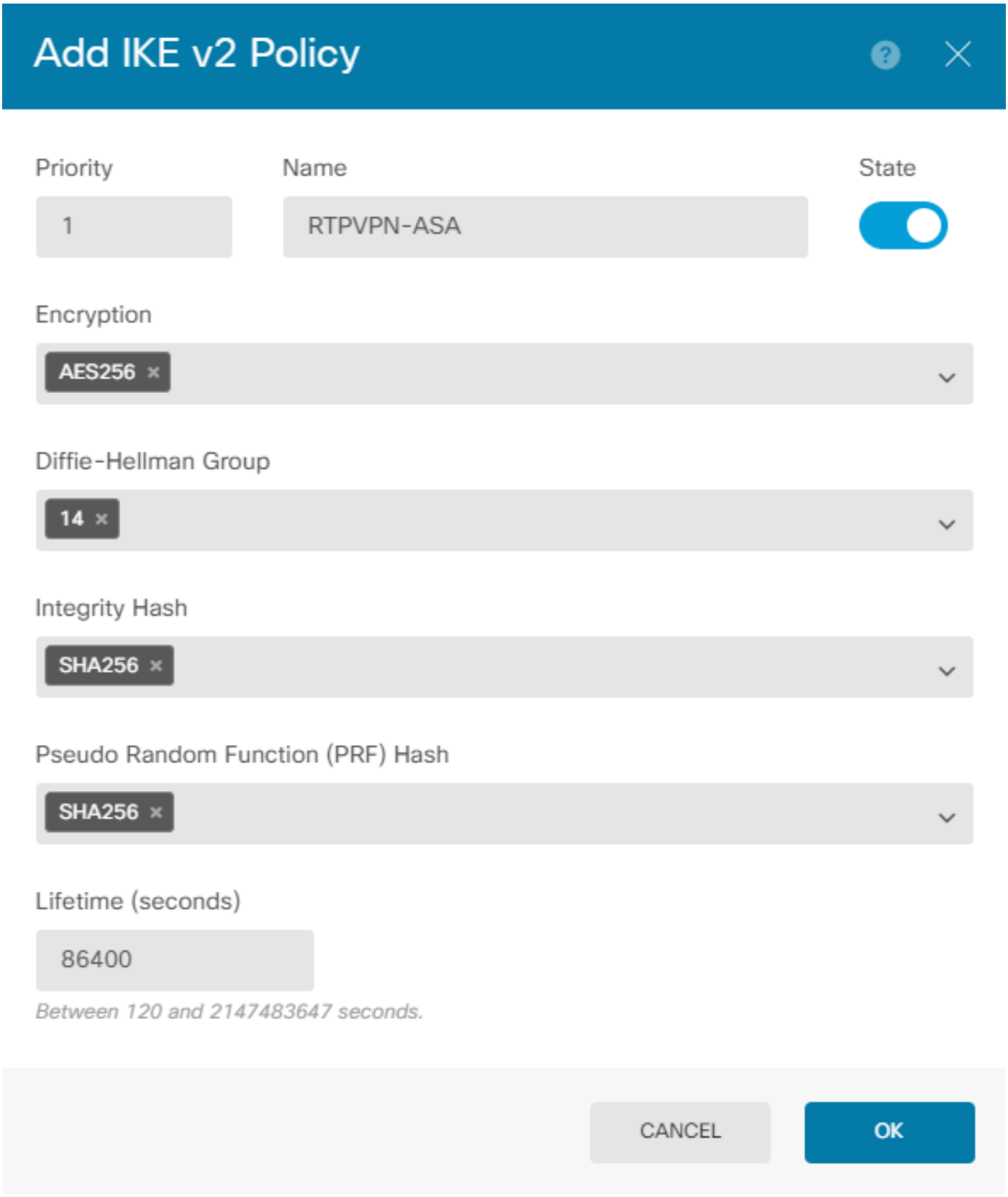


選擇Create New IKE Policy按鈕，如下圖所示。

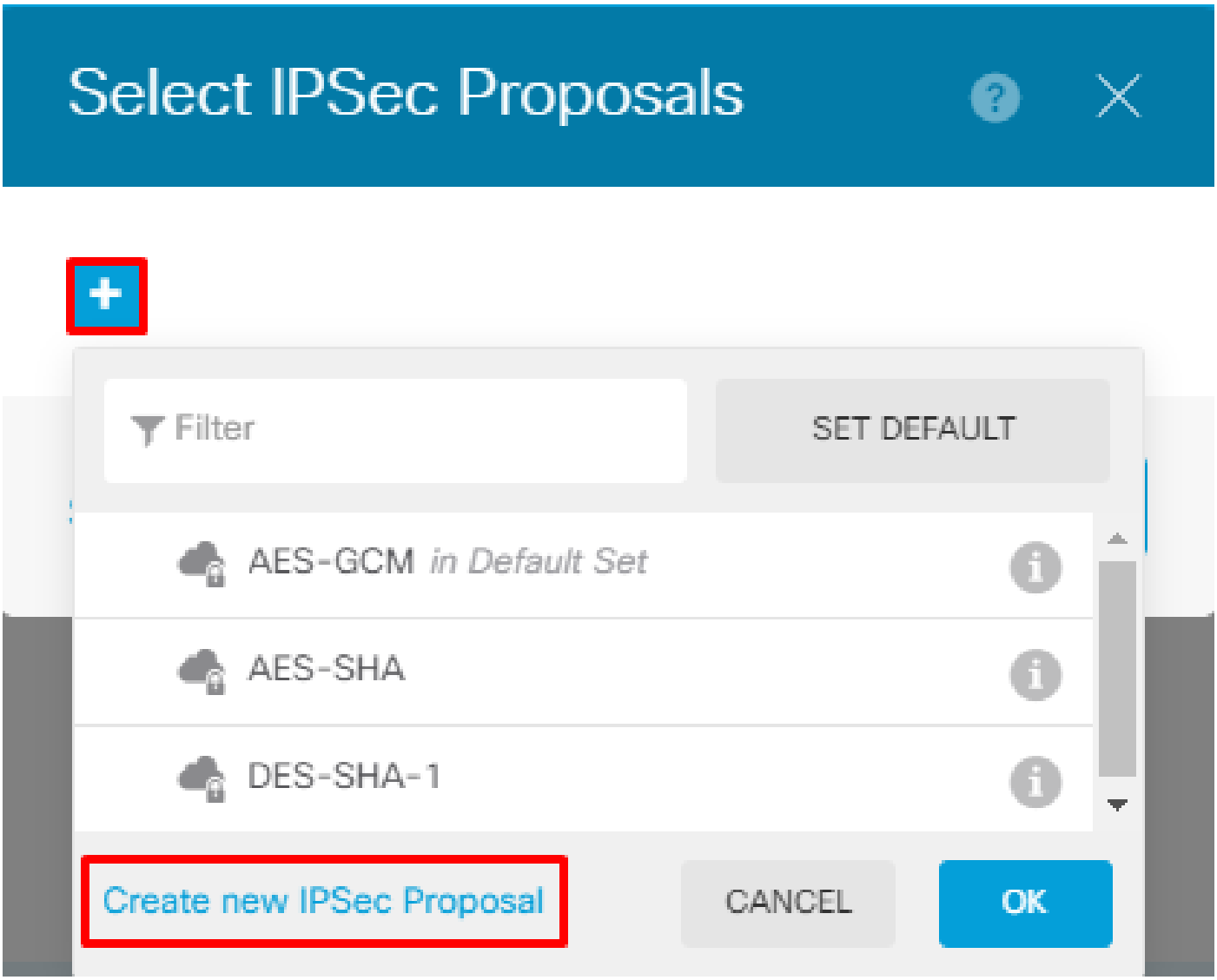


本指南將以下引數用於IKEv2初始交換：

加密AES-256
完整性SHA256
DH組14
PRF SHA256



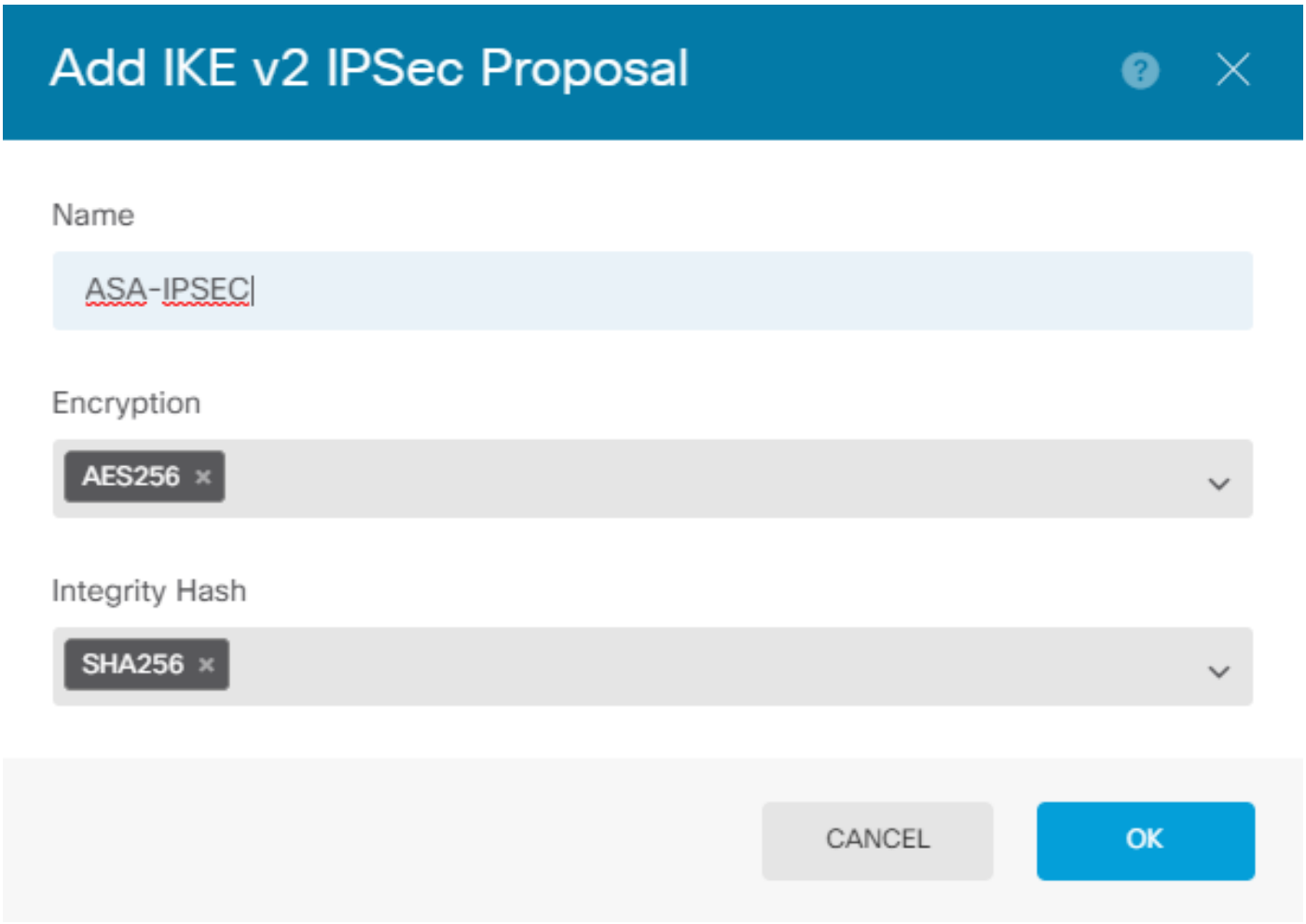
返回首頁後，選擇IPSec建議的Edit按鈕。如圖所示建立新的IPSec建議。



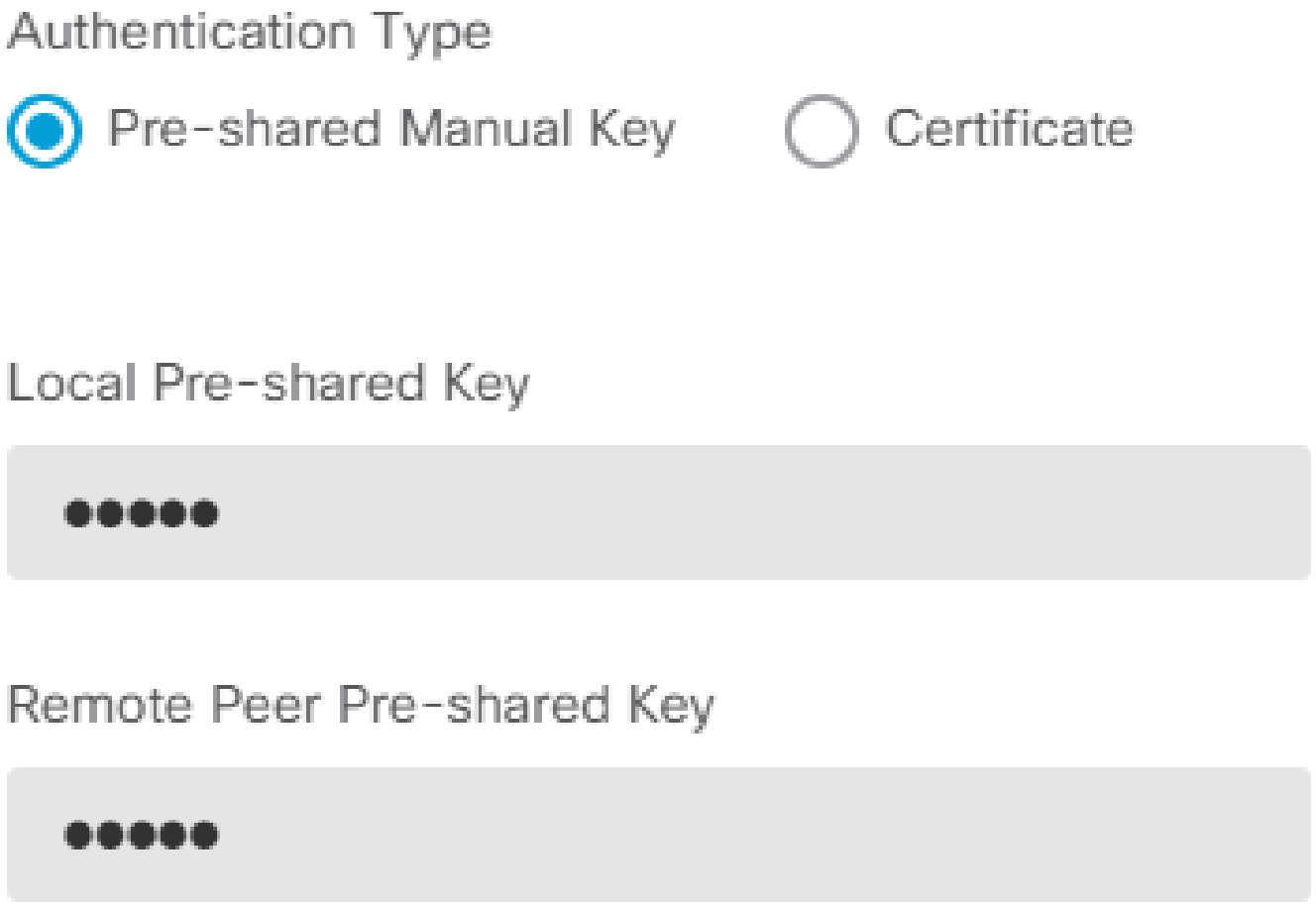
本指南將以下引數用於IPSec:

加密AES-256

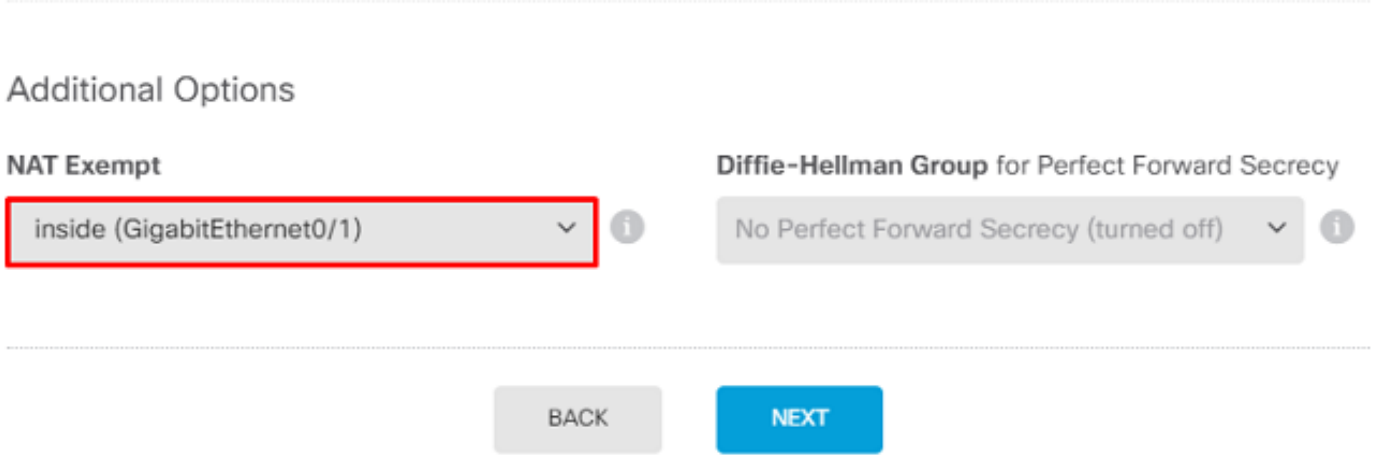
完整性SHA256



將驗證設定為預先共用金鑰，並輸入兩端使用的預先共用金鑰(PSK)。本指南使用思科的PSK，如下圖所示。



設定內部NAT豁免介面。如果使用了多個內部介面，則需要在Policies > NAT下建立手動NAT免除規則。



在最後一頁上，將顯示站點到站點連線的摘要。確保選擇了正確的IP地址，並且使用了正確的加密引數，然後點選「完成」按鈕。 部署新的站點到站點VPN。

使用CLI完成ASA配置。

ASA配置

1. 在ASA的外部介面上啟用IKEv2:

```
Crypto ikev2 enable outside
```

2.建立定義在FTD上配置的相同引數的IKEv2策略：

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

3.建立允許IKEv2協定的組策略：

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

4.為對等FTD公用IP位址建立通道組。引用組策略，並指定預共用金鑰：

```
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.建立定義要加密的流量的訪問清單：(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.建立引用FTD上指定的演算法的IKEv2 IPsec提議：

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

7.建立將配置關聯在一起的加密對映條目：

```
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.建立阻止防火牆NAT的NAT免除語句：

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

驗證

使用本節內容，確認您的組態是否正常運作。

嘗試通過VPN隧道發起流量。通過訪問ASA或FTD的命令列，可以使用packet tracer命令完成此操作。使用packet Tracer命令啟動VPN隧道時，必須運行兩次才能驗證隧道是否啟動。第一次發出該命令時，VPN隧道關閉，因此Packet Tracer命令無法使用VPN encrypt DROP。請勿使用防火牆的內部IP地址作為Packet Tracer中的源IP地址，因為此操作始終失敗。

```
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
```

若要監控通道狀態，請導覽至FTD或ASA的CLI。

在FTD CLI中，使用show crypto ikev2 sa指令驗證第1階段和第2階段。

```
> 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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

初始連線問題

構建VPN時，需要雙方協商隧道。因此，當您排除任何型別的通道故障時，最好讓對話雙方都參與進來。 有關如何調試IKEv2隧道的詳細指南可在此處找到：如何調試IKEv2 VPN

通道故障的最常見原因是連線問題。確定這一點的最佳方法是在裝置上捕獲資料包。

使用以下命令獲取裝置上的資料包捕獲：

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

捕獲到位後，嘗試通過VPN傳送流量，並在資料包捕獲中檢查雙向流量。

使用show cap capout命令檢查資料包捕獲。

```
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
```

流量特定的問題

使用者遇到的常見流量問題包括：

- FTD背後的路由問題 — 內部網路無法將封包路由回指派的IP位址和VPN使用者端。
- 訪問控制清單阻止流量。
- VPN流量不會繞過網路地址轉換(NAT)。

相關資訊

有關由FDM管理的FTD上的點對點VPN的詳細資訊，可在此處找到完整的配置指南。

- 由FDM管理的FTD配置指南。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。