# 配置ASA和FTD之間的IKEv2 IPv6站點到站點隧道

## 目錄



## 簡介

本文檔提供使用Internet金鑰交換版本2(IKEv2)協定在ASA（自適應安全裝置）和FTD（Firepower威脅防禦）之間設定IPv6站點到站點隧道的配置示例。設定包括端到端IPv6網路連線，ASA和FTD作為VPN終端裝置。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- ASA CLI配置基礎知識
- IKEv2和IPSEC協定的基本知識
- 瞭解IPv6編址和路由
- 通過FMC對FTD配置有基礎認識

### 採用元件

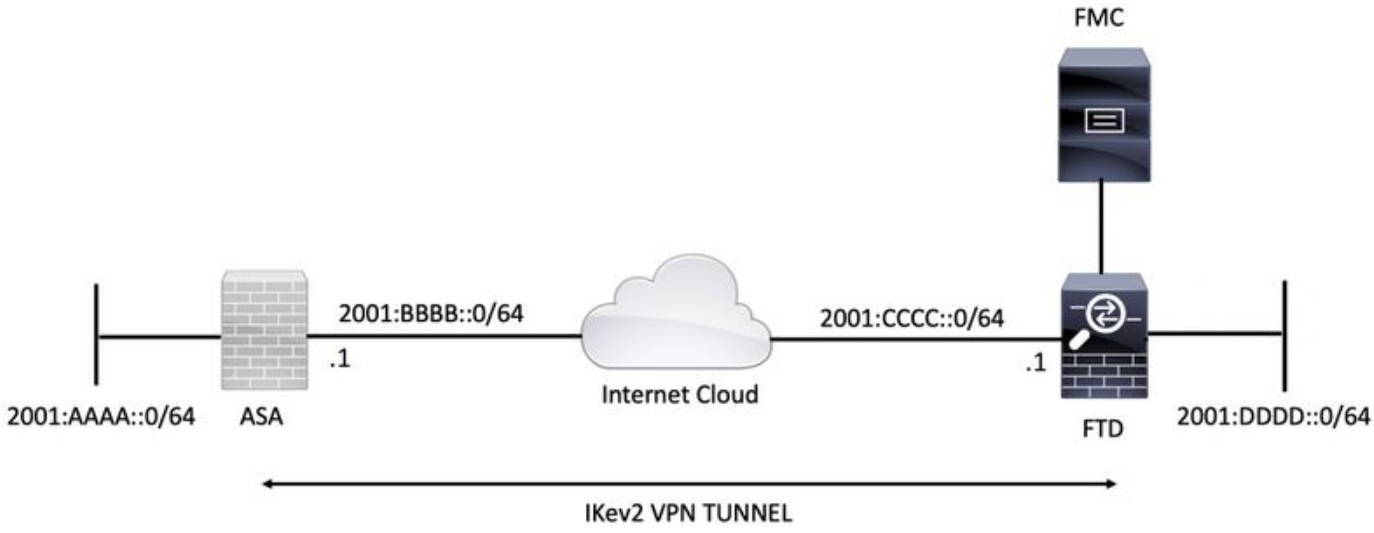
本文中的資訊是根據特定實驗室設定中的裝置所建立的虛擬環境。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在生產中，請確保您已瞭解任何指令可能造成的影響。

本文中的資訊係根據以下軟體和硬體版本：

- 運行9.6.(4)12的Cisco ASAv
- 執行6.5.0的Cisco FTDv
- 執行6.6.0的Cisco FMCv

# 設定

## 網路圖表




## ASA配置

本節介紹ASA上所需的配置。

步驟1.配置ASA介面。

```
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
```

步驟2.設定IPv6預設路由。

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

步驟3.配置IKEv2策略並在外部介面上啟用IKEv2。

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
```

```
group 14
prf sha256
lifetime seconds 86400

crypto ikev2 enable outside
```

步驟4.配置隧道組。

```
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
```

步驟5.建立對象和訪問控制清單(ACL)以匹配所需的流量。

```
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
```

步驟6.為相關流量配置身份網路地址轉換(NAT)規則。

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

步驟7.配置IKEv2 IPSec提議。

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

步驟8.設定加密對映並將其應用於外部介面。

```
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組態

本節提供使用FMC設定FTD的說明。

### 定義VPN拓撲

1.**Devices > VPN > Site To Site**

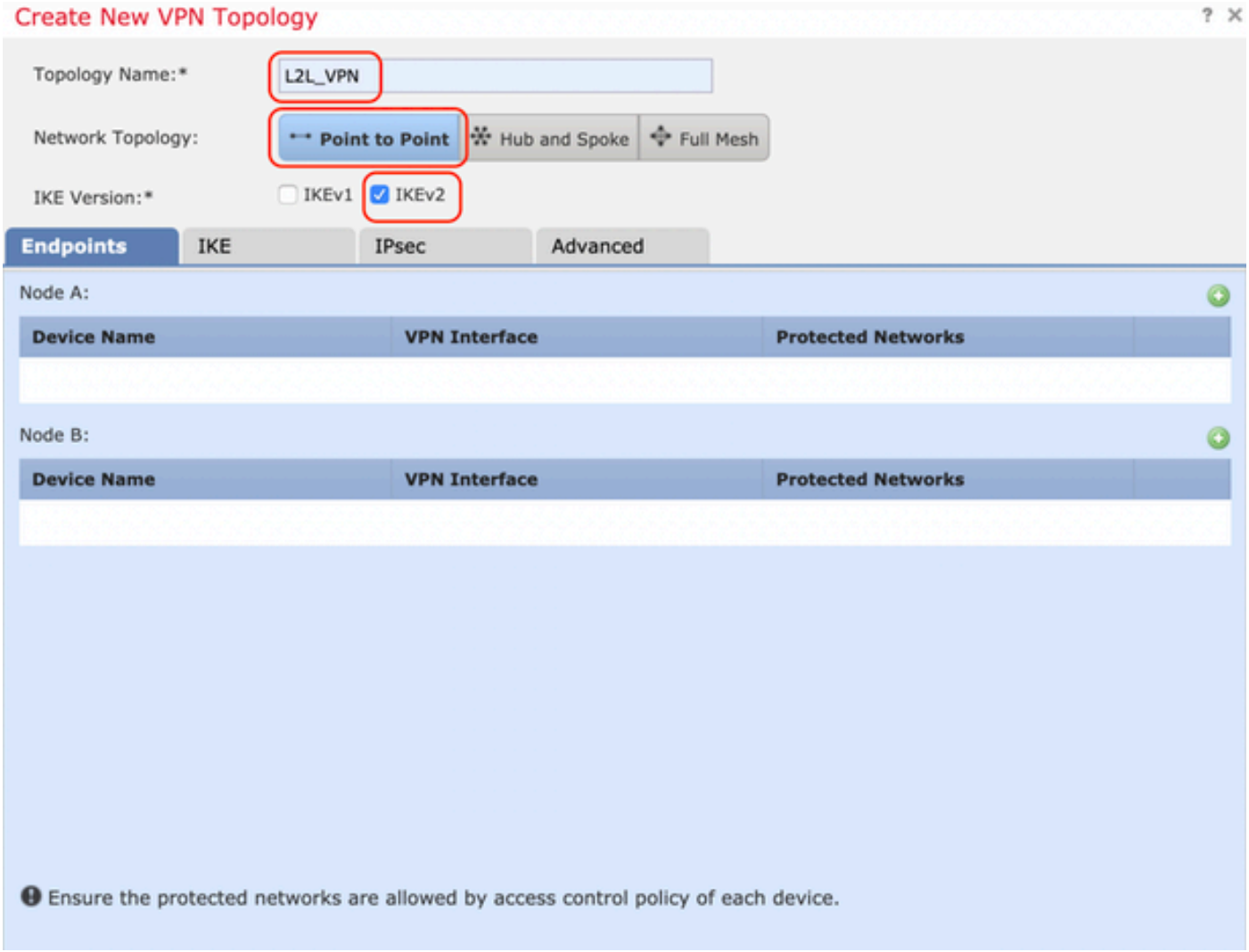
'VPN"Firepower'


步驟2.出現「建立新VPN拓撲」框。為VPN提供一個易於識別的名稱。

網路拓撲：點對點

IKE版本：IKEv2

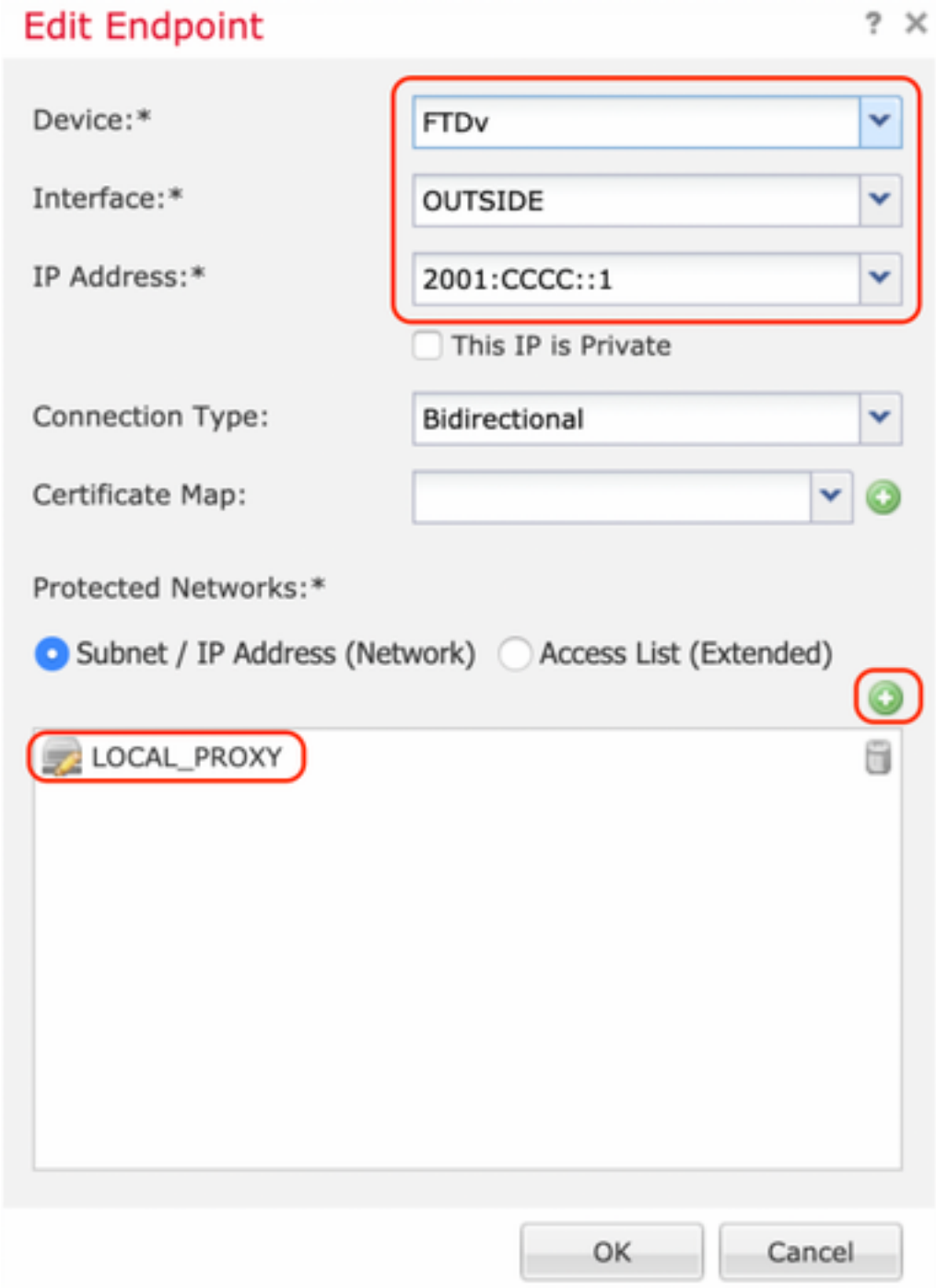
在此範例中，選擇端點Node A時，會顯示FTD。節點B是ASA。按一下綠色加號按鈕將裝置新增到拓撲中。

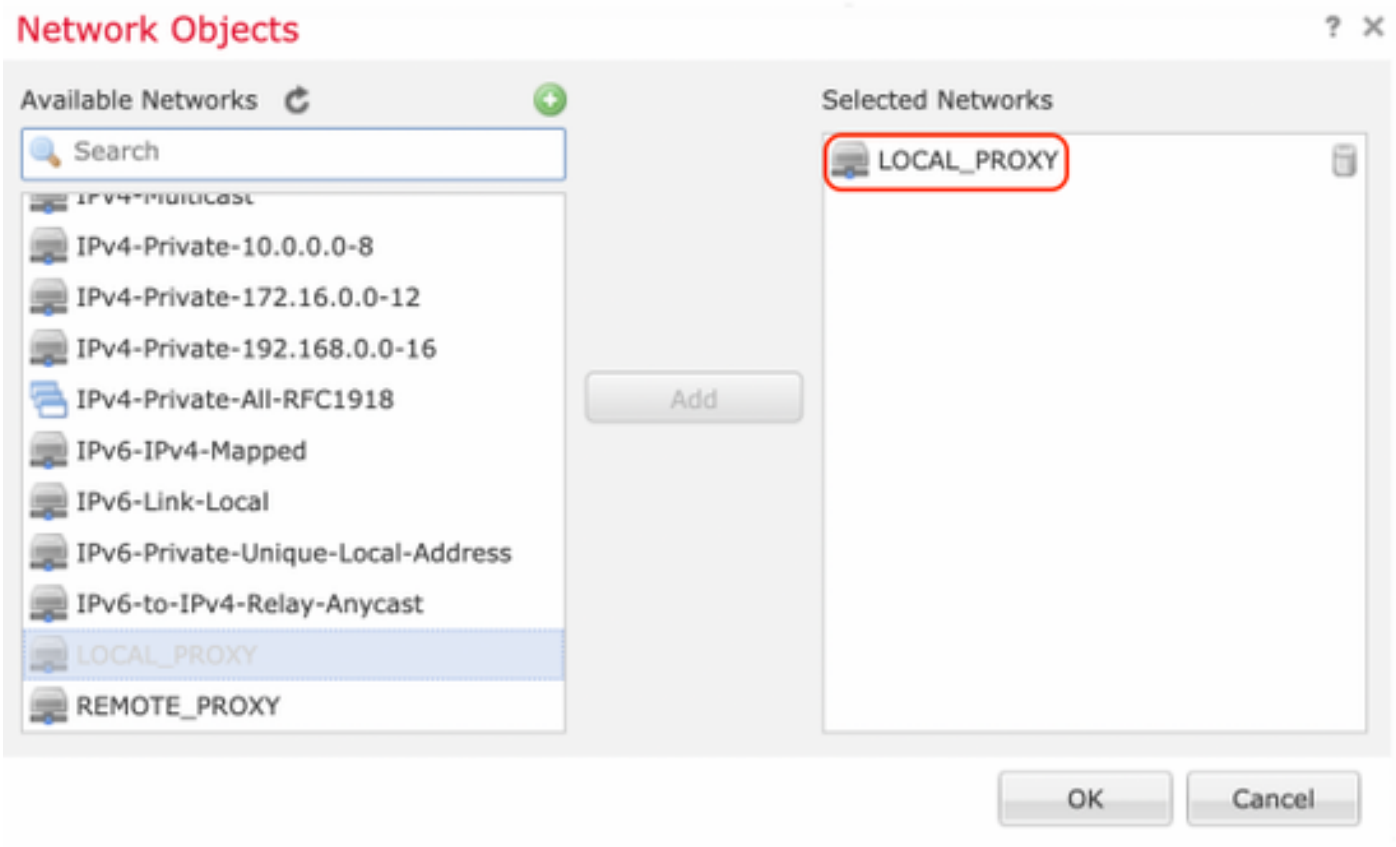



步驟3.將FTD新增為第一個端點。

選擇應用加密對映的介面。IP地址應從裝置配置中自動填充。

點選Protected Networks下的綠色加號圖示，選擇通過此VPN隧道加密的子網。在本示例中，FMC上的「本地代理」網路對象由IPv6子網「2001:DDD::/64」組成。

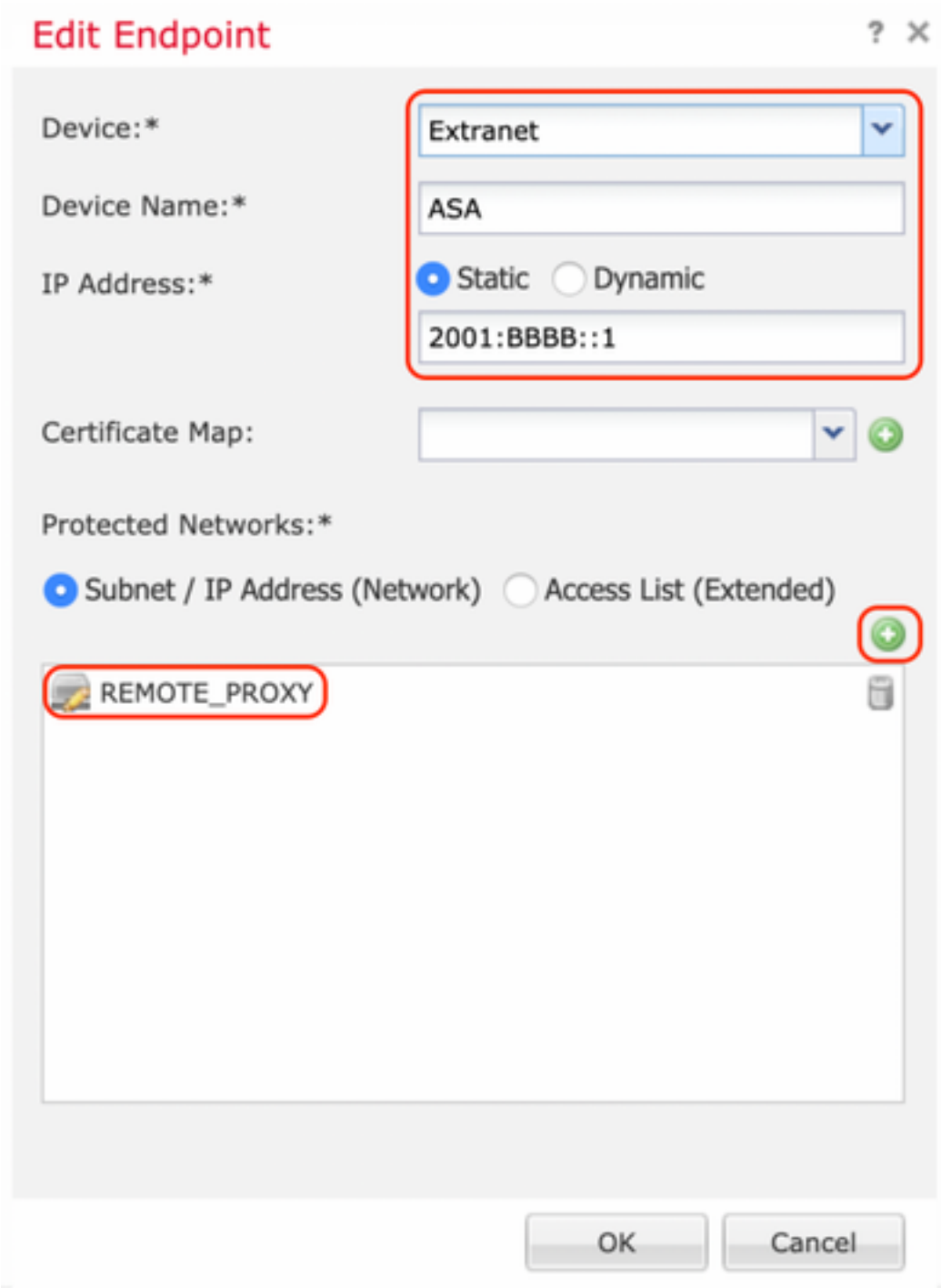

Edit Endpoint
Device:*
FTDv
Interface:*
OUTSIDE
IP Address:*
2001:CCCC::1
This IP is Private
Connection Type:
Bidirectional
Certificate Map:
Protected Networks:*
Subnet / IP Address (Network)
Access List (Extended)
LOCAL_PROXY
OK
Cancel




完成上述步驟後，FTD終端配置完成。

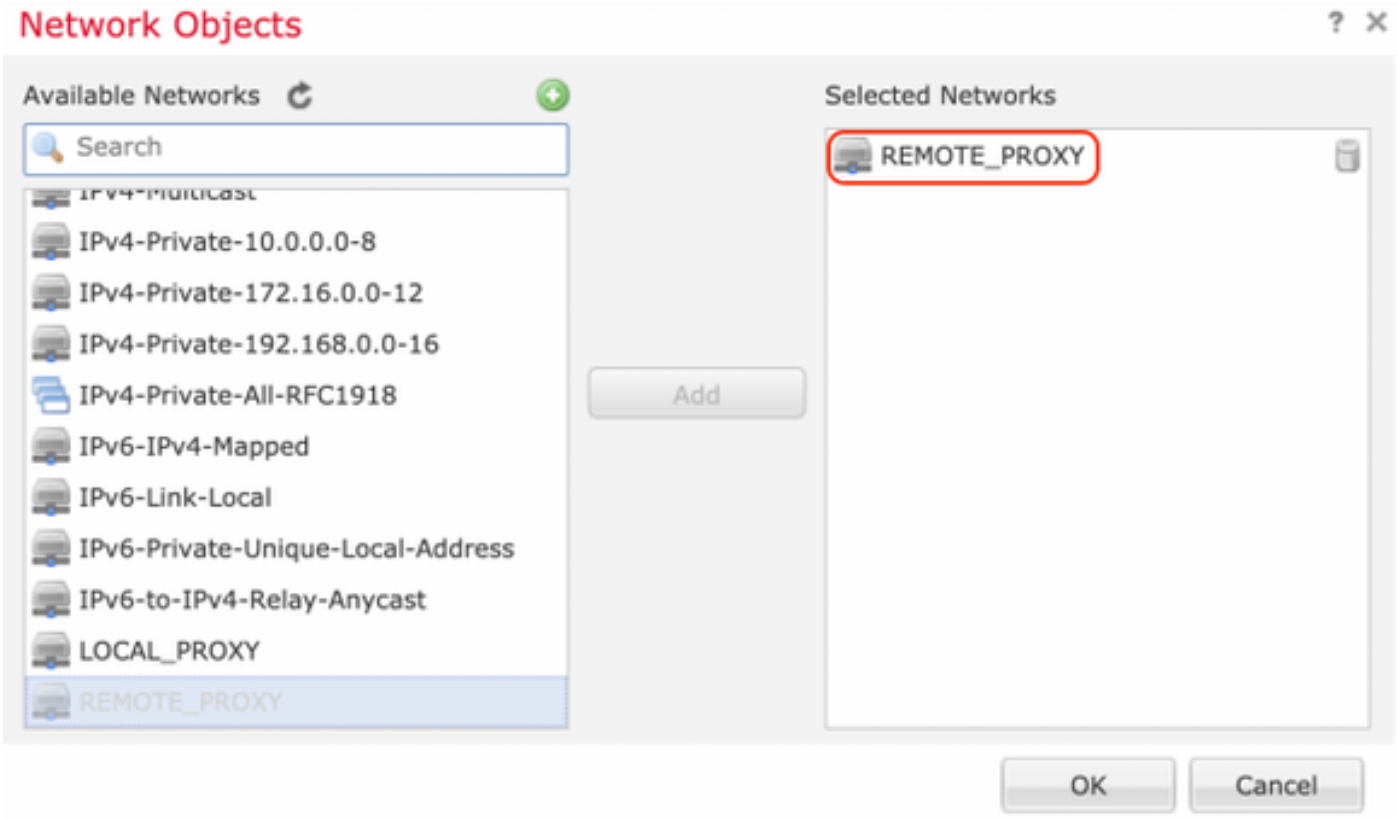
步驟4.點選配置示例中作為ASA的節點B的綠色加號圖示。不受FMC管理的裝置被視為外聯網裝置。新增裝置名稱和IP地址。

步驟5.選擇綠色的加號圖示以新增受保護的網路。



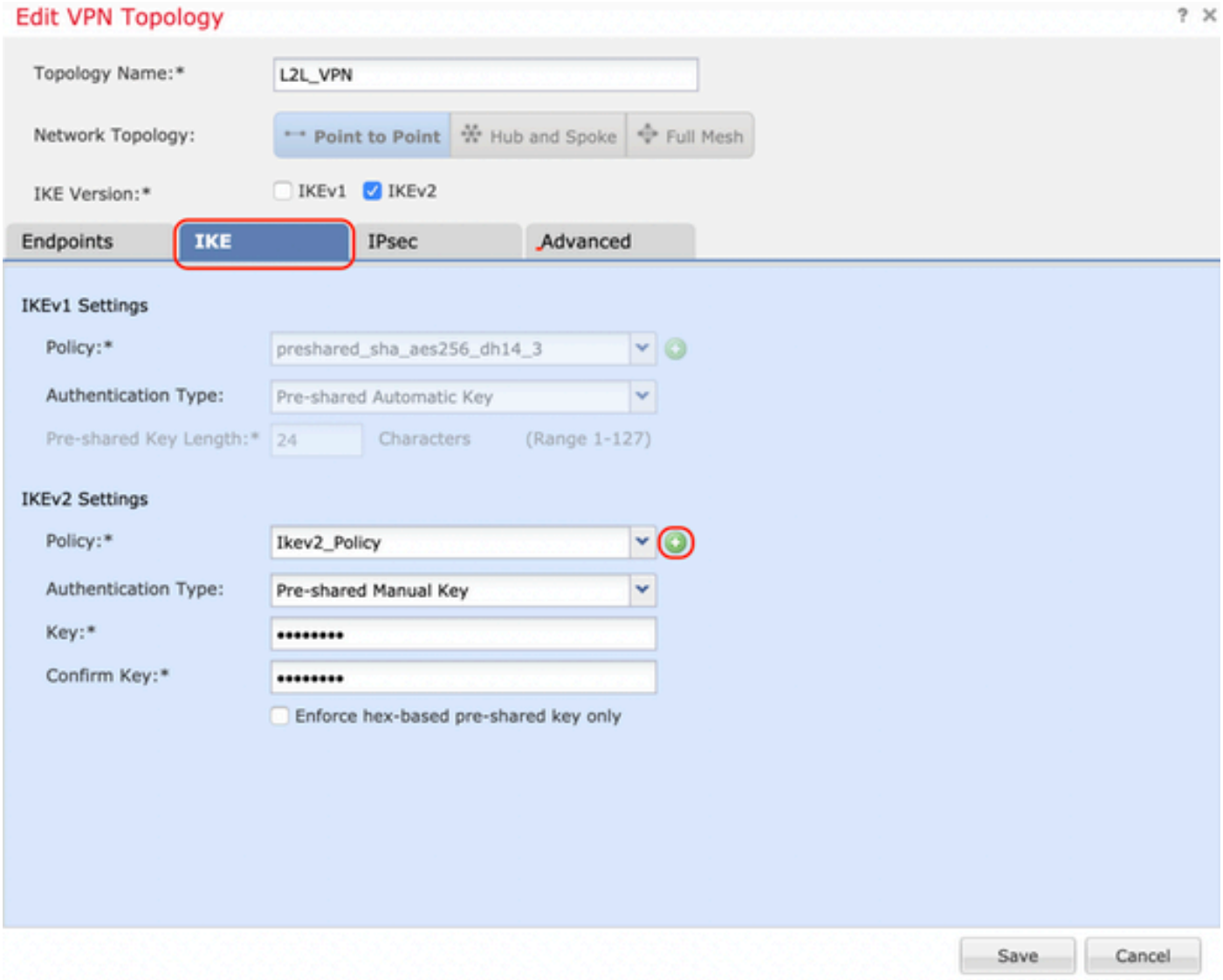

步驟6.選擇需要加密的ASA子網並將其新增到所選網路。

在本例中，「Remote Proxy」是ASA子網「2001:AAAA::/64」。




**配置IKE引數**

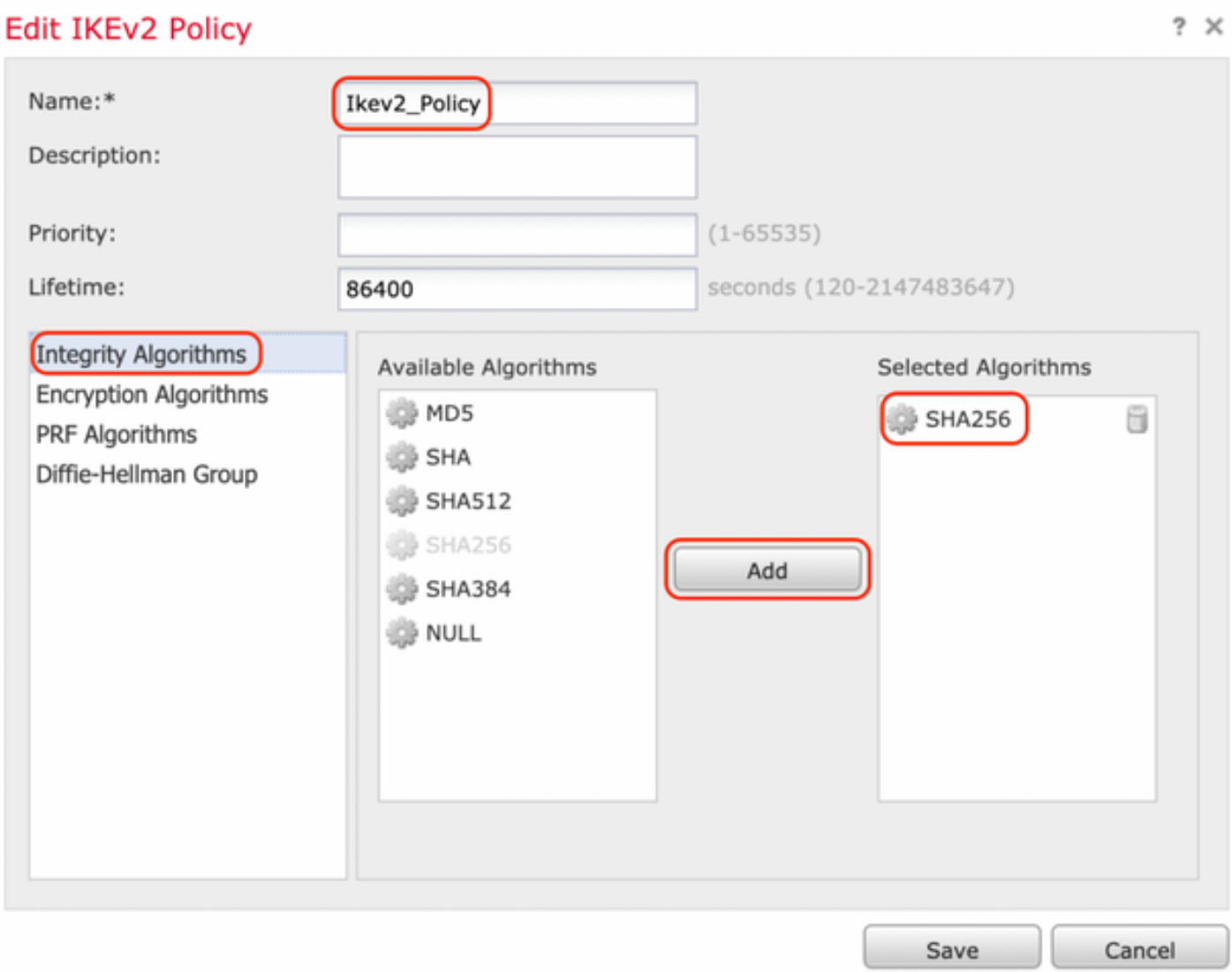
步驟1.在IKE頁籤下，指定要用於IKEv2初始交換的引數。按一下綠色加號圖示可建立新的IKE策略。

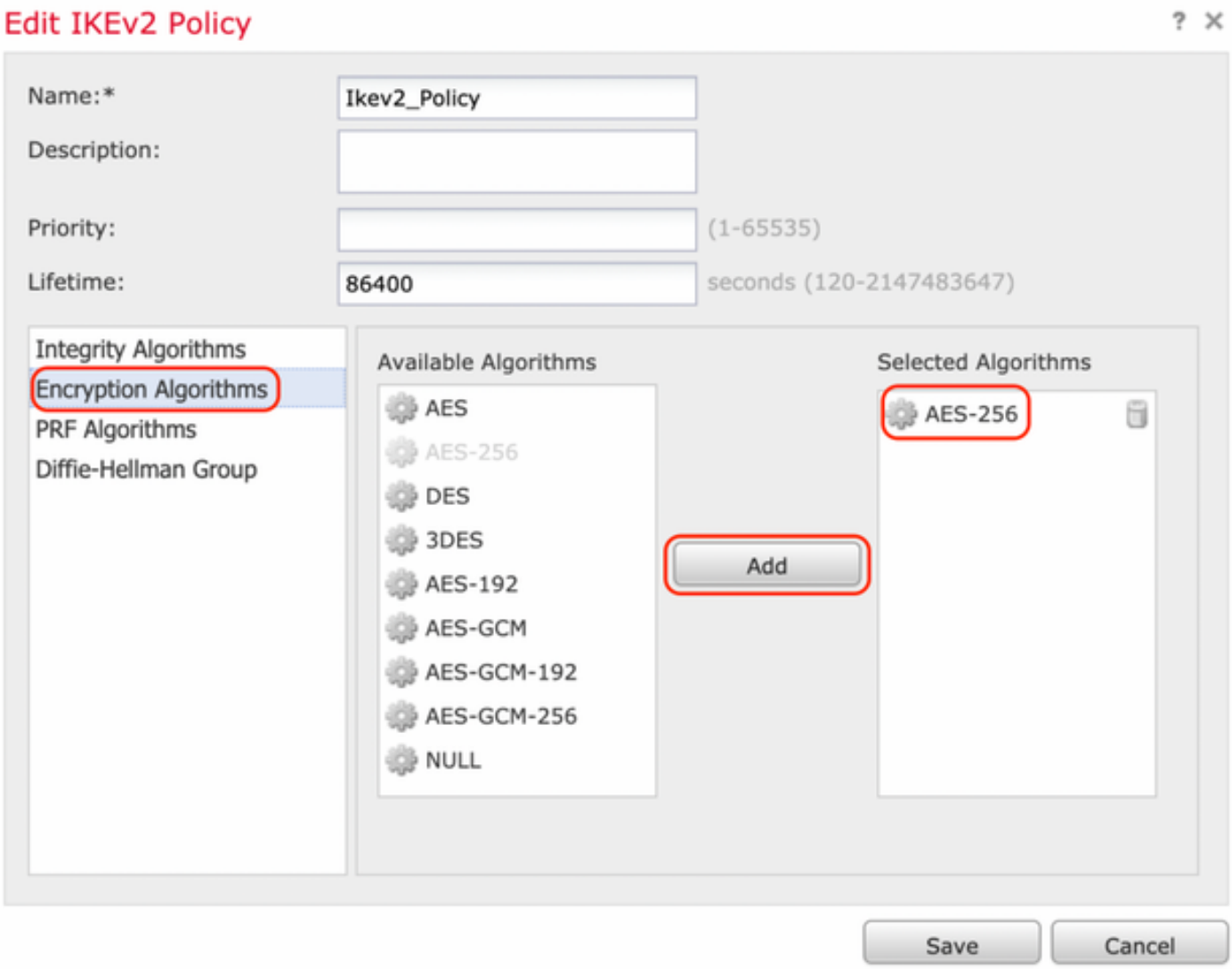


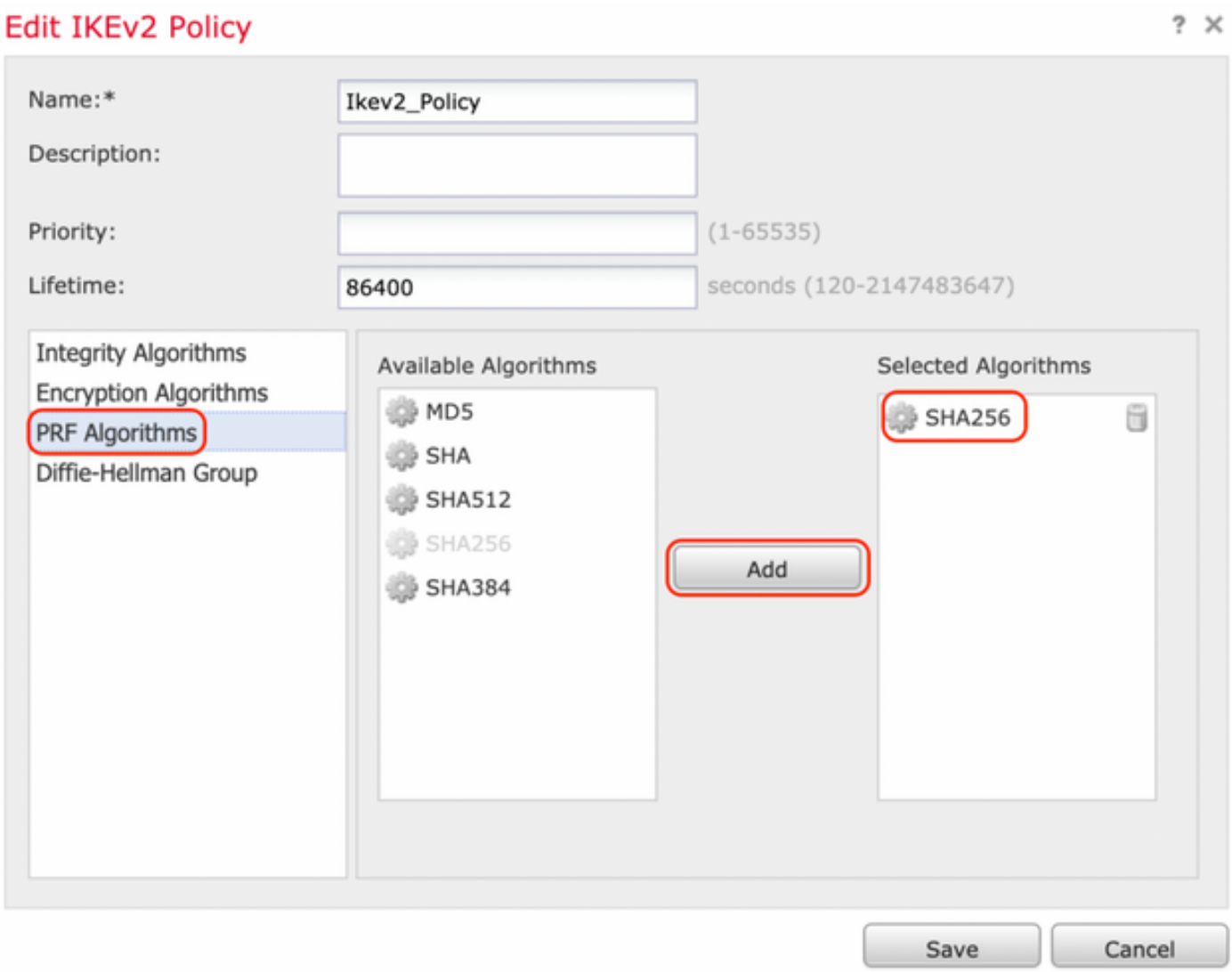

步驟2.在新的IKE策略中，指定連線的優先順序編號和階段1的生存期。本指南在初始交換中使用以下引數：
完整性(SHA256)、
加密(AES-256)、
PRF(SHA256)和
Diffie-Hellman群組（群組14）。

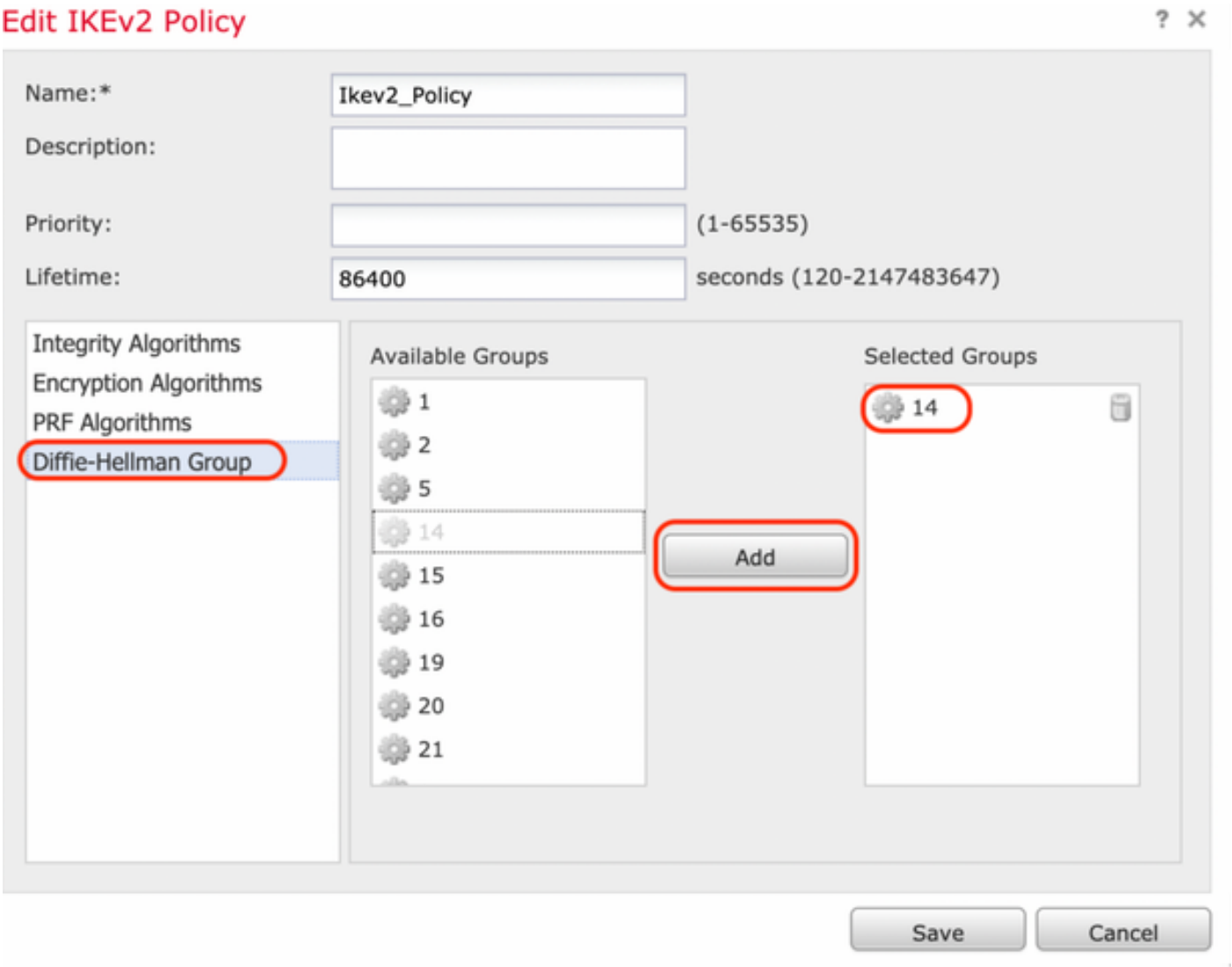
無論所選策略部分中有什麼，裝置上的所有IKE策略都將傳送到遠端對等裝置。將為VPN連線選擇第一個遠端對等體匹配項。

[可選]使用優先順序欄位選擇首先傳送的策略。首先傳送優先順序1。


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

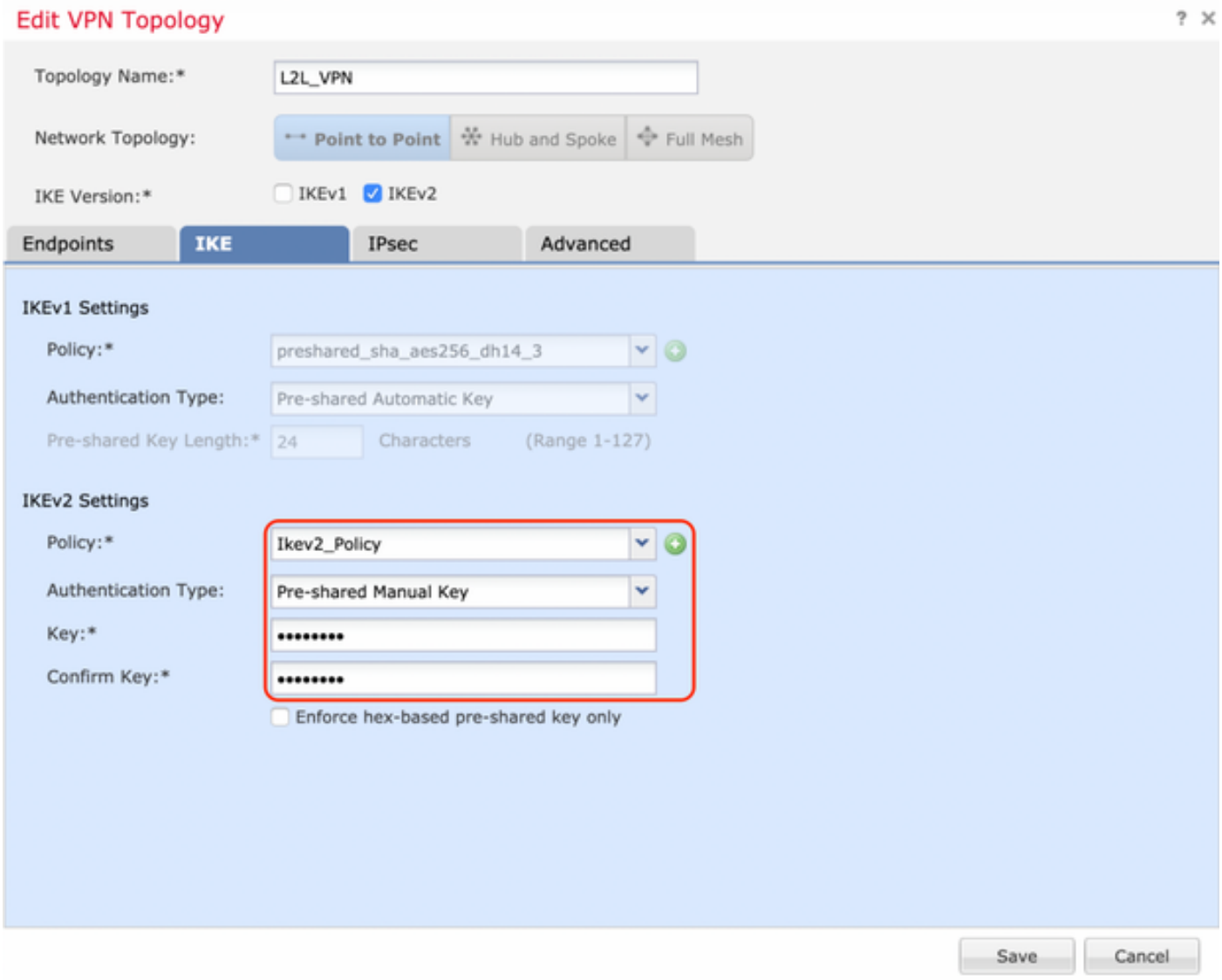

Edit IKEv2 Policy
Name:*
Ikev2_Policy
Description:
Priority:
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
AES
AES-256
DES
3DES
AES-192
AES-GCM
AES-GCM-192
AES-GCM-256
NULL
Add
Selected Algorithms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



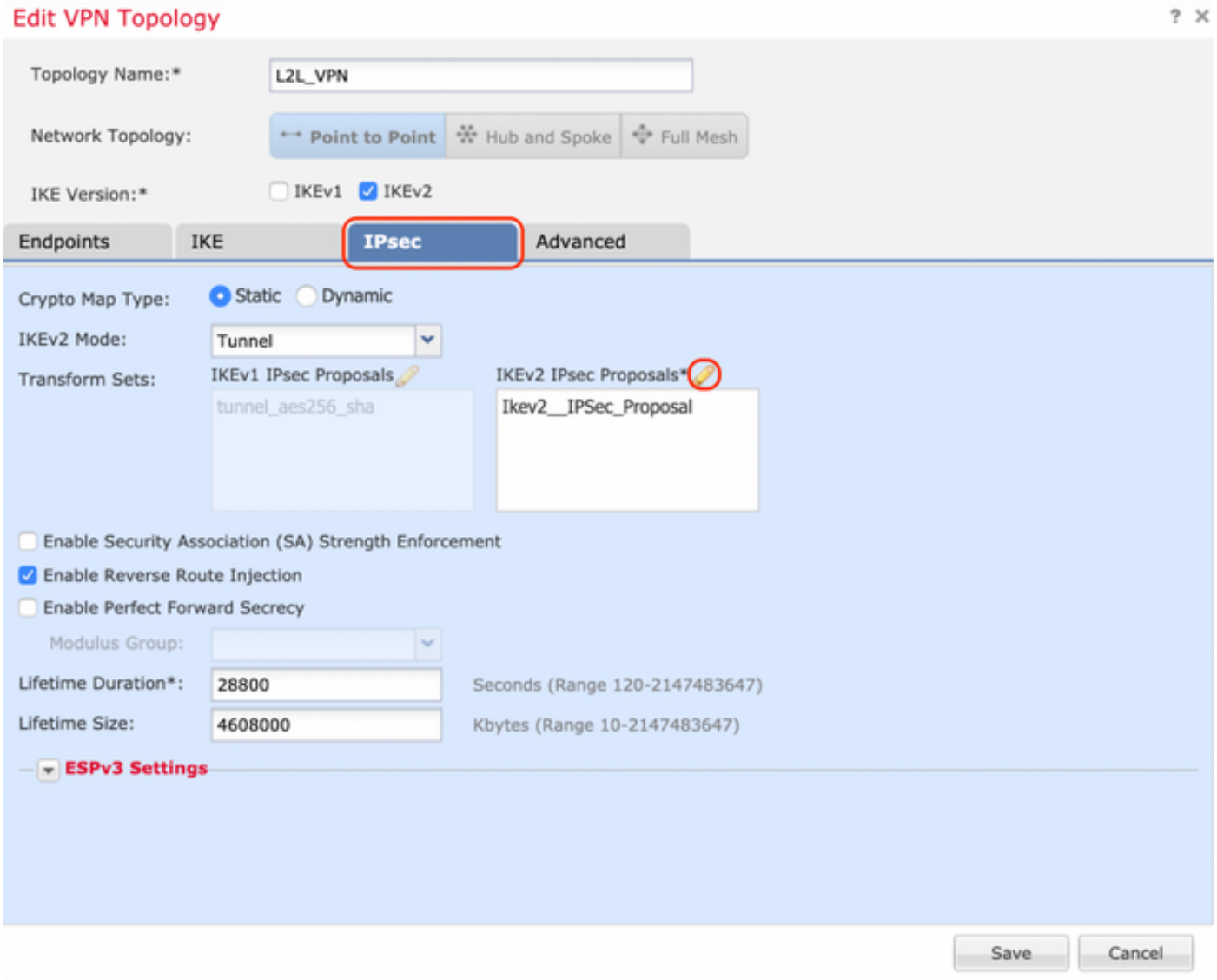

步驟3.新增引數後，選擇上述配置的策略，然後選擇身份驗證型別。

選擇預共用手動金鑰選項。在本指南中，使用預共用金鑰「cisco123」。




## 配置IPSEC引數

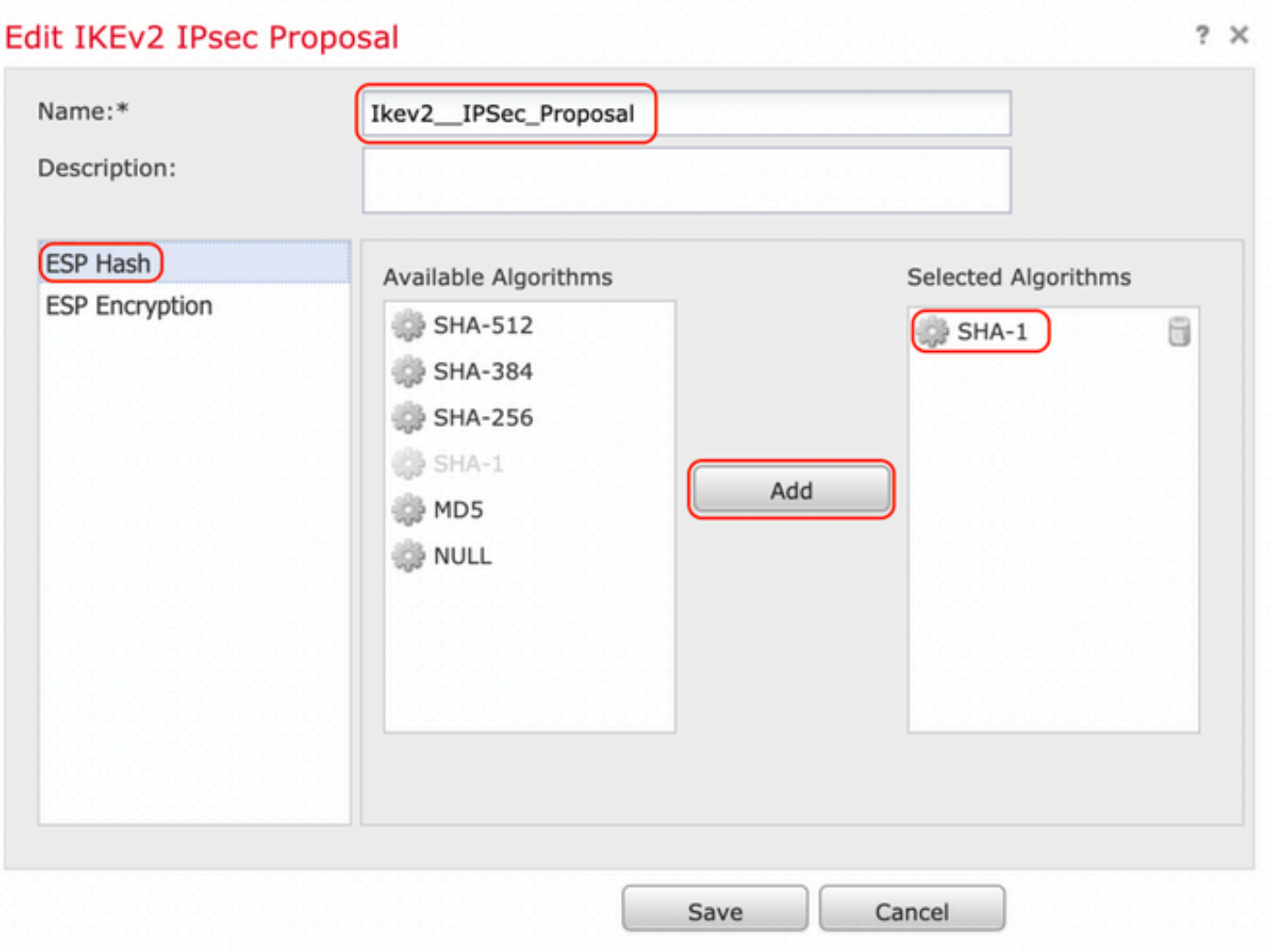
1.IPsecIPsec

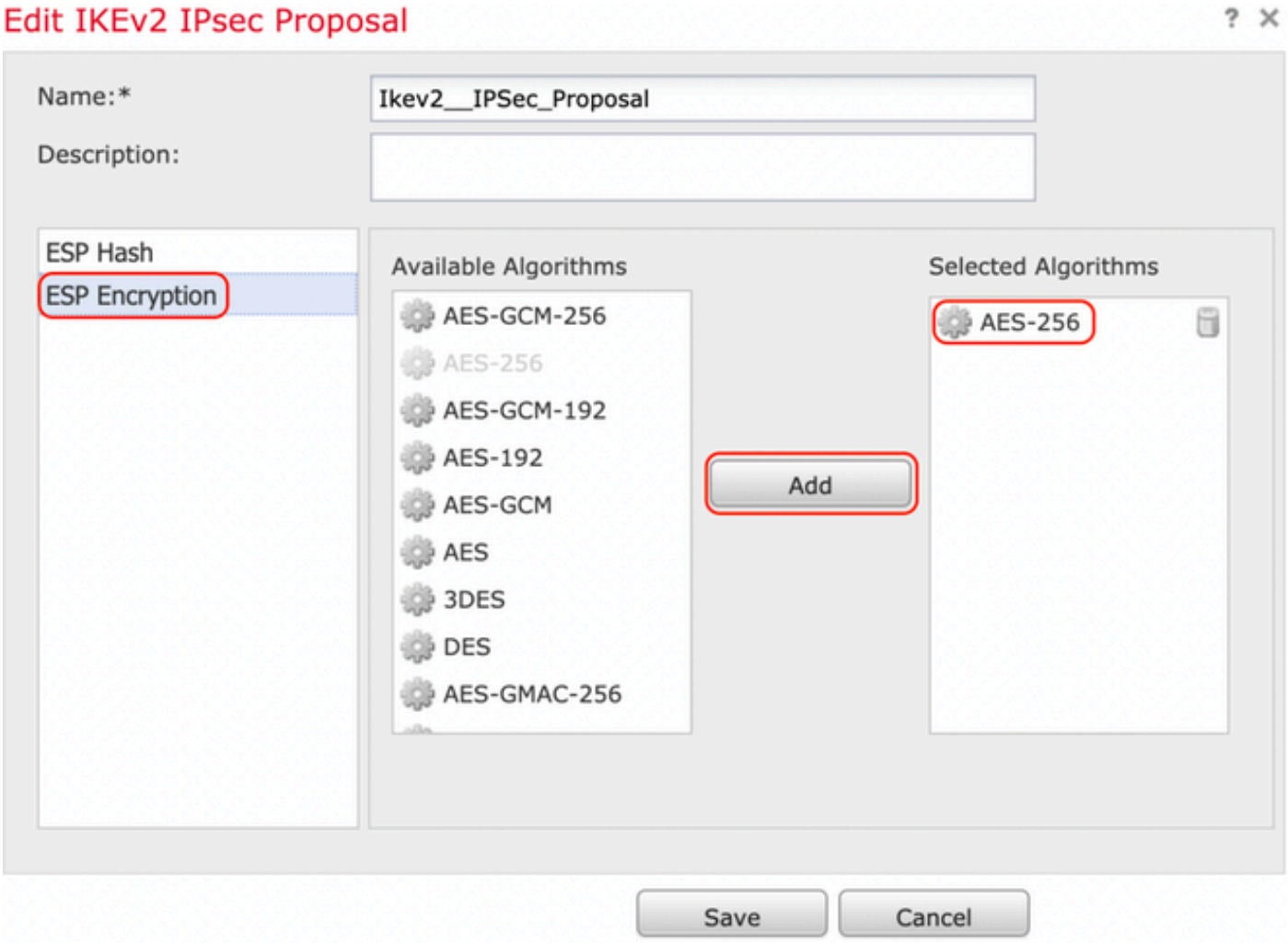



步驟2.通過選擇綠色加號圖示並輸入階段2引數，建立新的IKEv2 IPsec提議，如下所示：

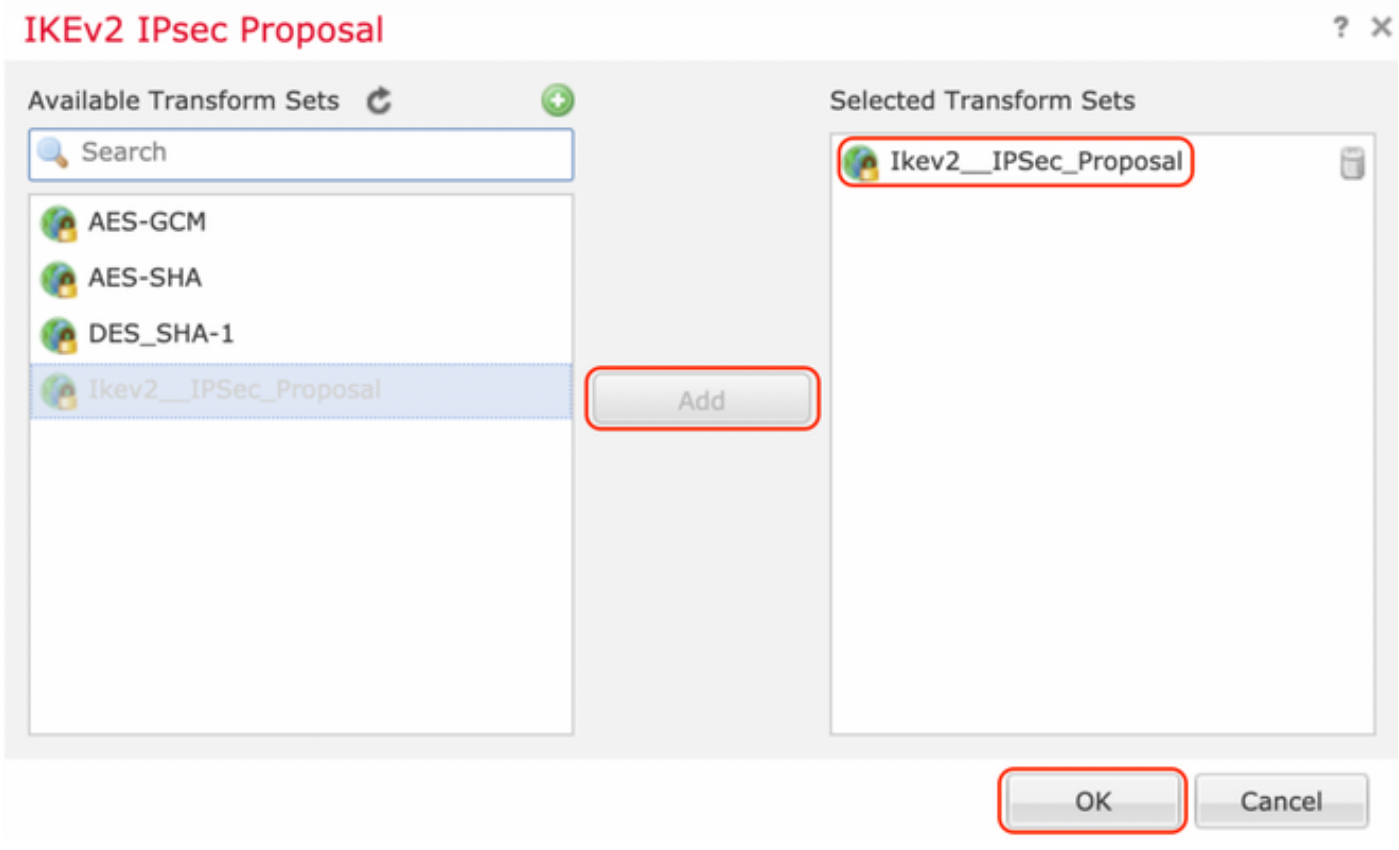
ESP雜湊：SHA-1

ESP加密：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

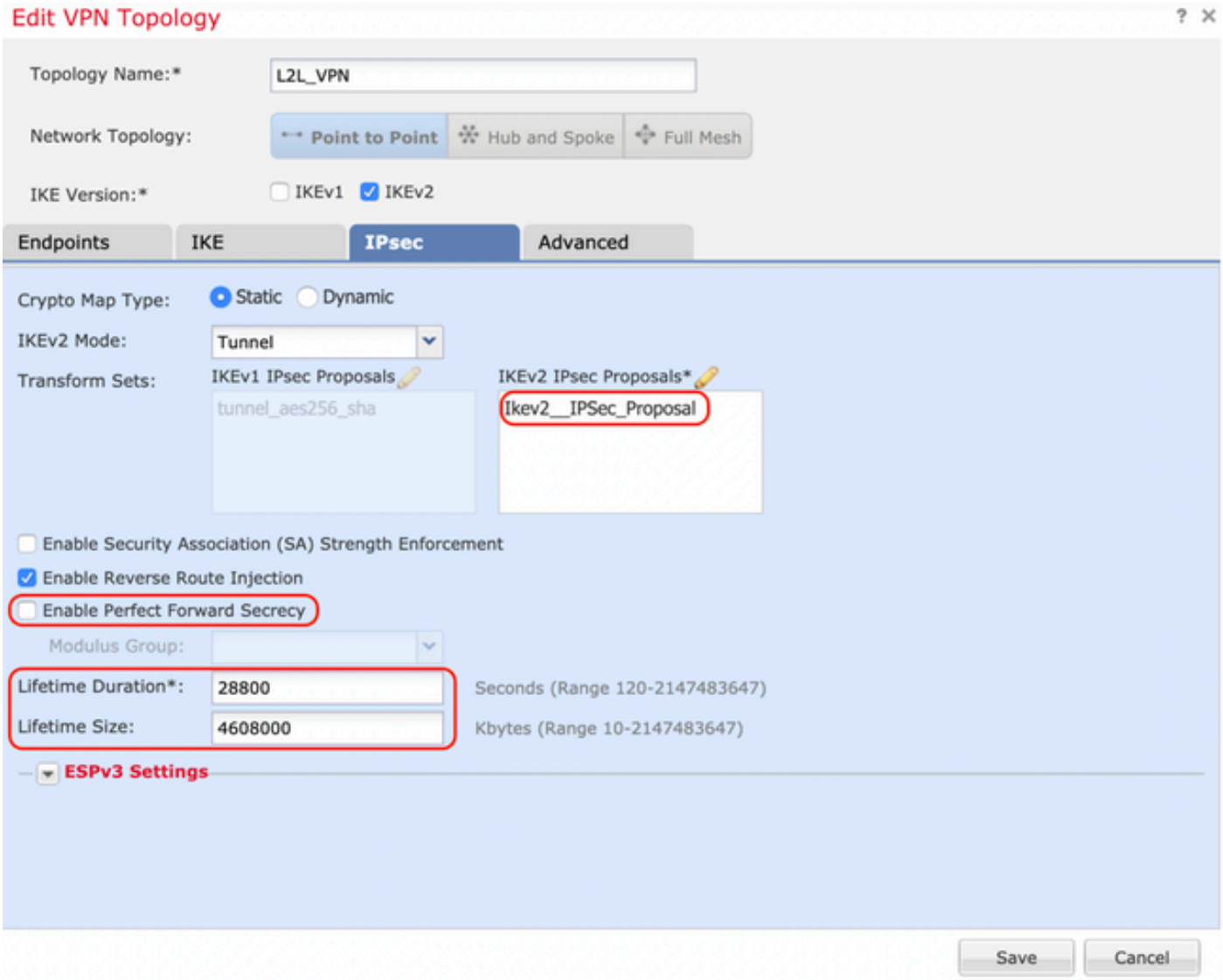



步驟3.建立新的IPsec方案後，將其新增到選定的轉換集。




步驟4.新選擇的IPsec建議現在列在IKEv2 IPsec建議下。

如果需要，可在此處編輯階段2生存期和PFS。在本例中，生存期設定為預設值，PFS被禁用。



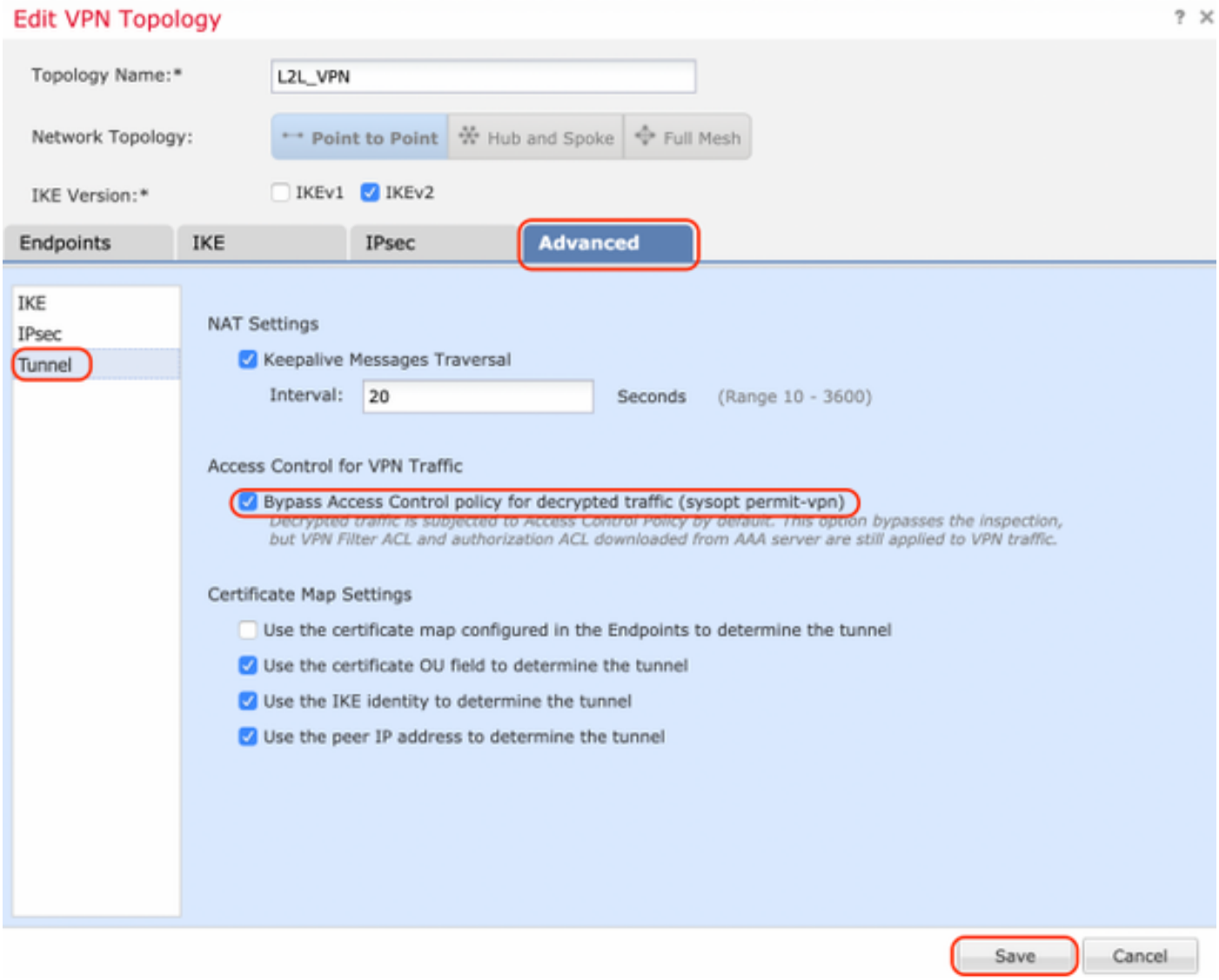

您必須配置以下步驟以繞過訪問控制或建立訪問控制策略規則以允許VPN子網通過FTD。

## 旁路存取控制

如果未啟用*sysopt permit-vpn*，則必須建立訪問控制策略以允許VPN流量通過FTD裝置。如果啟用sysopt permit-vpn，請跳過建立訪問控制策略。此配置示例使用「旁路訪問控制」選項。

可以在Advanced > Tunnel下啟用引數*sysopt permit-vpn*。

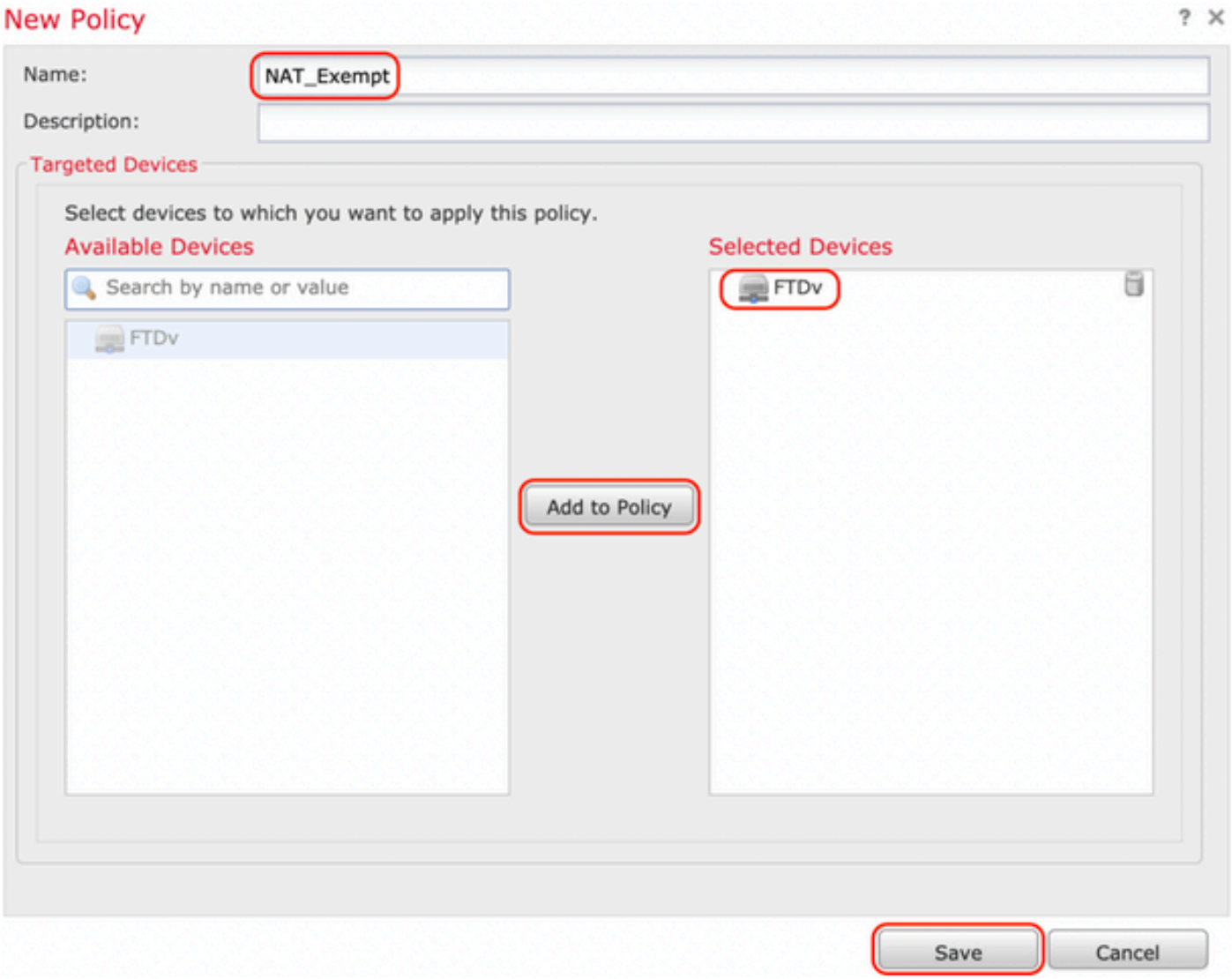
> **注意**：此選項可刪除使用訪問控制策略檢查來自使用者的流量的可能性。VPN過濾器或可下載ACL仍可用於過濾使用者流量。這是一個全域性命令，如果選中此覈取方塊，則此命令適用於所有VPN。



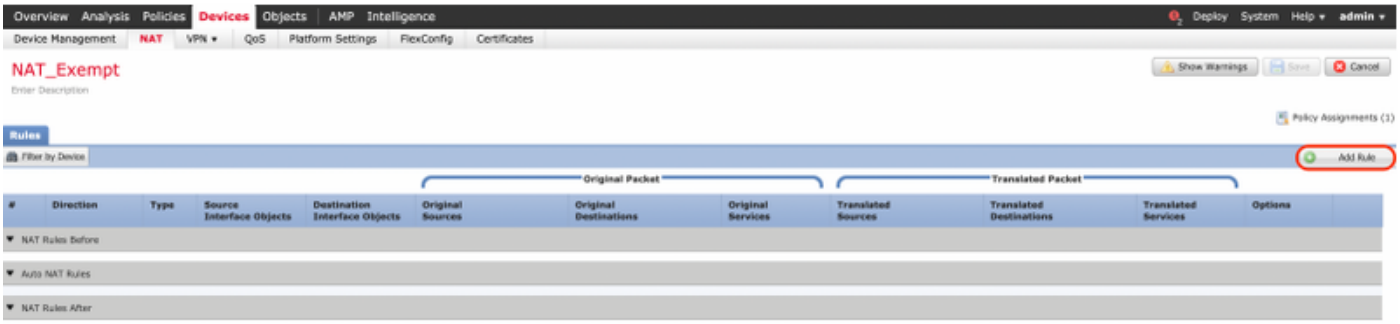

# 配置NAT免除

為VPN流量配置NAT免除語句。NAT豁免必須到位，以防止VPN流量匹配另一個NAT語句並錯誤地轉換VPN流量。

步驟1.導覽至**Devices > NAT** and c按一下**New Policy > Threat Defense NAT**建立新策略。



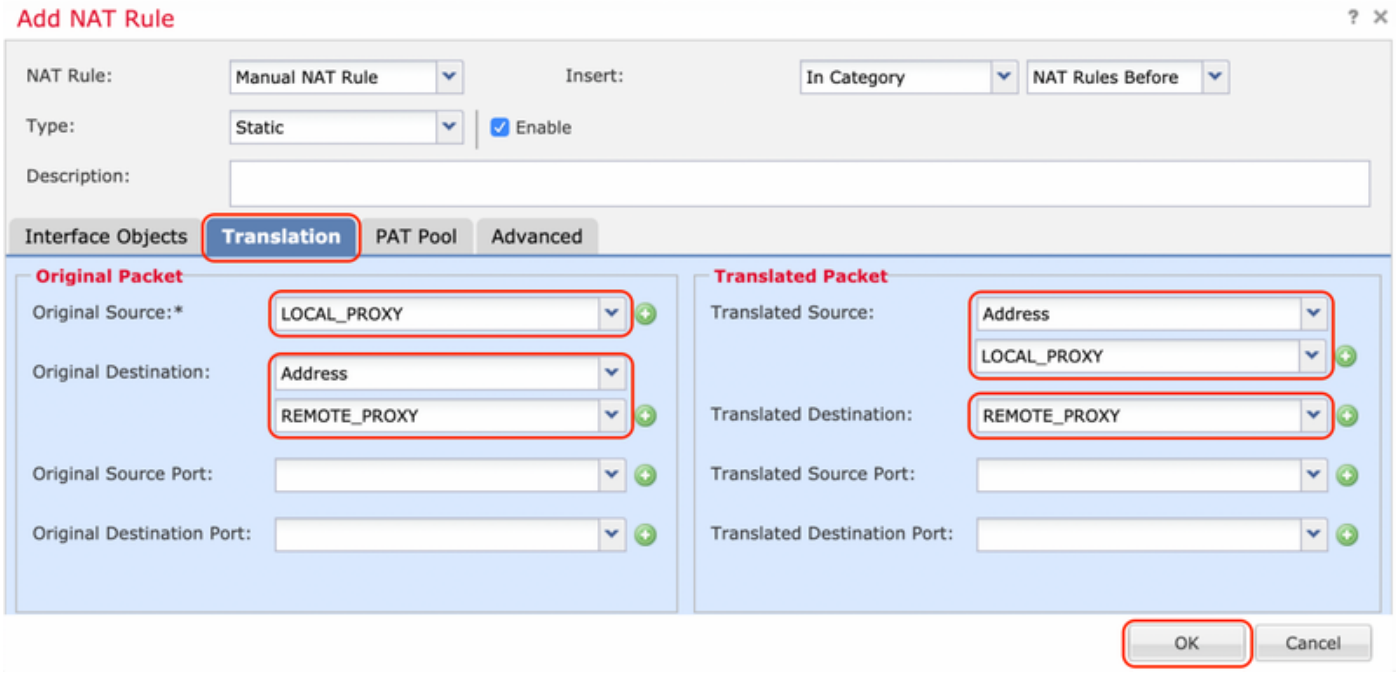

步驟2.按一下**Add Rule**。



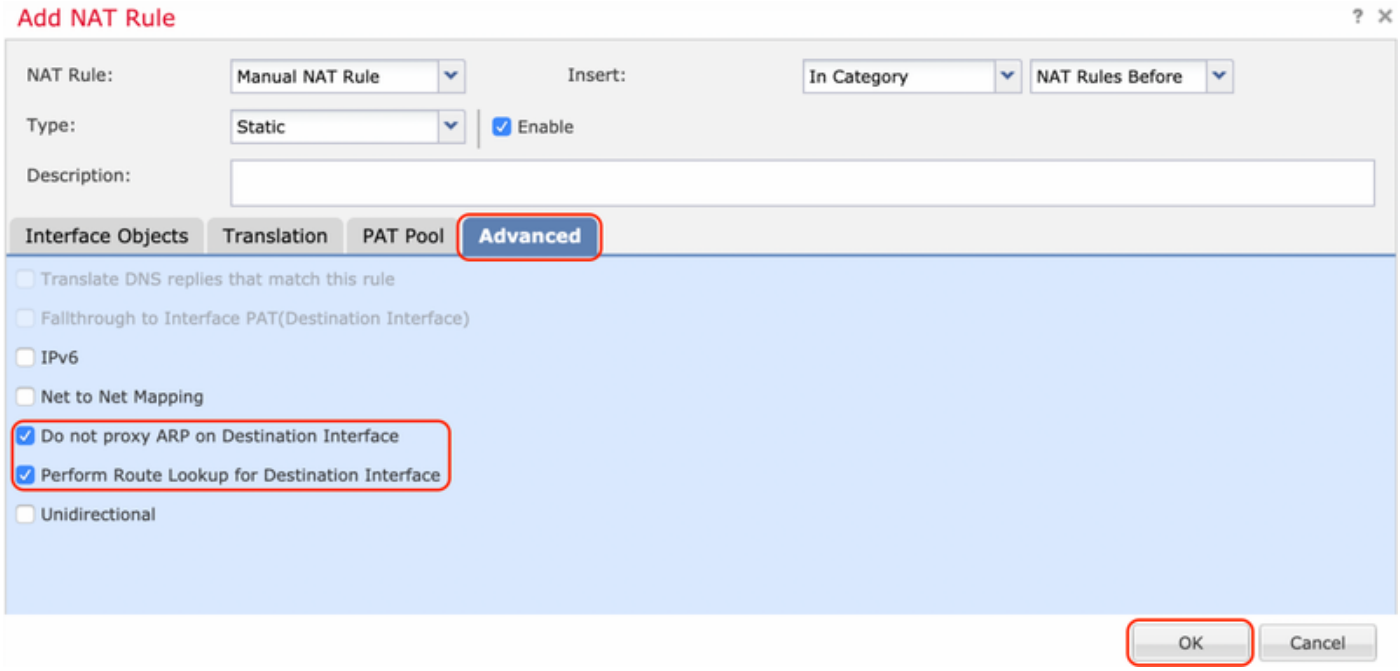

步驟3.建立新的靜態手動NAT規則。

參考NAT規則的內部和外部介面。在Interface Objects頁籤中指定介面可防止這些規則影響來自其他介面的流量。

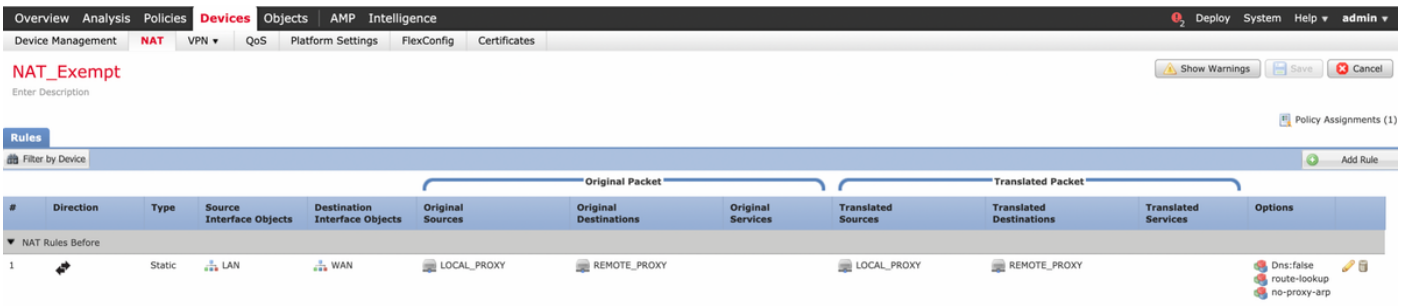
導航到Translation頁籤並選擇源子網和目標子網。由於這是NAT免除規則，請確保原始源/目標與轉換後的源/目標相同。



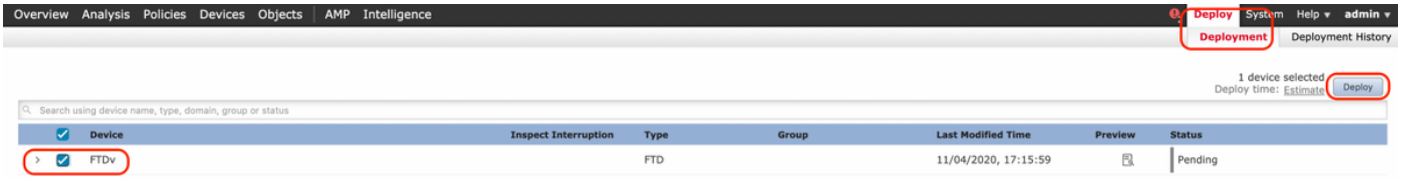

點選Advanced頁籤並啟用**no-proxy-arp**和**route-lookup**。




儲存此規則並在NAT清單中確認最終的NAT語句。




**步驟4.完成組態後，將組態儲存並部署到FTD。**




# 驗證

從LAN電腦發起感興趣的流量，或者您可以在ASA上運行下面的packet Tracer命令。

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

**附註：**其中Type = 128,Code=0表示ICMPv6「Echo Request」。

以下部分介紹可在ASAv或FTD LINA CLI上運行的命令，以檢查IKEv2隧道的狀態。

以下是ASA輸出的示例：

```
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
```

# 疑難排解

要排除ASA和FTD上的IKEv2隧道建立問題，請運行以下debug命令：

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

以下是供參考的有效IKEv2調試示例：
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

# 參考資料

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