在ASA和FTD之间配置IKEv2 IPv6站点到站点隧道

目录

简介

本文档提供了使用互联网密钥交换版本2(IKEv2)协议在ASA（自适应安全设备）和FTD（Firepower威胁防御）之间设置IPv6站点到站点隧道的配置示例。设置包括与ASA和FTD作为VPN终端设备的端到端IPv6网络连接。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA CLI配置的基本知识
- IKEv2和IPSEC协议的基本知识
- 了解IPv6编址和路由
- 通过FMC基本了解FTD配置

使用的组件

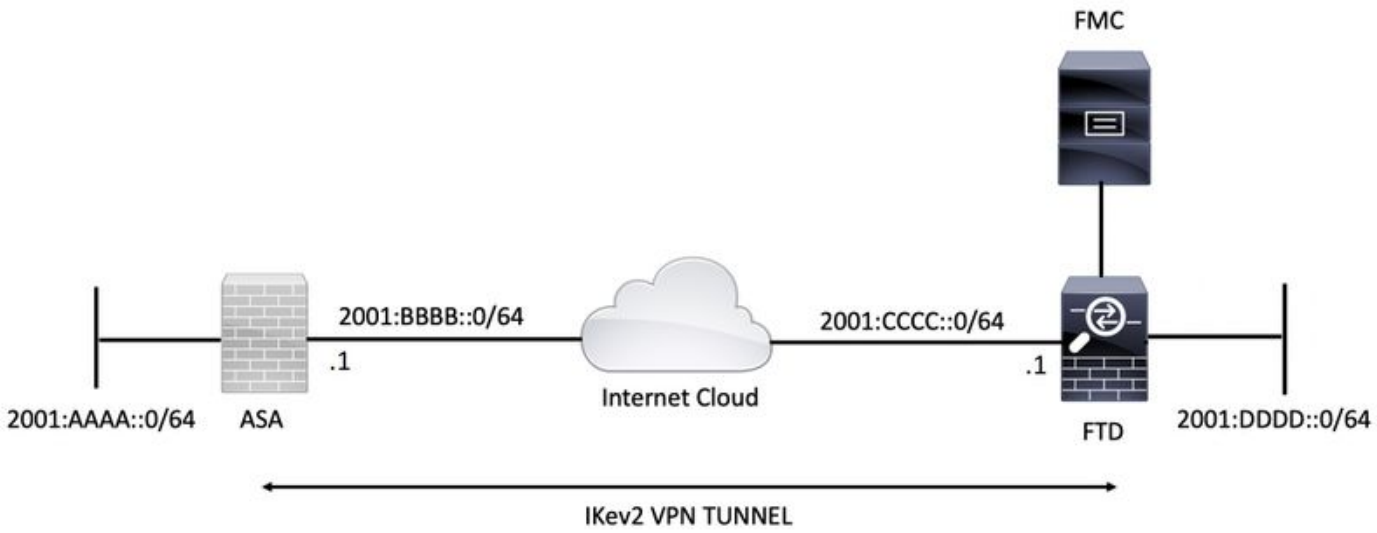
本文档中的信息基于虚拟环境，该虚拟环境是从特定实验室设置中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络正在生产，请确保您了解任何命令的潜在影响。

本文档中的信息基于以下软件和硬件版本：

- 运行9.6.(4)12的思科ASAv
- 运行6.5.0的思科FTDv
- 运行6.6.0的思科FMCv

配置

网络图



ASA 配置

本节介绍在ASA上所需的配置。

步骤1.配置ASA接口。

```
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
```

步骤2.设置IPv6默认路由。

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

步骤3.配置IKEv2策略并在外部接口上启用IKEv2。

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

crypto ikev2 enable outside
```

步骤4.配置隧道组。

```
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
```

步骤5.创建对象和访问控制列表(ACL)以匹配相关流量。

```
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
```

步骤6.为相关流量配置身份网络地址转换(NAT)规则。

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

步骤7.配置IKEv2 IPSec建议。

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

步骤8.设置加密映射并将其应用到外部接口。

```
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配置

本节提供使用FMC配置FTD的说明。

定义VPN拓扑

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

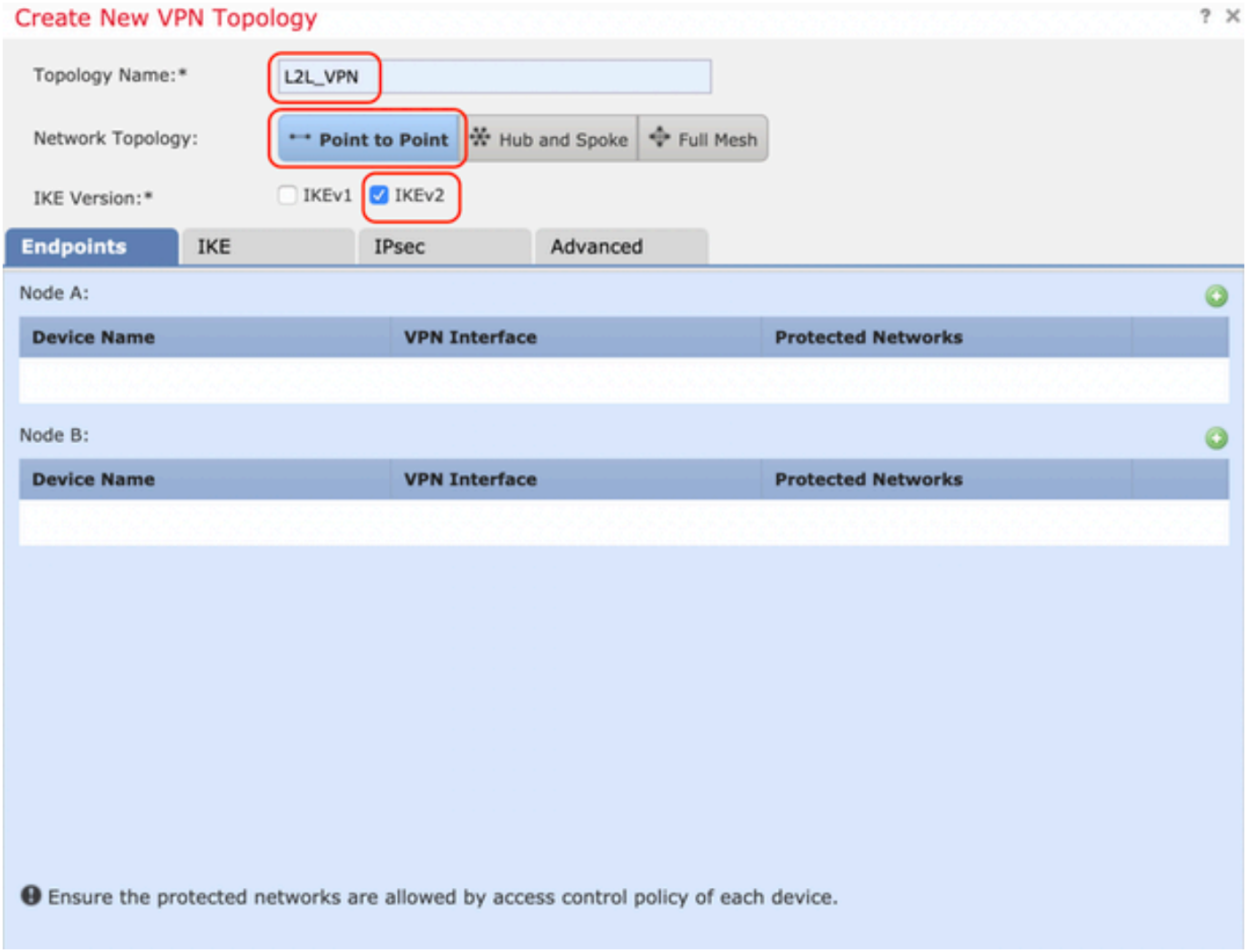
“VPN”“Firepower”

步骤2.出现“创建新VPN拓扑”框。为VPN提供一个易于识别的名称。

网络拓扑:点对点

IKE版本：IKEv2

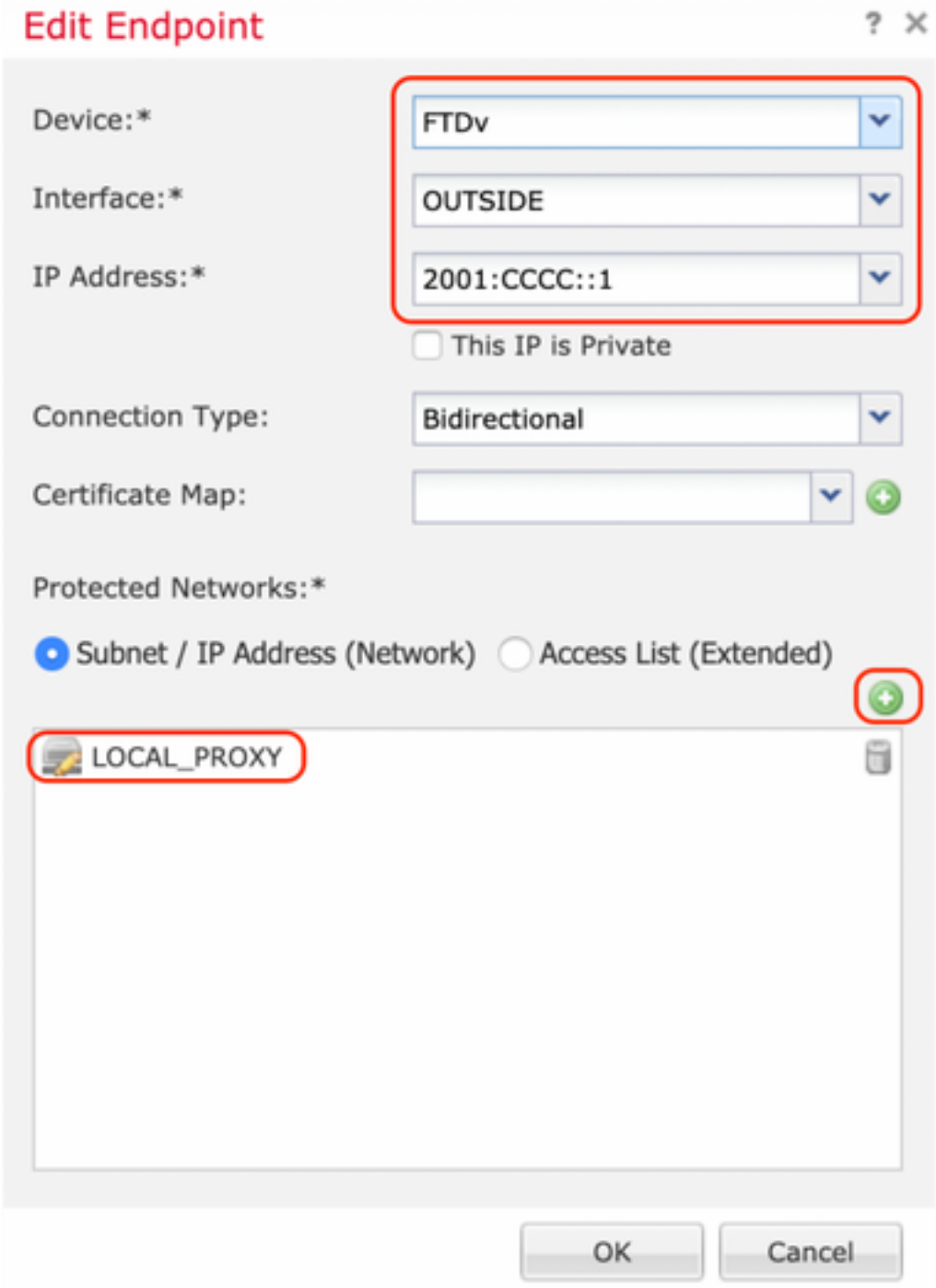
在本例中，选择终端时，节点A是FTD。节点B是ASA。单击绿色加号按钮将设备添加到拓扑。

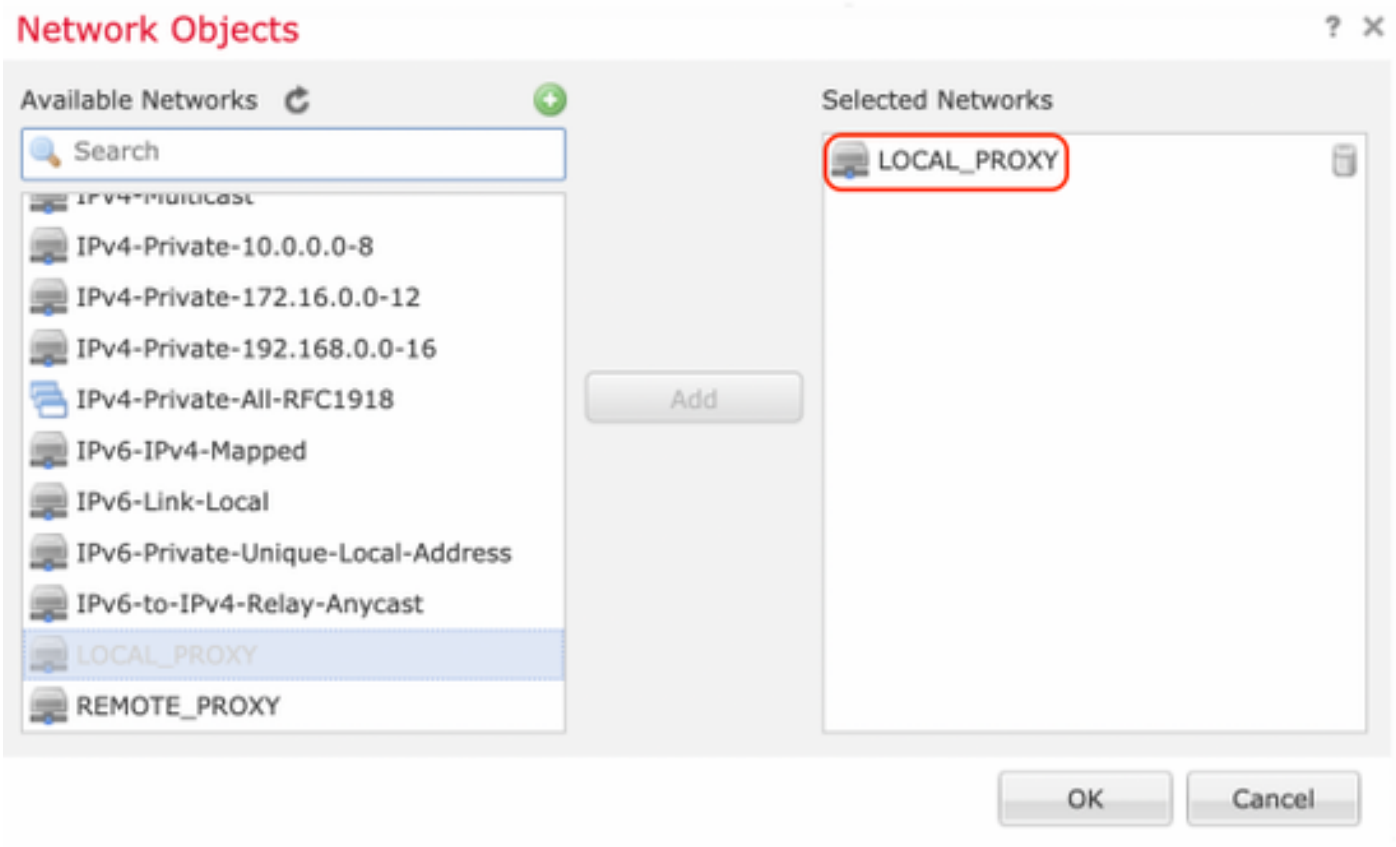


步骤3.将FTD添加为第一个终端。

选择应用加密映射的接口。IP地址应从设备配置中自动填充。

点击Protected Networks（受保护网络）下的绿色加号图标，选择通过此VPN隧道加密的子网。在本例中，FMC上的“本地代理”网络对象包含IPv6子网“2001:DDDD::/64”。

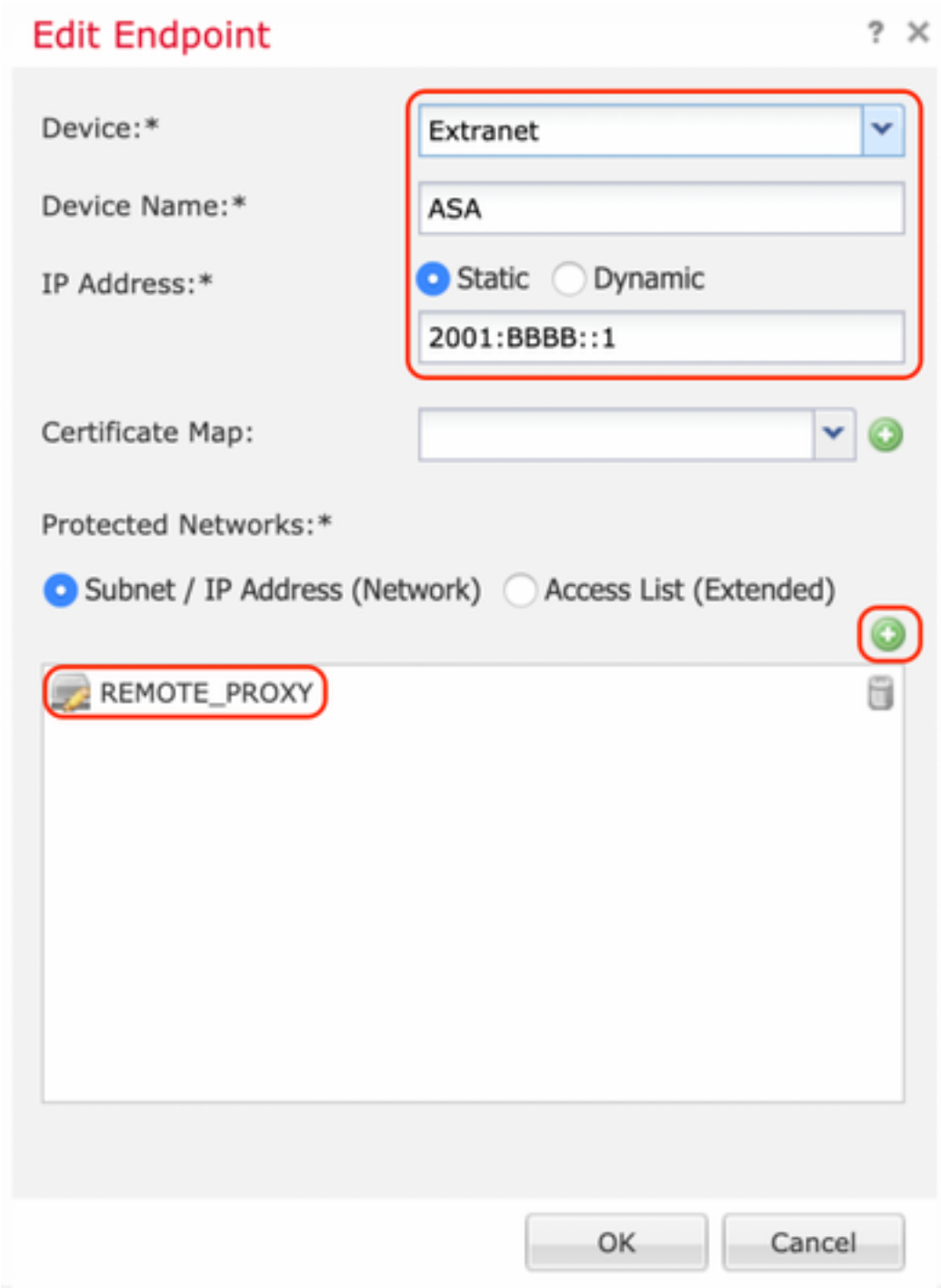

Edit Endpoint
Device:*
FTDv
Interface:*
OUTSIDE
IP Address:*
2001:CCCC::1
This IP is Private
Connection Type:
Bidirectional
Certificate Map:
Protected Networks:*
Subnet / IP Address (Network)
Access List (Extended)
LOCAL_PROXY
OK
Cancel



通过上述步骤，FTD终端配置完成。

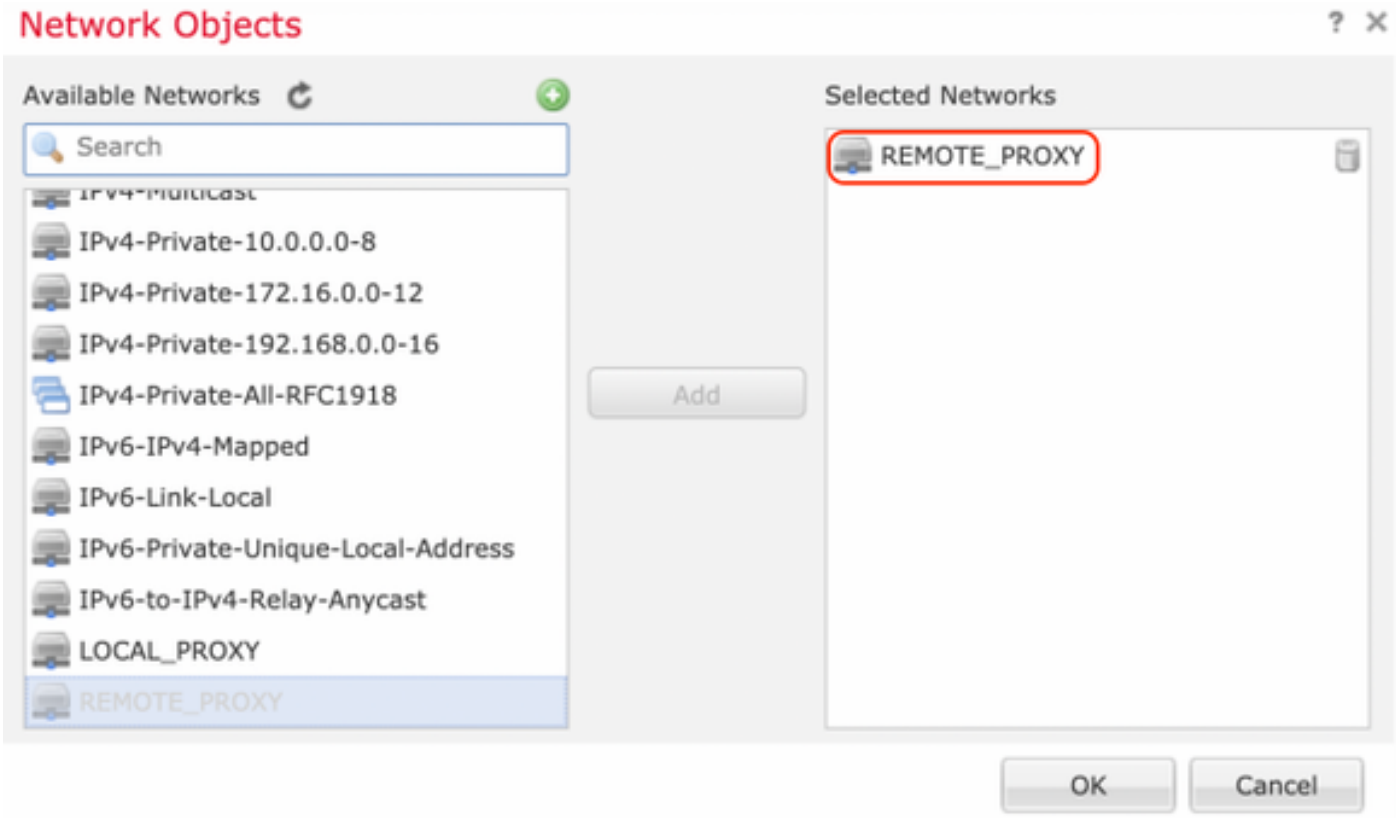
步骤4.点击节点B的绿色加号图标，该节点是配置示例中的ASA。不由FMC管理的设备被视为外联网。添加设备名称和IP地址。

步骤5.选择绿色加号图标以添加受保护的网络。



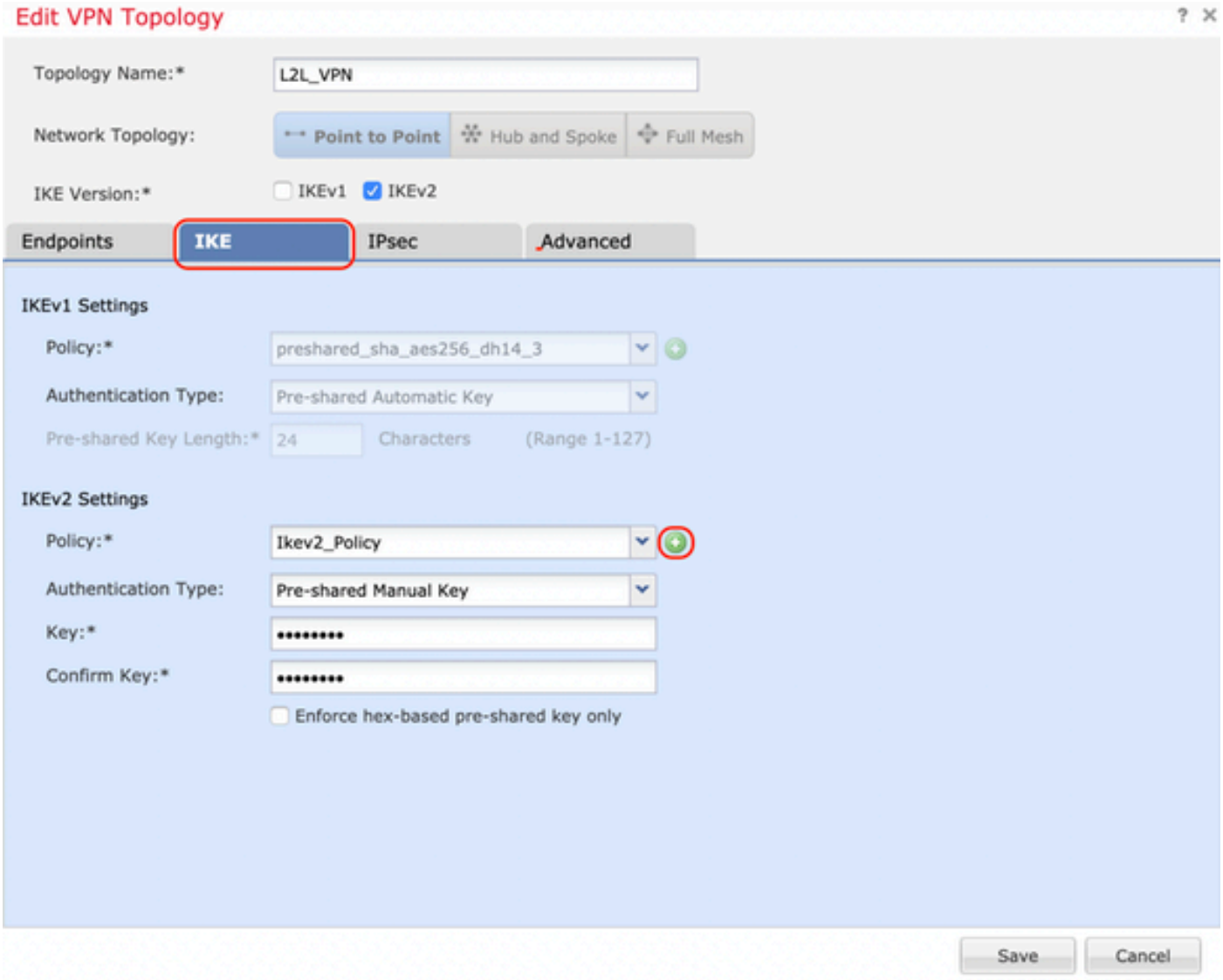
步骤6.选择需要加密的ASA子网并将其添加到所选网络。

“远程代理”是本例中的ASA子网“2001:AAAA::/64”。



配置IKE参数

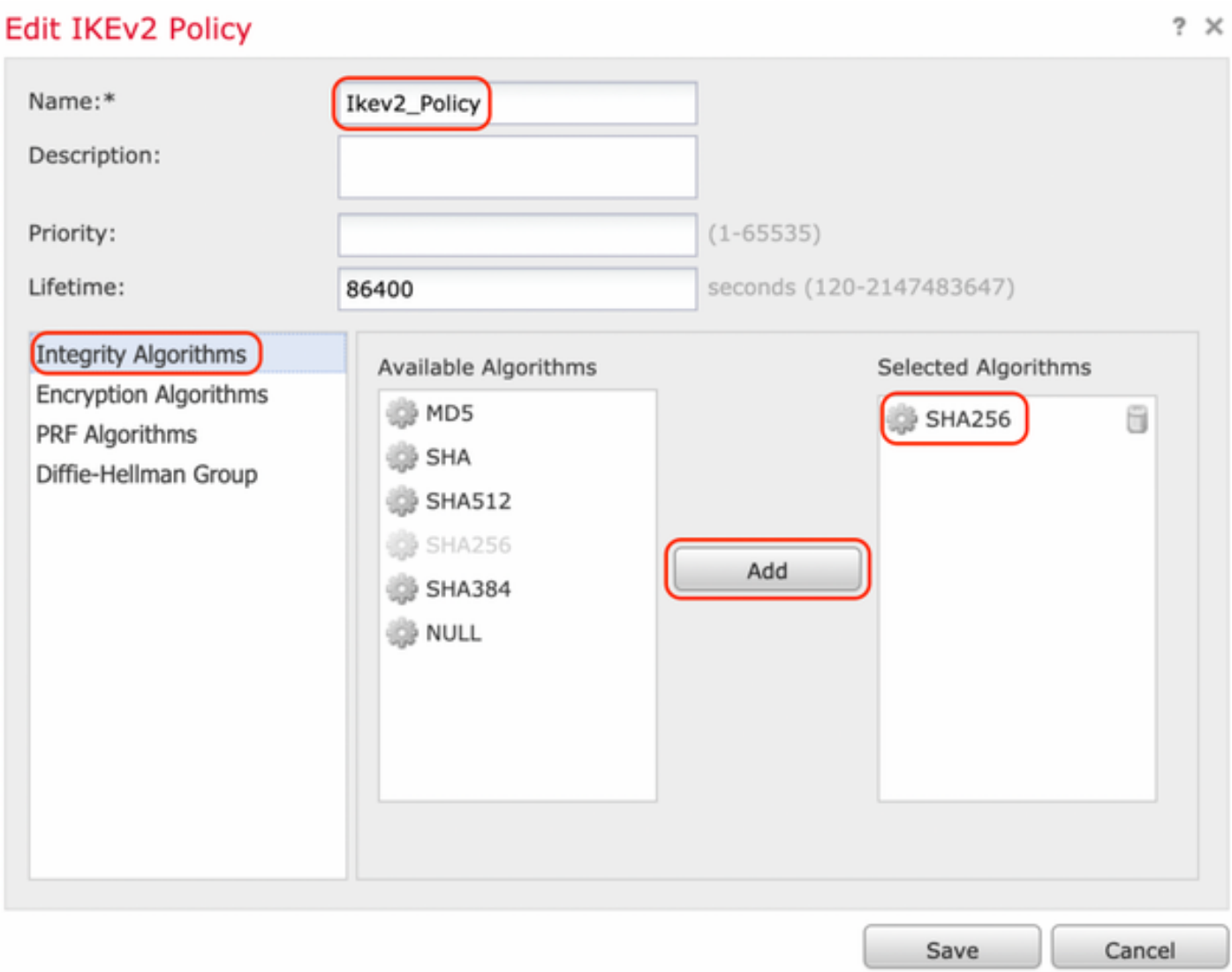
步骤1.在IKE选项卡下，指定用于IKEv2初始交换的参数。点击绿色加号图标以创建新的IKE策略。

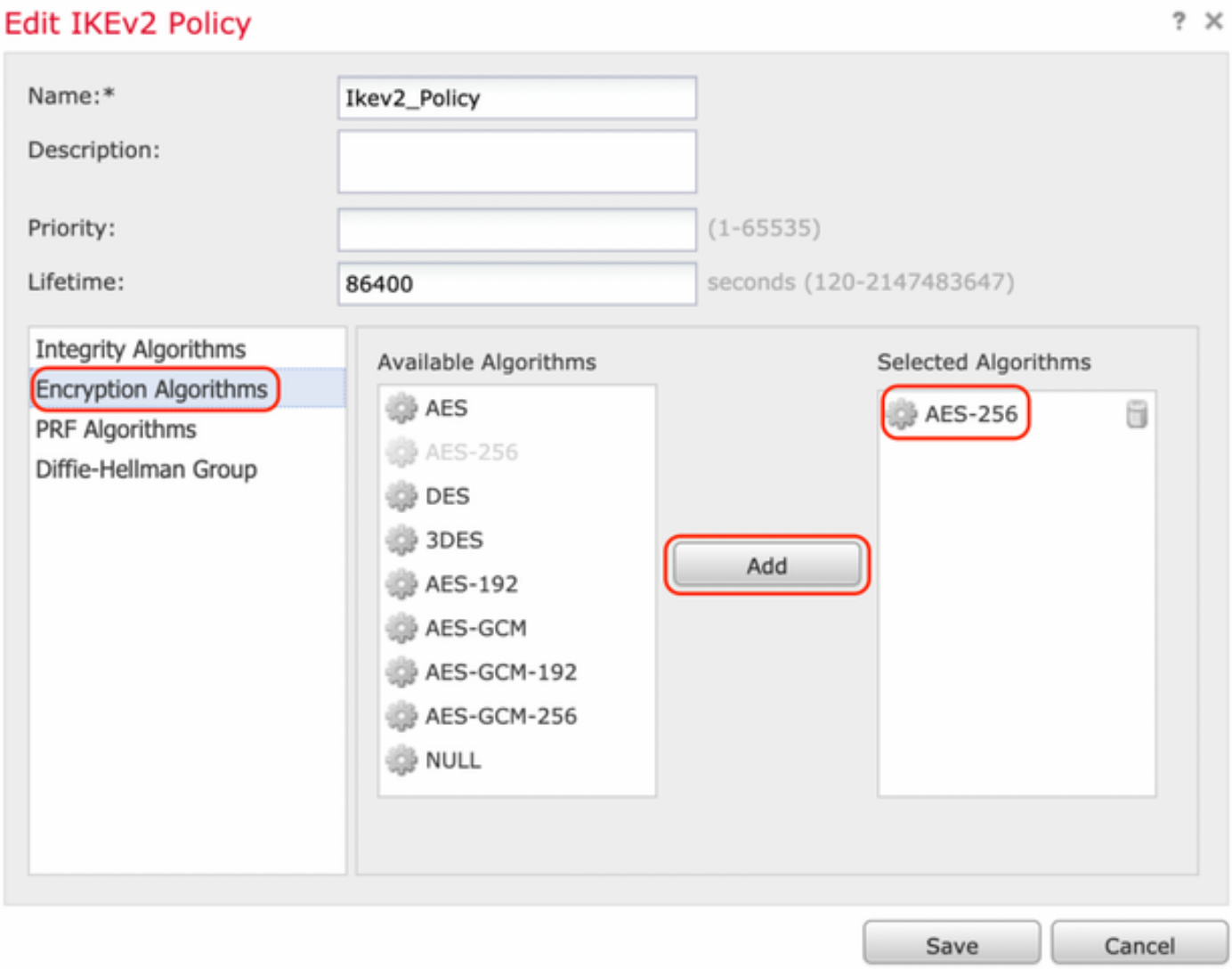


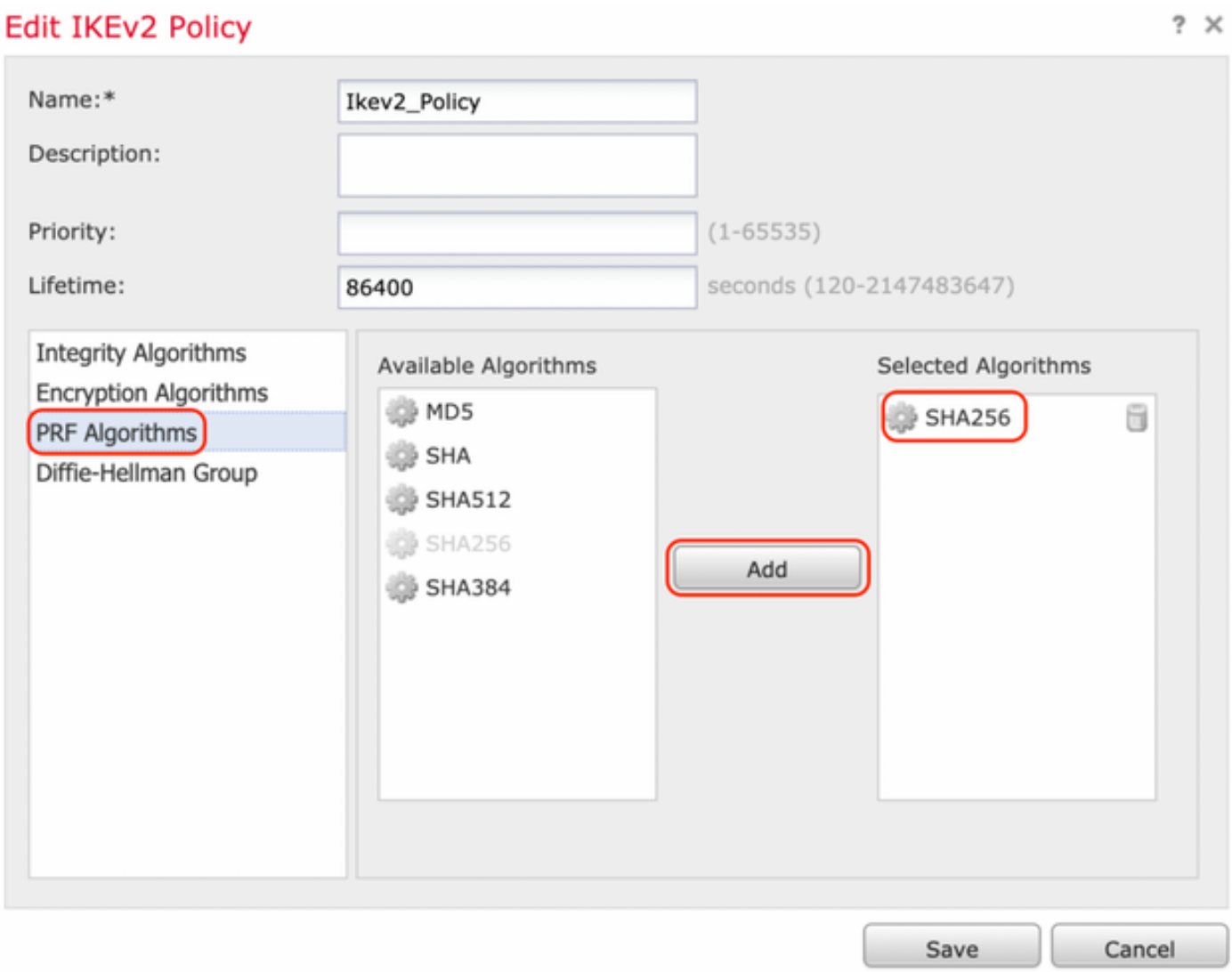
步骤2.在新的IKE策略中，指定优先级编号以及连接第1阶段的生存期。本指南使用以下参数进行初始交换：
完整性(SHA256)、
加密(AES-256)，
PRF(SHA256)和
Diffie-Hellman组（组14）。

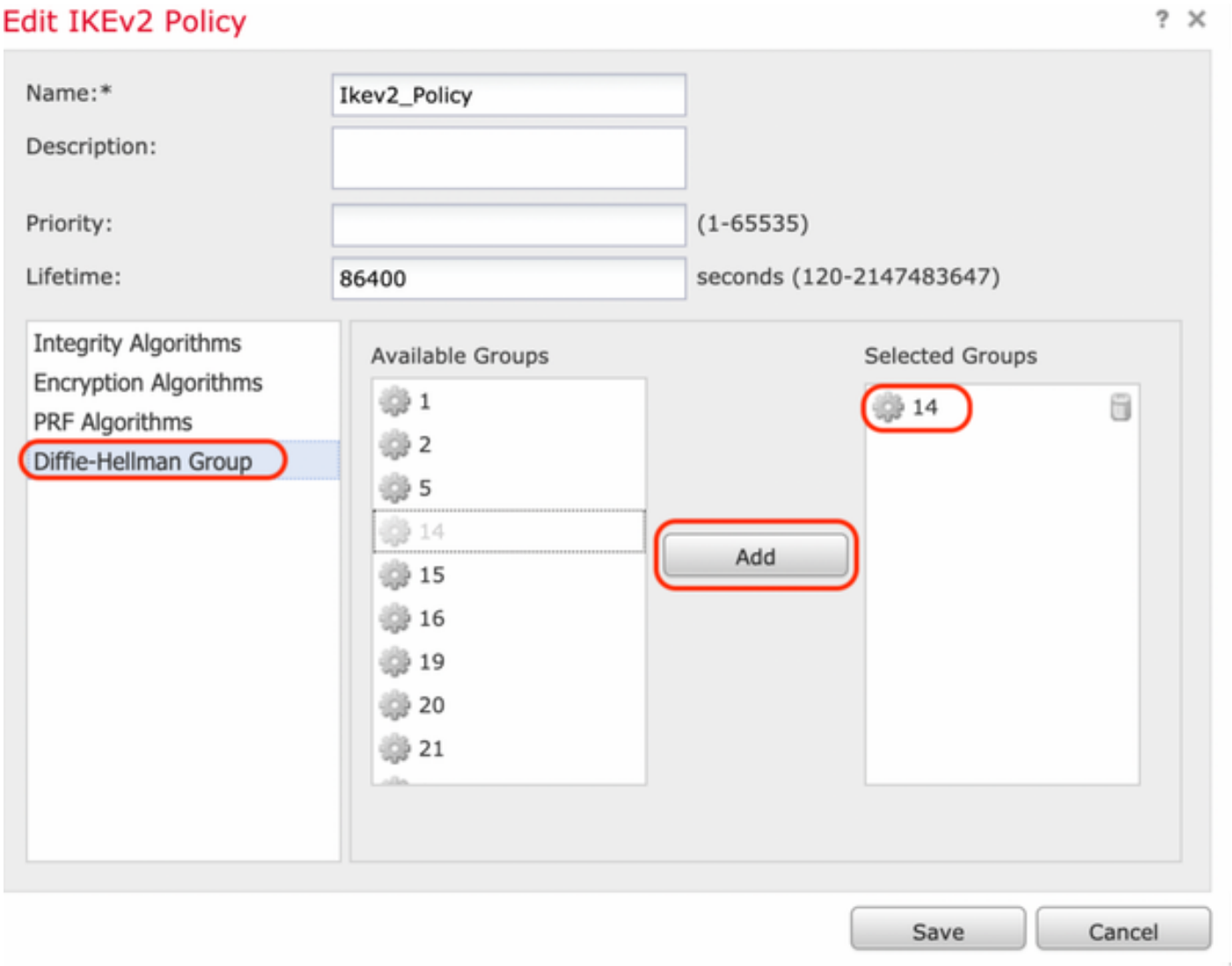
无论所选策略部分中的内容如何，设备上的所有IKE策略都将发送到远程对等体。将为VPN连接选择远程对等体匹配的第一个。

[可选]使用优先级字段选择首先发送的策略。优先级1首先发送。


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

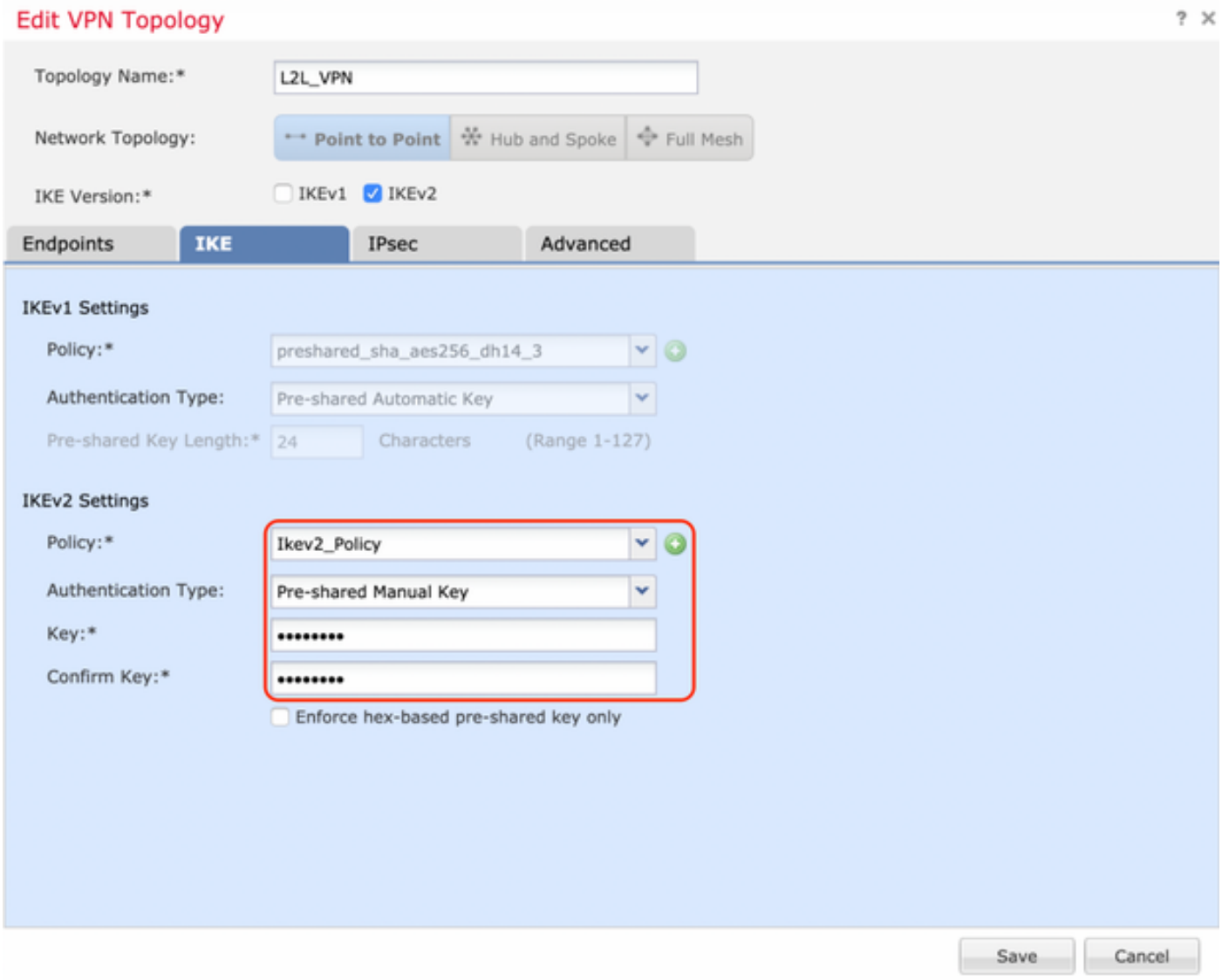

Edit IKEv2 Policy
Name:*
Ikev2_Policy
Description:
Priority:
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
AES
AES-256
DES
3DES
AES-192
AES-GCM
AES-GCM-192
AES-GCM-256
NULL
Add
Selected Algorithms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



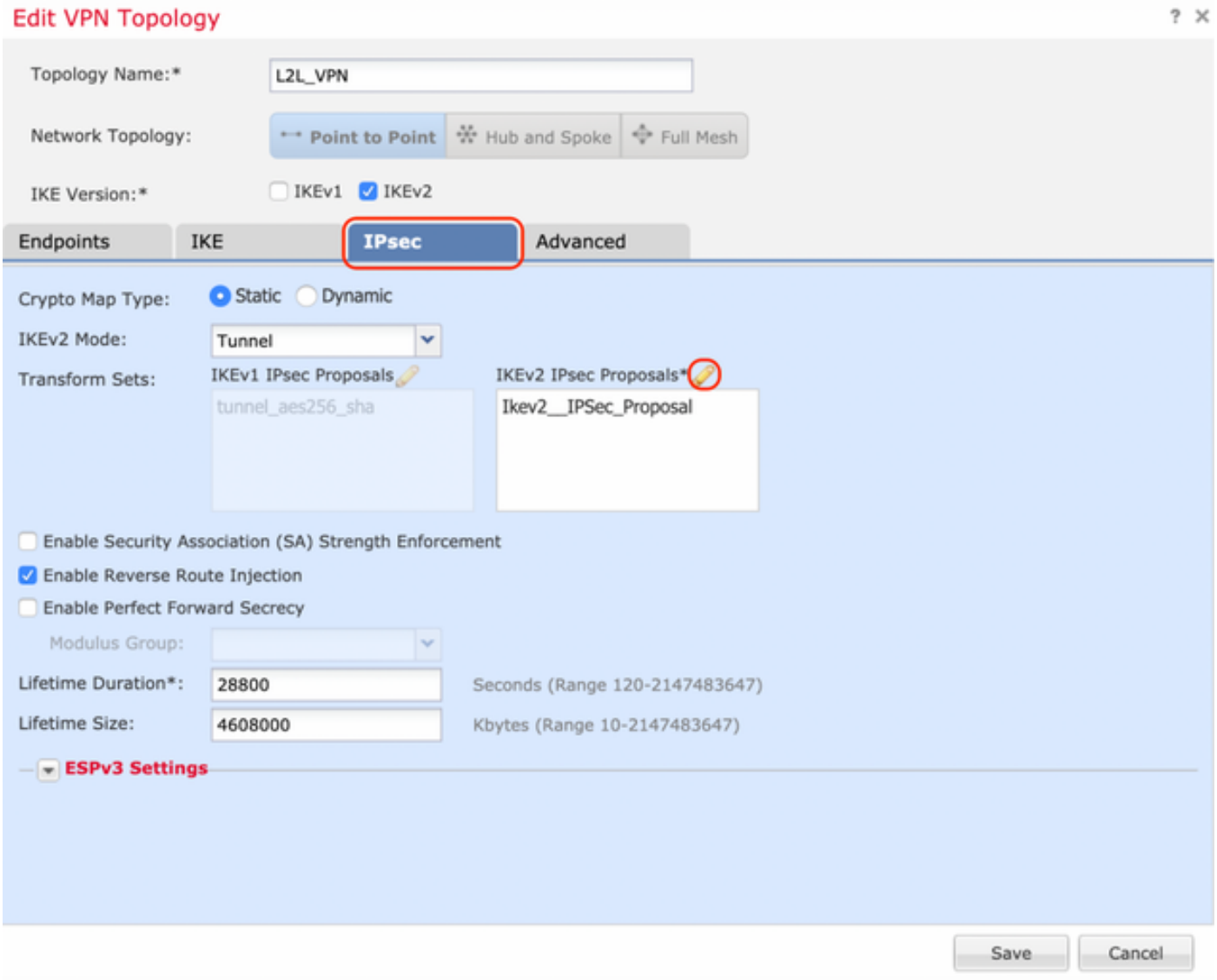
步骤3.添加参数后，选择上述配置的策略，然后选择身份验证类型。

选择预共享手动密钥选项。在本指南中，使用预共享密钥**cisco123**。



配置 IPSec 參數

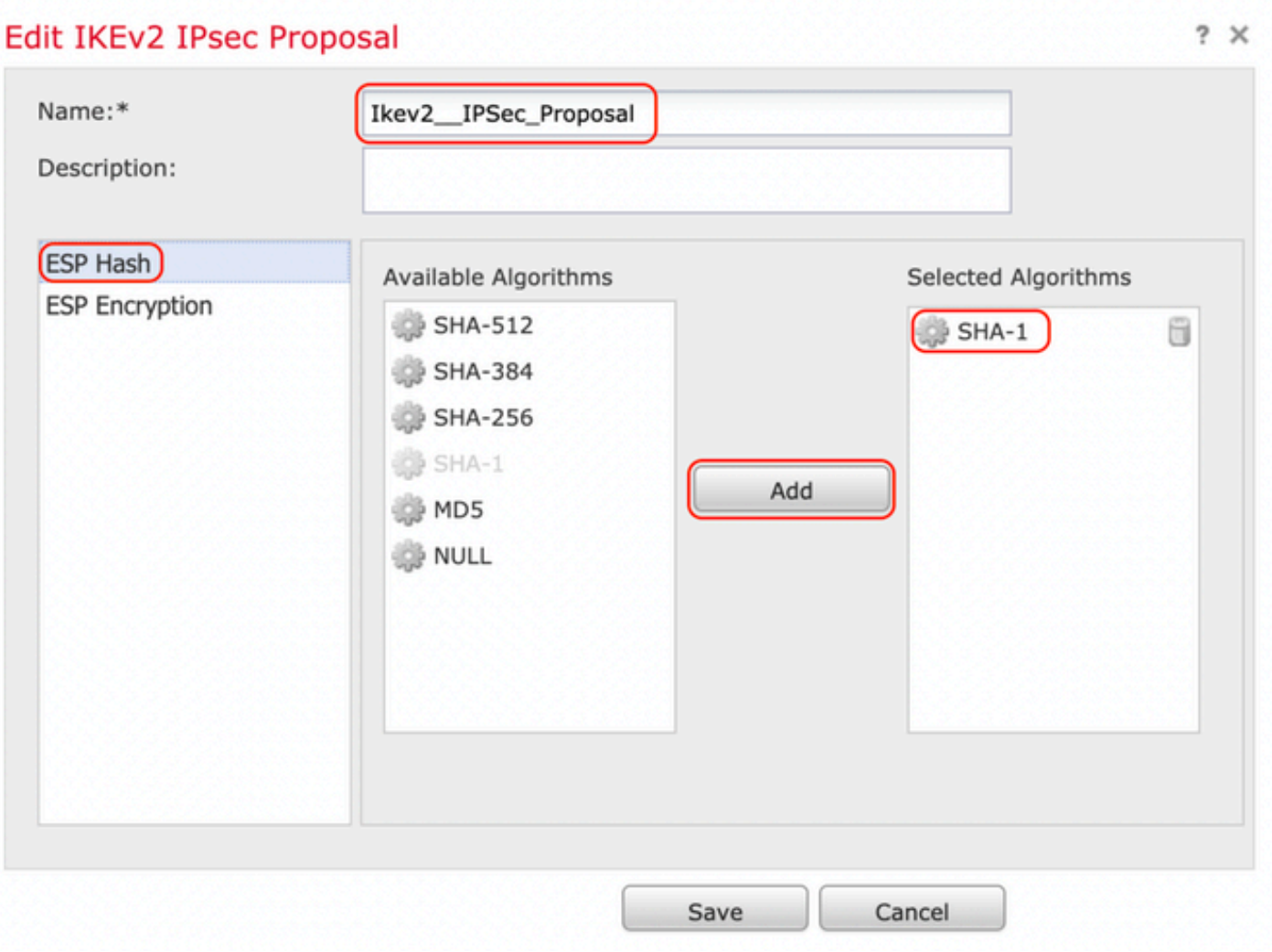
1.IPsecIPsec

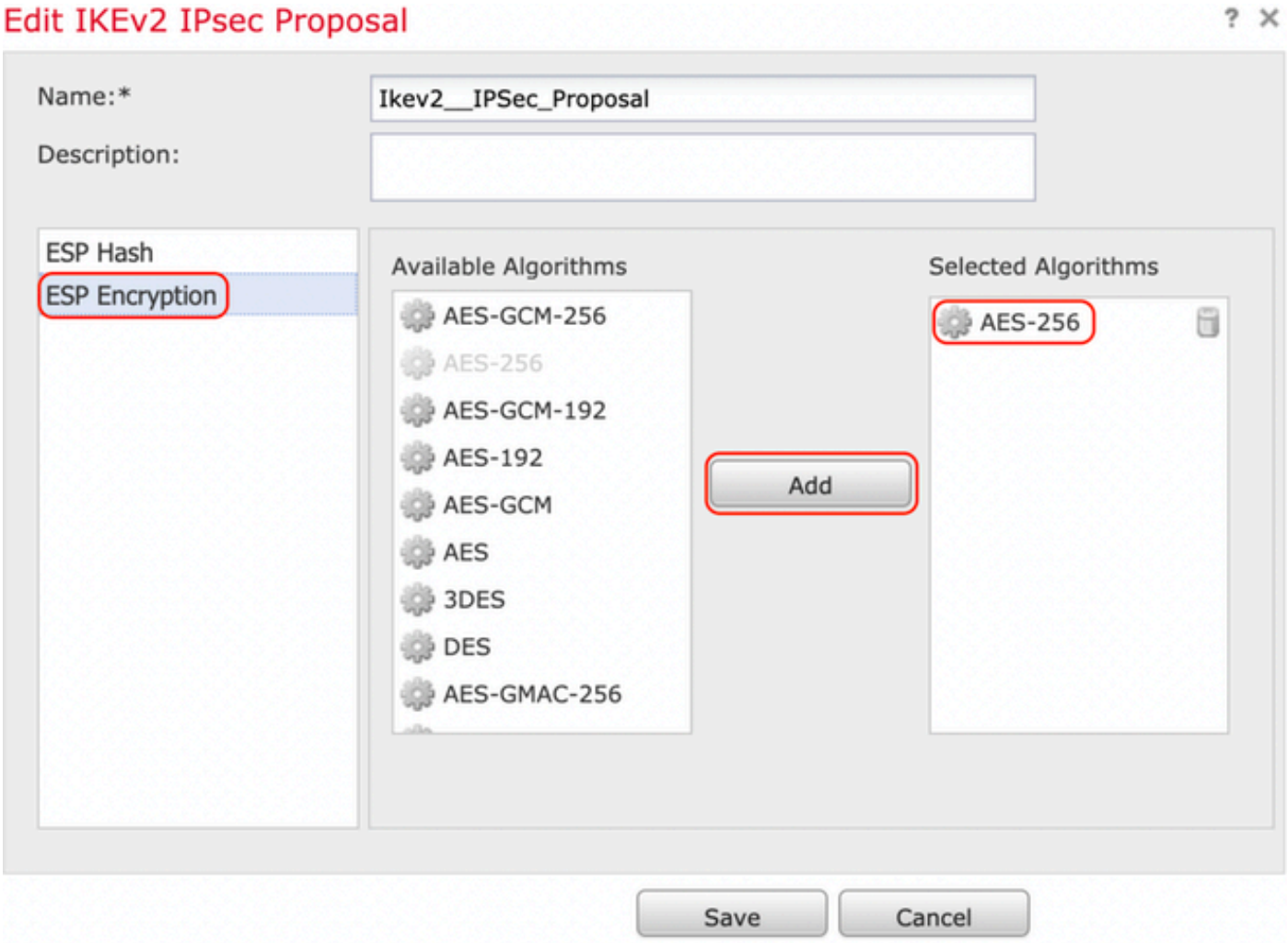


步骤2.通过选择绿色加号图标创建新的IKEv2 IPsec建议并输入阶段2参数，如下所示：

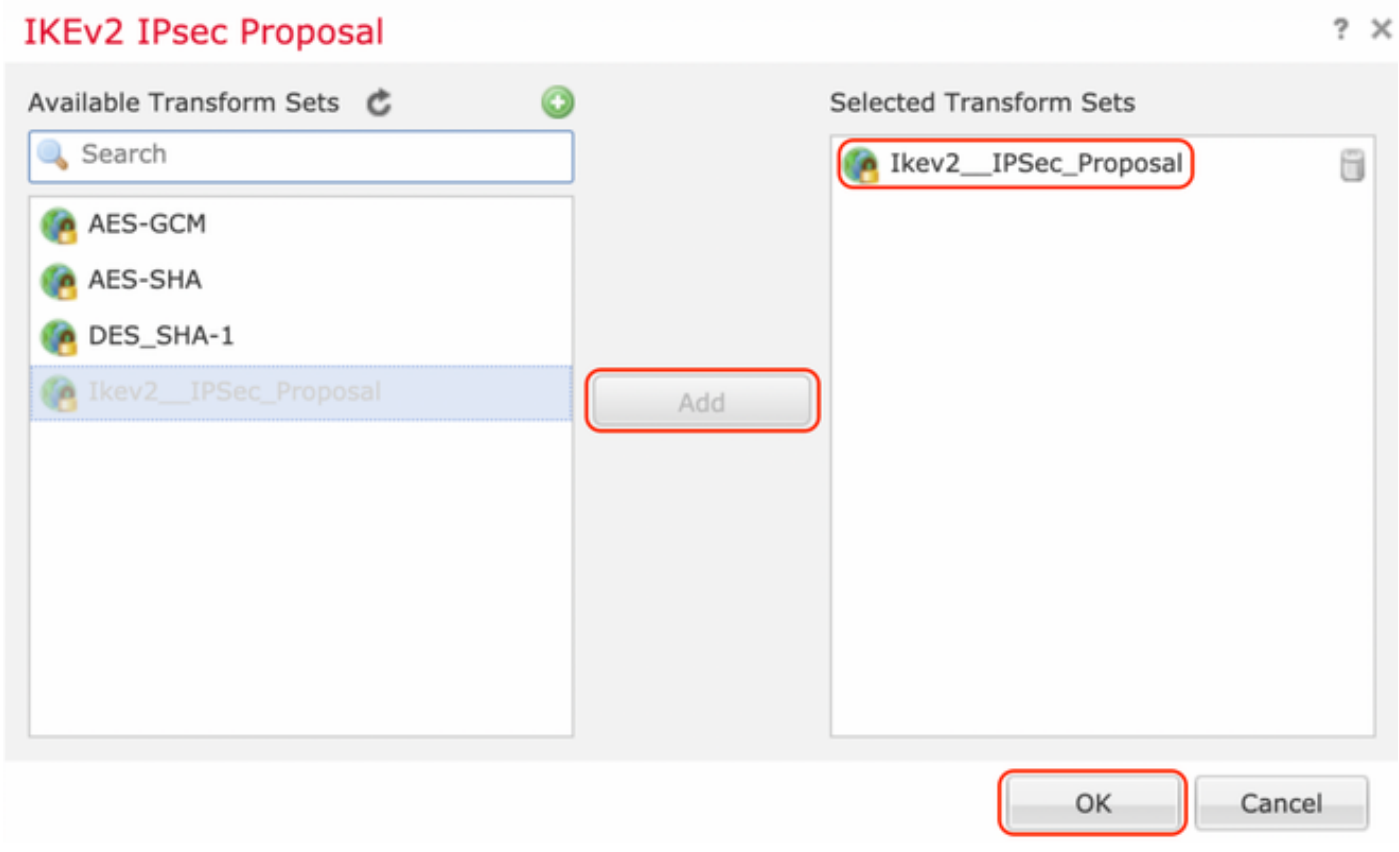
ESP哈希：SHA-1

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

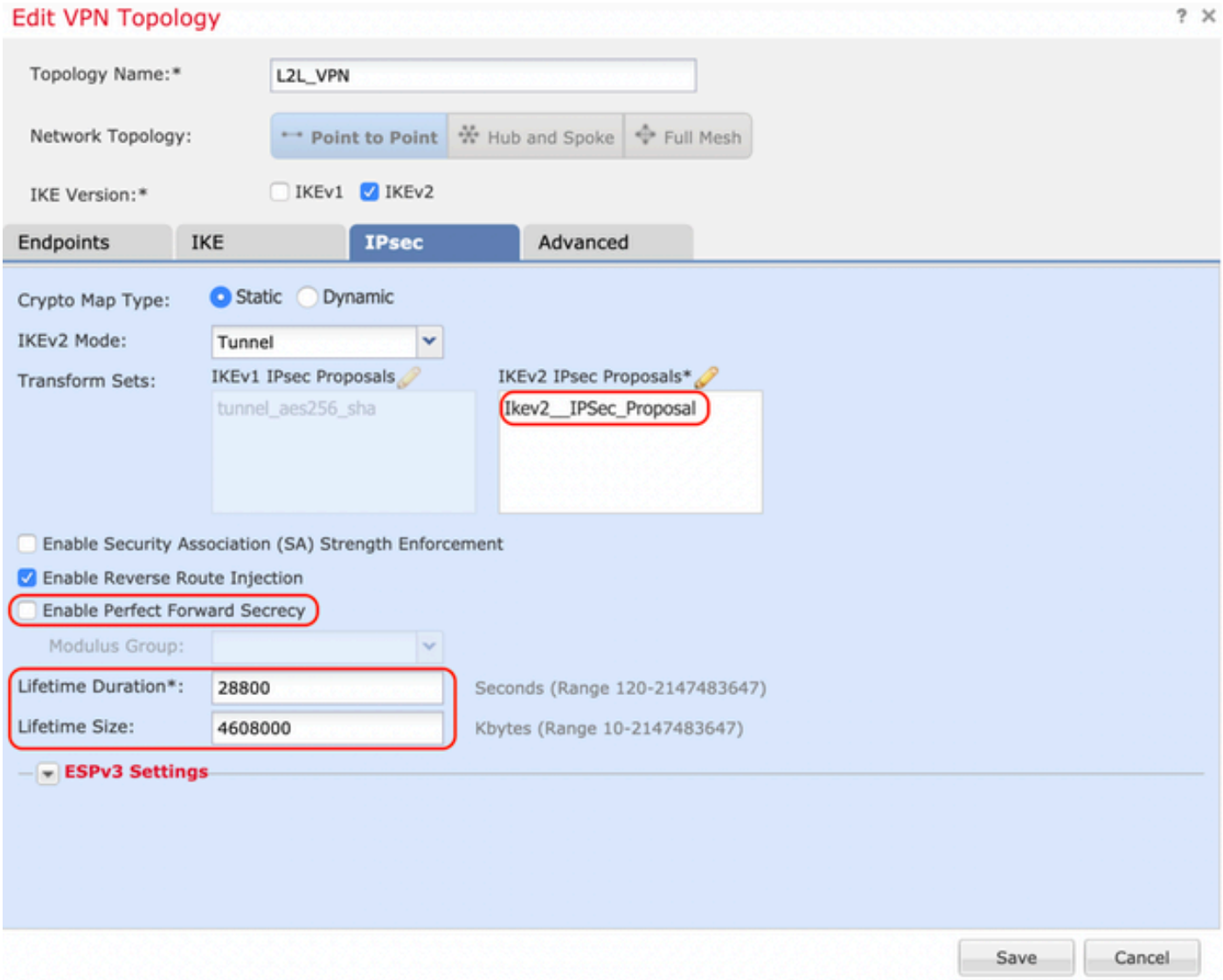


步骤3.创建新的IPsec建议后，将其添加到所选转换集。



步骤4.新选择的IPsec建议现在列在IKEv2 IPsec建议下。

如果需要，可在此处编辑第2阶段生命期和PFS。在本例中，生命期设置为默认值，并且PFS被禁用。



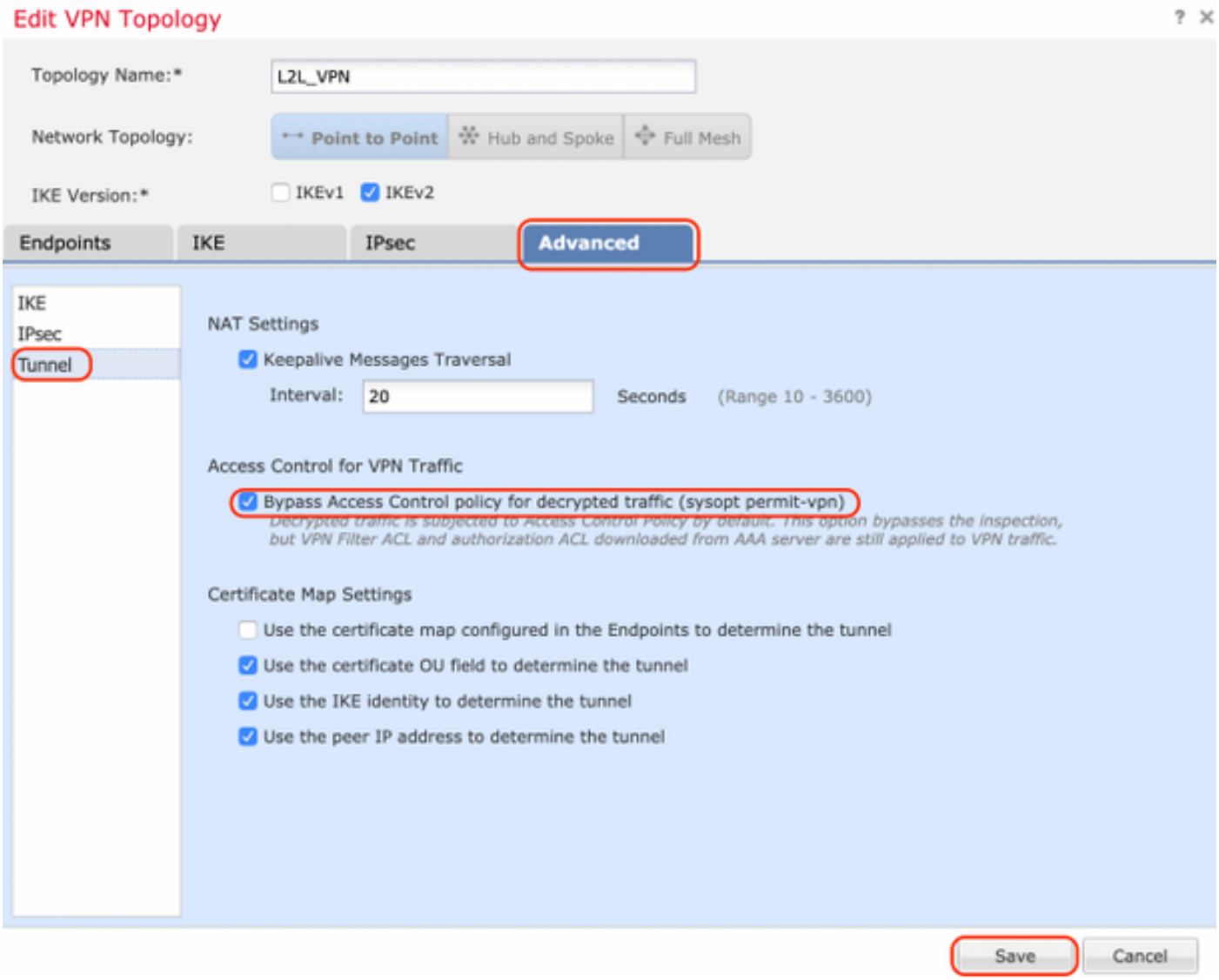
您必须配置以下步骤以绕过访问控制或创建访问控制策略规则以允许通过FTD的VPN子网。

旁路访问控制

如果*sysopt permit-vpn*未启用，则必须创建访问控制策略以允许VPN流量通过FTD设备。如果启用了sysopt permit-vpn，请跳过创建访问控制策略。此配置示例使用“旁路访问控制”选项。

在Advanced > Tunnel下，*可以启用参数sysopt permit-vpn*。

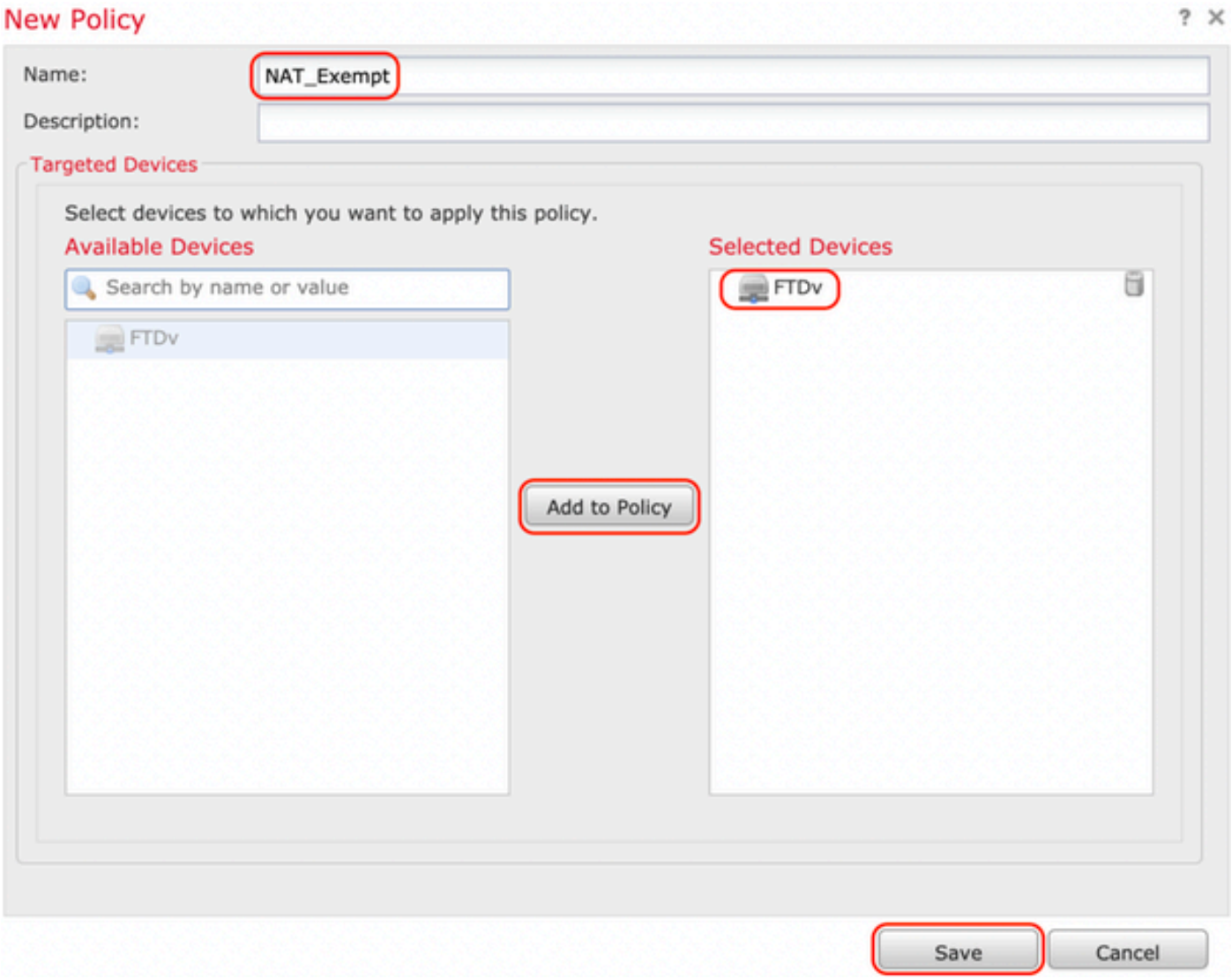
> **警告**：此选项消除了使用访问控制策略检查来自用户的流量的可能性。VPN过滤器或可下载ACL仍可用于过滤用户流量。这是全局命令，如果启用此复选框，则适用于所有VPN。



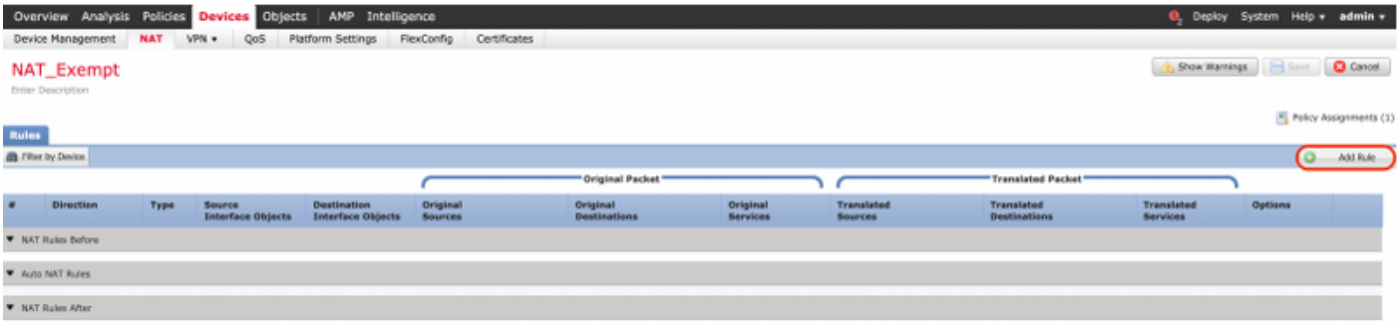
配置NAT免除

为VPN流量配置NAT免除语句。必须实施NAT免除，以防止VPN流量匹配另一NAT语句并错误转换VPN流量。

步骤1.导航至**Devices > NAT**和c通过单击New Policy > Threat Defense NAT**创建新策略**。



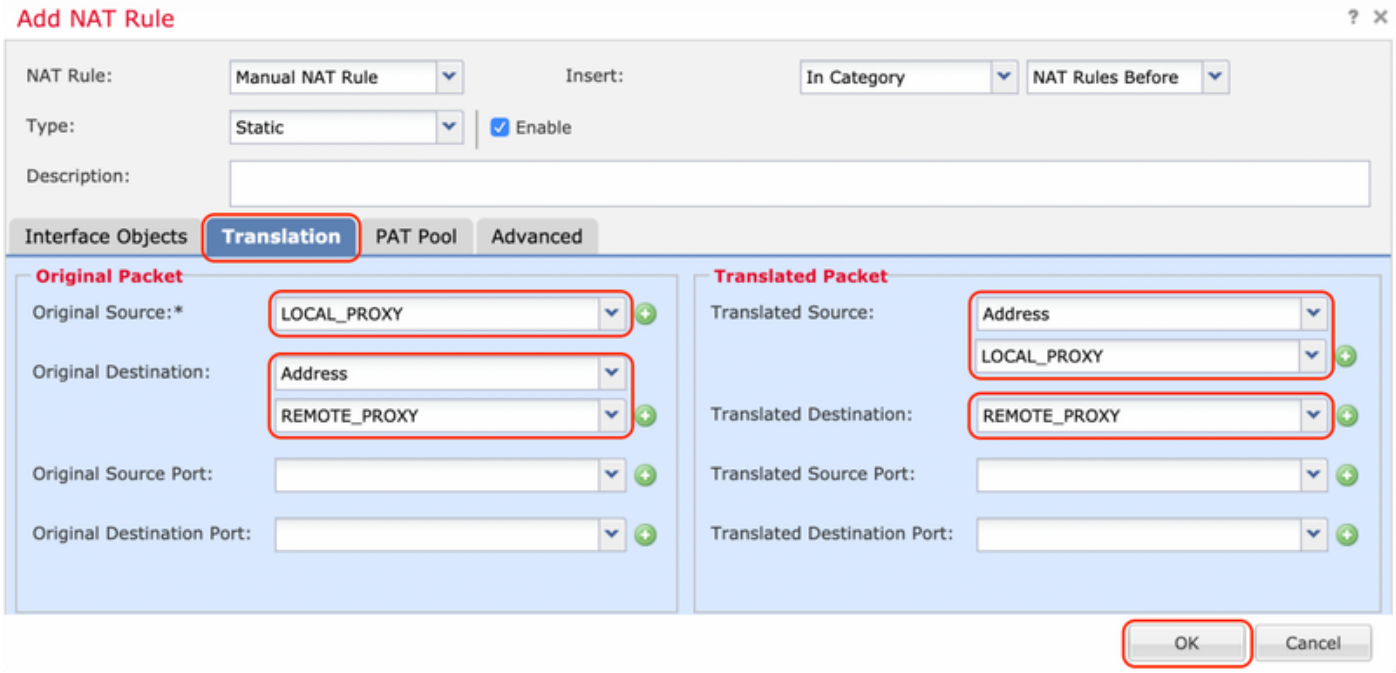
步骤2.单击“添加**规则”**。



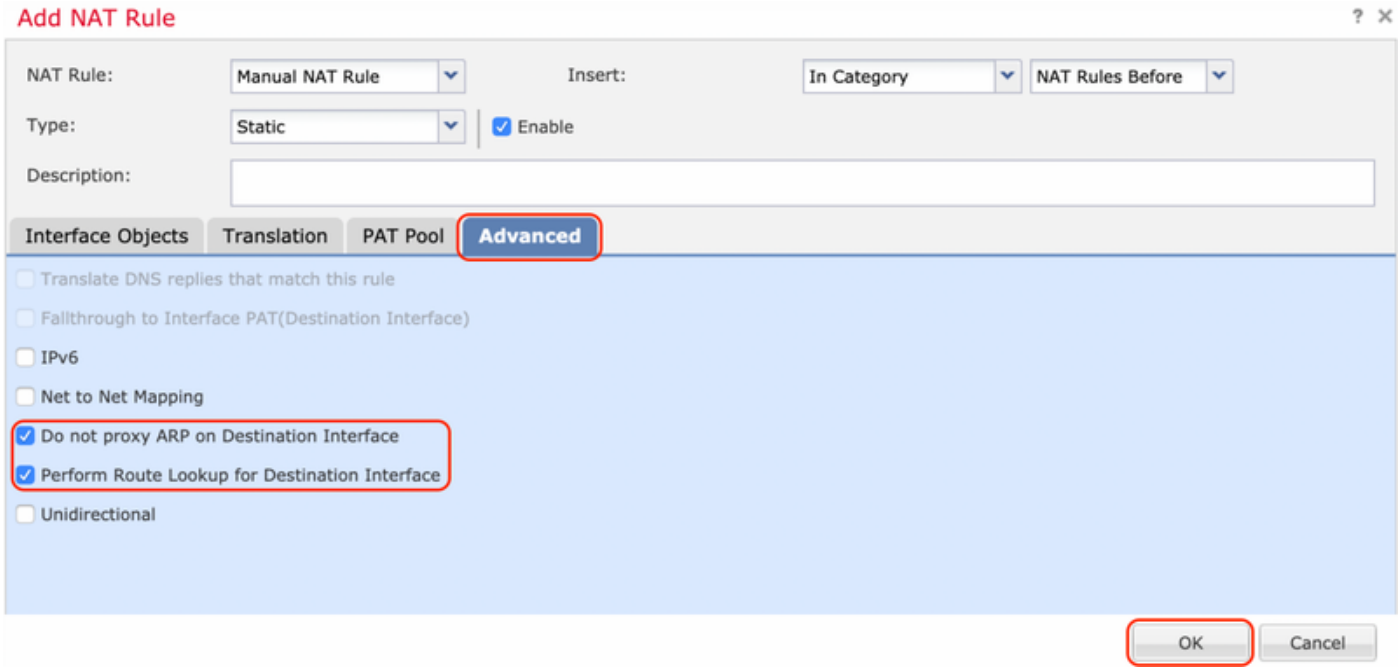
步骤3.创建新的静态手动NAT规则。

参考NAT规则的内部和外部接口。在接口对象选项卡中指定接口可防止这些规则影响来自其他接口的流量。

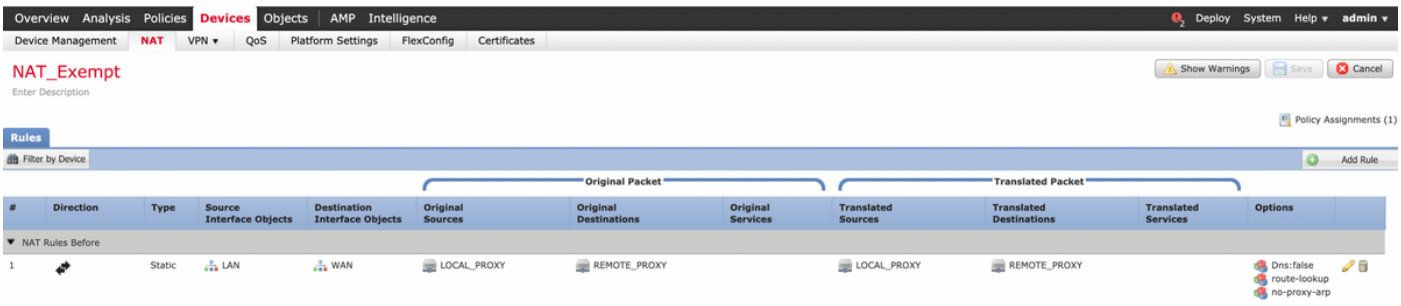
导航至Translation选项卡，并选择源子网和目标子网。由于这是NAT免除规则，请确保原始源/目标和转换后的源/目标相同。



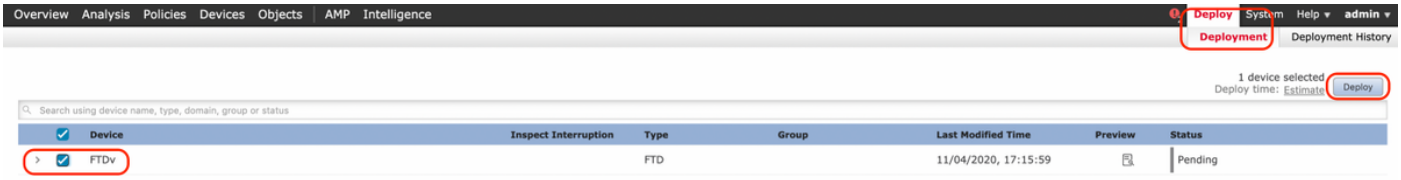
单击Advanced选项卡并启**用no-proxy-arp和route-lookup。**



保存此规则并确认NAT列表中的最终NAT语句。



步骤4.配置完成后，保存配置并将其部署到FTD。



验证

从LAN计算机启动相关流量，或者您可以在ASA上运行以下packet-tracer命令。

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

注意：此处Type = 128,Code=0表示ICMPv6“Echo Request”。

以下部分介绍可在ASAv或FTD LINA CLI上运行以检查IKEv2隧道状态的命令。

以下是ASA输出的示例：

```
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
```

故障排除

要排除ASA和FTD上的IKEv2隧道建立问题，请运行以下debug命令：

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

以下是工作IKEv2调试的示例以供参考：
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

参考

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