在FDM管理的FTD上配置站点到站点VPN

目录

简介

本文档介绍如何在FirePower设备管理器(FDM)管理的Firepower威胁防御(FTD)上配置站点到站点VPN。

先决条件

要求

Cisco 建议您了解以下主题：

- 对VPN的基本了解
- 体验FDN
- 使用自适应安全设备(ASA)命令行的体验

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科FTD 6.5
- ASA 9.10(1)32
- IKEv2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

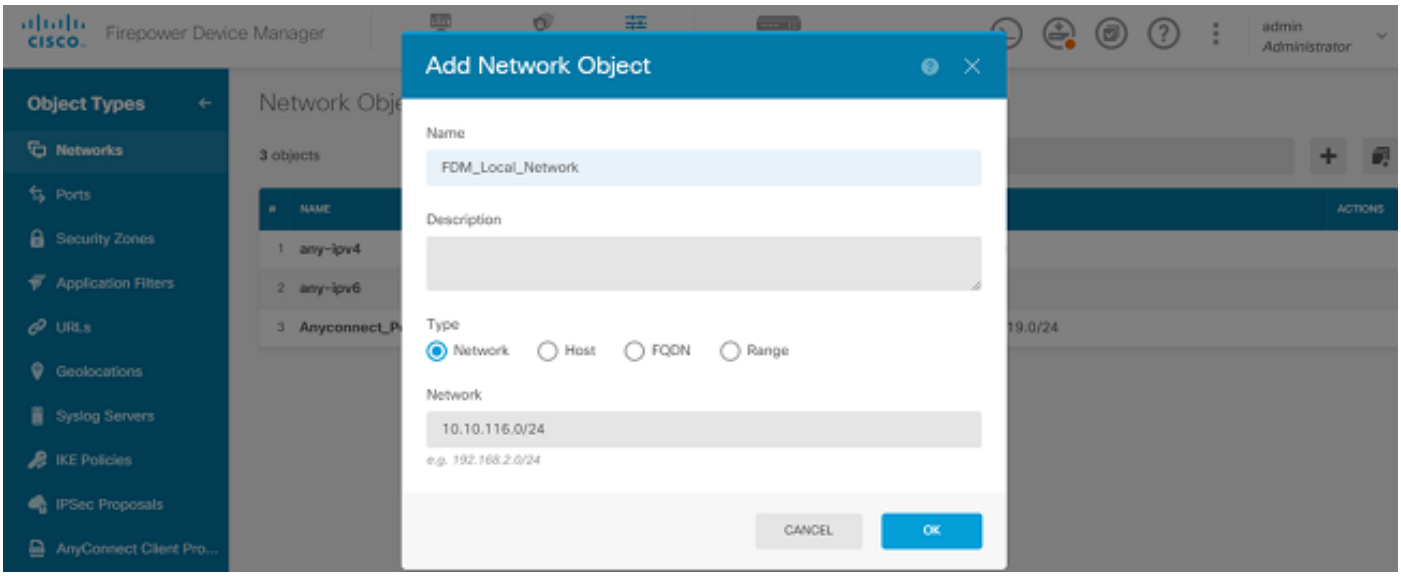
配置

从使用FDM的FTD配置开始。

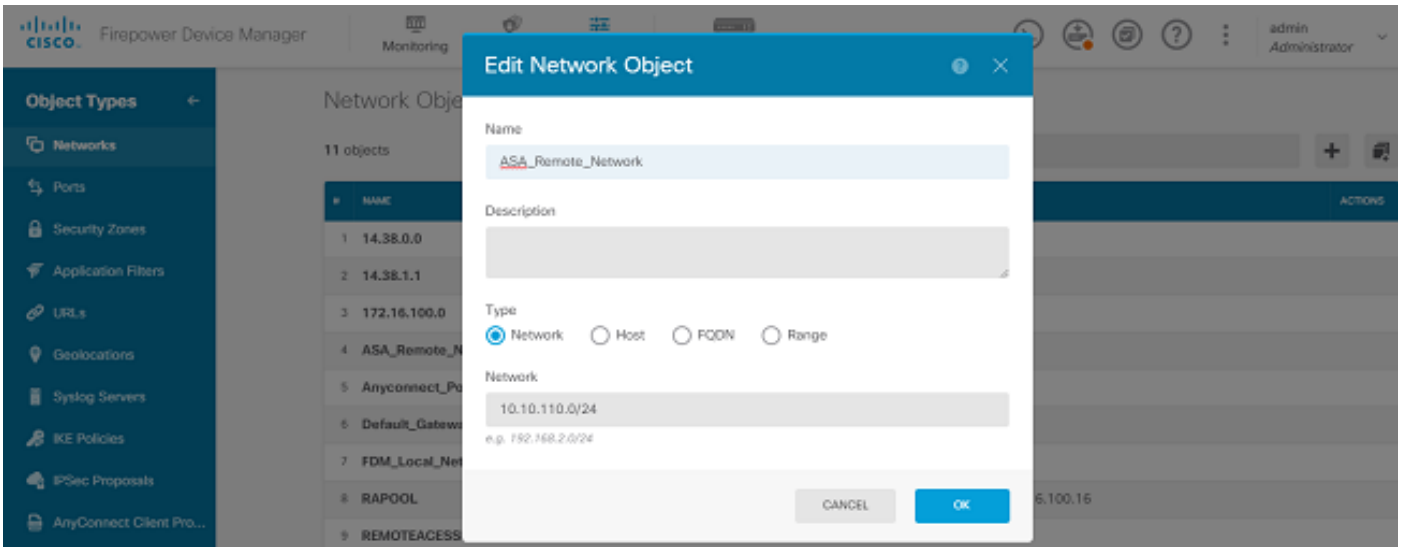
定义受保护的网络

导航到对象>网络>添加新网络。

通过FDM GUI配置LAN网络的对象。在FDM设备后面创建本地网络对象，如图所示。



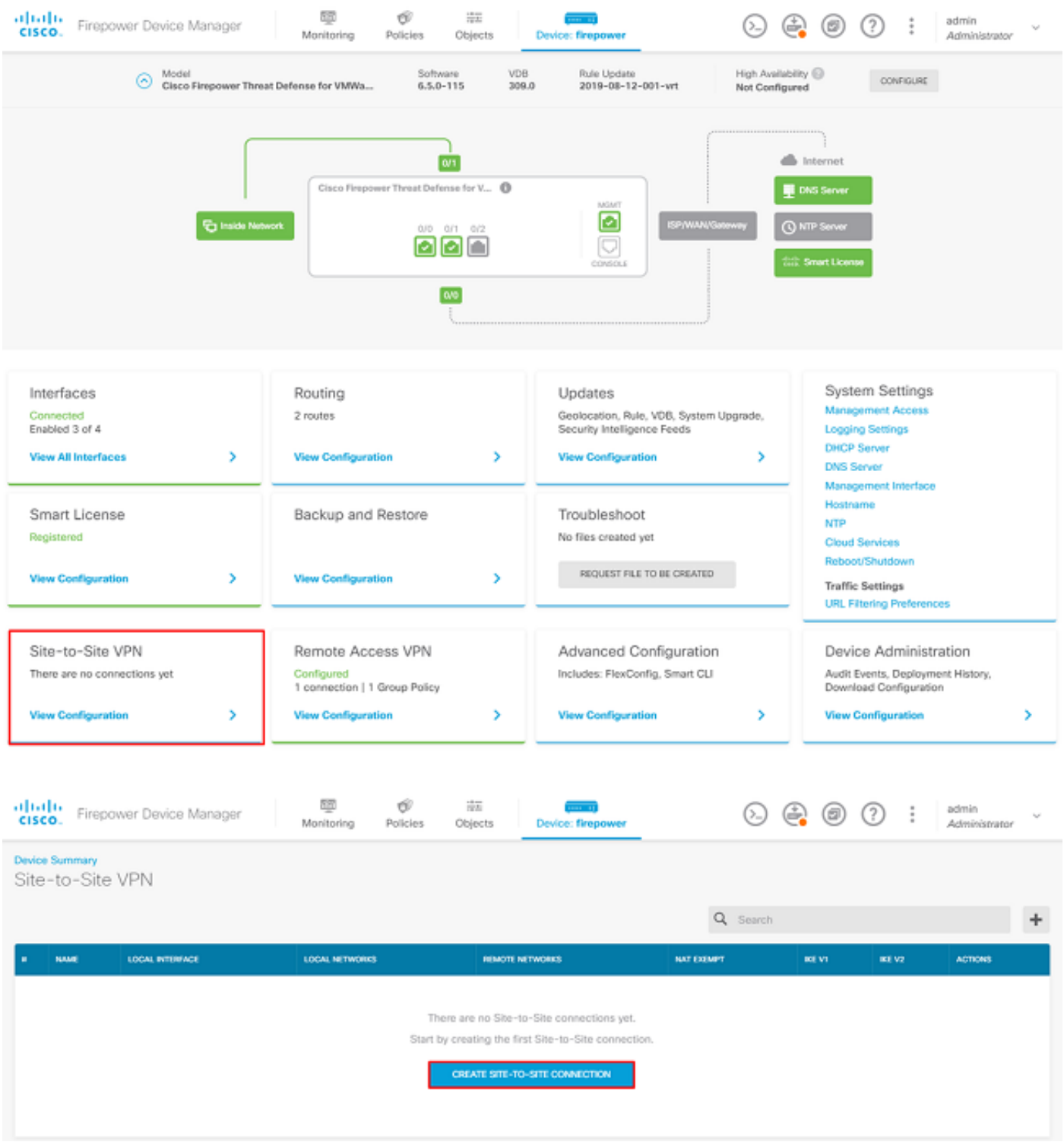
如图所示，在ASA设备后面创建远程网络对象。



配置站点到站点VPN

导航到站点到站点VPN >创建站点到站点连接。

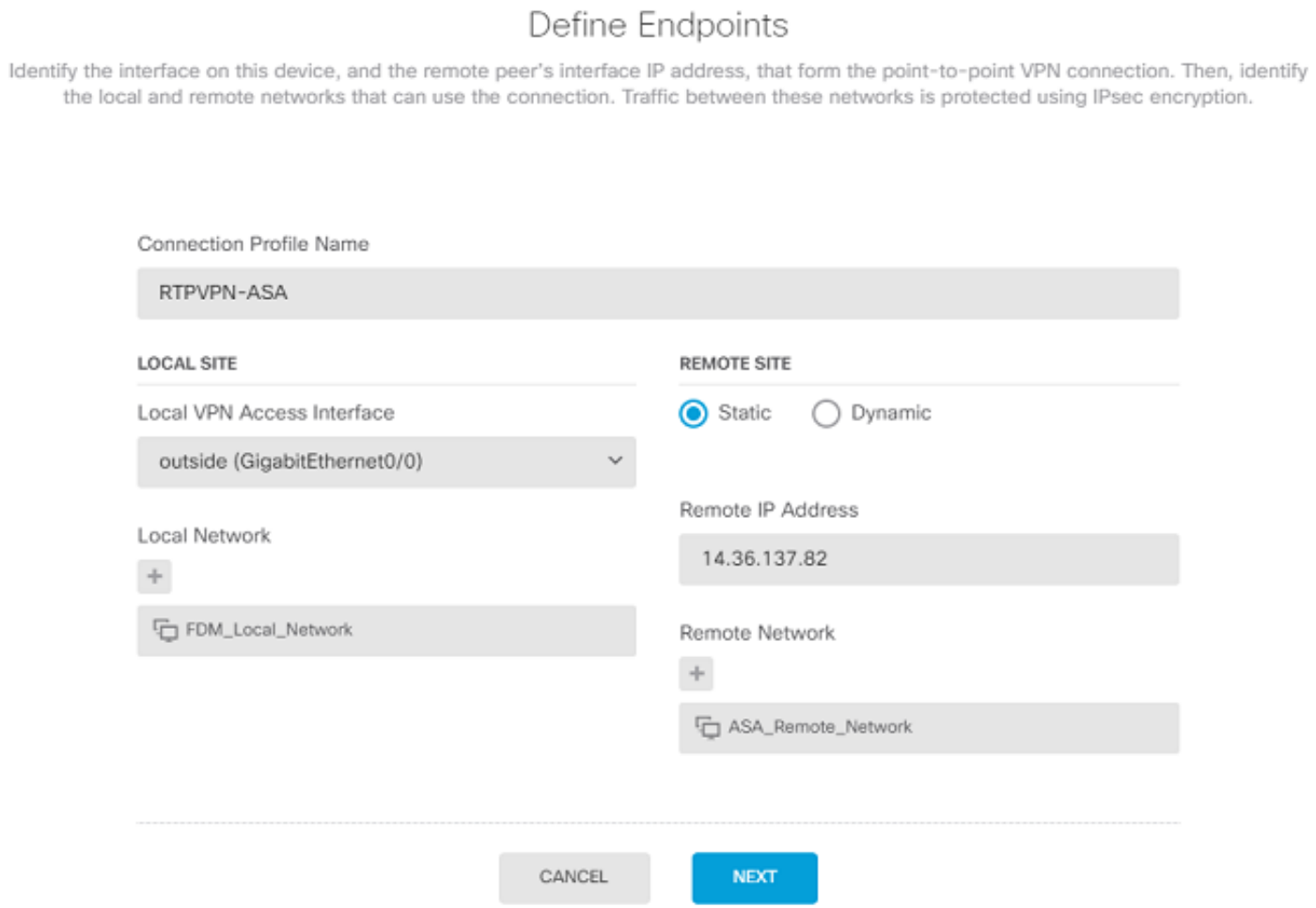
在FDM上执行“站点到站点”向导，如图所示。



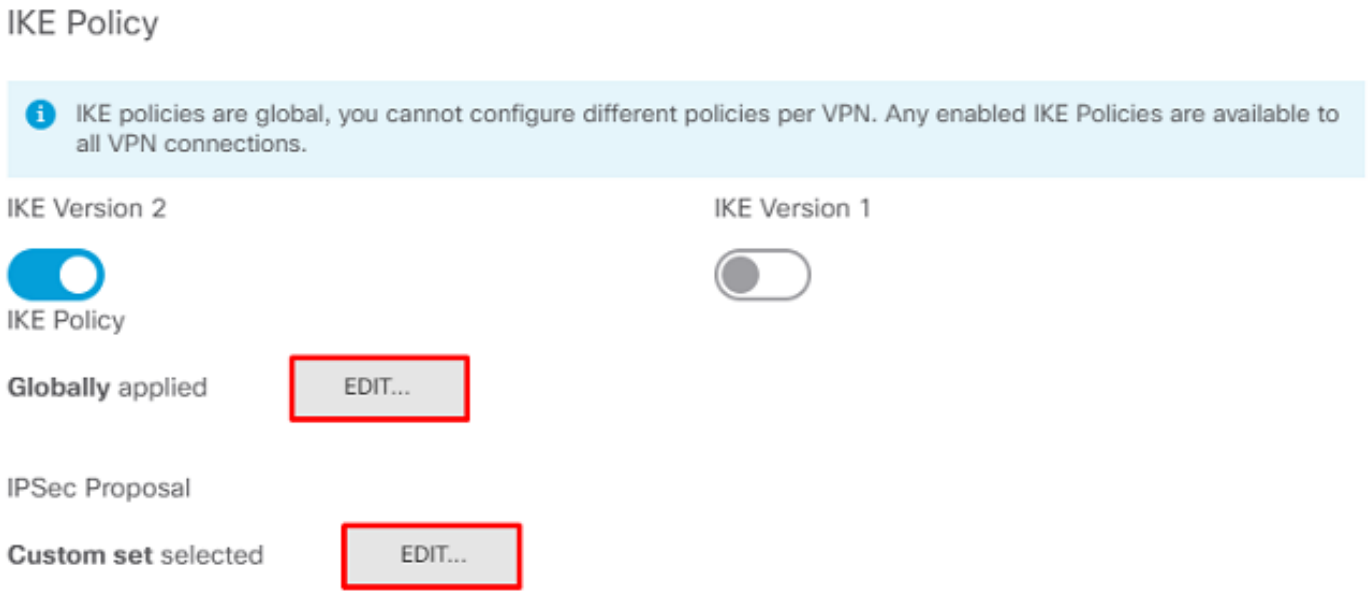
为站点到站点连接提供一个易于识别的连接配置文件名称。

为FTD选择正确的外部接口，然后选择Local network that needs be encrypted through the site to site VPN。

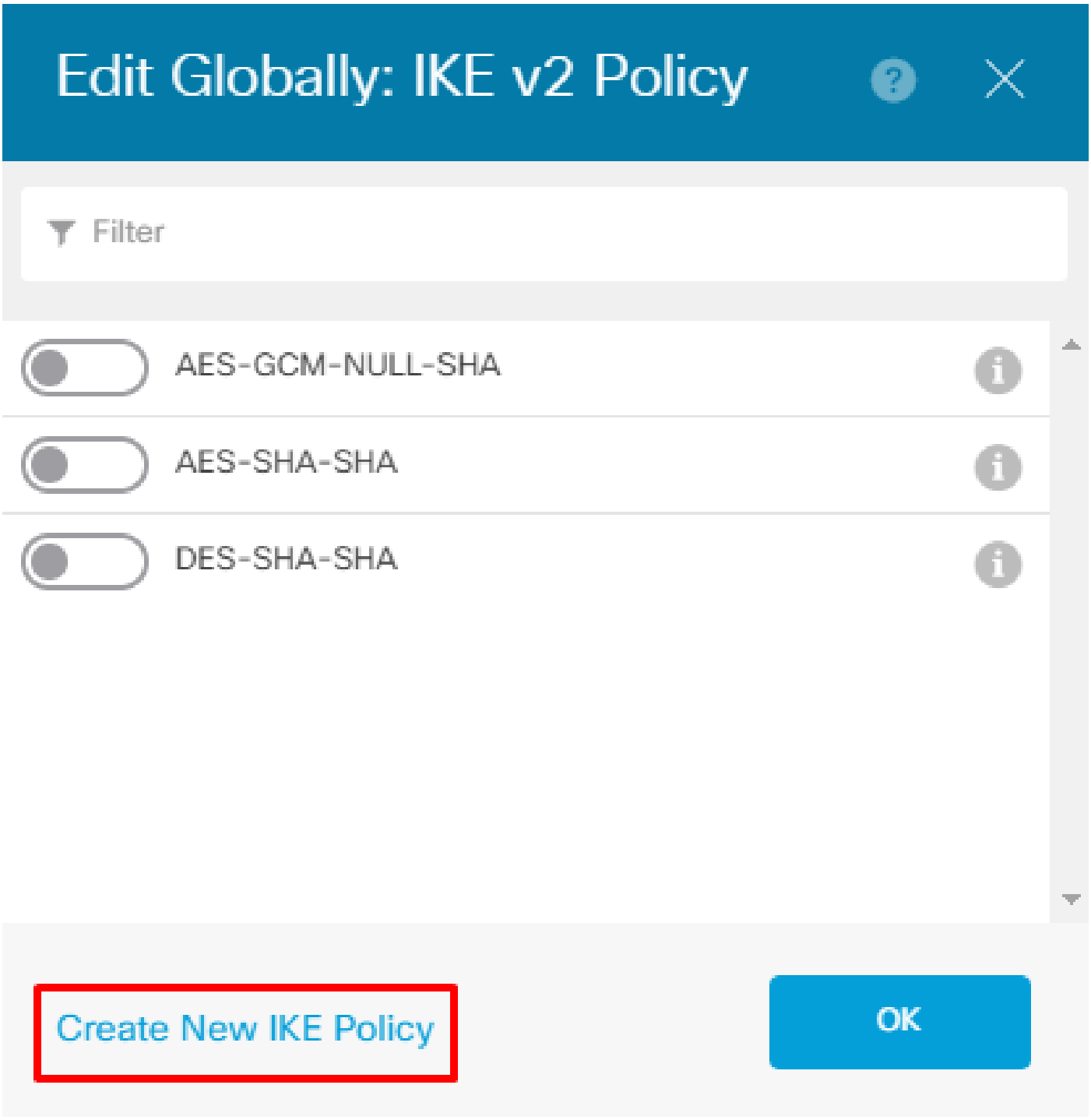
设置远程对等体的公共接口。然后，选择通过站点到站点VPN加密的远程对等设备的网络，如图所示。



在下一页上，选择Edit按钮以设置Internet密钥交换(IKE)参数，如图所示。

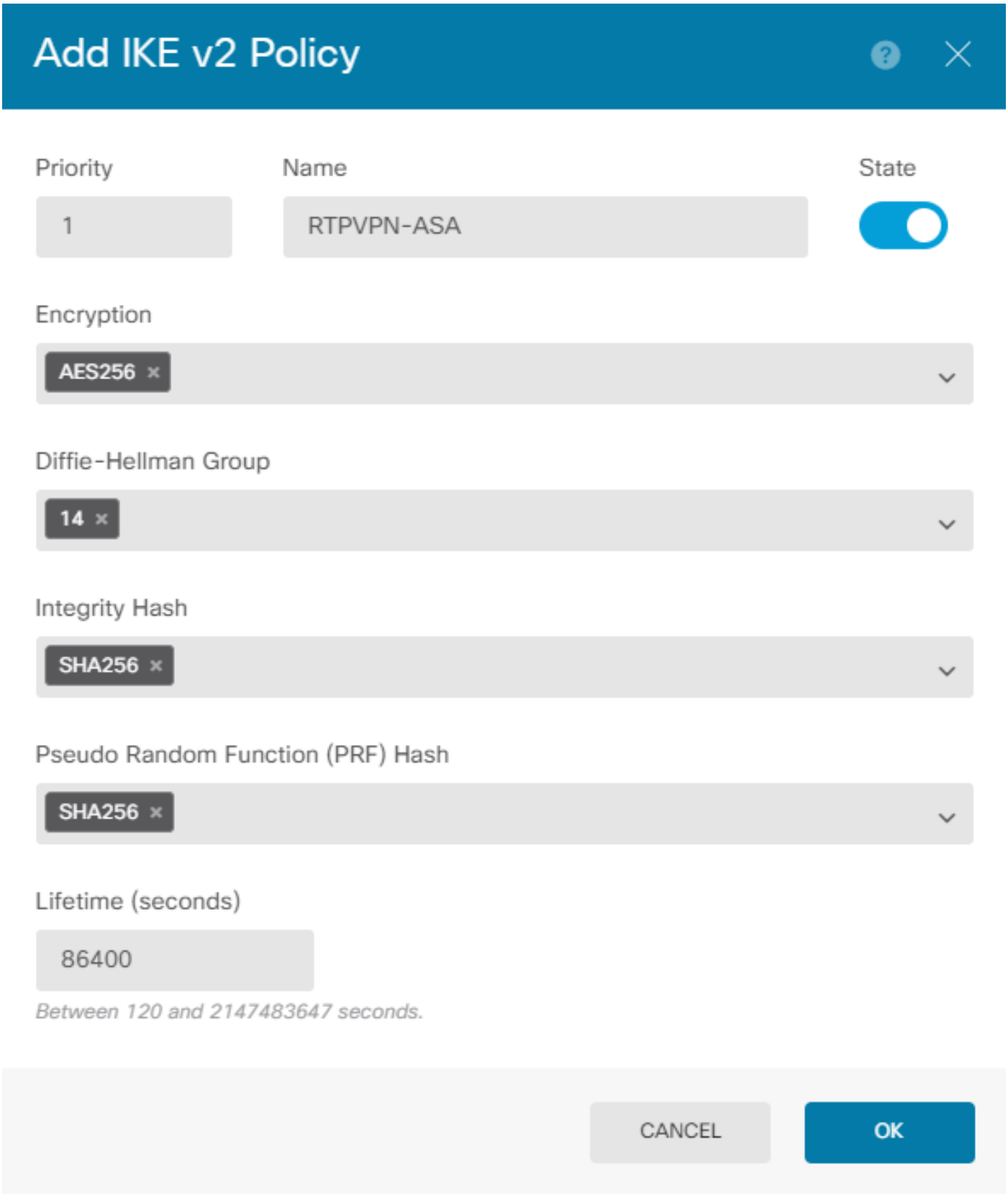


选择Create New IKE Policy按钮，如图所示。

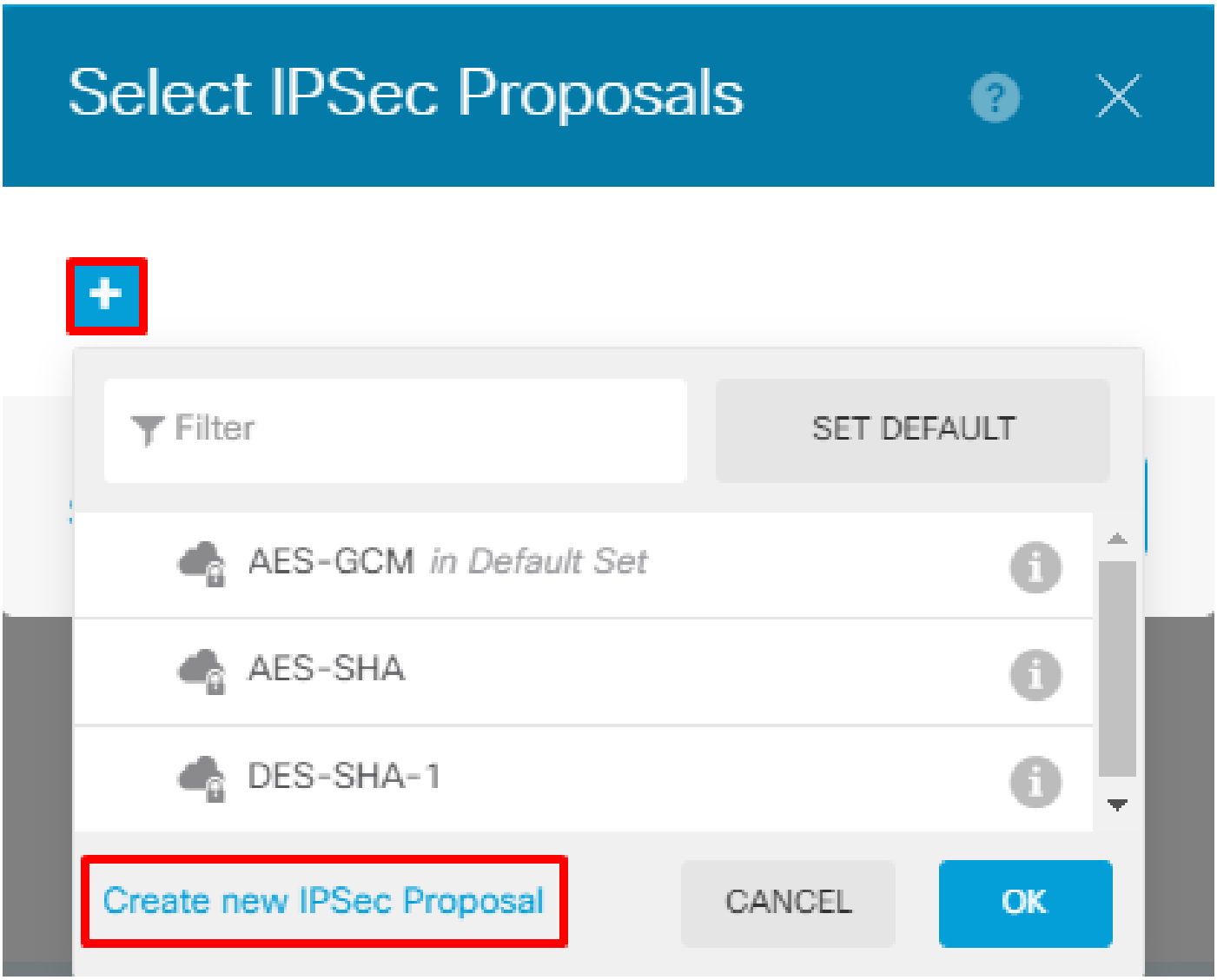


本指南将以下参数用于IKEv2初始交换：

加密AES-256
完整性SHA256
DH组14
PRF SHA256



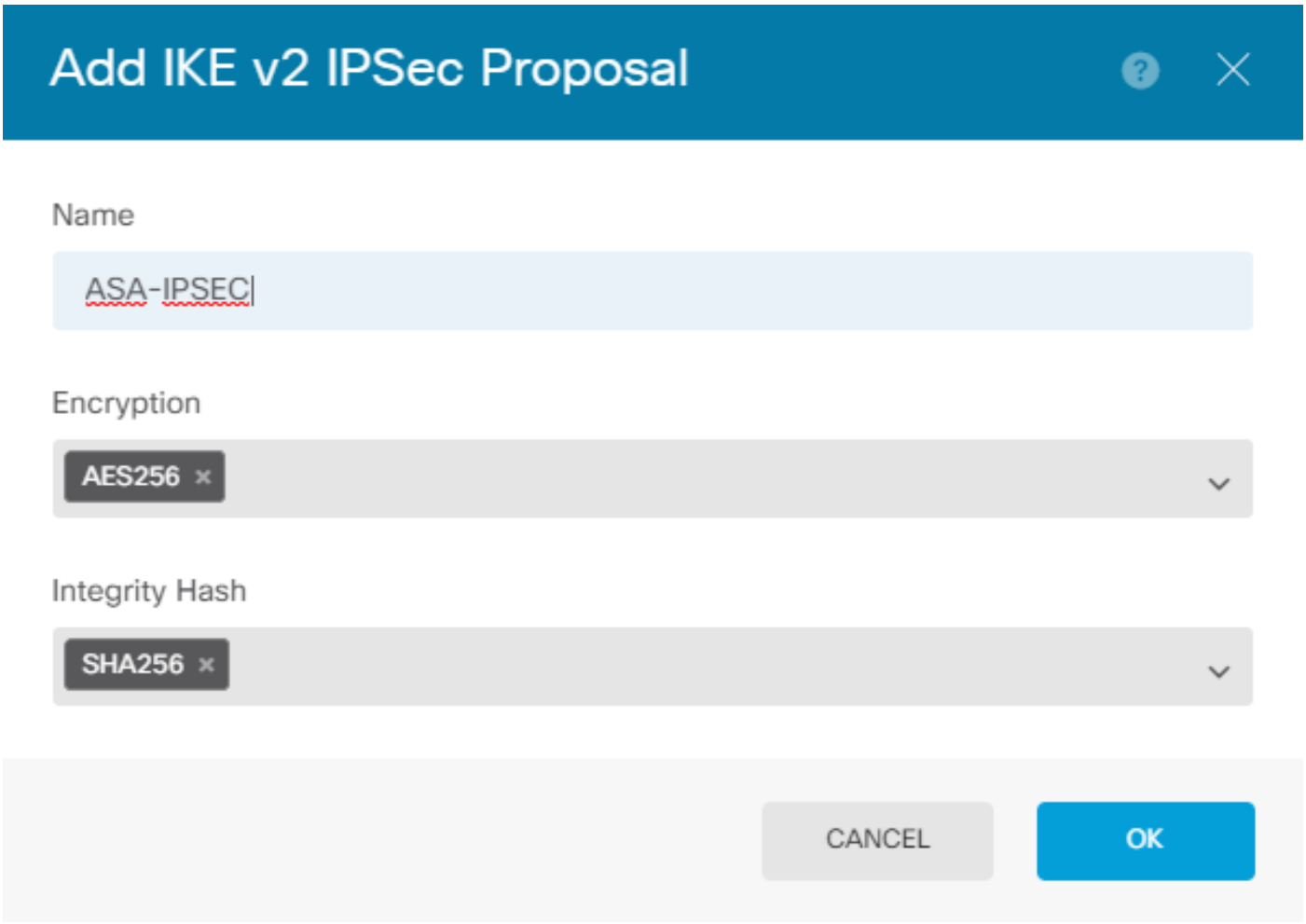
返回主页后，选择IPSec建议的Edit按钮。创建新的IPSec建议，如图所示。



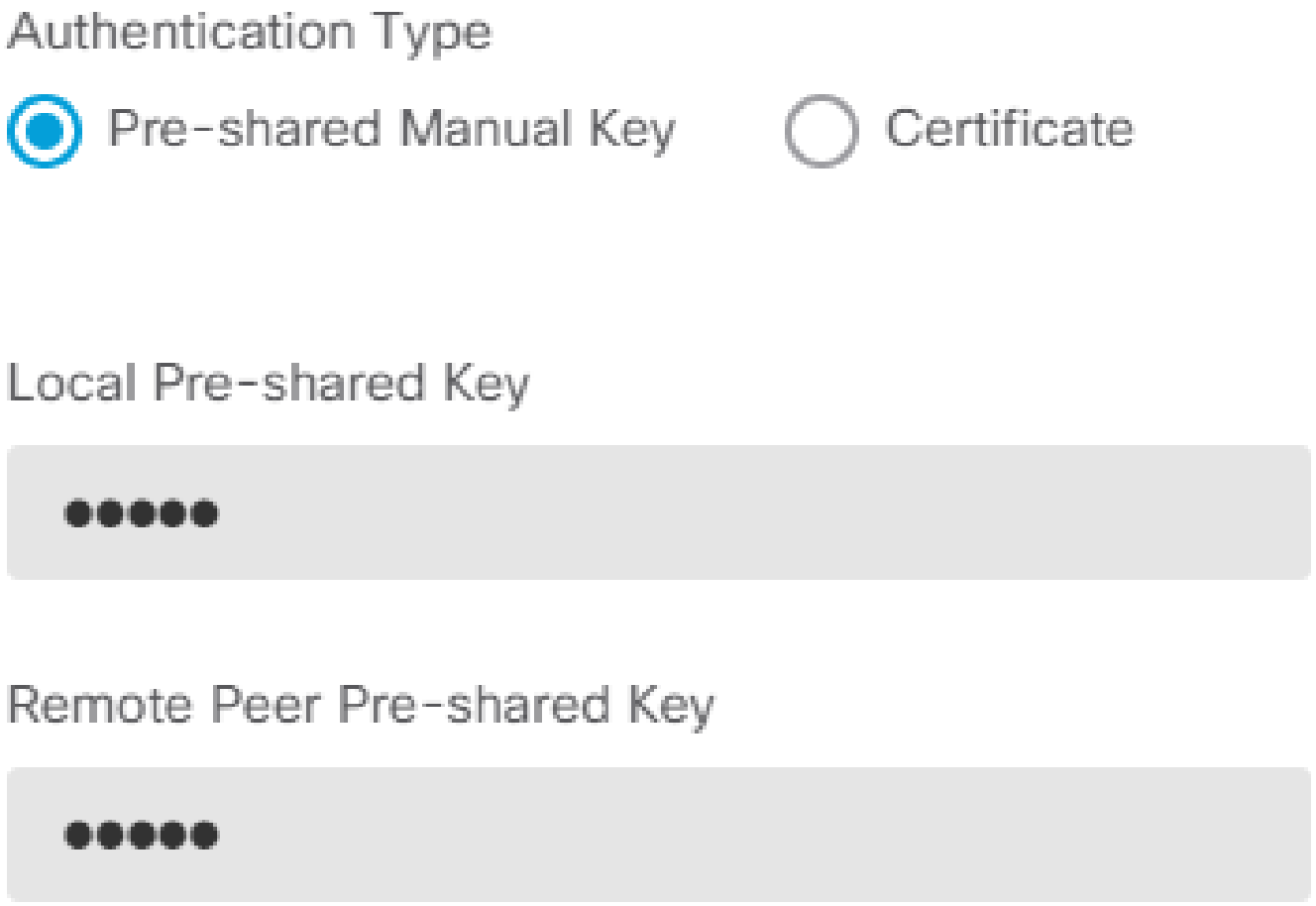
本指南将以下参数用于IPSec:

加密AES-256

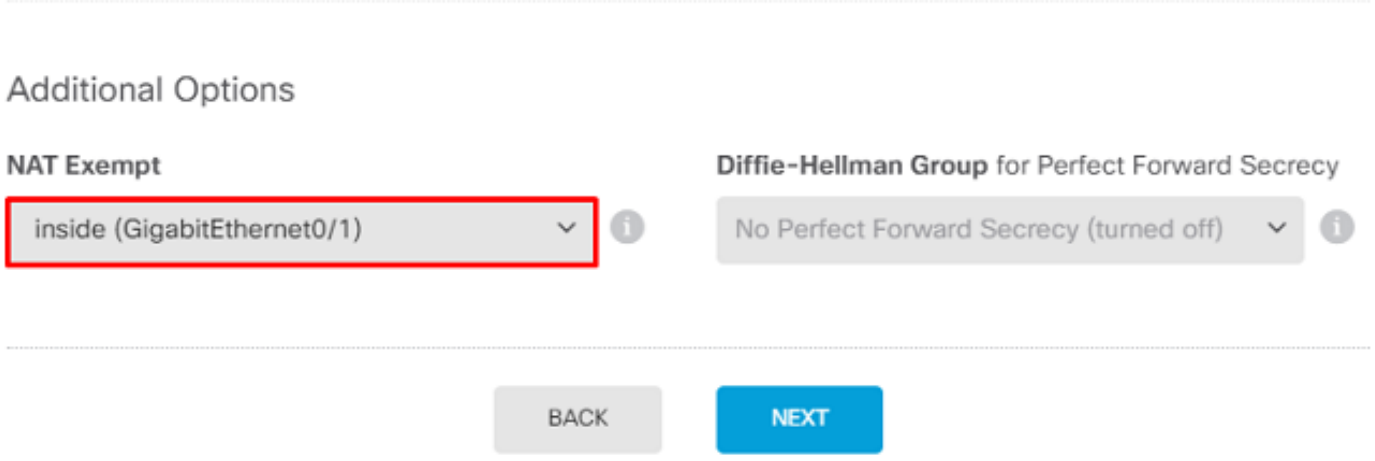
完整性SHA256



将身份验证设置为预共享密钥，并输入两端使用的预共享密钥(PSK)。本指南使用思科的PSK，如图所示。



设置内部NAT豁免接口。如果使用了多个内部接口，则需要在Policies > NAT下创建手动NAT免除规则。



在最后一页上，会显示站点到站点连接的摘要。确保选择了正确的IP地址，并且使用了正确的加密参数，然后点击“完成”按钮。 部署新的站点到站点VPN。

使用CLI完成ASA配置。

ASA 配置

1. 在ASA的外部接口上启用IKEv2:

```
Crypto ikev2 enable outside
```

2.创建定义在FTD上配置的相同参数的IKEv2策略：

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

3.创建允许IKEv2协议的组策略：

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

4.创建对等FTD公有IP地址的隧道组。引用组策略，并指定预共享密钥：

```
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.创建定义要加密的流量的访问列表：(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.创建引用FTD上指定的算法的IKEv2 IPsec提议：

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

7.创建将配置关联在一起的加密映射条目：

```
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.创建NAT免除语句，防止防火墙对VPN流量进行NAT:

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

验证

使用本部分可确认配置能否正常运行。

尝试通过VPN隧道发起流量。通过访问ASA或FTD的命令行，可以使用packet tracer命令完成此操作。使用packet-tracer命令启动VPN隧道时，必须运行两次才能验证隧道是否启动。首次发出该命令时，VPN隧道关闭，因此packet-tracer命令在VPN加密DROP时失败。请勿将防火墙的内部IP地址用作Packet Tracer中的源IP地址，因为此操作始终失败。

```
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
```

要监控隧道状态，请导航到FTD或ASA的CLI。

在FTD CLI中，使用命令show crypto ikev2 sa验证phase-1和phase-2。

```
> 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
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

初始连接问题

构建VPN时，需要双方协商隧道。因此，当您排除任何类型的隧道故障时，最好让对话双方都参与进来。 有关如何调试IKEv2隧道的详细指南位于：[如何调试IKEv2 VPN]

隧道故障的最常见原因是连接问题。确定这一点的最佳方法是在设备上捕获数据包。

使用此命令获取设备上的数据包捕获：

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

捕获到位后，尝试通过VPN发送流量并检查数据包捕获中的双向流量。

使用命令show cap capout检查数据包捕获。

```
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
```

特定流量问题

用户遇到的常见流量问题包括：

- FTD后的路由问题 — 内部网络无法将数据包路由回分配的IP地址和VPN客户端。
- 访问控制列表阻止流量。
- VPN流量未绕过网络地址转换(NAT)。

相关信息

有关由FDM管理的FTD上的站点到站点VPN的详细信息，可在此处找到完整的配置指南。

- 《FDM配置指南》管理的FTD。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。