在FMC管理的FTD上，使用备用ISP链路配置IPSec站点到站点隧道的故障切换

目录

简介

本文档介绍如何使用FMC管理的FTD上的IP SLA跟踪功能为ISP链路配置基于加密映射的故障切换。

作者：Amanda Nava，思科TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本了解虚拟专用网络(VPN)
- 使用FTD的经验
- 使用FMC的经验
- 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版本：

- FMC版本6.6.0
- FTD版本6.6.0
- ASA 9.14.1 版

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。

背景信息

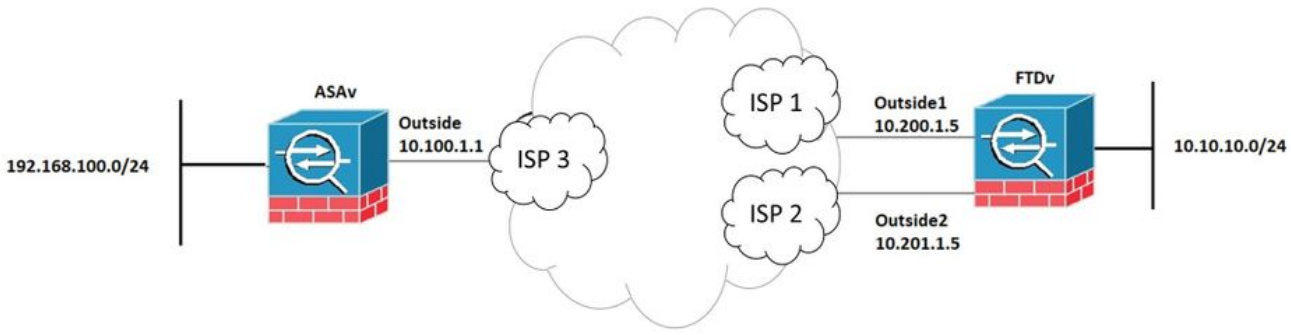
本文档介绍如何使用Firepower威胁防御(FTD)上的Internet协议服务级别协议(IP SLA)跟踪功能，为Internet服务提供商(ISP)备用链路配置基于加密映射的故障切换，由Firepower管理中心(FMC)管理。它还解释了当存在两个ISP且需要无缝故障切换时，如何为VPN流量配置网络地址转换(NAT)免除。

在此场景中，VPN从FTD建立到ASA，作为仅具有一个ISP接口的VPN对等体。FTD当时使用一个ISP链路来建立VPN。当主ISP链路断开时，FTD通过SLA Monitor接管辅助ISP链路，并建立VPN。

配置

网络图

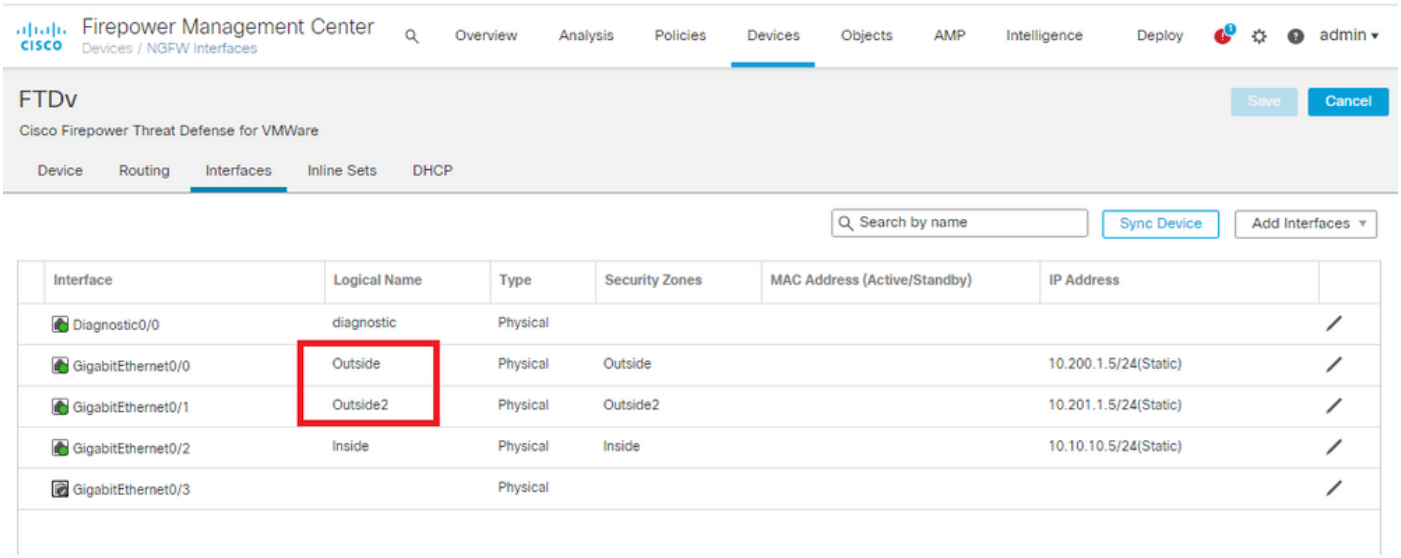
这是本文档中示例使用的拓扑：



配置FTD

步骤1:定义主要ISP接口和辅助ISP接口

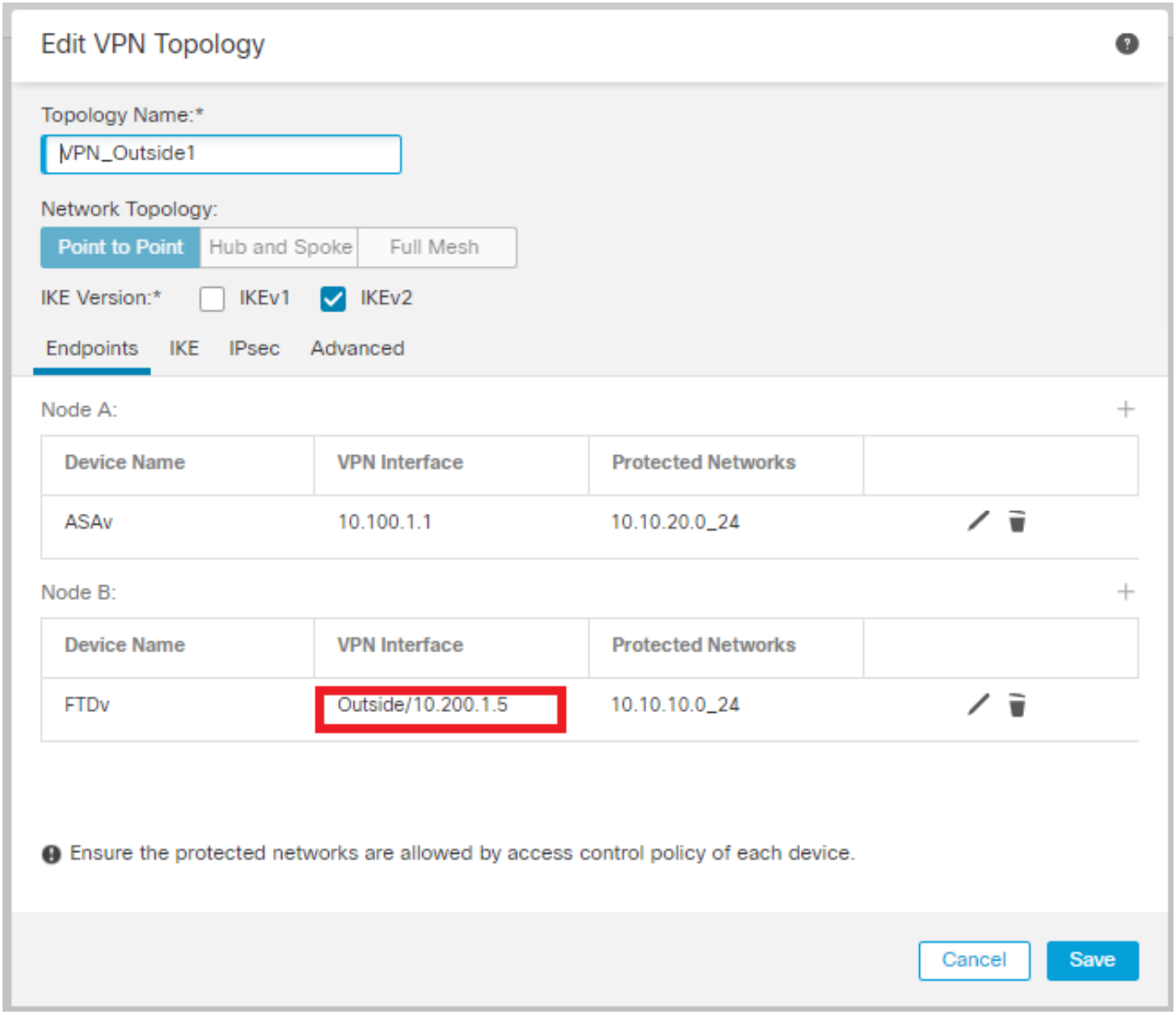
1.导航到设备>设备管理>接口，如图所示。



第二步：定义主ISP接口的VPN拓扑

1.导航到设备> VPN >站点到站点。 在添加VPN下，单击Firepower威胁防御设备，创建VPN并选择外部接口。

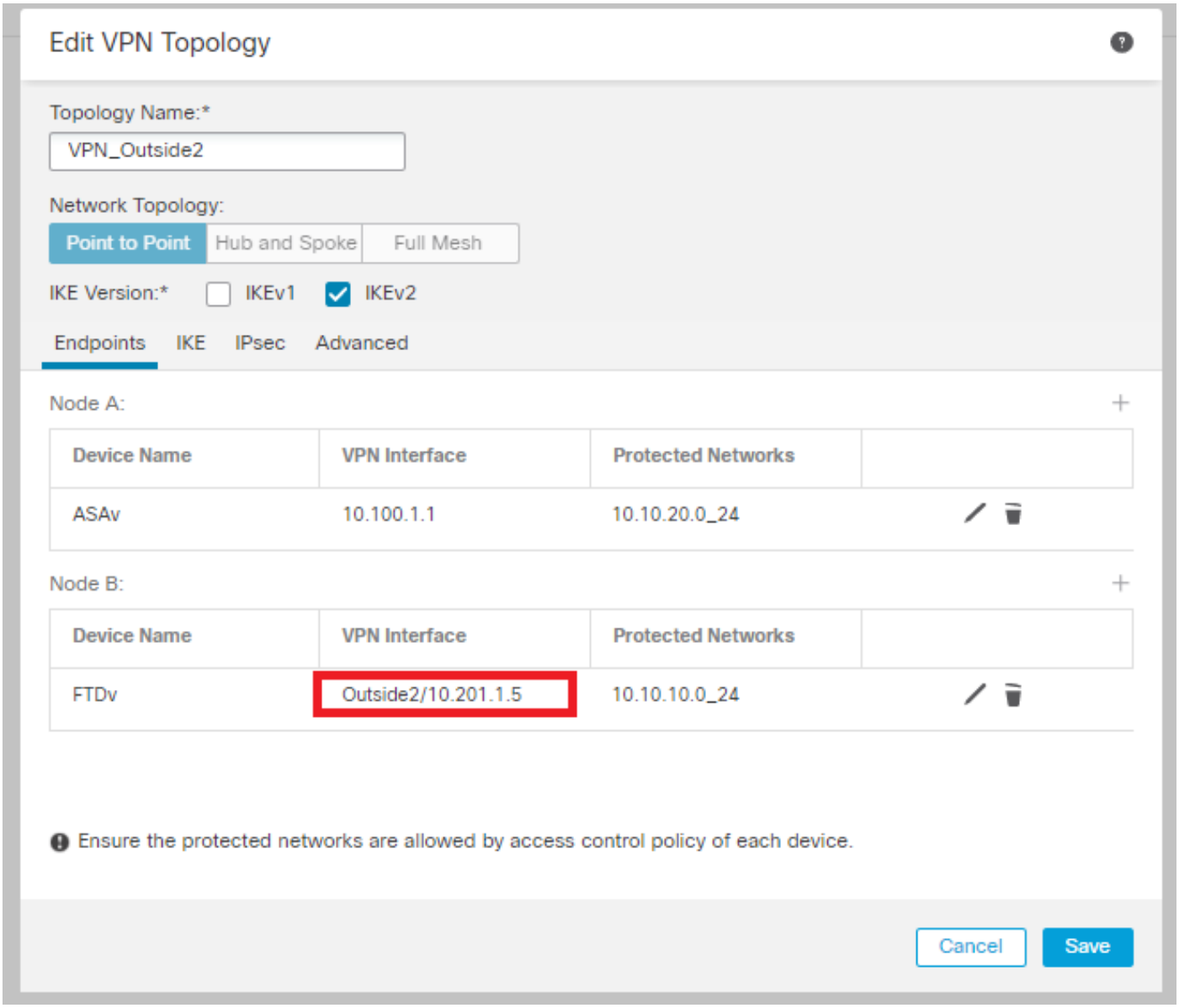
注意：本文档不介绍如何从头开始配置S2S VPN。有关FTD上S2S VPN配置的更多参考，请访问https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470-site-to-site-vpn-configuration-on-ftd-ma.html



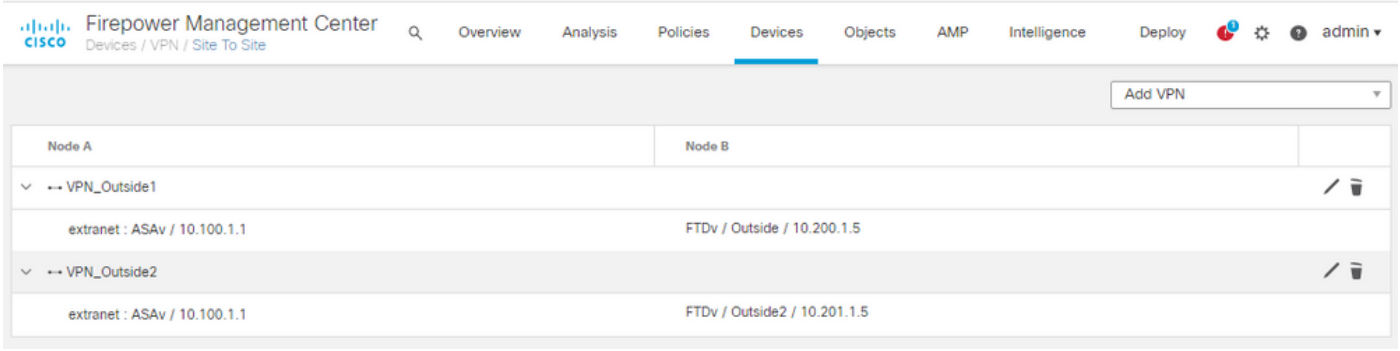
第三步：定义辅助ISP接口的VPN拓扑

1.导航到设备> VPN >站点到站点。 在Add VPN下，单击Firepower Threat Defense Device，创建VPN并选择Outside2接口。

注意：使用Outside2接口的VPN配置必须与Outside VPN拓扑完全相同，VPN接口除外。

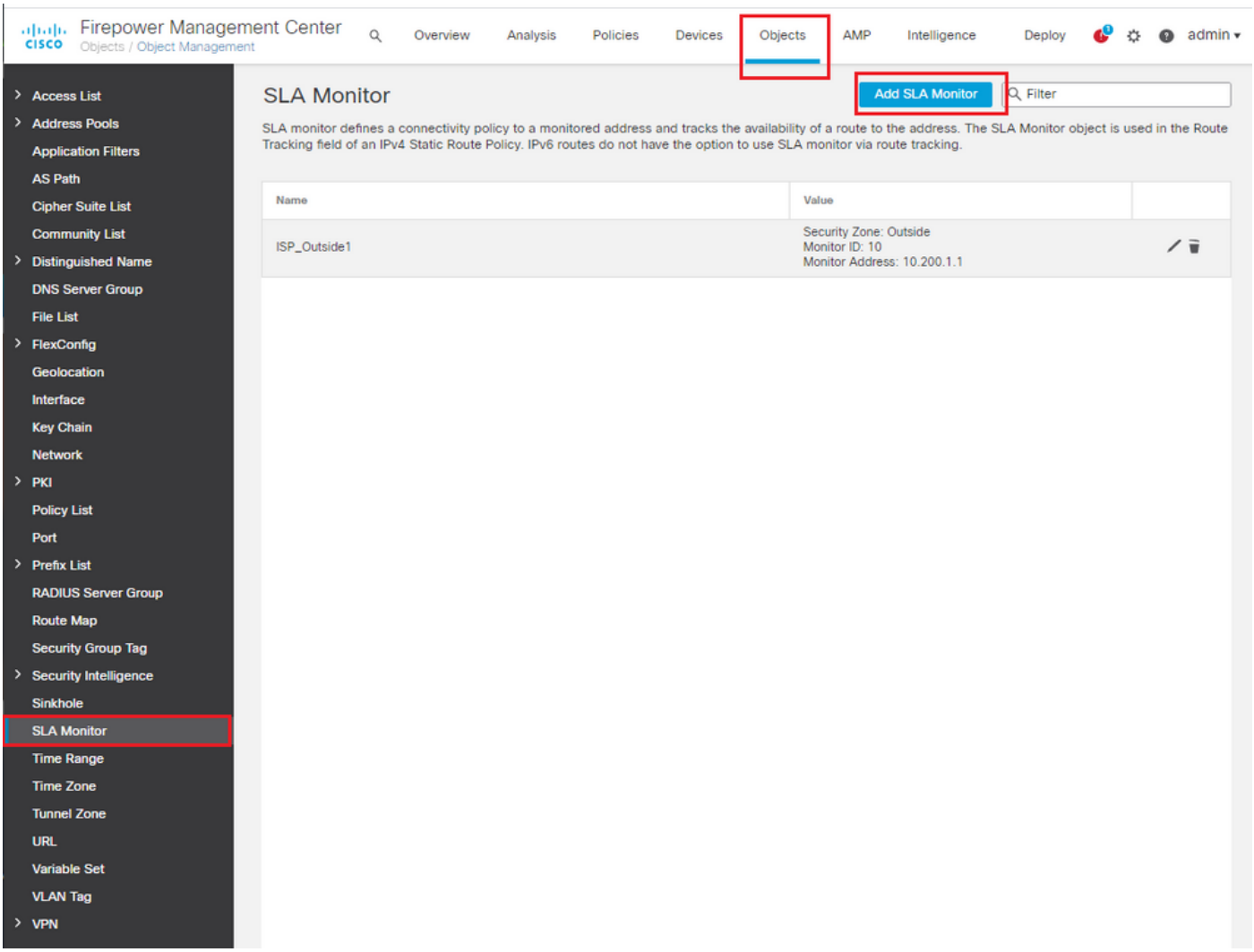


必须如图所示配置VPN拓扑。

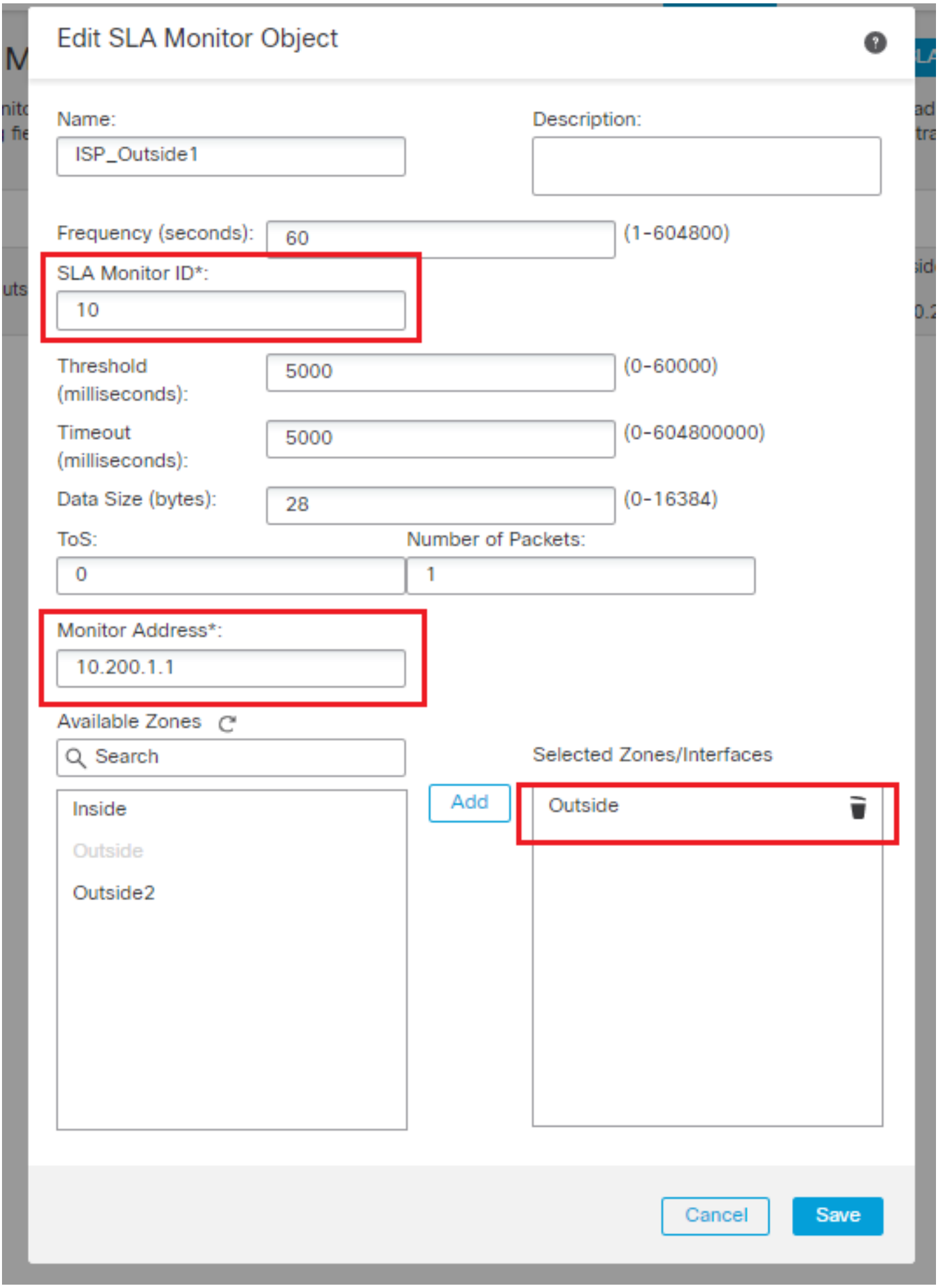


第四步：配置SLA监控器

1.导航到对象> SLA监控>添加SLA监控。 在添加VPN下，单击Firepower威胁防御设备，然后配置SLA监控器，如图所示。

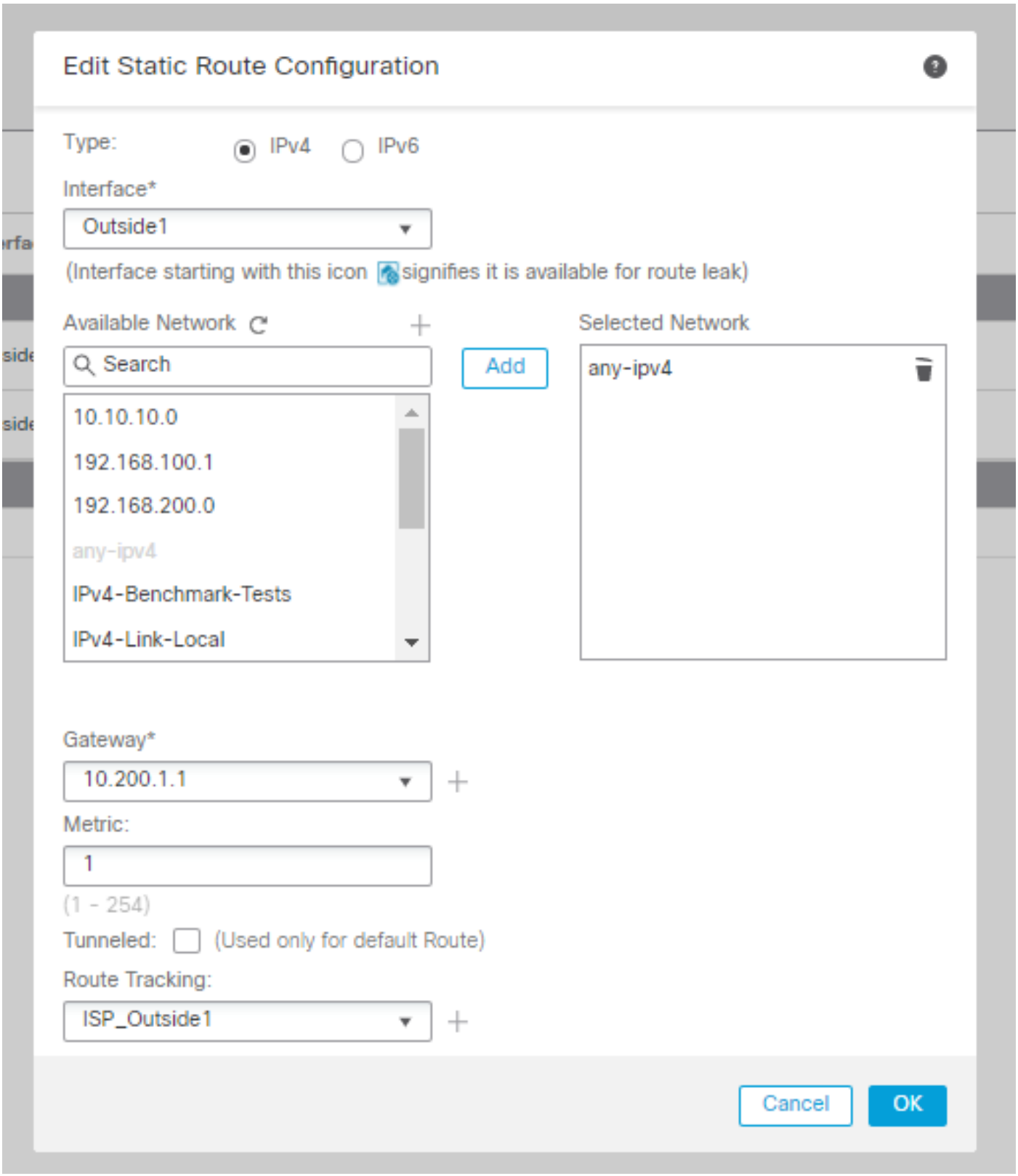


2.对于SLA Monitor ID*字段，请使用Outside next-hop IP address。

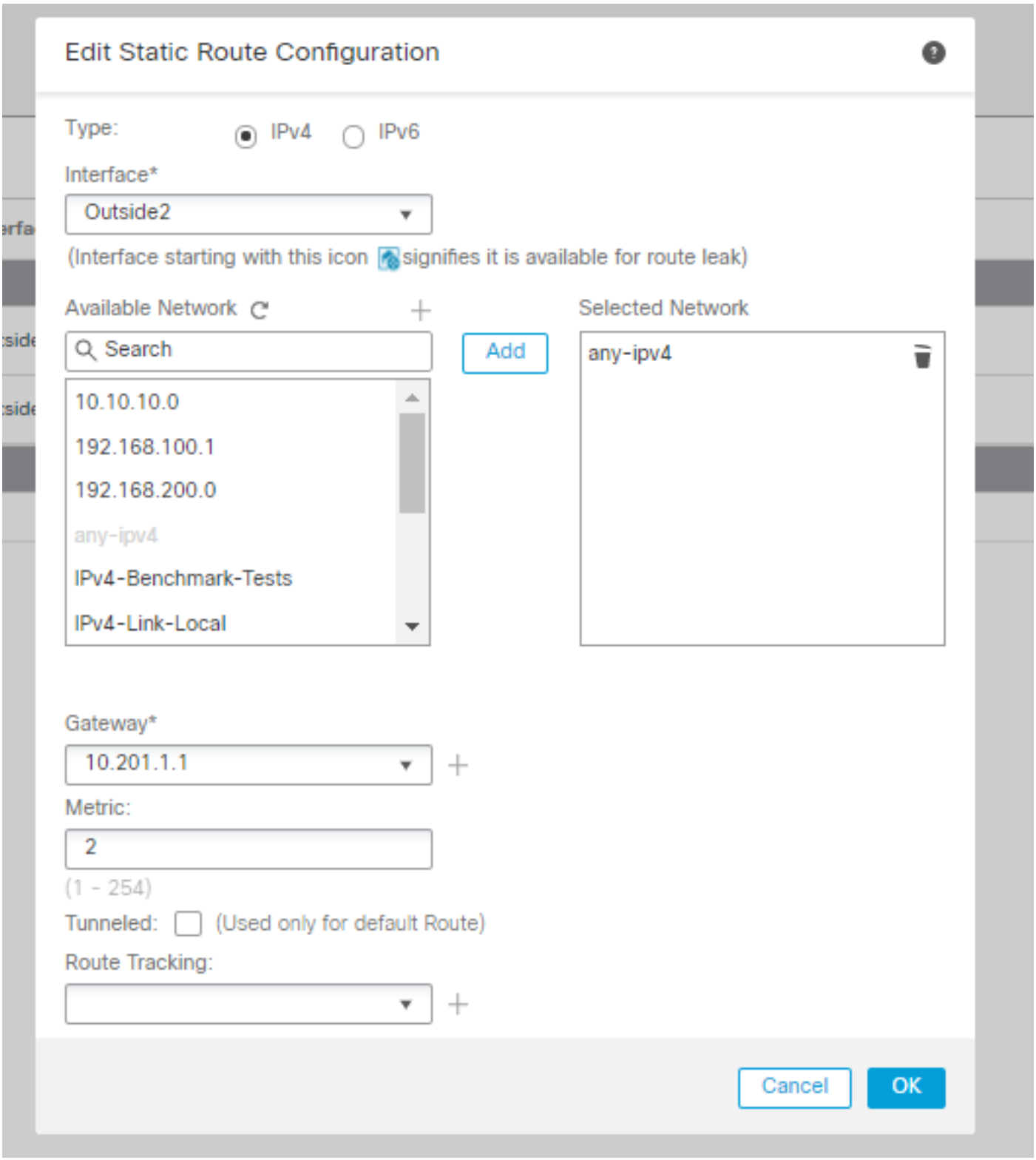

Edit SLA Monitor Object
Name:
ISP_Outside1
Description:
Frequency (seconds):
60
(1-604800)
SLA Monitor ID*:
10
Threshold (milliseconds):
5000
(0-60000)
Timeout (milliseconds):
5000
(0-604800000)
Data Size (bytes):
28
(0-16384)
ToS:
0
Number of Packets:
1
Monitor Address*:
10.200.1.1
Available Zones
Search
Inside
Outside
Outside2
Add
Selected Zones/Interfaces
Outside
Cancel
Save

第五步：使用SLA监控器配置静态路由

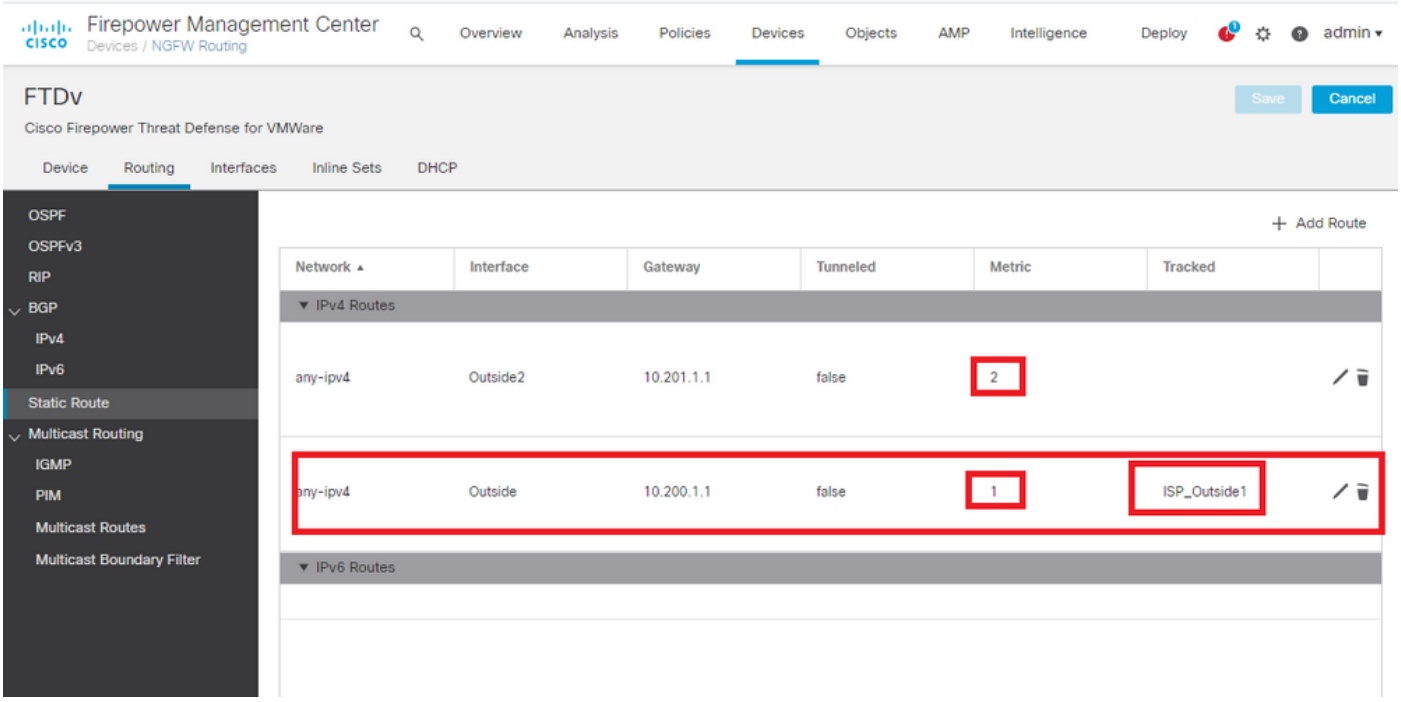
1.导航到设备>路由>静态路由。选择Add Route，并使用Route tracking字段中的SLA Monitor信息（步骤4中创建）配置外部（主）接口的默认路由。



2.配置Outside2（辅助）接口的默认路由。Metric值必须高于主默认路由。本部分不需要路由跟踪字段。

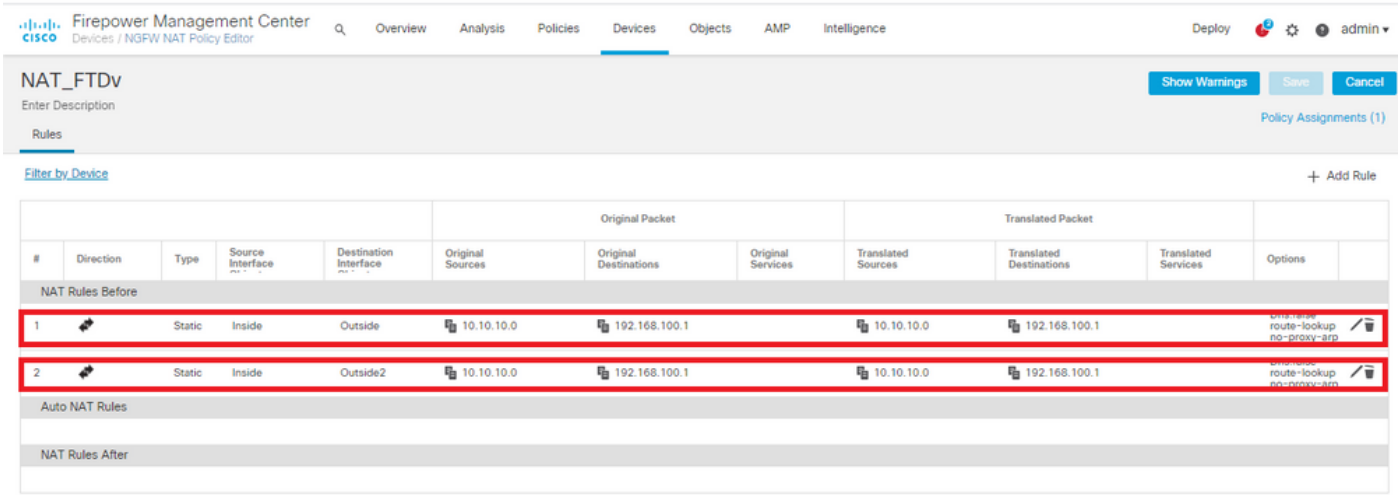

Edit Static Route Configuration
Type:
IPv4
IPv6
Interface*
Outside2
(Interface starting with this icon signifies it is available for route leak)
Available Network
Search
Add
Selected Network
any-ipv4
10.10.10.0
192.168.100.1
192.168.200.0
any-ipv4
IPv4-Benchmark-Tests
IPv4-Link-Local
Gateway*
10.201.1.1
Metric:
2
(1 - 254)
Tunneled:
(Used only for default Route)
Route Tracking:
Cancel
OK

必须如图所示配置路由。



第六步：配置NAT免除

1.导航到设备> NAT > NAT策略，然后选择以FTD设备为目标的策略。选择Add Rule并配置每个ISP接口（Outside和Outside2）的NAT免除。除目标接口外，NAT规则必须相同。



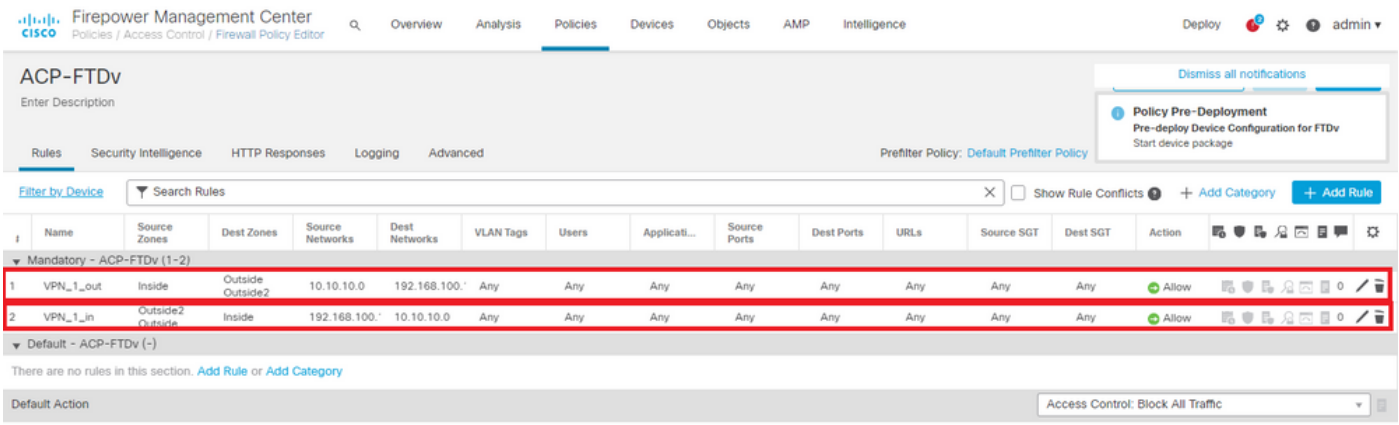
注意：对于此场景，两个NAT规则都要求启用路由查找。否则，流量将到达第一条规则，并且不会保留至故障切换路由。如果未启用路由查找，流量将始终使用（第一个NAT规则）外部接口发送。启用Route-lookup后，流量始终保持到通过SLA监控器控制的路由表。

步骤 7.为相关流量配置访问控制策略

1.定位至策略>访问控制>选择访问控制策略。 要添加规则，请点击Add Rule，如图所示。

配置一条从Inside到Outside区域（Outside1和Outside2）的规则，允许从10.10.10.0/24到192.168.100/24的相关流量。

配置从Outside zones（Outside1和Outside 2）到Inside的另一个规则，允许从192.168.100/24到10.10.10.0/24的相关流量。



配置 ASA

注意：对于此特定场景，在IKEv2加密映射上配置备份对等体，此功能要求ASA在9.14.1或更高版本上。如果您的ASA运行的是较旧版本，请使用IKEv1作为解决方法。有关详细信息，请参阅Cisco Bug ID CSCud22276。

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 IKEV2 internal
group-policy IKEV2 attributes
 vpn-tunnel-protocol ikev2
```

4.为每个外部FTD IP地址（Outside1和Outside2）创建一个隧道组。引用组策略并指定预共享密钥：

```
tunnel-group 10.200.1.5 type ipsec-l2l
tunnel-group 10.200.1.5 general-attributes
 default-group-policy IKEV2
tunnel-group 10.200.1.5 ipsec-attributes
 ikev2 remote-authentication pre-shared-key Cisco123
 ikev2 local-authentication pre-shared-key Cisco123

tunnel-group 10.201.1.5 type ipsec-l2l
tunnel-group 10.201.1.5 general-attributes
 default-group-policy IKEV2
tunnel-group 10.201.1.5 ipsec-attributes
 ikev2 remote-authentication pre-shared-key Cisco123
 ikev2 local-authentication pre-shared-key Cisco123
```

5.创建定义要加密的流量的访问列表：(FTD — 子网10.10.10.0/24)(ASA子网192.168.100.0/24):

```
Object network FTD-Subnet
 Subnet 10.10.10.0 255.255.255.0
Object network ASA-Subnet
 Subnet 192.168.100.0 255.255.255.0
access-list VPN_1 extended permit ip 192.168.100.0 255.255.255.0 10.10.10.0 255.255.255.0
```

6.创建ikev2 ipsec-proposal以引用FTD上指定的算法：

```
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 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，并添加Outside1和Outside2 FTD IP地址：

```
crypto map CSM_Outside_map 1 match address VPN_1
crypto map CSM_Outside_map 1 set peer 10.200.1.5 10.201.1.5
crypto map CSM_Outside_map 1 set ikev2 ipsec-proposal CSM_IP_1
crypto map CSM_Outside_map 1 set reverse-route
crypto map CSM_Outside_map 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 ASA-Subnet ASA-Subnet destination static FTD-Subnet FTD-Subnet
```

验证

使用本部分可确认配置能否正常运行。

FTD

在命令行中，使用show crypto ikev2 sa命令验证VPN状态。

注意：已建立VPN，其中Outside1的IP地址(10.200.1.5)为本地地址。

```
firepower# sh crypto  ikev2 sa

IKEv2 SAs:

Session-id:24, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 Remote
373101057 10.200.1.5/500                                        10.100.1.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/37 sec
Child sa: local selector  10.10.10.0/0 - 10.10.10.255/65535
          remote selector 192.168.100.0/0 - 192.168.100.255/65535
          ESP spi in/out: 0x829ed58d/0x2051ccc9
```

路由

默认路由显示Outside1的下一跳IP地址。

```
firepower# sh route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.200.1.1 to network 0.0.0.0
```

```
S*       0.0.0.0 0.0.0.0 [1/0] via 10.200.1.1, Outside1
C        10.10.10.0 255.255.255.0 is directly connected, Inside
L        10.10.10.5 255.255.255.255 is directly connected, Inside
C        10.200.1.0 255.255.255.0 is directly connected, Outside1
L        10.200.1.5 255.255.255.255 is directly connected, Outside1
C        10.201.1.0 255.255.255.0 is directly connected, Outside2
L        10.201.1.5 255.255.255.255 is directly connected, Outside2
```

跟踪

如show track 1输出所示，“Reachability is Up”。

```
firepower#   sh track 1
Track 1
  Response Time Reporter 10 reachability
  Reachability is Up                        <-----
  36 changes, last change 00:00:04
  Latest operation return code: OK
  Latest RTT (millisecs) 1
  Tracked by:
    STATIC-IP-ROUTING 0
```

NAT

需要确认相关流量通过Outside1接口到达NAT免除规则。

使用“packet-tracer input Inside icmp 10.10.1 8 0 192.168.100.10 detail”命令验证应用于相关流量的NAT规则。

```
firepower# packet-tracer input inside icmp 10.10.10.1 8 0 192.168.100.1 det

---------------OMITTED OUTPUT -----------------
Phase: 4
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.
Additional Information:
NAT divert to egress interface Outside1(vrfid:0)
Untranslate 192.168.100.1/0 to 192.168.100.1/0

---------------OMITTED OUTPUT -----------------

Phase: 7
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.
Additional Information:
```

```
Static translate 10.10.10.1/0 to 10.10.10.1/0
 Forward Flow based lookup yields rule:
 in  id=0x2b3e09576290, priority=6, domain=nat, deny=false
        hits=19, user_data=0x2b3e0c341370, cs_id=0x0, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Inside(vrfid:0), output_ifc=Outside1(vrfid:0)

Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true
        hits=3596, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

---------------OMITTED OUTPUT -----------------
Phase: 12
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x2b3e0c8d0250, priority=70, domain=encrypt, deny=false
        hits=5, user_data=0x16794, cs_id=0x2b3e0b633c60, reverse, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=any(vrfid:65535), output_ifc=Outside1

Phase: 13
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x2b3e095d49a0, priority=6, domain=nat-reverse, deny=false
        hits=1, user_data=0x2b3e0c3544f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Inside(vrfid:0), output_ifc=Outside1(vrfid:0)

Phase: 14
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x2b3e0c8ad890, priority=70, domain=ipsec-tunnel-flow, deny=false
        hits=5, user_data=0x192ec, cs_id=0x2b3e0b633c60, reverse, flags=0x0, protocol=0
        src ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Outside1(vrfid:0), output_ifc=any
```

```
Phase: 15
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true
        hits=3598, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

---------------OMITTED OUTPUT -----------------

Result:
input-interface: Inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: Outside1(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

执行故障转移

在本示例中，故障切换是通过在IP SLA监控器配置中使用的Outside1的下一跳上关闭来执行的。

```
firepower# sh sla monitor configuration 10
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 10
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.200.1.1
Interface: Outside1
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

路由

默认路由现在使用Outside2的下一跳IP地址，可达性为Down。

```
firepower# sh route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.201.1.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [2/0] via 10.201.1.1, Outside2
C        10.10.10.0 255.255.255.0 is directly connected, Inside
L        10.10.10.5 255.255.255.255 is directly connected, Inside
C        10.200.1.0 255.255.255.0 is directly connected, Outside1
L        10.200.1.5 255.255.255.255 is directly connected, Outside1
C        10.201.1.0 255.255.255.0 is directly connected, Outside2
L        10.201.1.5 255.255.255.255 is directly connected, Outside2
```

跟踪

如show track 1输出所示，此时“Reachability is Down”。

```
firepower# sh track 1
Track 1
Response Time Reporter 10 reachability
Reachability is Down <----
37 changes, last change 00:17:02
Latest operation return code: Timeout
Tracked by:
STATIC-IP-ROUTING 0
```

NAT

```
firepower# packet-tracer input inside icmp 10.10.10.1 8 0 192.168.100.1 det
---------------OMITTED OUTPUT -----------------

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,Outside2) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.
Additional Information:
Static translate 10.10.10.1/0 to 10.10.10.1/0
 Forward Flow based lookup yields rule:
```

```
 in  id=0x2b3e0c67d470, priority=6, domain=nat, deny=false
        hits=44, user_data=0x2b3e0c3170e0, cs_id=0x0, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Inside(vrfid:0), output_ifc=Outside2(vrfid:0)

---------------OMITTED OUTPUT -----------------
Phase: 9
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x2b3e0c67bdb0, priority=70, domain=encrypt, deny=false
        hits=1, user_data=0x1d4cfb24, cs_id=0x2b3e0c273db0, reverse, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=any(vrfid:65535), output_ifc=Outside2

Phase: 10
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (Inside,Outside2) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x2b3e0c6d5bb0, priority=6, domain=nat-reverse, deny=false
        hits=1, user_data=0x2b3e0b81bc00, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Inside(vrfid:0), output_ifc=Outside2(vrfid:0)

Phase: 11
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x2b3e0c8a14f0, priority=70, domain=ipsec-tunnel-flow, deny=false
        hits=1, user_data=0x1d4d073c, cs_id=0x2b3e0c273db0, reverse, flags=0x0, protocol=0
        src ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Outside2(vrfid:0), output_ifc=any

Phase: 12
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true
        hits=3669, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

---------------OMITTED OUTPUT -----------------
```

```
Result:
input-interface: Inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: Outside2(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

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）。