使用FDM在FTD上配置双ISP

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 网络图

验证

简介

本文档介绍如何使用安全防火墙系列的防火墙设备管理器(FDM)配置双Internet服务提供商(ISP)故障切换。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本路由
- Firewall Device Manager控制面板知识
- 至少有两个Internet服务提供商连接到安全防火墙。

使用的组件

本文档中的信息基于以下软件和硬件版本：

·运行7.7.X版本或更高版本的Cisco Secure Firewall。

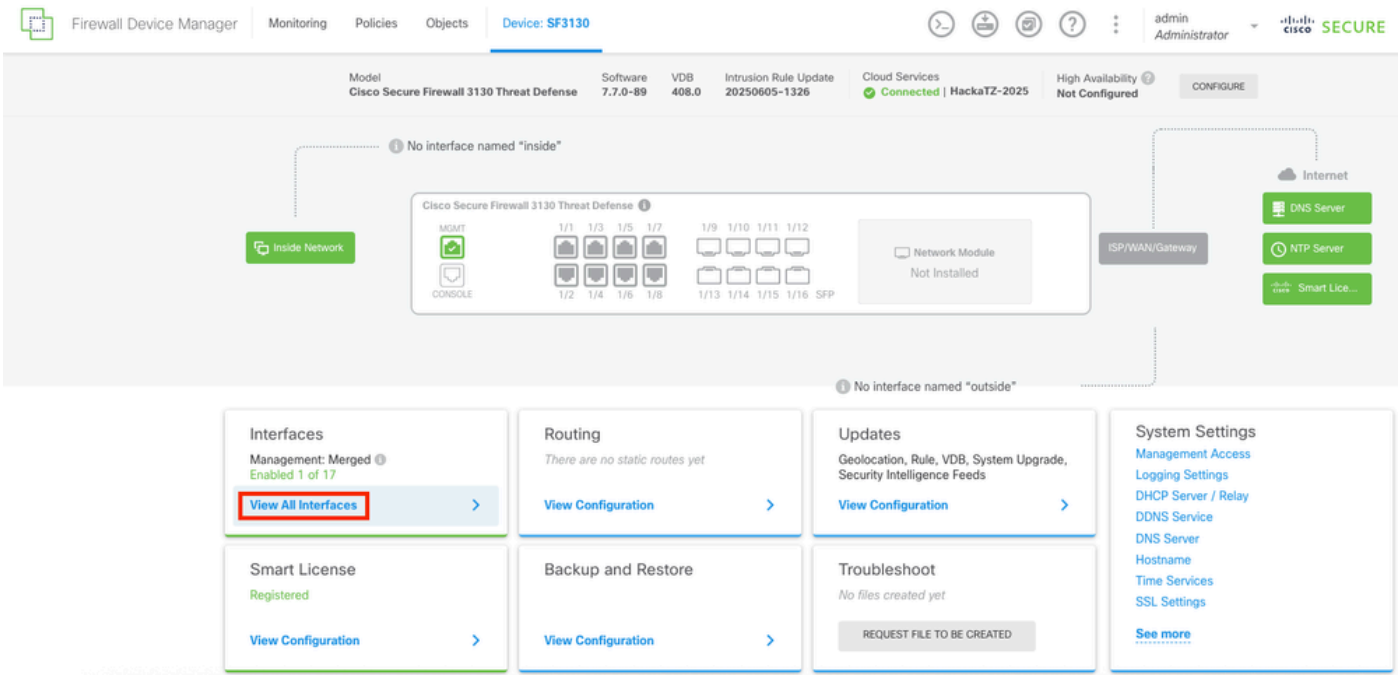
· Secure Firewall 3130（7.7.0版本）。

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

步骤1:

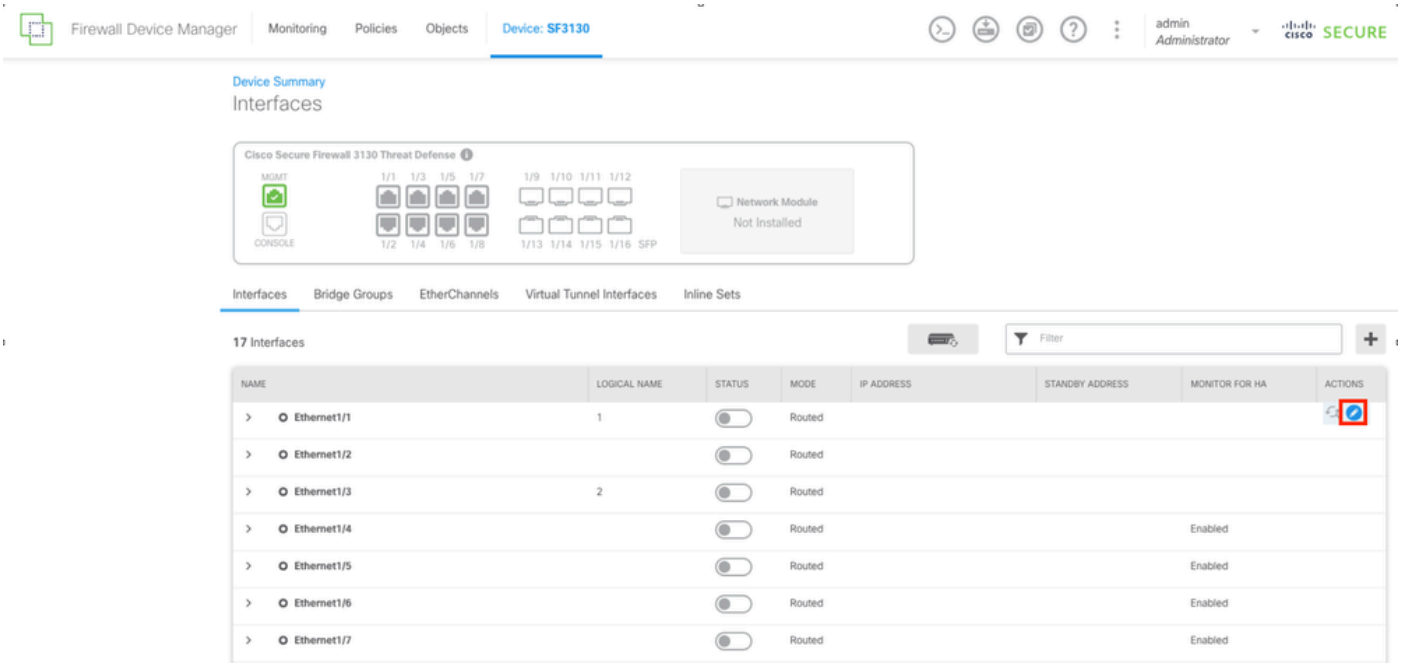
在安全防火墙上登录FDM，然后选择View All Interfaces按钮导航到interfaces部分。



FDM主仪表板

Step 2.

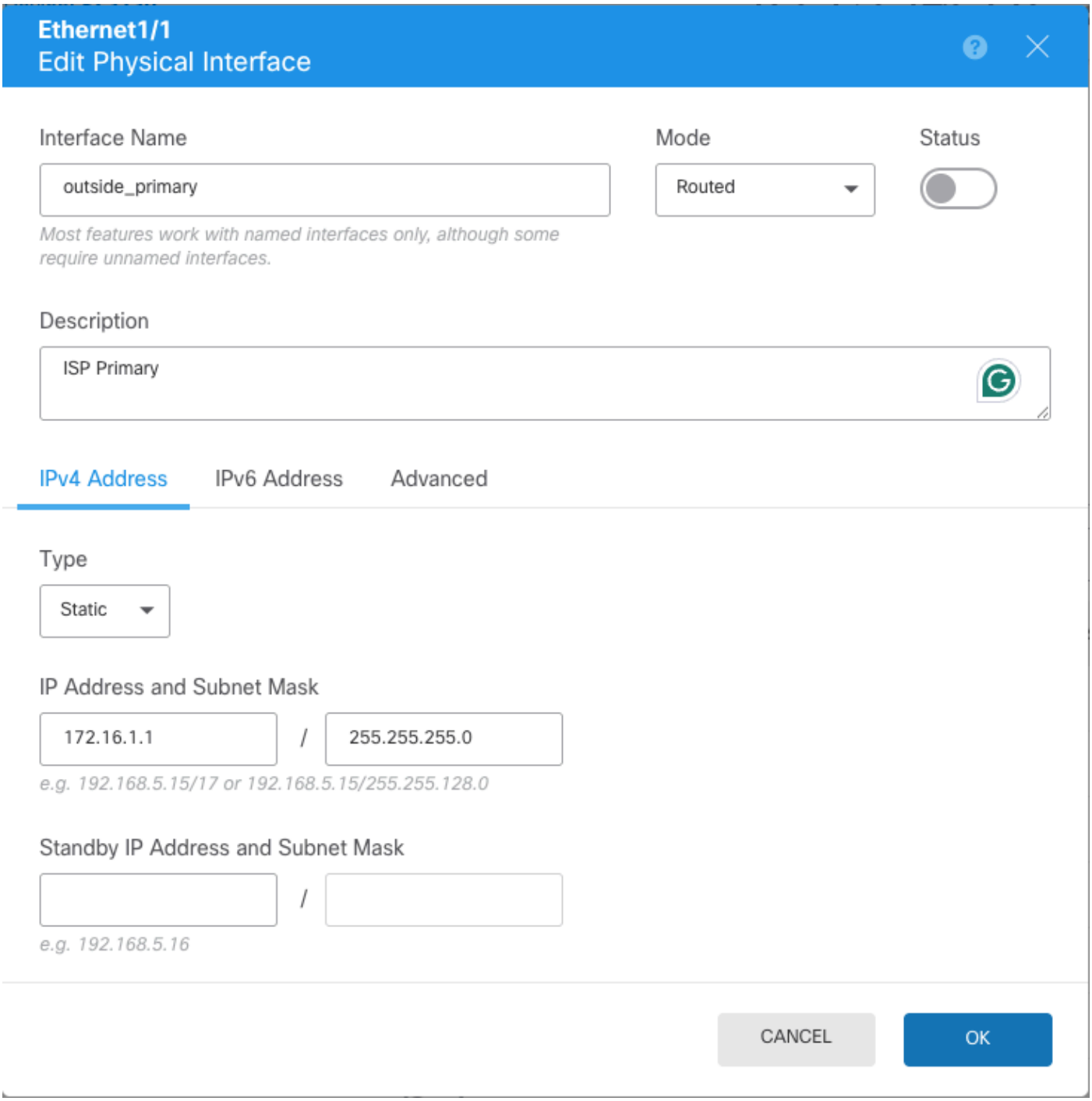
要配置主ISP连接的接口，首先选择所需的接口。选择相应的interface按钮以继续。在本示例中，使用的接口是Ethernet1/1。



Interfaces选项卡

第 3 步：

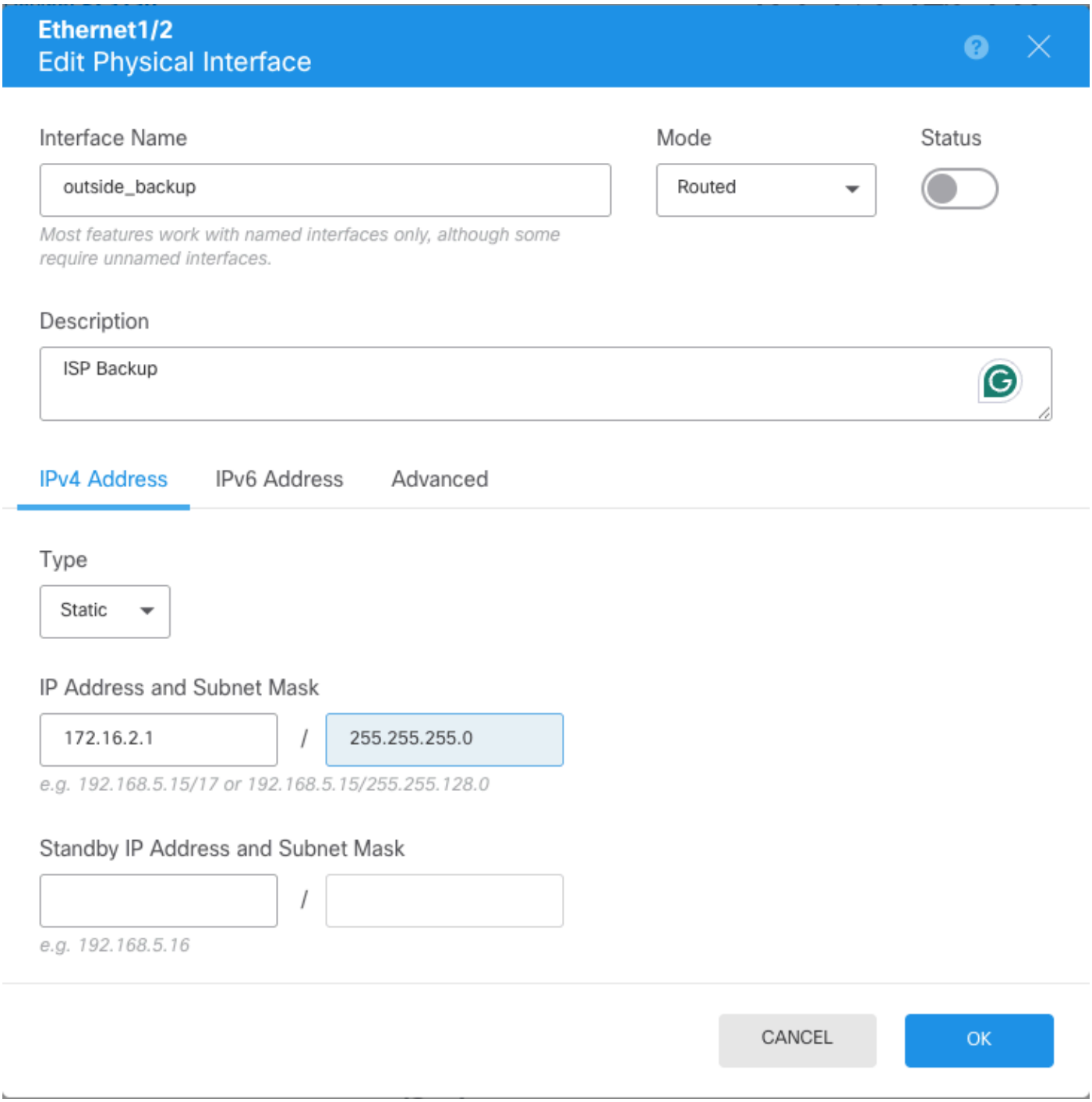
使用适合您的主ISP连接的正确参数配置接口。在本示例中，接口为outside_primary。



主ISP接口的配置

第 4 步：

对辅助ISP接口重复相同的过程。在本示例中，使用接口Ethernet1/2。

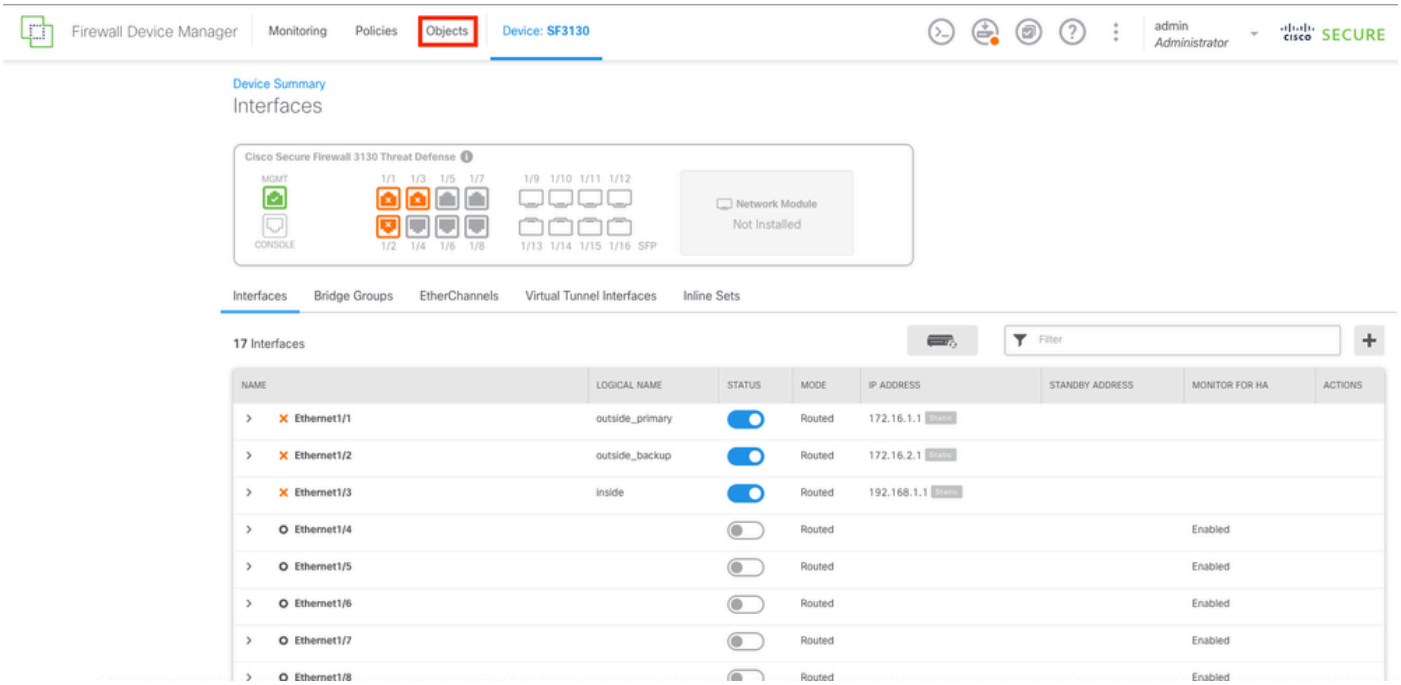


配置辅助ISP接口

第 5 步：

为ISP配置两个接口后，下一步是为主接口设置SLA监控器。

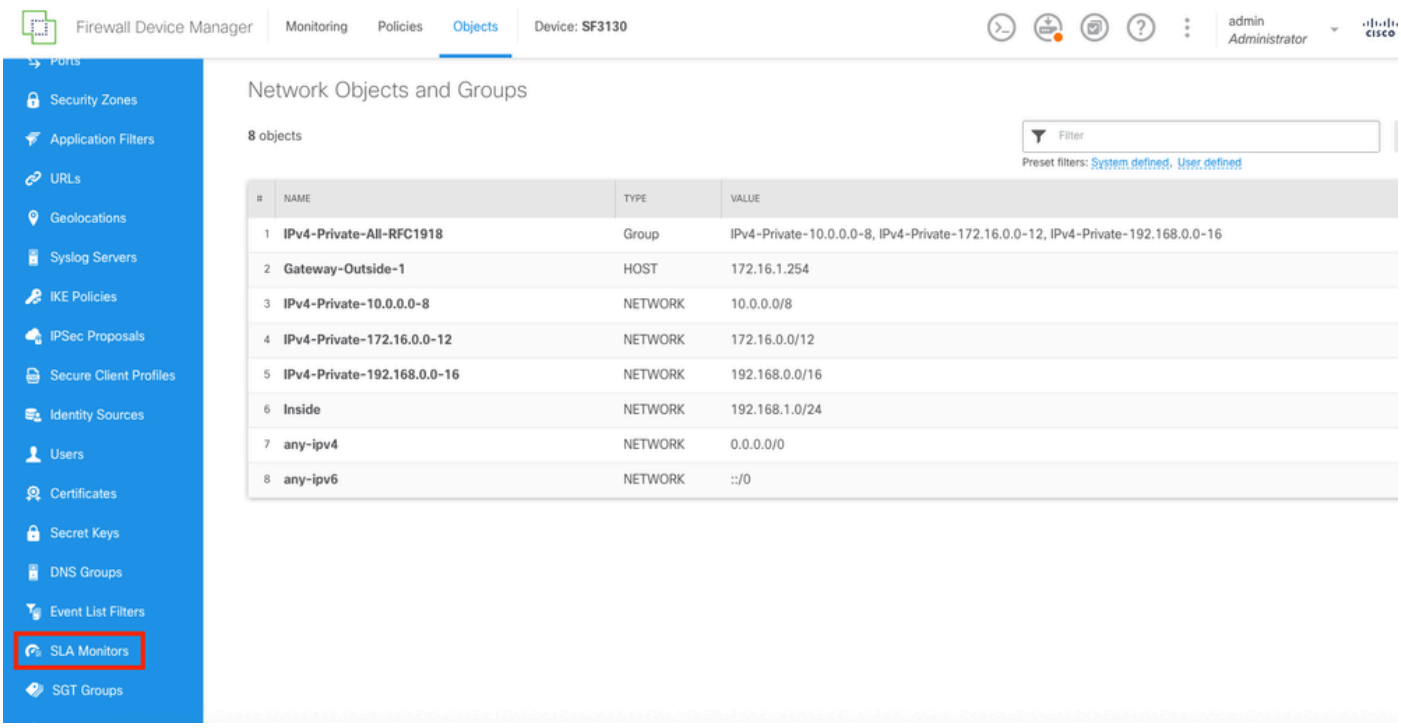
通过选择位于菜单顶部的对象按钮导航到对象部分。



配置的接口

第六步：

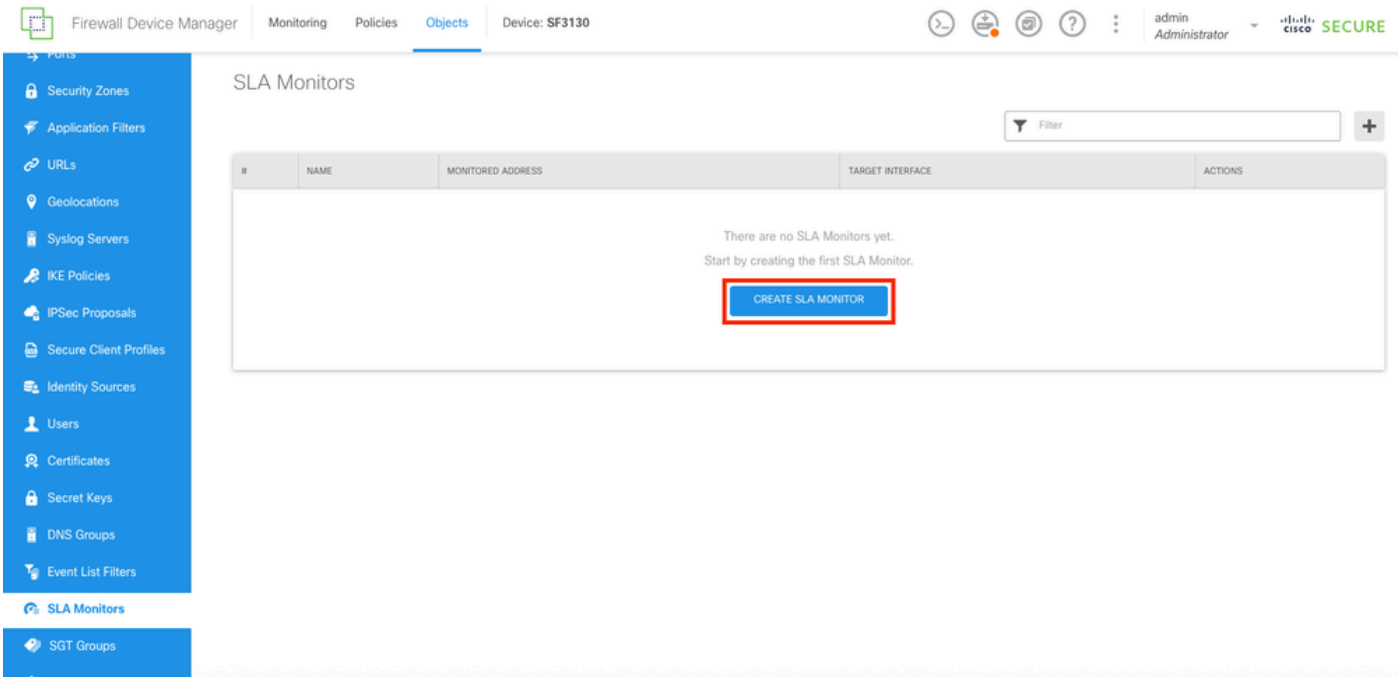
在左侧列中选择SLA Monitors按钮。



Objects屏幕

第 7 步：

通过选择Create SLA Monitor按钮创建新的SLA监控器。



SLA Monitor部分

步骤 8

配置主ISP连接的参数。

Add SLA Monitor Object

Name

Outside_Primary_ISP

Description

Monitor for ISP Primary

Monitor Address

Gateway-Outside-1

Target Interface

outside_primary (Ethernet1/1)

IP ICMP ECHO OPTIONS

Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold

5000 milliseconds

0 - 2147483647

Timeout

5000 milliseconds

0 - 604800000

Frequency

60000 milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

28 bytes

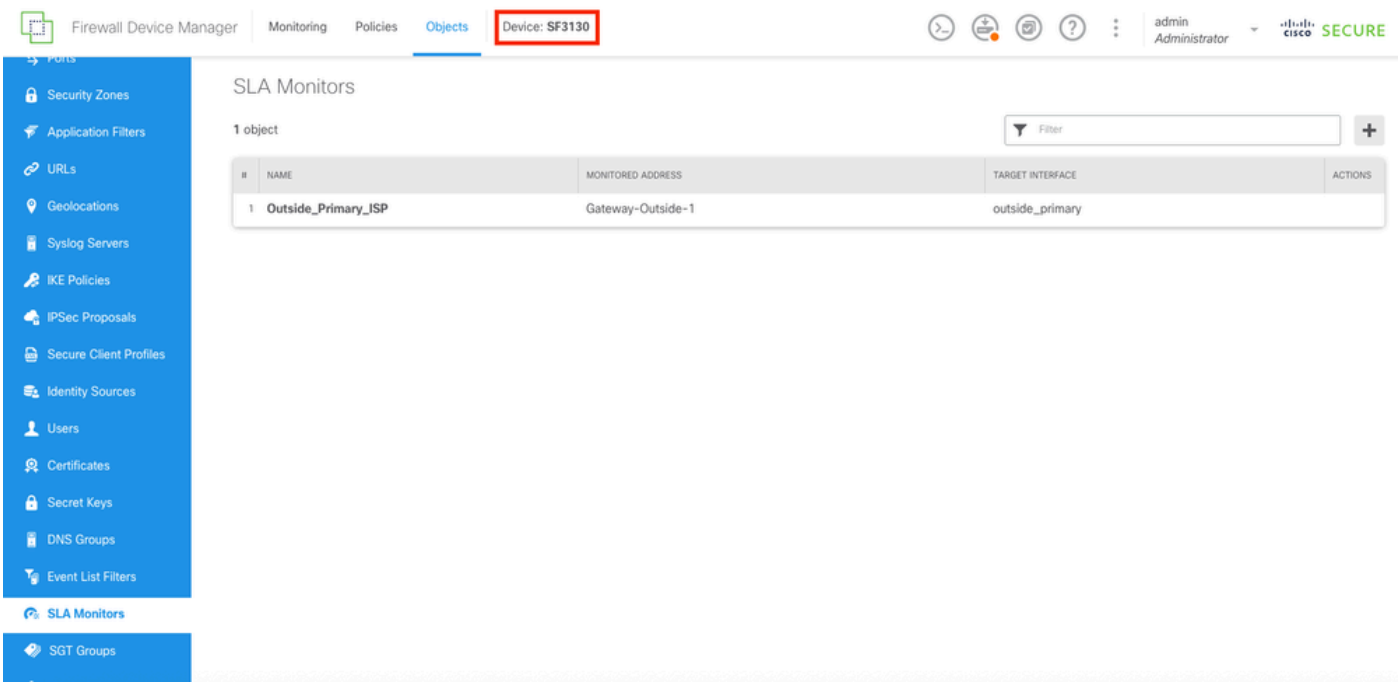
0 - 16384

CANCEL OK

SLA对象创建

步骤 9

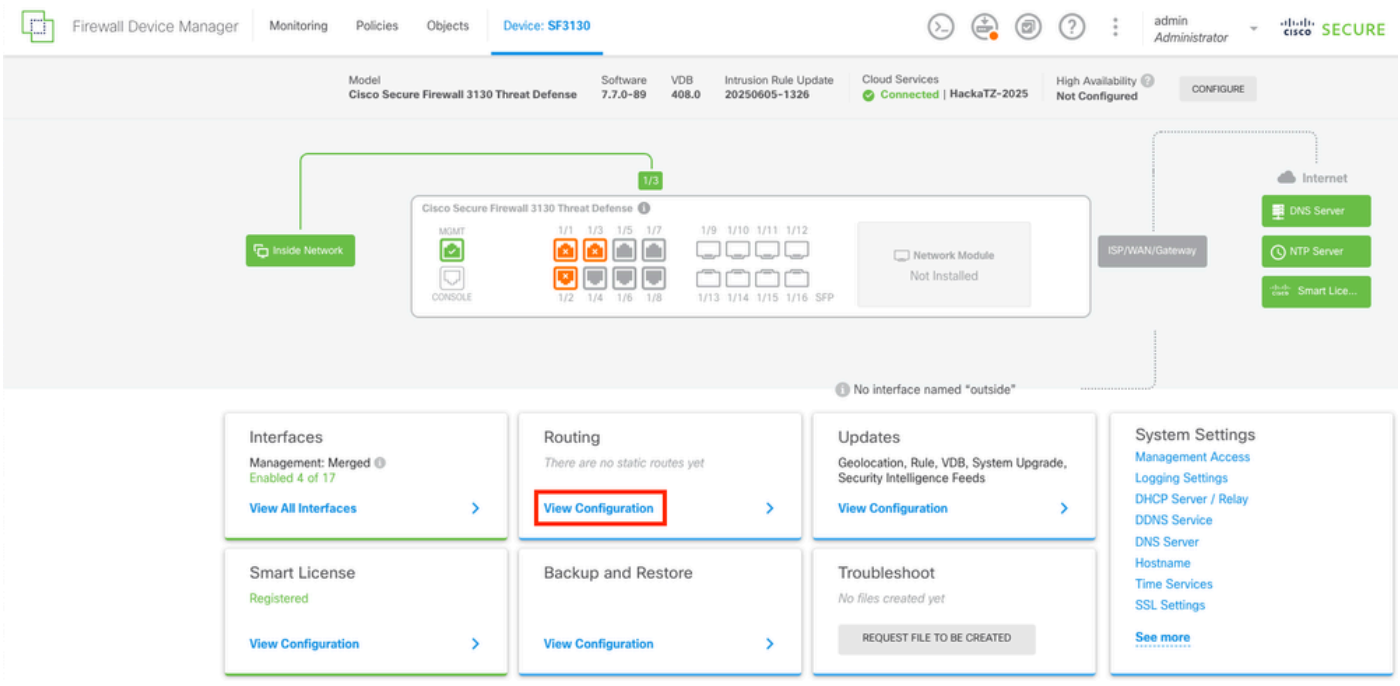
创建对象后，必须创建接口的静态路由。选择Device(设备)按钮导航到主控制面板。



已创建SLA监控

步骤 10

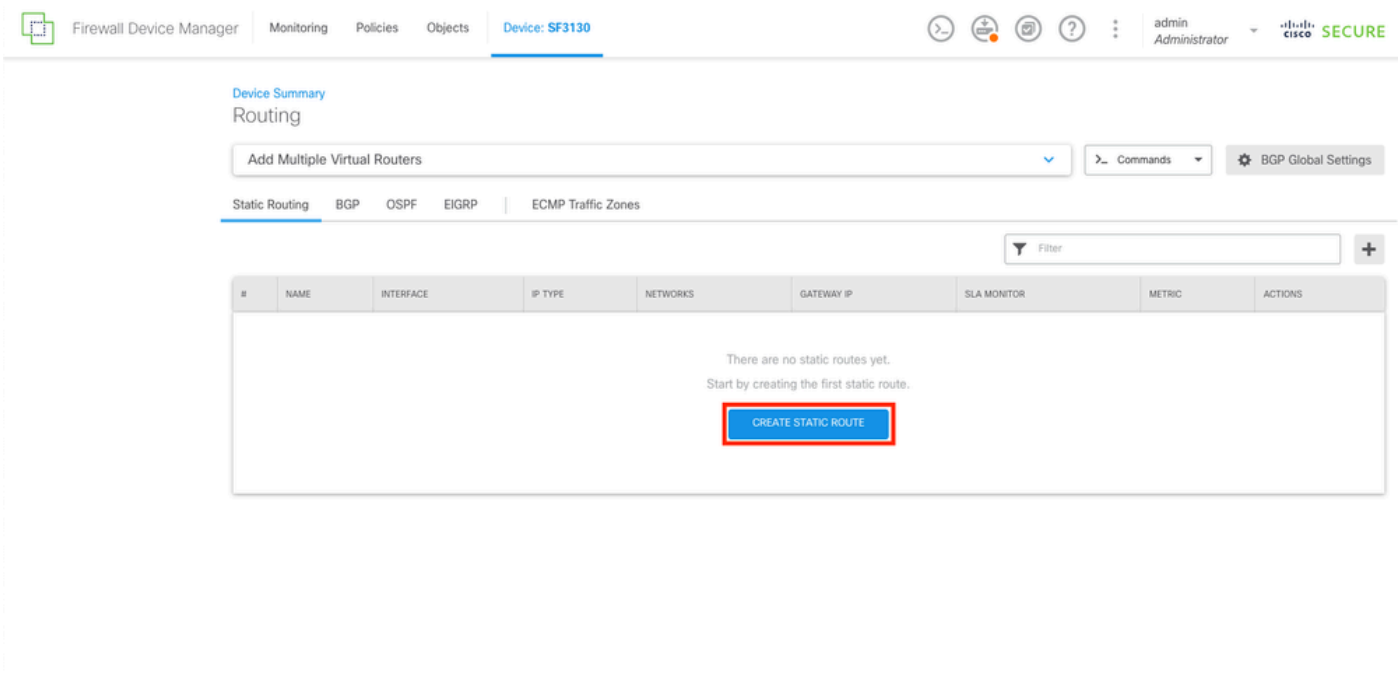
选择Routing Panel中的View Configuration，导航到Routing Section。



主控制面板

步骤 11

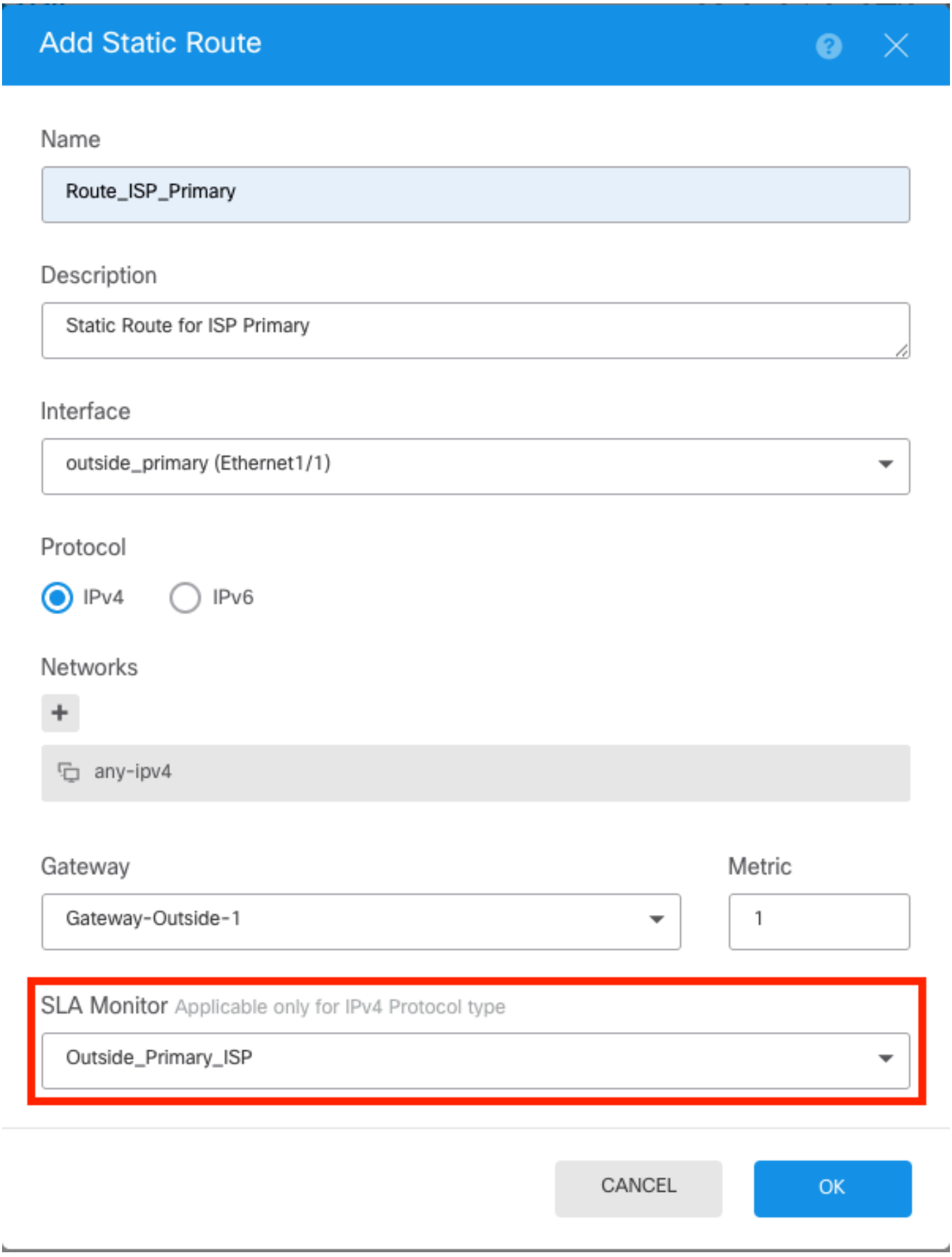
在Static Routing（静态路由）选项卡上，为两个ISP创建2条默认静态路由。要创建新的静态路由，请选择CREATE STATIC ROUTE按钮。



Static Routing部分

步骤 12

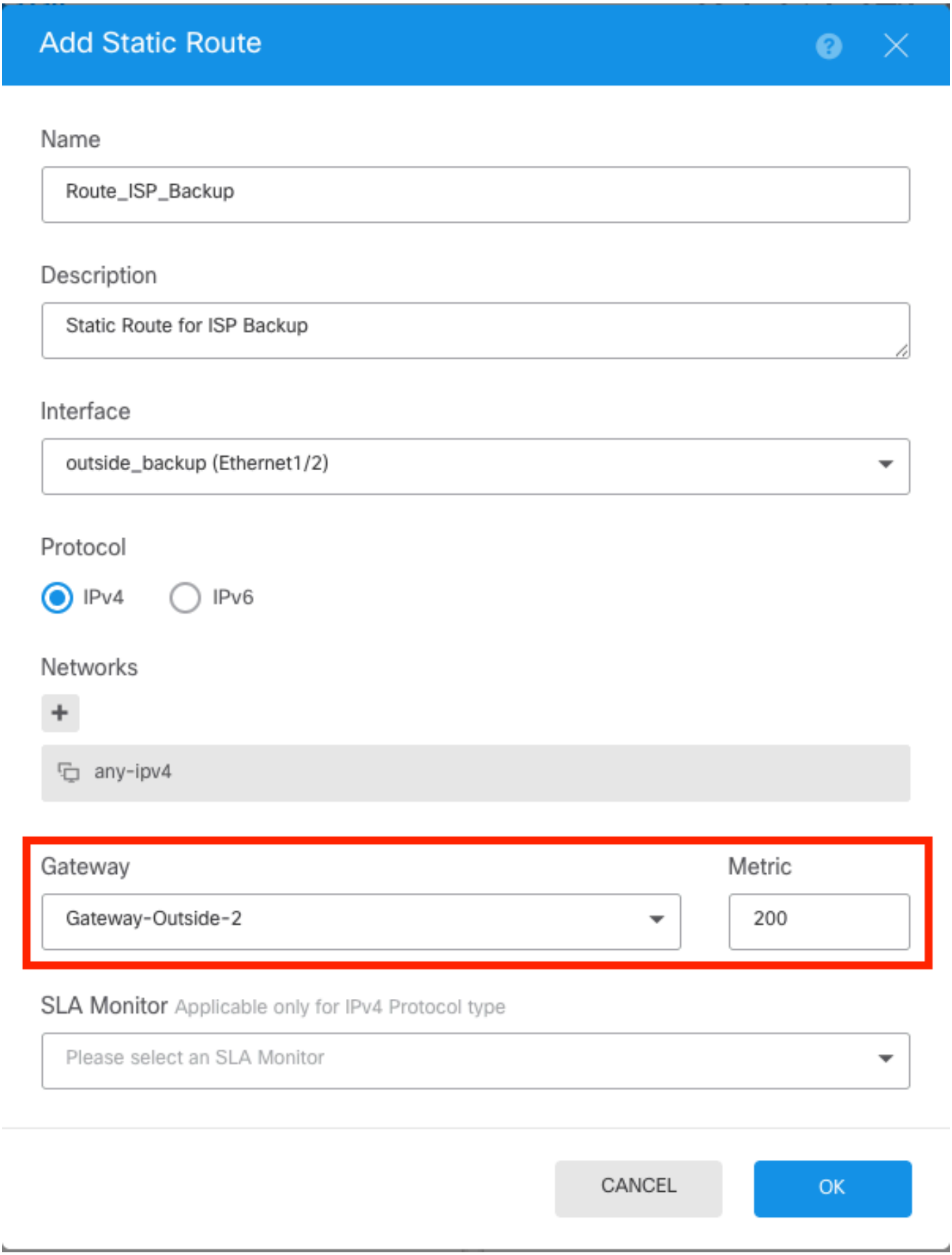
首先，为主ISP创建静态路由。最后，添加在上一步中创建的SLA监控器对象。



主ISP的静态路由

步骤 13

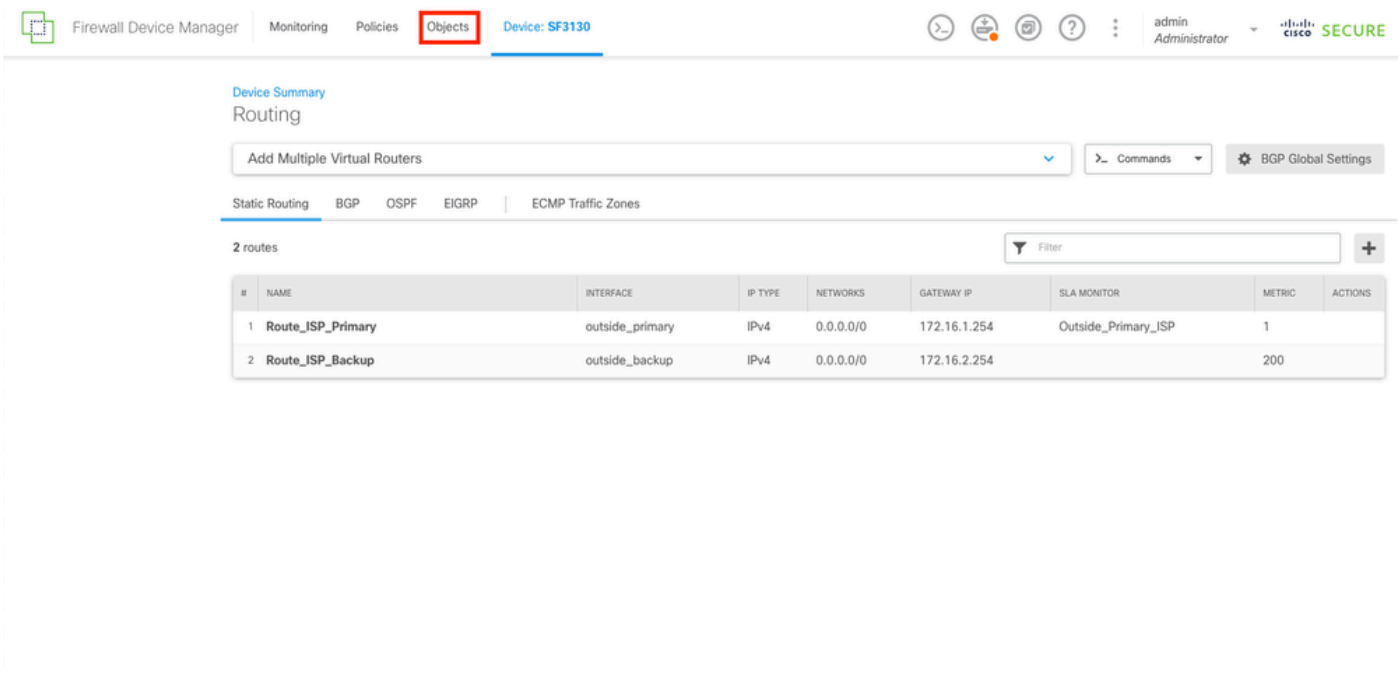
重复最后一步，为ISP辅助创建一条默认路由，该路由具有适当的网关和不同的度量。在本例中，它增加到200。



辅助ISP的静态路由

步骤 14

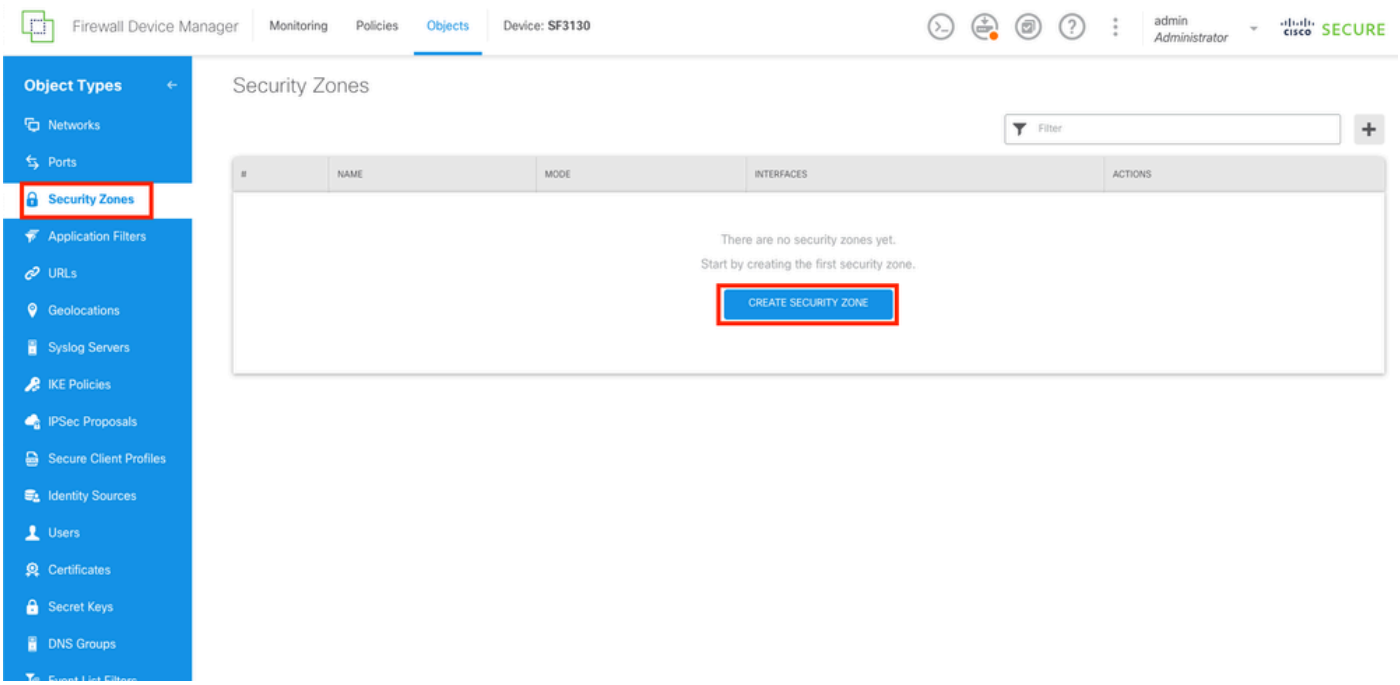
创建两个静态路由后，必须创建安全区域。通过选择顶部的对象按钮导航到对象部分。



创建的静态路由

步骤 15

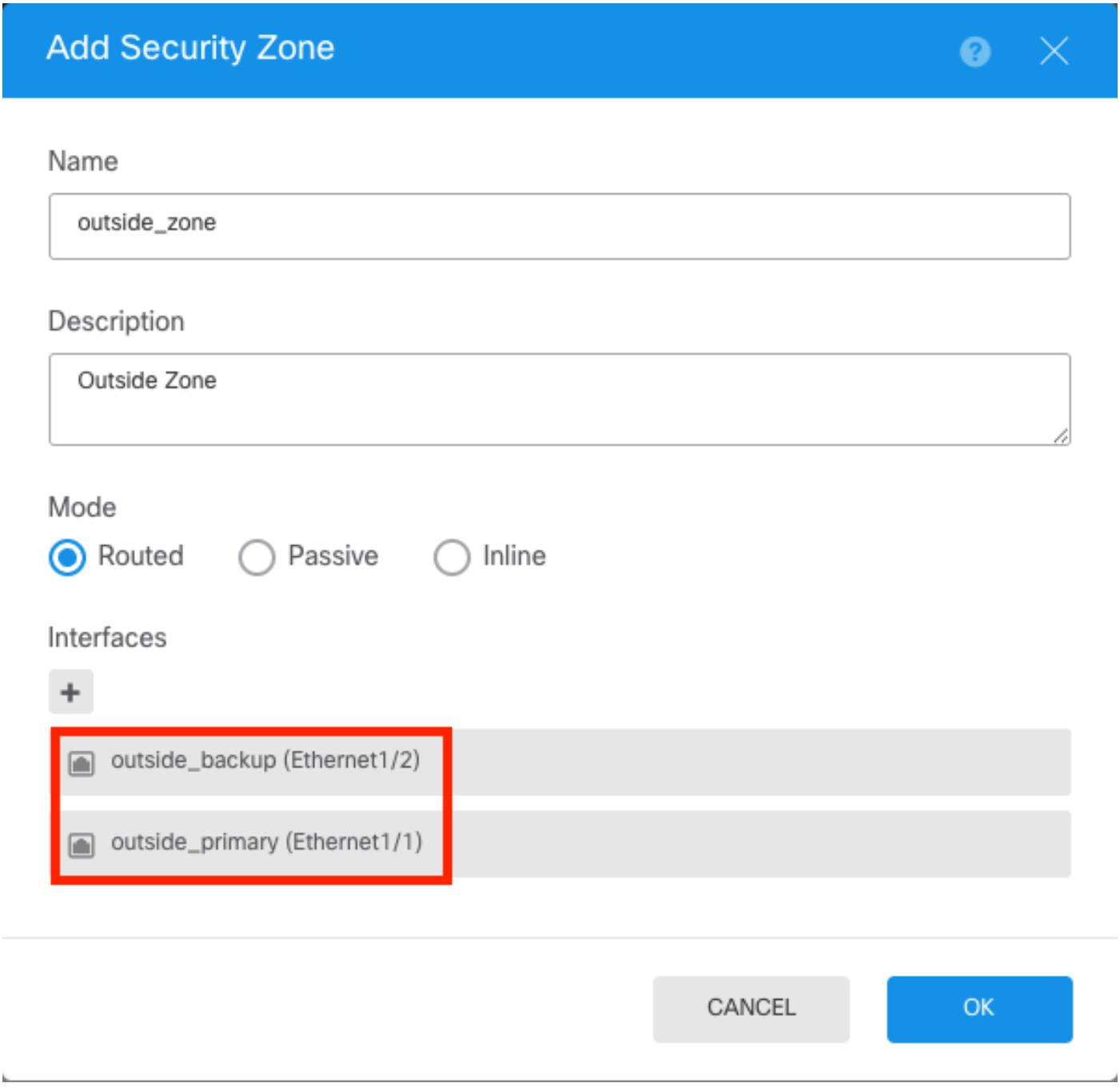
在Security Zones按钮的左列中选择Security Zones按钮，导航到Security Zones部分，然后通过选择CREATE SECURITY ZONE按钮创建一个新区域。



Security Zones部分

步骤 16

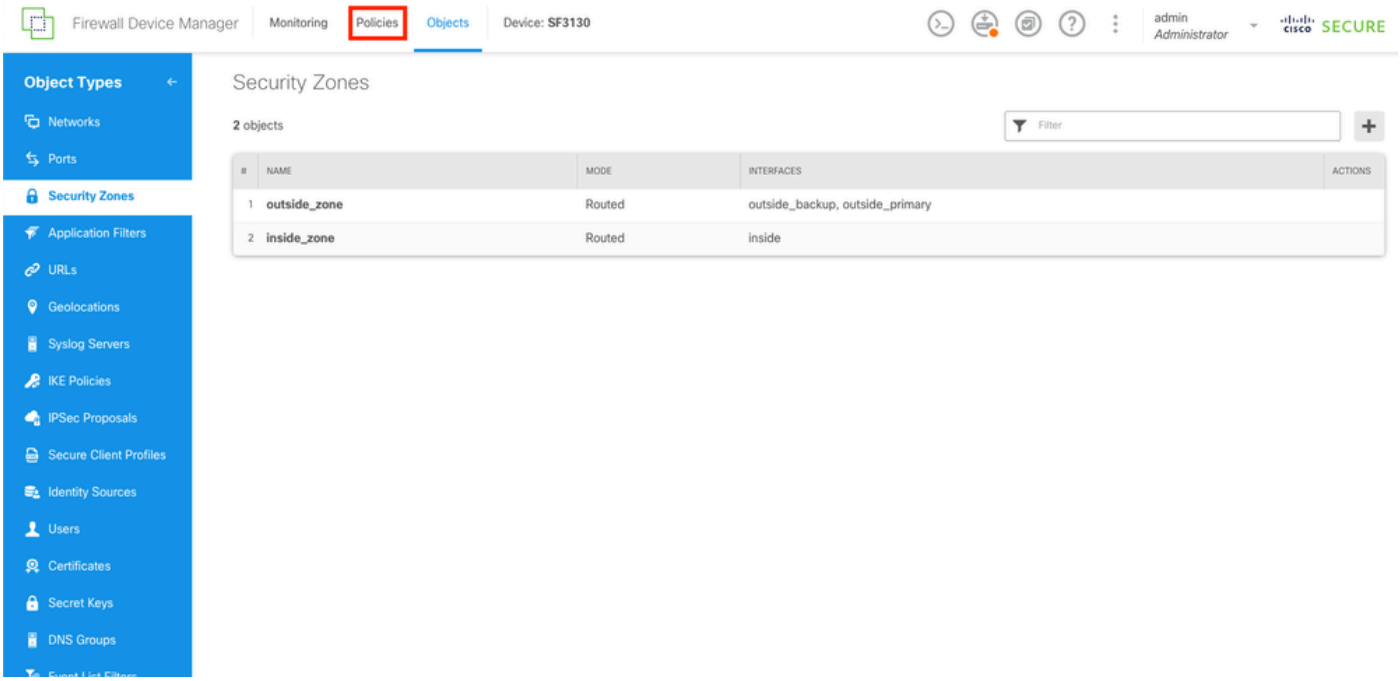
为ISP连接创建Outside Security Zone和两个外部接口。



外部安全区域

步骤 17

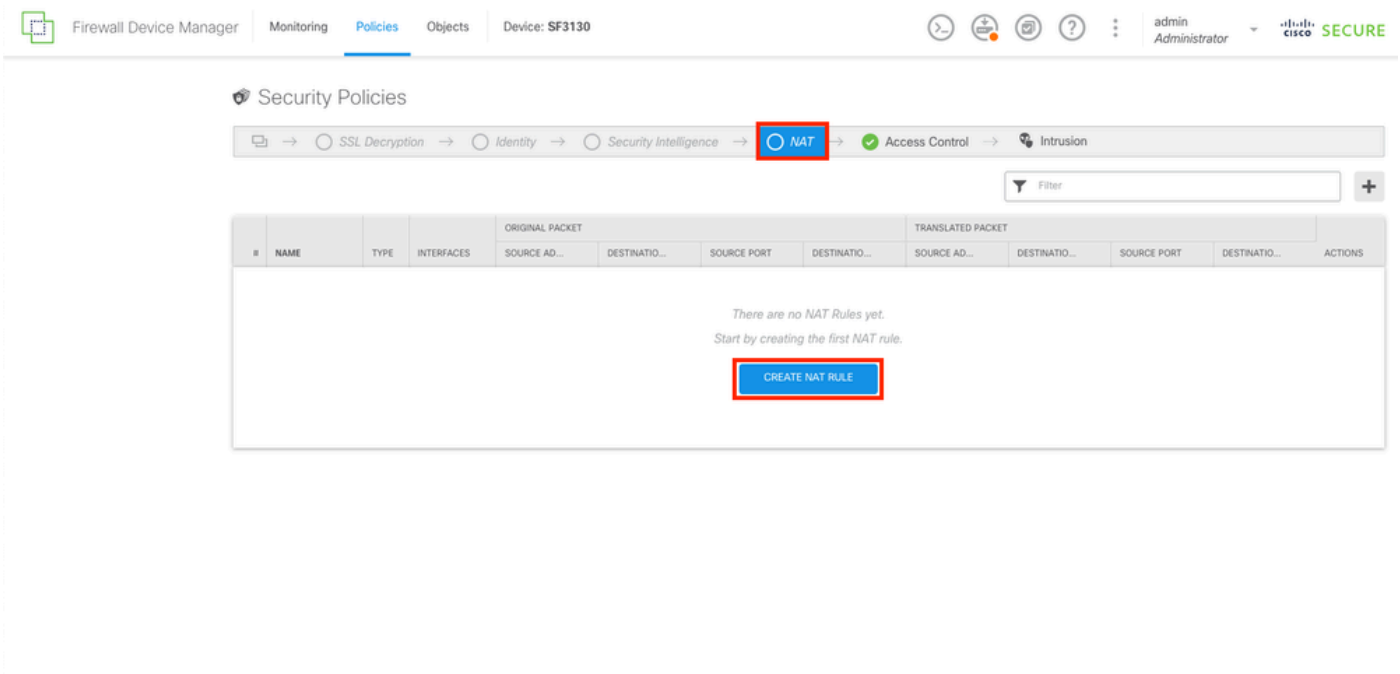
创建安全区域后，必须创建NAT。选择顶部的Policies按钮导航到Policies部分。



已创建安全区域

第 18 步：

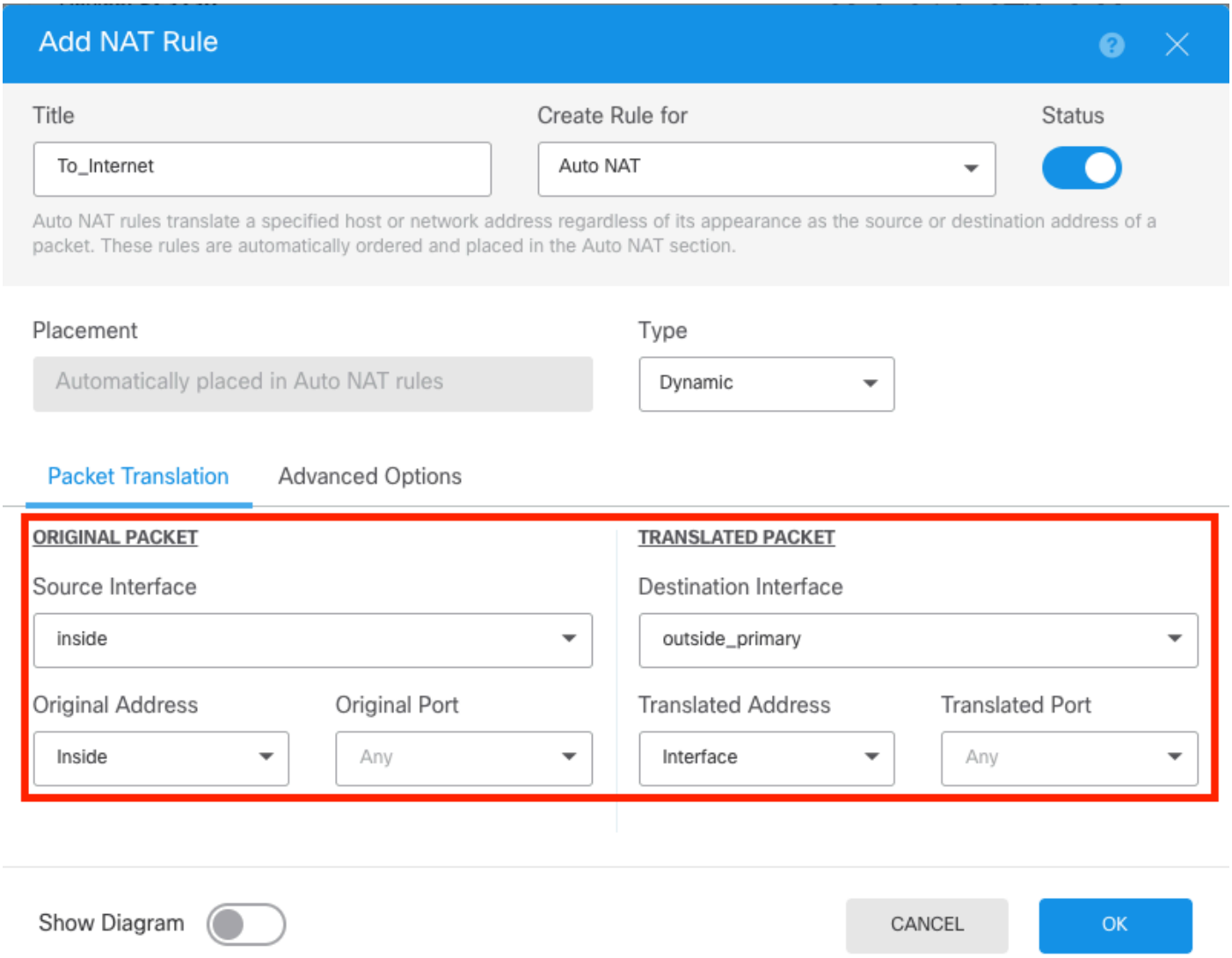
选择NAT按钮导航到NAT部分，然后选择CREATE NAT RULE按钮创建新规则。



NAT部分

第 19 步：

对于ISP故障切换，配置必须有2条通过外部接口的路由。首先，用于主外部接口与主ISP的连接。

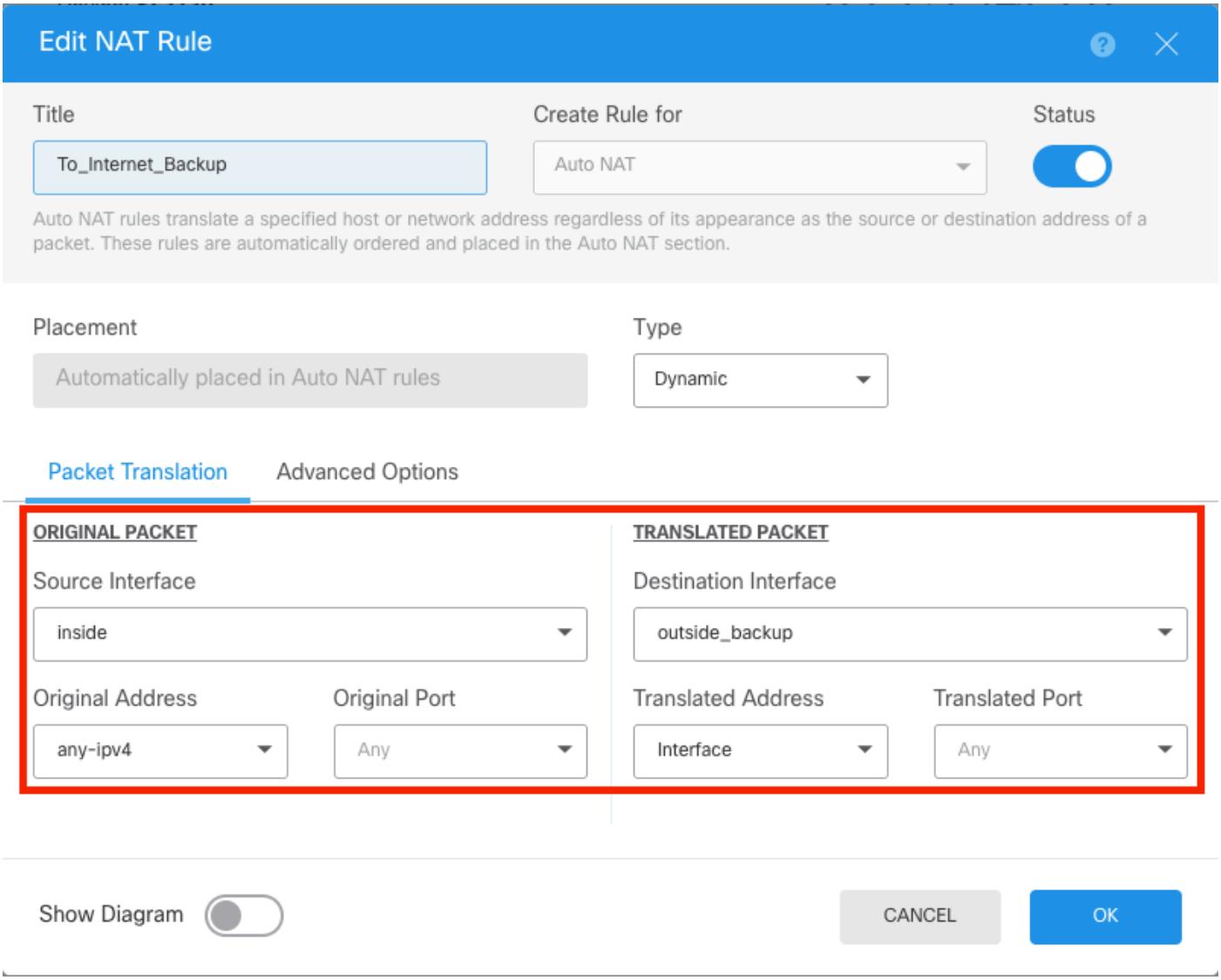


主ISP的NAT

第 20 步：

现在，为辅助ISP连接配置第二个NAT。

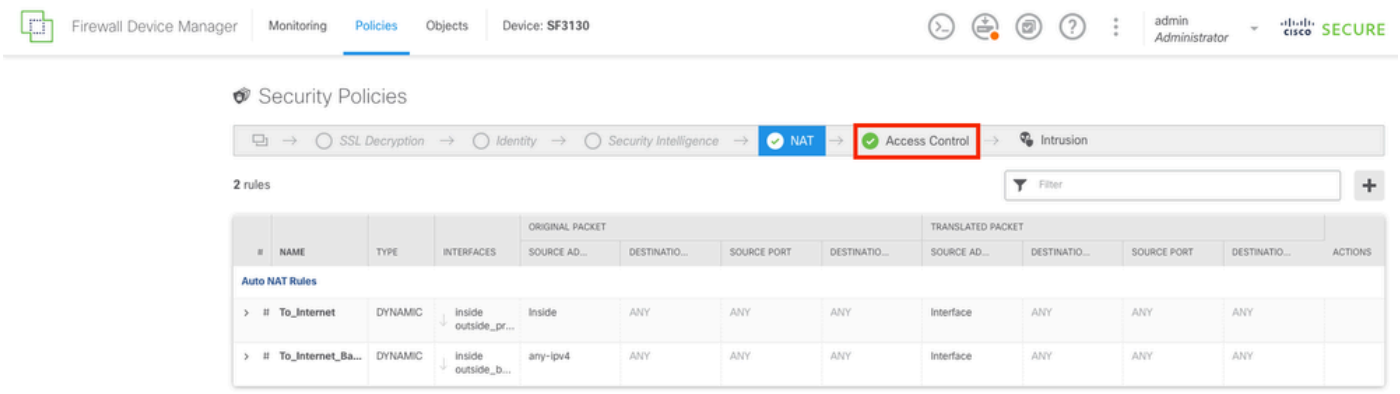
注意：对于原始地址，不能使用同一网络。在本例中，对于辅助ISP，Original Address是对象any-ipv4。



辅助ISP的NAT

第 21 步：

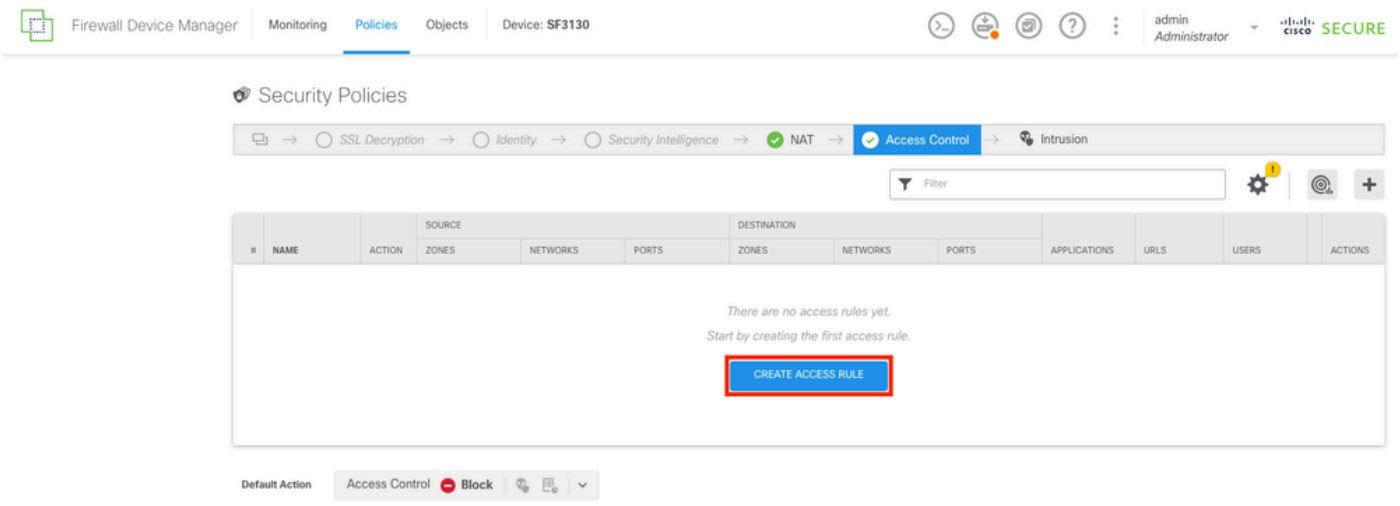
创建两个NAT规则后，必须建立访问控制规则以允许出站流量。选择Access Control按钮。



已创建NAT规则

第 22 步：

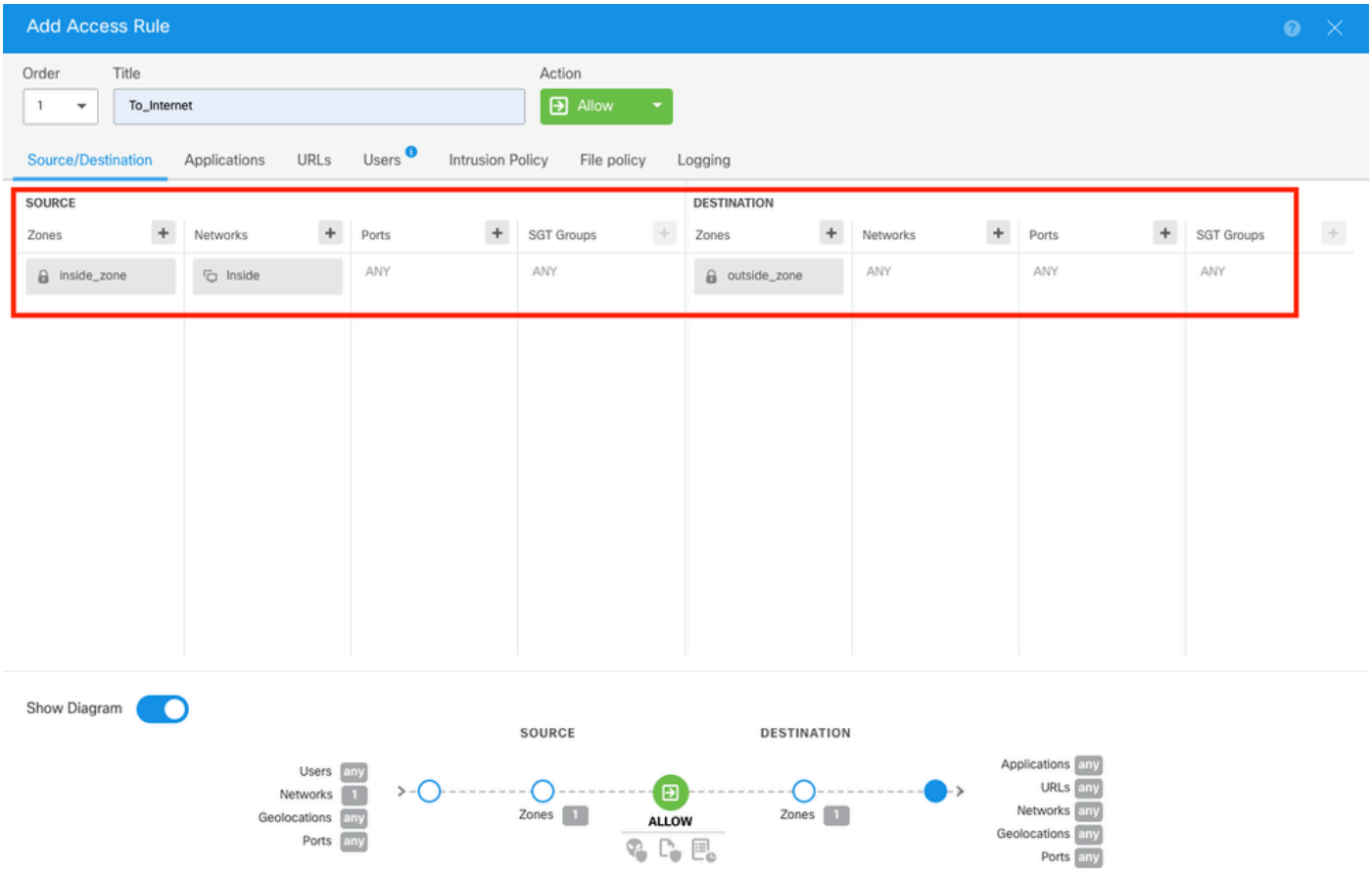
要创建访问控制规则，请选择CREATE ACCESS RULE按钮。



访问控制部分

第 23 步：

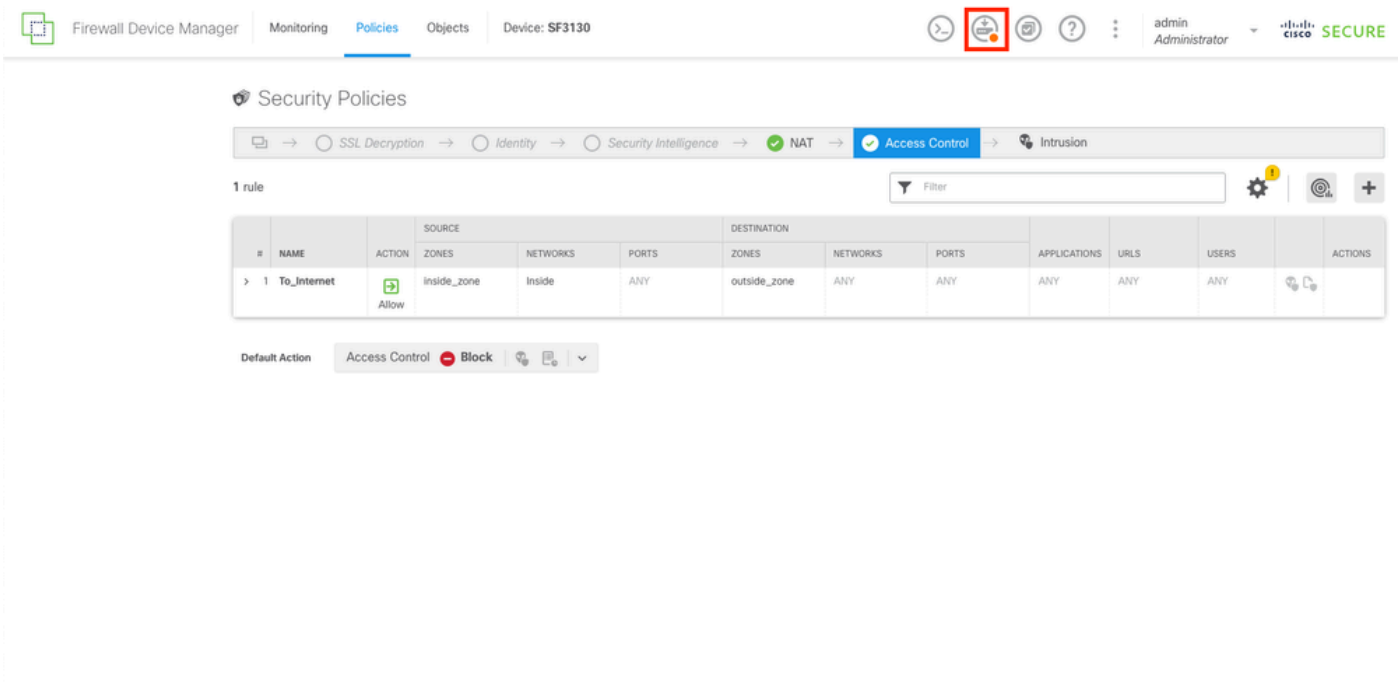
选择区域和网络。



访问控制规则

第 24 步：

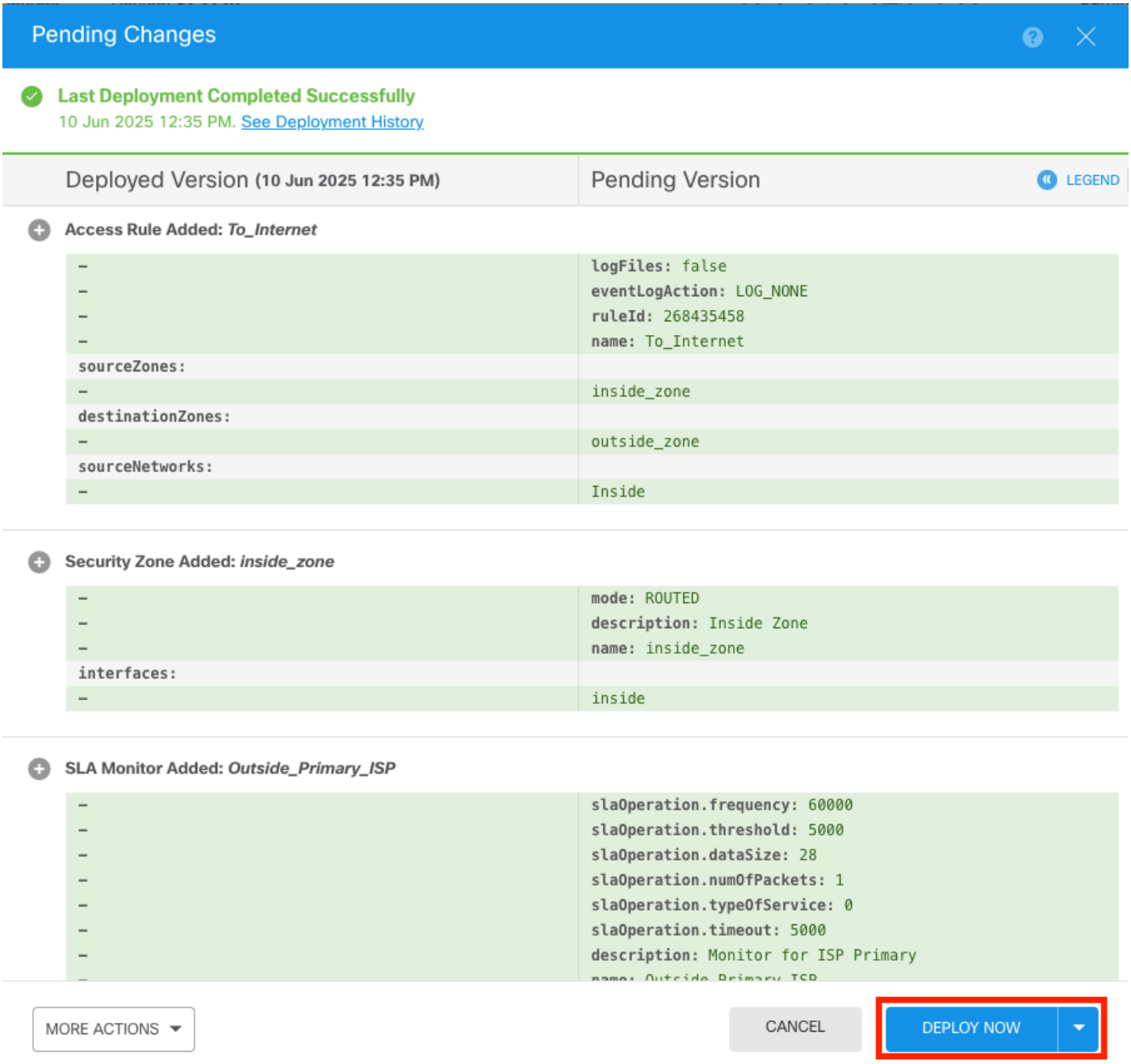
创建访问控制规则后，通过选择顶部的Deploy按钮继续部署所有更改。



已创建访问控制规则

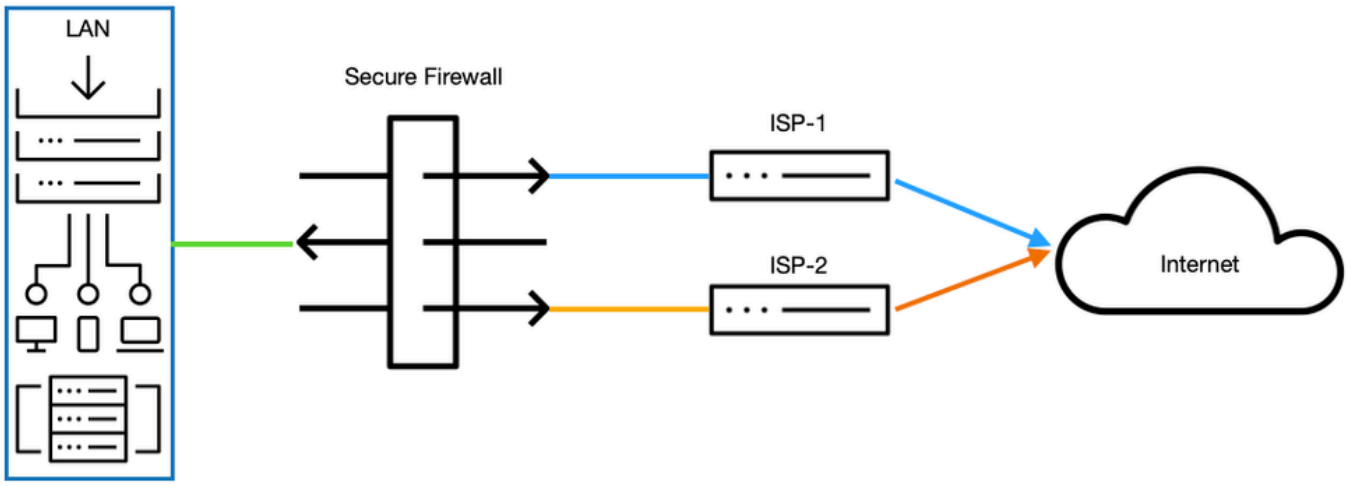
第 25 步：

验证更改，然后选择Deploy Now按钮。



部署验证

网络图



网络图

验证

<#root>

>

system support diagnostic-cli

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

SF3130#

show ip

System IP Addresses:
Interface Name IP address Subnet mask Method
Ethernet1/1 outside_primary 172.16.1.1 255.255.255.0 manual

------------> THE PRIMARY INTERFACE OF THE ISP IS SET

Ethernet1/2 outside_backup 172.16.2.1 255.255.255.0 manual

------------> THE SECONDARY INTERFACE OF THE ISP IS SET

Ethernet1/3 inside 192.168.1.1 255.255.255.0 manual

SF3130#

show interface ip brief

Interface IP-Address OK? Method Status Protocol
Ethernet1/1 172.16.1.1 YES manual up up

------------------> THE INTERFACE IS UP AND RUNNING

```
Ethernet1/2 172.16.2.1  YES manual   up      up
```

------------------> THE INTERFACE IS UP AND RUNNING

```
Ethernet1/3 192.168.1.1 YES manual   up      up

SF3130#
```

show route

```
Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 172.16.1.254, outside_primary
```

----> THE DEFAULT ROUTE IS CONNECTED THROUGH THE PRIMARY ISP

```
C  172.16.1.0  255.255.255.0   is directly connected, outside_primary
L  172.16.1.1  255.255.255.255 is directly connected, outside_primary
C  172.16.2.0  255.255.255.0   is directly connected, outside_backup
L  172.16.2.1  255.255.255.255 is directly connected, outside_backup
C  192.168.1.0 255.255.255.0   is directly connected, inside
L  192.168.1.1 255.255.255.255 is directly connected, inside

SF3130#
```

show run route

```
route outside_primary 0.0.0.0 0.0.0.0 172.16.1.254 1 track 1
route outside_backup  0.0.0.0 0.0.0.0 172.16.2.254 200

SF3130#
```

show sla monitor configuration

---> CHECKING THE SLA MONITOR CONFIGURATION

```
SA Agent, Infrastructure Engine-II
Entry number: 539523651
Owner:
Tag:
Type of operation to perform: echo
Target address: 172.16.1.254
Interface: outside_primary
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 3000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
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:

SF3130#
```

show sla monitor operational-state

```
Entry number: 739848060
Modification time: 01:24:11.029 UTC Thu Jun 12 2025
Number of Octets Used by this Entry: 1840
Number of operations attempted: 0
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Pending
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
```

---------------------------> THE ISP PRIMARY IS IN A HEALTHY STATE

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds) : Unknown
Latest operation return code: Unknown
Latest operation start time: Unknown

AFTERARGBSETHBNDGFSHNDFGSDBFB

SF3130#
```

show interface ip brief

```
Interface   IP-Address  OK? Method Status Protocol
Ethernet1/1 172.16.1.1  YES manual  down   down
```

------------------> THE PRIMARY ISP IS DOWN

```
Ethernet1/2 172.16.2.1  YES manual   up     up
Ethernet1/3 192.168.1.1 YES manual   up     up

SF3130#
```

show route

```
Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [200/0] via 172.16.2.254, outside_backup
```

---------> AFTER THE ISP PRIMARY FAILS, INSTANTLY THE ISP BACKUP IS FAILOVER AND IS INSTALL IN THE ROUTI

```
C  172.16.2.0 255.255.255.0    is directly connected, outside_backup
L  172.16.2.1 255.255.255.255  is directly connected, outside_backup
C  192.168.1.0 255.255.255.0   is directly connected, inside
L  192.168.1.1 255.255.255.255 is directly connected, inside

SF3130#
```

show sla monitor operational-state

```
Entry number: 739848060
Modification time: 01:24:11.140 UTC Thu Jun 12 2025
Number of Octets Used by this Entry: 1840
Number of operations attempted: 0
Number of operations skipped: 0
Current seconds left in Life: Forever
```

```
Operational state of entry: Pending
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
```

----------> AFTER THE DOWNTIME OF THE PRIMARY ISP THE TIMEOUT IS FLAGGED

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds) : Unknown
Latest operation return code: Unknown
Latest operation start time: Unknown

SF3130#
```

show route

```
Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 172.16.1.254, outside_primary
```

----------> AFTER A FEW SECONDS ONCE THE PRIMARY INTERFACE IS BACK THE DEFAULT ROUTE INSTALLS AGAIN IN

```
C 172.16.1.0 255.255.255.0    is directly connected, outside_primary
L 172.16.1.1 255.255.255.255  is directly connected, outside_primary
C 172.16.2.0 255.255.255.0    is directly connected, outside_backup
L 172.16.2.1 255.255.255.255  is directly connected, outside_backup
C 192.168.1.0 255.255.255.0   is directly connected, inside
L 192.168.1.1 255.255.255.255 is directly connected, inside
```

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）。

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）。