Configurar ISP Duplo no FTD Usando o FDM

Contents

Introdução

Este documento descreve como configurar o failover do Provedor de Serviços de Internet Duplo (ISP) usando o Gerenciador de Dispositivos de Firewall (FDM) para o Secure Firewall Series.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Roteamento básico
- Conhecimento do painel do Gerenciador de dispositivos de firewall
- Pelo menos dois provedores de serviço de Internet conectados ao firewall seguro.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

· Cisco Secure Firewall executando a versão 7.7.X ou versões superiores.

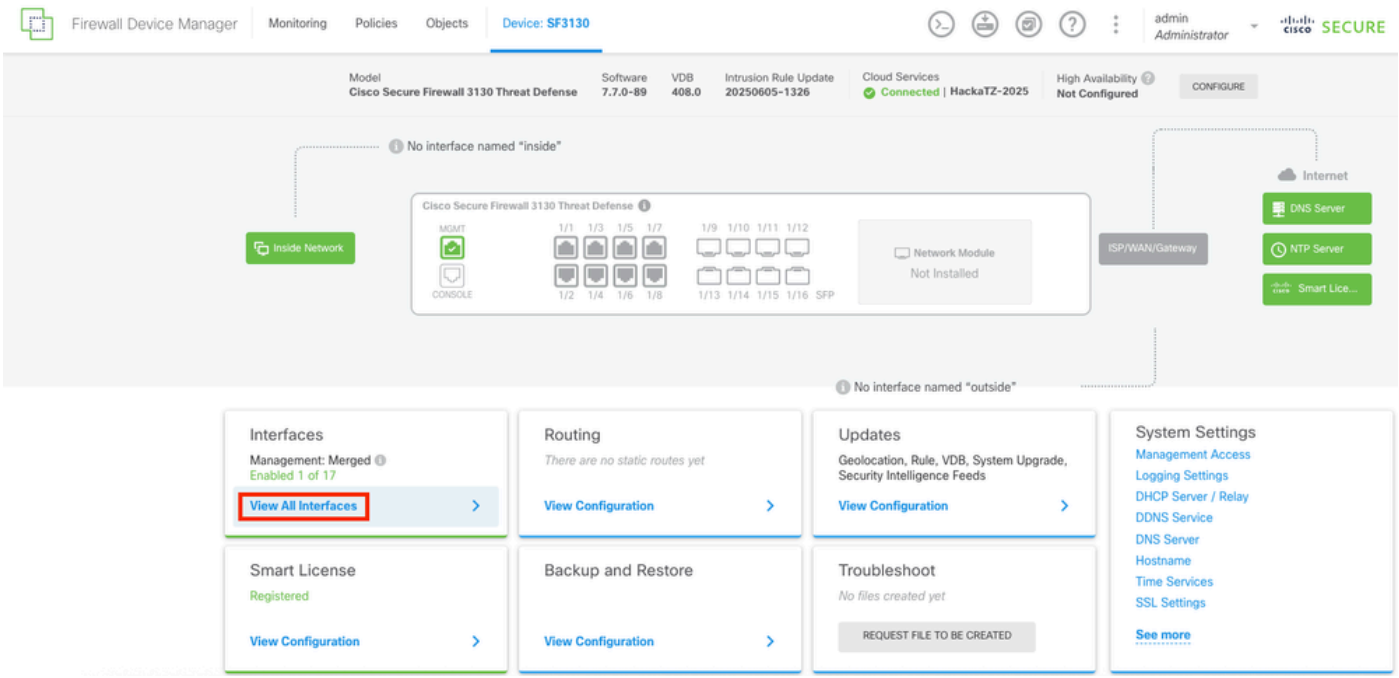
· Secure Firewall 3130 com versão 7.7.0.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Etapa 1.

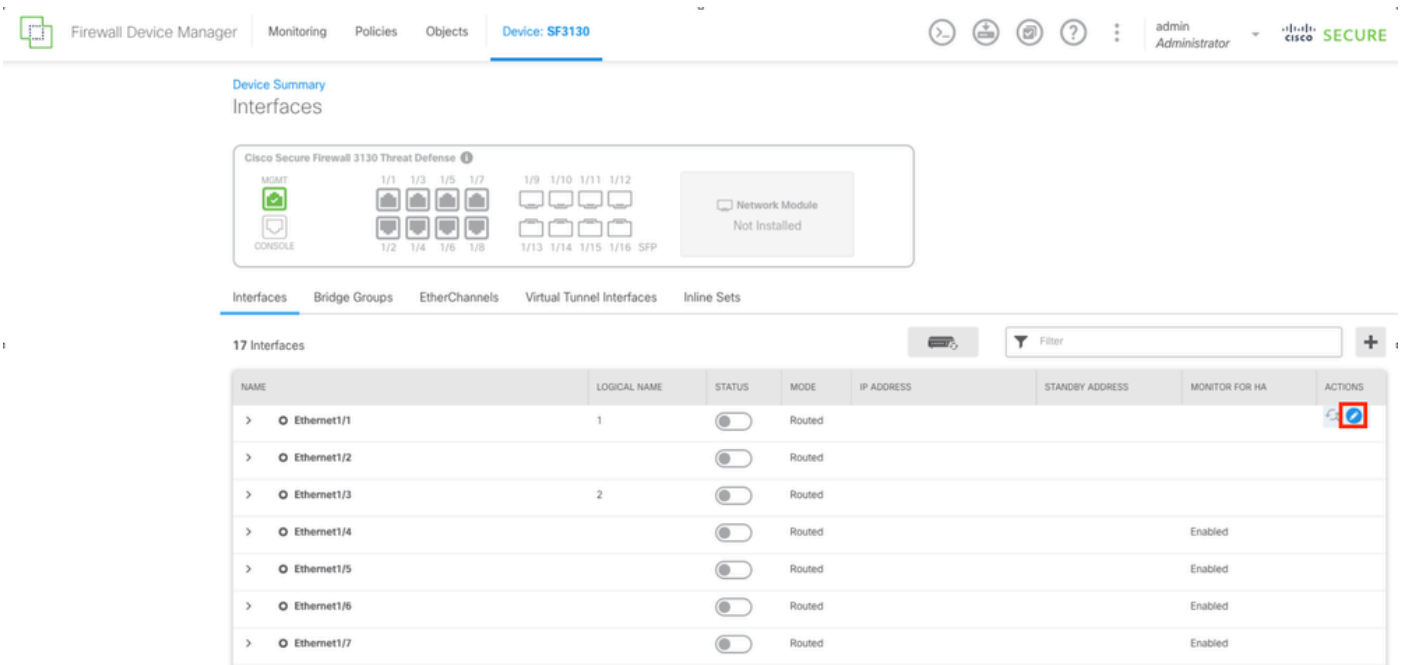
Efetue login no FDM no Firewall Seguro e navegue até a seção interfaces selecionando o botão Exibir Todas as Interfaces.



Painel Principal do FDM

Etapa 2.

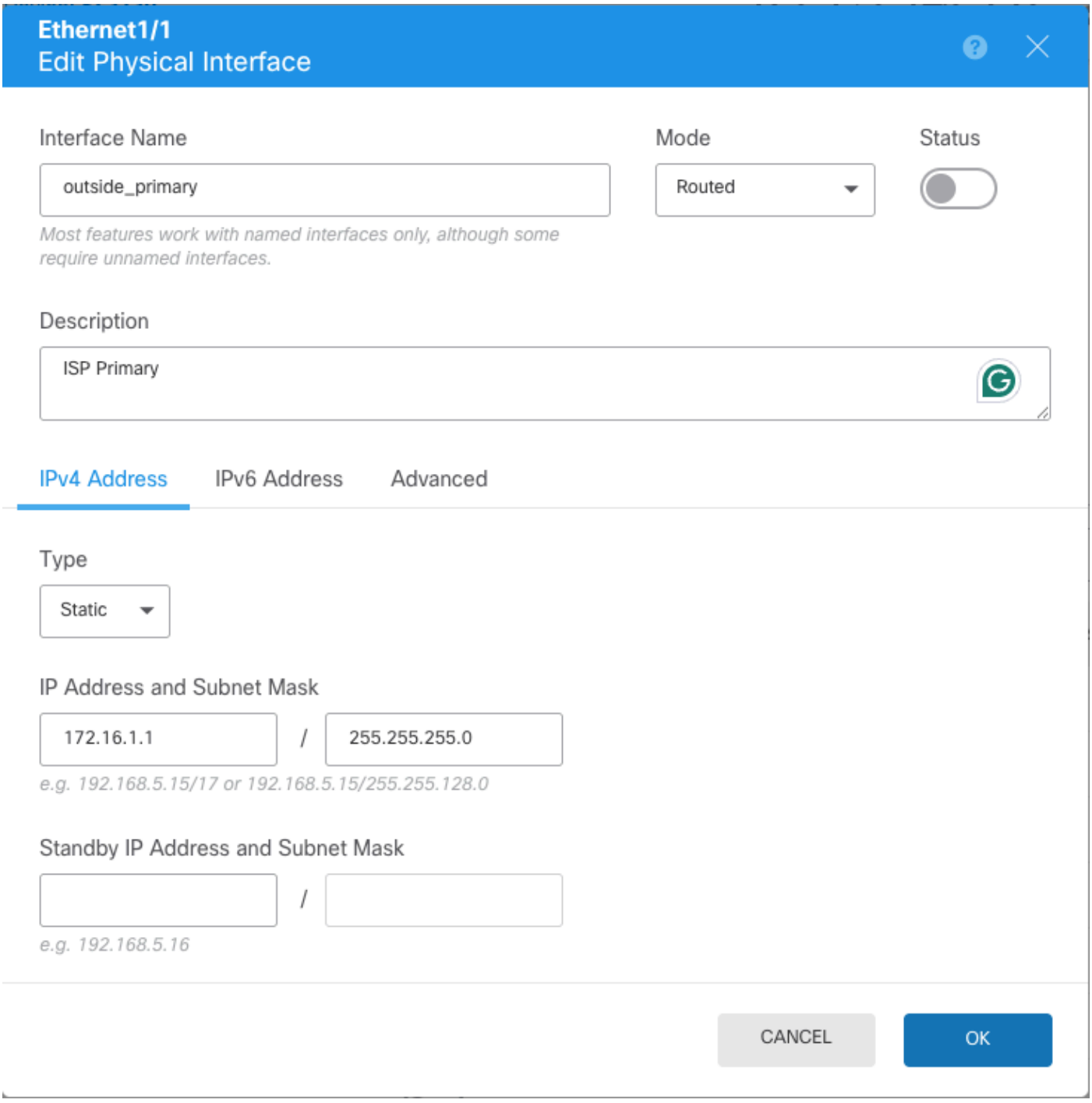
Para configurar a interface para a conexão principal do ISP, comece selecionando a interface desejada. Selecionando o botão de interface correspondente para continuar. Neste exemplo, a interface usada é Ethernet1/1.



Guia Interfaces

Etapa 3.

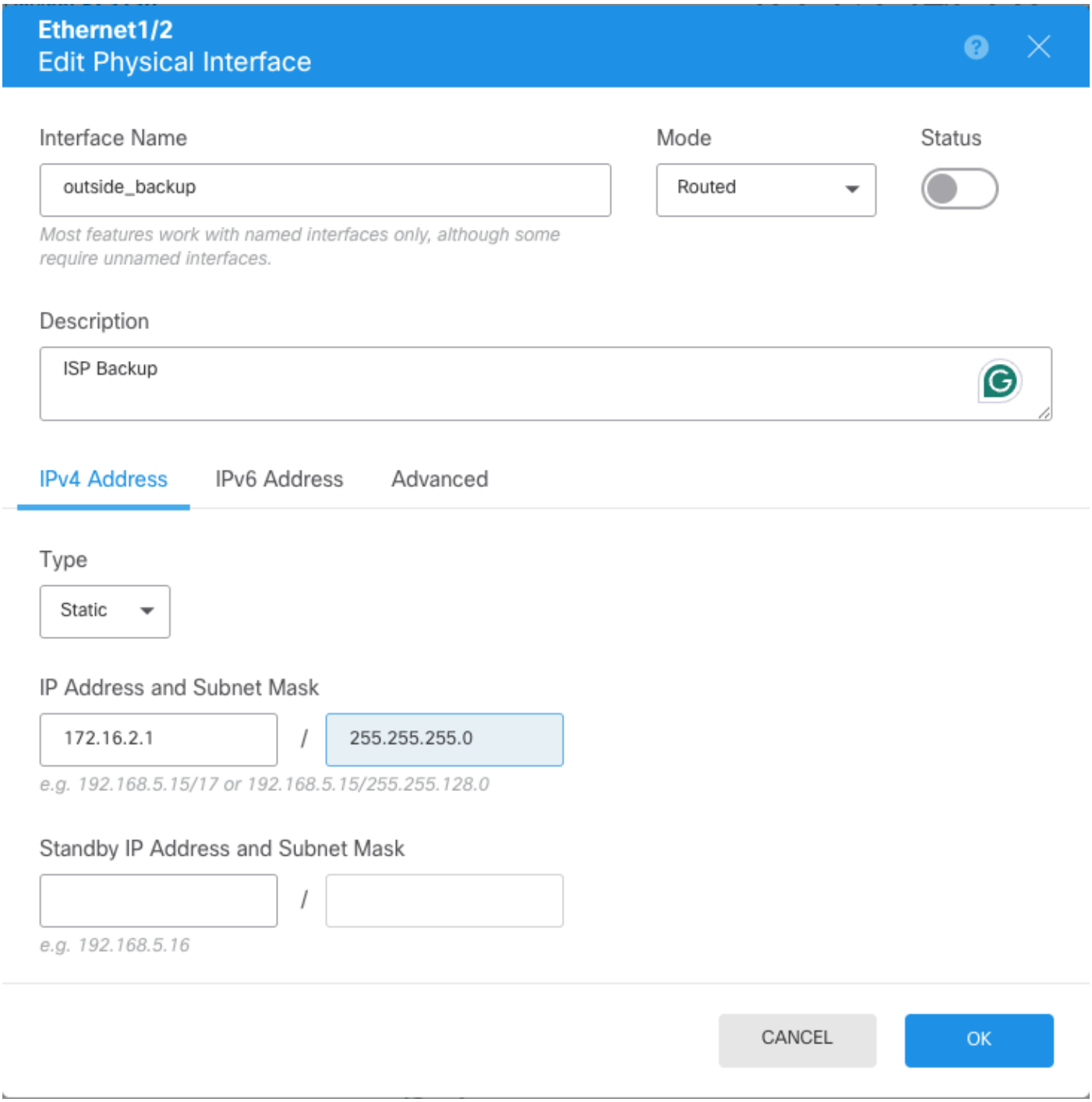
Configure a interface com os parâmetros corretos para sua conexão principal do ISP. Neste exemplo, a interface é outside_primary.



Configuração da interface primária do ISP

Etapa 4.

Repita o mesmo processo para a interface ISP secundária. Neste exemplo, a interface Ethernet1/2 é usada.

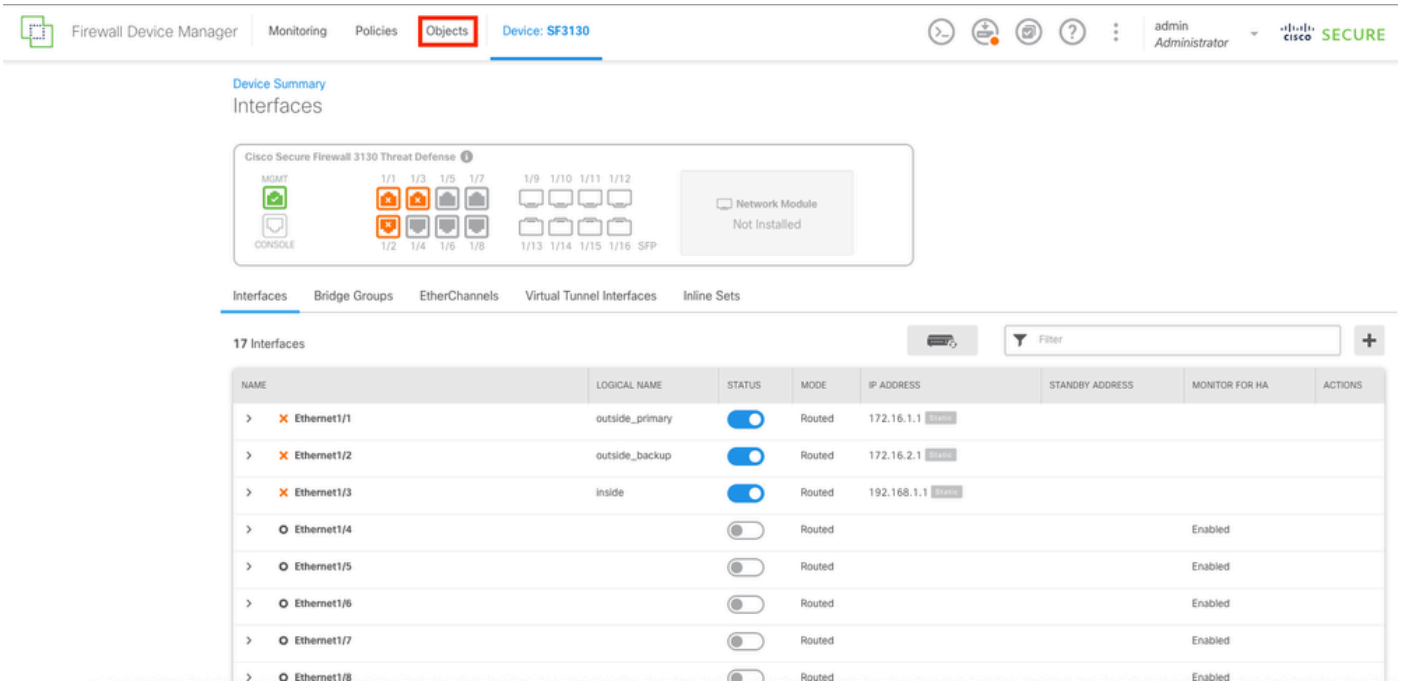


Configuração da interface secundária do ISP

Etapa 5.

Depois de configurar as duas interfaces para os ISPs, a próxima etapa é configurar o Monitor SLA para a interface primária.

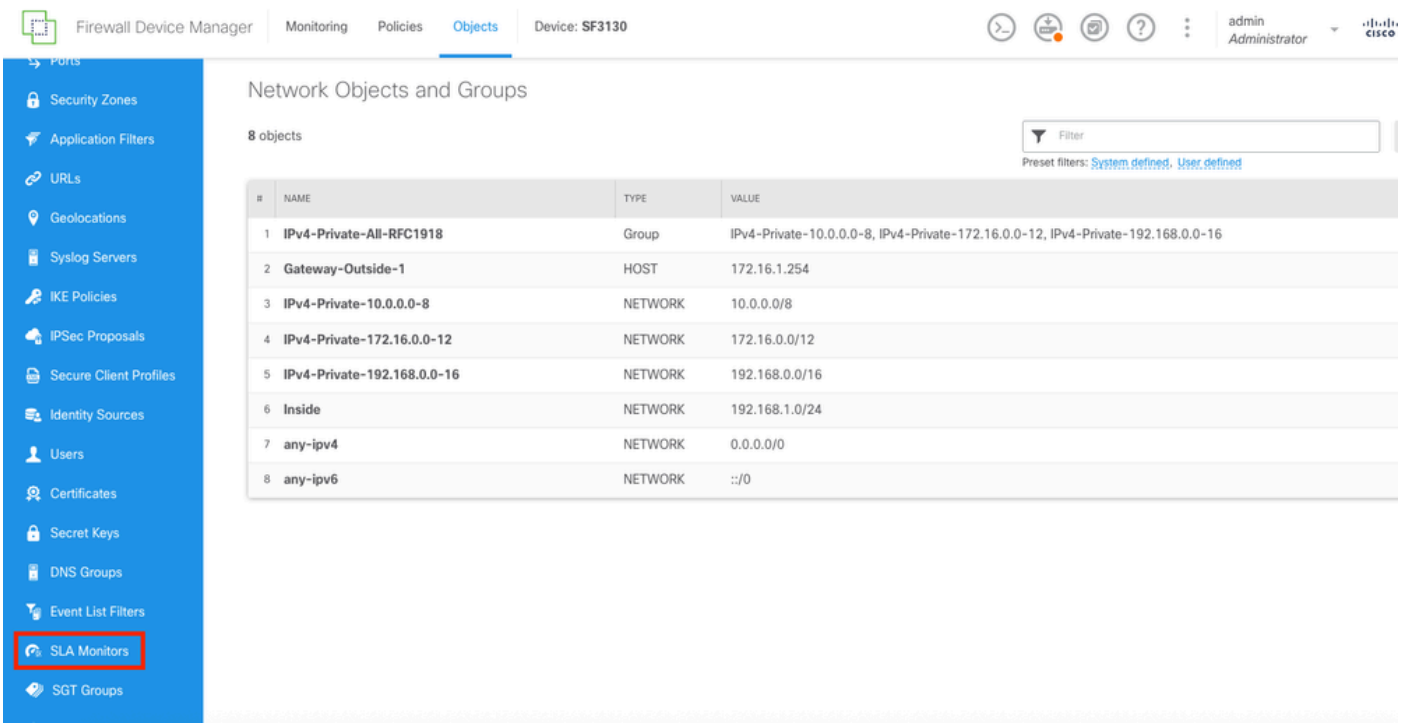
Navegue até a seção Objetos selecionando o botão Objetos localizado na parte superior do menu.



Interfaces configuradas

Etapa 6.

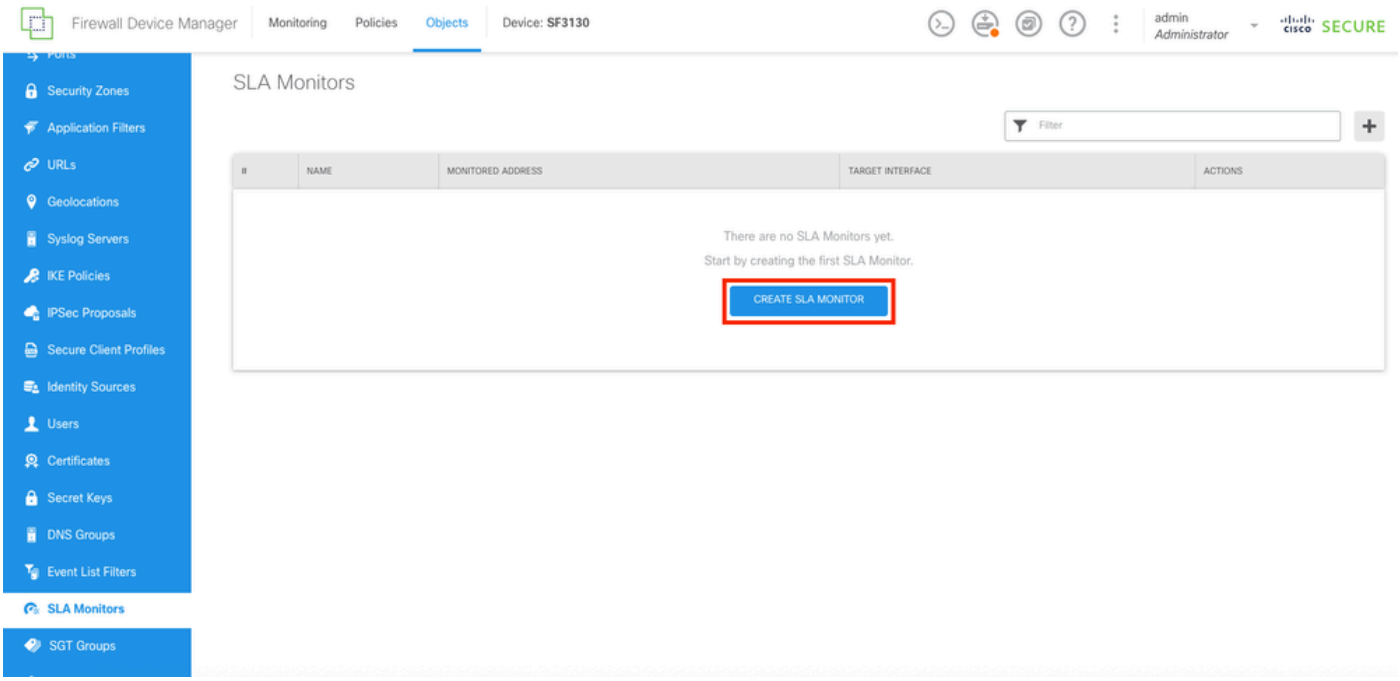
Selecione na coluna esquerda o botão Monitores de SLA.



Tela de Objetos

Passo 7.

Crie um novo Monitor de SLA selecionando o botão Criar Monitor de SLA.



Seção Monitor do SLA

Etapa 8.

Configure os parâmetros para a conexão do ISP Principal.

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

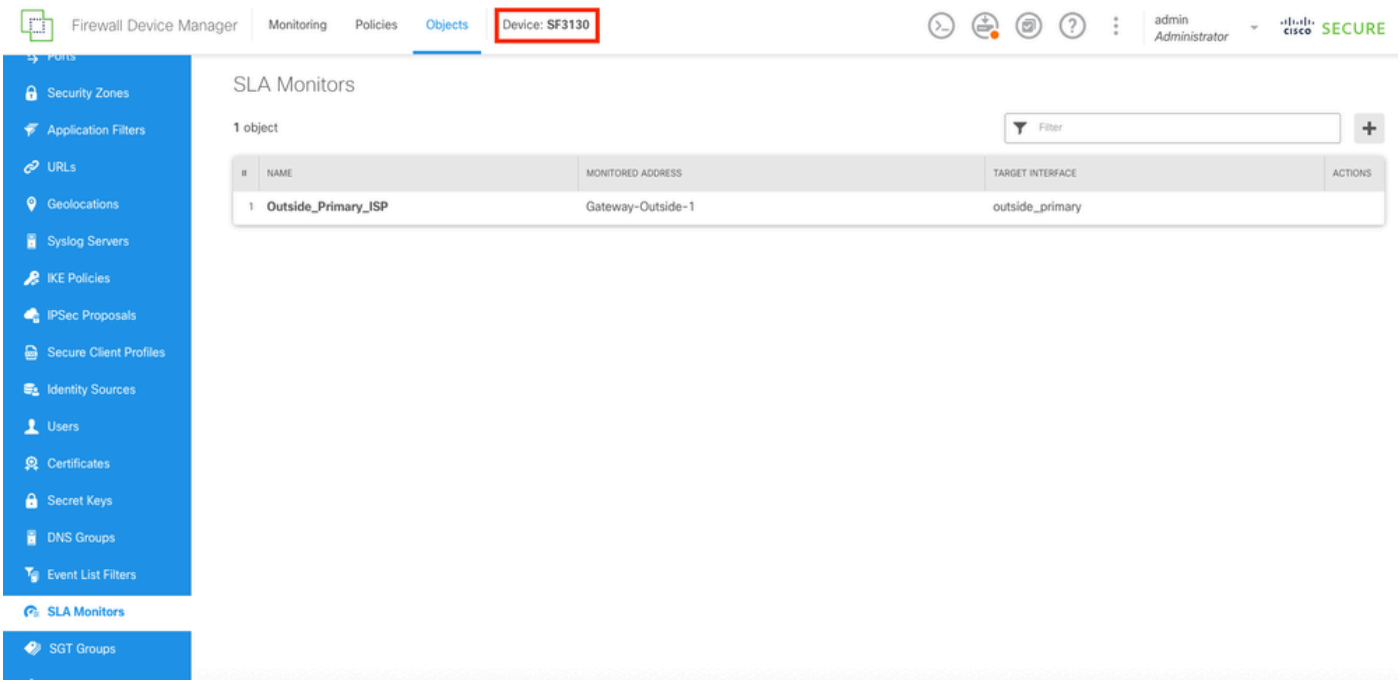
0 - 16384

CANCEL OK

Criação de objeto de SLA

Etapa 9.

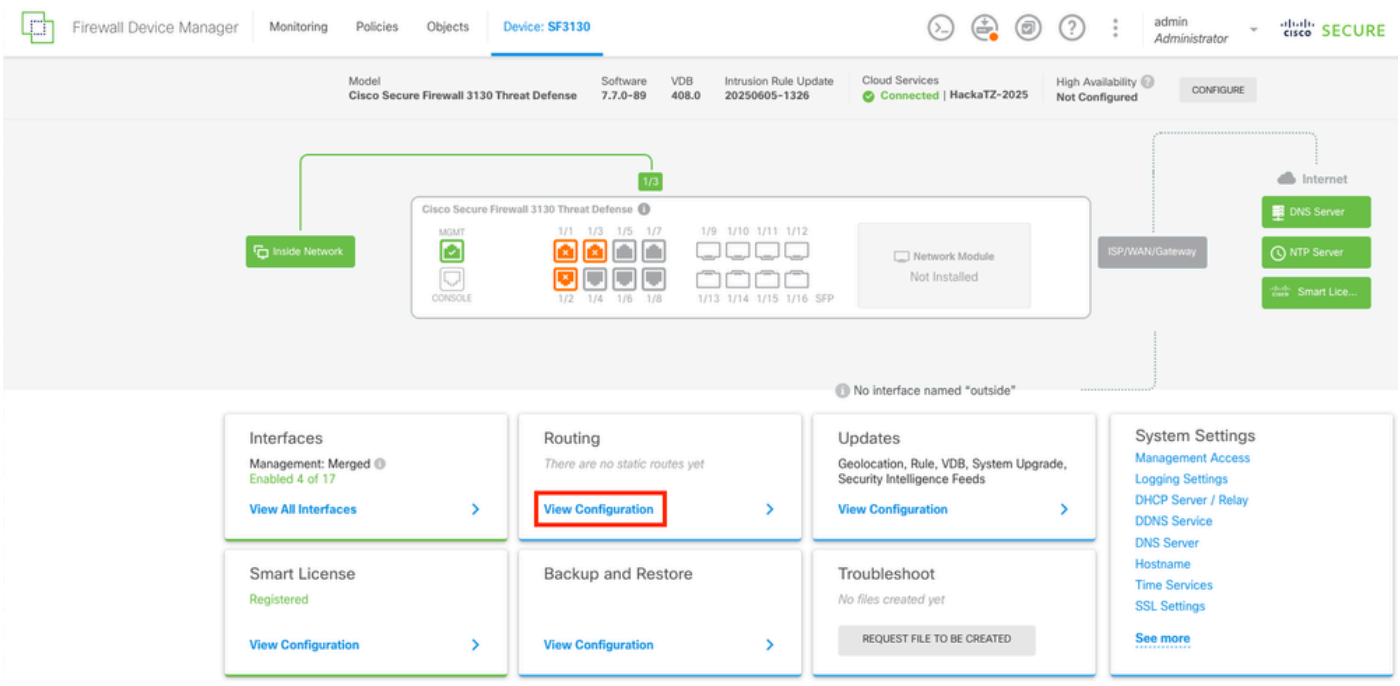
Depois que o objeto for criado, a rota estática para as interfaces deverá criá-lo. Navegue até o painel principal selecionando o botão Device.



Monitor do SLA criado

Etapa 10.

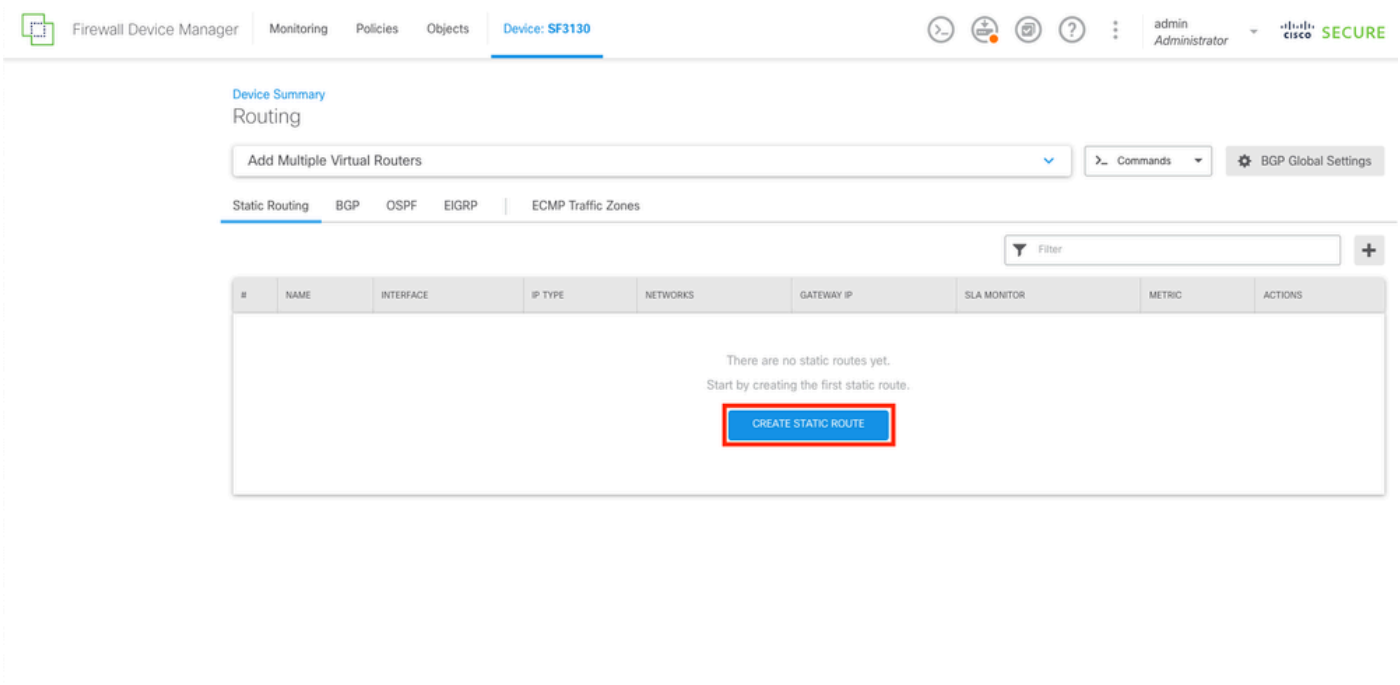
Navegue até a Seção de roteamento selecionando a Configuração de exibição no Painel de roteamento.



Painel principal

Etapa 11.

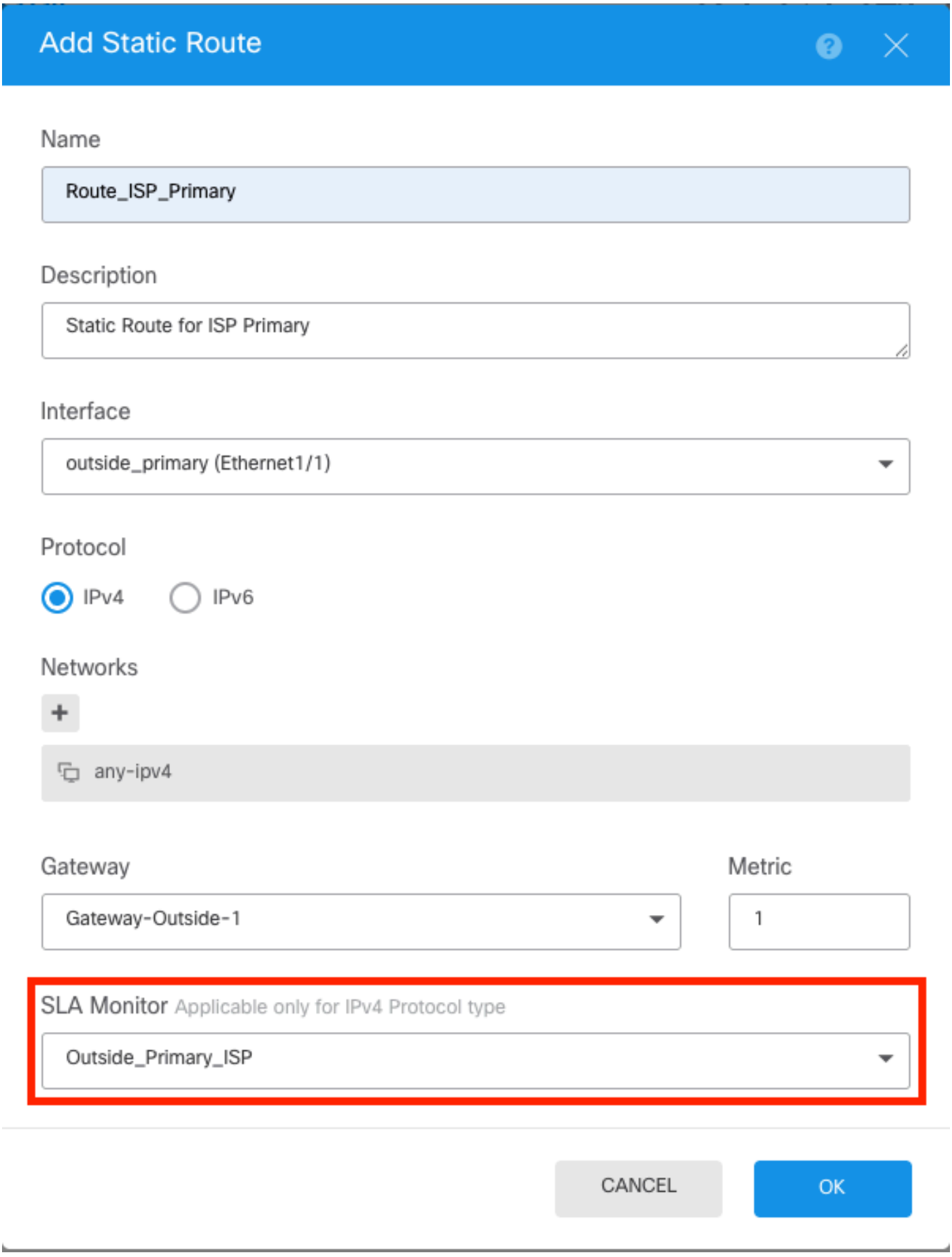
Na guia Static Routing (Roteamento estático), crie as 2 rotas estáticas padrão para ambos os ISPs. Para criar uma nova rota estática, selecione o botão CREATE STATIC ROUTE.



Seção de roteamento estático

Etapa 12.

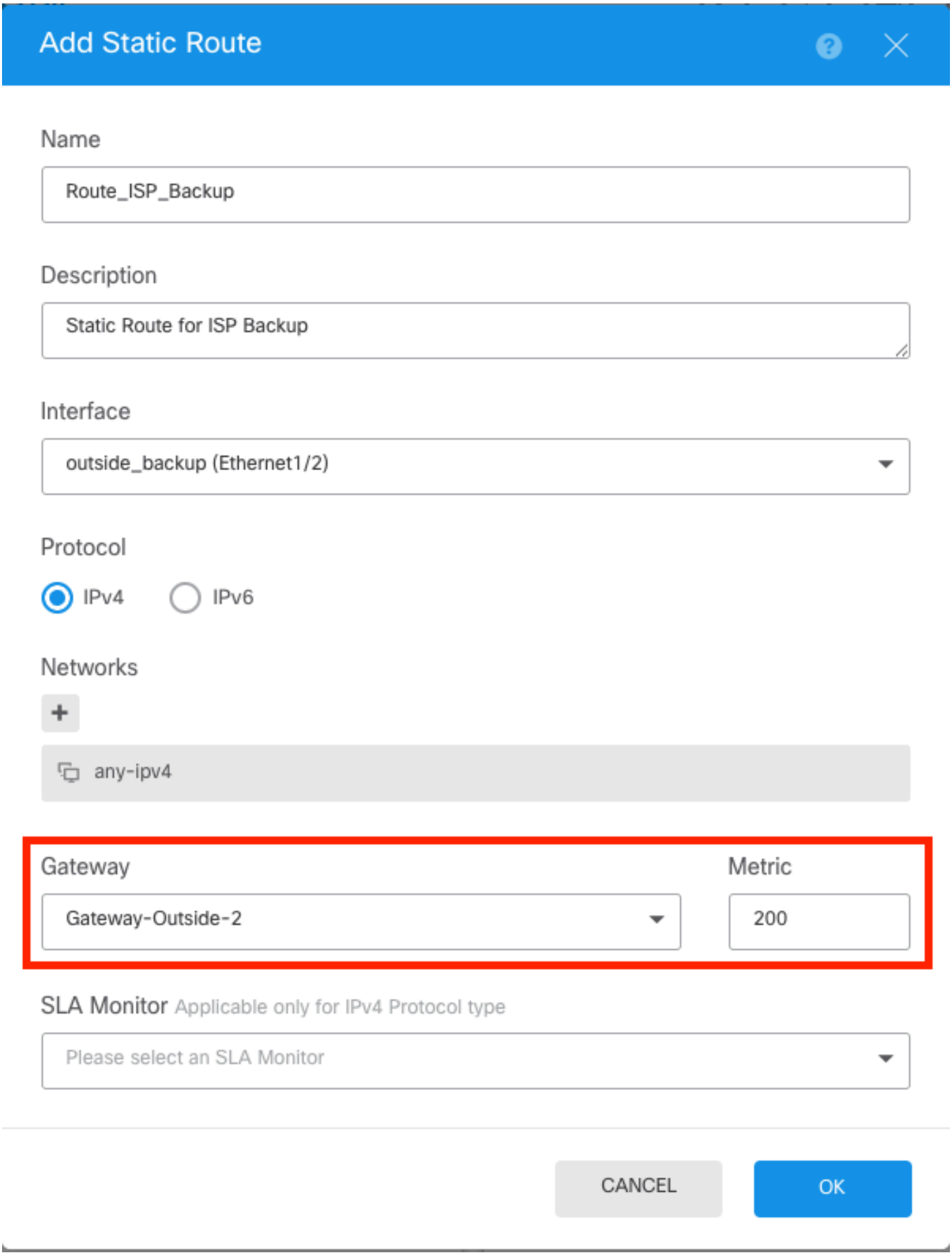
Primeiro, crie a rota estática para o ISP primário. No final, adicione o objeto de monitor de SLA que foi criado na última etapa.



Rota estática para ISP primário

Etapa 13.

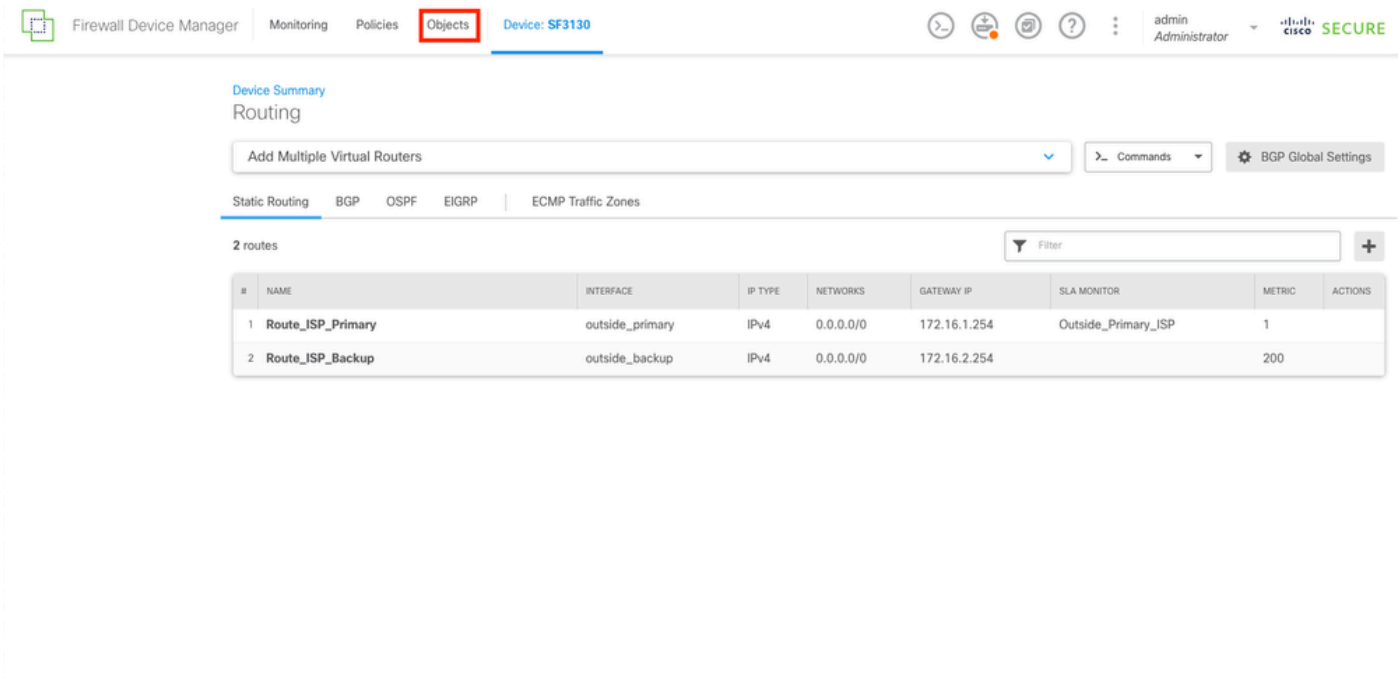
Repita a última etapa e crie uma rota padrão, para o ISP secundário com o gateway apropriado e uma Métrica diferente. Neste exemplo, ele foi aumentado para 200.



Rota estática para ISP secundário

Etapa 14.

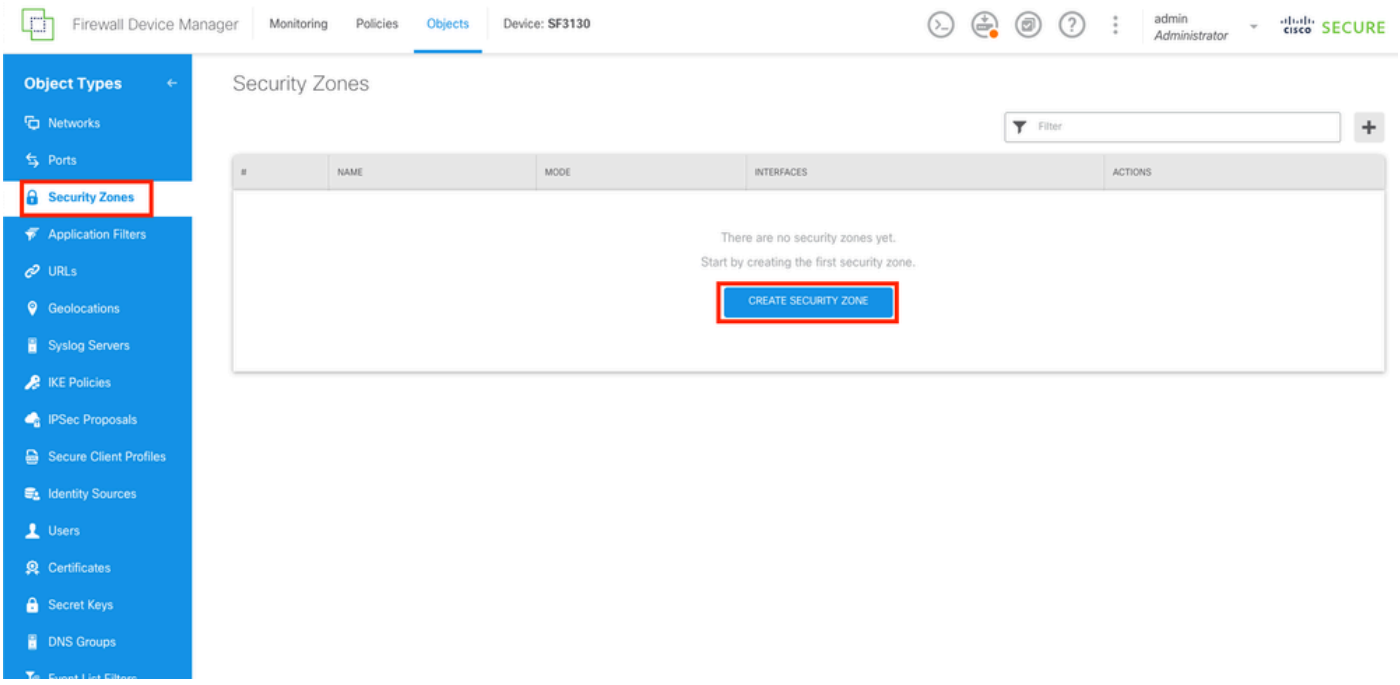
Depois que as duas rotas estáticas forem criadas, uma zona de segurança deverá ser criada. Navegue até a seção Objetos selecionando o botão Objetos na parte superior.



Rotas estáticas criadas

Etapa 15.

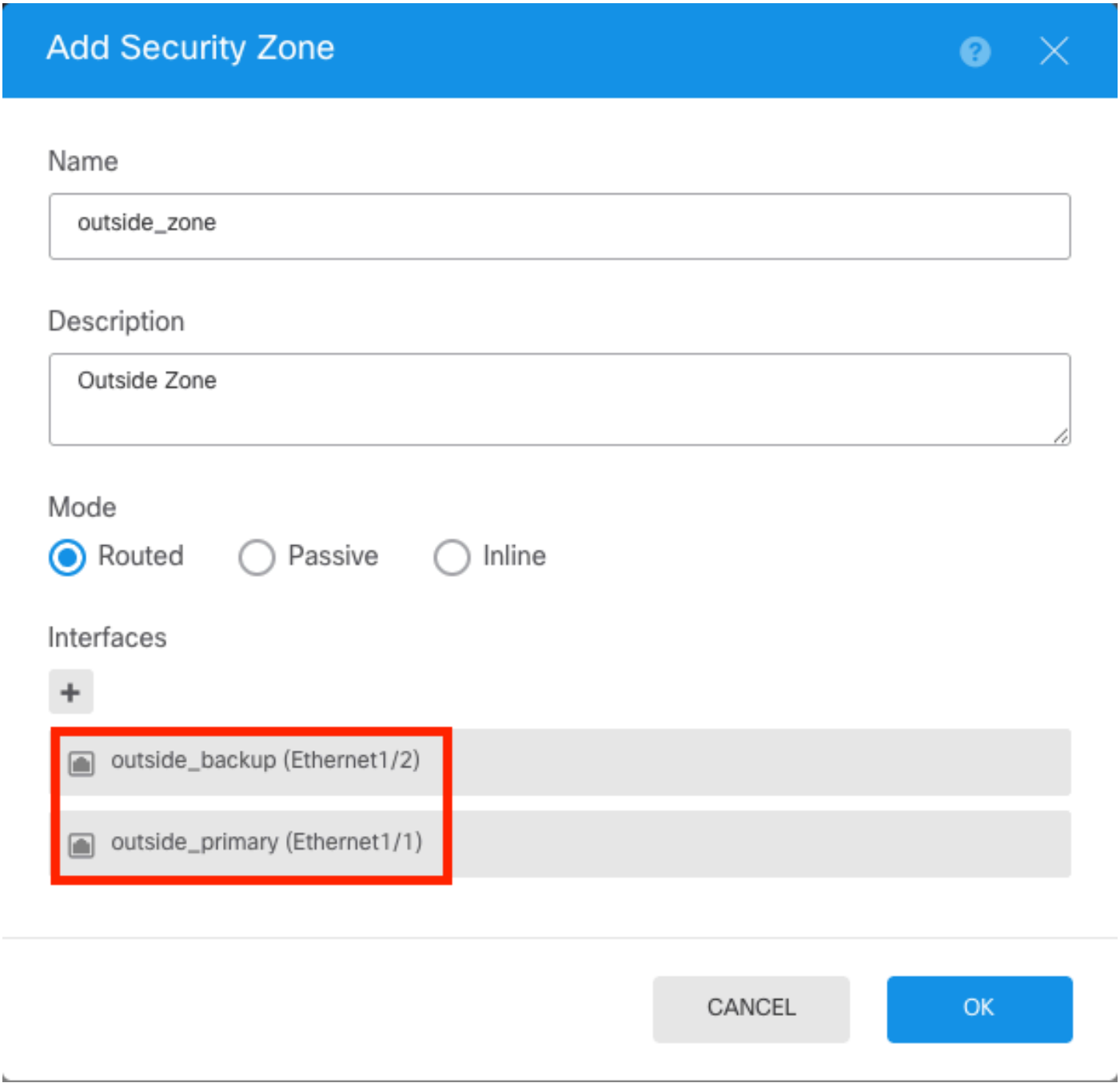
Navegue até a seção Zonas de segurança selecionando na coluna esquerda o botão Zonas de segurança e crie uma nova zona selecionando o botão CRIAR ZONA DE SEGURANÇA.



Seção Zonas de Segurança

Etapa 16.

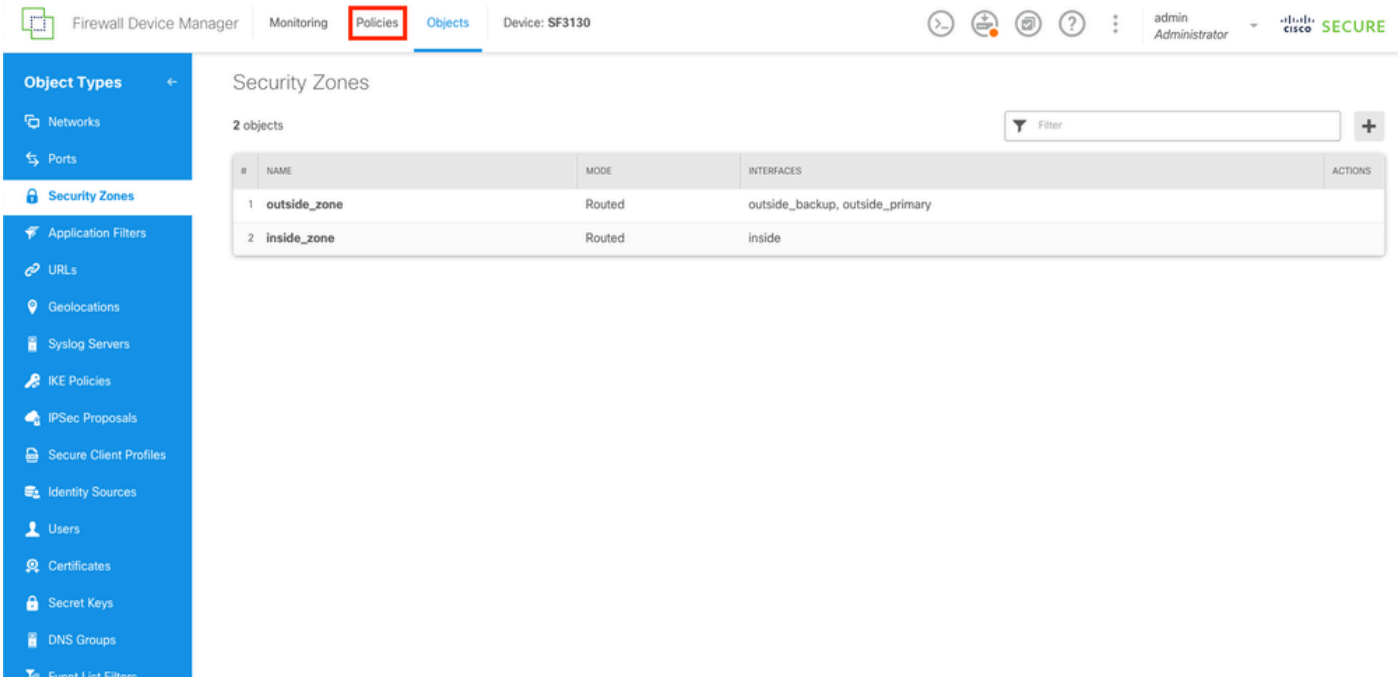
Crie a Outside Security Zone com as duas interfaces externas para as conexões dos ISPs.



Zona de Segurança Externa

Etapa 17.

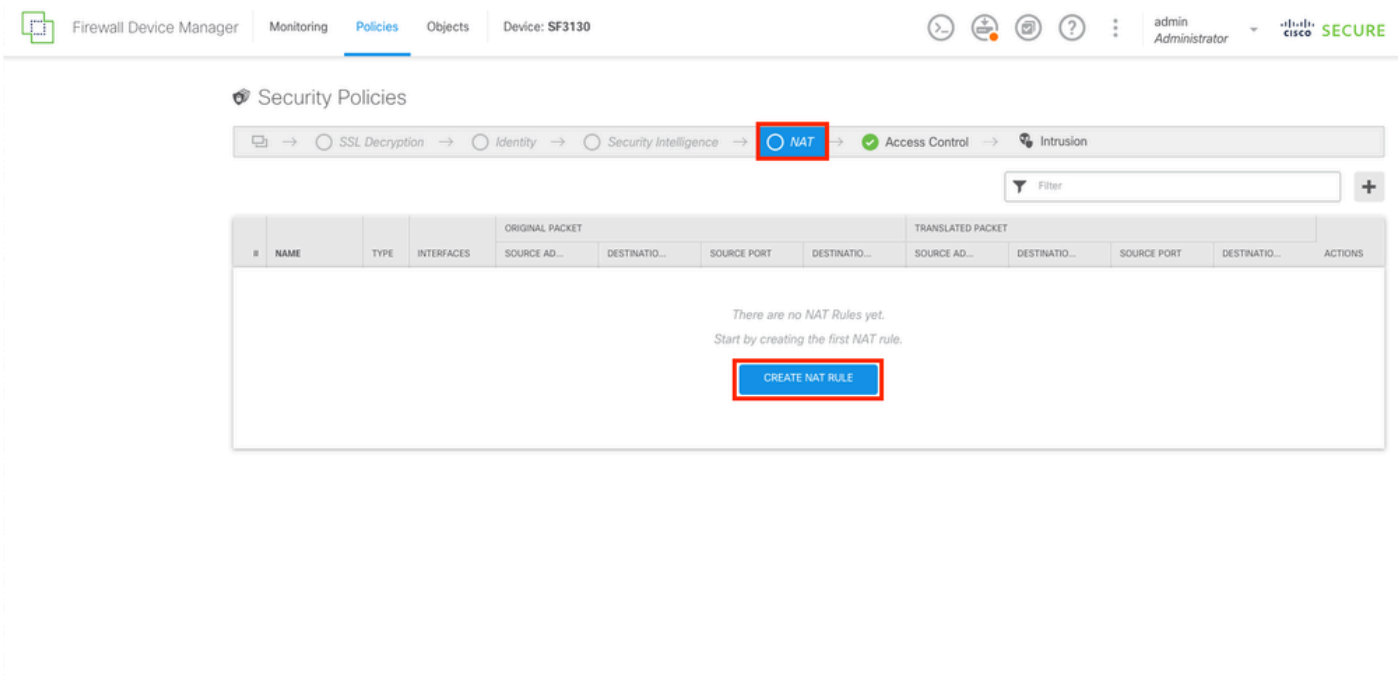
Depois que a zona de segurança for criada, um NAT deverá ser criado. Navegue até a seção Policies selecionando o botão Policies na parte superior.



Zonas de segurança criadas

Etapa 18.

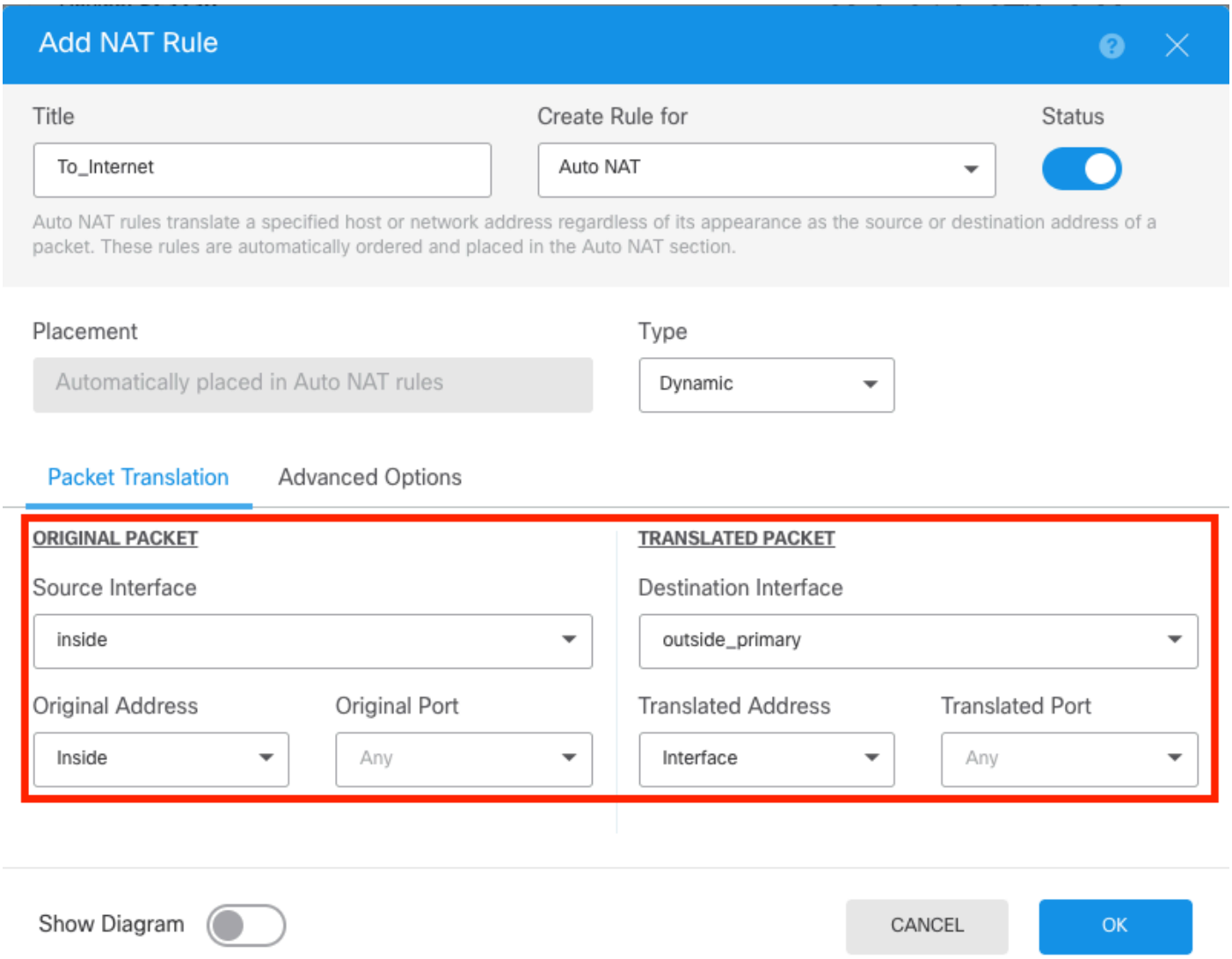
Navegue até a seção NAT selecionando o botão NAT e crie uma nova regra selecionando o botão CREATE NAT RULE.



Seção NAT

Etapa 19.

Para o failover do ISP, a configuração deve ter 2 rotas através de interfaces externas. Primeiro, para a conexão da interface externa primária com o ISP primário.

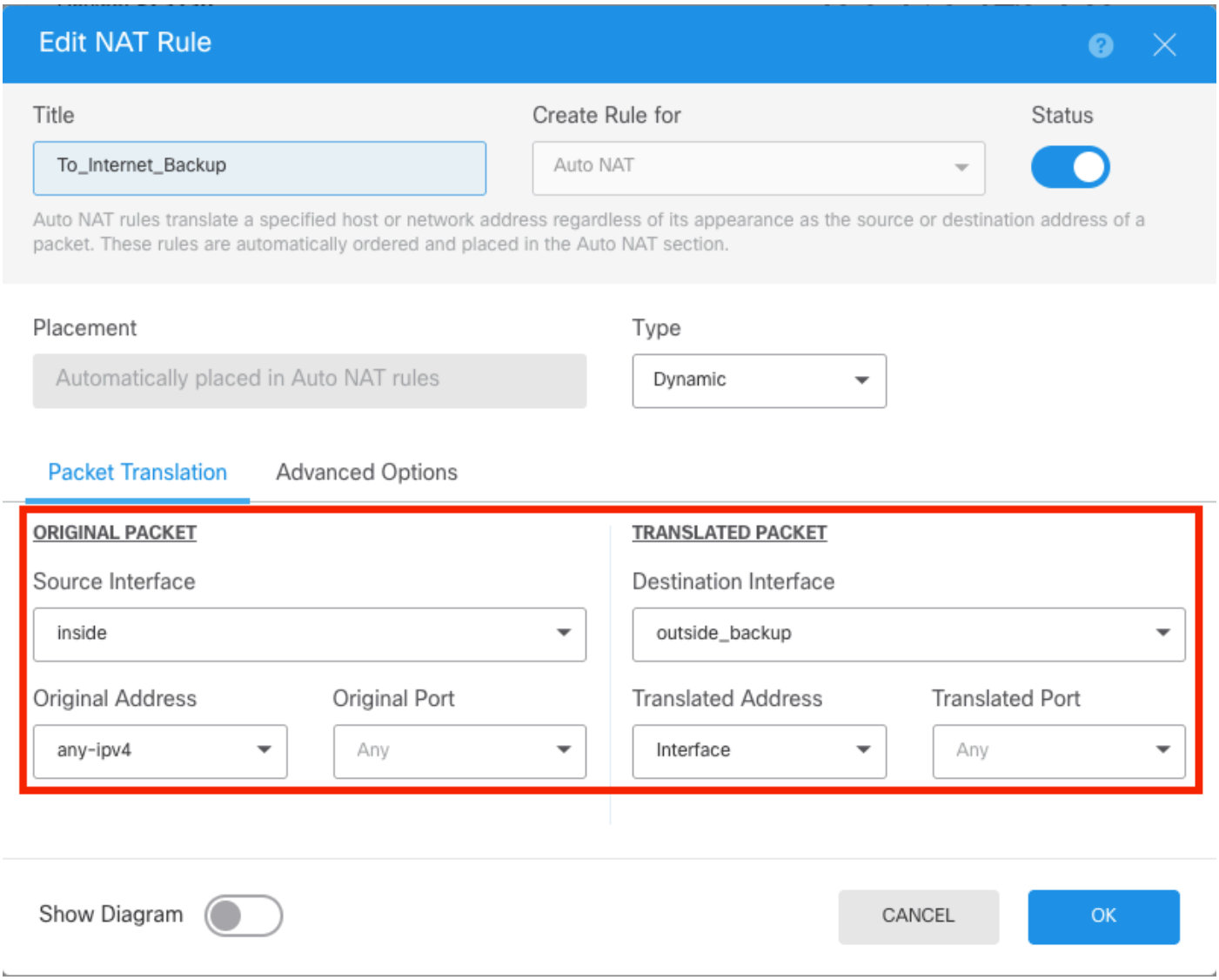


NAT para ISP primário

Etapa 20.

Agora, um segundo NAT para a conexão do ISP secundário.

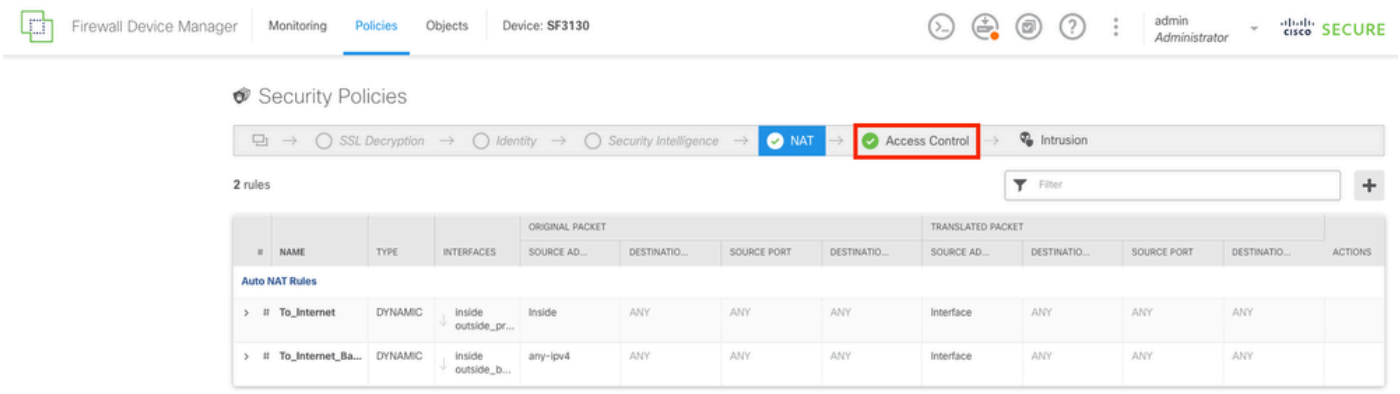
Note: Para o endereço original, a mesma rede não pode ser usada. Neste exemplo, para o ISP secundário, o Endereço original é o objeto any-ipv4.



NAT para ISP secundário

Etapa 21.

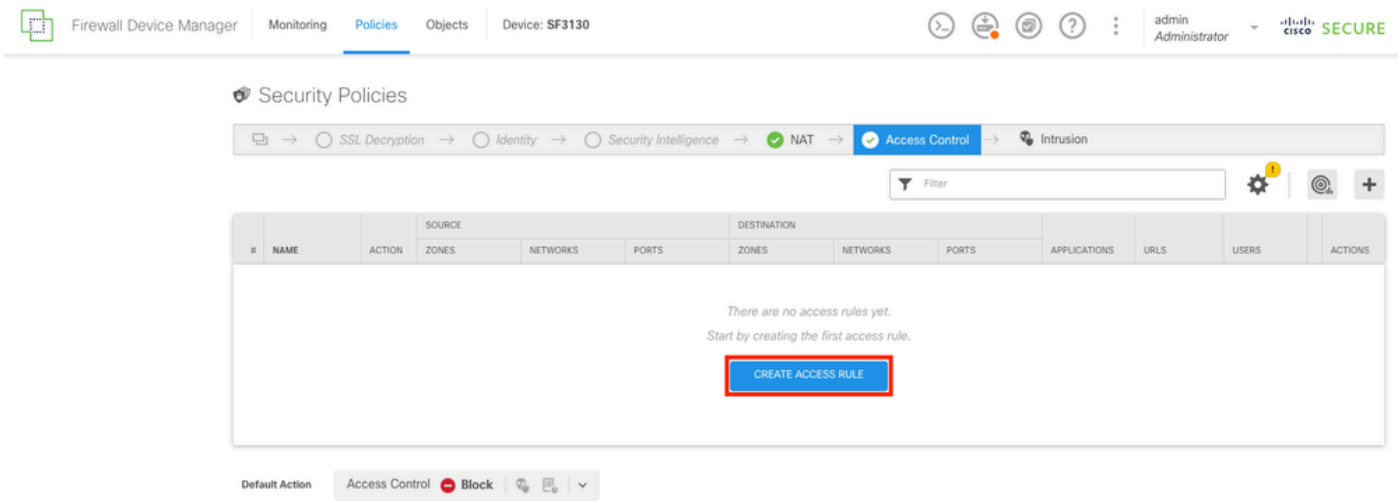
Depois de criar as duas regras de NAT, uma Regra de controle de acesso deve ser estabelecida para permitir o tráfego de saída. Selecione o botão Controle de acesso.



Regras NAT criadas

Etapa 22.

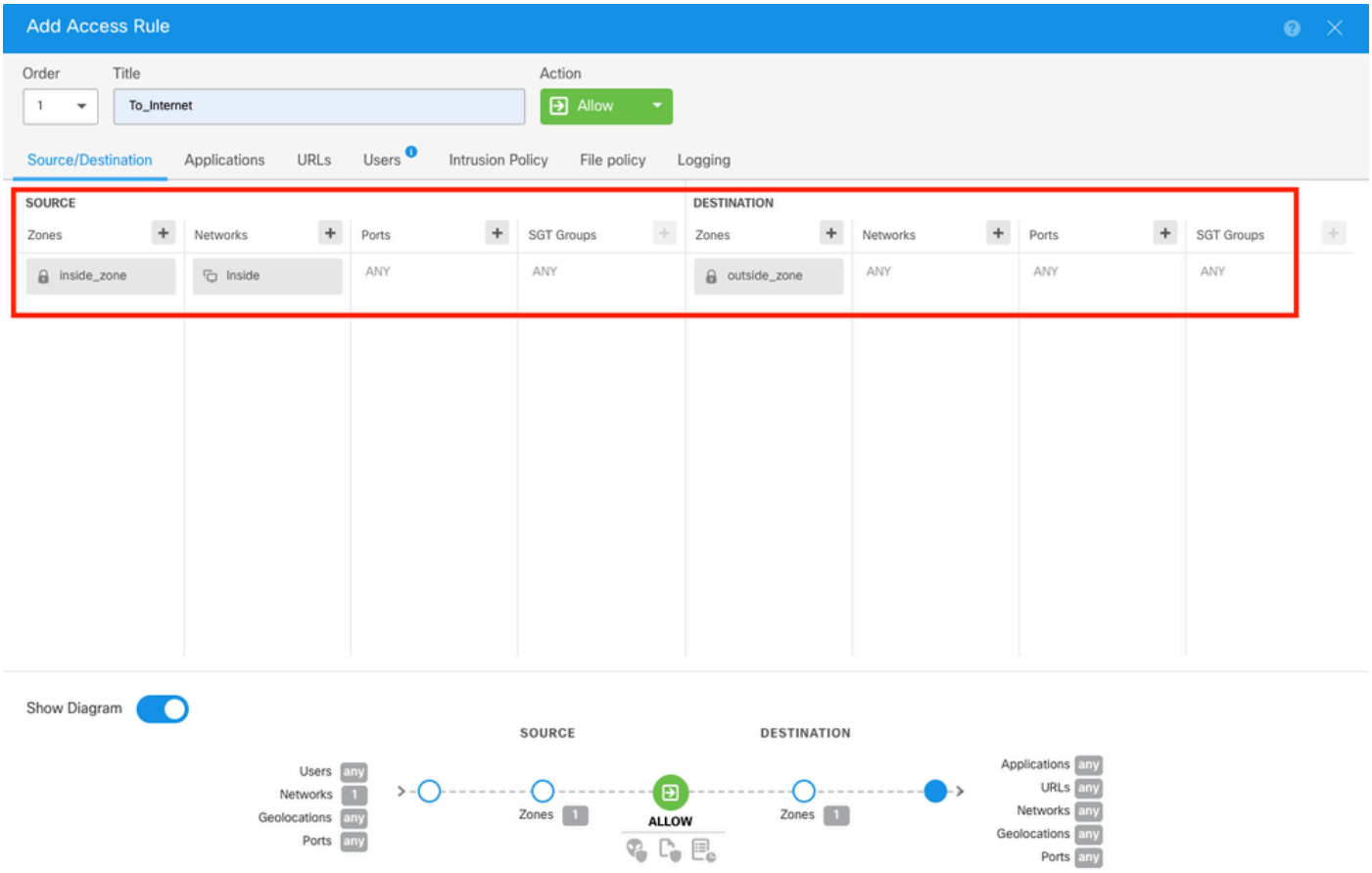
Para criar a Regra de Controle de Acesso, selecione o botão CRIAR REGRA DE ACESSO.



Seção de Controle de Acesso

Etapa 23.

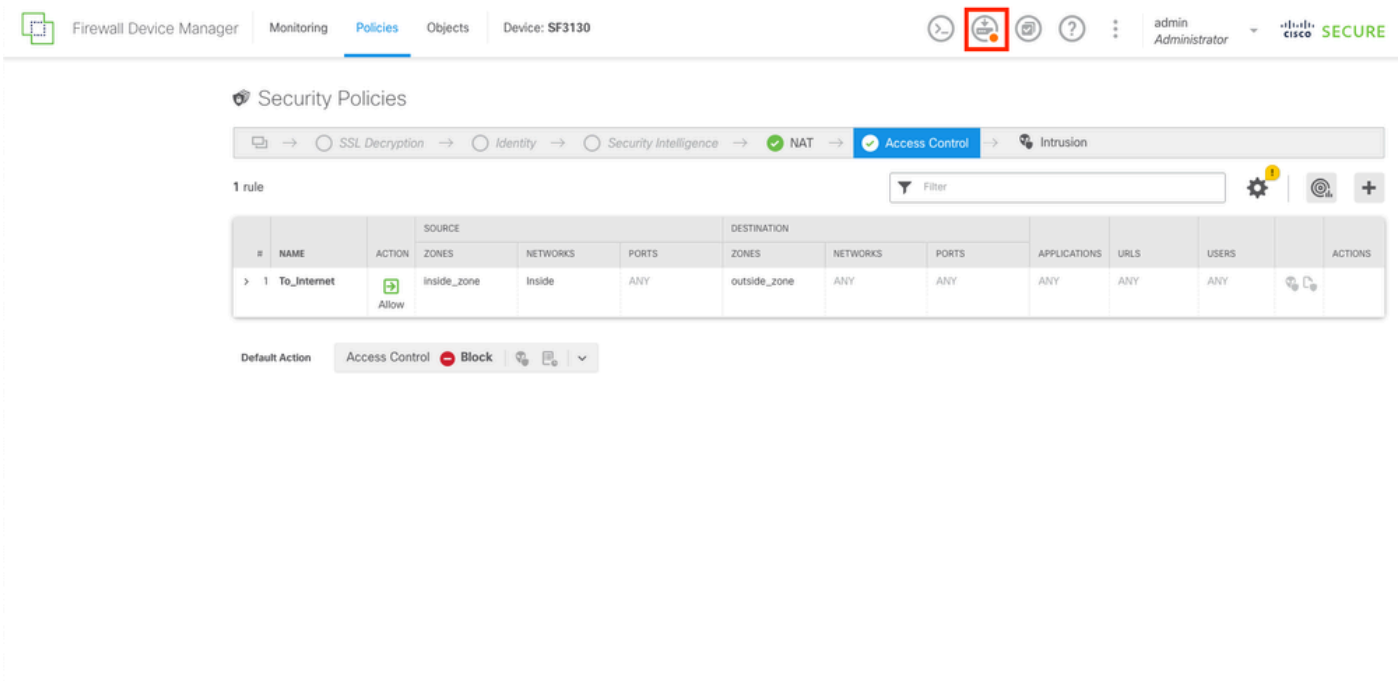
Selecione as zonas e redes desejadas.



Regra de controle de acesso

Etapa 24.

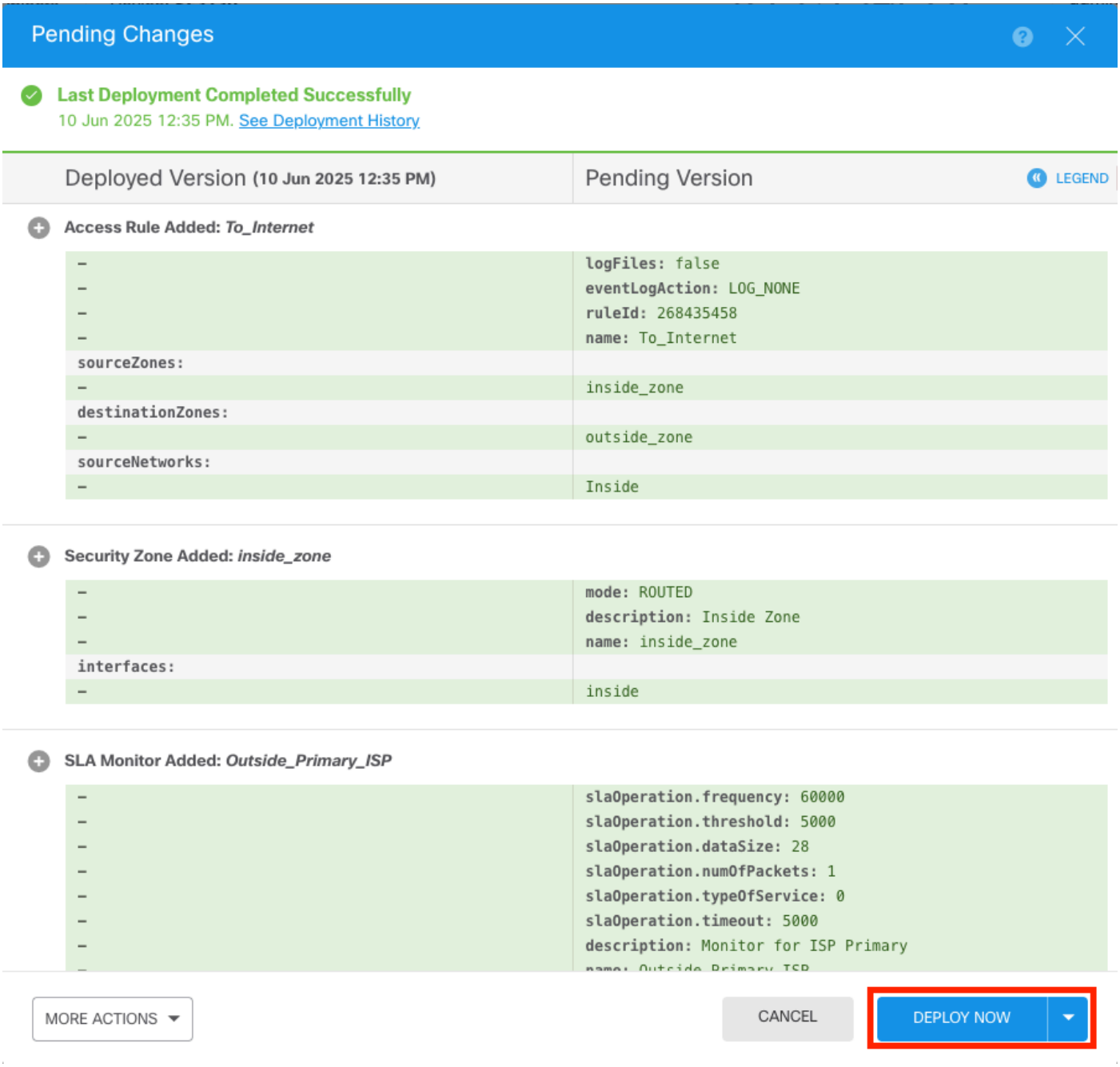
Depois que a Regra de controle de acesso for criada, continue para implantar todas as alterações selecionando o botão Implantar na parte superior.



Regra de Controle de Acesso Criada

Etapa 25.

Verifique as alterações e selecione o botão Implantar agora.



Verificação de Implantação

Diagrama de Rede

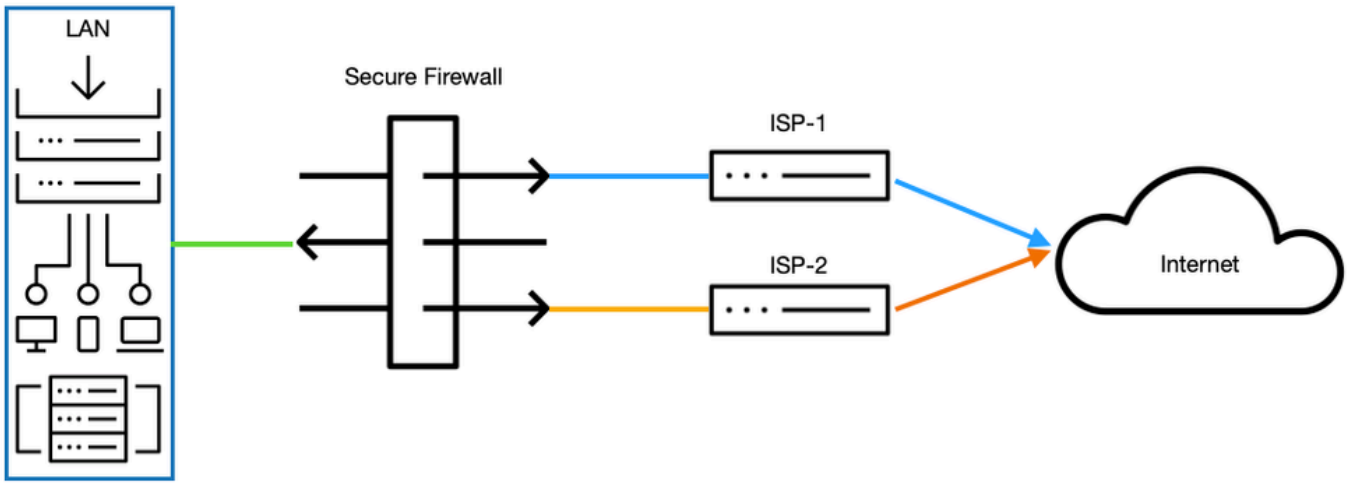


Diagrama de Rede

Verificar

<#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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.