Configuración de ISP dual en FTD mediante FDM

Contenido

Introducción

Este documento describe cómo configurar la conmutación por fallo del proveedor de servicios de Internet (ISP) dual mediante el Administrador de dispositivos de firewall (FDM) para la serie de firewall seguro.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Routing básico
- Conocimiento del panel del administrador de dispositivos de firewall
- Al menos 2 proveedores de servicios de Internet conectados al firewall seguro.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

· Cisco Secure Firewall con la versión 7.7.X o versiones posteriores.

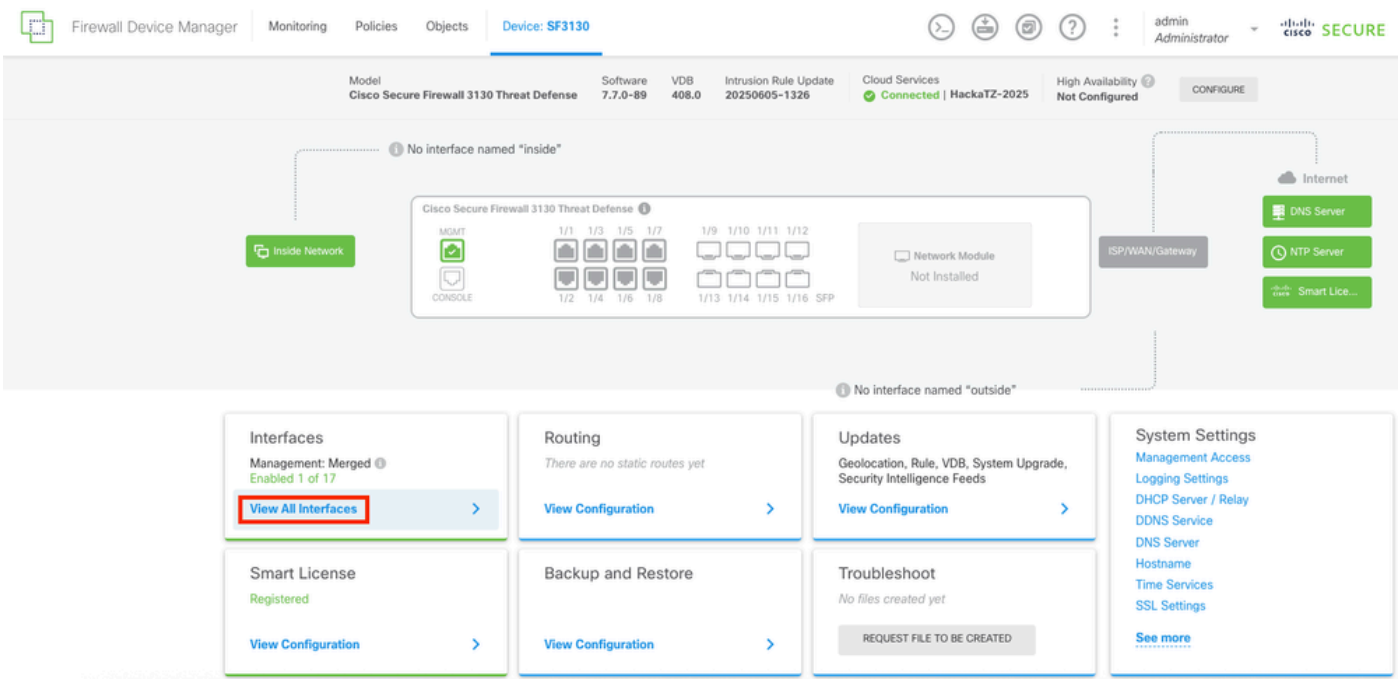
· Secure Firewall 3130 con versión 7.7.0.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Paso 1.

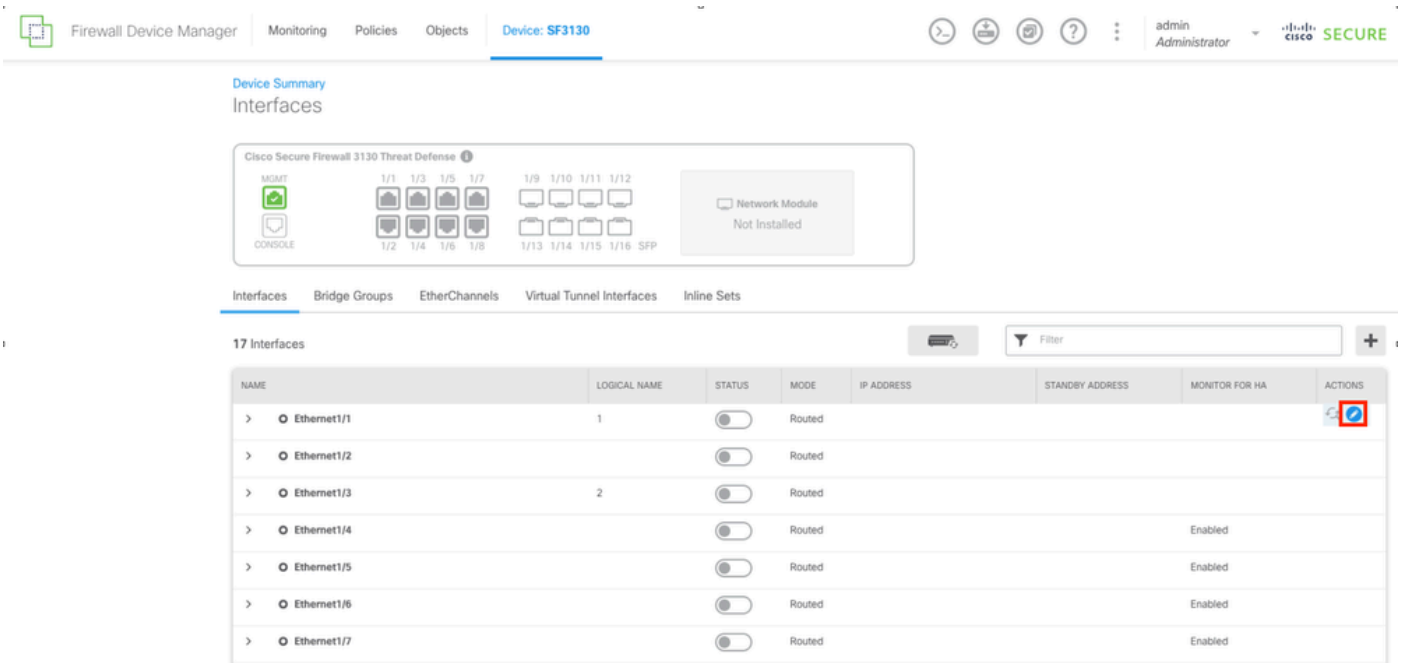
Inicie sesión en FDM en Secure Firewall y navegue hasta la sección de interfaces seleccionando el botón View All Interfaces.



Panel principal de FDM

Paso 2.

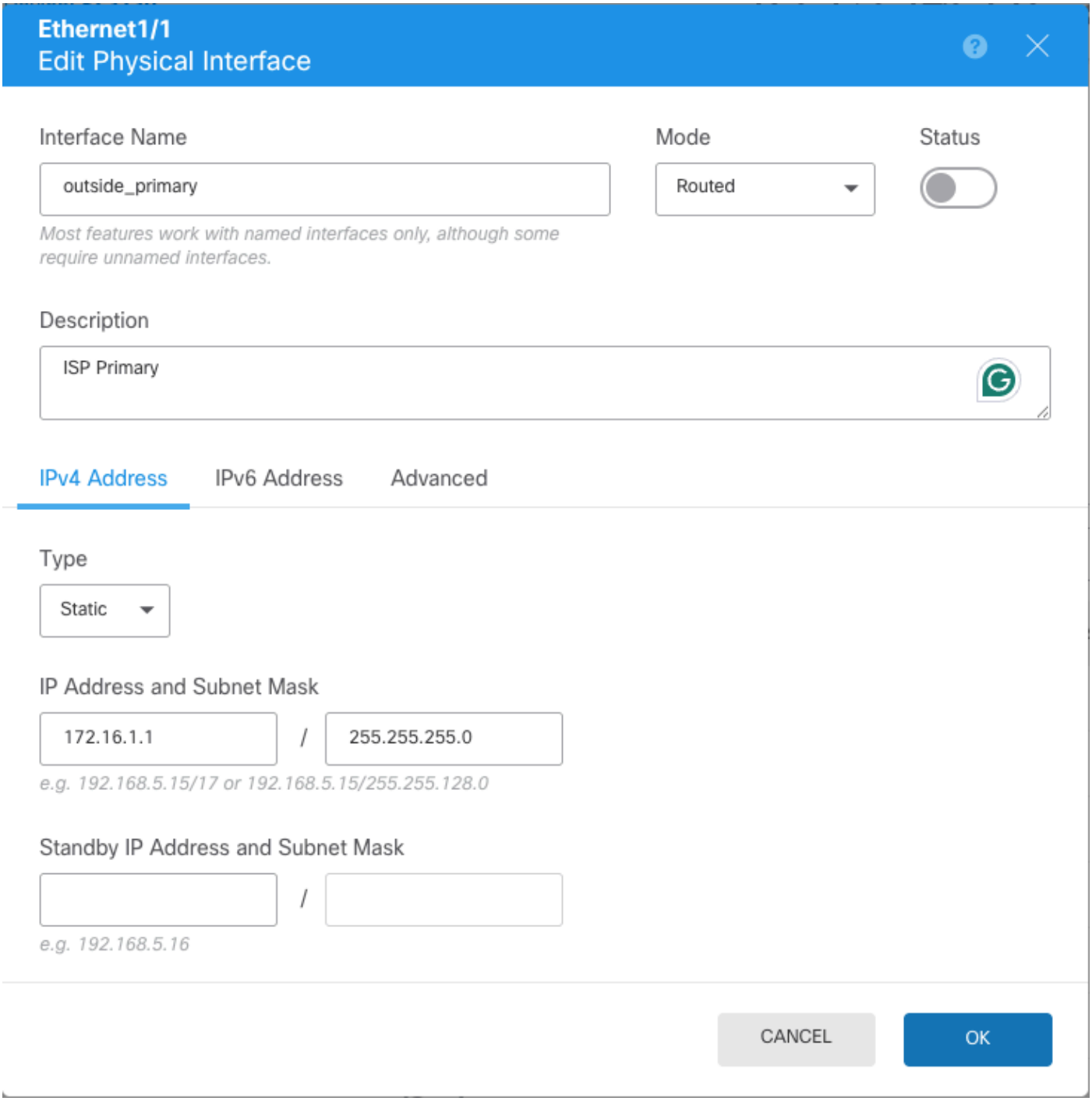
Para configurar la interfaz para la conexión del ISP primario, comience seleccionando la interfaz que desee. Seleccionar el botón de interfaz correspondiente para continuar. En este ejemplo, la interfaz utilizada es Ethernet1/1.



Ficha Interfaces

Paso 3.

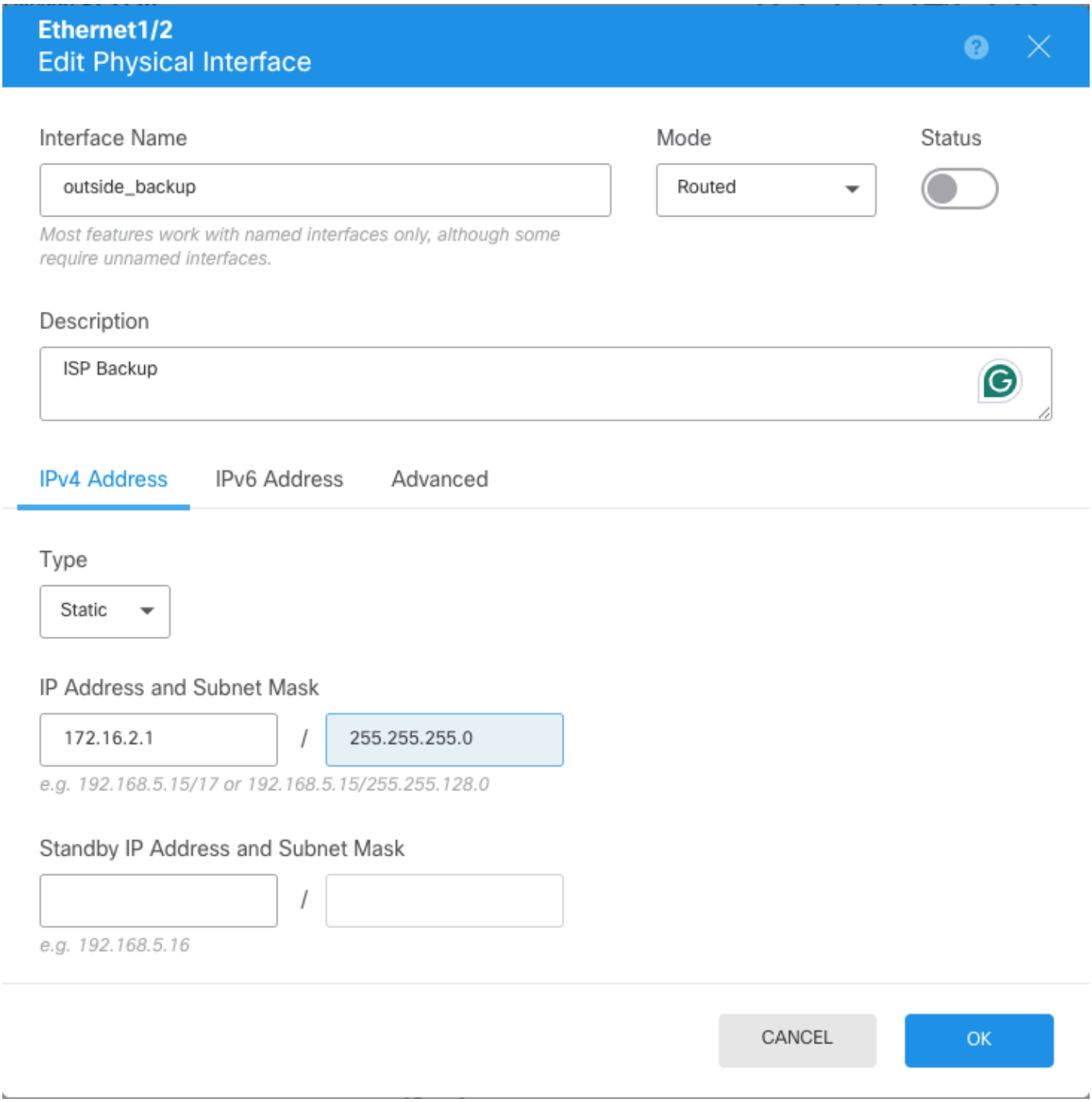
Configure la interfaz con los parámetros correctos para su conexión ISP principal. En este ejemplo, la interfaz es outside_primary.



Configuración de la interfaz ISP principal

Paso 4.

Repita el mismo proceso para la interfaz ISP secundaria. En este ejemplo, se utiliza la interfaz Ethernet1/2.

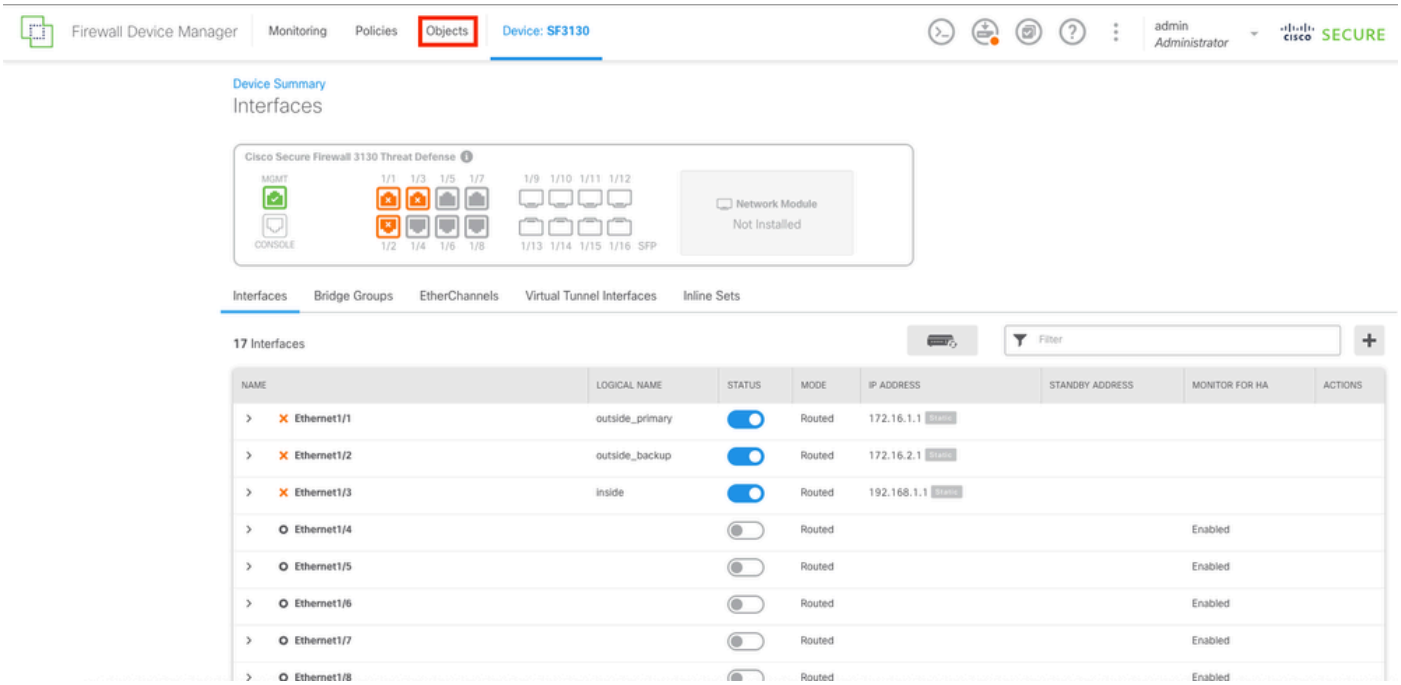


Configuración de la interfaz ISP secundaria

Paso 5.

Después de configurar las dos interfaces para los ISP, el siguiente paso es configurar el Monitor de SLA para la interfaz principal.

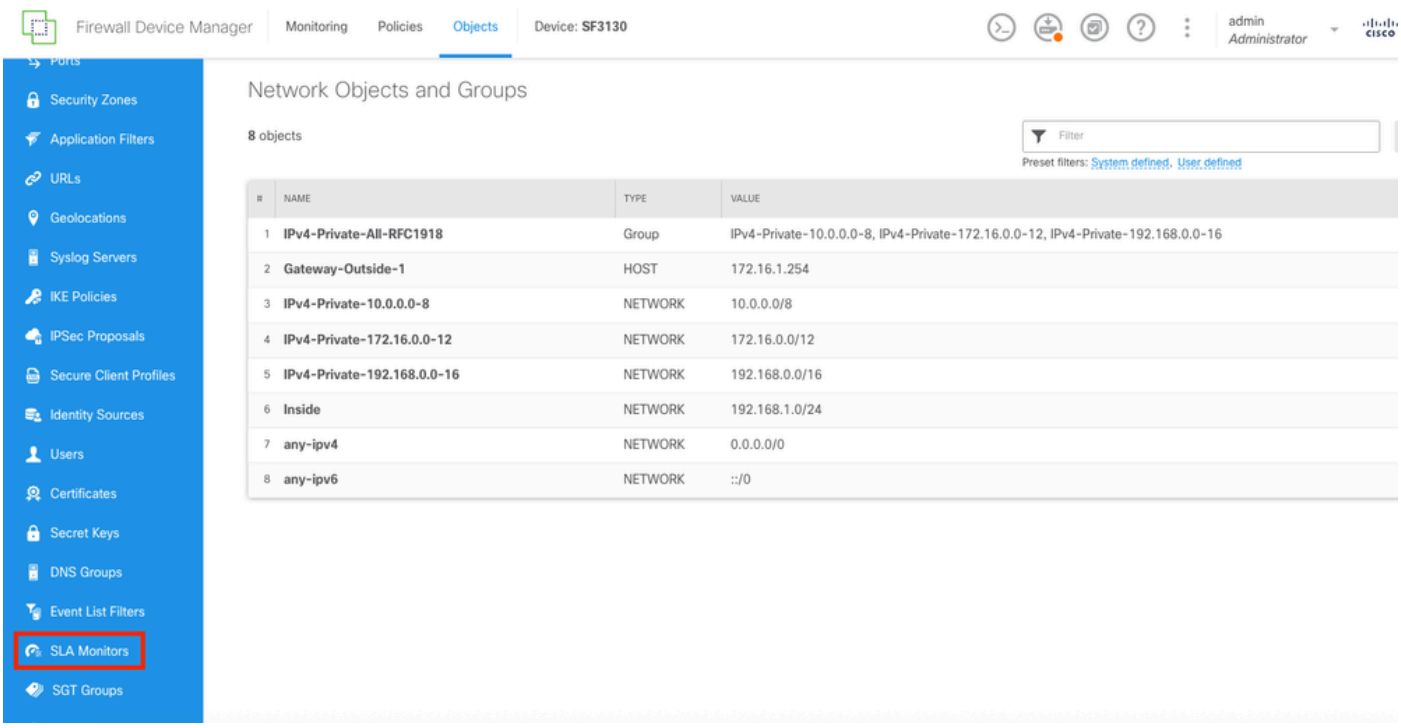
Vaya a la sección Objetos seleccionando el botón Objetos situado en la parte superior del menú.



Interfaces configuradas

Paso 6.

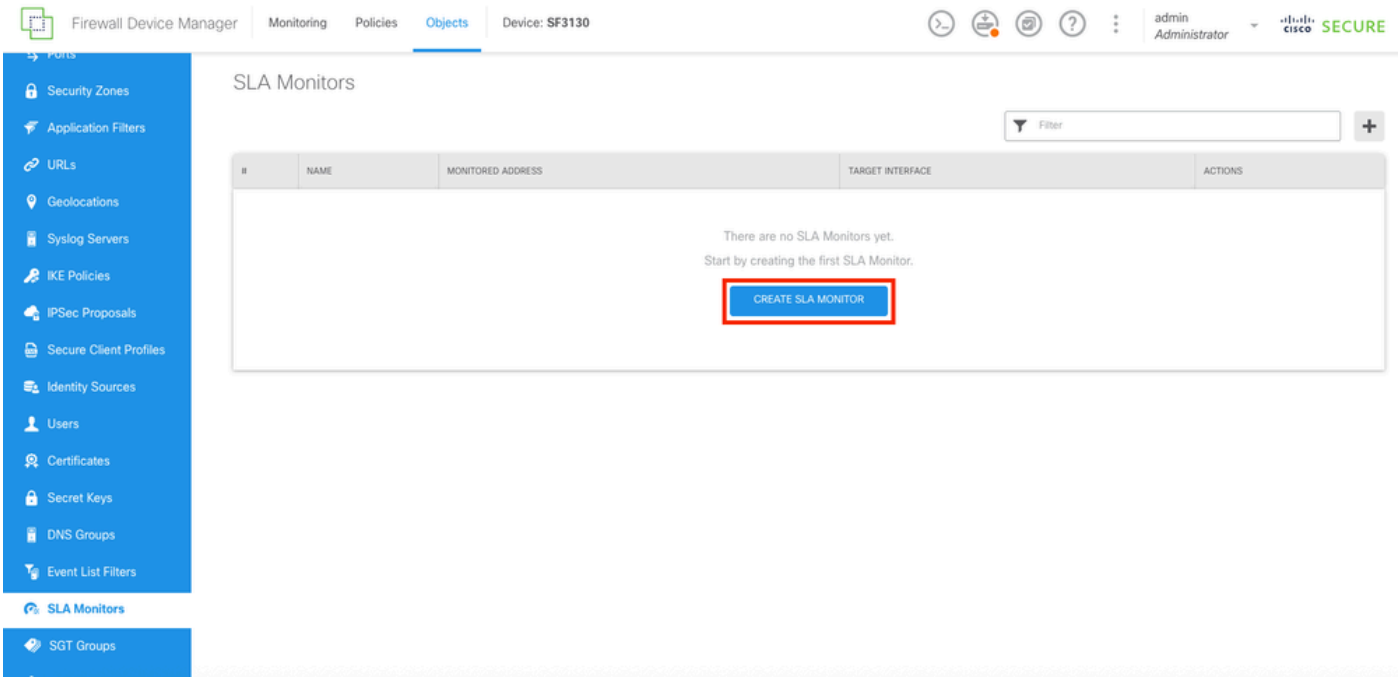
Seleccione en la columna de la izquierda el botón Monitores de SLA.



Pantalla Objetos

Paso 7.

Cree un nuevo monitor de SLA seleccionando el botón Create SLA Monitor.



Sección Supervisión de SLA

Paso 8.

Configure los parámetros para la conexión del ISP primario.

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

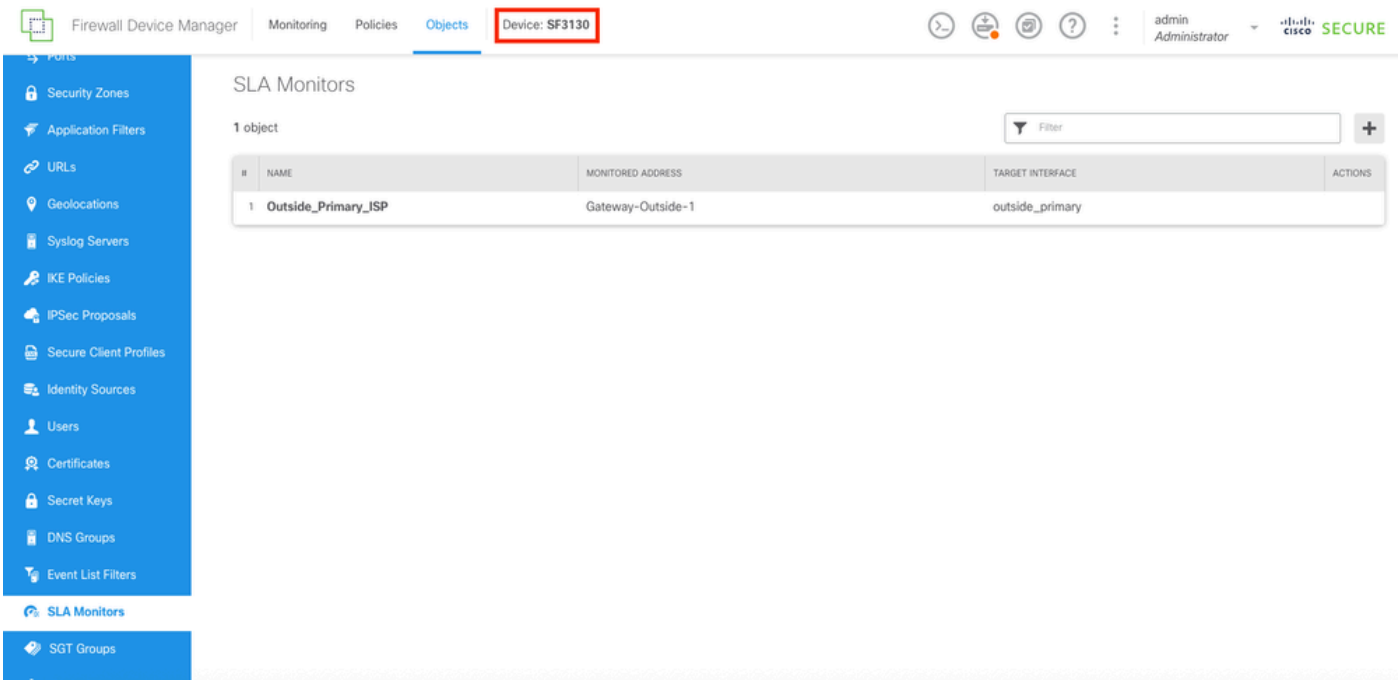
0 - 16384

CANCEL OK

Creación de objetos SLA

Paso 9.

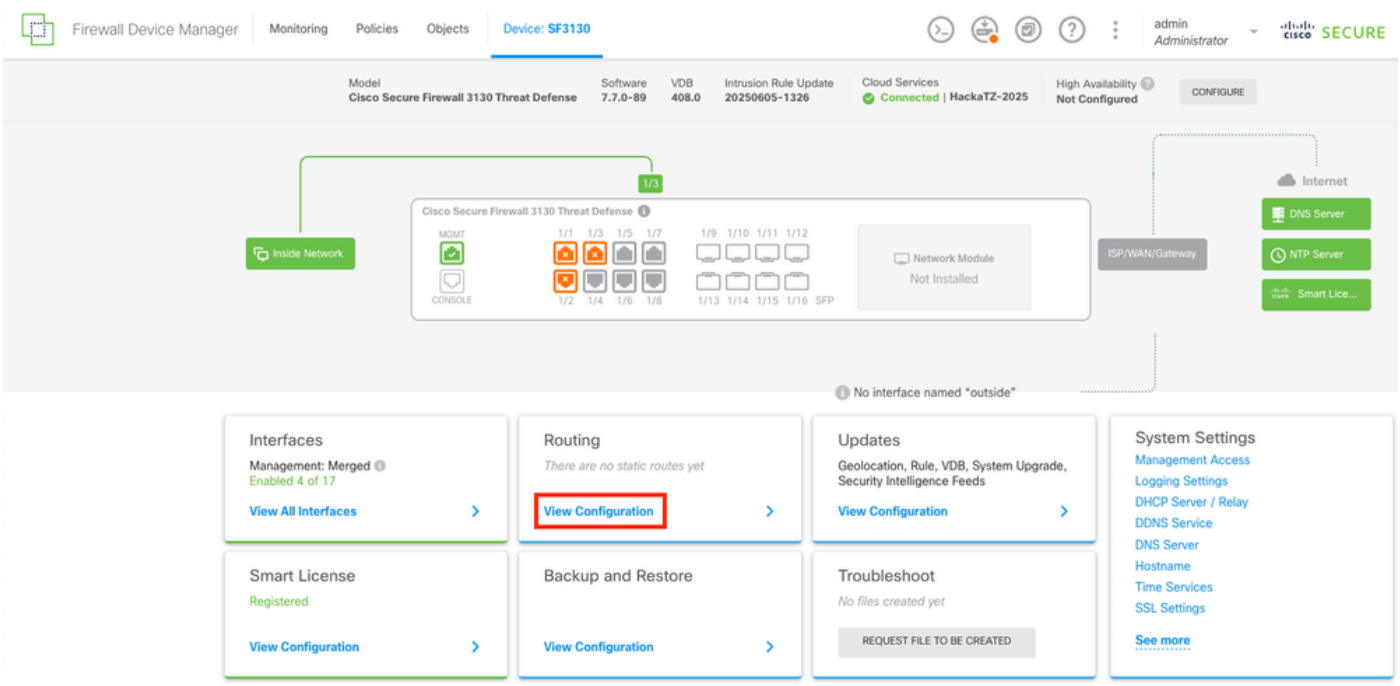
Una vez creado el objeto, la ruta estática de las interfaces debe crearlo. Vaya al panel principal seleccionando el botón Device.



Monitor de SLA creado

Paso 10.

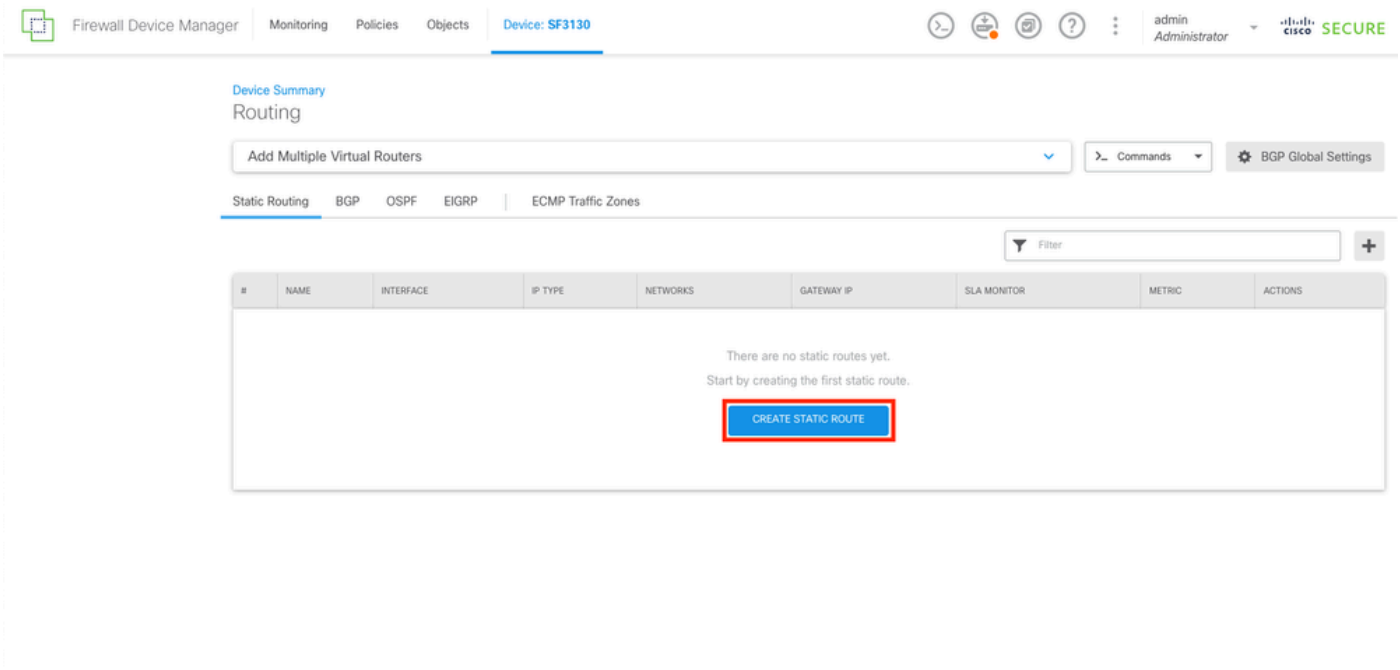
Navegue hasta la Sección de ruteo seleccionando Ver configuración en el Panel de ruteo.



Panel principal

Paso 11.

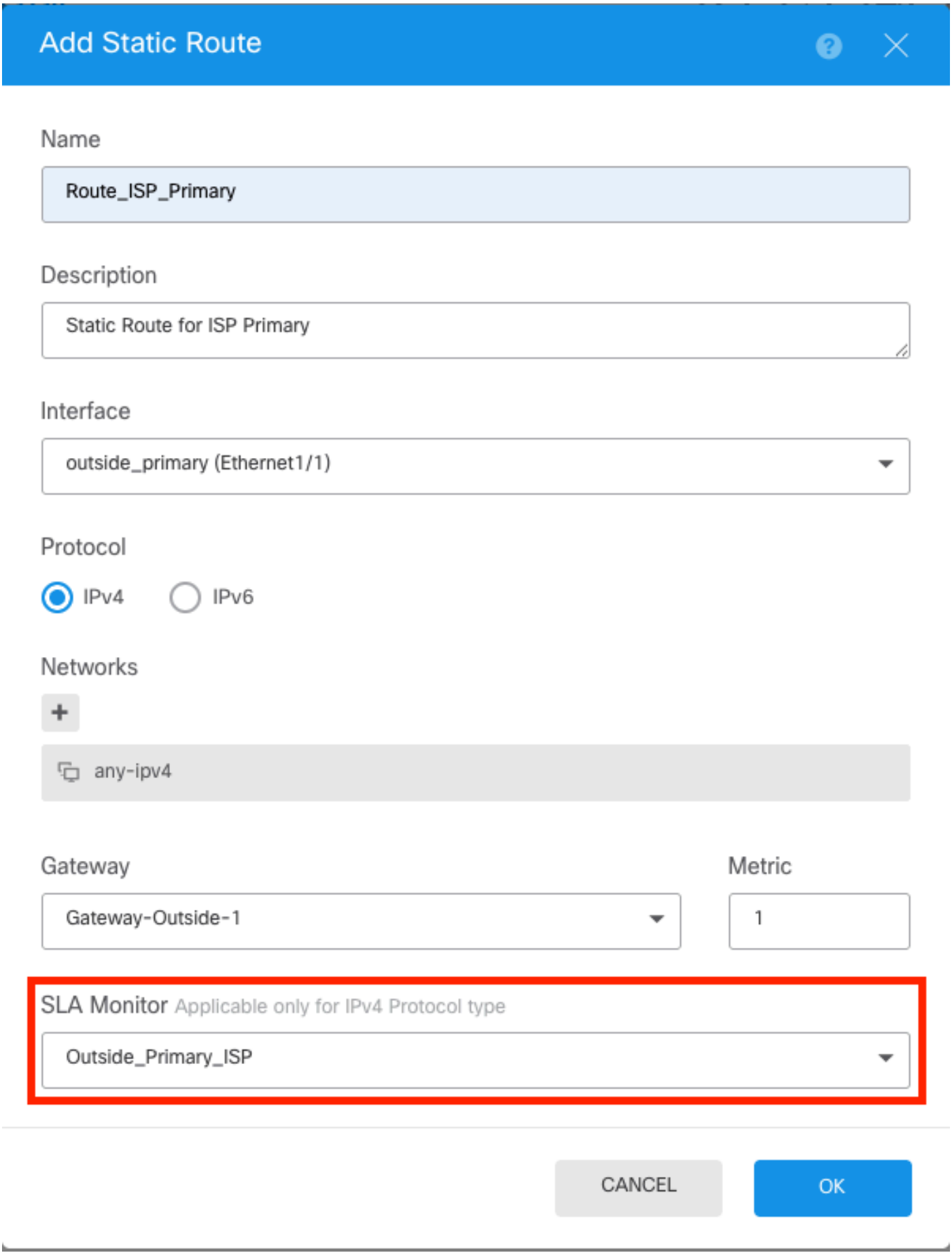
En la ficha Static Routing (Enrutamiento estático), cree las dos rutas estáticas predeterminadas para ambos ISP. Para crear una nueva ruta estática, seleccione el botón CREATE STATIC ROUTE.



Sección de Ruteo Estático

Paso 12.

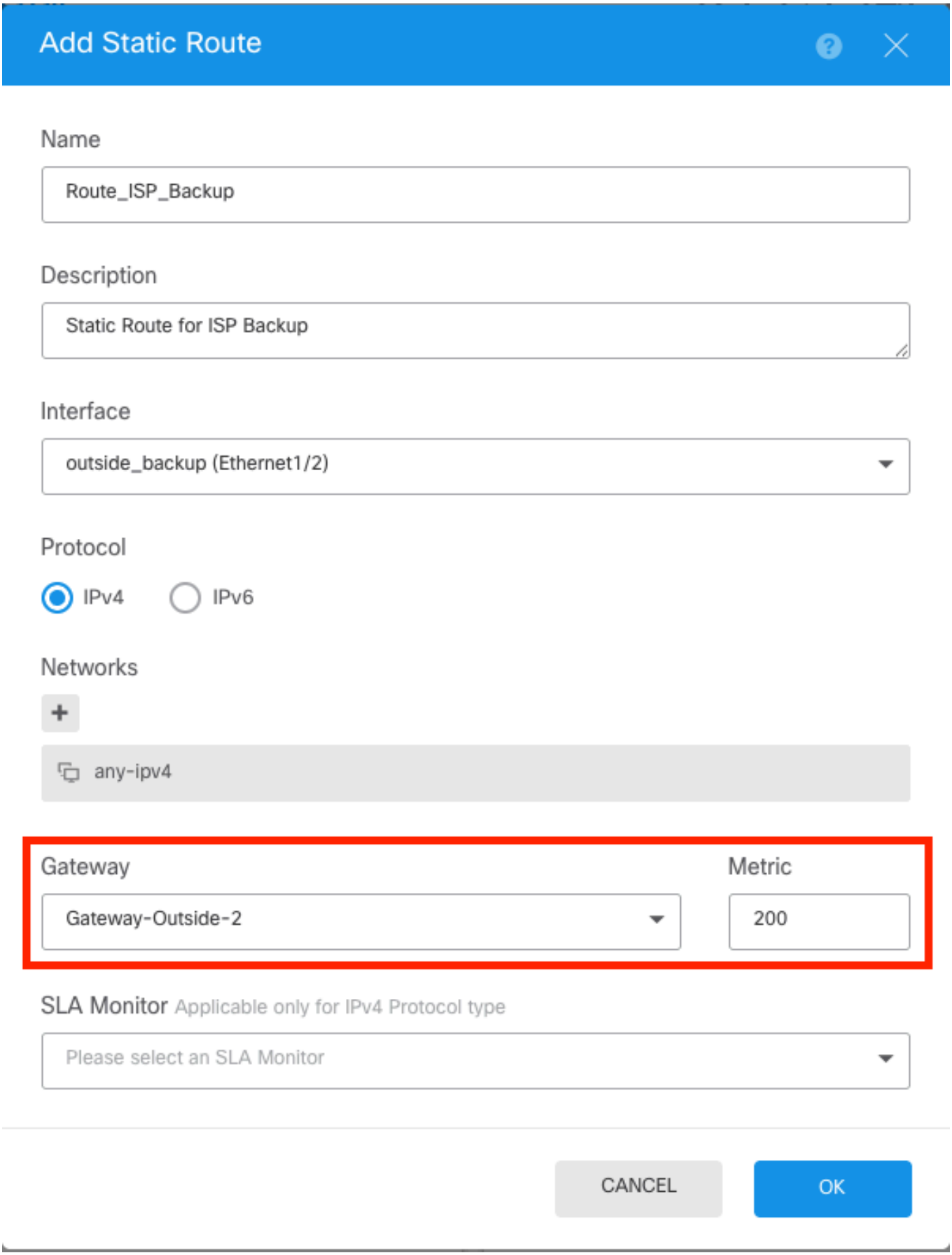
Primero, cree la ruta estática para el ISP primario. Al final, agregue el objeto de monitoreo SLA que se creó en el último paso.



Ruta estática para ISP principal

Paso 13.

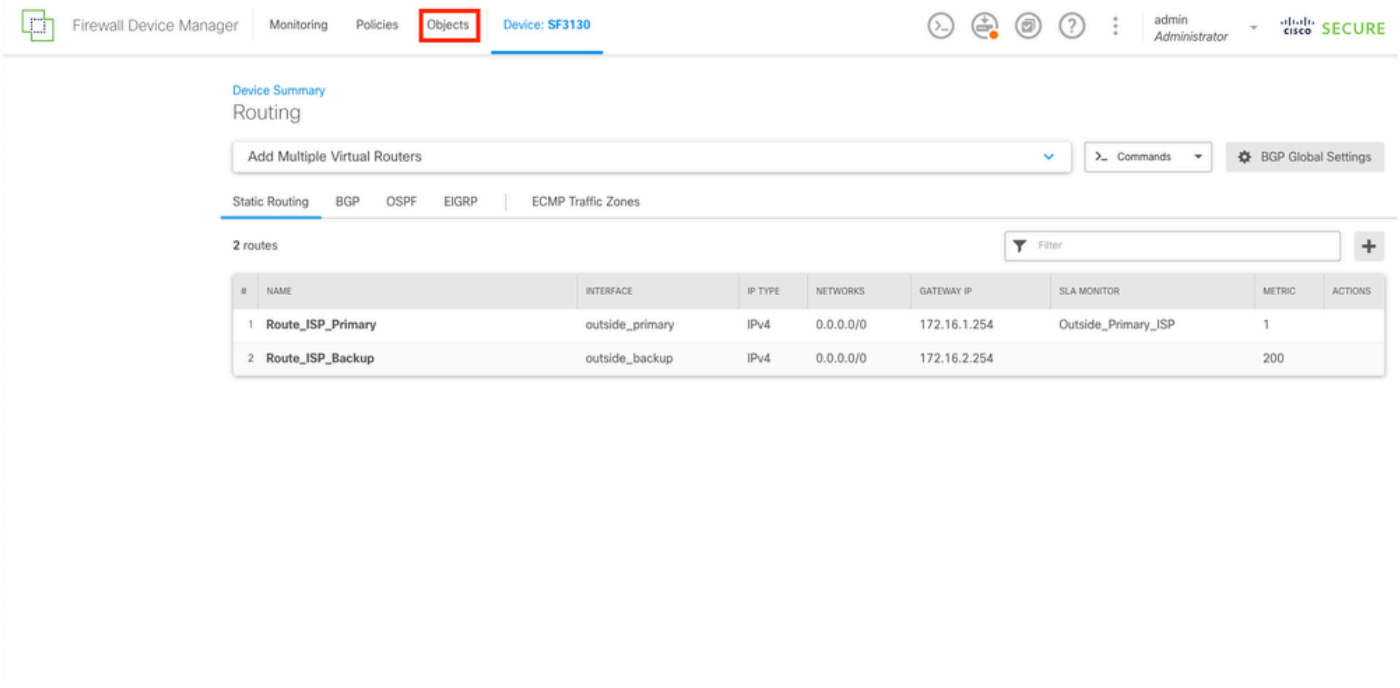
Repita el último paso y cree una ruta predeterminada, para el ISP secundario con el gateway adecuado y una métrica diferente. En este ejemplo, se aumentó a 200.



Ruta estática para ISP secundario

Paso 14.

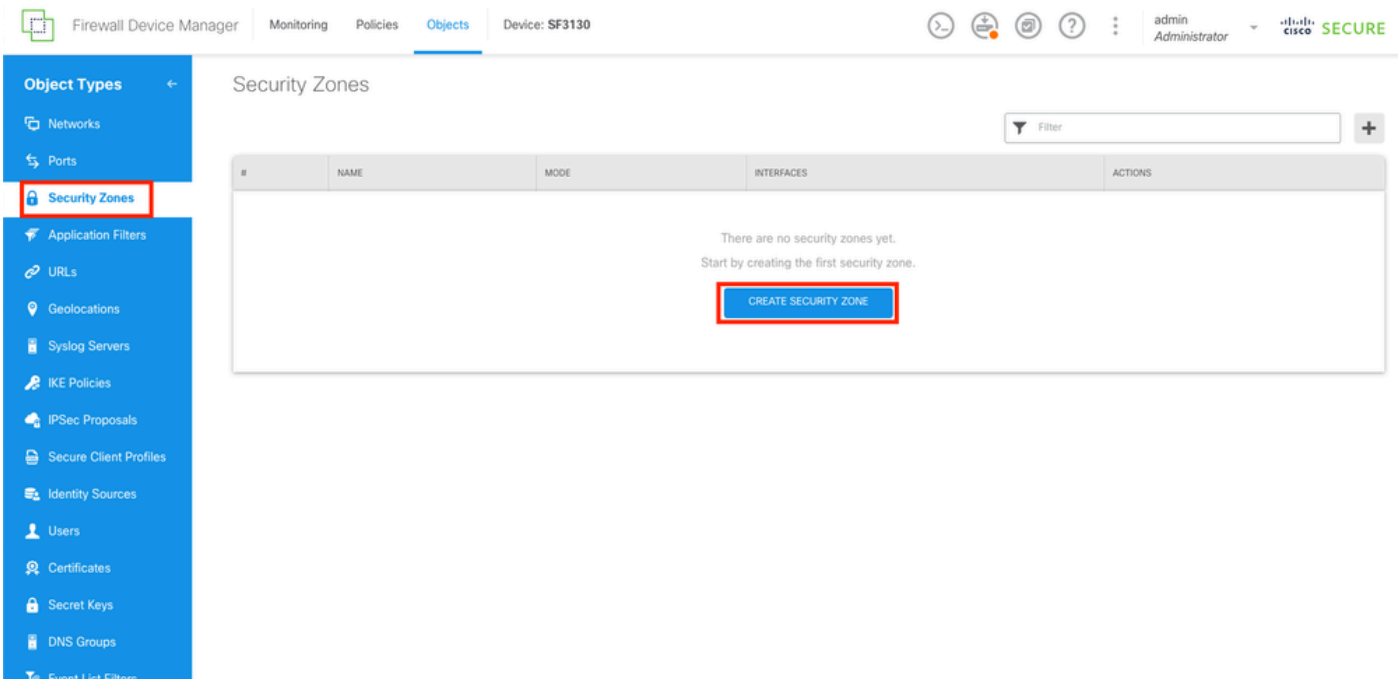
Una vez creadas ambas rutas estáticas, debe crearse una zona de seguridad. Navegue hasta la sección Objetos seleccionando el botón Objetos en la parte superior.



Rutas estáticas creadas

Paso 15.

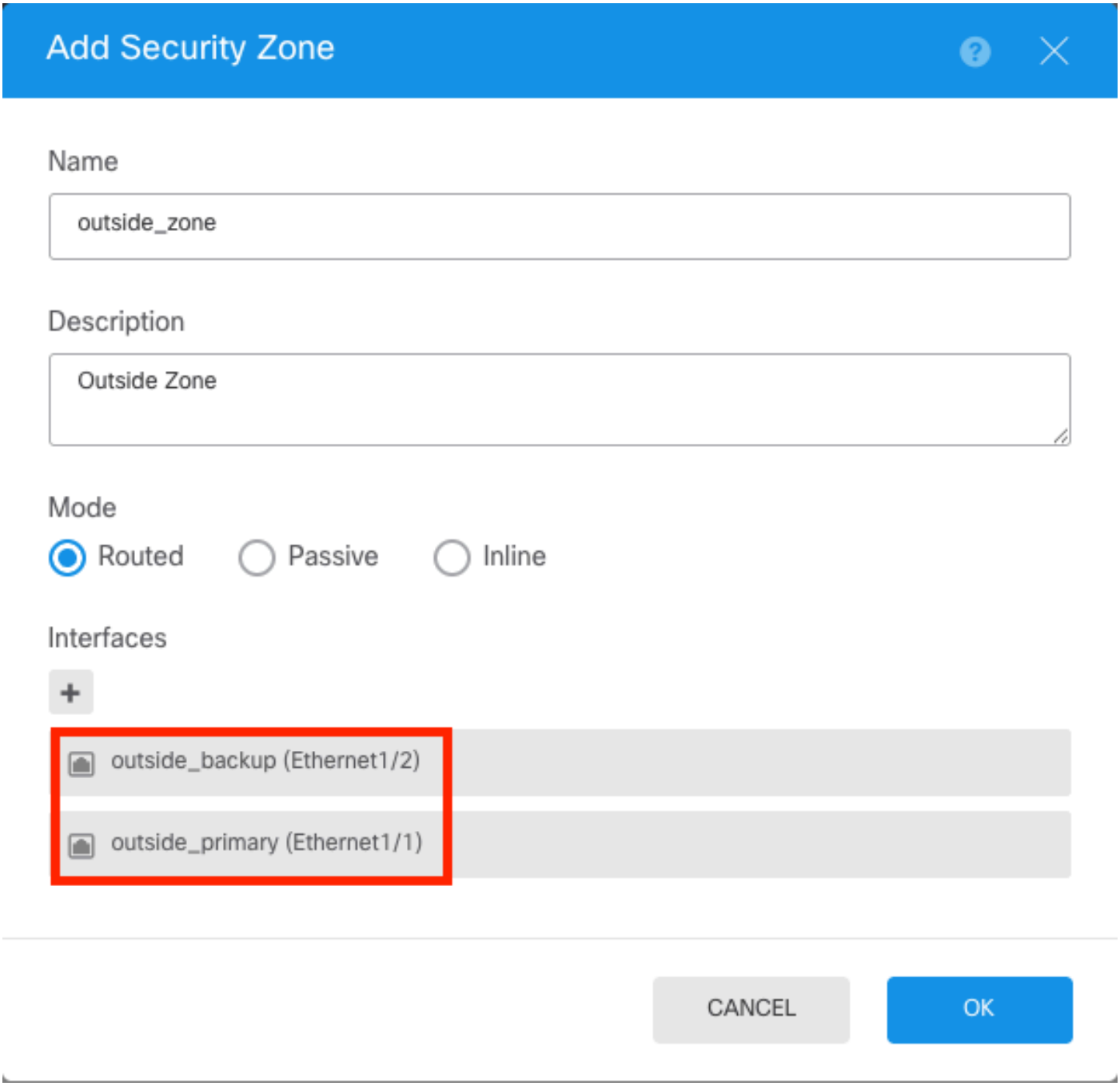
Navegue hasta la sección Zonas de seguridad seleccionando en la columna izquierda el botón Zonas de seguridad, y luego cree una nueva zona seleccionando el botón CREATE SECURITY ZONE.



Sección Zonas de Seguridad

Paso 16.

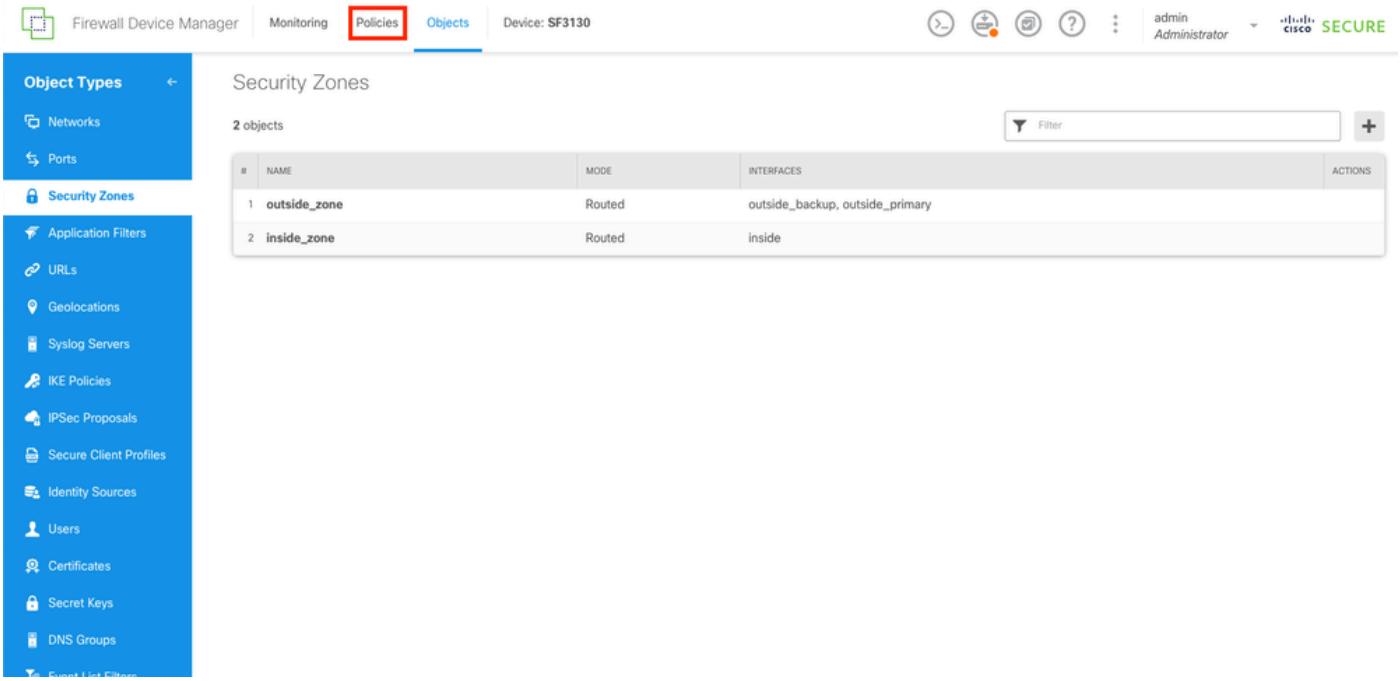
Cree la Zona de seguridad externa con las dos interfaces externas para las conexiones de los ISP.



Zona de seguridad externa

Paso 17.

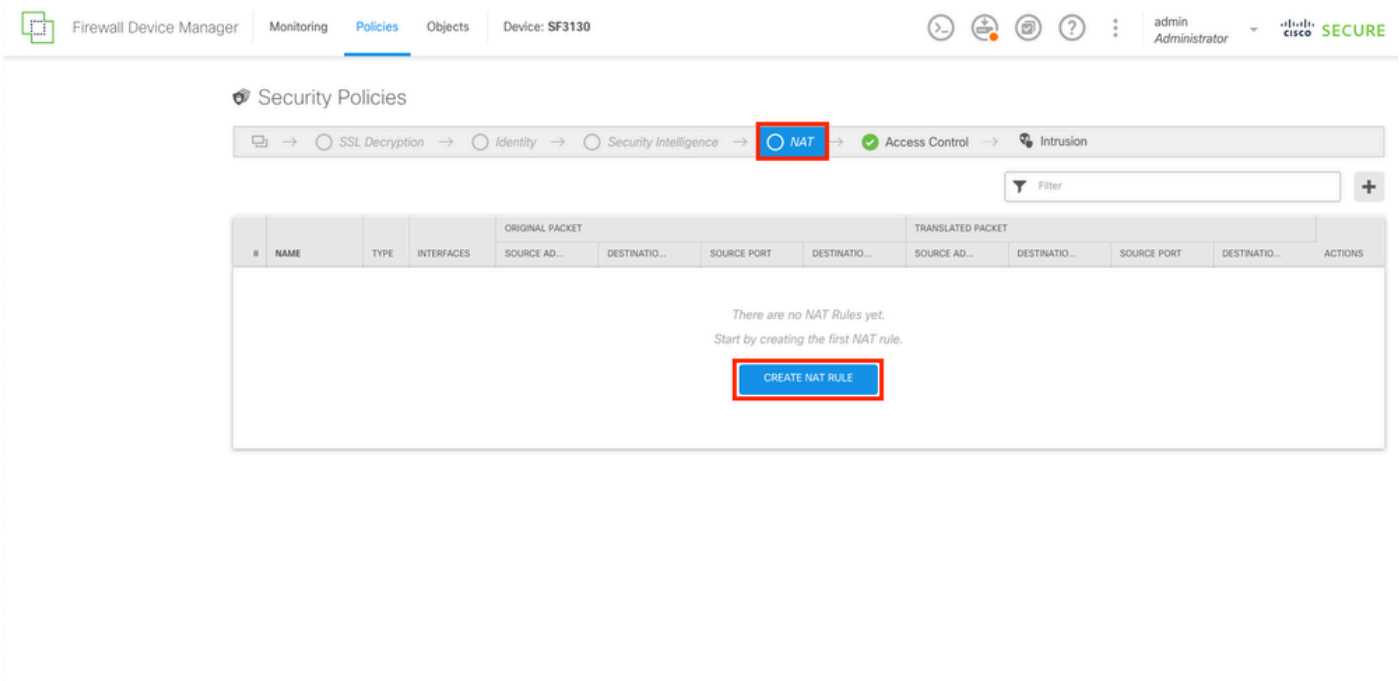
Una vez creada la zona de seguridad, debe crearse una NAT. Vaya a la sección Políticas seleccionando el botón Políticas en la parte superior.



Zonas de seguridad creadas

Paso 18.

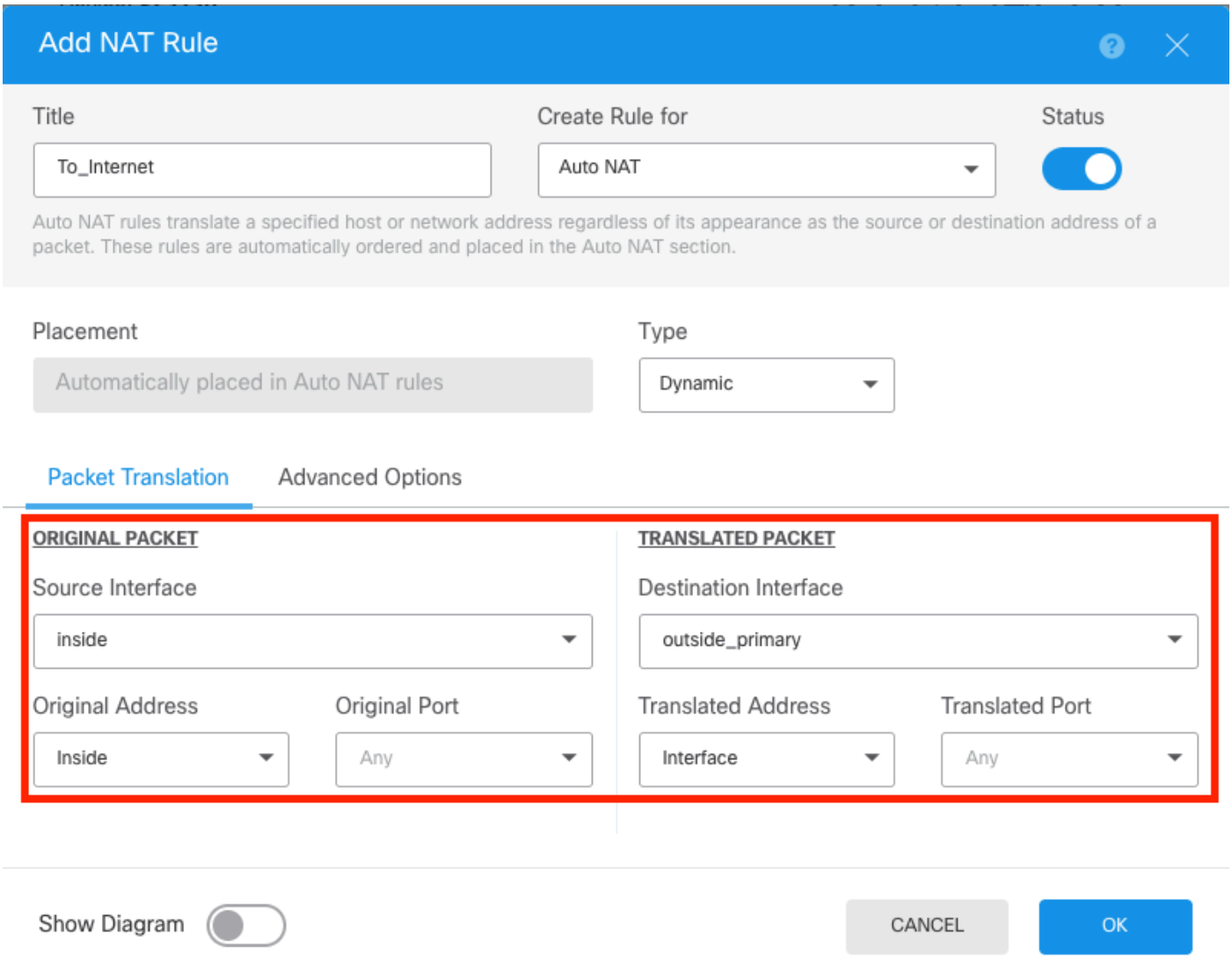
Navegue hasta la sección NAT seleccionando el botón NAT, y luego cree una nueva regla seleccionando el botón CREATE NAT RULE.



Sección NAT

Paso 19.

Para la conmutación por fallas del ISP, la configuración debe tener 2 rutas a través de interfaces externas. En primer lugar, para la conexión de la interfaz externa principal al ISP principal.

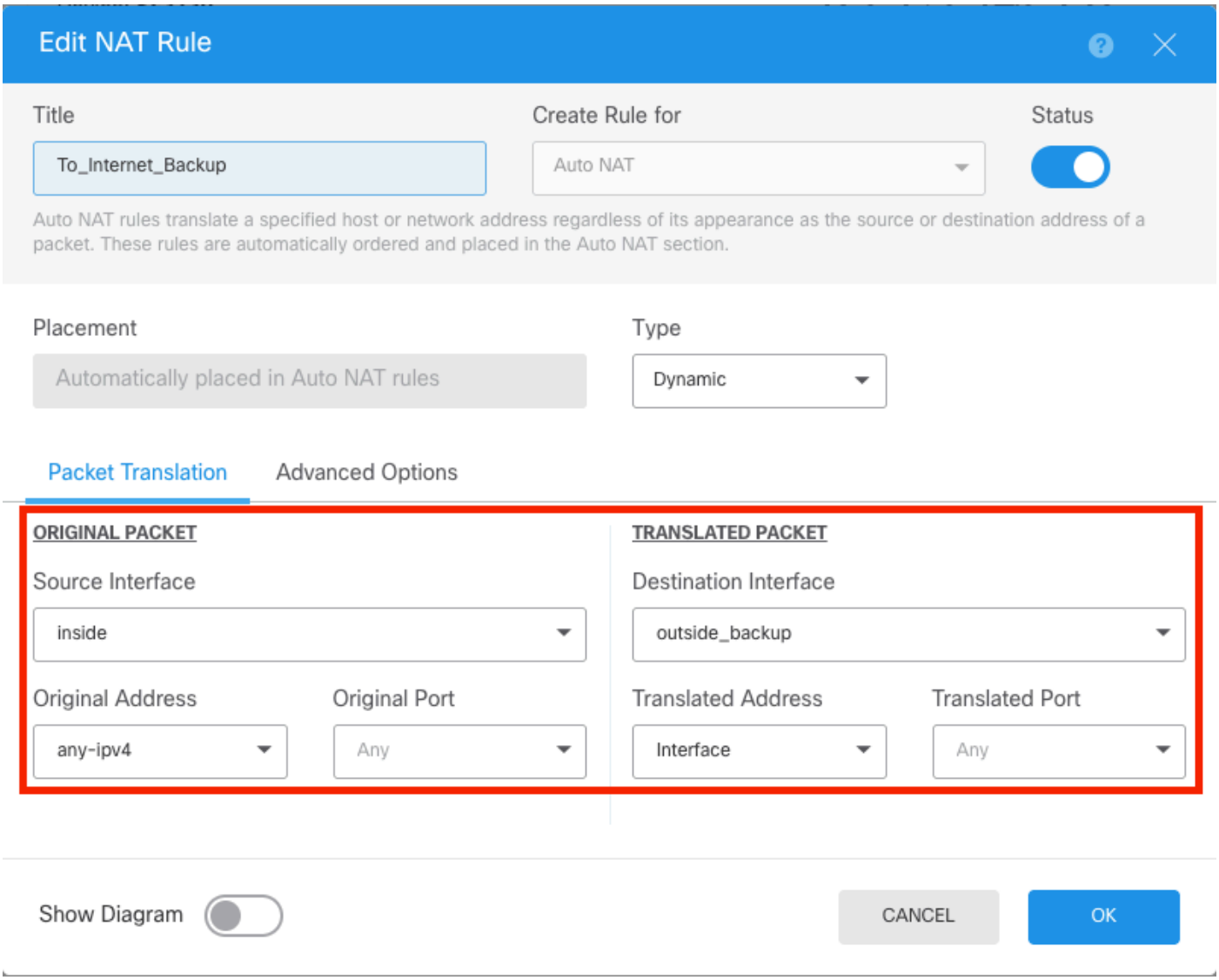


NAT para ISP principal

Paso 20.

Ahora, una segunda NAT para la conexión del ISP secundario.

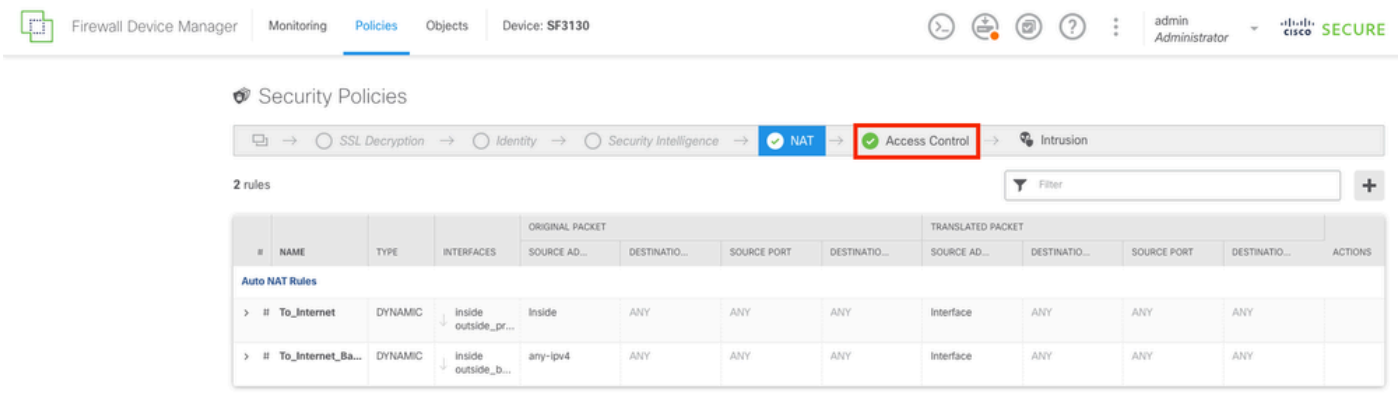
Nota: No se puede utilizar la misma red para la dirección original. En este ejemplo, para el ISP secundario, la dirección original es el objeto any-ipv4.



NAT para ISP secundario

Paso 21.

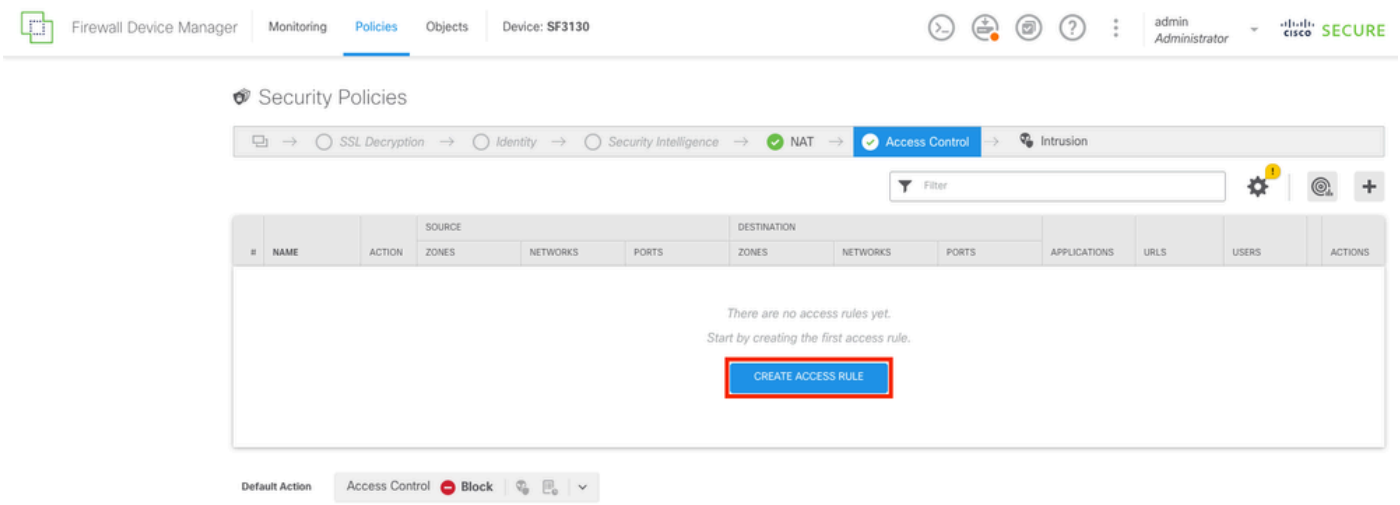
Después de crear ambas reglas NAT, se debe establecer una regla de control de acceso para permitir el tráfico saliente. Seleccione el botón Control de acceso.



Reglas NAT creadas

Paso 22.

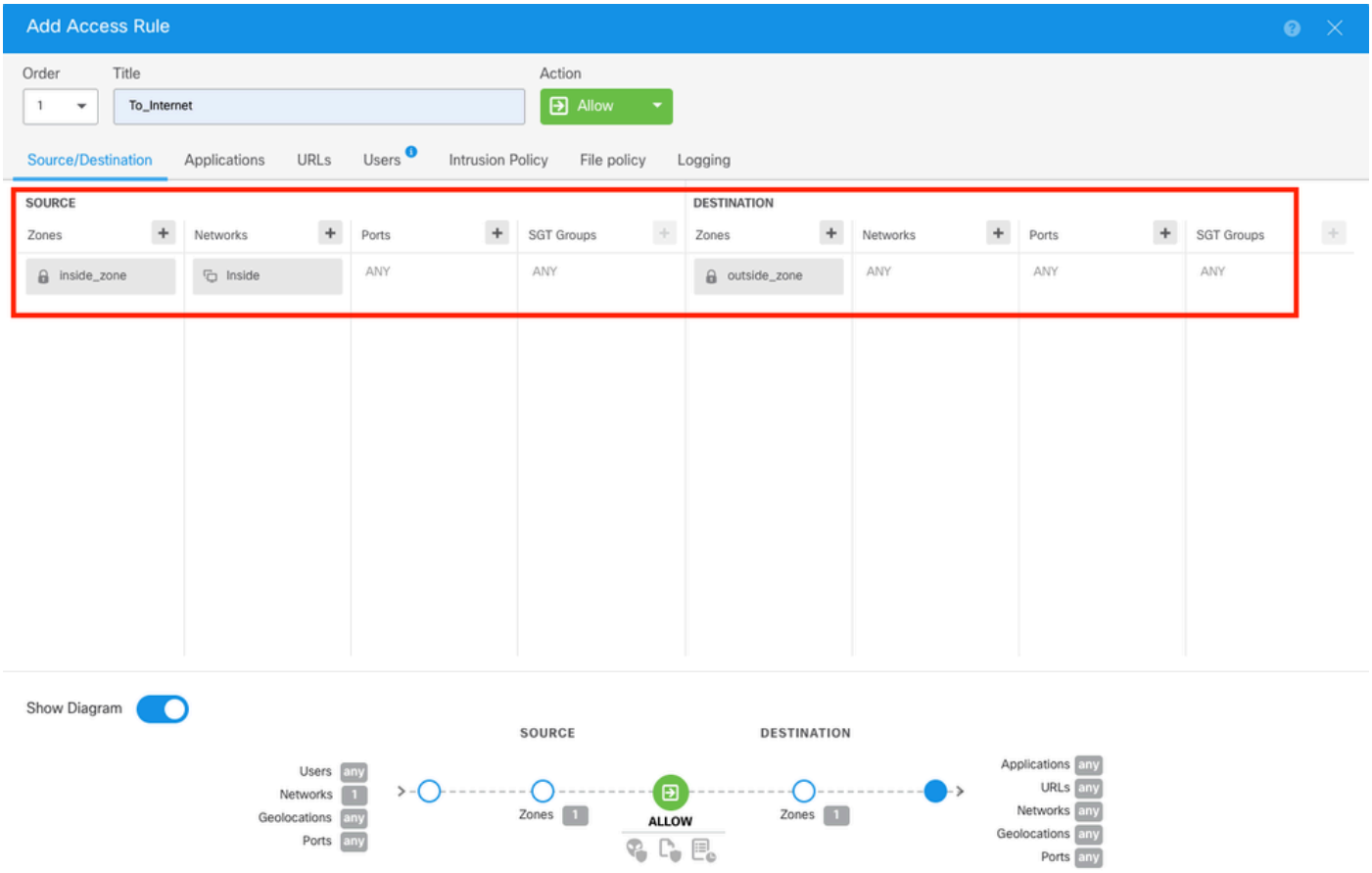
Para crear la regla de control de acceso, seleccione el botón CREATE ACCESS RULE.



Sección de control de acceso

Paso 23.

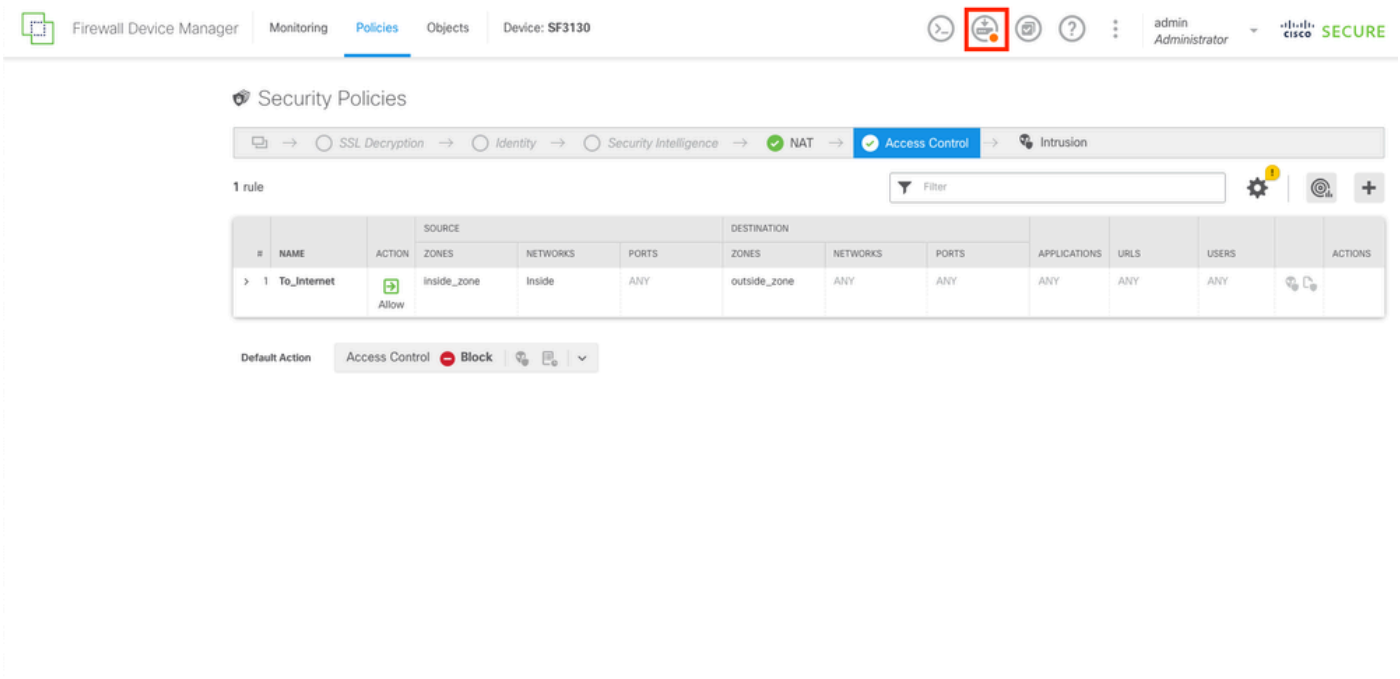
Seleccione las zonas y redes deseadas.



Regla de control de acceso

Paso 24.

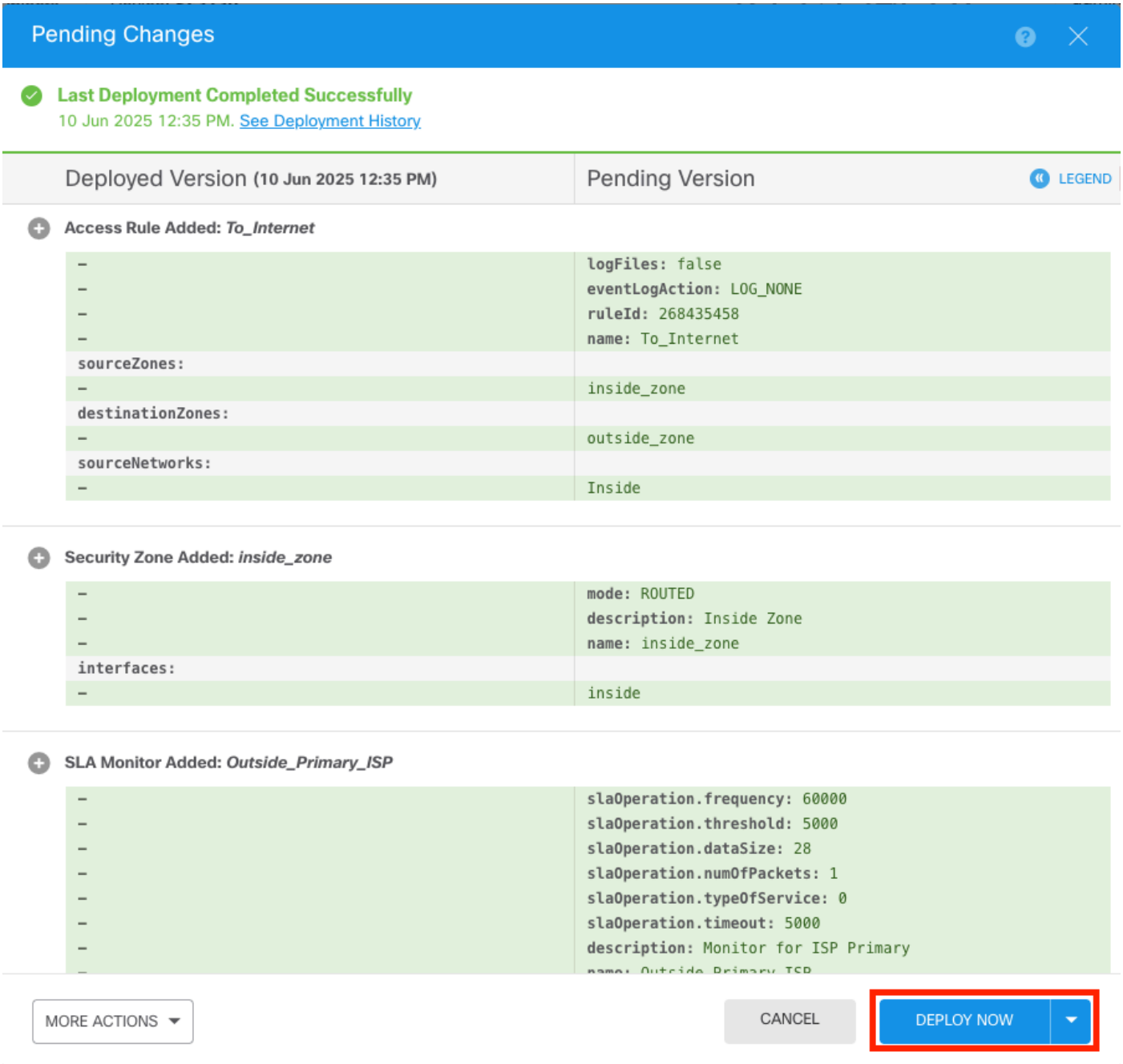
Una vez creada la regla de control de acceso, continúe con la implementación de todos los cambios seleccionando el botón Deploy en la parte superior.



Regla de control de acceso creada

Paso 25.

Verifique los cambios y, a continuación, seleccione el botón Deploy Now.



Verificación de implementación

Diagrama de la red

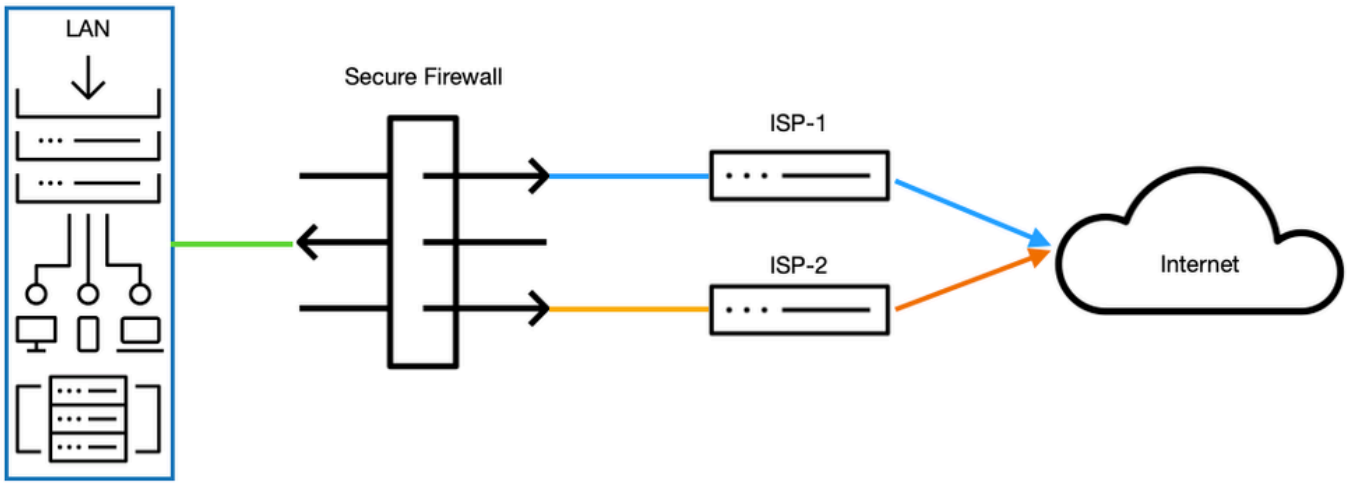


Diagrama de la red

Verificación

<#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
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).