Configuración de ECMP con IP SLA en FTD gestionado por FDM

Contenido

Introducción

Este documento describe cómo configurar ECMP junto con IP SLA en un FTD administrado por FDM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de ECMP en Cisco Secure Firewall Threat Defence (FTD)
- Configuración de SLA de IP en Cisco Secure Firewall Threat Defence (FTD)
- Cisco Secure Firewall Device Manager (FDM)

Componentes Utilizados

La información de este documento se basa en esta versión de software y hardware:

- Cisco FTD versión 7.4.1 (Compilación 172)

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.

Antecedentes

Este documento describe cómo configurar Equal-Cost Multi-Path (ECMP) junto con el Acuerdo de nivel de servicio de protocolo de Internet (IP SLA) en un FTD de Cisco gestionado por Cisco FDM. ECMP permite agrupar interfaces en FTD y equilibrar la carga del tráfico a través de varias interfaces. IP SLA es un mecanismo que supervisa la conectividad de extremo a extremo mediante el intercambio de paquetes regulares. Junto con ECMP, se puede implementar IP SLA para garantizar la disponibilidad del salto siguiente. En este ejemplo, ECMP se utiliza para distribuir paquetes de forma equitativa a través de dos circuitos de proveedor de servicios de Internet (ISP). Al mismo tiempo, un SLA de IP realiza un seguimiento de la conectividad, lo que garantiza una transición fluida a cualquier circuito disponible en caso de fallo.

Los requisitos específicos para este documento incluyen:

- Acceso a los dispositivos con una cuenta de usuario con privilegios de administrador
- Cisco Secure Firewall Threat Defence versión 7.1 o superior

Configurar

Diagrama de la red

En este ejemplo, Cisco FTD tiene dos interfaces externas: outside1 y outside2 . Cada uno se conecta a una gateway ISP, outside1 y outside2 pertenece a la misma zona ECMP denominada outside.

El tráfico de la red interna se rutea a través de FTD y se equilibra la carga a Internet a través de los dos ISP.

Al mismo tiempo, FTD utiliza IP SLAs para monitorear la conectividad a cada gateway ISP. En caso de fallo en cualquiera de los circuitos del ISP, el FTD conmuta por error al otro gateway del ISP para mantener la continuidad empresarial.

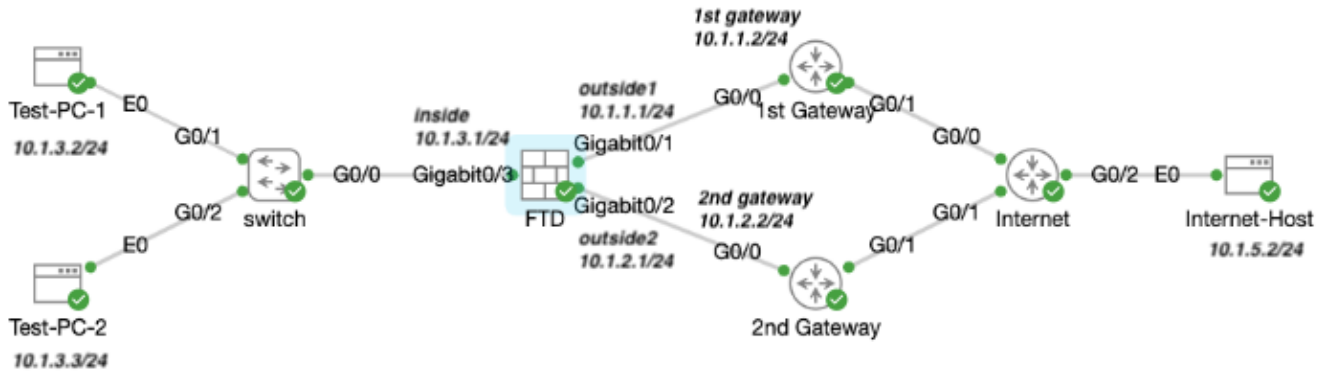
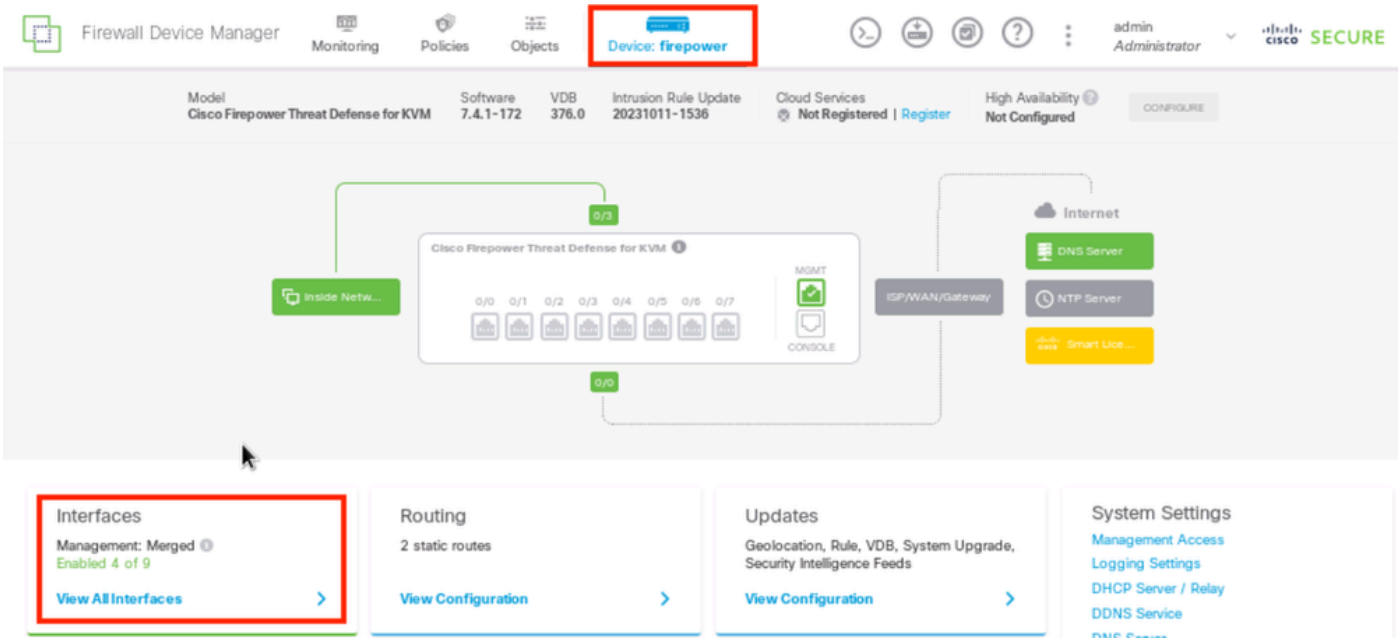


Diagrama de la red

Configuraciones

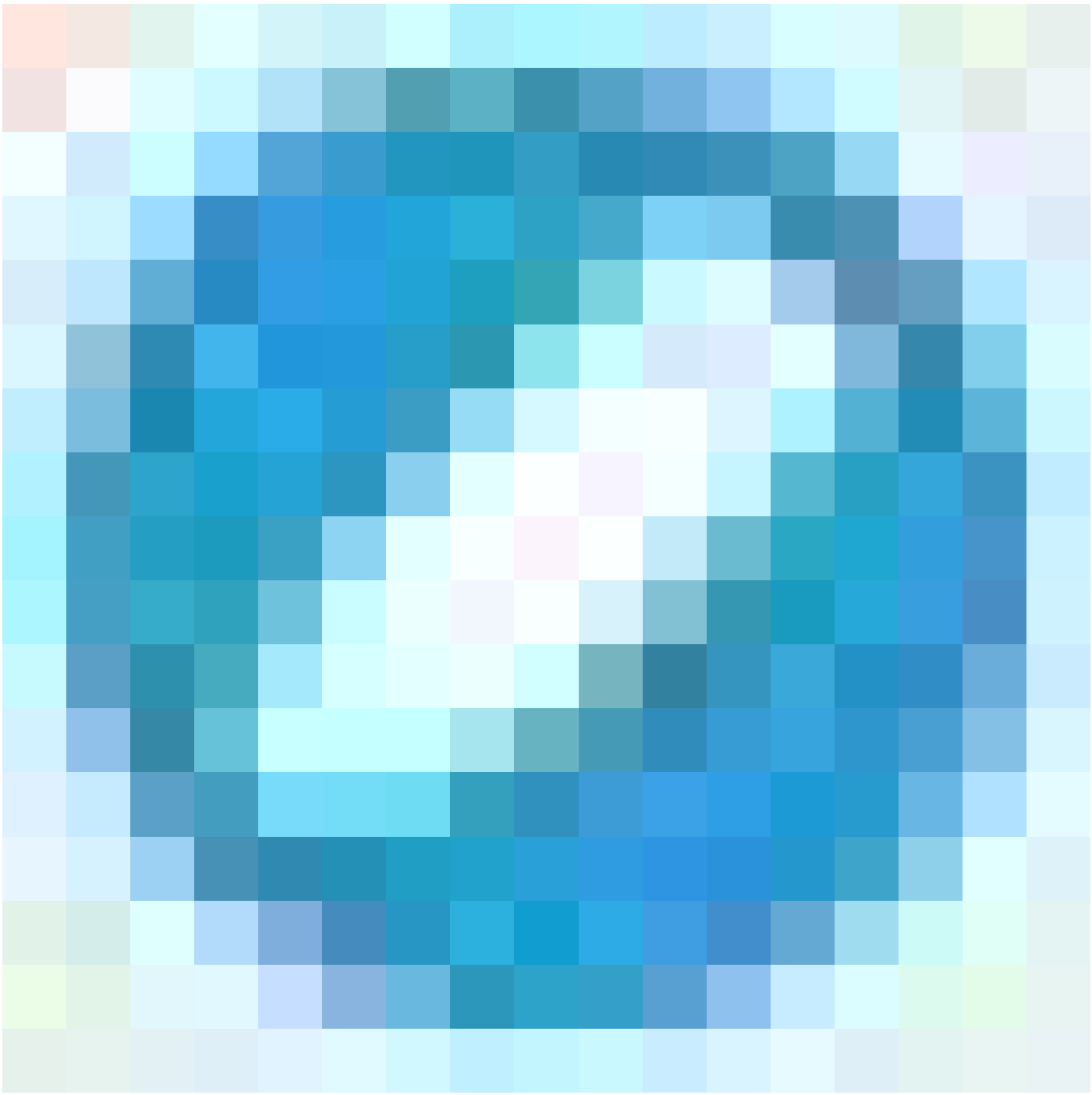
Paso 0. Preconfigurar interfaces/objetos

Inicie sesión en la GUI web de FDM, haga clic en Device y, a continuación, haga clic en el enlace del resumen Interfaces. La lista Interfaces muestra las interfaces disponibles, sus nombres, direcciones y estados.

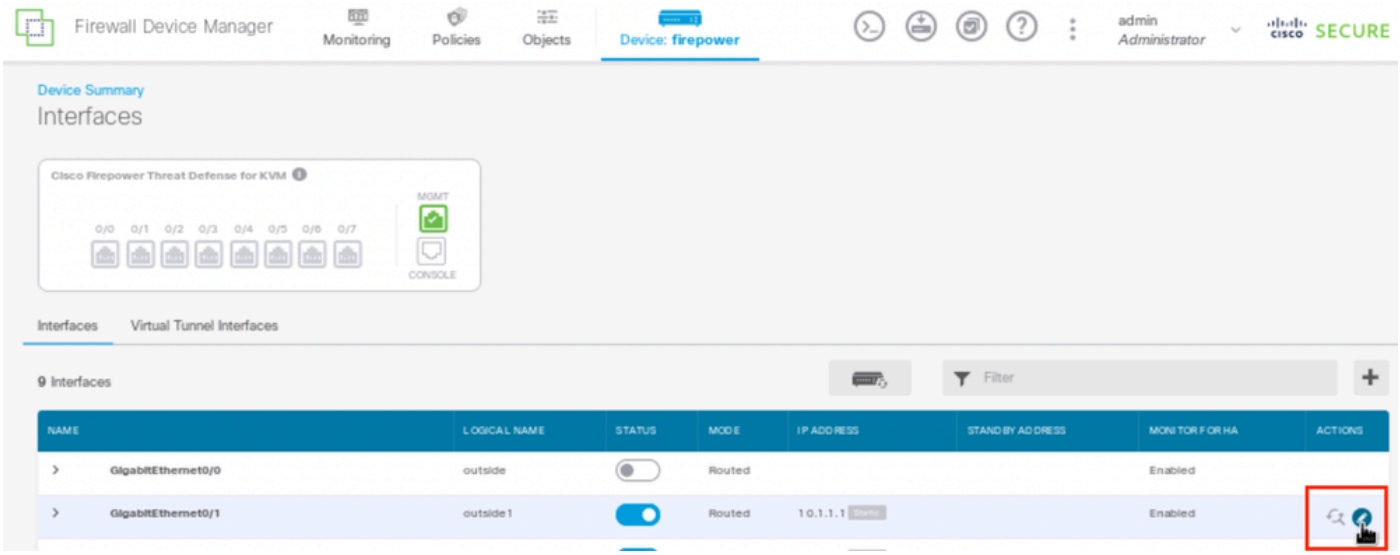


Interfaz de dispositivo FDM

Haga clic en el icono de edición (



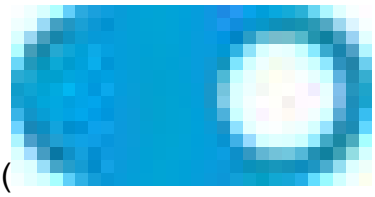
) de la interfaz física que desea editar. En este ejemplo GigabitEthernet0/1.



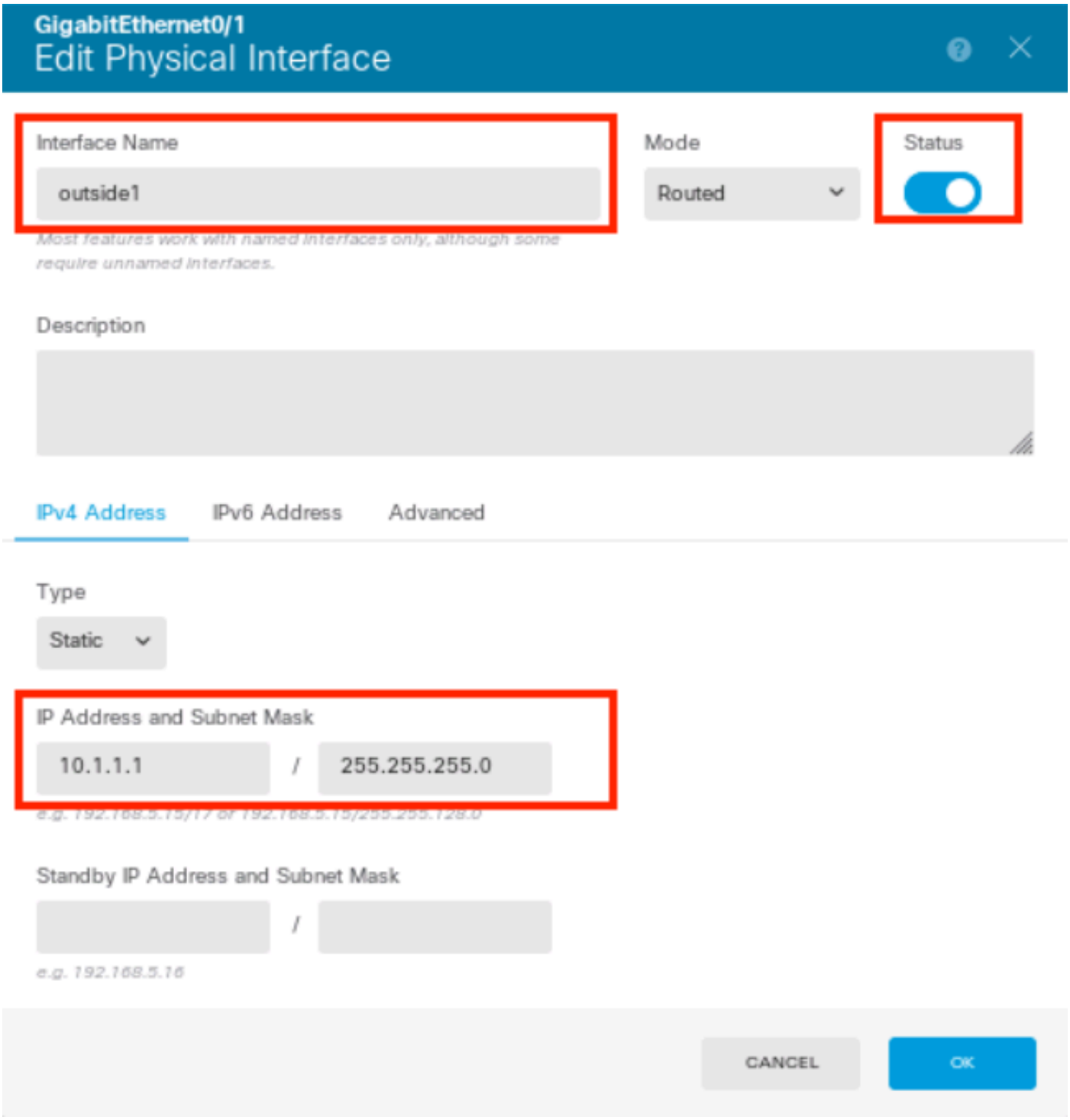
Paso 0 Interfaz Gi0/1

En la ventana Edit Physical Interface:

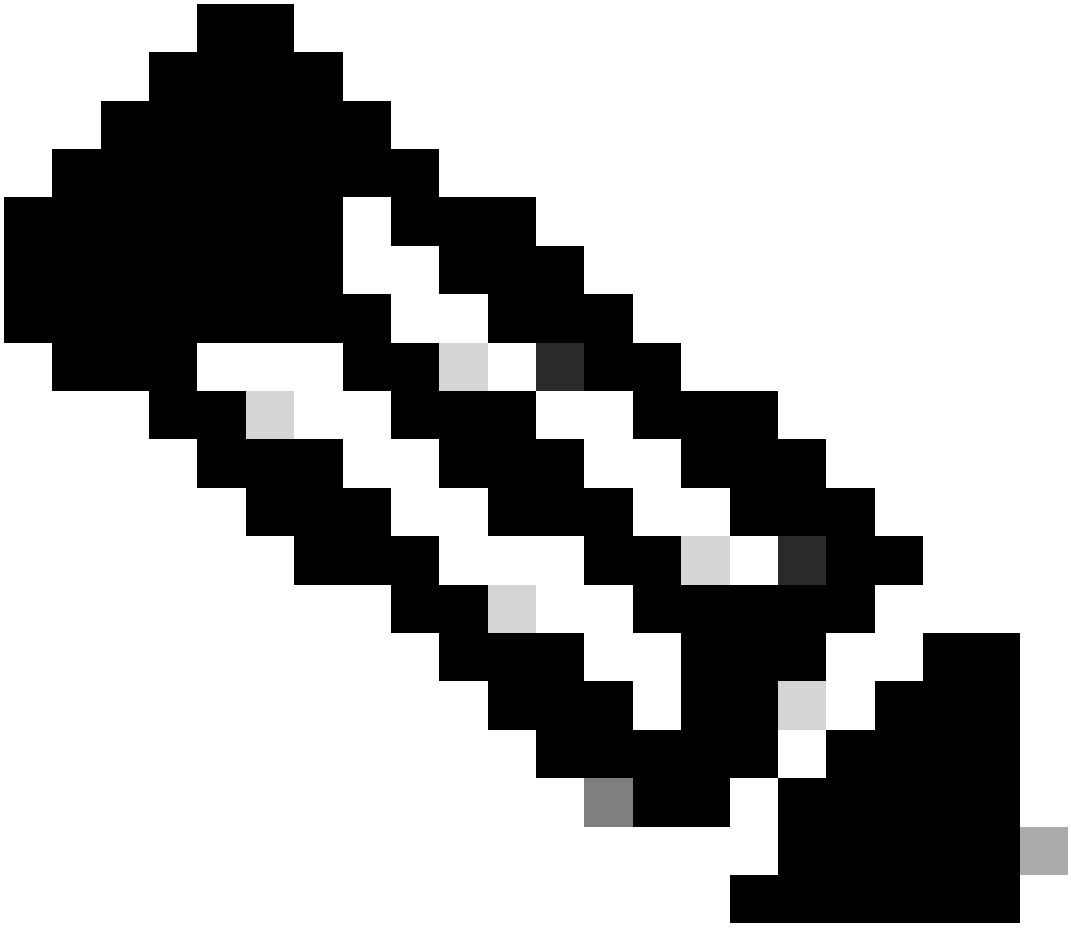
1. Establezca el Nombre de interfaz , en este caso outside1 .



2. Establezca el control deslizante Estado en el parámetro habilitado ( ).
3. Haga clic en la ficha IPv4 Address y configure la dirección IPv4, en este caso 10.1.1.1/24.
4. Click OK.

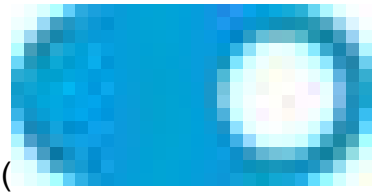


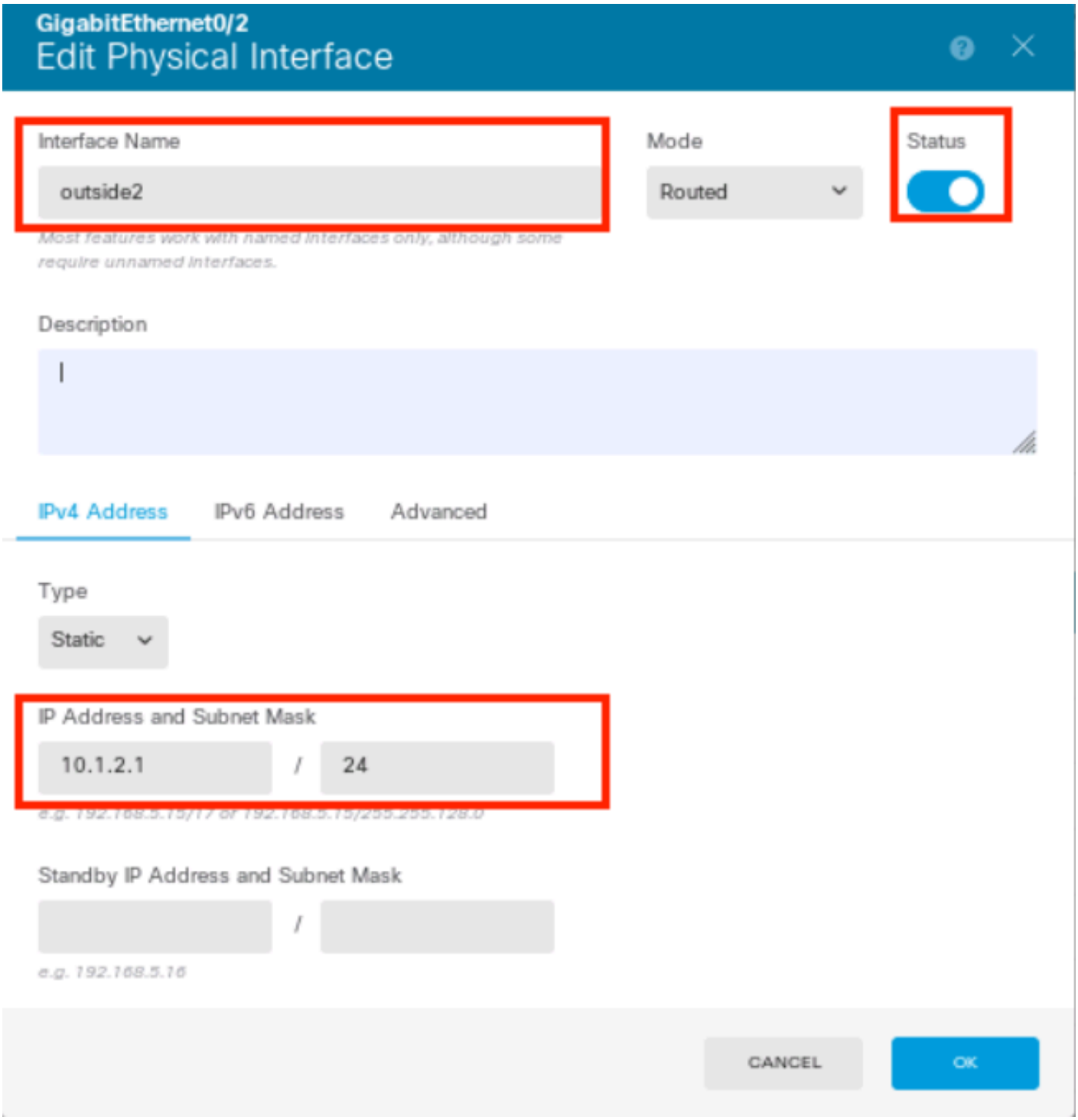
Paso 0 Editar Interfaz Gi0/1



Nota: Sólo las interfaces enrutadas se pueden asociar a una zona ECMP.

Repita los pasos similares para configurar la interfaz para la conexión del ISP secundario, en este ejemplo la interfaz física es GigabitEthernet0/2 . En la ventana Edit Physical Interface:

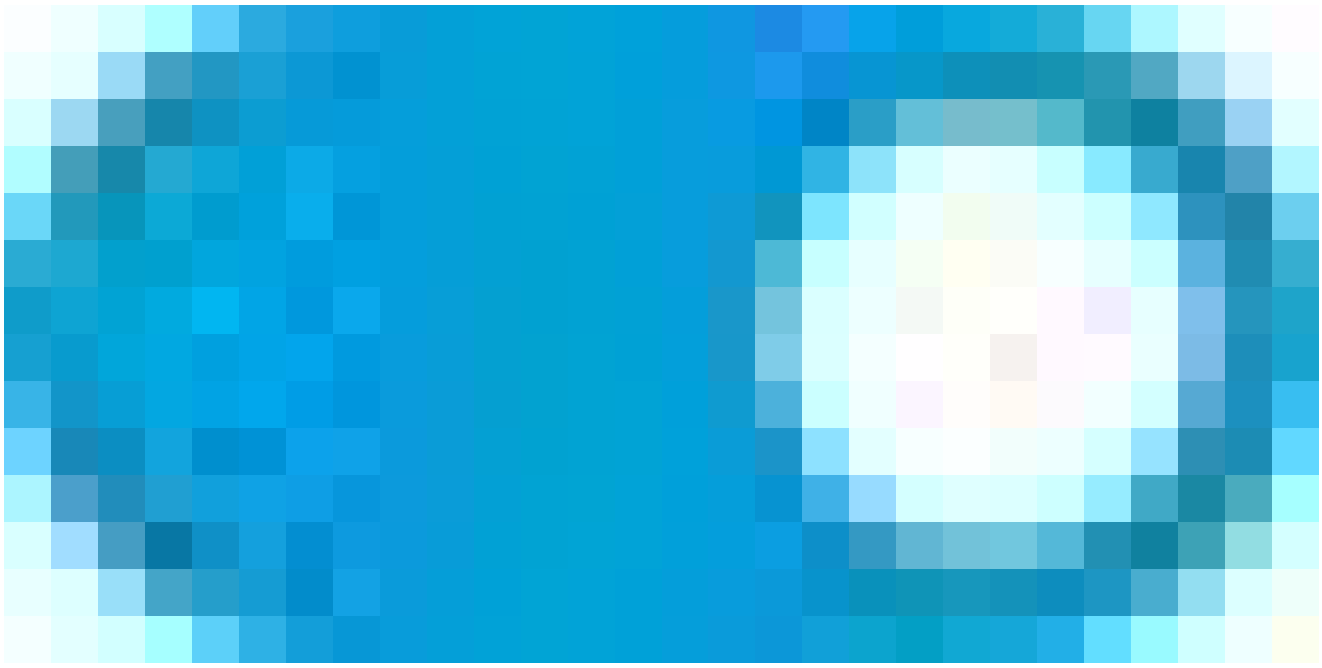
1. Establezca el Nombre de interfaz , en este caso outside2.
2. Establezca el control deslizante Estado en el parámetro habilitado ().
3. Haga clic en la pestaña IPv4 Address y configure la dirección IPv4, en este caso 10.1.2.1/24.
4. Click OK.



Paso 0 Editar Interfaz Gi0/2

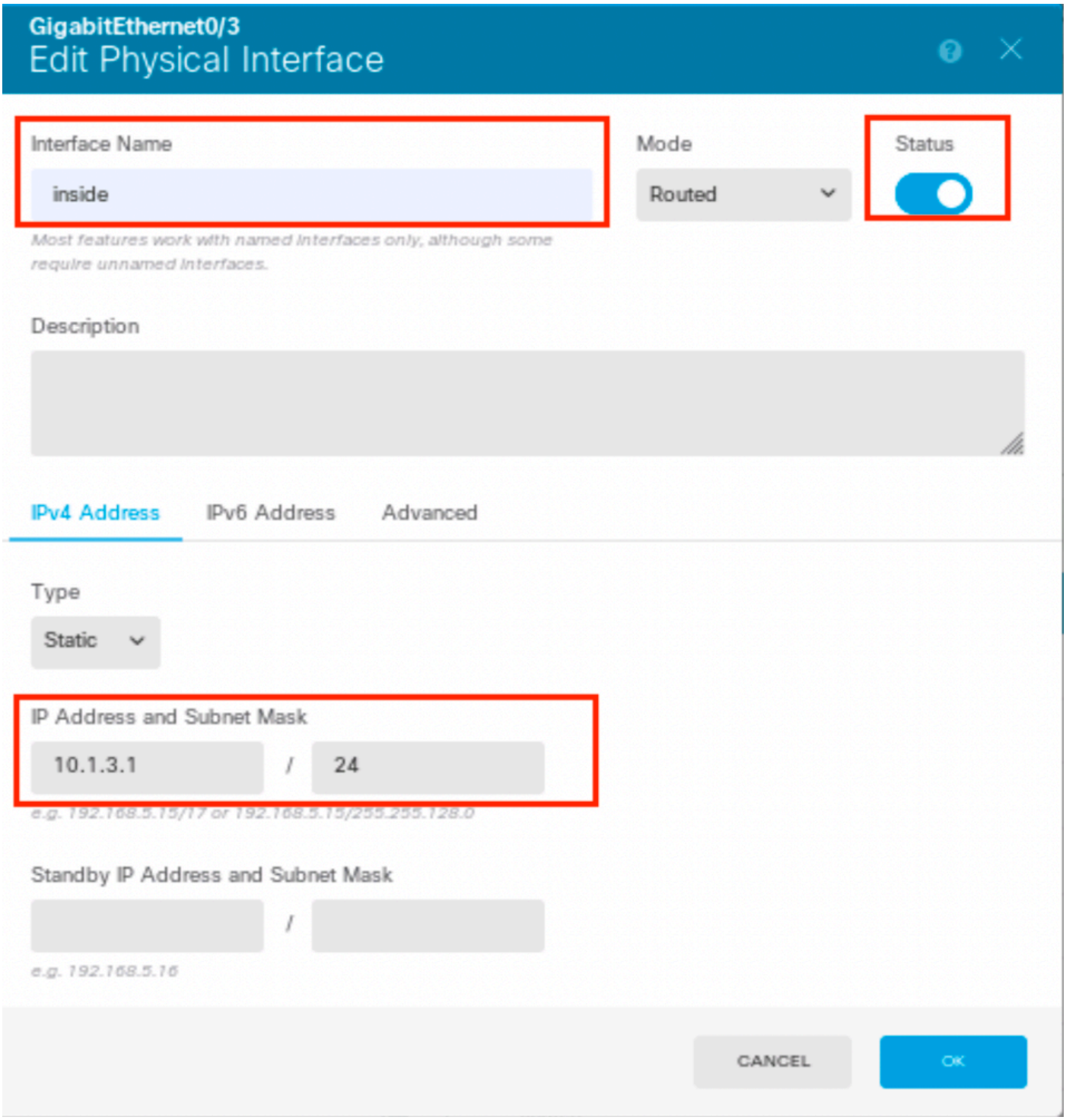
Repita los pasos similares para configurar la interfaz para la conexión interna; en este ejemplo, la interfaz física es GigabitEthernet0/3. En la ventana Edit Physical Interface:

1. Establezca el Nombre de la interfaz , en este caso dentro .
2. Establezca el control deslizante Estado en el parámetro habilitado (

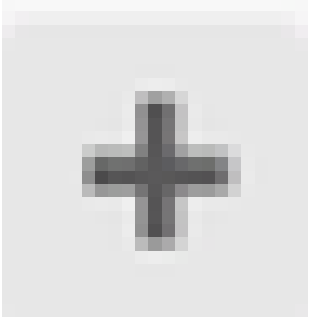


).

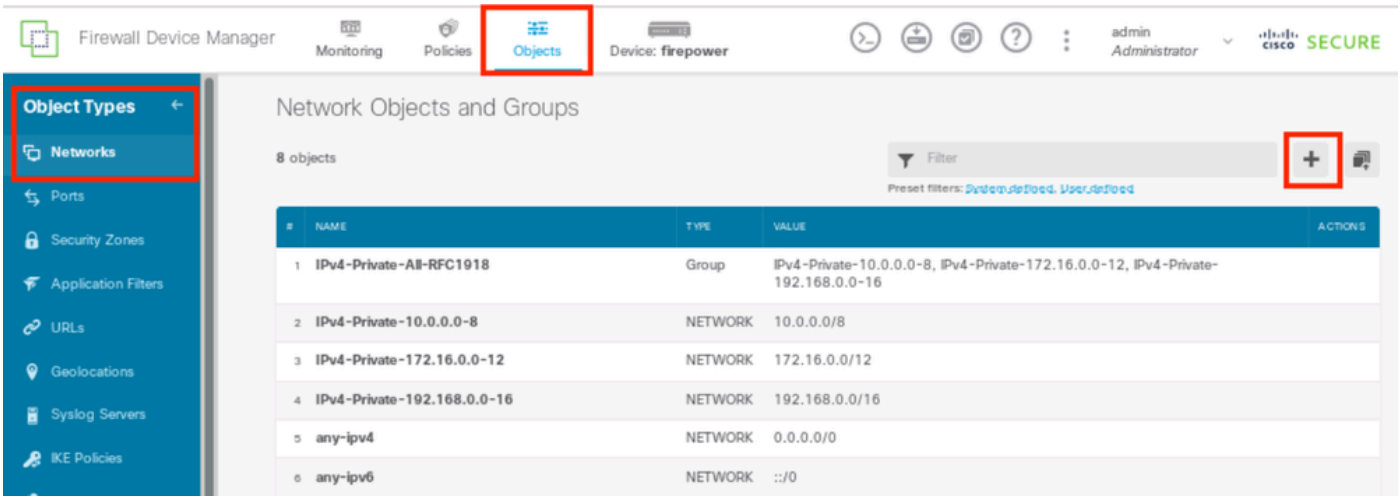
3. Haga clic en la ficha IPv4 Address y configure la dirección IPv4, en este caso 10.1.3.1/24.
4. Click OK.



Paso 0 Editar Interfaz Gi0/3



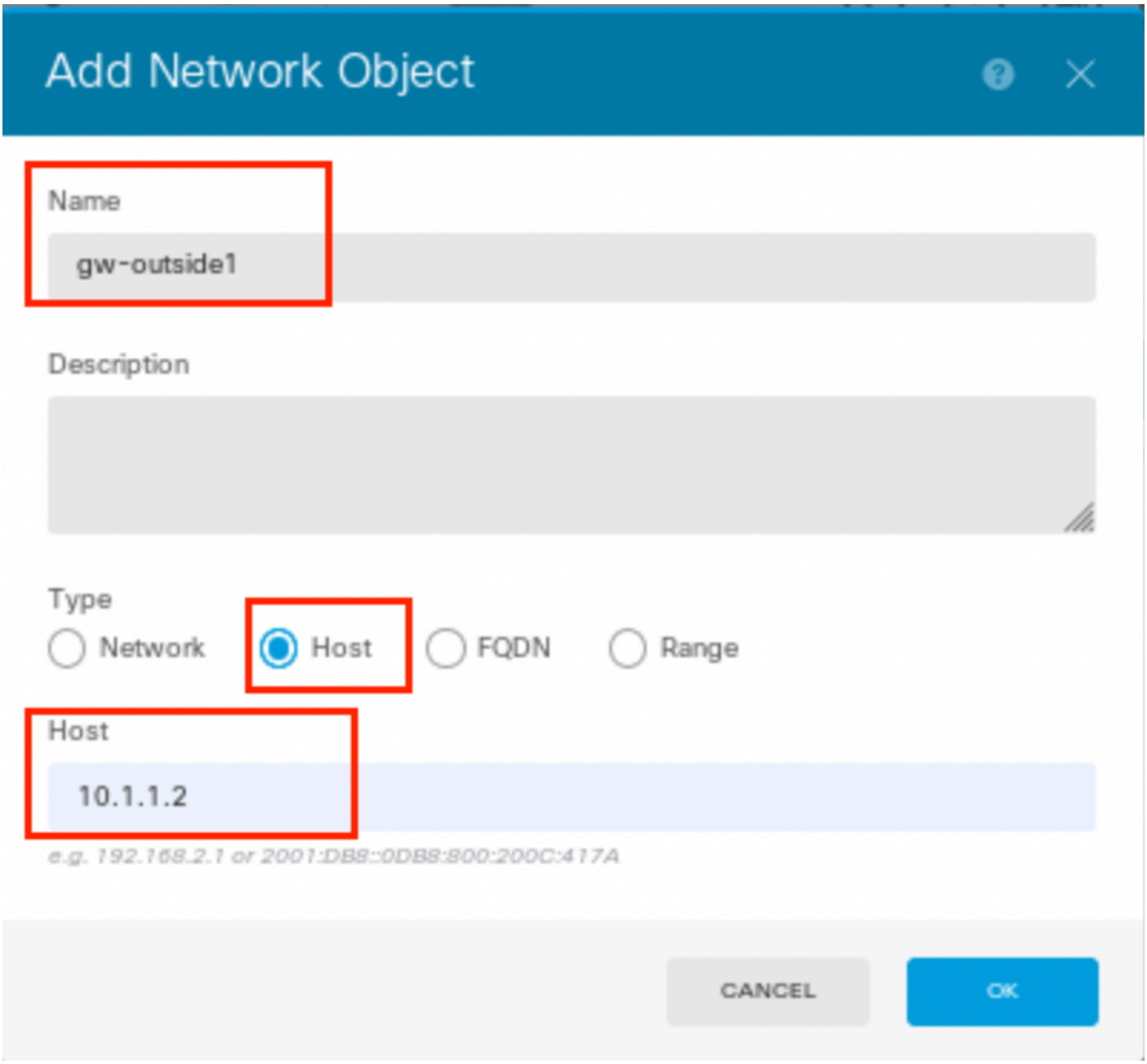
Vaya a Objetos > Tipos de objeto > Redes , haga clic en el icono de añadir ( ) para añadir un nuevo objeto.



Paso 0 Objeto1

En la ventana Add Network Object , configure la primera gateway ISP:

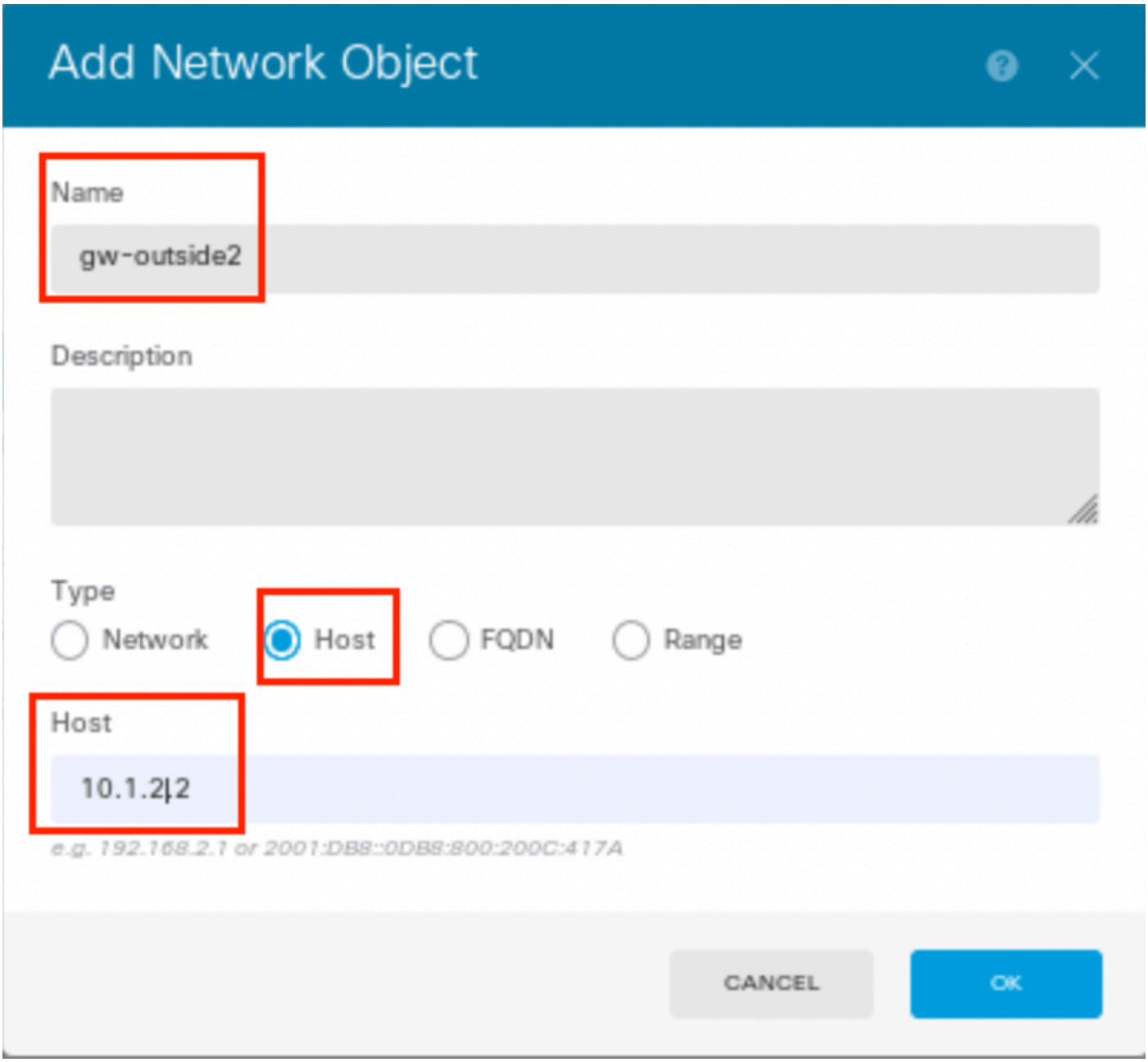
1. Establezca el Nombre del objeto, en este caso gw-outside1.
2. Seleccione el Tipo del objeto, en este caso Host.
3. Establezca la dirección IP del host , en este caso 10.1.1.2.
4. Click OK.



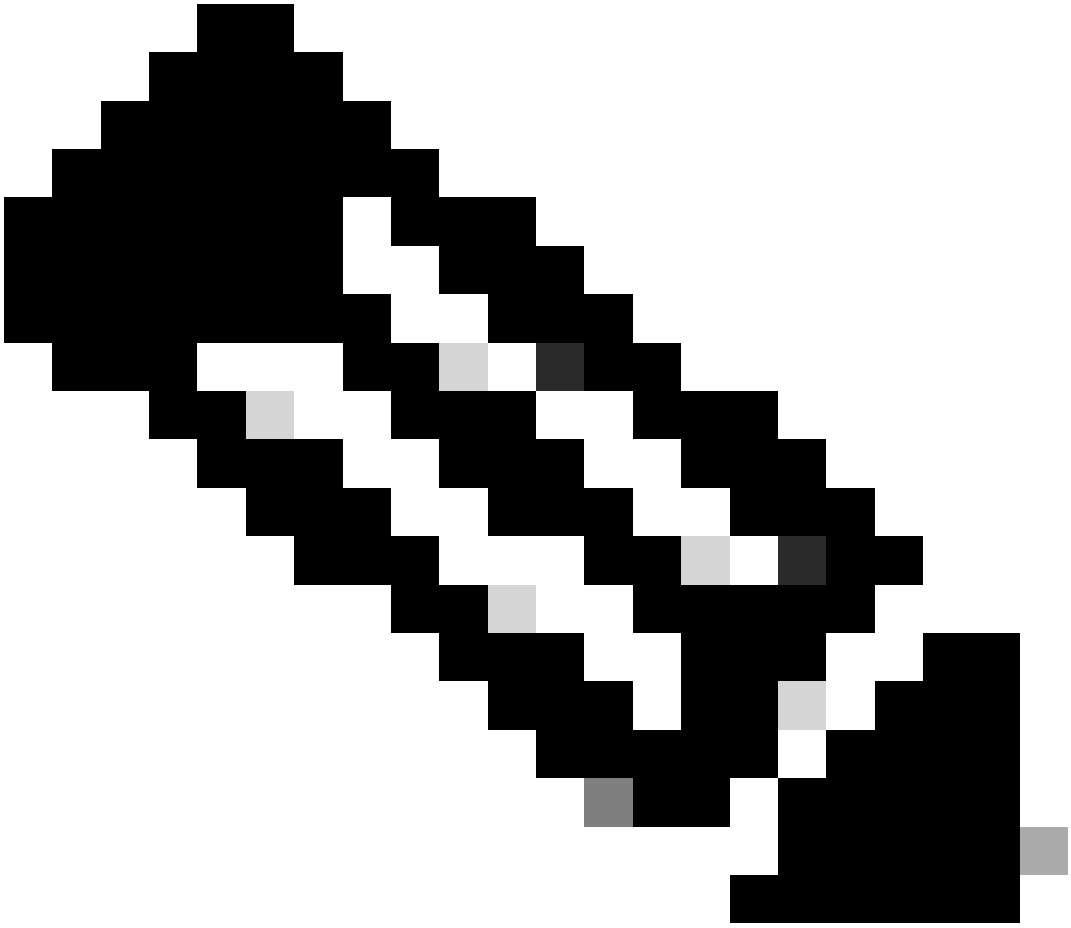
Paso 0 Objeto2

Repita los pasos similares para configurar otro objeto de red para la segunda gateway del ISP:

1. Establezca el Nombre del objeto, en este caso gw-outside2.
2. Seleccione el Tipo del objeto, en este caso Host.
3. Establezca la dirección IP del host , en este caso 10.1.2.2.
4. Click OK.



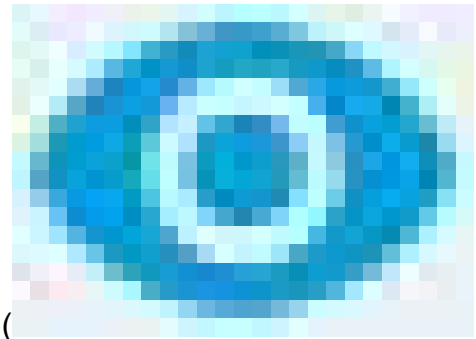
Paso 0 Objeto3



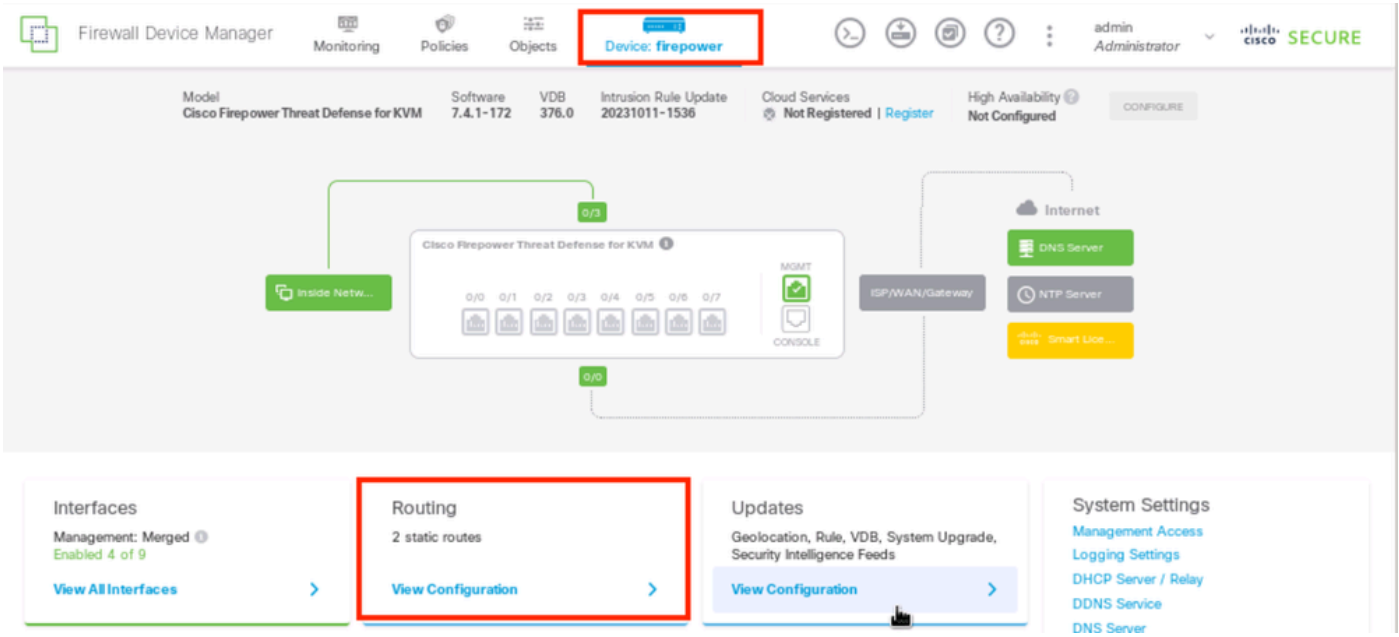
Nota: Debe tener la política de control de acceso configurada en FTD para permitir el tráfico, esta parte no se incluye en este documento.

Paso 1. Configuración de la zona ECMP

Navegue hasta Dispositivo , luego haga clic en el link en el resumen de Ruteo.



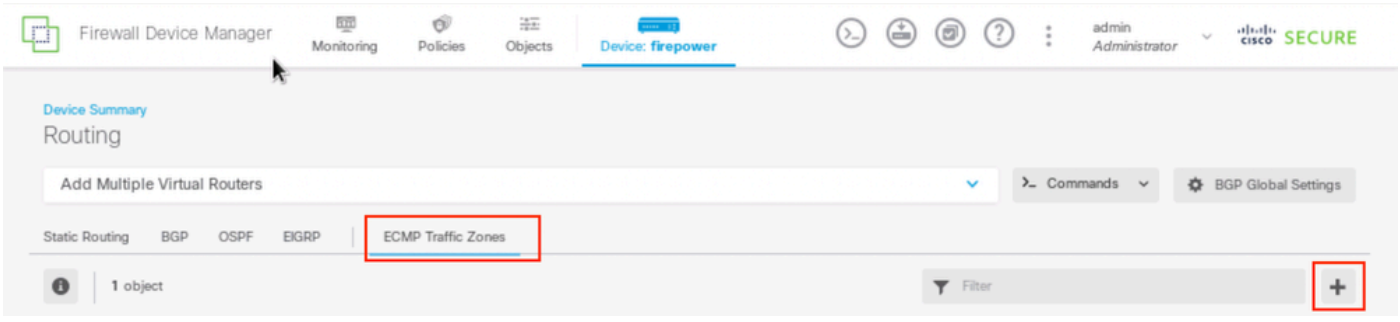
Si ha activado los routers virtuales, haga clic en el icono de vista ( ) del router en el que está configurando una ruta estática. En este caso, los routers virtuales no están habilitados.



Paso 1 ECMP Zone1

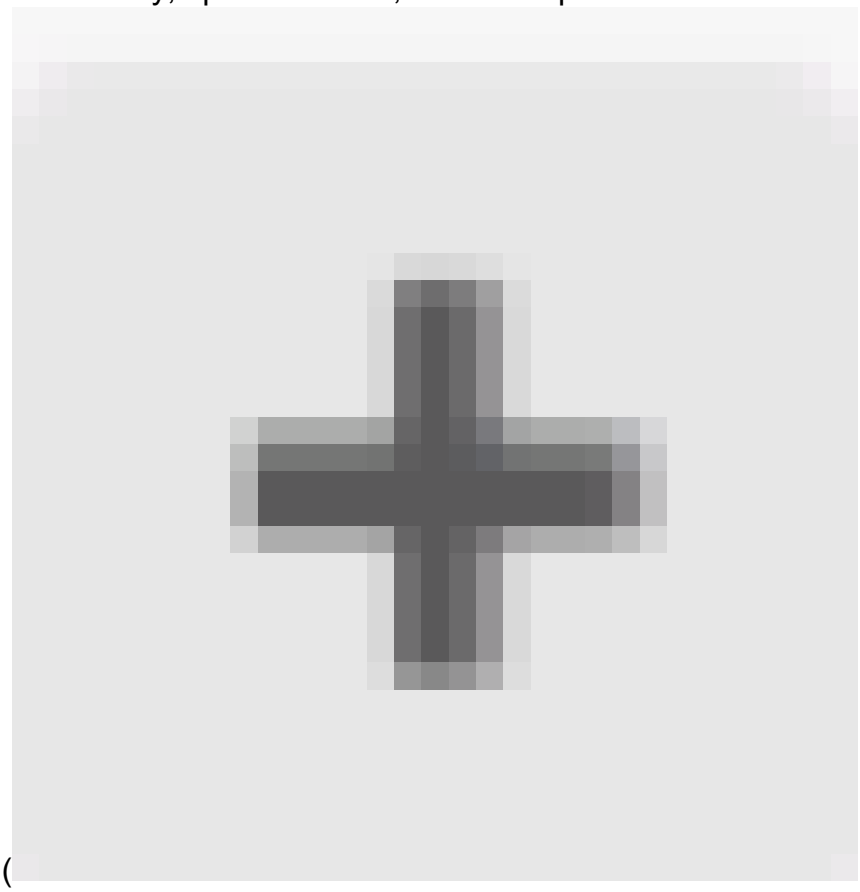
Haga clic en la pestaña Zonas de tráfico ECMP y, a continuación, haga clic en el icono de adición (

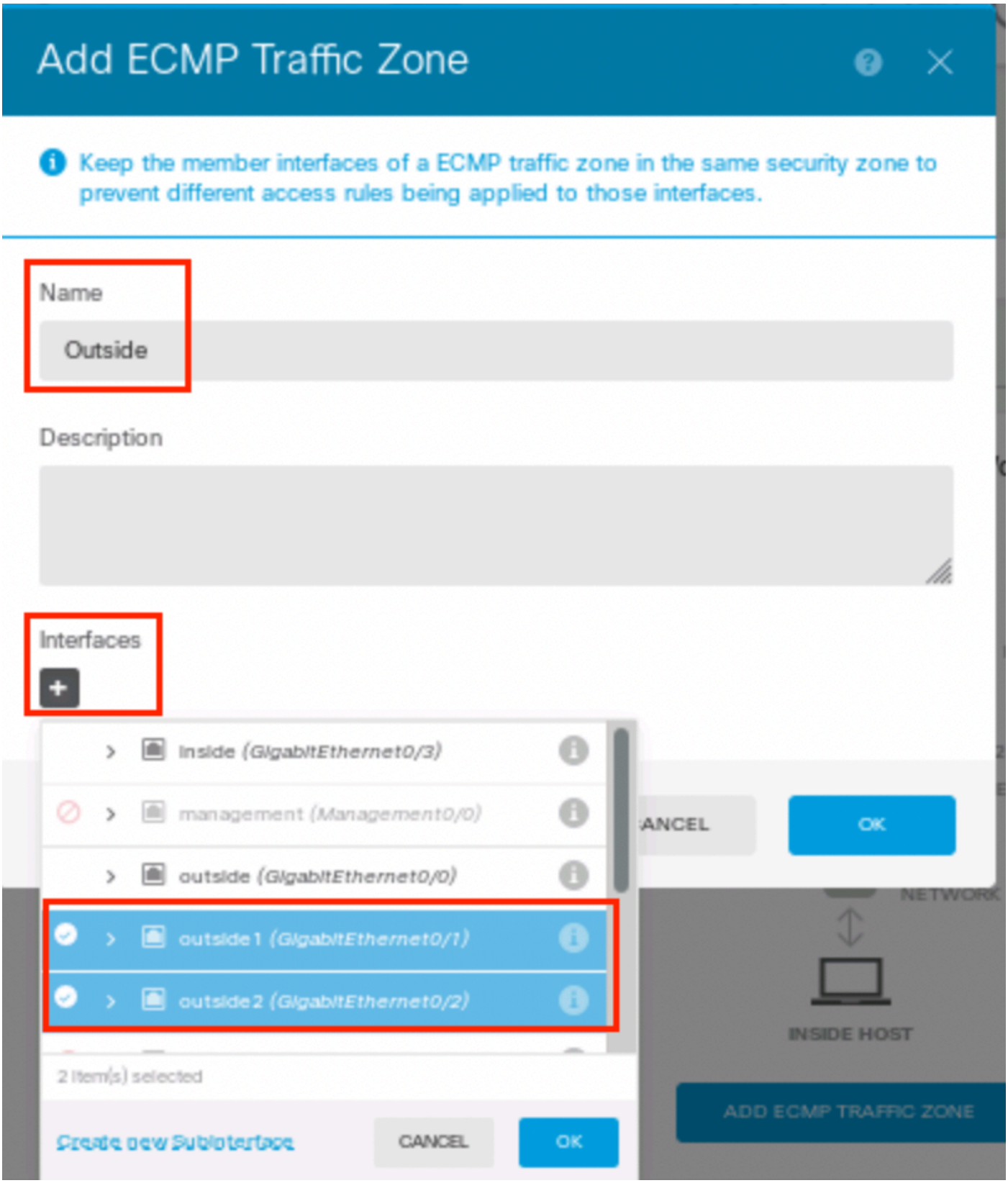
) para agregar una nueva zona.



Paso 1 ECMP Zone2

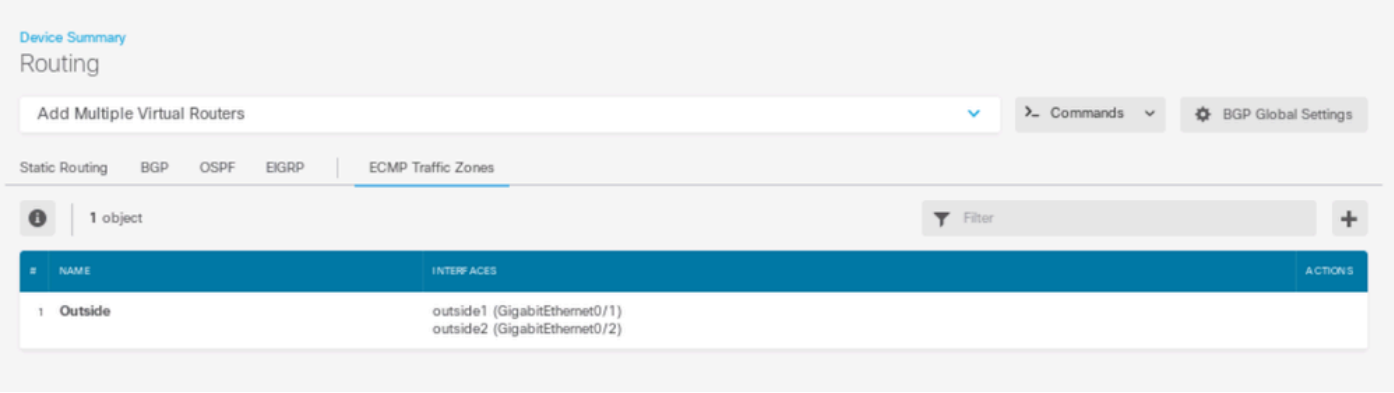
En la ventana Add ECMP Traffic Zone:

1. Establezca el Nombre para la zona ECMP y, opcionalmente, una descripción.
2. Haga clic en el icono de adición () para seleccionar un máximo de 8 interfaces para incluirlas en la zona. En este ejemplo, el nombre de ECMP es Outside , las interfaces outside1 y outside2 se agregan a la zona.
3. Click OK.

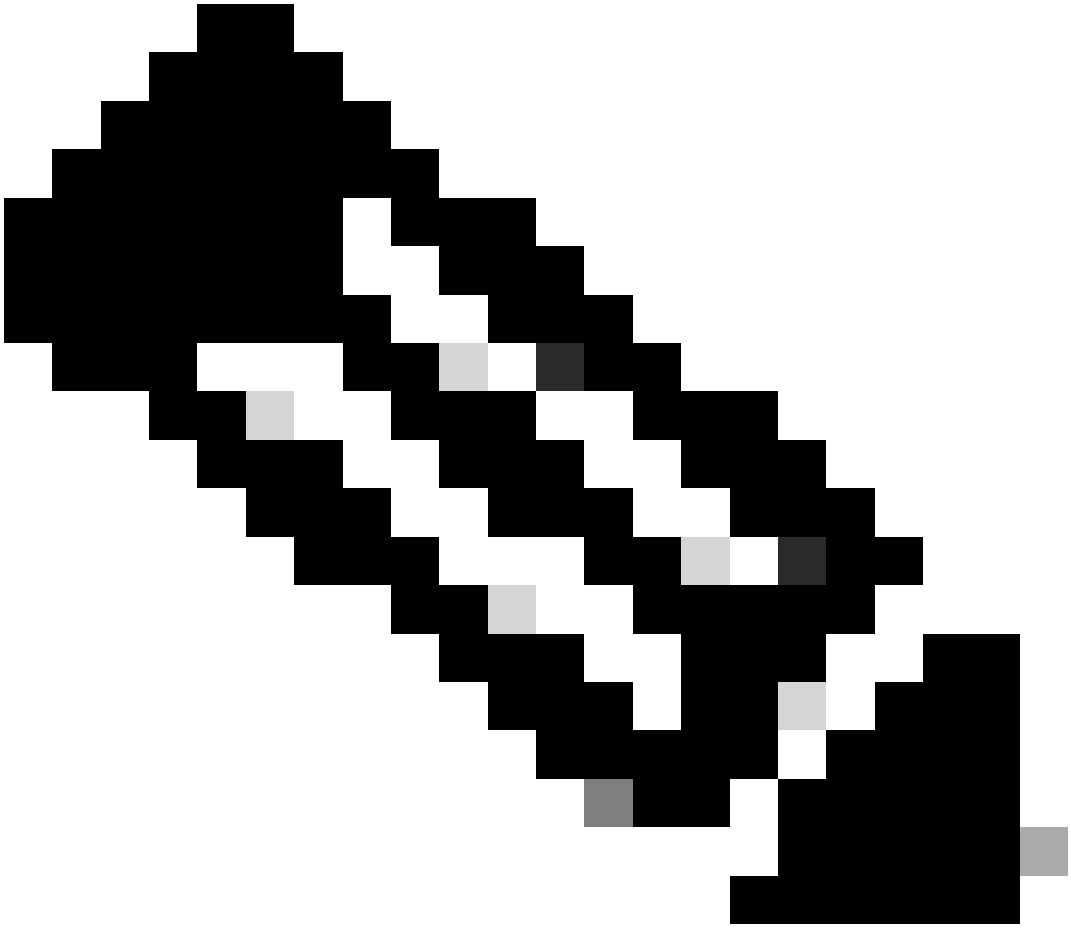


Paso 1 ECMP Zone3

Las interfaces outside1 y outside2 se han agregado correctamente a la zona ECMP outside .



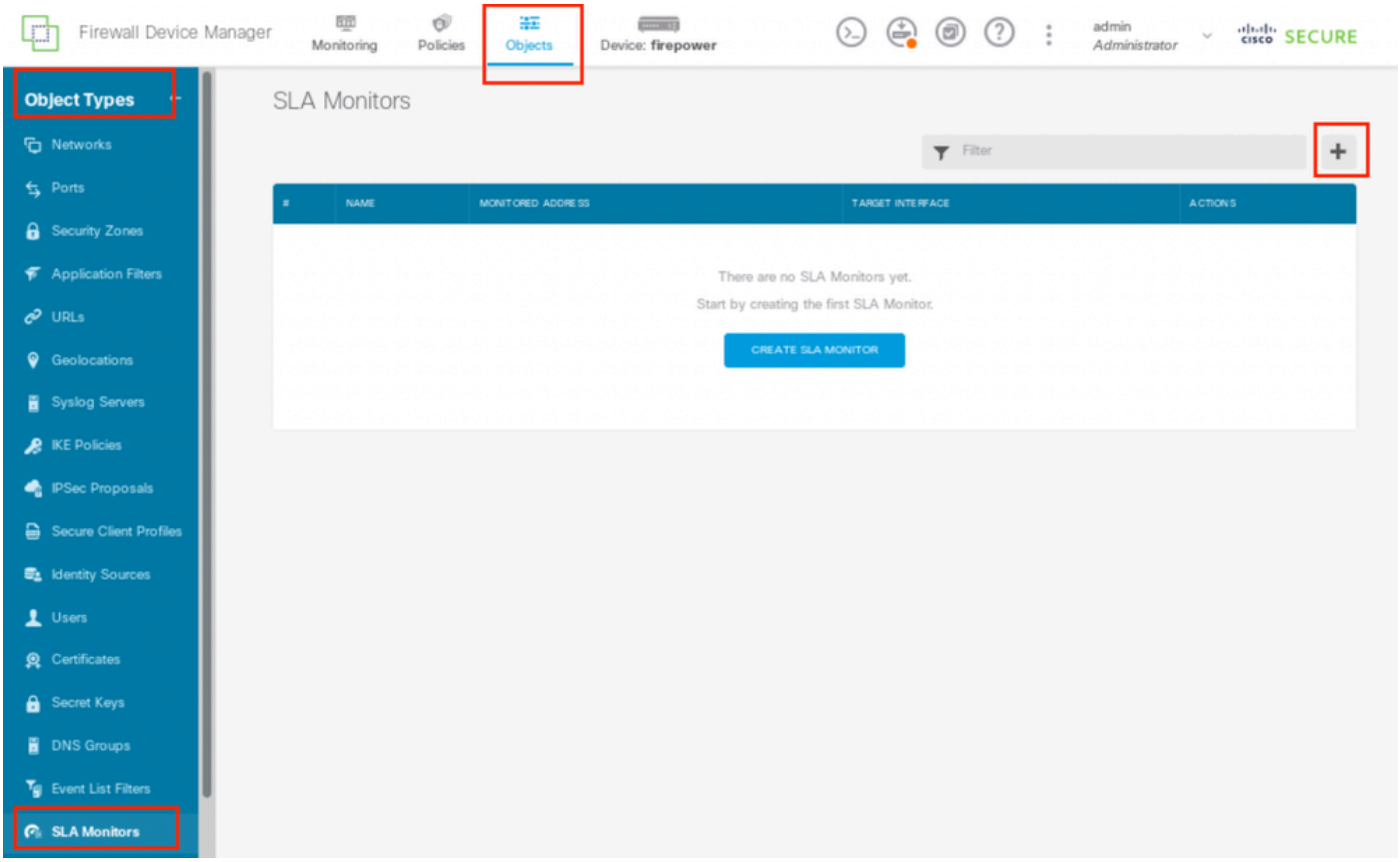
Paso 1 ECMP Zone4



Nota: Una zona de tráfico de enrutamiento ECMP no está relacionada con zonas de seguridad. La creación de una zona de seguridad que contiene las interfaces outside1 y outside2 no implementa una zona de tráfico para fines de ruteo ECMP.

Paso 2. Configurar objetos de SLA de IP

Para definir los objetos SLA utilizados para supervisar la conectividad con cada gateway, navegue hasta Objetos > Tipos de objeto > Monitores SLA, haga clic en el icono de agregar ( ) para agregar un nuevo monitor SLA para la primera conexión ISP.



Paso 2 IP SLA1

En la ventana Add SLA Monitor Object :

1. Establezca el Nombre para el objeto de monitoreo SLA y, opcionalmente, una descripción, en este caso sla-outside1.
2. Establezca la Dirección del monitor , en este caso gw-outside1 (la primera gateway ISP).
3. Establezca la Interfaz de destino a través de la cual se puede alcanzar la dirección de monitoreo, en este caso outside1 .
4. Además, también es posible ajustar el tiempo de espera y el umbral . Click OK.

Add SLA Monitor Object

Name

sla-outside1

Description

Monitor Address

gw-outside1

Target Interface

outside1 (GigabitEthernet0/1)

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

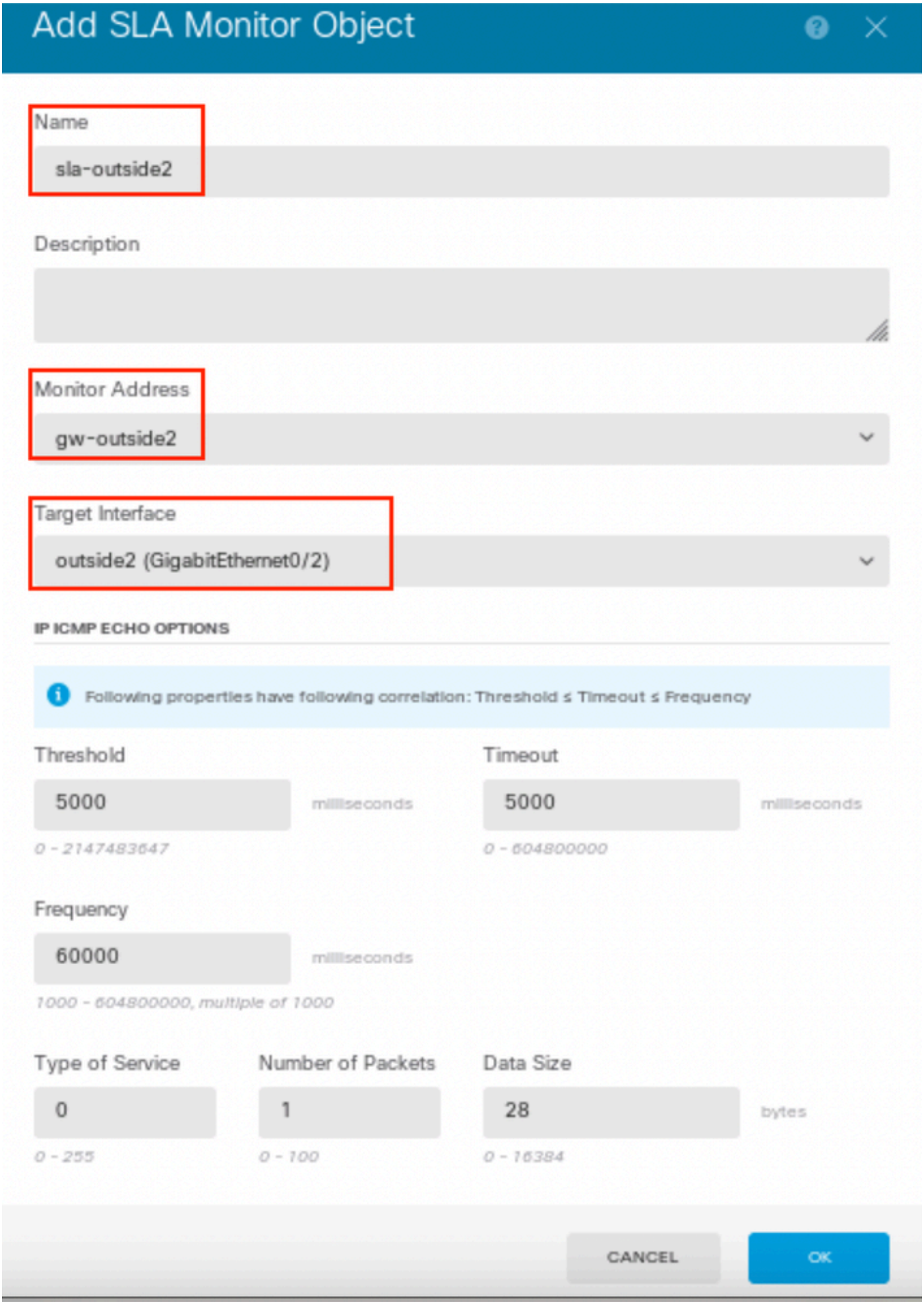
28 bytes

0 - 16384

CANCEL OK

Repita el paso similar para configurar otro objeto de monitoreo de SLA para la segunda conexión ISP, en la ventana Agregar Objeto de Monitor de SLA:

1. Establezca el Nombre para el objeto de monitoreo SLA y, opcionalmente, una descripción, en este caso sla-outside2 .
2. Establezca la Dirección del monitor , en este caso gw-outside2 (la segunda gateway ISP).
3. Establezca la interfaz de destino a través de la cual se puede alcanzar la dirección del monitor, en este caso outside2.
4. Además, también es posible ajustar el tiempo de espera y el umbral. Click OK.

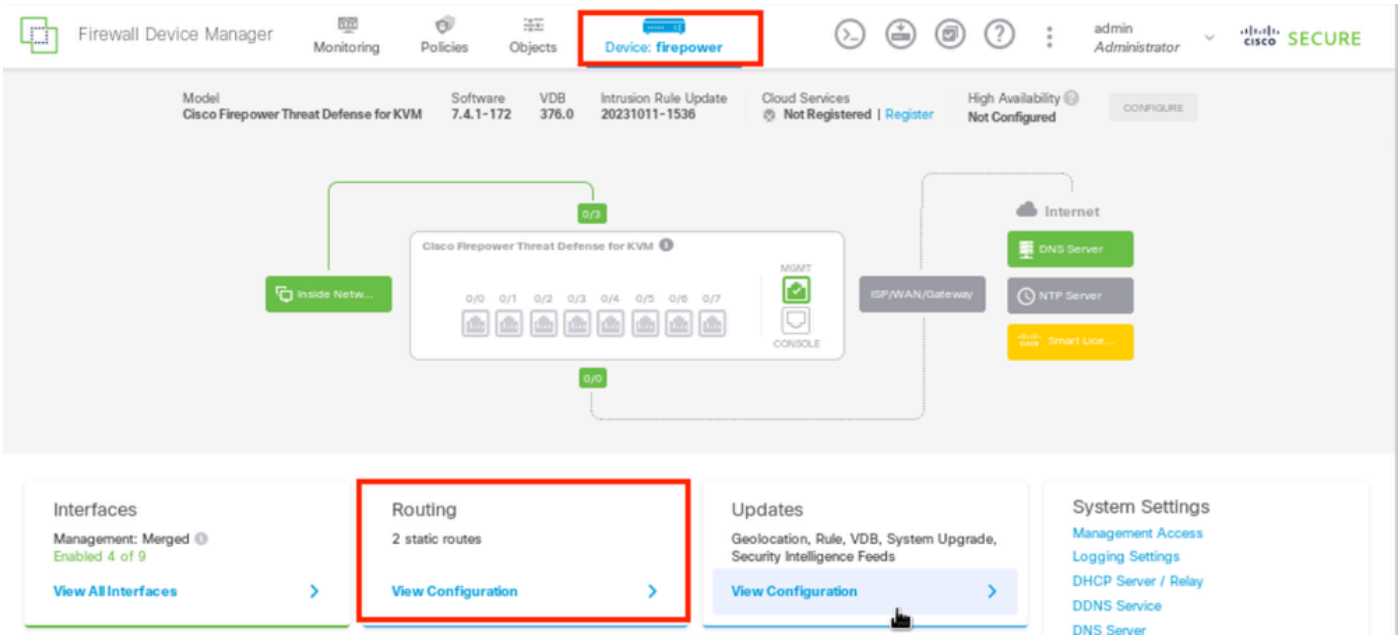

Add SLA Monitor Object
Name
sla-outside2
Description
Monitor Address
gw-outside2
Target Interface
outside2 (GigabitEthernet0/2)
IP ICMP ECHO OPTIONS
Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency
Threshold
5000
milliseconds
0 - 2147483647
Timeout
5000
milliseconds
0 - 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

Paso 2: IP SLA3

Paso 3. Configuración de Rutas Estáticas con Route Track

Navegue hasta Dispositivo , luego haga clic en el link en el resumen de Ruteo.

Si ha activado los routers virtuales, haga clic en el icono de vista ( ) del router en el que está configurando una ruta estática. En este caso, los routers virtuales no están habilitados.



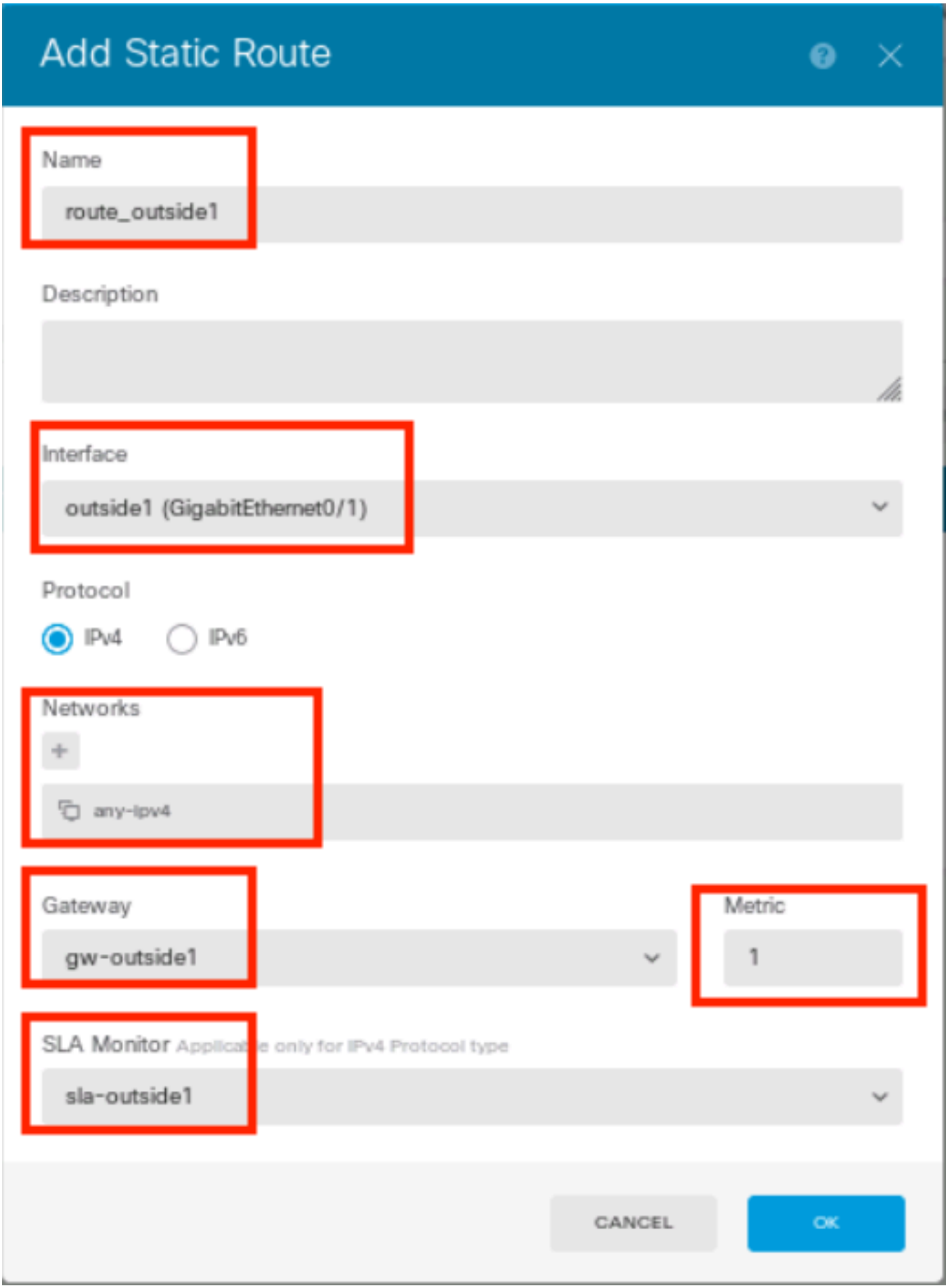
Paso 3 Ruta 1

En la página Static Routing, haga clic en el icono de agregar ( )

) para agregar una nueva ruta estática para el primer enlace ISP.

En la ventana Add Static Route:

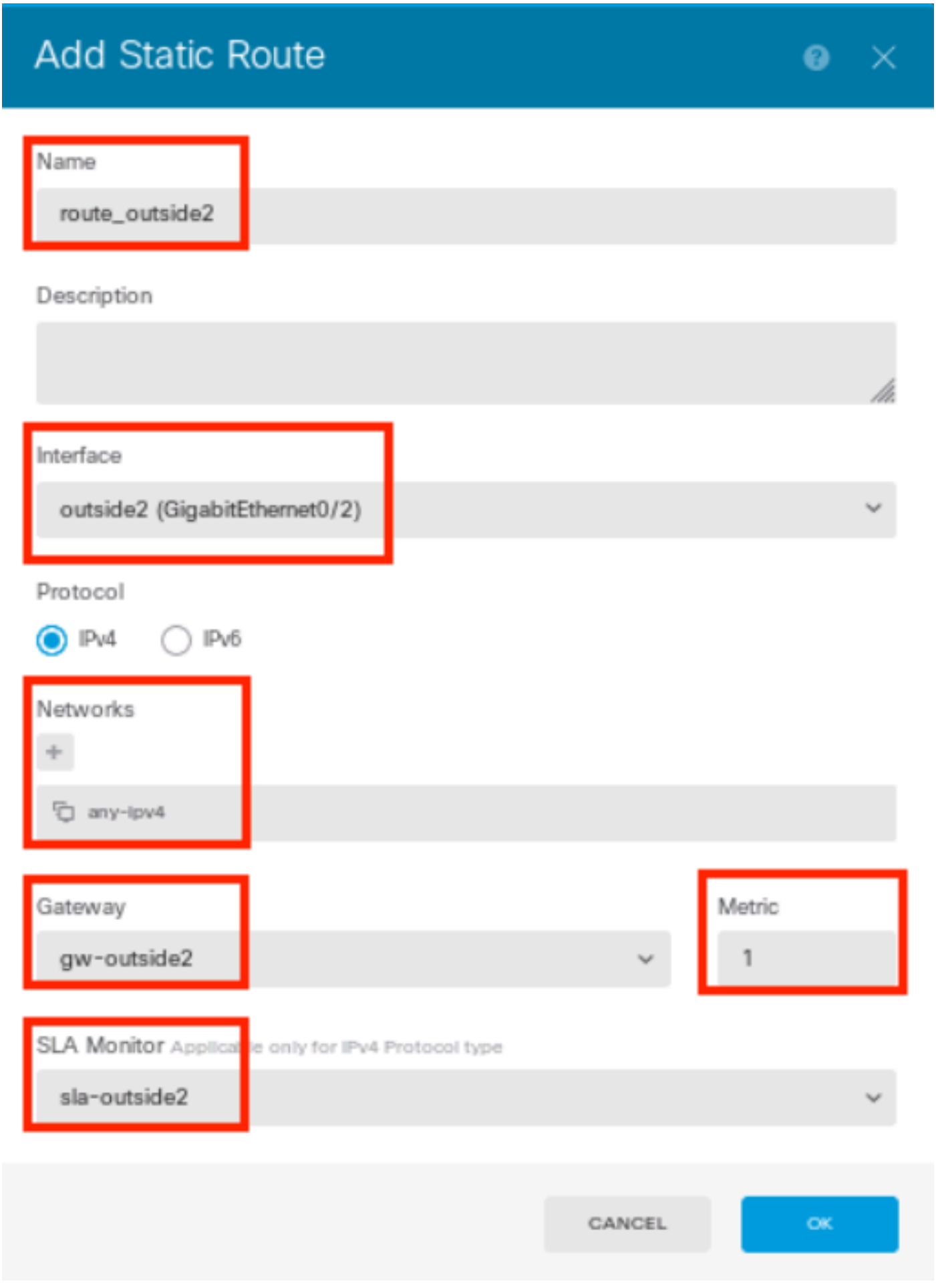
1. Establezca el Nombre de la ruta y, opcionalmente, la descripción. En este caso, route_outside1.
2. En la lista desplegable Interface, seleccione la interfaz a través de la cual desea enviar el tráfico. La dirección de gateway debe ser accesible a través de la interfaz. En este caso, outside1 (GigabitEthernet0/1).
3. Seleccione las redes que identifican las redes o los hosts de destino que utilizan la puerta de enlace en esta ruta. En este caso, el any-ipv4 predefinido.
4. En la lista desplegable Gateway, seleccione el objeto de red que identifica la dirección IP del gateway. El tráfico se envía a esta dirección. En este caso, gw-outside1 (el primer gateway ISP).
5. Establezca la Métrica de la ruta, entre 1 y 254. En este ejemplo 1.
6. En la lista desplegable Monitor de SLA, seleccione el objeto de monitor de SLA. En este caso sla-outside1.
7. Click OK.


Add Static Route
Name
route_outside1
Description
Interface
outside1 (GigabitEthernet0/1)
Protocol
IPv4
IPv6
Networks
any-ipv4
Gateway
gw-outside1
Metric
1
SLA Monitor
sla-outside1
CANCEL
OK

Paso 3 Ruta 2

Repita el paso similar para configurar otra ruta estática para la segunda conexión ISP, en la ventana Add Static Route :

1. Establezca el Nombre de la ruta y, opcionalmente, la descripción. En este caso, route_outside2.
2. En la lista desplegable Interface, seleccione la interfaz a través de la cual desea enviar el tráfico. La dirección de gateway debe ser accesible a través de la interfaz. En este caso, outside2 (GigabitEthernet0/2).
3. Seleccione las redes que identifican las redes o los hosts de destino que utilizan la puerta de enlace en esta ruta. En este caso, el any-ipv4 predefinido.
4. En la lista desplegable Gateway, seleccione el objeto de red que identifica la dirección IP del gateway. El tráfico se envía a esta dirección. En este caso, gw-outside2 (el segundo gateway ISP).
5. Establezca la Métrica de la ruta, entre 1 y 254. En este ejemplo 1.
6. En la lista desplegable Monitor de SLA, seleccione el objeto de monitor de SLA. En este escenario, sla-outside2.
7. Click OK.


Add Static Route
Name
route_outside2
Description
Interface
outside2 (GigabitEthernet0/2)
Protocol
IPv4
IPv6
Networks
any-ipv4
Gateway
gw-outside2
Metric
1
SLA Monitor
sla-outside2
CANCEL
OK

Paso 3 Ruta 3

Tiene 2 rutas a través de las interfaces outside1 y outside2 con rutas de ruta.

Paso 3 Ruta 4

Implemente el cambio en FTD.

Verificación

Inicie sesión en la CLI del FTD, ejecute el comando show zone para comprobar la información sobre las zonas de tráfico ECMP, incluidas las interfaces que forman parte de cada zona.

<#root>

> show zone
Zone:

Outside

```
 ecmp
    Security-level: 0
```

Zone member(s): 2

outside2 GigabitEthernet0/2

outside1 GigabitEthernet0/1

Ejecute el comando show running-config route para verificar la configuración en ejecución para la configuración de ruteo, en este caso hay dos rutas estáticas con pistas de ruta.

<#root>

> show running-config route

route outside1 0.0.0.0 0.0.0.0 10.1.1.2 1 track 1

route outside2 0.0.0.0 0.0.0.0 10.1.2.2 1 track 2

Ejecute el comando show route para verificar la tabla de ruteo, en este caso hay dos rutas predeterminadas a través de la interfaz outside1 y outside2 con el mismo costo, el tráfico se puede distribuir entre dos circuitos ISP.

<#root>

> show 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, BI - BGP InterVRF
Gateway of last resort is 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2

[1/0] via 10.1.1.2, outside1

C 10.1.1.0 255.255.255.0 is directly connected, outside1
L 10.1.1.1 255.255.255.255 is directly connected, outside1
C 10.1.2.0 255.255.255.0 is directly connected, outside2
L 10.1.2.1 255.255.255.255 is directly connected, outside2
C 10.1.3.0 255.255.255.0 is directly connected, inside
L 10.1.3.1 255.255.255.255 is directly connected, inside

Ejecute el comando show sla monitor configuration para verificar la configuración del monitor SLA.

<#root>

> show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 1037119999
Owner:
Tag:

Type of operation to perform: echo

Target address: 10.1.1.2

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:

Entry number: 1631063762
Owner:
Tag:
```

Type of operation to perform: echo

Target address: 10.1.2.2

Interface: outside2

```
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:
```

Ejecute el comando show sla monitor operational-state para confirmar el estado del Monitor SLA. En este caso, puede encontrar "Tiempo de espera agotado: FALSO" en la salida del comando, que indica que el eco ICMP al gateway está respondiendo, por lo que la ruta predeterminada a través de la interfaz de destino está activa e instalada en la tabla de ruteo.

<#root>

> show sla monitor operational-state
Entry number: 1037119999
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 79
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never

Connection loss occurred: FALSE

Timeout occurred: FALSE

Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 05:32:32.791 UTC Tue Jan 30 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 1631063762
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 79
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE

Timeout occurred: FALSE

Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 05:32:32.791 UTC Tue Jan 30 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Equilibrio de carga

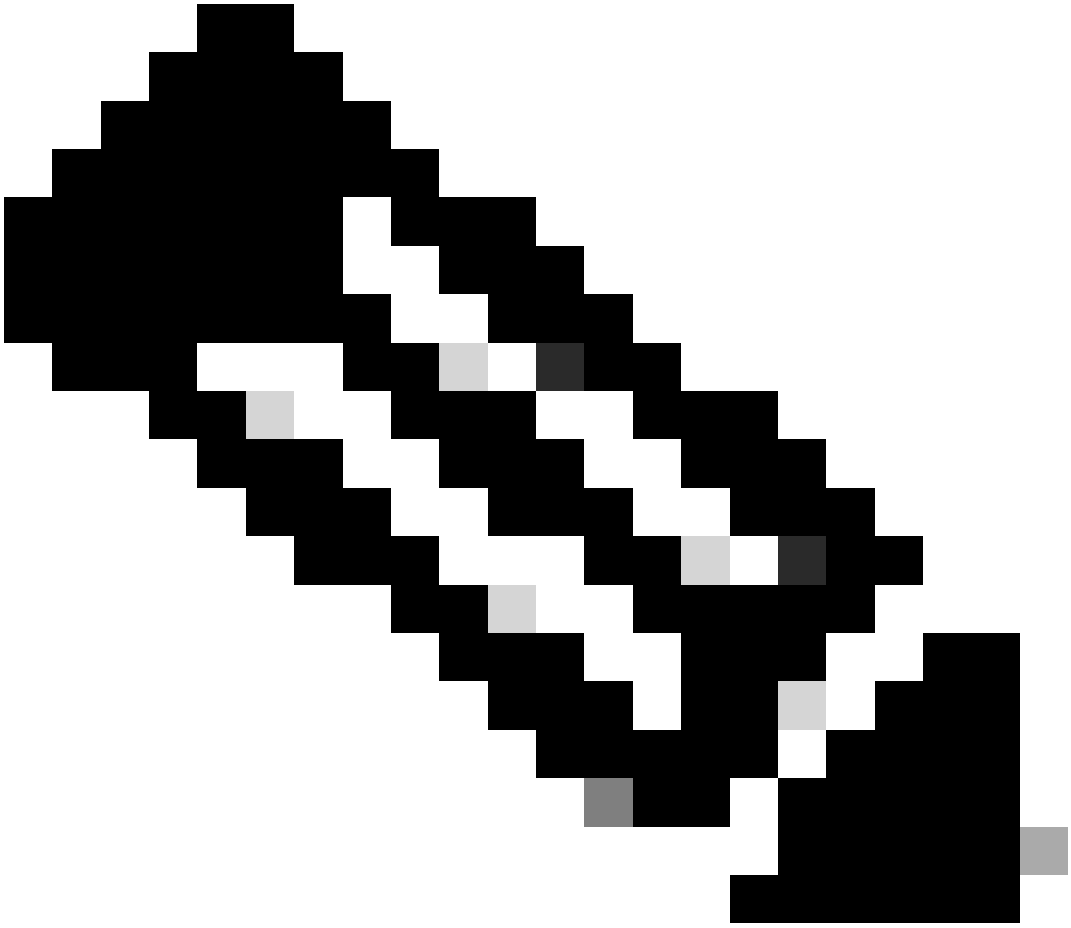
Tráfico inicial a través de FTD para verificar si la carga de ECMP equilibra el tráfico entre las puertas de enlace en la zona ECMP. En este caso, inicie la conexión SSH desde Test-PC-1 (10.1.3.2) y Test-PC-2 (10.1.3.4) hacia Internet-Host (10.1.5.2), ejecute el comando show conn para confirmar que el tráfico está balanceado por carga entre dos links ISP, Test-PC-1 (10.1.3.2) pasa a través de la interfaz outside1, Test-PC-2 (10.1.3.4) pasa a través de la interfaz outside2.

<#root>

> show conn
4 in use, 14 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect

TCP inside 10.1.3.4:41652 outside2 10.1.5.2:22, idle 0:02:10, bytes 5276, flags UIO N1

TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:00:04, bytes 5276, flags UIO N1



Nota: El tráfico tiene una carga equilibrada entre las puertas de enlace especificadas en función de un algoritmo que aplica hash a las direcciones IP de origen y destino, la interfaz entrante, el protocolo, el origen y los puertos de destino. cuando ejecute la prueba, el tráfico que simula se puede dirigir a la misma puerta de enlace debido al algoritmo hash. Se espera que esto cambie cualquier valor entre las 6 tuplas (IP de origen, IP de destino, interfaz entrante, protocolo, puerto de origen y puerto de destino) para realizar cambios en el resultado de hash.

Ruta perdida

Si el link a la primera gateway del ISP está inactivo, en este caso, apague el primer router de gateway para simular. Si el FTD no recibe una respuesta de eco del primer gateway ISP dentro del temporizador de umbral especificado en el objeto Monitor SLA, el host se considera inalcanzable y se marca como inactivo. La ruta de seguimiento a la primera gateway también se elimina de la tabla de routing.

Ejecute el comando show sla monitor operational-state para confirmar el estado actual del Monitor de SLA. En este caso, puede encontrar

"Tiempo de espera agotado: Verdadero" en el resultado del comando, que indica que el eco ICMP al primer gateway ISP no responde.

<#root>

> show sla monitor operational-state
Entry number: 1037119999
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 121
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE

Timeout occurred: TRUE

Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 06:14:32.801 UTC Tue Jan 30 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0 RTTMin: 0 RTTMax: 0
NumOfRTT: 0 RTTSum: 0 RTTSum2: 0

Entry number: 1631063762
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 121
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE

Timeout occurred: FALSE

Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 06:14:32.802 UTC Tue Jan 30 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Ejecute el comando **show route** para verificar la tabla de ruteo actual, se elimina la ruta hacia la primera gateway ISP a través de la interfaz outside1, sólo hay una ruta predeterminada activa hacia la segunda gateway ISP a través de la interfaz outside2.

<#root>

> show 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, BI - BGP InterVRF
Gateway of last resort is 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2

C 10.1.1.0 255.255.255.0 is directly connected, outside1
L 10.1.1.1 255.255.255.255 is directly connected, outside1
C 10.1.2.0 255.255.255.0 is directly connected, outside2
L 10.1.2.1 255.255.255.255 is directly connected, outside2
C 10.1.3.0 255.255.255.0 is directly connected, inside
L 10.1.3.1 255.255.255.255 is directly connected, inside

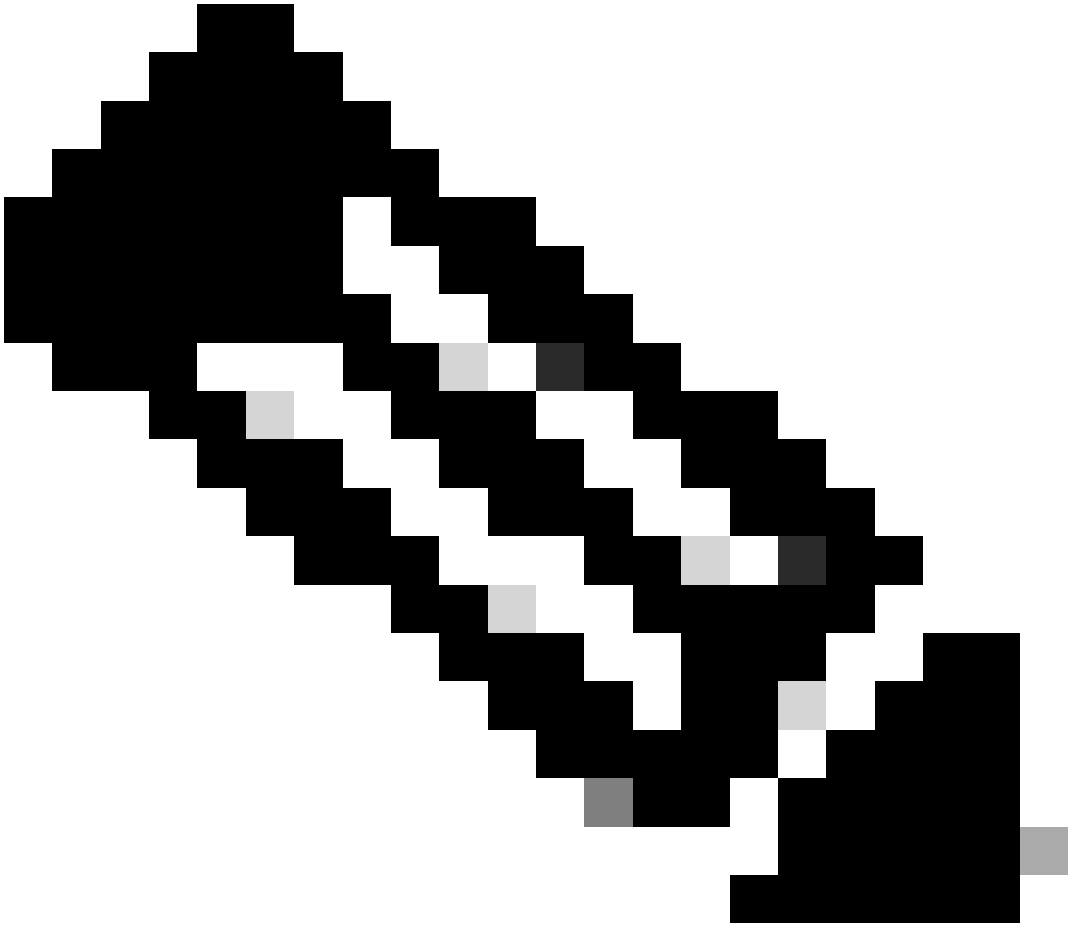
Ejecute el comando show conn , puede encontrar que las dos conexiones aún están activas. Las sesiones SSH también están activas en Test-PC-1 (10.1.3.2) y Test-PC-2 (10.1.3.4) sin ninguna interrupción.

<#root>

> show conn
4 in use, 14 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect

TCP inside 10.1.3.4:41652 outside2 10.1.5.2:22, idle 0:19:29, bytes 5276, flags UIO N1

TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:17:22, bytes 5276, flags UIO N1



Nota: Puede observar que en la salida de show conn , la sesión SSH de Test-PC-1 (10.1.3.2) aún está a través de la interfaz outside1, aunque la ruta predeterminada a través de la interfaz outside1 se ha eliminado de la tabla de ruteo. Esto se espera y, por diseño, el tráfico real fluye a través de la interfaz outside2. Si inicia una nueva conexión de Test-PC-1 (10.1.3.2) a Internet-Host (10.1.5.2), puede encontrar que todo el tráfico se realiza a través de la interfaz outside2.

Troubleshoot

Para validar el cambio de la tabla de ruteo, ejecute el comando debug ip routing .

En este ejemplo, cuando el link a la primera gateway ISP está inactivo, la ruta a través de la interfaz outside1 se elimina de la tabla de ruteo.

<#root>

> debug ip routing
IP routing debugging is on

RT:

ip_route_delete 0.0.0.0 0.0.0.0 via 10.1.1.2, outside1

ha_cluster_synced 0 routetype 0

RT: del 0.0.0.0 via 10.1.1.2, static metric [1/0]NP-route: Delete-Output 0.0.0.0/0 hop_count:1 , via 0.0

RT(mgmt-only):

NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, outside2

NP-route: Update-Input 0.0.0.0/0 hop_count:1 Distance:1 Flags:0X0 , via 10.1.2.2, outside2

Ejecute el comando show route para confirmar la tabla de ruteo actual.

<#root>

> show 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, BI - BGP InterVRF
Gateway of last resort is 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2

C 10.1.1.0 255.255.255.0 is directly connected, outside1
L 10.1.1.1 255.255.255.255 is directly connected, outside1
C 10.1.2.0 255.255.255.0 is directly connected, outside2
L 10.1.2.1 255.255.255.255 is directly connected, outside2
C 10.1.3.0 255.255.255.0 is directly connected, inside
L 10.1.3.1 255.255.255.255 is directly connected, inside

Cuando el link a la primera gateway ISP está activo nuevamente, la ruta a través de la interfaz outside1 se agrega nuevamente a la tabla de ruteo.

<#root>

> debug ip routing
IP routing debugging is on

RT(mgmt-only):

```
NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, outside2
```

```
NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.1.2, outside2
```

```
NP-route: Update-Input 0.0.0.0/0 hop_count:2 Distance:1 Flags:0X0 , via 10.1.2.2, outside2
via 10.1.1.2, outside1
```

Ejecute el comando show route para confirmar la tabla de ruteo actual.

> show 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, BI - BGP InterVRF
Gateway of last resort is 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2
[1/0] via 10.1.1.2, outside1
C 10.1.1.0 255.255.255.0 is directly connected, outside1
L 10.1.1.1 255.255.255.255 is directly connected, outside1
C 10.1.2.0 255.255.255.0 is directly connected, outside2
L 10.1.2.1 255.255.255.255 is directly connected, outside2
C 10.1.3.0 255.255.255.0 is directly connected, inside
L 10.1.3.1 255.255.255.255 is directly connected, inside

Información Relacionada

- Soporte técnico y descargas de Cisco

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).