Configuración de ECMP con IP SLA en FTD gestionado por FMC

Contenido

Introducción

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

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 Management Center (FMC)

Componentes Utilizados

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

- Cisco FTD versión 7.4.1

- Cisco FMC versión 7.4.1

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 FMC. 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

- Cisco Secure Firewall Management Center 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.

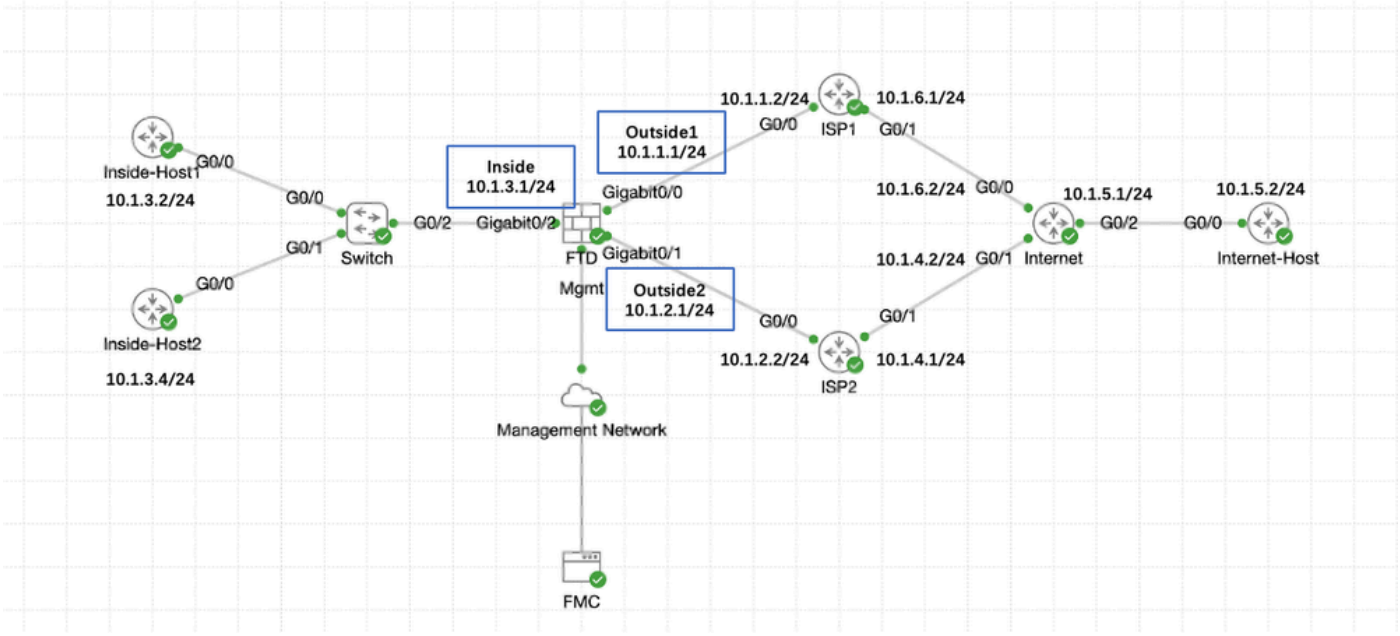
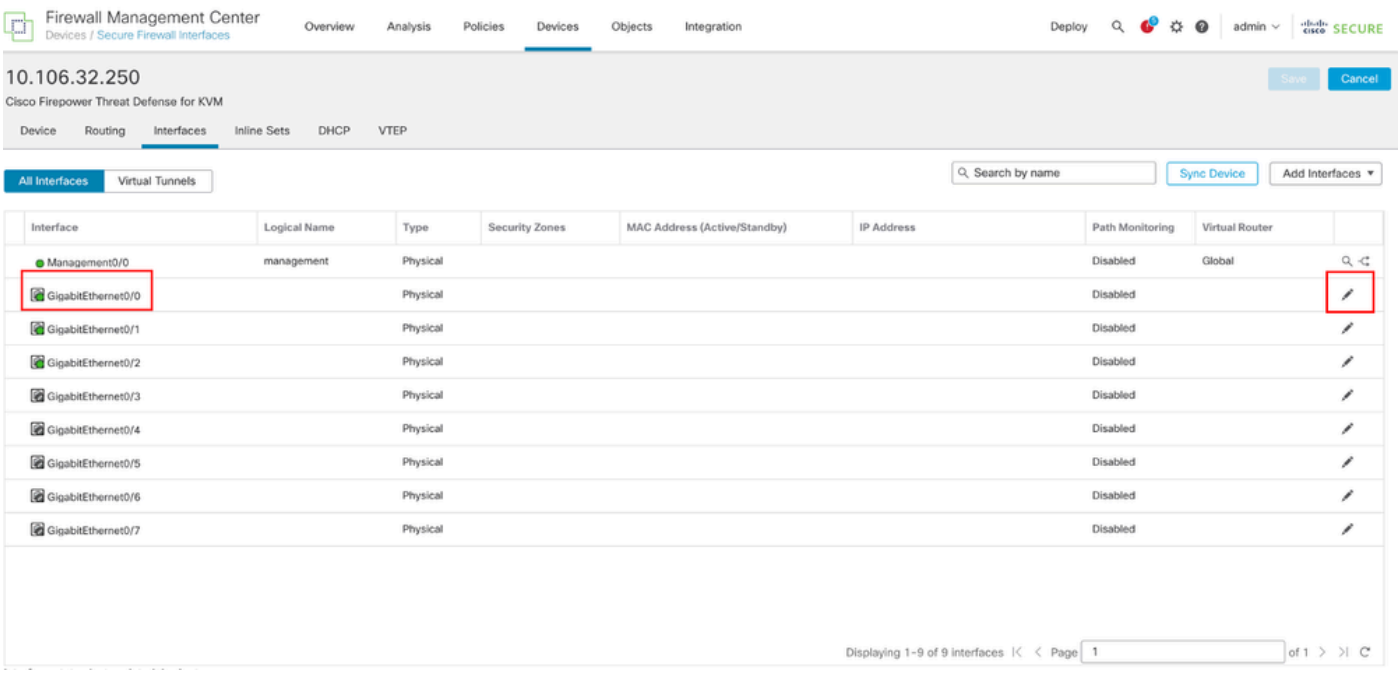


Diagrama de la red

Configuraciones

Paso 0. Preconfigurar interfaces/objetos de red

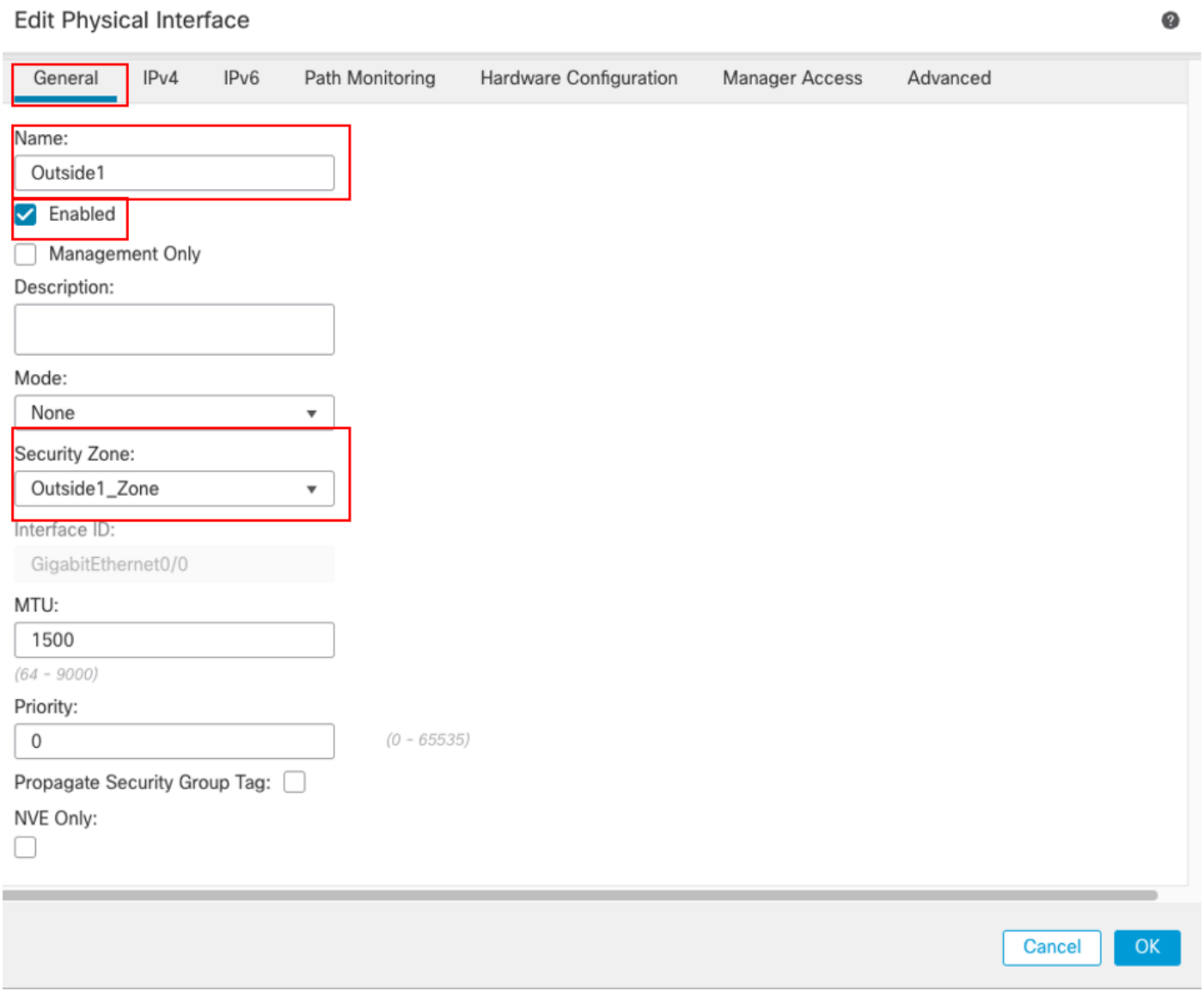
Inicie sesión en la GUI web de FMC, seleccione Devices>Device Management y haga clic en el botón Edit para acceder a su dispositivo de defensa contra amenazas. La página Interfaces está seleccionada de forma predeterminada. Haga clic en el botón Edit para la interfaz que desea editar, en este ejemplo GigabitEthernet0/0.



Edit Interface Gi0/0

En la ventana Edit Physical Interface, en la pestaña General:

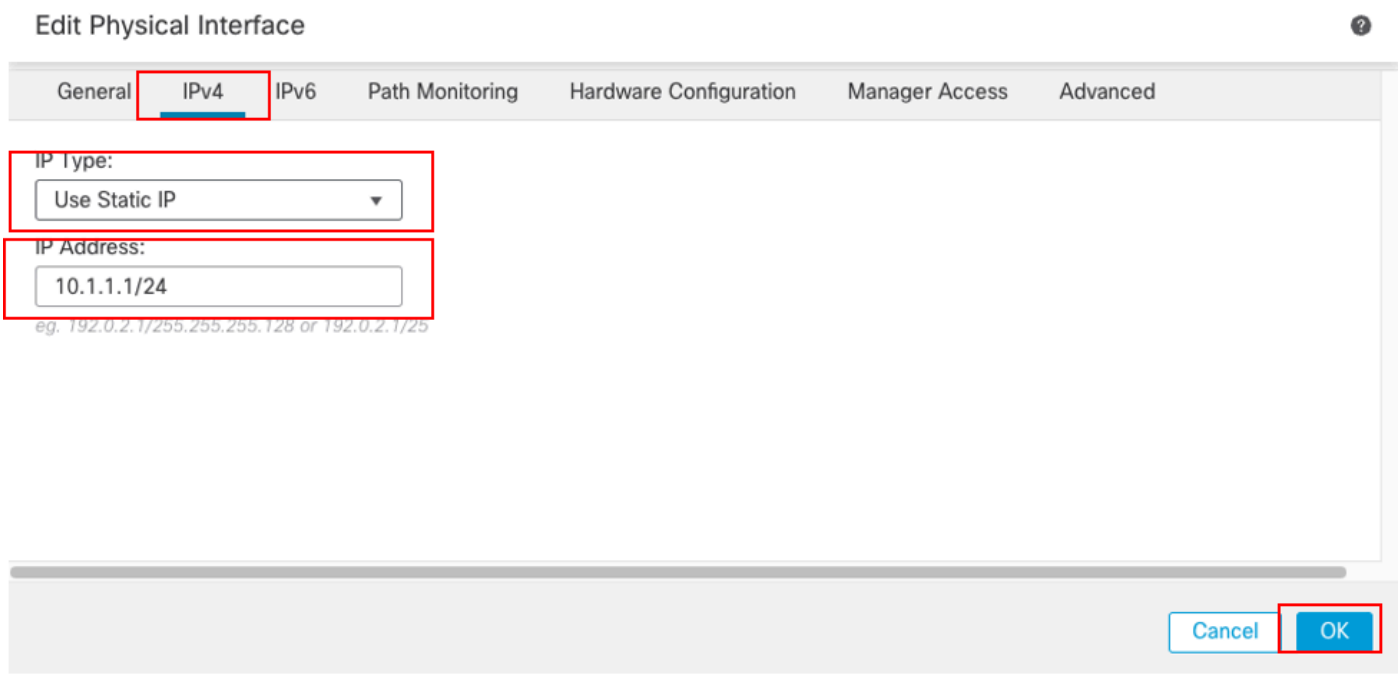
1. Establezca el Name, en este caso Outside1.
2. Active la interfaz marcando la casilla de verificación Enabled.
3. En la lista desplegable Security Zone, seleccione una zona de seguridad existente o cree una nueva, en este ejemplo Outside1_Zone.



Interfaz Gi0/0 General

En la pestaña IPv4:

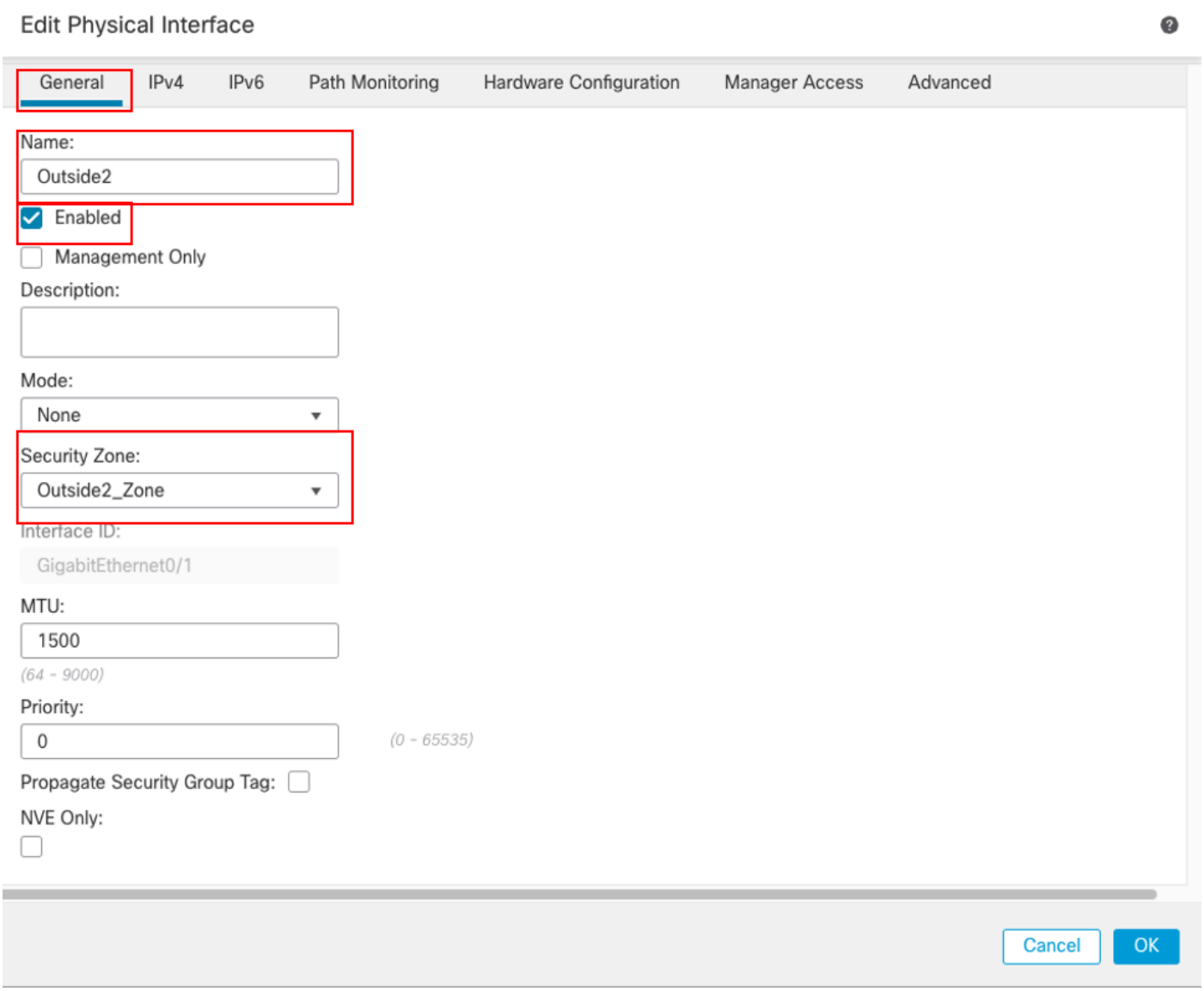
1. Elija una de las opciones de la lista desplegable IP Type, en este ejemplo Use Static IP.
2. Establezca la dirección IP, en este ejemplo 10.1.1.1/24.
3. Click OK.



Interfaz Gi0/0 IPv4

Repita un paso similar para configurar la interfaz GigabitEthernet0/1, en la ventana Edit Physical Interface, en la pestaña General:

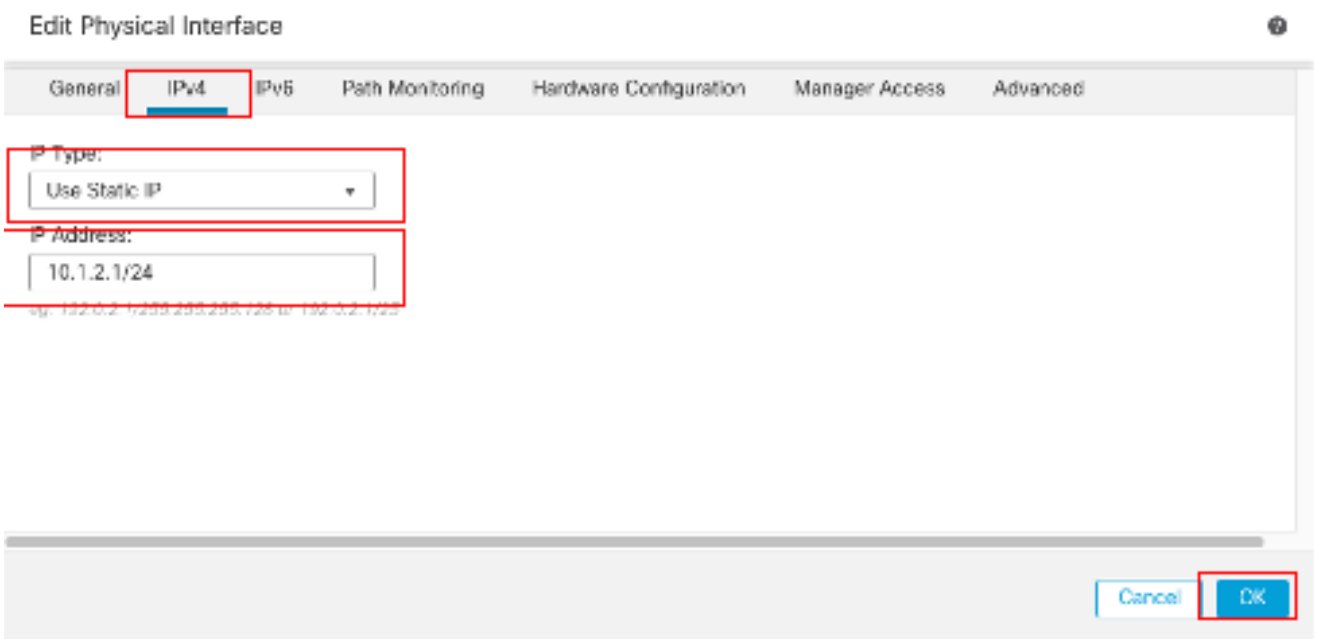
1. Establezca el Nombre, en este caso Outside2.
2. Active la interfaz marcando la casilla de verificación Enabled.
3. En la lista desplegable Security Zone, seleccione una zona de seguridad existente o cree una nueva, en este ejemplo Outside2_Zone.



Interfaz Gi0/1 General

En la pestaña IPv4:

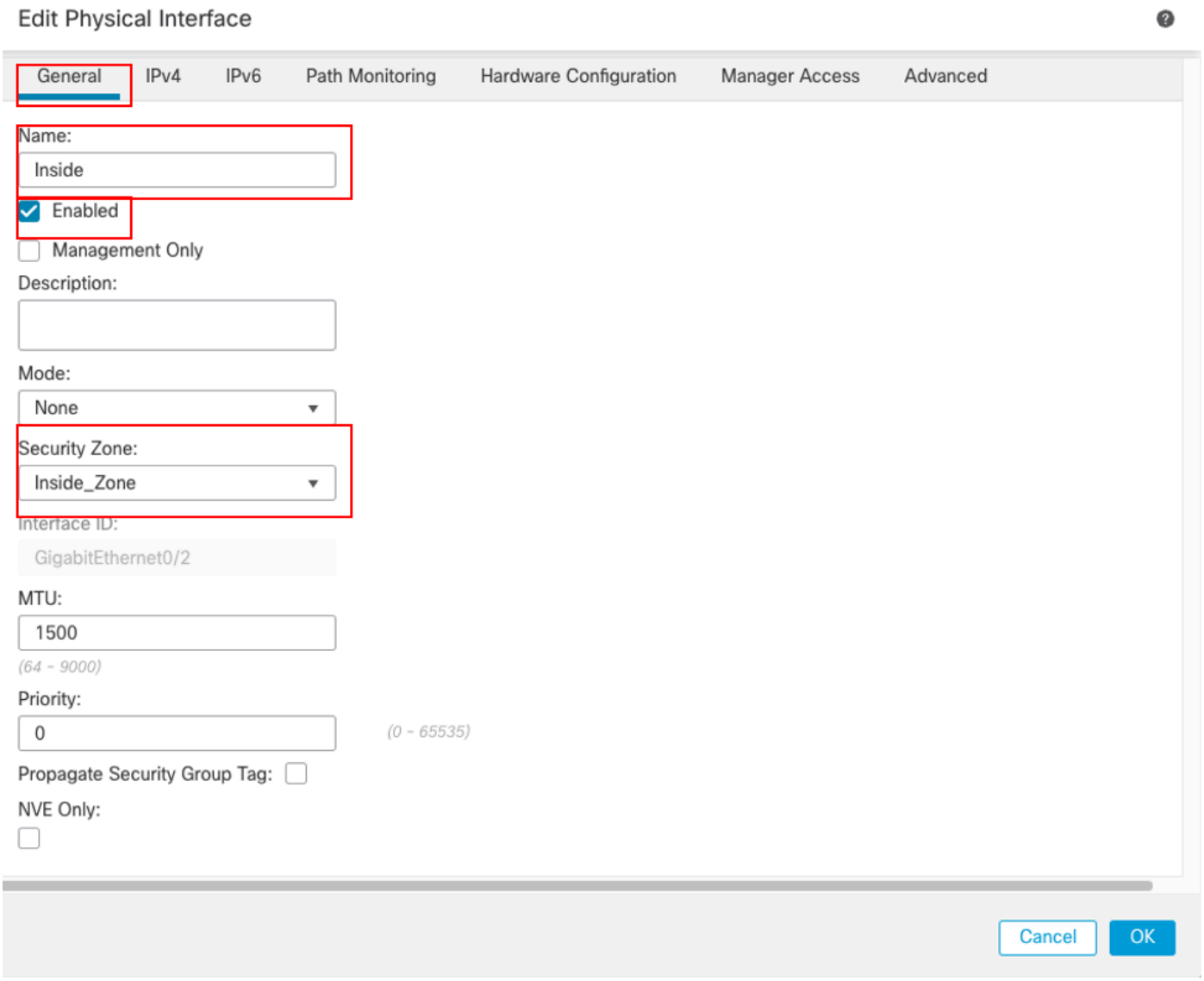
1. Elija una de las opciones de la lista desplegable IP Type, en este ejemplo Use Static IP.
2. Establezca la dirección IP, en este ejemplo 10.1.2.1/24.
3. Click OK.



Interfaz Gi0/1 IPv4

Repita un paso similar para configurar la interfaz GigabitEthernet0/2, en la ventana Edit Physical Interface, en la pestaña General:

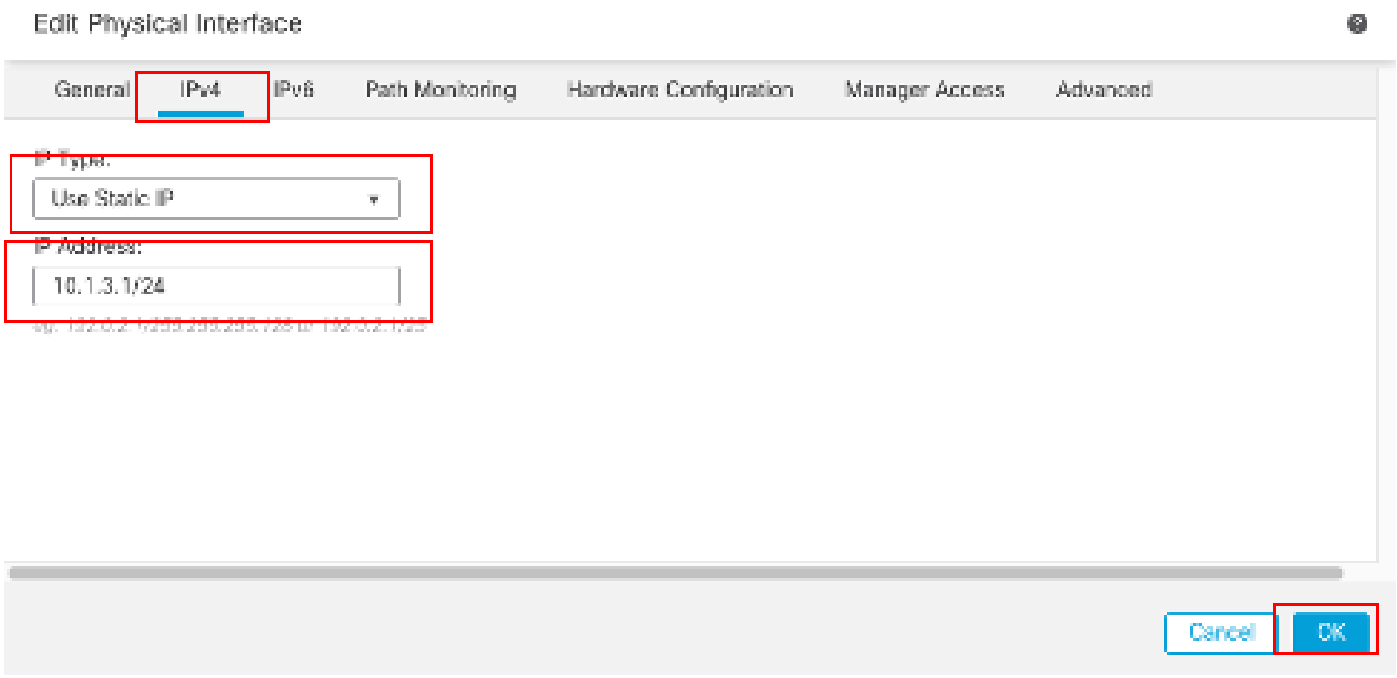
1. Establezca el Nombre, en este caso Dentro.
2. Active la interfaz marcando la casilla de verificación Enabled.
3. En la lista desplegable Security Zone, seleccione una zona de seguridad existente o cree una nueva, en este ejemplo Inside_Zone.



Interfaz Gi0/2 General

En la pestaña IPv4:

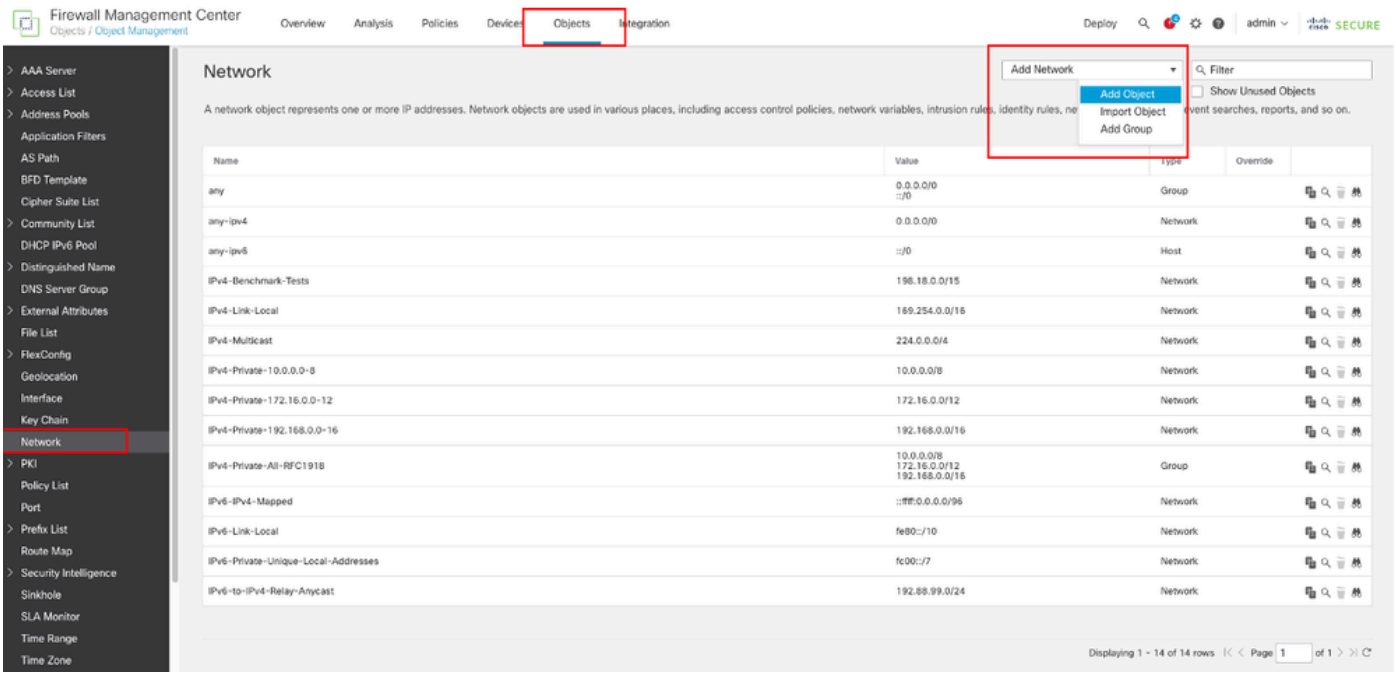
1. Elija una de las opciones de la lista desplegable IP Type, en este ejemplo Use Static IP.
2. Establezca la dirección IP, en este ejemplo 10.1.3.1/24.
3. Click OK.



Interfaz Gi0/2 IPv4

Haga clic en Guardar e Implementar la configuración.

Navegue hasta Objetos > Administración de objetos, elija Red de la lista de tipos de objeto, elija Agregar objeto del menú desplegable Agregar red para crear un objeto para la primera gateway ISP.

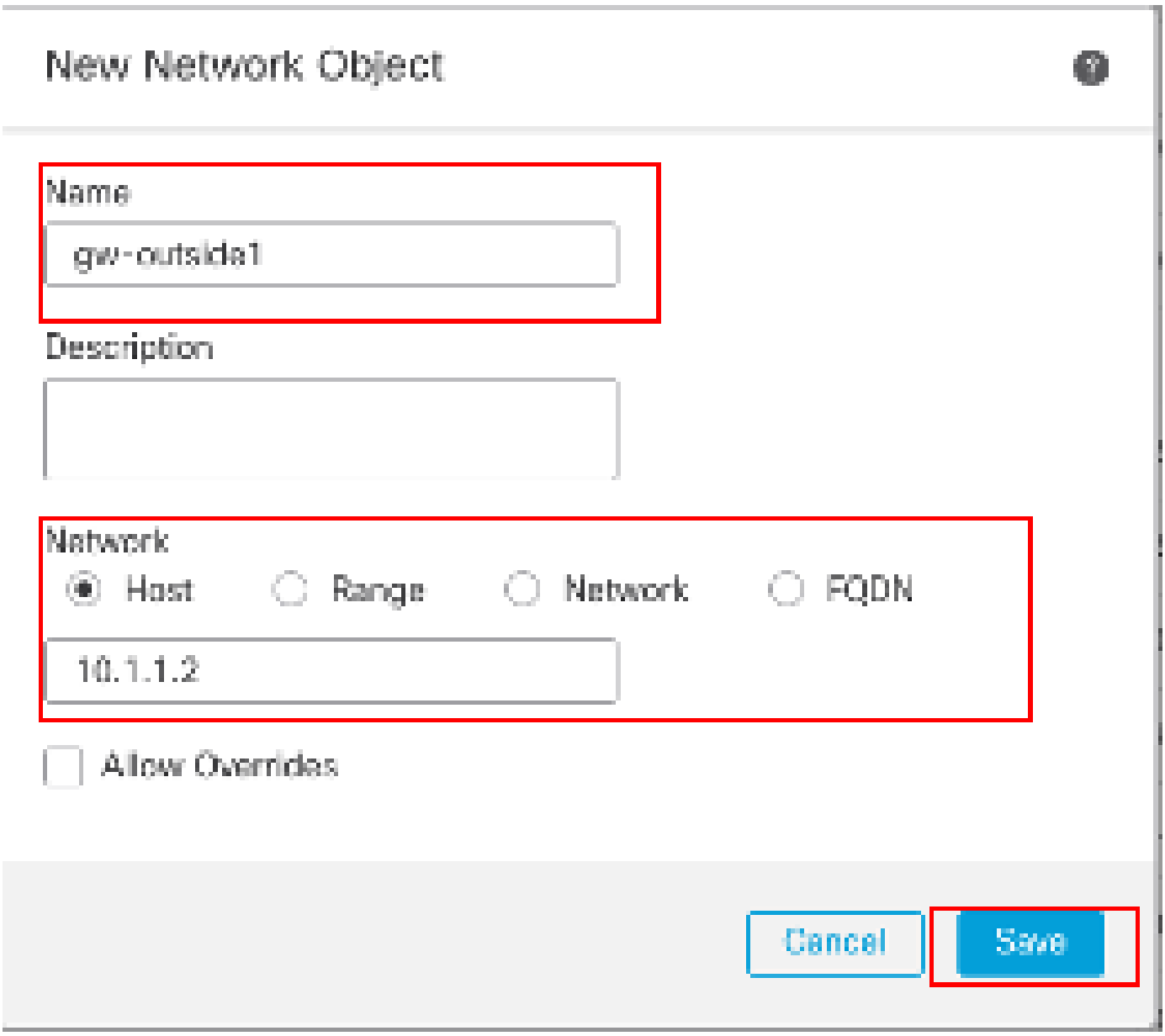


Objeto de red

En la ventana New Network Object:

1. Establezca el Name, en este ejemplo gw-outside1.
2. En el campo Network, seleccione la opción requerida e ingrese un valor apropiado, en este ejemplo Host y 10.1.1.2.

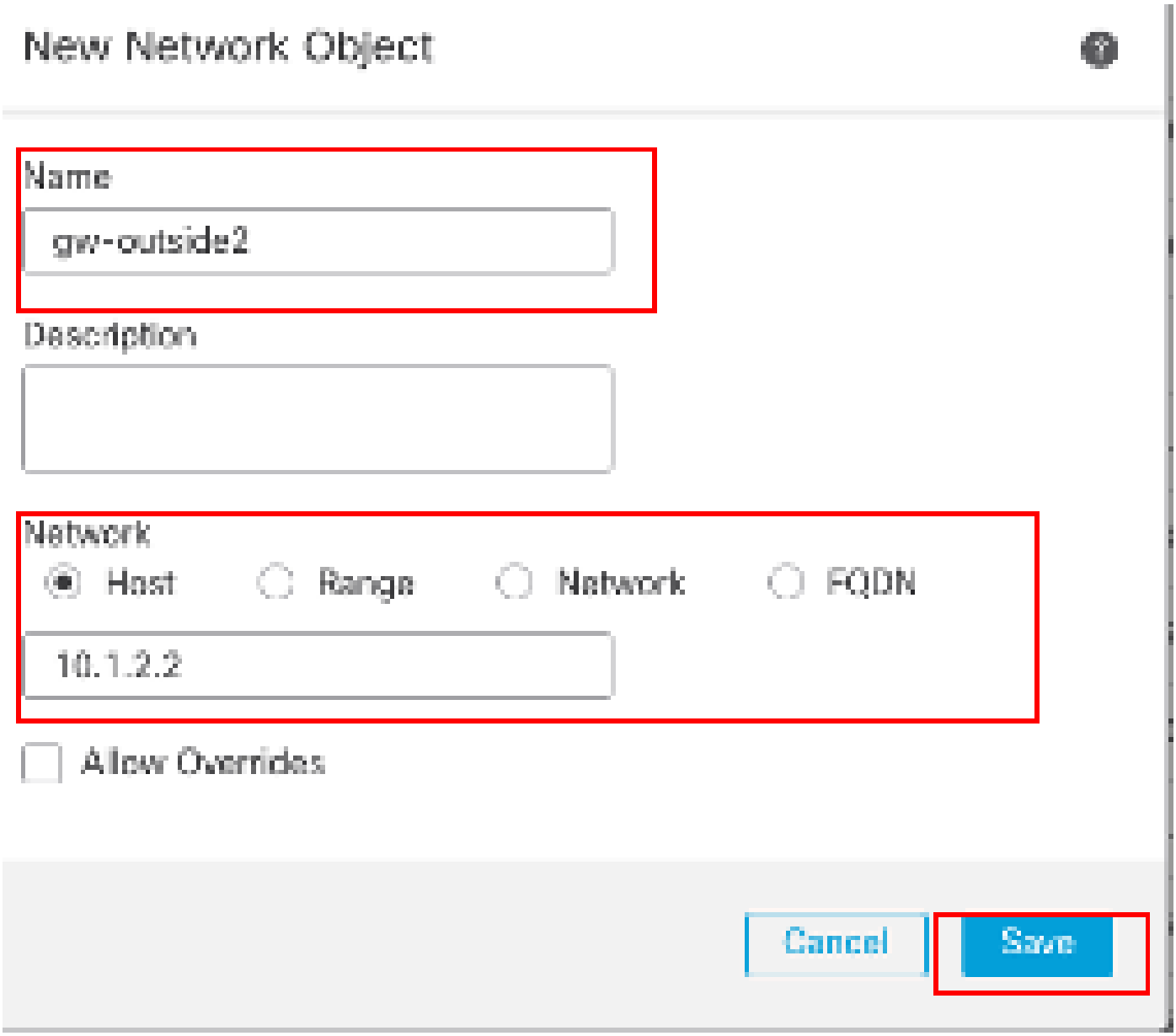
3. Click Save.



Objeto Gw-outside1

Repita pasos similares para crear otro objeto para la segunda puerta de enlace del ISP. En la ventana New Network Object:

1. Establezca el Name, en este ejemplo gw-outside2.
2. En el campo Network, seleccione la opción requerida e ingrese un valor apropiado, en este ejemplo Host y 10.1.2.2.
3. Click Save.

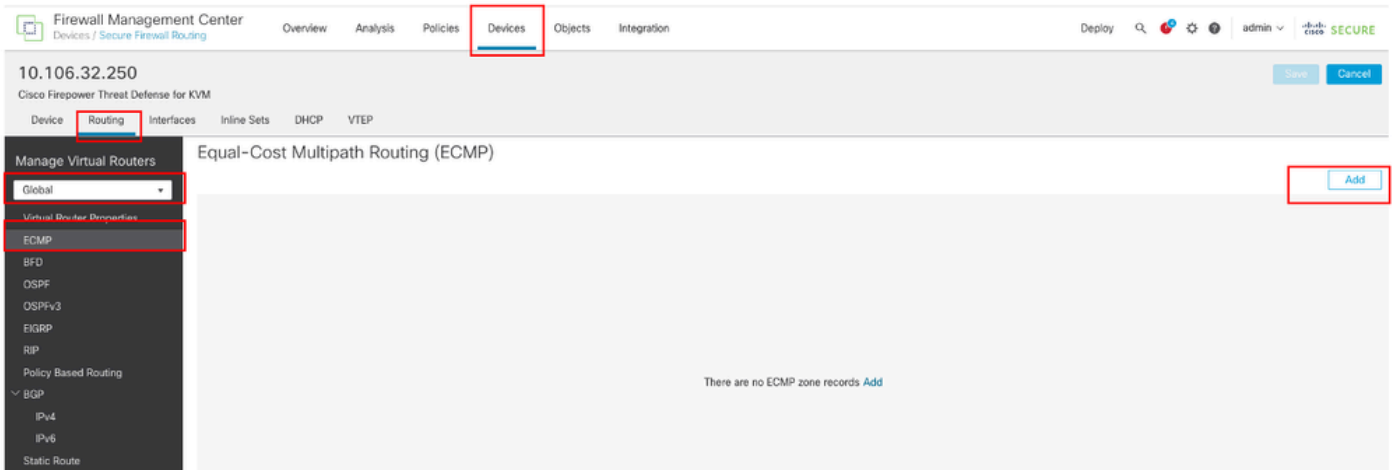


Objeto Gw-outside2

Paso 1. Configuración de la zona ECMP

Navegue hasta Devices > Device Management y edite el dispositivo de defensa contra amenazas, haga clic en Routing. En la lista desplegable router virtual, seleccione el router virtual en el que desea crear la zona ECMP. Puede crear zonas ECMP en routers virtuales globales y routers virtuales definidos por el usuario. En este ejemplo, elija Global.

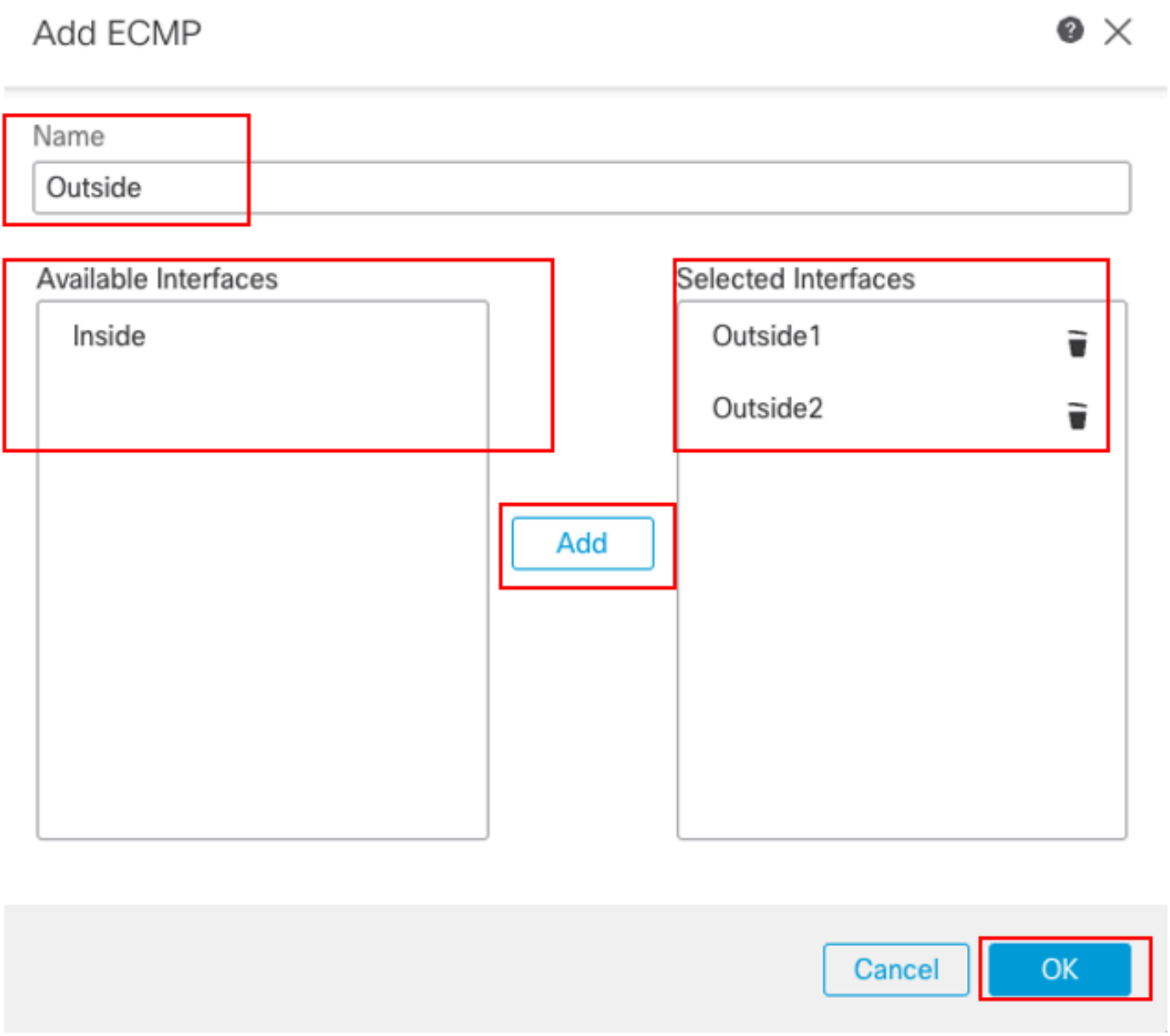
Haga clic en ECMP y, a continuación, en Agregar.



Configuración de la zona ECMP

En la ventana Add ECMP:

1. Establezca Name para la zona ECMP, en este ejemplo Outside.
2. Para asociar interfaces, seleccione la interfaz en el cuadro Interfaces disponibles y, a continuación, haga clic en Agregar. En este ejemplo, Outside1 y Outside2.
3. Click OK.

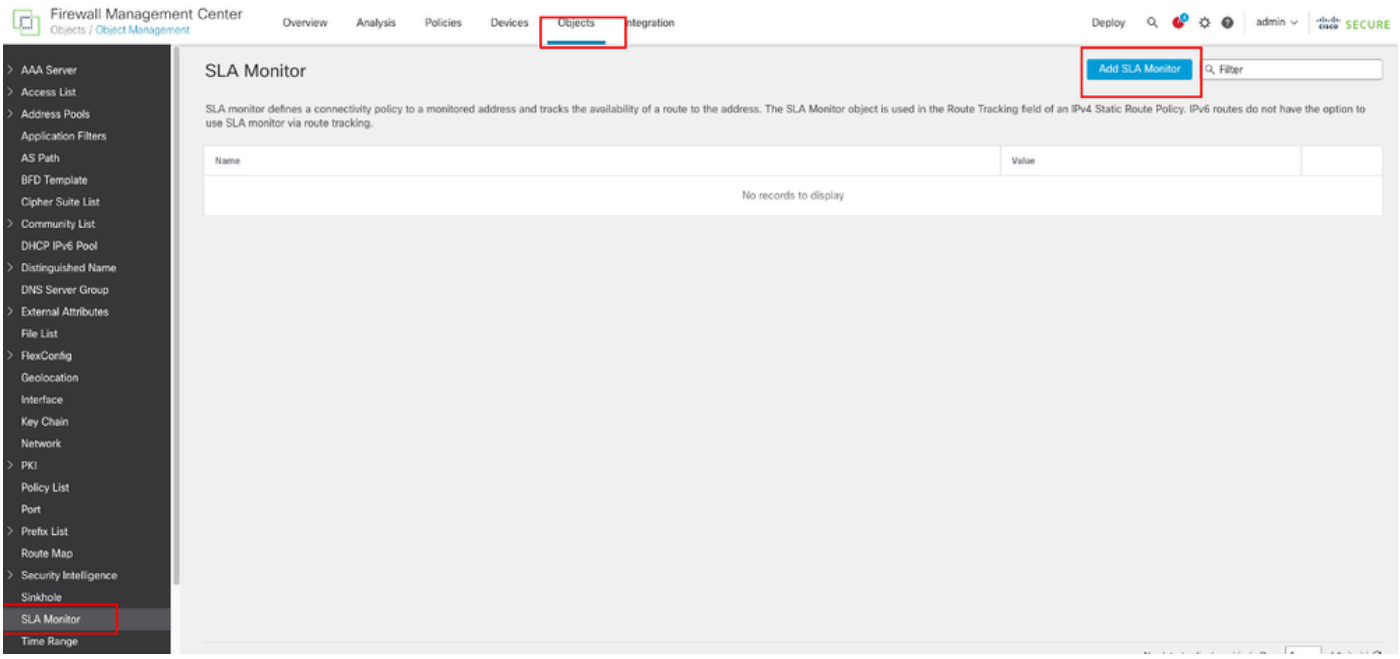


Configuración de la zona ECMP externa

Haga clic en Guardar e Implementar la configuración.

Paso 2. Configurar objetos de SLA de IP

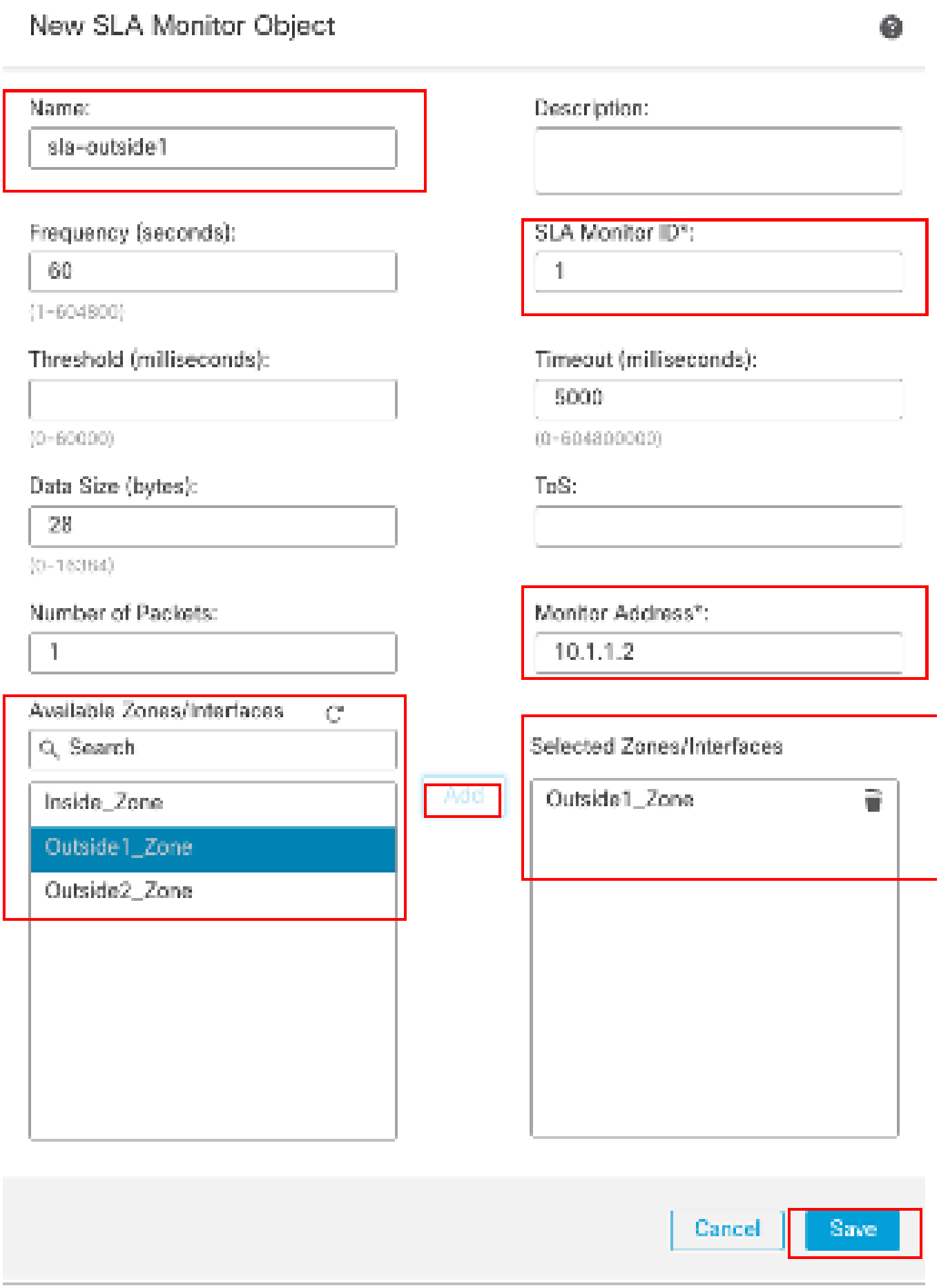
Navegue hasta Objetos > Gestión de Objetos, Elija SLA Monitor de la lista de tipos de objetos, Haga clic en Agregar SLA Monitor para agregar un nuevo SLA monitor para el primer gateway ISP.



Crear supervisión de SLA

En la ventana New SLA Monitor Object:

1. Establezca el Nombre para el objeto de monitoreo SLA, en este caso sla-outside1.
2. Ingrese el número de ID de la operación SLA en el campo SLA Monitor ID. Los valores varían entre 1 y 2147483647. Puede crear un máximo de 2000 operaciones de SLA en un dispositivo. Cada número de ID debe ser único para la política y la configuración del dispositivo. En este ejemplo 1.
3. Ingrese la dirección IP que está siendo monitoreada para disponibilidad por la operación SLA, en el campo Dirección Monitoreada. En este ejemplo, 10.1.1.2.
4. La lista Zonas/Interfaces Disponibles muestra las zonas y los grupos de interfaces. En la lista Zonas/Interfaces, agregue las zonas o grupos de interfaces que contienen las interfaces a través de las cuales el dispositivo se comunica con la estación de administración. Para especificar una única interfaz, debe crear una zona o los grupos de interfaz para la interfaz. En este ejemplo, Outside1_Zone.
5. Click Save.

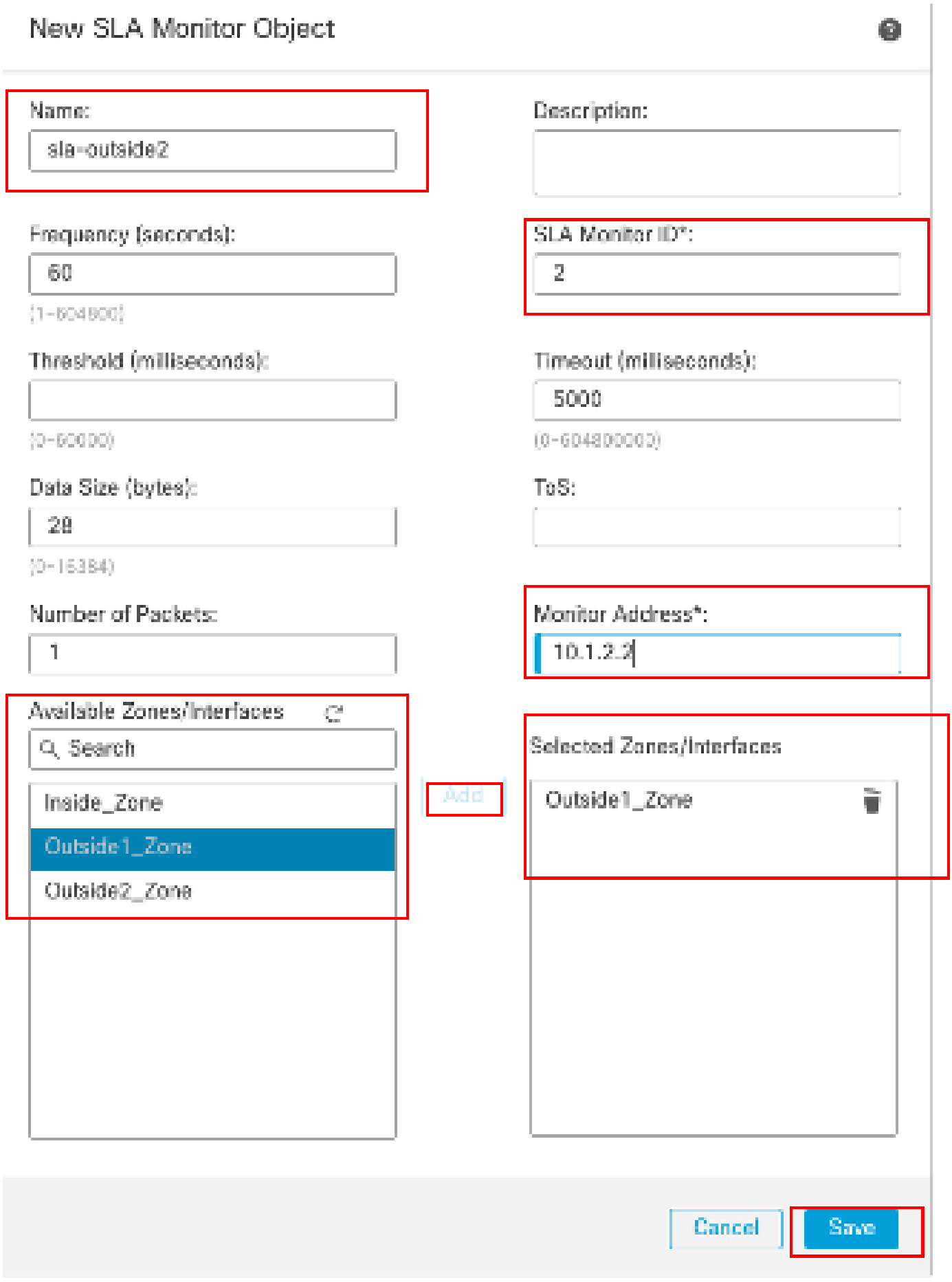


SLA Object Sla-outside1

Repita pasos similares para crear otro monitor de SLA para el segundo gateway del ISP.

En la ventana New SLA Monitor Object:

1. Establezca el Nombre para el objeto de monitoreo SLA, en este caso sla-outside2.
2. Ingrese el número de ID de la operación SLA en el campo SLA Monitor ID. Los valores varían entre 1 y 2147483647. Puede crear un máximo de 2000 operaciones de SLA en un dispositivo. Cada número de ID debe ser único para la política y la configuración del dispositivo. En este ejemplo 2.
3. Ingrese la dirección IP que está siendo monitoreada para disponibilidad por la operación SLA, en el campo Dirección Monitoreada. En este ejemplo 10.1.2.2.
4. La lista Zonas/Interfaces Disponibles muestra las zonas y los grupos de interfaces. En la lista Zonas/Interfaces, agregue las zonas o grupos de interfaces que contienen las interfaces a través de las cuales el dispositivo se comunica con la estación de administración. Para especificar una única interfaz, debe crear una zona o los grupos de interfaz para la interfaz. En este ejemplo, Outside2_Zone.
5. Click Save.

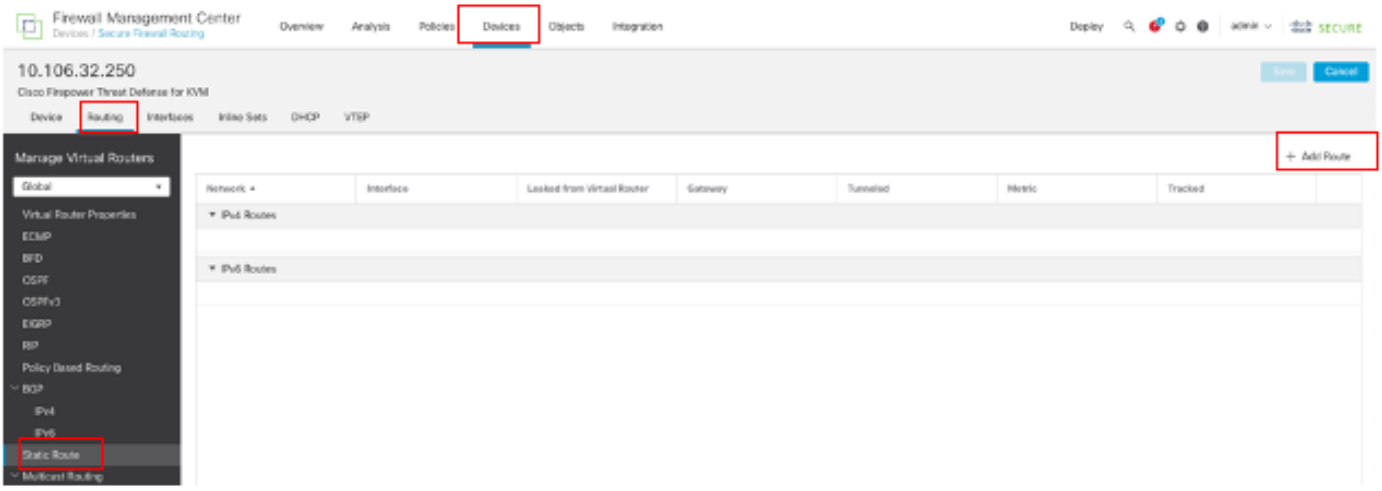


SLA Object Sla-outside2

Paso 3. Configuración de Rutas Estáticas con Route Track

Navegue hasta Devices > Device Management, y edite el dispositivo de defensa contra amenazas, haga clic en Routing, En la lista desplegable routers virtuales, seleccione el router virtual para el cual está configurando una ruta estática. En este ejemplo, Global.

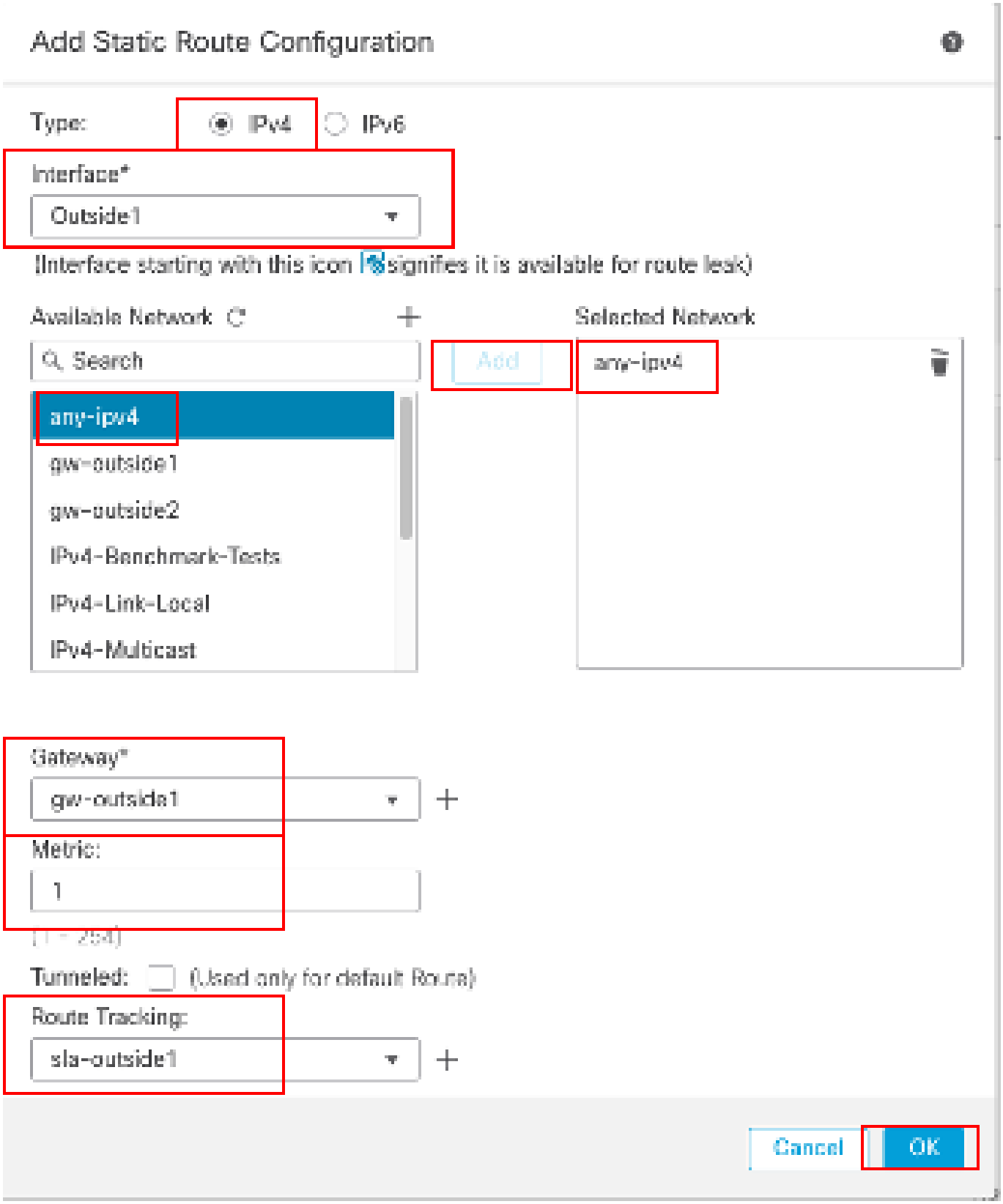
Seleccione Static Route, haga clic en Add Route para agregar la ruta predeterminada a la primera gateway ISP.



Configurar ruta estática

En la ventana Add Static Route Configuration:

1. Haga clic en IPv4 o IPv6, según el tipo de ruta estática que esté agregando. En este ejemplo, IPv4.
2. Elija la Interfaz a la que se aplica esta ruta estática. En este ejemplo, Outside1.
3. En la lista Available Network, elija la red de destino. En este ejemplo any-ipv4.
4. En el campo Gateway o IPv6 Gateway, ingrese o elija el router de gateway que es el siguiente salto para esta ruta. Puede proporcionar una dirección IP o un objeto Networks/Hosts. En este ejemplo gw-outside1.
5. En el campo Metric, ingrese el número de saltos a la red de destino. Los valores válidos oscilan entre 1 y 255; el valor predeterminado es 1. En este ejemplo 1.
6. Para monitorear la disponibilidad de la ruta, ingrese o elija el nombre de un objeto Monitor de SLA que defina la política de monitoreo, en el campo Seguimiento de Ruta. En este ejemplo sla-outside1.
7. Click OK.

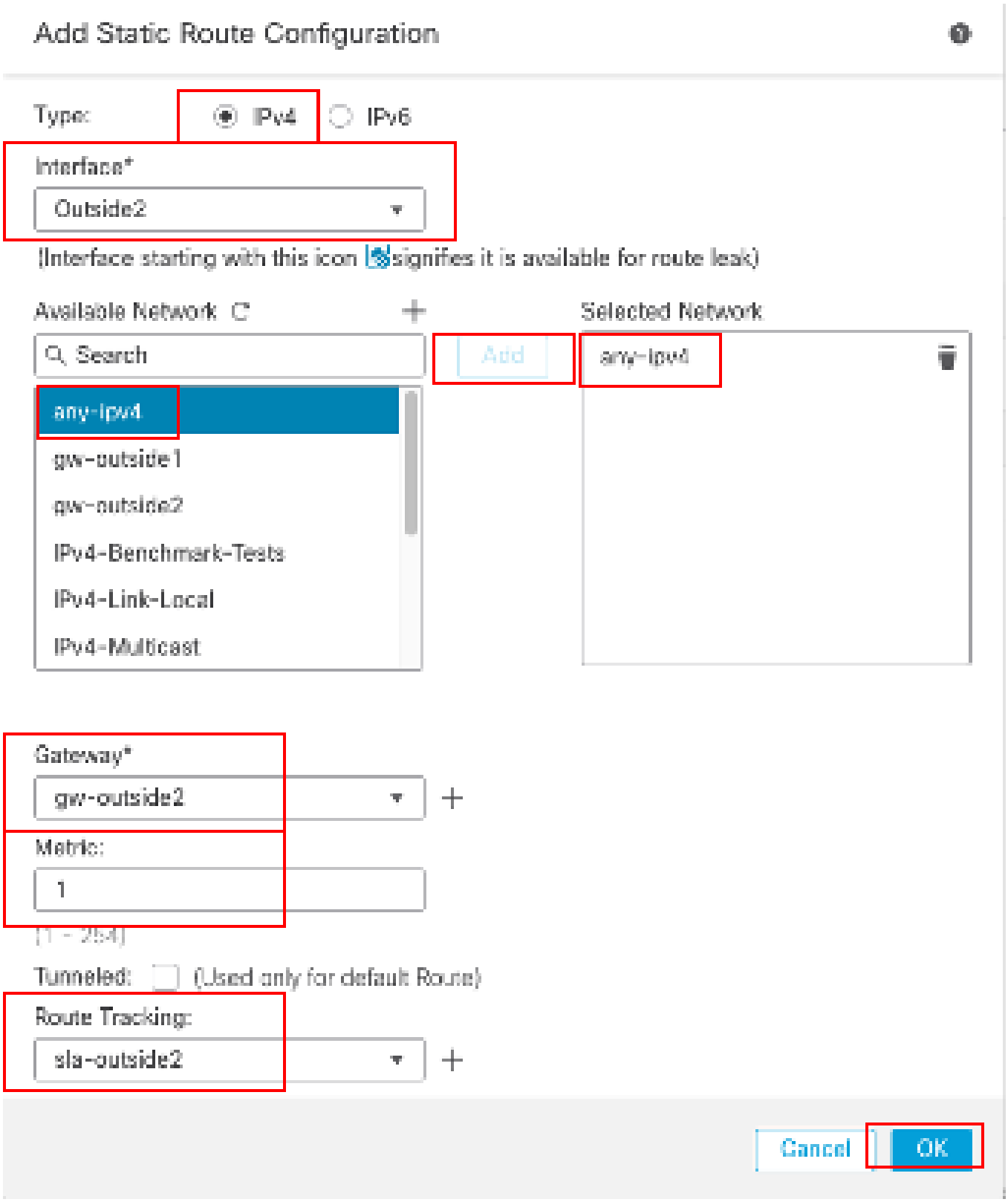


Agregar ISP de ruta estática primero

Repita pasos similares para agregar la ruta predeterminada a la segunda puerta de enlace del ISP. En la ventana Add Static Route Configuration:

1. Haga clic en IPv4 o IPv6, según el tipo de ruta estática que esté agregando. En este ejemplo, IPv4.
2. Elija la Interfaz a la que se aplica esta ruta estática. En este ejemplo Outside2.

3. En la lista Available Network, elija la red de destino. En este ejemplo any-ipv4.
4. En el campo Gateway o IPv6 Gateway, ingrese o elija el router de gateway que es el siguiente salto para esta ruta. Puede proporcionar una dirección IP o un objeto Networks/Hosts. En este ejemplo gw-outside2.
5. En el campo Metric, ingrese el número de saltos a la red de destino. Los valores válidos oscilan entre 1 y 255; el valor predeterminado es 1. Asegúrese de especificar la misma métrica que la primera ruta, en este ejemplo 1.
6. Para monitorear la disponibilidad de la ruta, ingrese o elija el nombre de un objeto Monitor de SLA que defina la política de monitoreo, en el campo Seguimiento de Ruta. En este ejemplo sla-outside2.
7. Click OK.



Agregar segundo ISP de ruta estática

Haga clic en Guardar e Implementar la configuración.

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 GigabitEthernet0/1

Outside1 GigabitEthernet0/0

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: 1
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: 2
```

```
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 "**Se agotó el tiempo de espera: FALSO**" en la salida del comando, lo 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: 1
Modification time: 09:31:28.785 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 82
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: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 2
Modification time: 09:31:28.785 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 82
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

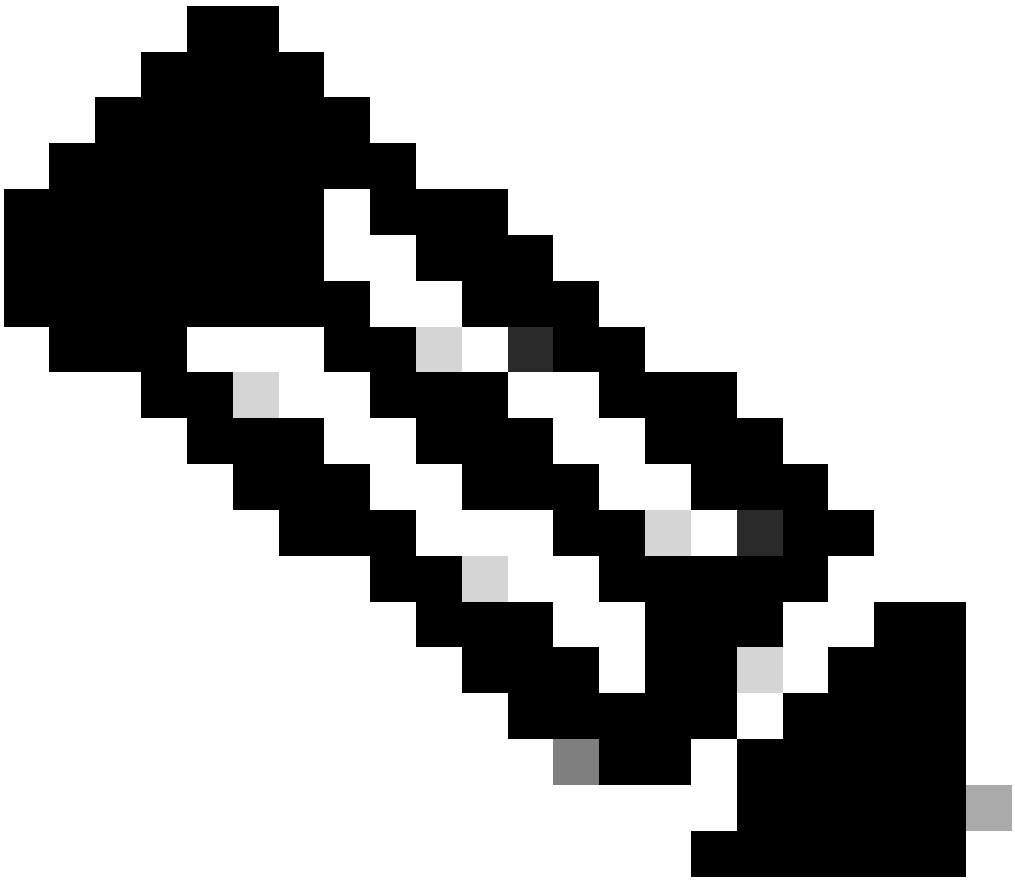
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

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 telnet desde Inside-Host1 (10.1.3.2) y Inside-Host2 (10.1.3.4) hacia Internet-Host (10.1.5.2), ejecute el comando **show conn** para confirmar que el tráfico está equilibrado de carga entre dos links ISP, Inside-Host1 (10.1.3.2) pasa a través de la interfaz outside1, Inside-Host2 (10.1.3.4) pasa a través de la interfaz outside2.

```
> show conn
2 in use, 3 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 2 most enabled, 0 most in effect

TCP Inside 10.1.3.2:46069 Outside1 10.1.5.2:23, idle 0:00:24, bytes 1329, flags UIO N1
TCP Inside 10.1.3.4:61915 Outside2 10.1.5.2:23, idle 0:00:04, bytes 1329, 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 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: 1
Modification time: 09:31:28.783 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 104
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: 11:14:28.813 UTC Thu Feb 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0 RTTMin: 0 RTTMax: 0
NumOfRTT: 0 RTTSum: 0 RTTSum2: 0

Entry number: 2
Modification time: 09:31:28.783 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
```

```
Number of operations attempted: 104
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: 11:14:28.813 UTC Thu Feb 15 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
```

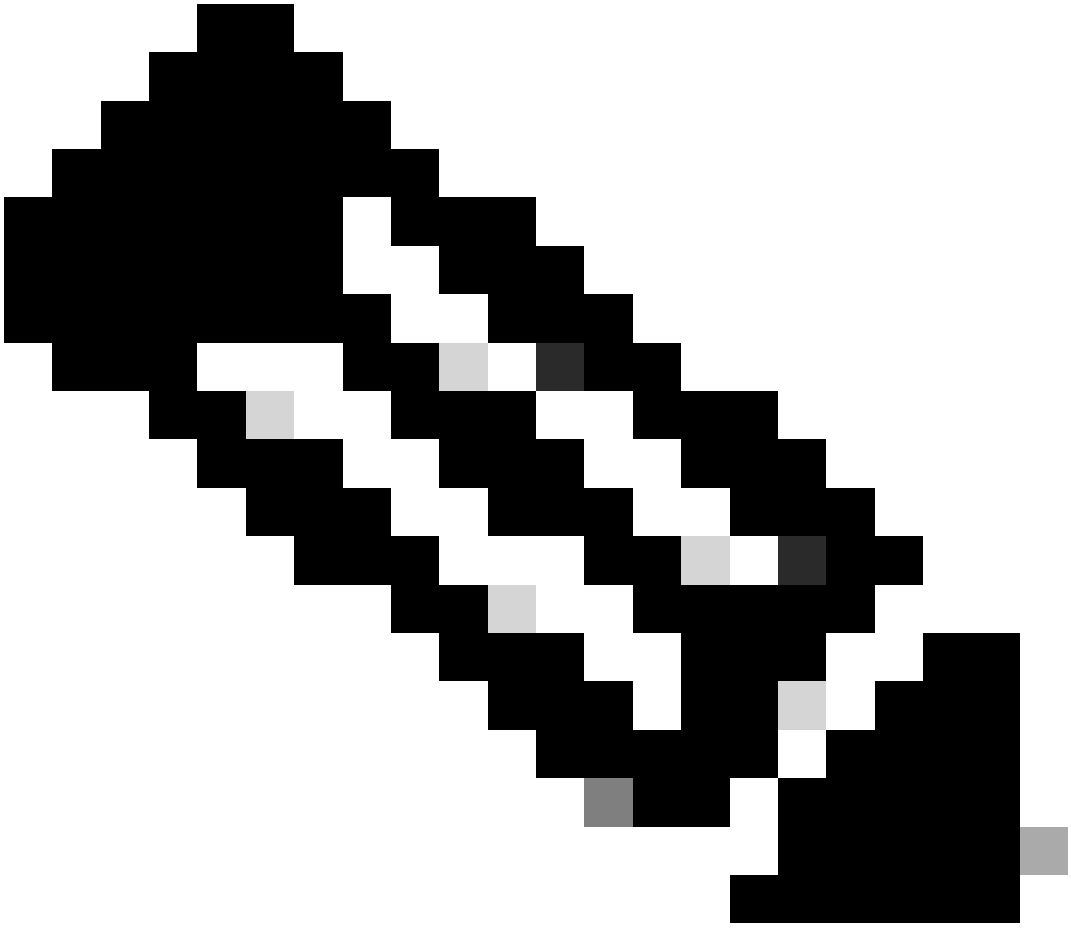
Ejecute el comando show conn , puede encontrar que las dos conexiones aún están activas. las sesiones telnet también están activas en Inside-Host1 (10.1.3.2) e Inside-Host2 (10.1.3.4) sin ninguna interrupción.

<#root>

```
> show conn
2 in use, 3 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 2 most enabled, 0 most in effect
```

```
TCP Inside 10.1.3.2:46069 Outside1 10.1.5.2:23, idle 0:00:22, bytes 1329, flags UIO N1
```

```
TCP Inside 10.1.3.4:61915 Outside2 10.1.5.2:23, idle 0:00:02, bytes 1329, flags UIO N1
```



Nota: Puede observar que en la salida de show conn , la sesión telnet de Inside-Host1 (10.1.3.2) sigue a través de la interfaz outside1, aunque la ruta por defecto a través de la interfaz outside1 se ha eliminado de la tabla de routing. Esto se espera y, por diseño, el tráfico real fluye a través de la interfaz outside2. Si inicia una nueva conexión desde Inside-Host1 (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
```

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.

<#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
```

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).