Implementar interfaz de datos redundante en Azure FTD administrado por CD-FMC

Contenido

Introducción

Este documento describe los pasos para configurar un FTD virtual gestionado por cdFMC para utilizar la función de interfaz de datos de acceso del administrador redundante.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Firewall Management Center
- Orquestador de defensa de Cisco

Componentes Utilizados

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

- Centro de gestión de firewall en la nube
- Virtual Secure Firewall Threat Defence versión 7.3.1 alojado en Azure Cloud.

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.

Productos Relacionados

Este documento también puede utilizarse con estas versiones de software y hardware:

- Cualquier dispositivo físico capaz de ejecutar Firepower Threat Defence versión 7.3.0 o superior.

Antecedentes

Este documento muestra los pasos para configurar y verificar un vFTD administrado por cdFMC para utilizar dos interfaces de datos con fines de administración. Esta función suele ser útil cuando los clientes necesitan una segunda interfaz de datos para administrar su FTD a través de Internet mediante un segundo ISP. De forma predeterminada, el FTD realiza un equilibrio de carga de ordenamiento cíclico para el tráfico de administración entre ambas interfaces; esto se puede modificar en una implementación de Active/Backup como se describe en este documento.

La interfaz de datos redundante para la función de gestión se introdujo en la versión 7.3.0 de Secure Firewall Threat Defence. Se da por supuesto que el vFTD tiene acceso a un servidor de nombres que puede resolver URL para el acceso a CDO.

Configuración

Diagrama de la red

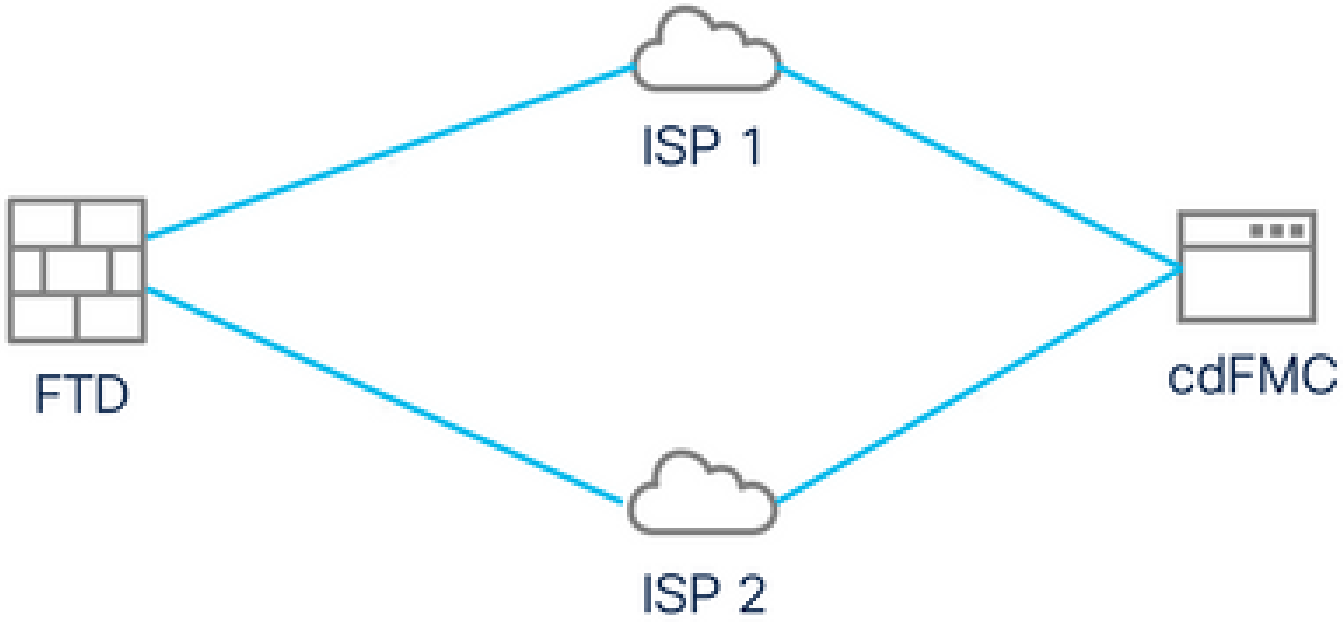


Diagrama de la red

Configuración de una interfaz de datos para el acceso a la gestión

Inicie sesión en el dispositivo a través de la consola y configure una de las interfaces de datos para el acceso a la administración con el comando configure network management-data-interface:

<#root>

>

configure network management-data-interface

**Note: The Management default route will be changed to route through the data interfaces. If you are conn
interface with SSH, your connection may drop. You must reconnect using the console port.**

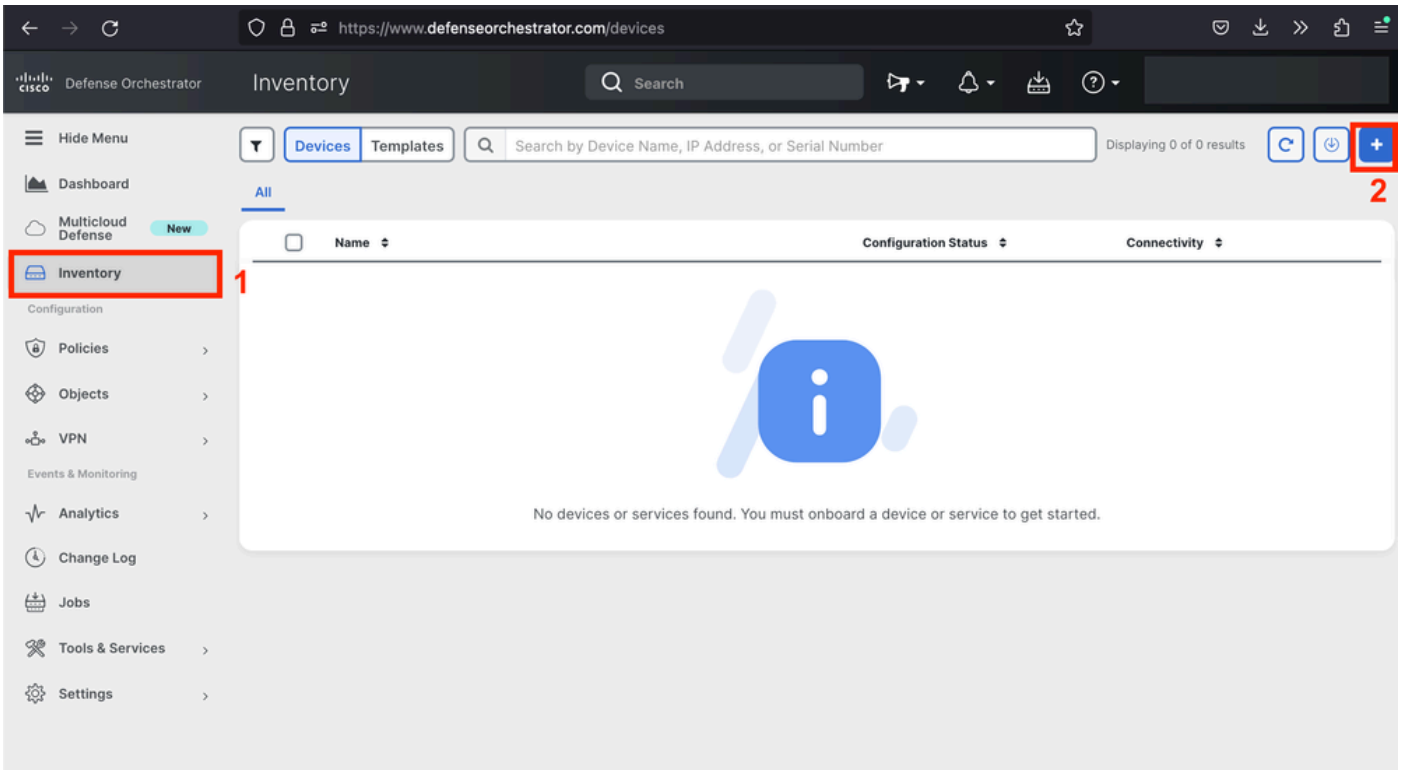
```
Data interface to use for management:

GigabitEthernet0/0

Specify a name for the interface [outside]:

outside-1

IP address (manual / dhcp) [dhcp]:

manual

IPv4/IPv6 address:

10.6.2.4

Netmask/IPv6 Prefix:

 255.255.255.0

Default Gateway:

10.6.2.1
```

Tenga en cuenta que la interfaz de administración original no se puede configurar para utilizar DHCP. Puede utilizar el comando show network para verificar esto.

Incorporación del FTD con CDO

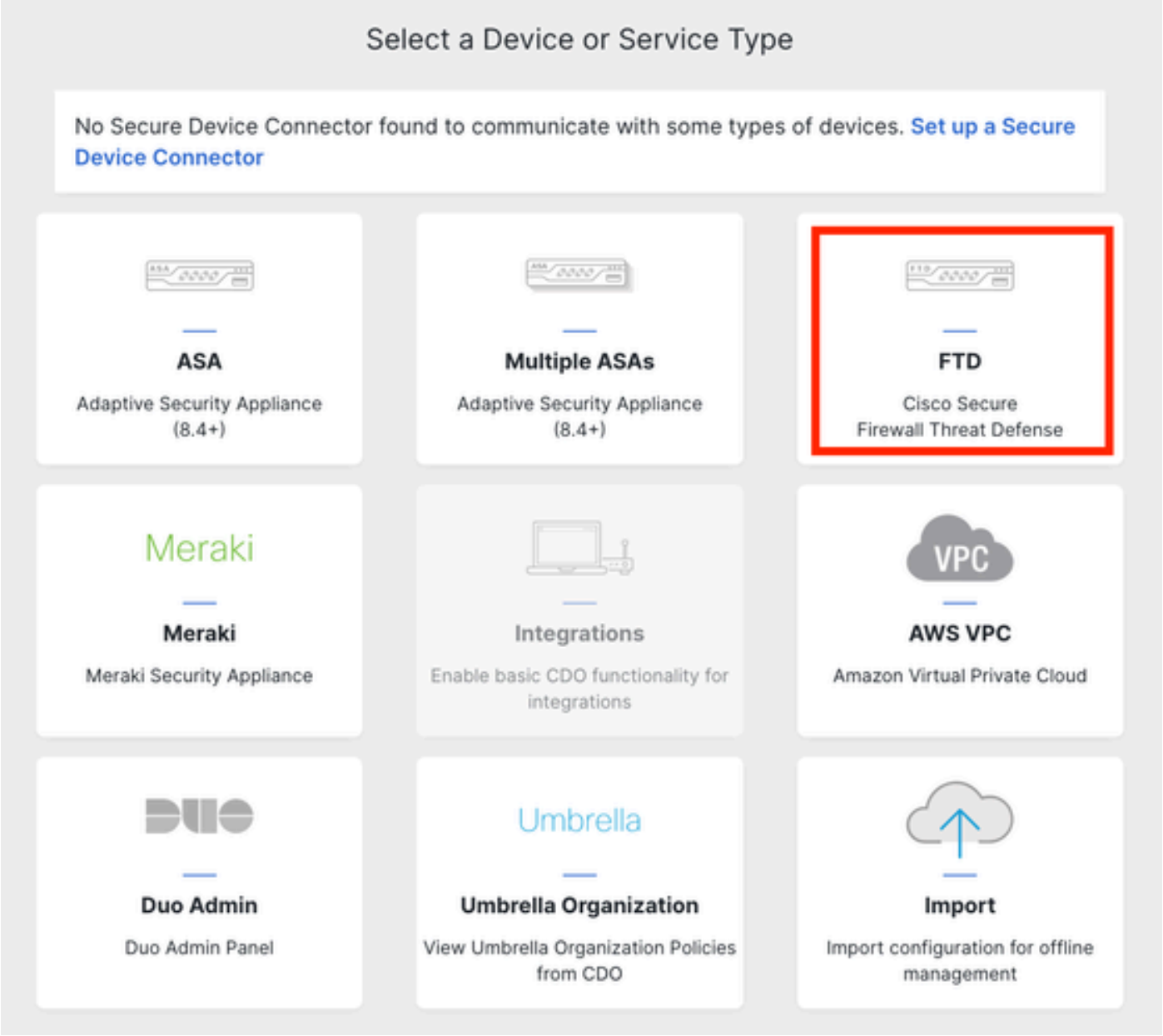
Este proceso incorpora el FTD de Azure con CDO para que pueda ser administrado por un FMC proporcionado en la nube. El proceso utiliza una clave de registro CLI, lo que resulta útil si el dispositivo tiene una dirección IP asignada mediante DHCP. Otros métodos de incorporación, como el aprovisionamiento mediante la función de registro táctil y los números de serie, solo se admiten en las plataformas Firepower 1000, Firepower 2100 o Secure Firewall 3100.

Paso 1. En el portal de CDO, navegue hasta Inventario y luego haga clic en la opción Onboard:



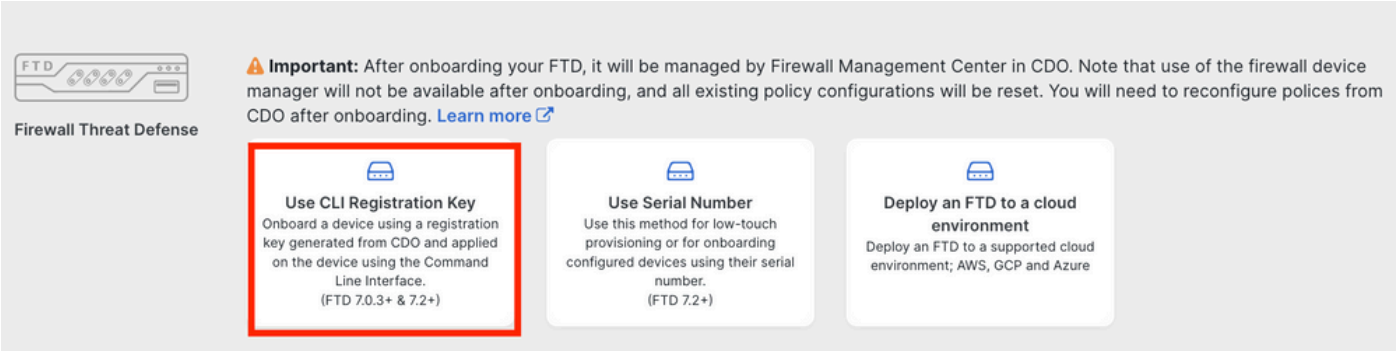
Página Inventario

Paso 2. Haga clic en el cuadro FTD:



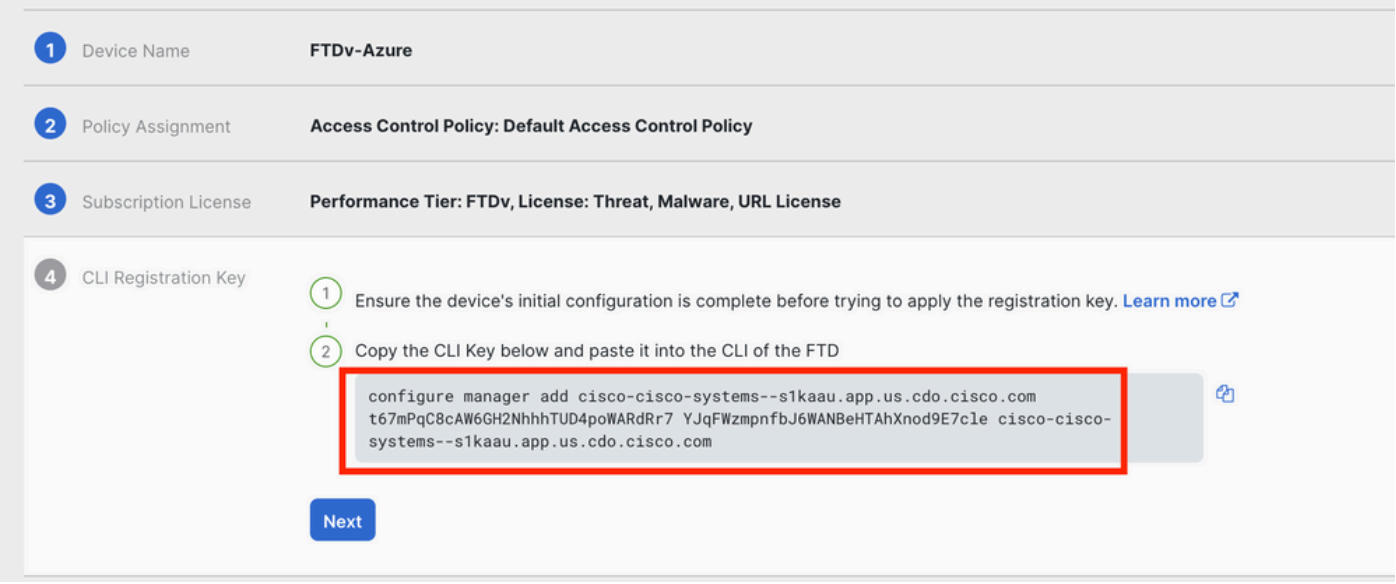
Incorporación del FTD

Paso 3. Elija la opción Use CLI Registration key:

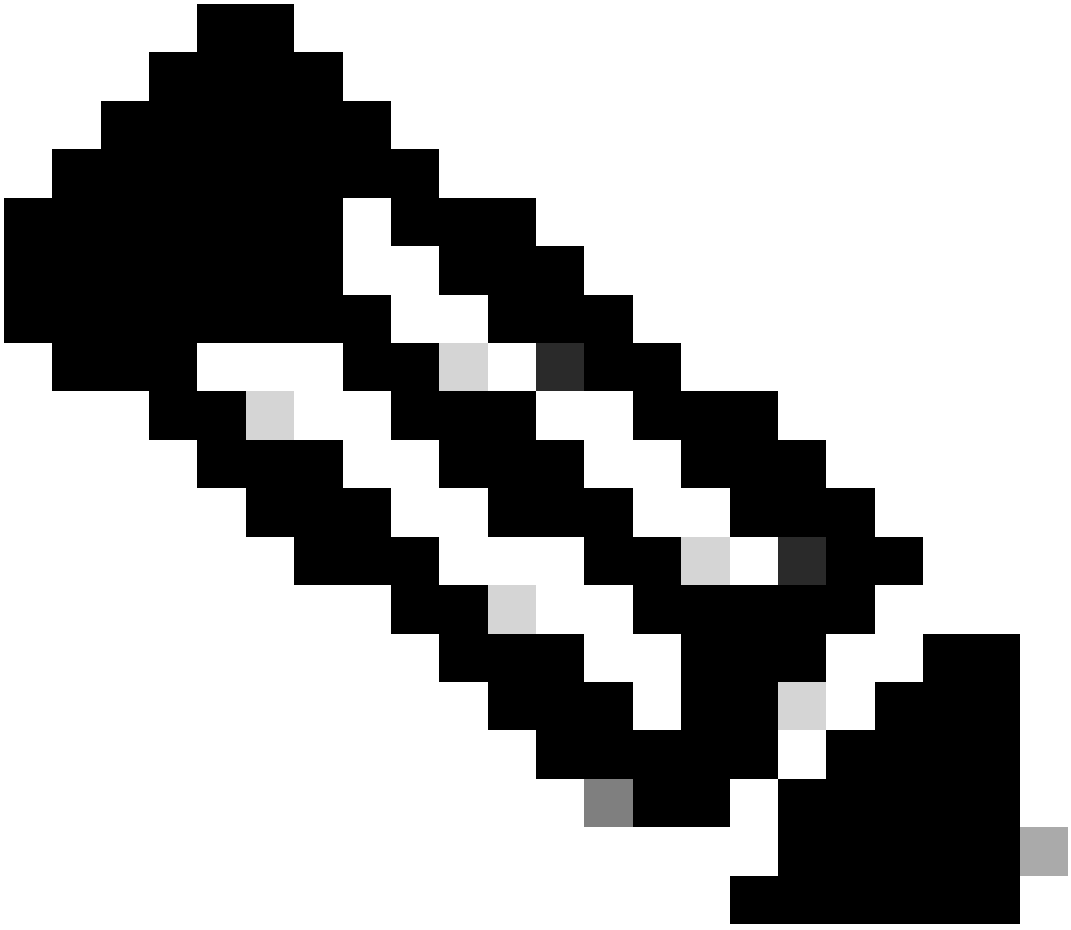


Utilizar la clave de registro de CLI

Paso 4. Copie la clave CLI a partir del comando configure manager:



Copiar comando de Configure Manager



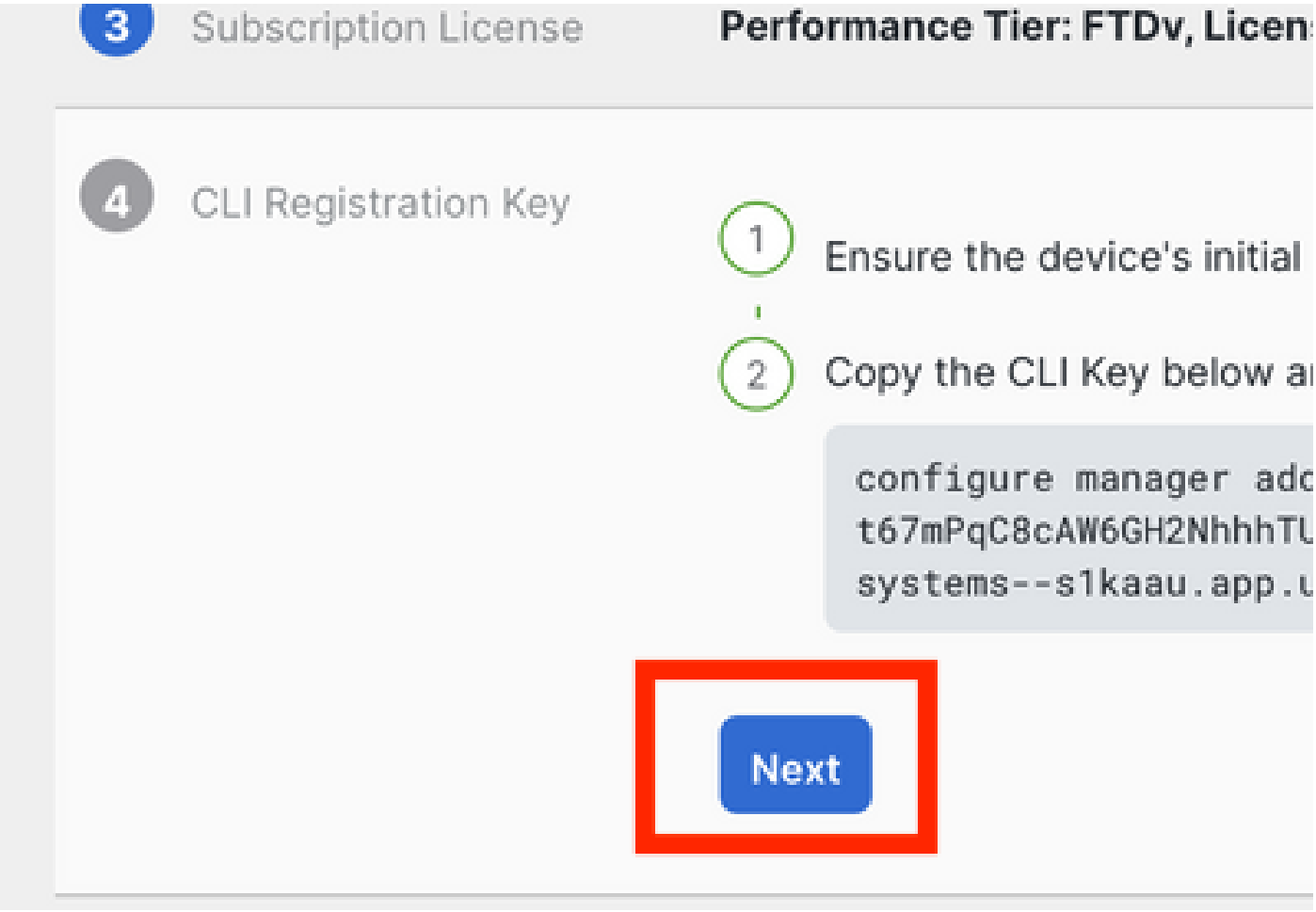
Nota: La clave de CLI coincide con el formato utilizado en los registros de FTD con FMC

en las instalaciones, donde puede configurar un ID de NAT para permitir el registro cuando el dispositivo administrado está detrás de un dispositivo NAT: configure manager add <fmc-hostname-or-ipv4> <registration-key> <nat-id> <display-name>

Paso 5. Pegue el comando en la CLI de FTD. Debe recibir este mensaje si la comunicación se ha realizado correctamente:

```
Manager cisco-cisco-systems--s1kaau.app.us.cdo.cisco.com successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

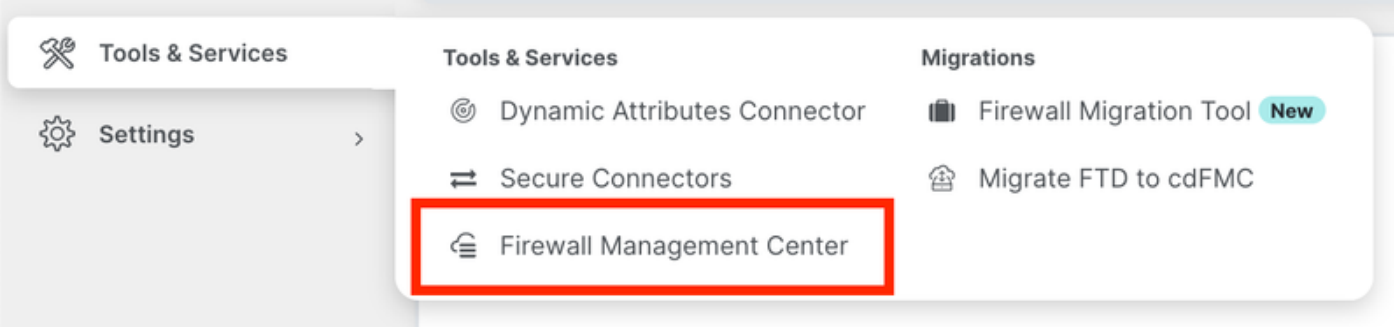
Paso 6. Vuelva al CDO y haga clic en Next:



Haga clic en Next (Siguiente)

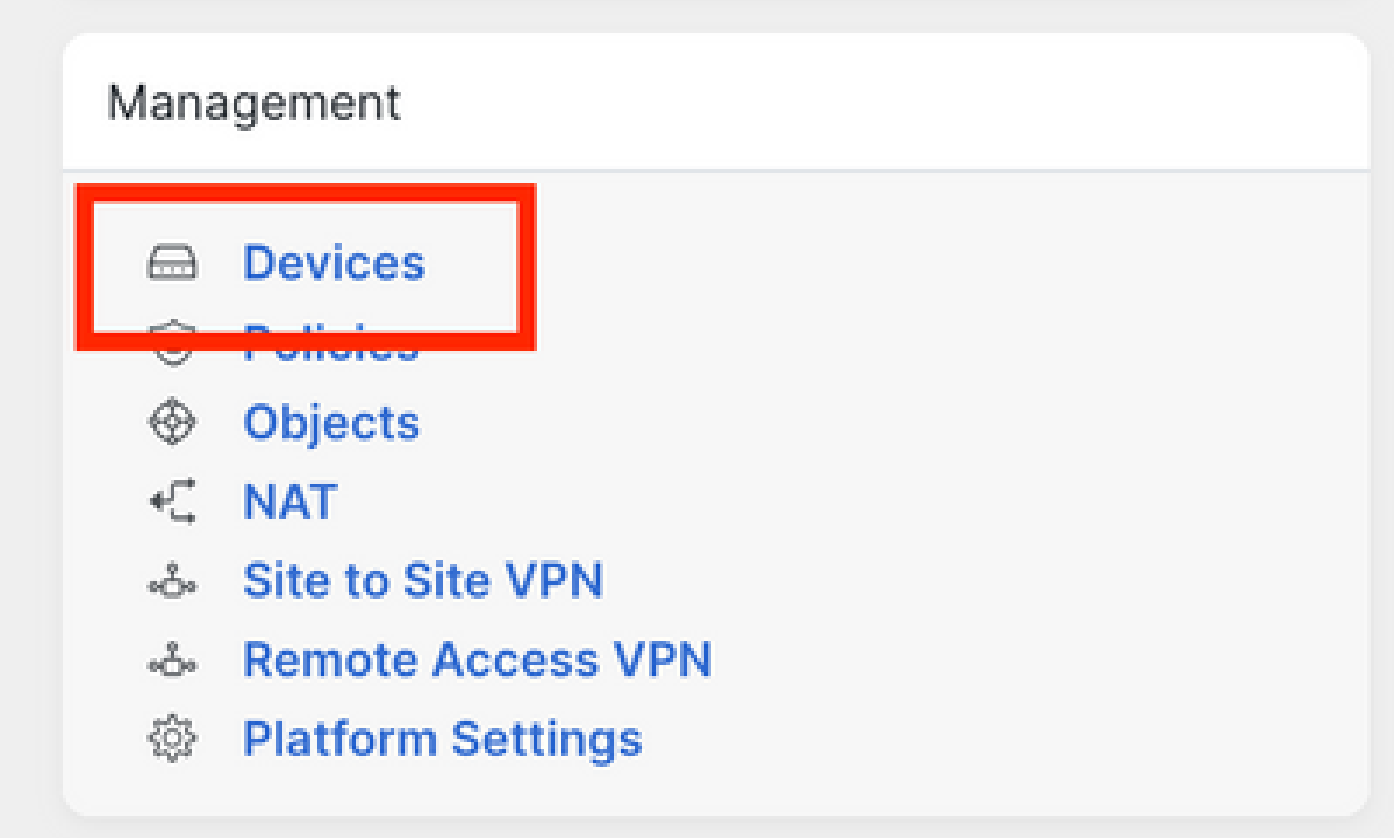
CDO continúa el proceso de inscripción y se muestra un mensaje que indica que tardará mucho tiempo en completarse. Puede comprobar el estado del proceso de inscripción haciendo clic en el enlace Devices de la página Services.

Paso 7. Acceda a su CSP a través de la página Herramientas y servicios.



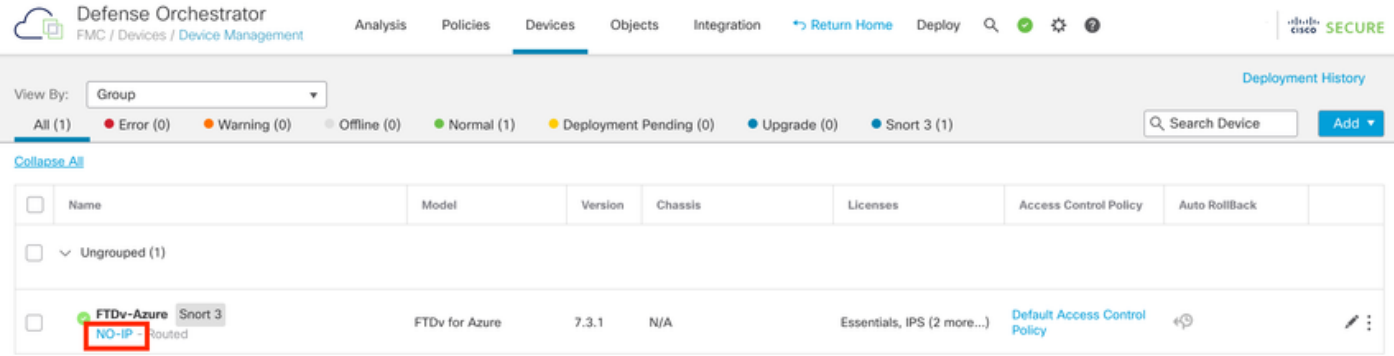
Acceso al cdFMC

Haga clic en el enlace Devices.



Haga clic en Dispositivos

Su FTD está ahora incorporado en CDO y puede ser gestionado por el FMC proporcionado en la nube. Observe en la siguiente imagen que aparece un NO-IP bajo el nombre del dispositivo. Esto se espera en un proceso de onboarding usando la clave de registro CLI.

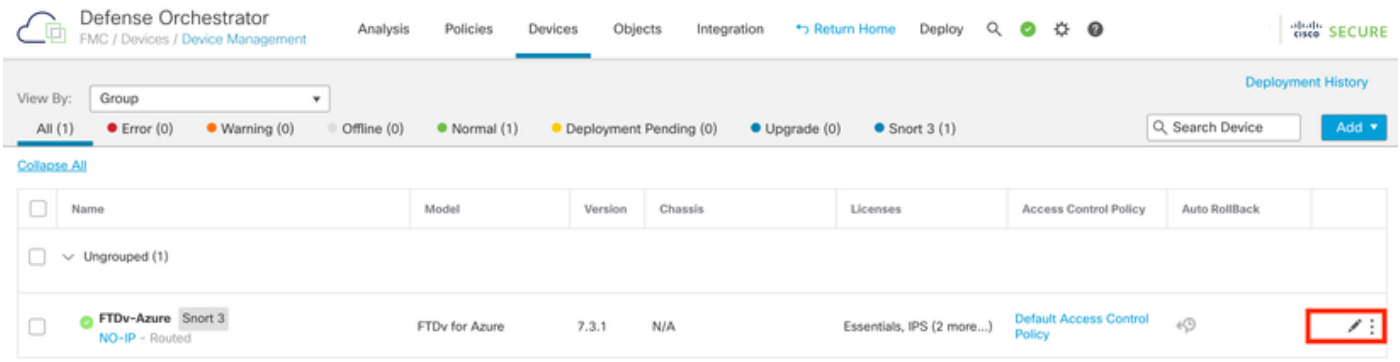


FTD gestionado

Configuración de una interfaz de datos redundante para el acceso del administrador

Este proceso asigna una segunda interfaz de datos para el acceso a la administración.

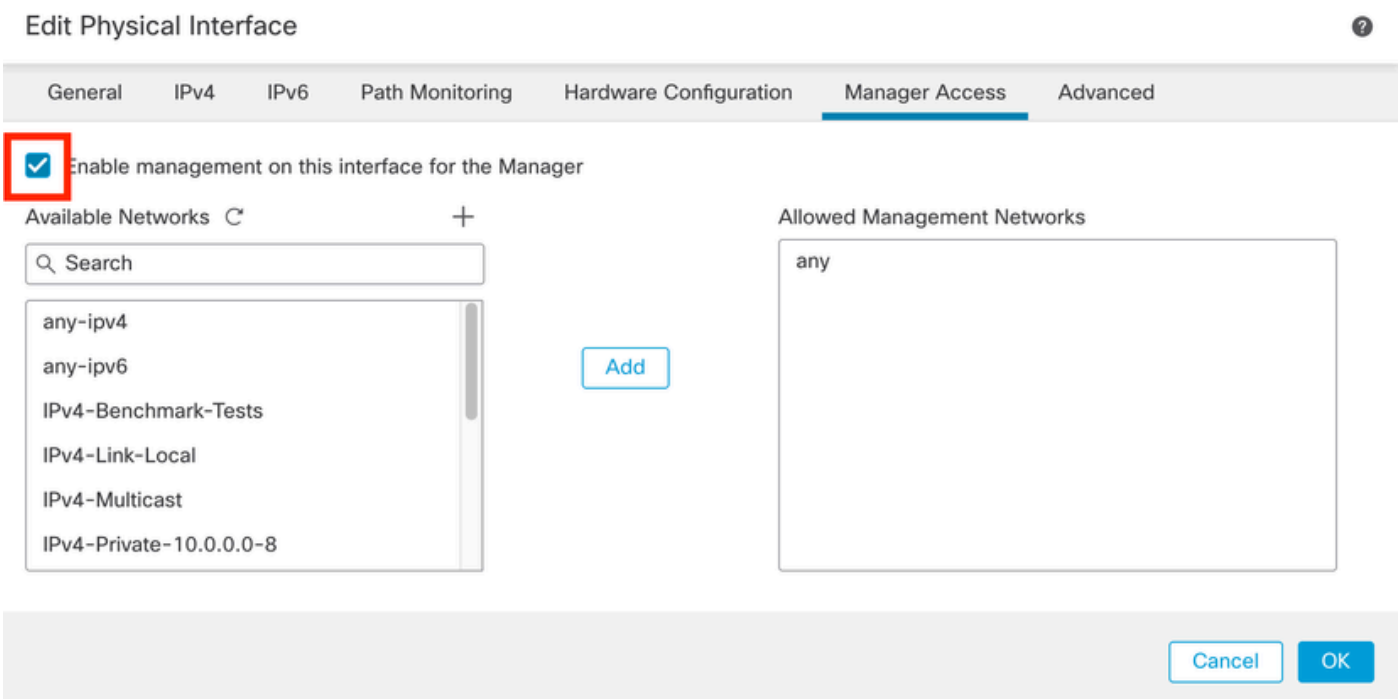
Paso 1. En la pestaña Devices, haga clic en el icono del lápiz para acceder al modo de edición de FTD:



Editar el FTD

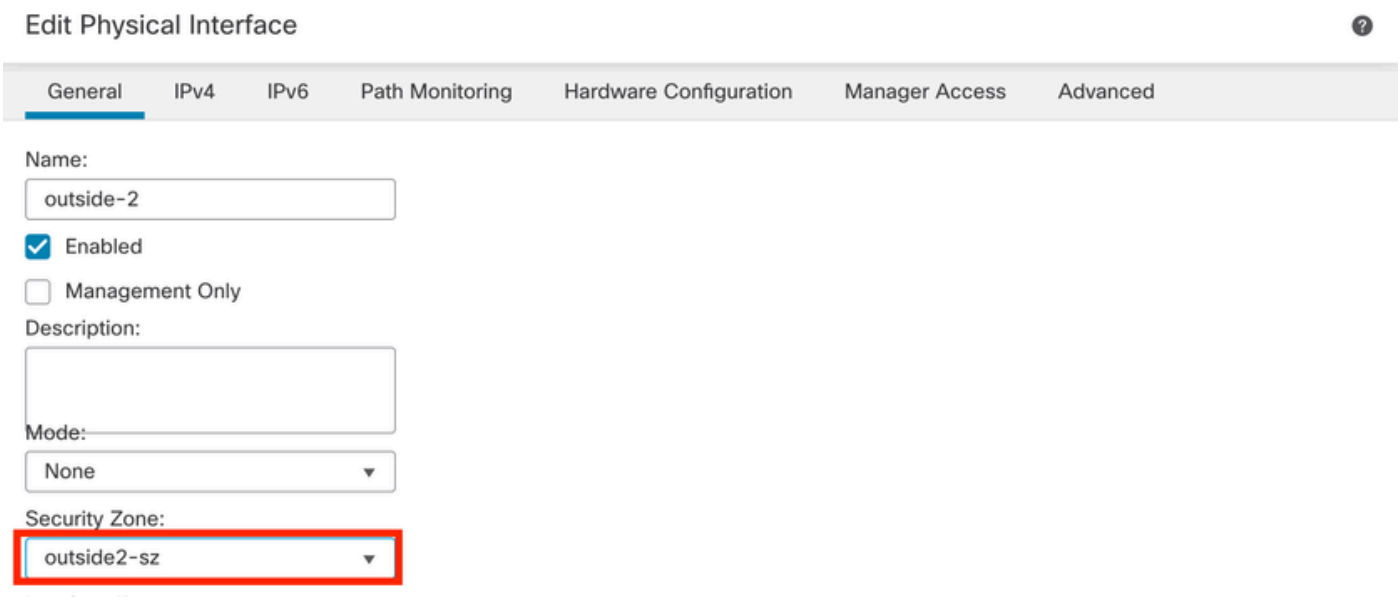
Paso 2. Desde la pestaña Interface, edite la interfaz que se va a asignar como interfaz de administración redundante. Si esto no se hizo anteriormente, configure un nombre de interfaz y una dirección IP.

Paso 3. En la pestaña Acceso al administrador, active la casilla de verificación Habilitar administración en esta interfaz para el administrador:



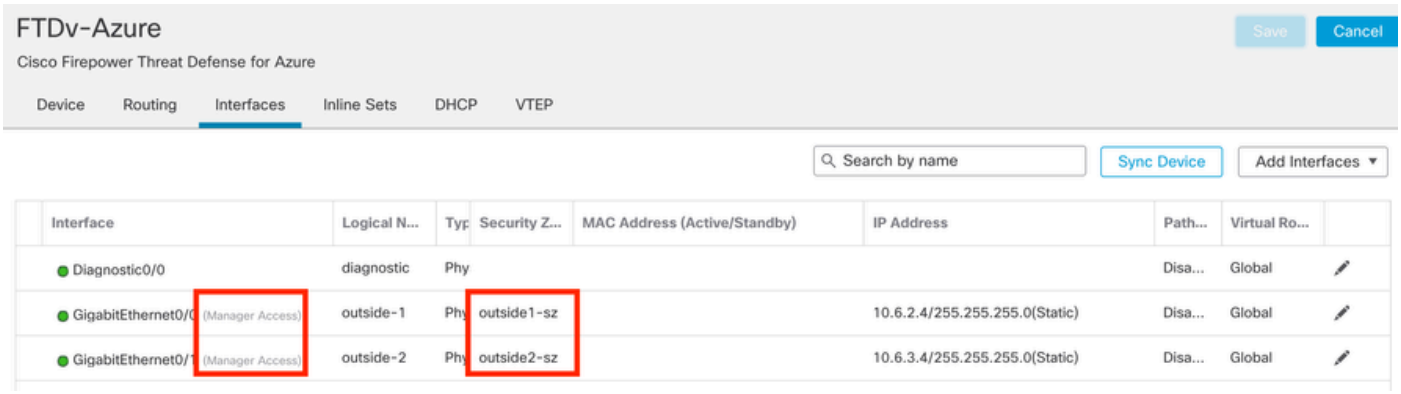
Habilitación del acceso del administrador

Paso 4. En la pestaña General, asegúrese de que la interfaz esté asignada a una zona de seguridad y haga clic en OK:



Zona de seguridad para interfaz de datos redundante

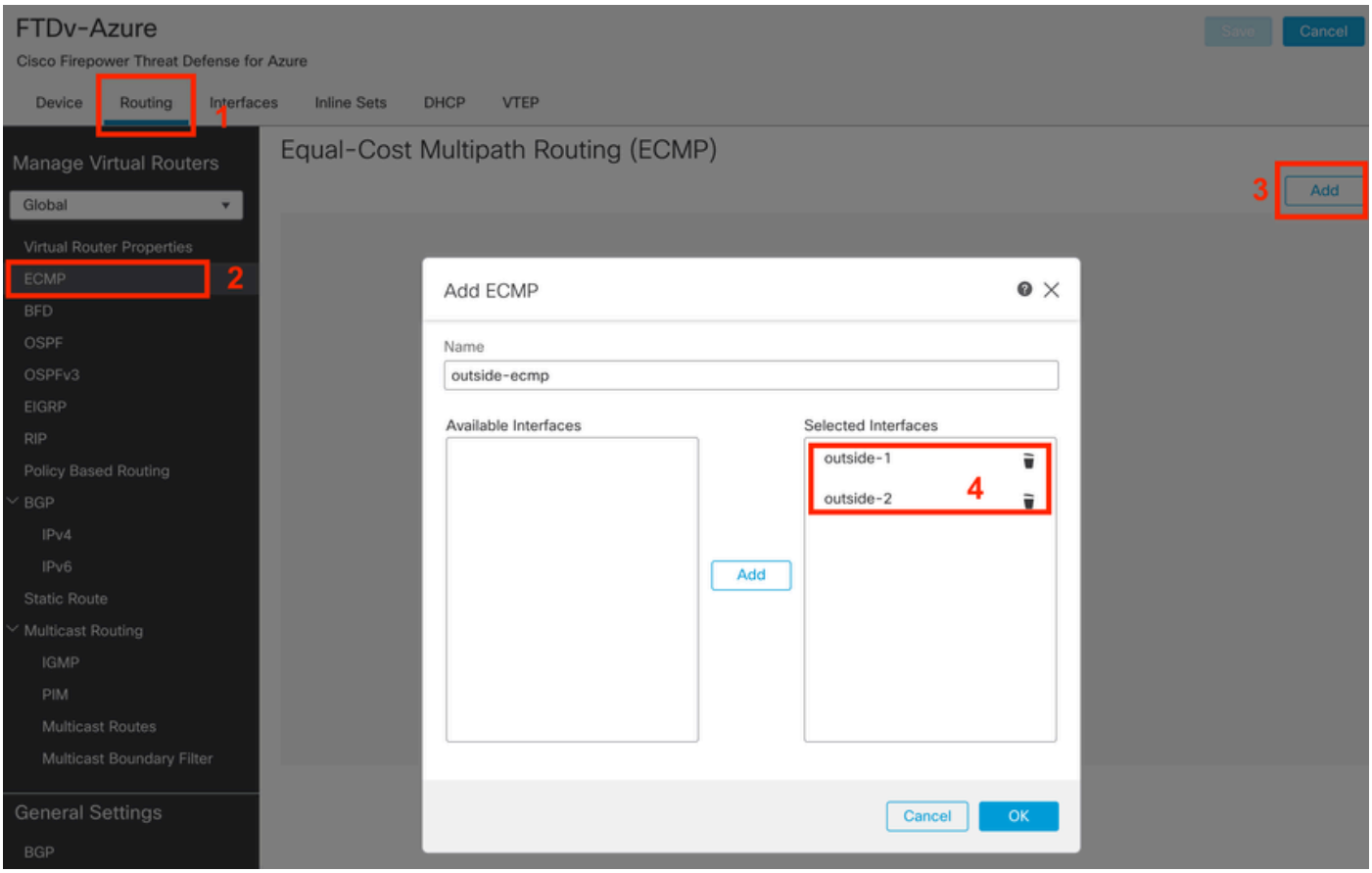
Paso 5. Observe que ahora ambas interfaces tienen la etiqueta Manager Access. Además, asegúrese de que la interfaz de datos principal se haya asignado a una zona de seguridad diferente:



Revisión de configuración de interfaz

En la siguiente sección, los pasos del 6 al 10 están pensados para configurar dos rutas predeterminadas de igual costo para alcanzar el CDO, cada una de las cuales es monitoreada por un proceso de seguimiento de SLA independiente. El seguimiento de SLA garantiza que existe una ruta funcional para comunicarse con el cdFMC mediante la interfaz supervisada.

Paso 6. Vaya a la pestaña Routing y en el menú ECMP cree una nueva zona ECMP con ambas interfaces en ella:

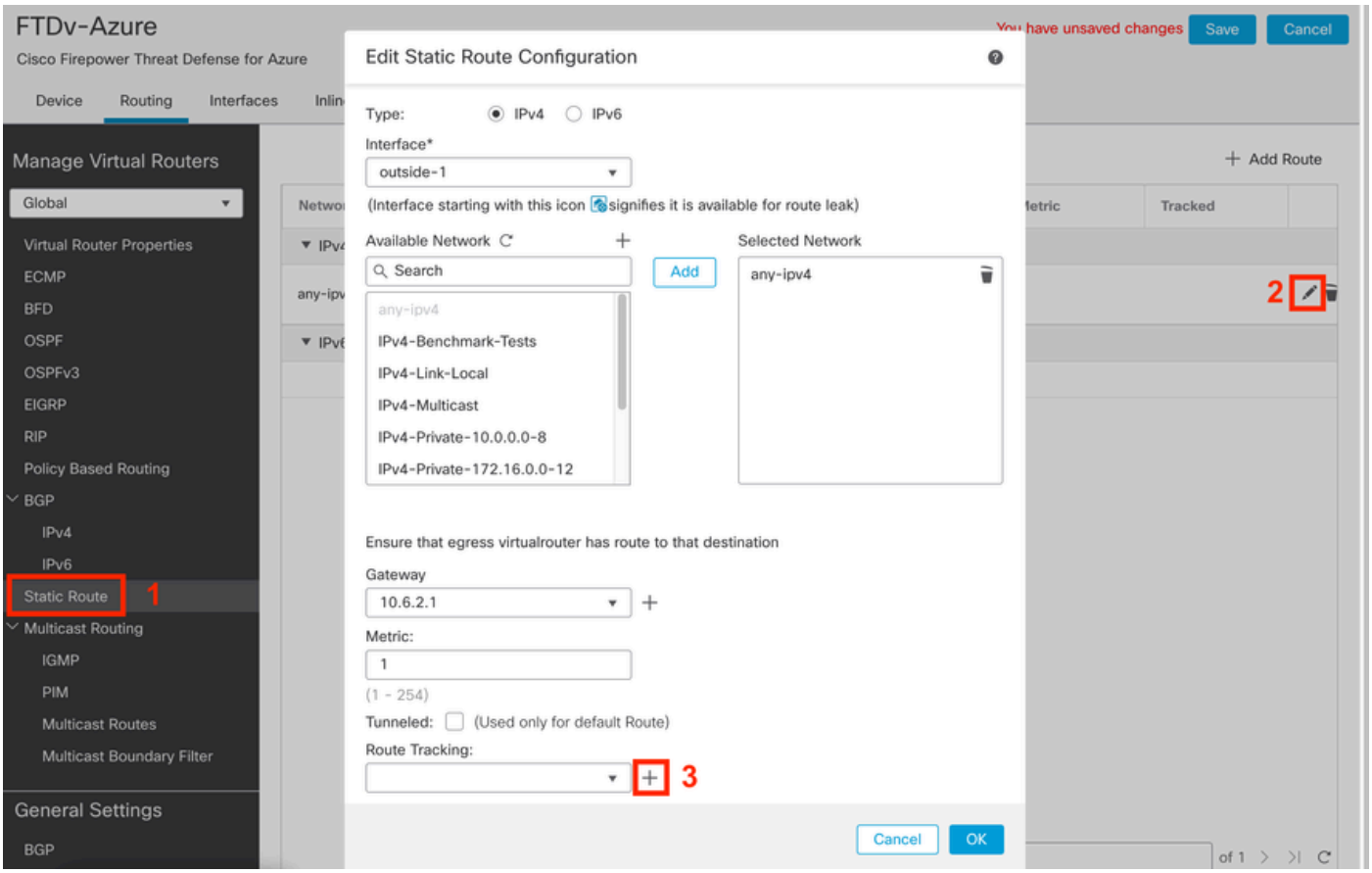


Configuración de una zona ECMP

Haga clic en Aceptar y Guardar.

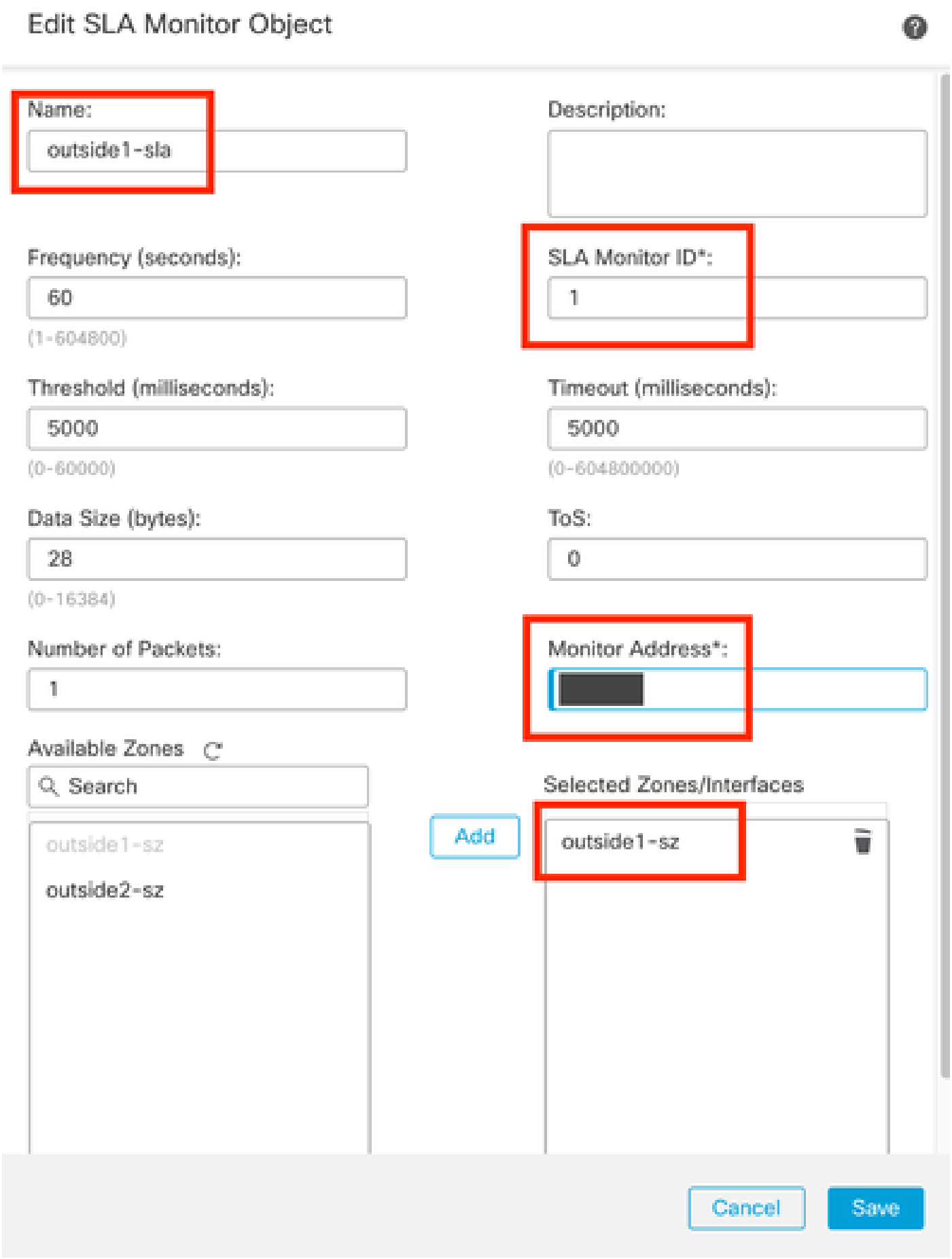
Paso 7. En la pestaña Routing, vaya a Static Routes .

Haga clic en el icono del lápiz para editar la ruta principal. A continuación, haga clic en el signo más para agregar un nuevo objeto de seguimiento de SLA:



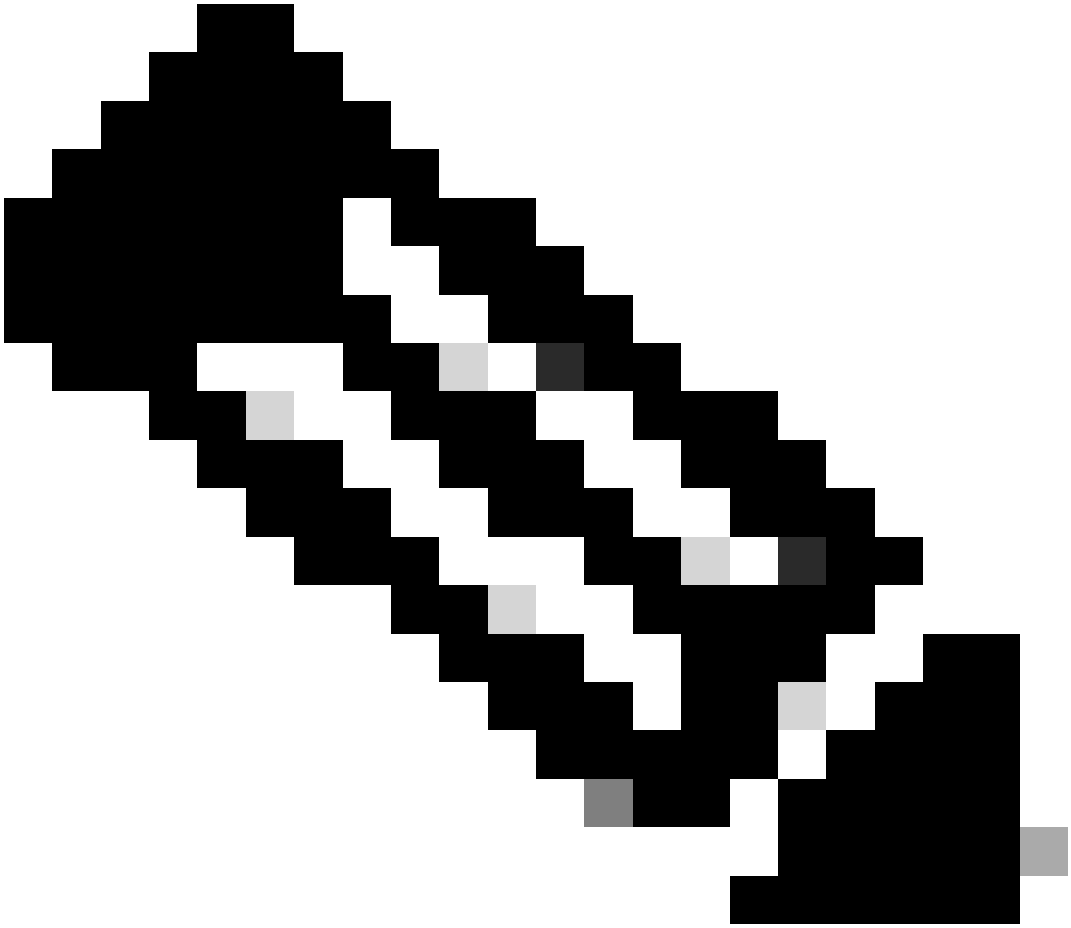
Editar ruta principal para agregar el seguimiento de SLA

Paso 8. Los parámetros requeridos para un seguimiento de SLA funcional se resaltan en la siguiente imagen. Opcionalmente, puede ajustar otras configuraciones como Número de paquetes, Tiempo de espera y Frecuencia.



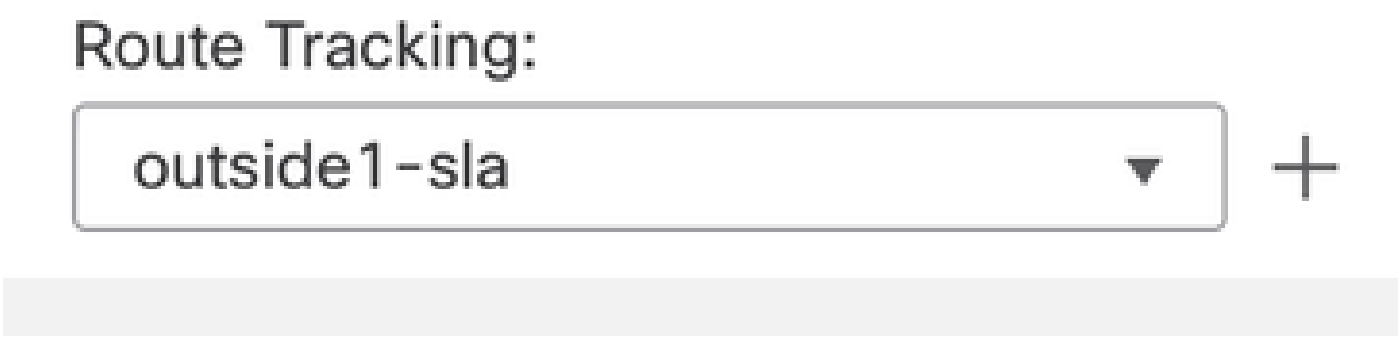
Configuración del seguimiento de SLA para ISP 1

En este ejemplo, se utilizó la IP de DNS de Google para supervisar las capacidades de FTD para alcanzar Internet (y CDO) a través de la interfaz outside1. Haga clic en ok cuando esté listo.



> Nota: Asegúrese de que está realizando el seguimiento de una IP que ya se ha comprobado que es accesible desde la interfaz externa de FTD. La configuración de una pista con una IP inalcanzable puede hacer que la ruta predeterminada caiga en este FTD y, a continuación, impedir su capacidad para comunicarse con CDO.

Paso 9. Haga clic en Guardar y asegúrese de que el nuevo seguimiento de SLA esté asignado a la ruta que apunta a la interfaz principal:

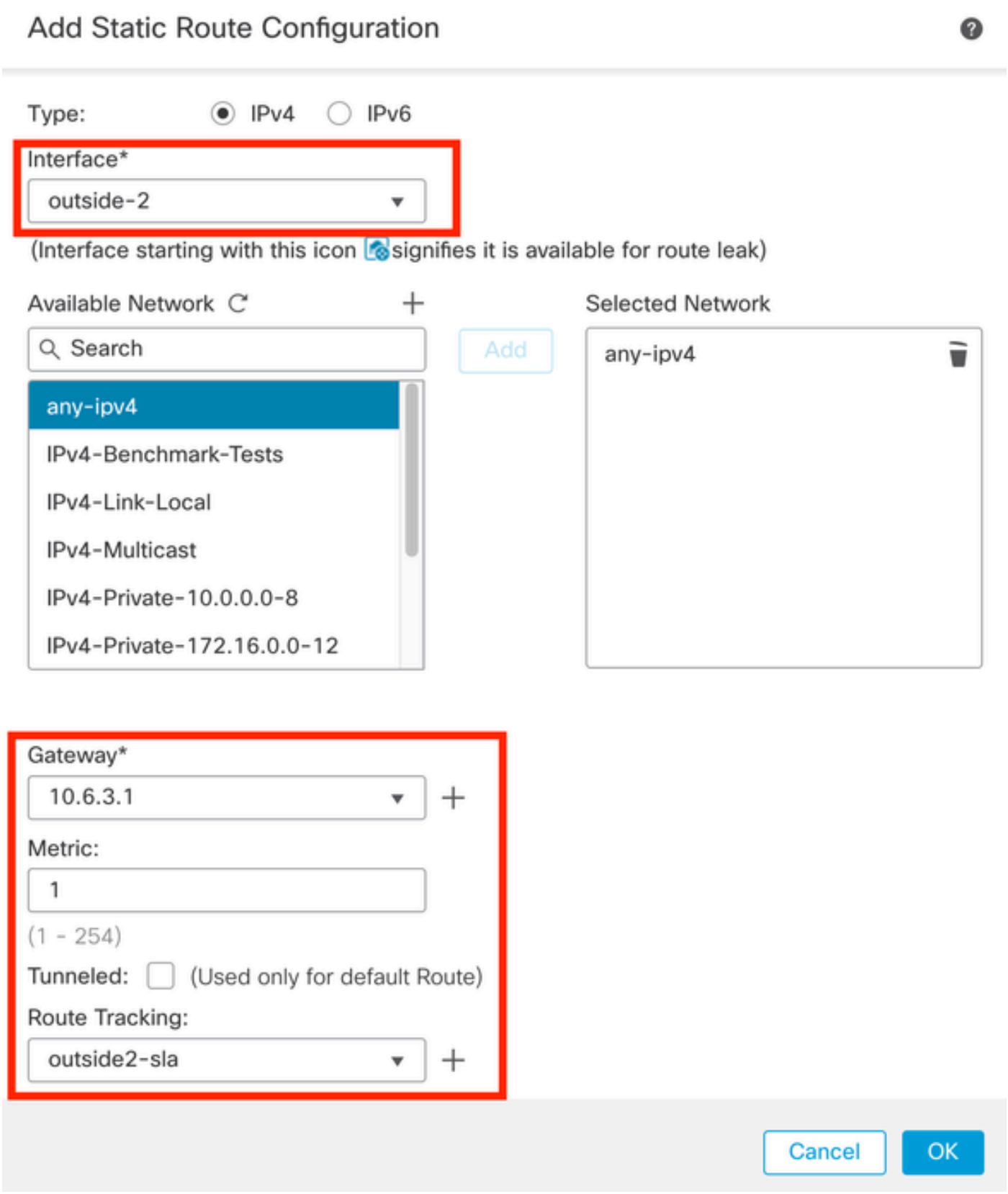


Seguimiento de SLA externo 1

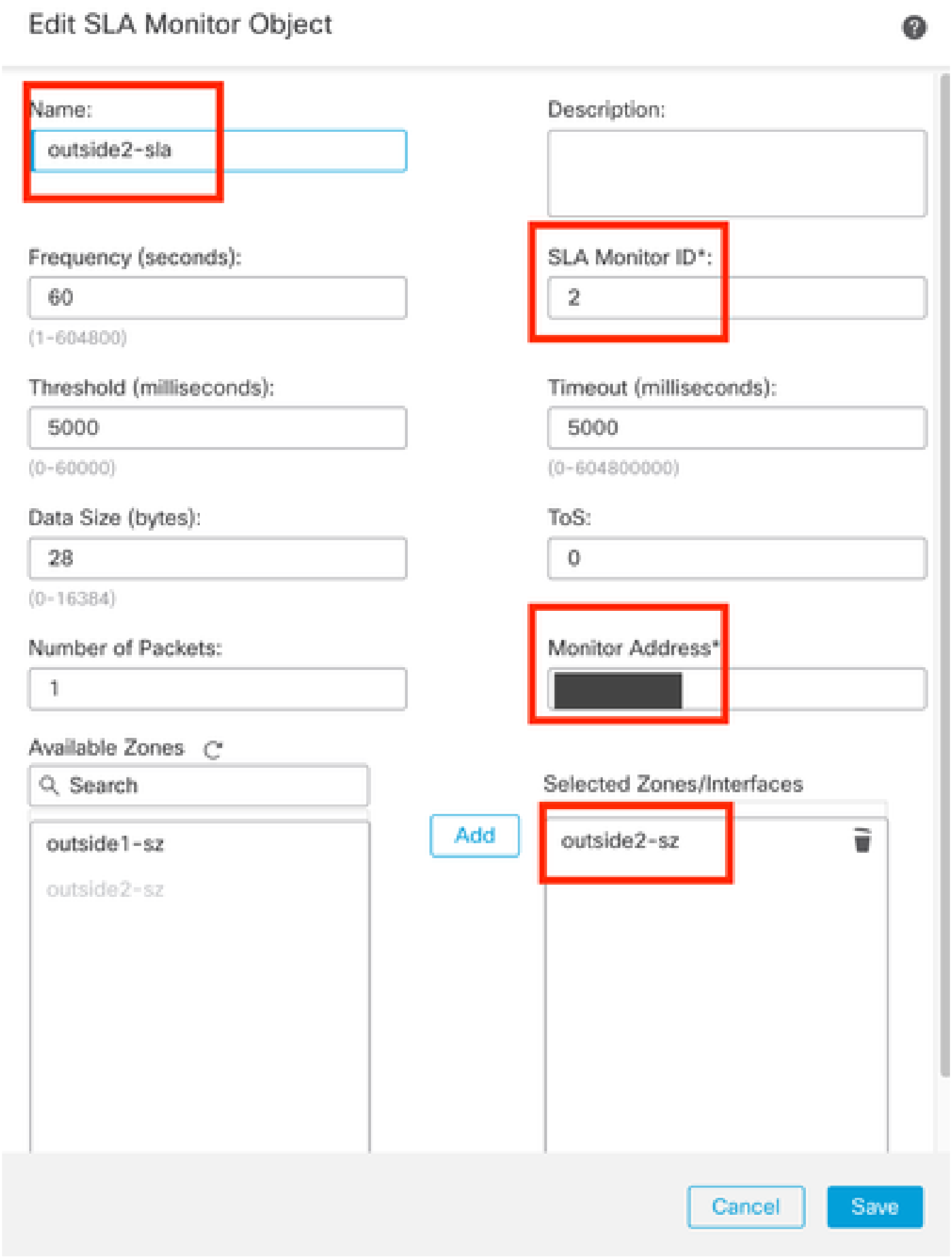
Una vez que haga clic en Aceptar, aparecerá un mensaje emergente con el siguiente mensaje de ADVERTENCIA:

Advertencia de configuración

Paso 10. Haga clic en la opción Add Route para agregar una nueva ruta para la interfaz de datos redundante. Observe en la siguiente imagen que el valor de Métrica para la ruta es el mismo; además, el seguimiento de SLA tiene un ID diferente:



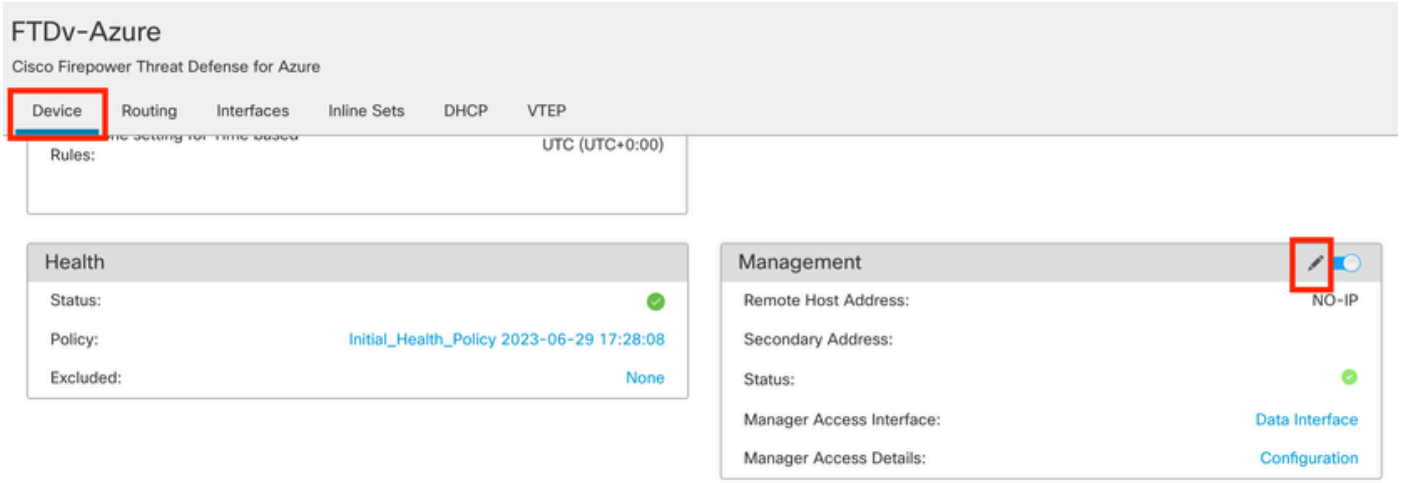
Configurar ruta estática redundante



Configurar el seguimiento para la interfaz de datos redundante

Click Save.

Paso 11. Opcionalmente, puede especificar la IP de la interfaz de datos secundaria en Device > Management . Sin embargo, esto no es necesario dado que el método de onboarding actual utilizó el proceso de clave de registro CLI:



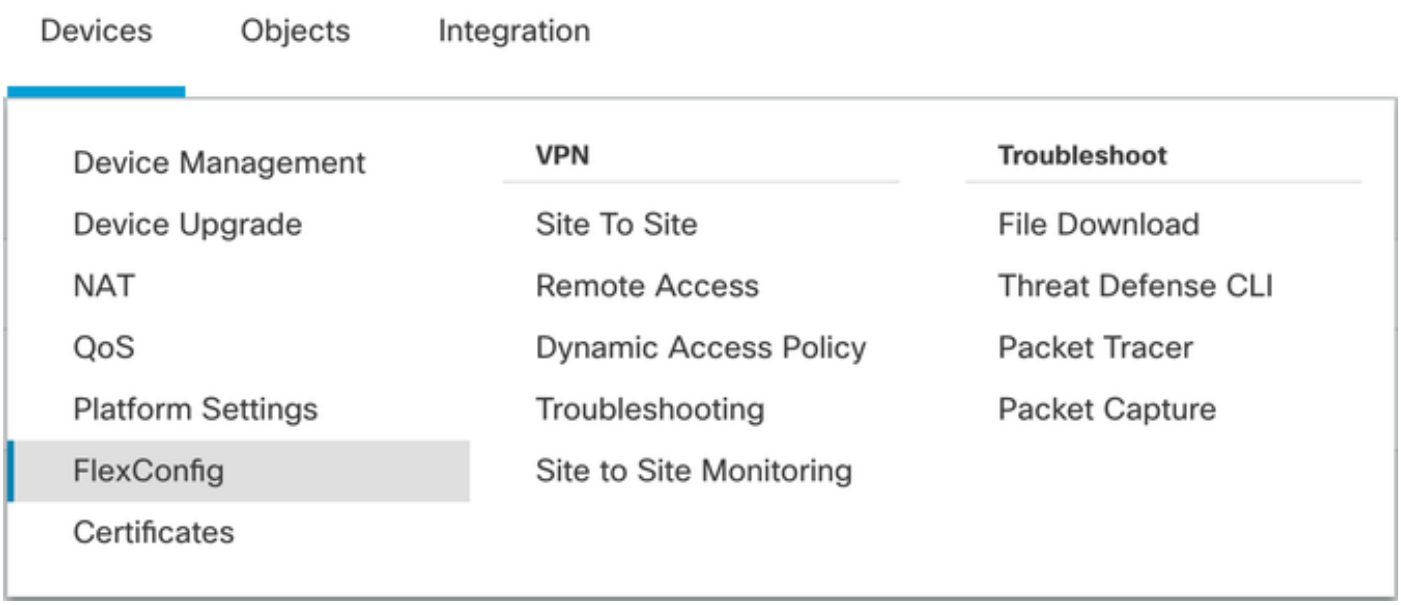
(Opcional) Especifique una IP para la interfaz de datos redundante en el campo de administración

Paso 12. Implemente los cambios.

(Opcional) Establezca un Costo de Interfaz para un Modo de Interfaz Activo/de Respaldo:

De forma predeterminada, la administración redundante sobre la interfaz de datos utiliza el ordenamiento cíclico para distribuir el tráfico de administración entre ambas interfaces. De forma alternativa, si un enlace WAN tiene un ancho de banda superior al otro y prefiere que éste sea el enlace de gestión principal, mientras que el otro permanece como copia de seguridad, puede asignar al enlace principal un coste de 1 y asignar al enlace de copia de seguridad un coste de 2. En el siguiente ejemplo, la interfaz GigabitEthernet0/0 se mantiene como el link WAN principal mientras que GigabitEthernet0/1 sirve como el link de administración de respaldo:

1. Navegue hasta Devices > FlexConfig link y cree una política flexConfig. En caso de que ya haya una política flexConfig configurada y asignada a su FTD, edítela:

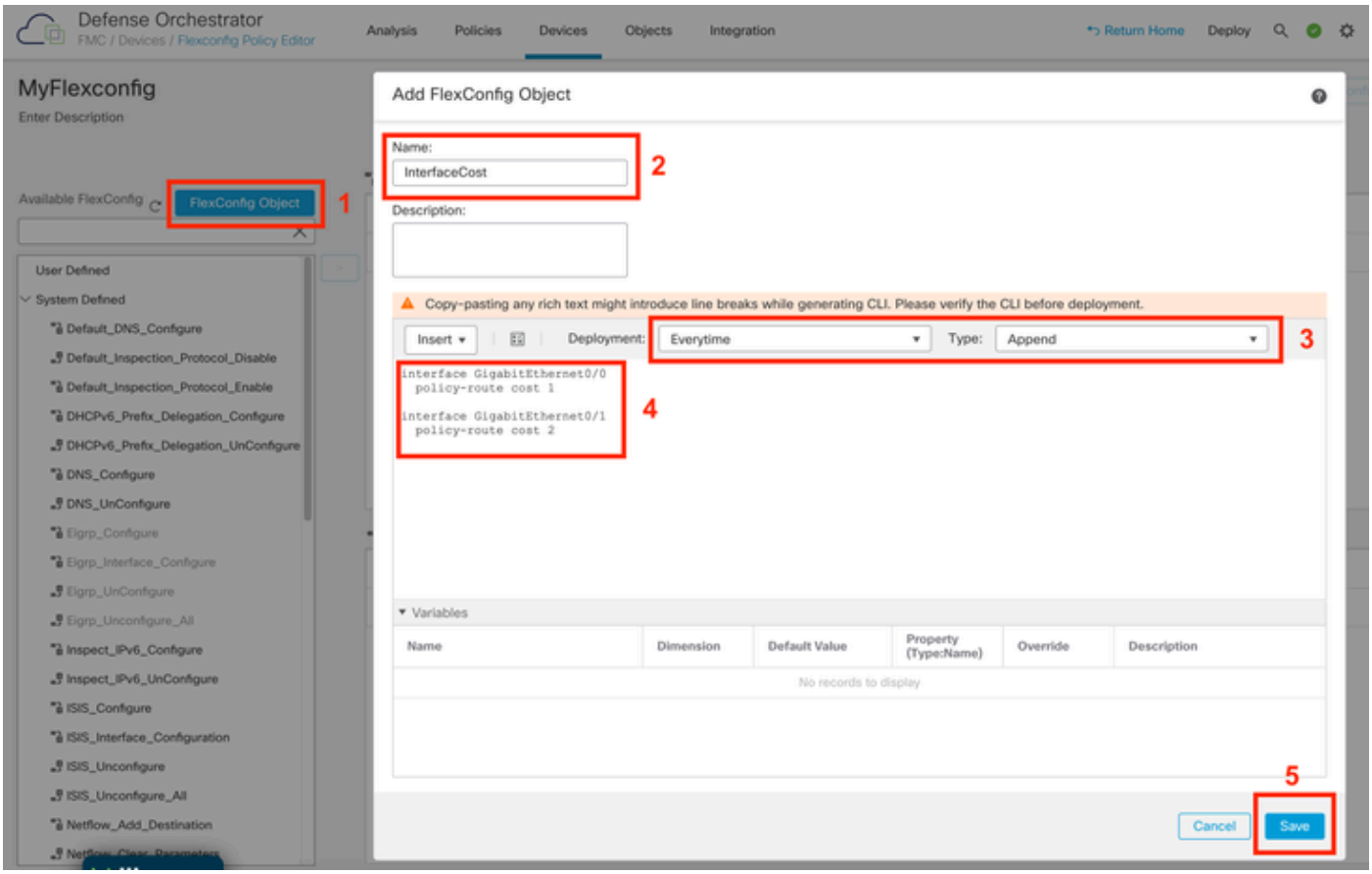


Acceso al menú FlexConfig

2. Cree un nuevo objeto FlexConfig:

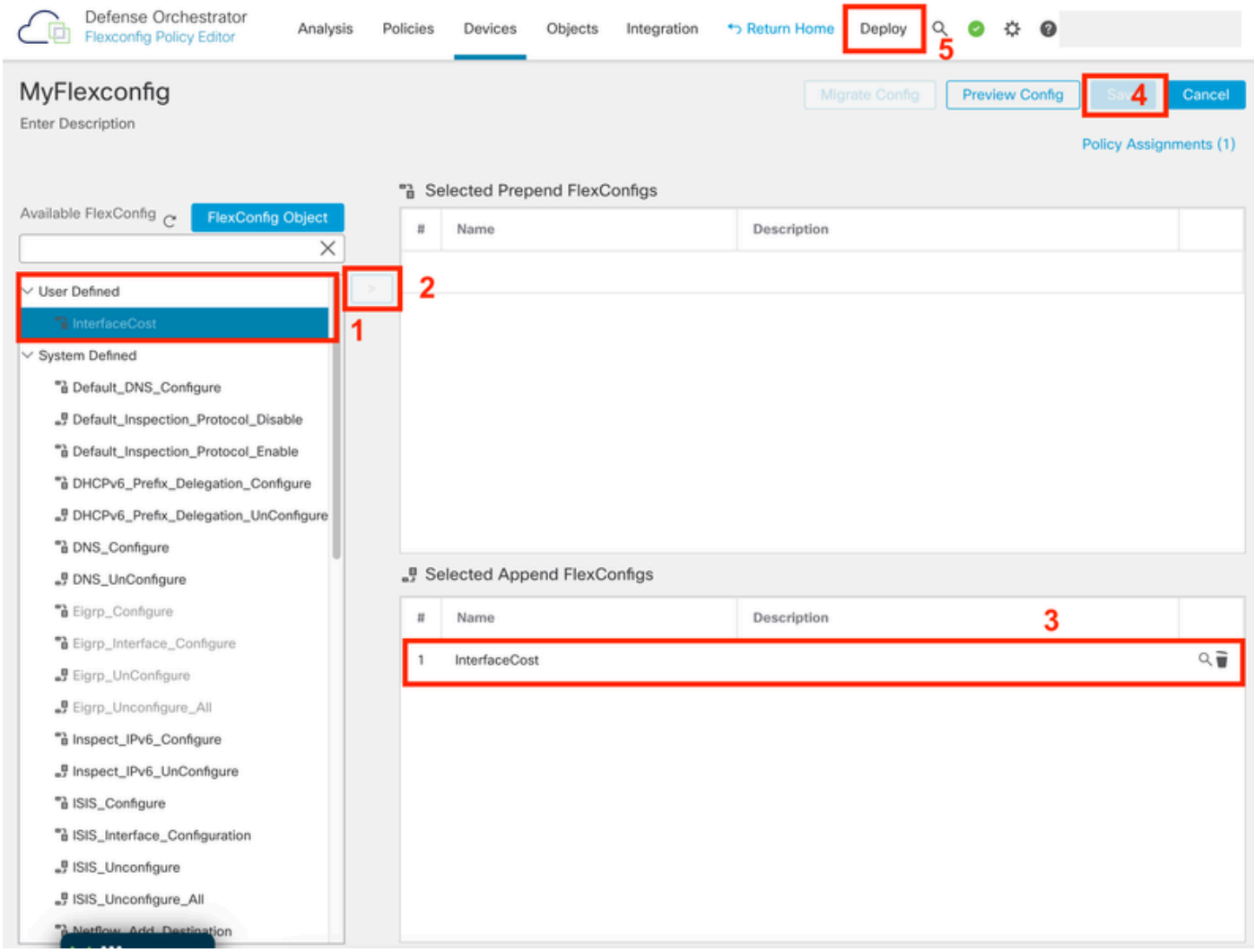
- Dé un nombre al objeto FlexConfig.
- Elija Everytime y Append en las secciones Deployment y Type respectivamente.
- Establezca el costo para las interfaces con los siguientes comandos como se muestra en la Imagen 22.
- Click Save.

```
<#root>
interface GigabitEthernet0/0

  policy-route cost 1

<=== A cost of 1 means this will be the primary interface for management communication with CDO tenant.
interface GigabitEthernet0/1

  policy-route cost 2

<=== Cost 2 sets this interface as a backup interface.
```



Adición de un objeto Flexconfig

3. Elija el objeto creado recientemente y agréguelo a la sección Seleccionado Anexar FlexConfigs como se muestra en la imagen. Guarde los cambios e implemente la configuración.



Asignación del Objeto a la Política Flexconfig

4. Implemente los cambios.

Verificación

1. Para verificar, utilice el comando show network. Se forma una nueva instancia para la interfaz de administración redundante:

```
> show network

<<---------- output omitted for brevity ---------->>

=====================[ eth0 ]=====================
State : Enabled
Link : Up
Channels : Management & Events
Mode : Non-Autonegotiation
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 60:45:BD:D8:62:D7
---------------------[ IPv4 ]---------------------
Configuration : Manual
```

```
Address : 10.6.0.4
Netmask : 255.255.255.0
----------------------[ IPv6 ]----------------------
Configuration : Disabled

================[ Proxy Information ]================
State : Disabled
Authentication : Disabled
. . .

===============[ GigabitEthernet0/0 ]===============
State : Enabled
Link : Up
Name : outside-1
MTU : 1500
MAC Address : 60:45:BD:D8:6F:5C
----------------------[ IPv4 ]----------------------
Configuration : Manual
Address : 10.6.2.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
----------------------[ IPv6 ]----------------------
Configuration : Disabled

===============[ GigabitEthernet0/1 ]===============
State : Enabled
Link : Up
Name : outside-2
MTU : 1500
MAC Address : 60:45:BD:D8:67:CA
----------------------[ IPv4 ]----------------------
Configuration : Manual
Address : 10.6.3.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
----------------------[ IPv6 ]----------------------
Configuration : Disabled
```

2. La interfaz ahora es parte del dominio sftunnel. Puede confirmar esto con los comandos show sftunnel interfaces y show running-config sftunnel:

```
<#root>

>

show sftunnel interfaces


Physical Interface Name of the Interface
GigabitEthernet0/0 outside-1
GigabitEthernet0/1 outside-2

>

show running-config sftunnel


sftunnel interface outside-2
sftunnel interface outside-1
```

```
sftunnel port 8305
sftunnel route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346
```

3. Una ruta basada en políticas se deletrea automáticamente. Si no especificó un costo de interfaz, la opción adaptive-interface configura el procesamiento de ordenamiento cíclico para balancear la carga del tráfico de administración entre ambas interfaces:

```
<#root>

>

show running-config route-map


!
route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346 permit 5
 match ip address FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392
 set adaptive-interface cost outside-1 outside-2

>

show access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392


access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392; 1 elements; name hash: 0x8e8cb508
access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392 line 1 extended permit tcp any any eq 8305 (hi
```

4. Utilice el comando show running-config interface <interface> para verificar las configuraciones de la interfaz:

```
<#root>

>

 show running-config interface GigabitEthernet 0/0


!
interface GigabitEthernet0/0
nameif outside-1
security-level 0
zone-member outside-ecmp
ip address 10.6.2.4 255.255.255.0
policy-route cost 1

>

show running-config interface GigabitEthernet 0/1


!
interface GigabitEthernet0/1
nameif outside-2
security-level 0
zone-member outside-ecmp
ip address 10.6.3.4 255.255.255.0
```

```
policy-route cost 2
```

Se pueden utilizar algunos comandos adicionales para verificar el seguimiento de las rutas configuradas:

```
<#root>

>

show track


Track 1
Response Time Reporter 2 reachability
Reachability is Up                    <============== Ensure reachability is up for the monitored interfa
2 changes, last change 09:45:00
Latest operation return code: OK
Latest RTT (millisecs) 10
Tracked by:
STATIC-IP-ROUTING 0
Track 2
Response Time Reporter 1 reachability
Reachability is Up                    <============== Ensure reachability is up for the monitored interfa
2 changes, last change 09:45:00
Latest operation return code: OK
Latest RTT (millisecs) 1
Tracked by:
STATIC-IP-ROUTING 0


>

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 10.6.3.1 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.6.3.1, outside-2
                   [1/0] via 10.6.2.1, outside-1
C 10.6.2.0 255.255.255.0 is directly connected, outside-1
L 10.6.2.4 255.255.255.255 is directly connected, outside-1
C 10.6.3.0 255.255.255.0 is directly connected, outside-2
L 10.6.3.4 255.255.255.255 is directly connected, outside-2
```

Información Relacionada

- Soporte técnico y descargas de Cisco
- Gestión de la defensa frente a amenazas de firewall con el centro de gestión de firewall en la nube de Cisco Defense Orchestrator

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).