Configuración de BFD en Secure Firewall Threat Defence con Flex-Config

Contenido

Introducción

Este documento describe cómo configurar el protocolo BFD en Secure Firewall Management Center que ejecuta 7.2 y versiones anteriores con Flex-Config.

Prerequisites

Protocolo de gateway fronterizo (BGP) configurado en Cisco Secure Firewall Threat Defense (FTD) con Cisco Secure Firewall Management Center (FMC).

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

-Protocolo BGP
-Conceptos BFD

Componentes Utilizados

-Cisco Secure Firewall Management Center con versión 7.2 o anterior.

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

La detección de reenvío bidireccional (BFD) es un protocolo de detección diseñado para proporcionar tiempos de detección de fallos de ruta de reenvío rápido para todos los tipos de medios, encapsulaciones, topologías y protocolos de routing.

Configurar

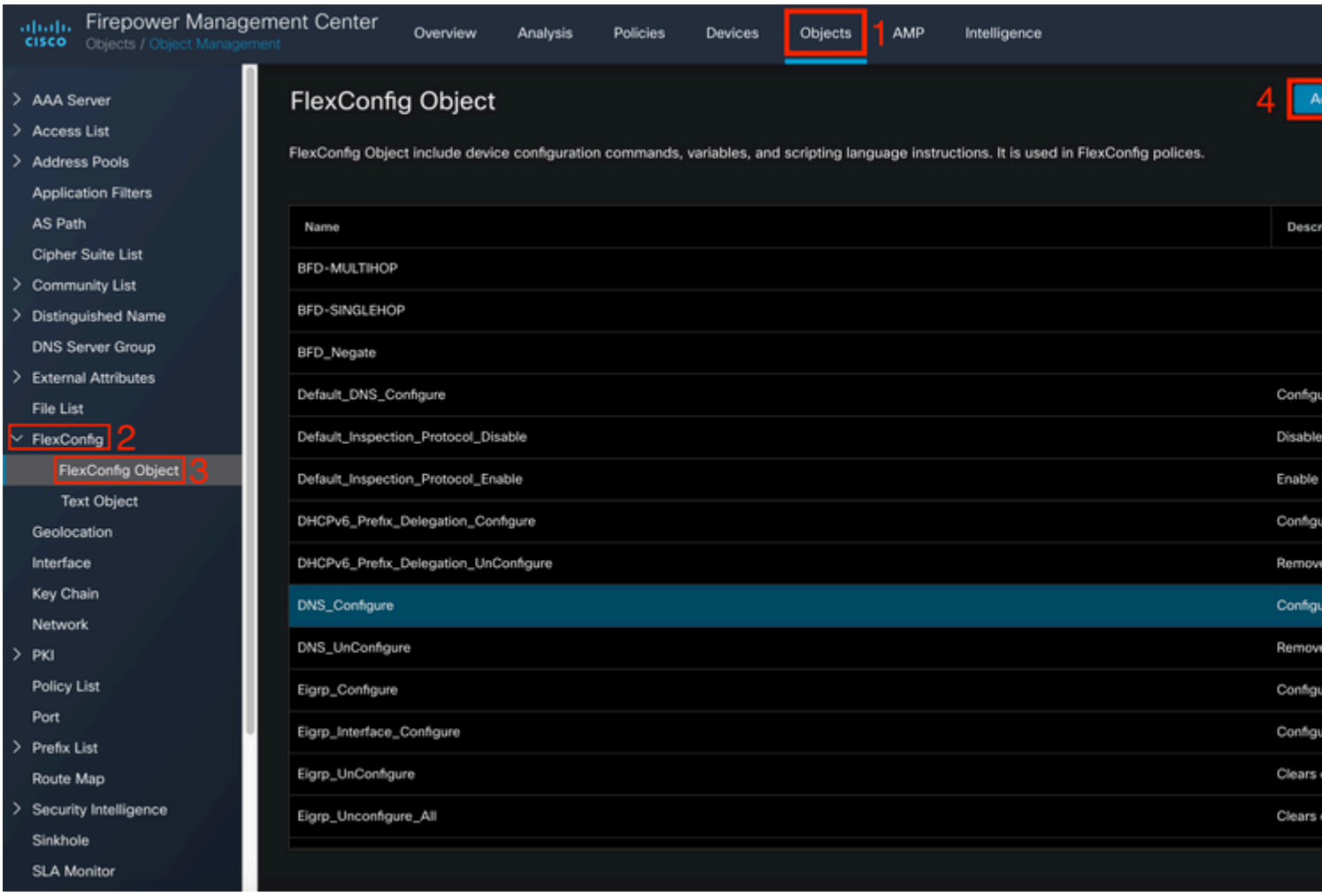
Las configuraciones BFD en FMC que ejecutan versiones 7.2 y anteriores deben configurarse con objetos y políticas Flex-Config.

Paso 1.

Cree la plantilla BFD mediante el objeto Flexconfig.

La plantilla BFD especifica un conjunto de valores de intervalo BFD. Los valores del intervalo BFD configurados en la plantilla BFD no son específicos de una única interfaz. También puede configurar la autenticación para las sesiones de un solo salto y multisalto.

Para crear el objeto Flex-Config, seleccione la opción **Objects Tab** en la parte superior, haga clic en el botón **FlexConfig** en la columna izquierda y, a continuación, haga clic en el botón **FlexConfig Object** y, a continuación, en **Add FlexConfig Object**.



Paso 2.

Agregue los parámetros necesarios para el protocolo BFD:

La plantilla BFD especifica un conjunto de valores de intervalo BFD. Los valores del intervalo BFD configurados en la plantilla BFD no son específicos de una única interfaz. También puede configurar la autenticación para las sesiones de un solo salto y multisalto.

```
bfd-template [single-hop | multi-hop] template_name
```

- single-hop - Especifica una plantilla BFD de un solo salto.
- multi-hop: especifica una plantilla BFD de salto múltiple.
- template_name: especifica el nombre de la plantilla. El nombre de la plantilla no puede contener espacios.
- (Opcional) Configure Echo en una plantilla BFD de un solo salto.

Nota: Sólo puede activar el modo Eco en una plantilla de un solo salto.

Configure los intervalos en la plantilla BFD:

```
interval both milliseconds | microseconds {both | min-tx} microseconds | min-tx milliseconds echo
```

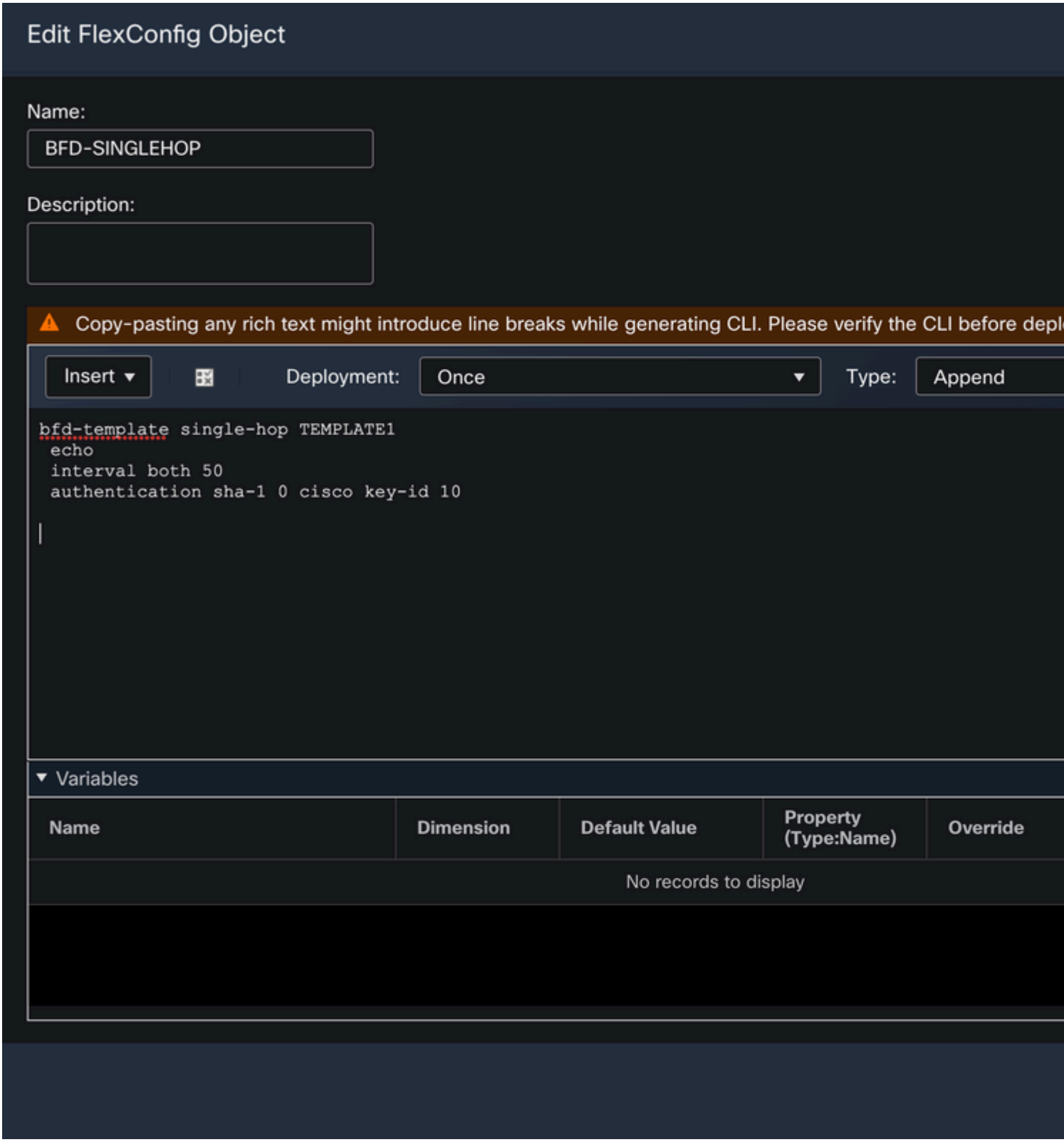
- both: capacidad de intervalo mínimo de transmisión y recepción.
- El intervalo en milisegundos. El rango es 50 a 999.
- microseconds: especifica el intervalo BFD en microsegundos para bothandmin-tx.
- microsegundos: el intervalo es de 50 000 a 999 000.
- min-tx: la capacidad del intervalo de transmisión mínimo.

Configure la autenticación en la plantilla BFD:

```
authentication {md5 | meticulous-mds | meticulous-sha-1 | sha-1}[0|8] wordkey-id id
```

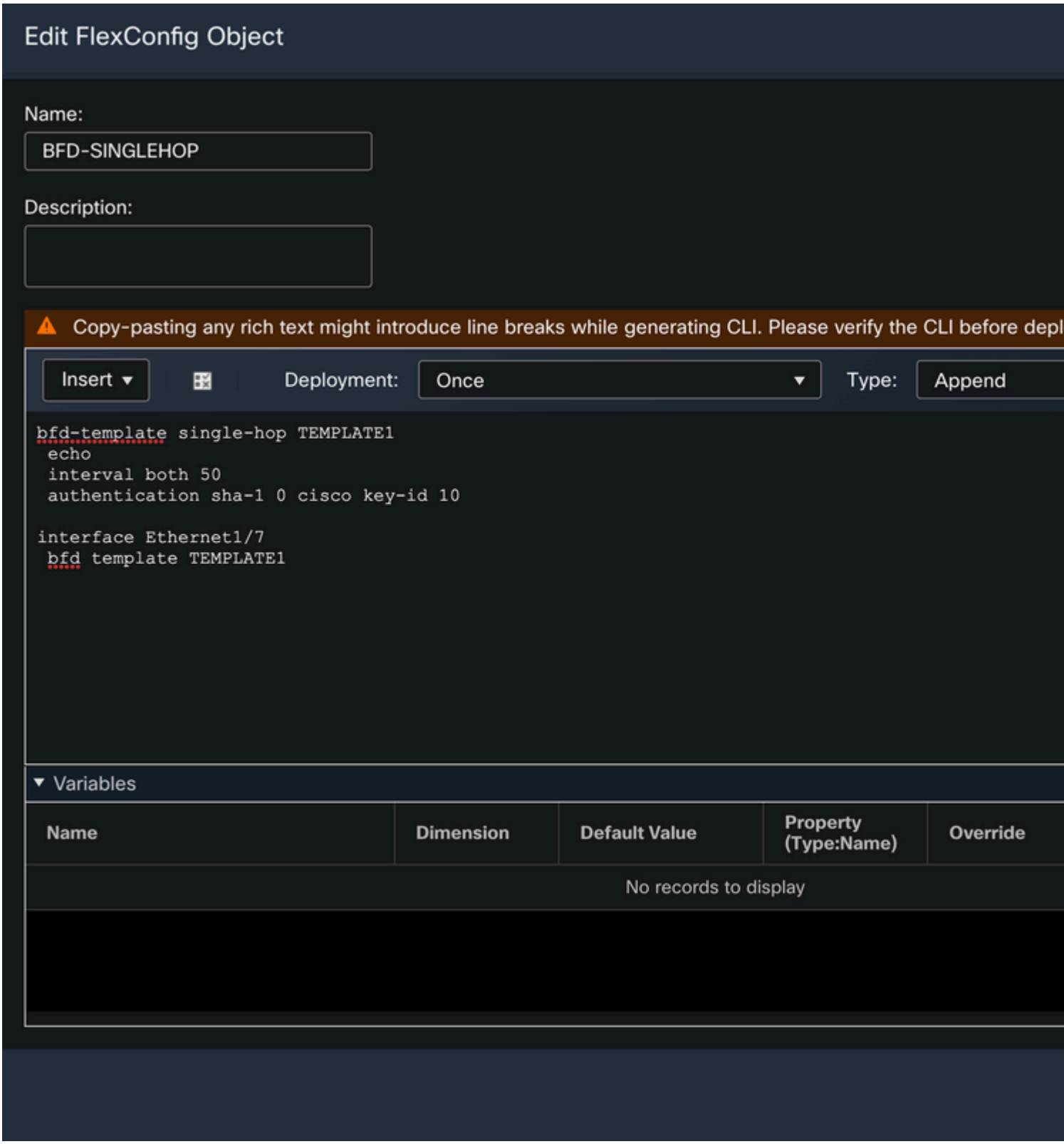
- authentication: especifica el tipo de autenticación.
- md5: autenticación Message Digest 5 (MD5).
- meticulous-md5: meticulosa autenticación MD5 con clave.
- meticulous-sha-1: meticulosa autenticación de claves SHA-1.
- sha-1: autenticación de claves SHA-1.
- 0|8â€”0 especifica que le sigue una contraseña NO CIFRADA. 8 especifica que a continuación aparece una contraseña CIFRADA.
- palabra: la contraseña (clave) de BFD, que es una contraseña/clave de un solo dígito de hasta 29 caracteres. Las contraseñas que comienzan con un dígito seguido de un espacio en blanco no son compatibles; por ejemplo, 0 pass y 1 no son válidas.
- key-id: el ID de clave de autenticación.
- id: la ID de clave compartida que coincide con la cadena de clave. El intervalo es de 0 a 255

caracteres.



Paso 3.

Asocie la plantilla BFD a la interfaz.



Nota: Asocie la plantilla multisalto BFD con un mapa de destinos.

Paso 4 (opcional).

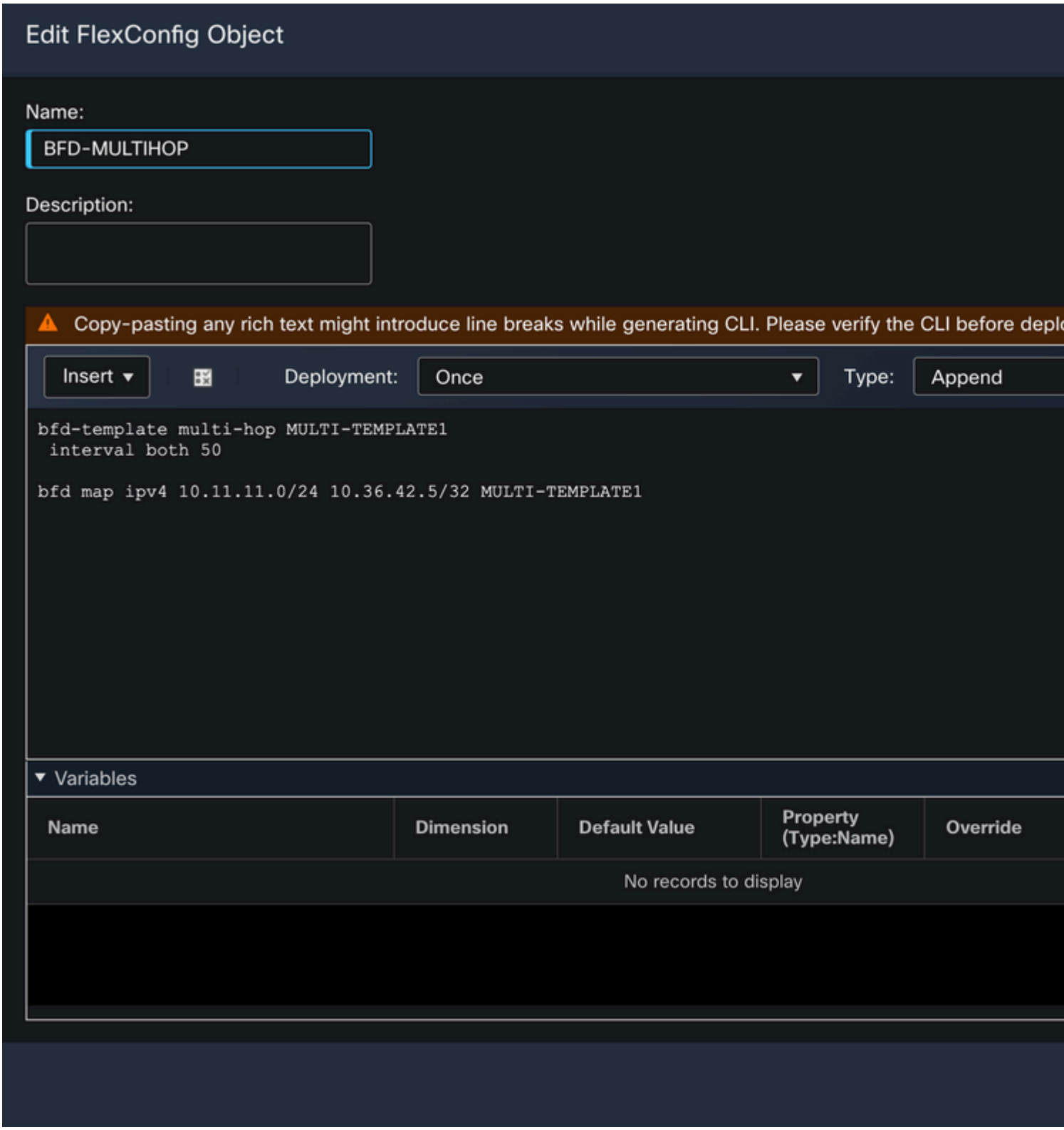
Cree un mapa BFD que contenga destinos que pueda asociar a una plantilla de salto múltiple. Debe tener una plantilla BFD de salto múltiple ya configurada.

Asocie la plantilla multisalto BFD con un mapa de destinos:

```
bfd map {ipv4 | ipv6} destination/cdir source/cdire template-name
```

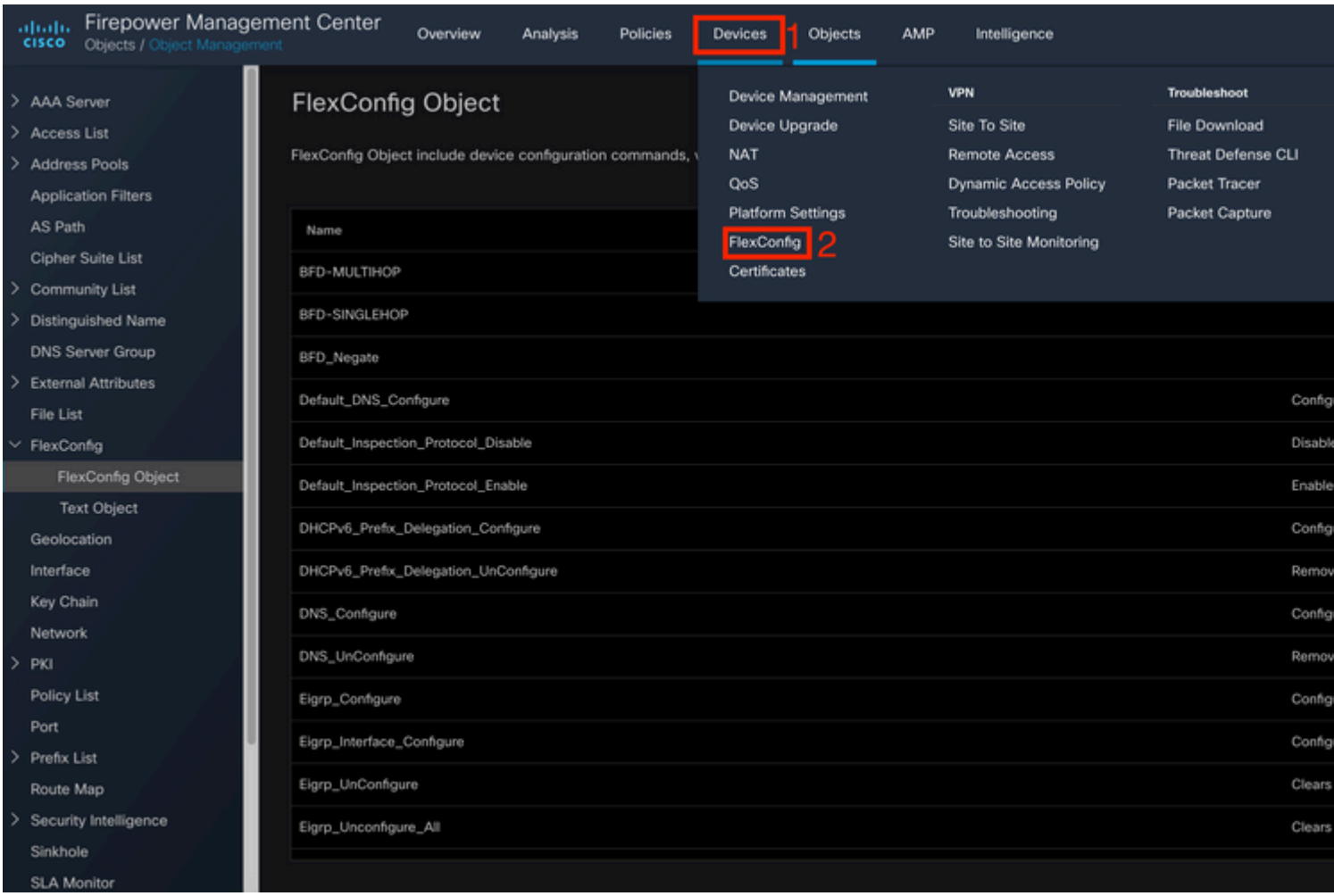
- ipv4: configura una dirección IPv4.
- ipv6: configura una dirección IPv6.
- destination/cdir: especifica el prefijo/longitud de destino. El formato es A.B.C.D/<0-32>.
- source/cdir: especifica el prefijo/longitud de destino. El formato es X:X:X;X::X/<0-128>.
- template-name: especifica el nombre de la plantilla de salto múltiple asociada a este mapa BFD.

Haga clic en el **Save** para guardar el objeto.



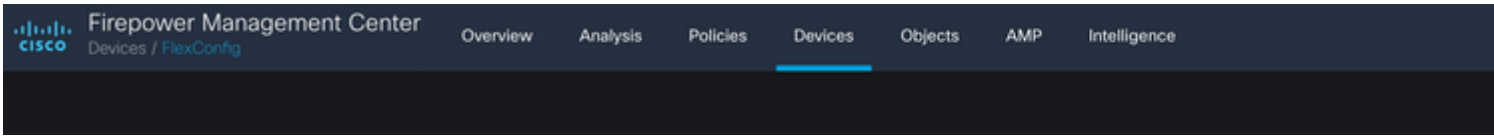
Paso 5.

Haga clic en el **Devices** en la parte superior y seleccione la ficha **FlexConfig** opción.



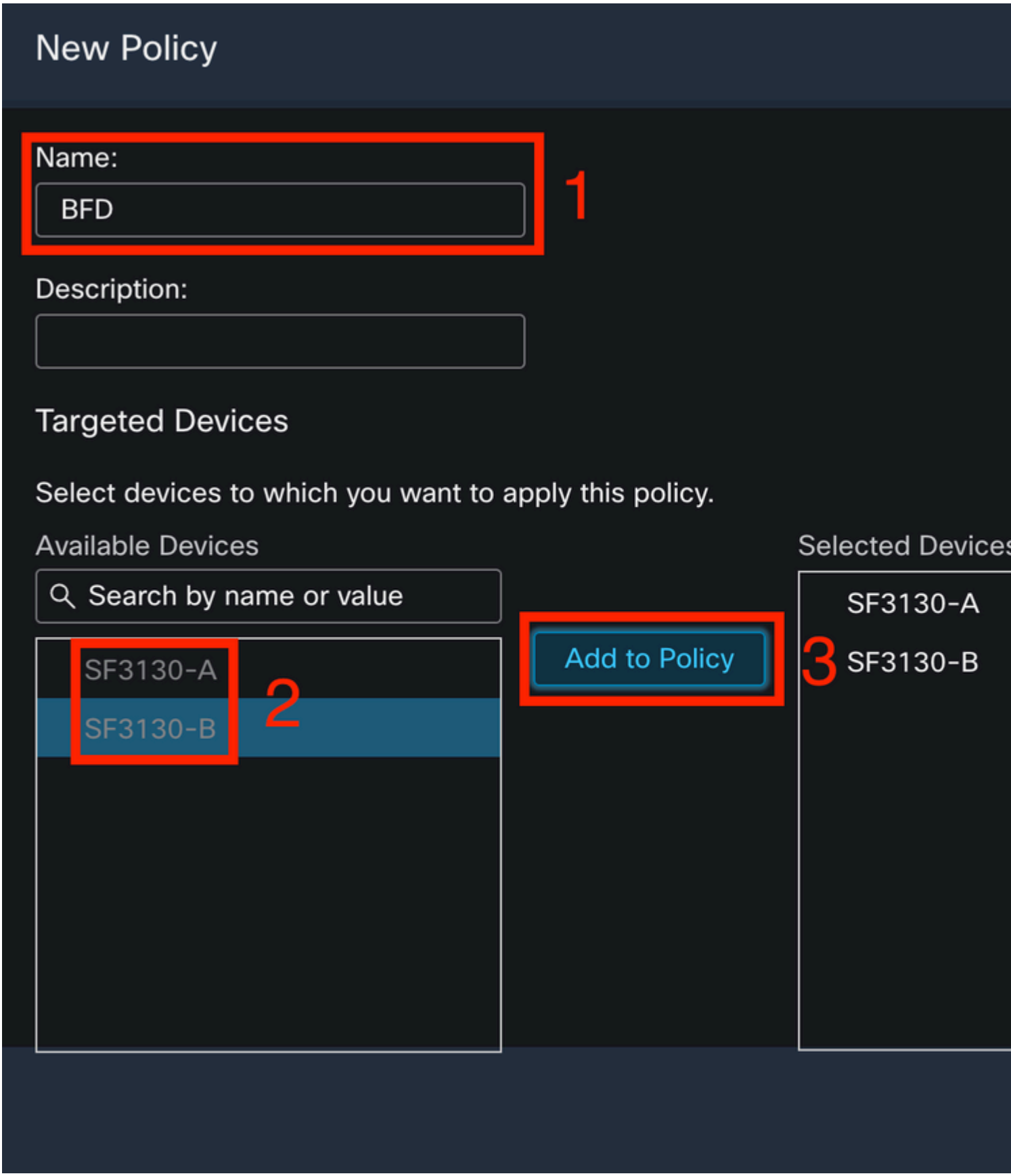
Paso 6.

Para crear una nueva política FlexConfig, haga clic en el botón **New Policy** botón.



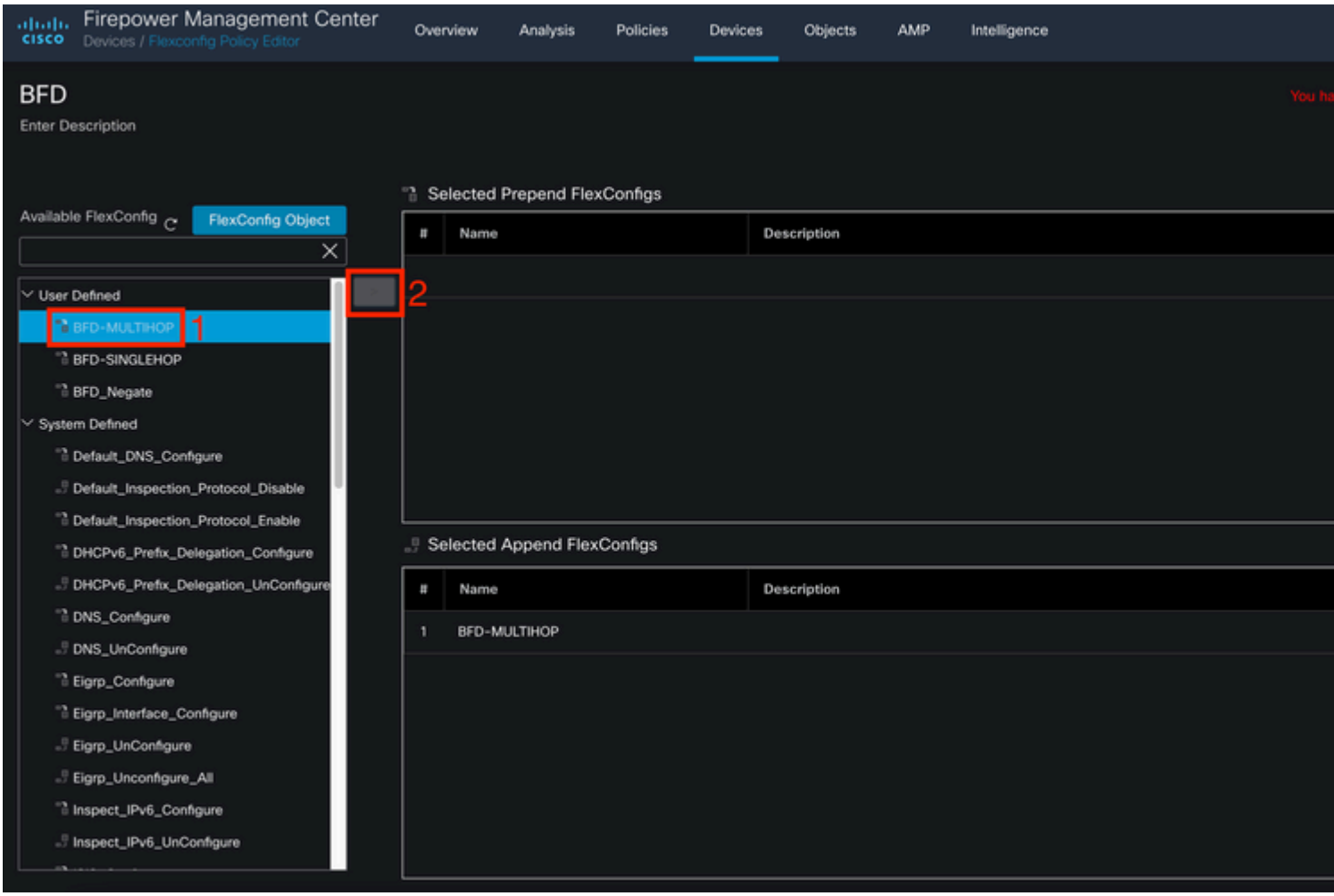
Paso 7.

Name seleccione la política y los dispositivos asignados a la política. Haga clic en el **Add to Policy** a continuación, haga clic en **Save**botón.



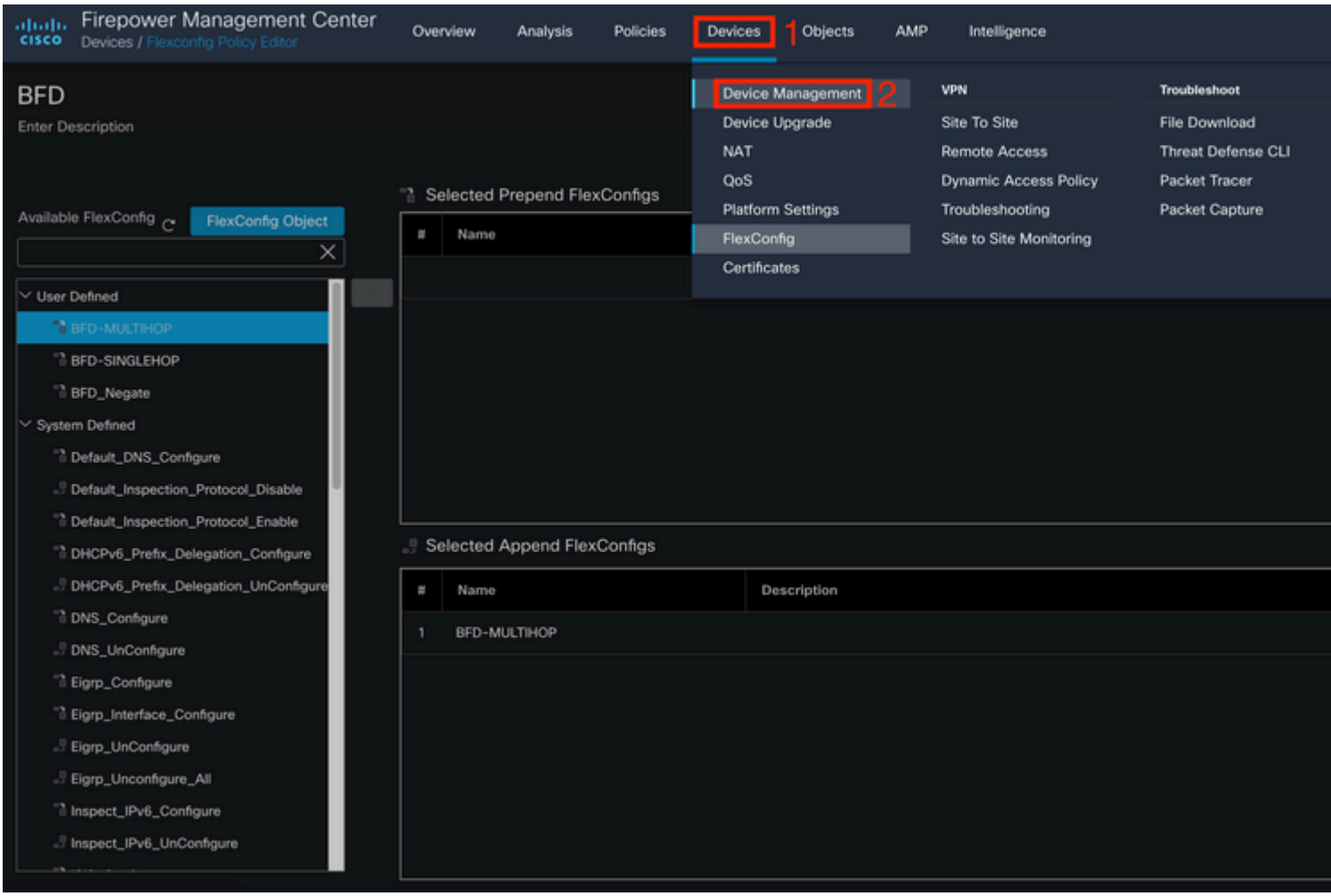
Paso 8.

Seleccione el objeto FlexConfig en la columna de la izquierda y haga clic en el botón > para agregar el objeto a la directiva FlexConfig y haga clic en el botón **Save** botón.



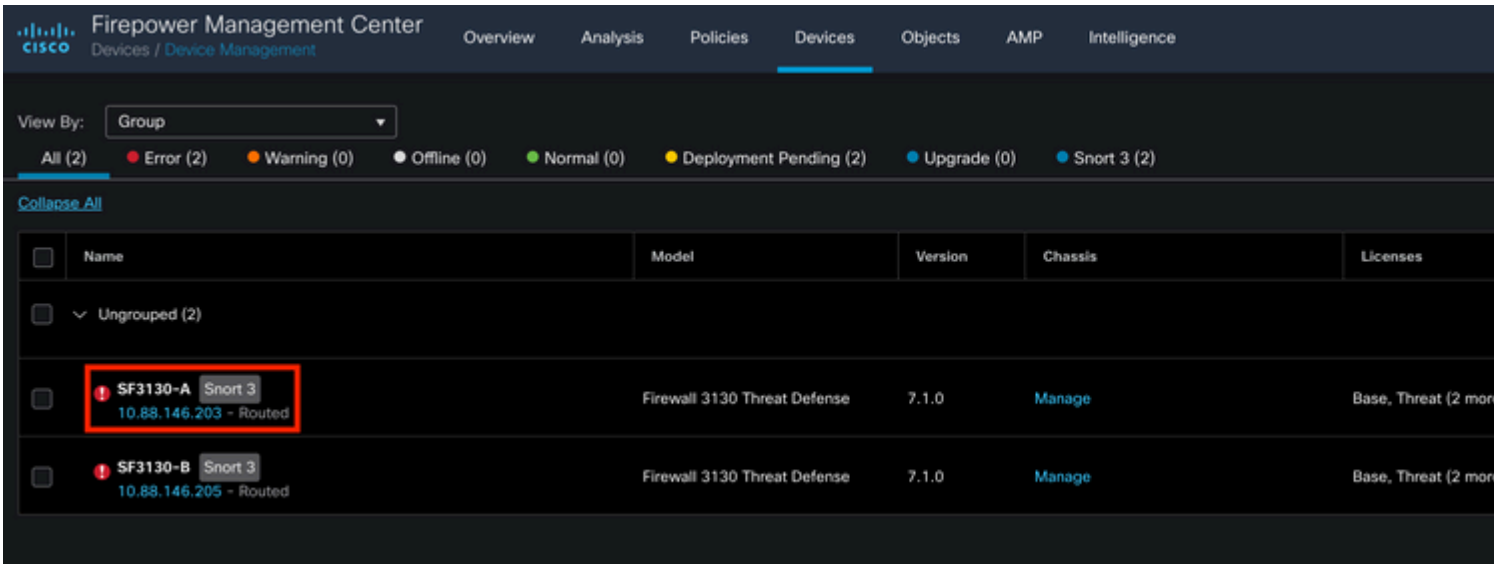
Paso 9.

Haga clic en el **Devices** en la parte superior y haga clic en el botón **Device Management** opción.



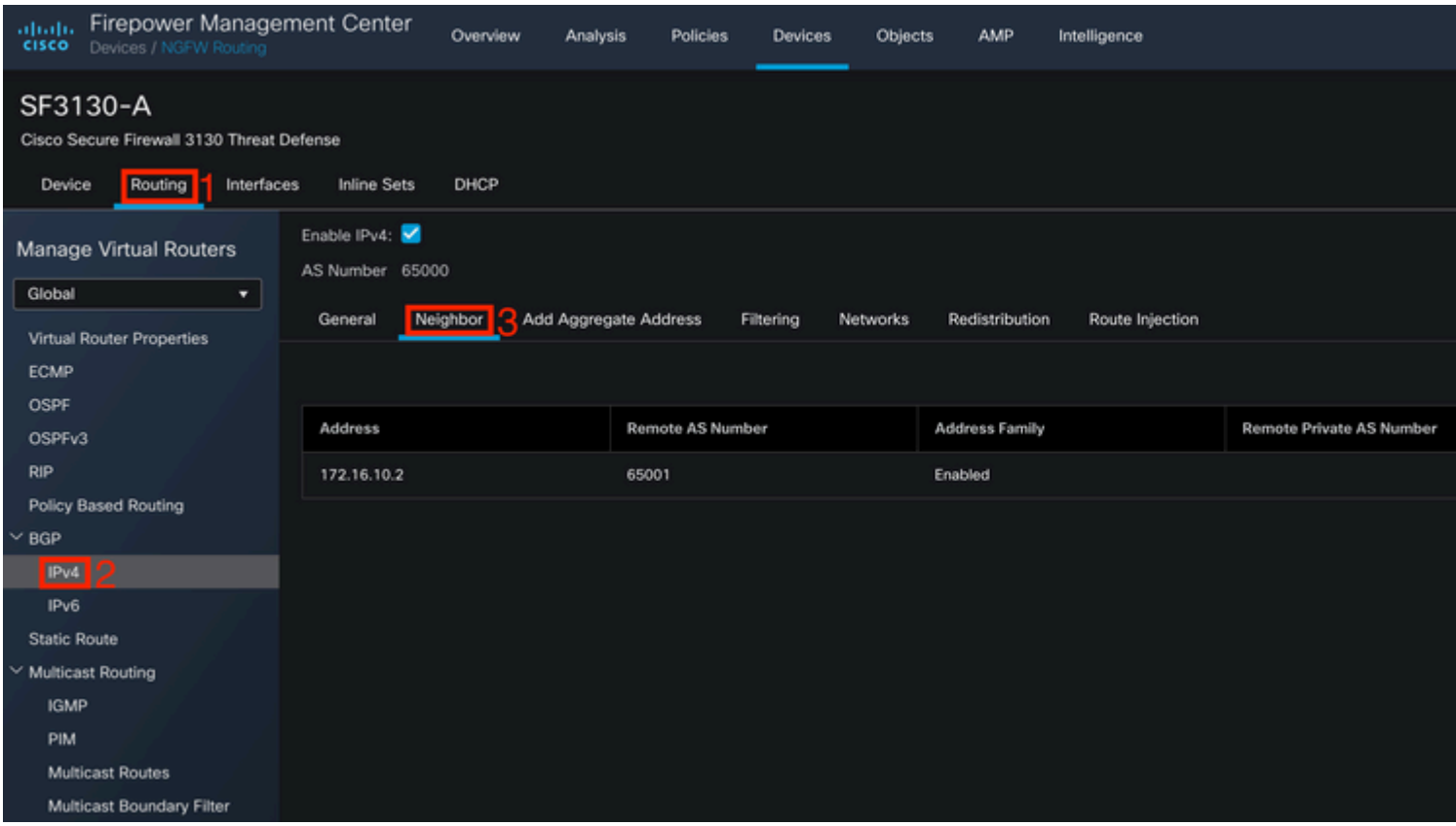
Paso 10.

Seleccione el dispositivo al que se va a asignar la configuración BFD.



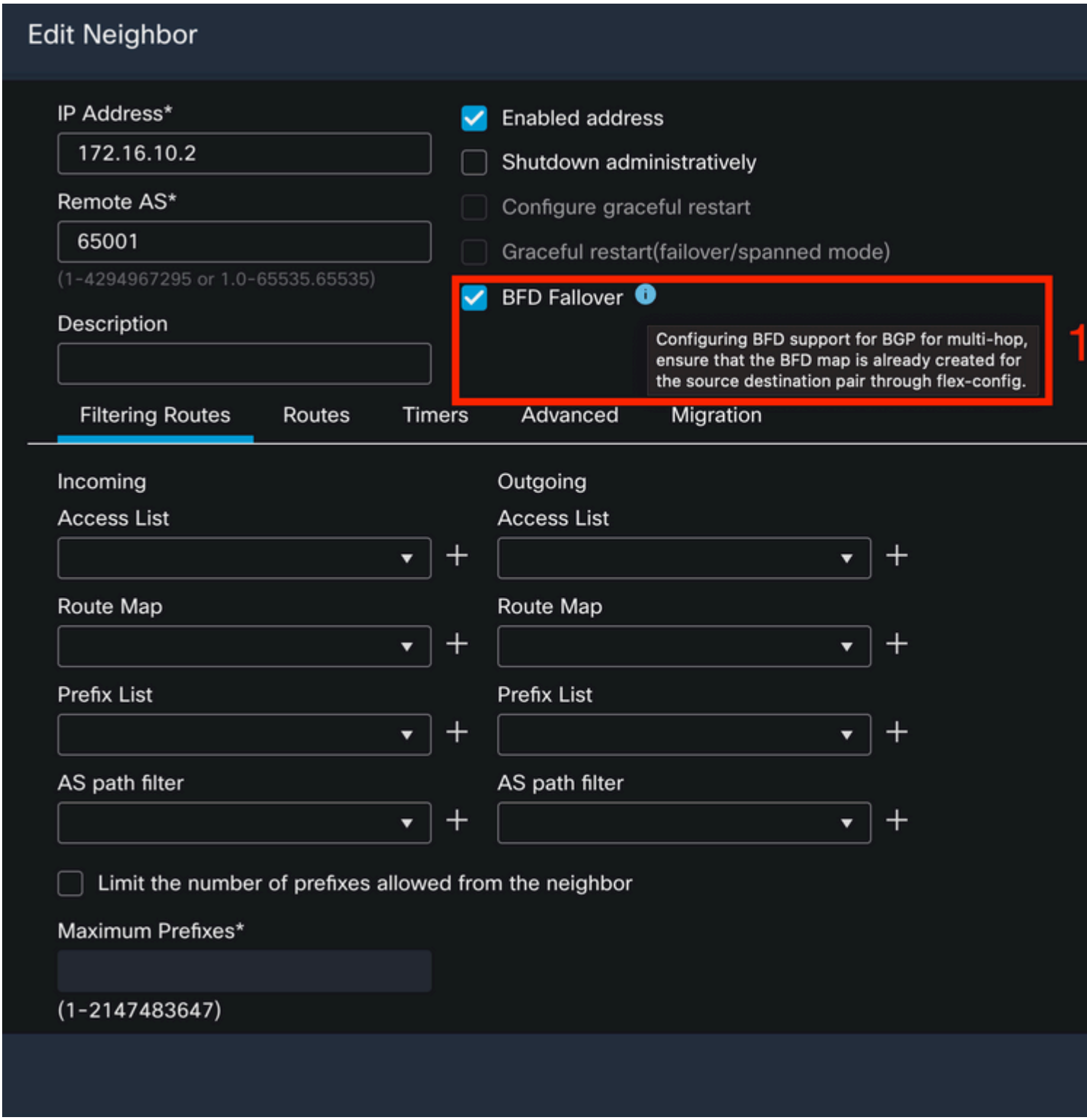
Paso 11.

Haga clic en el Routing y, a continuación, haga clic en el botón**IPv4** or **IPv6**, en función de su configuración en la sección BGP de la columna izquierda, haga clic en el botón **Neighbor** y haga clic en el botón editar lápiz para editarlo.



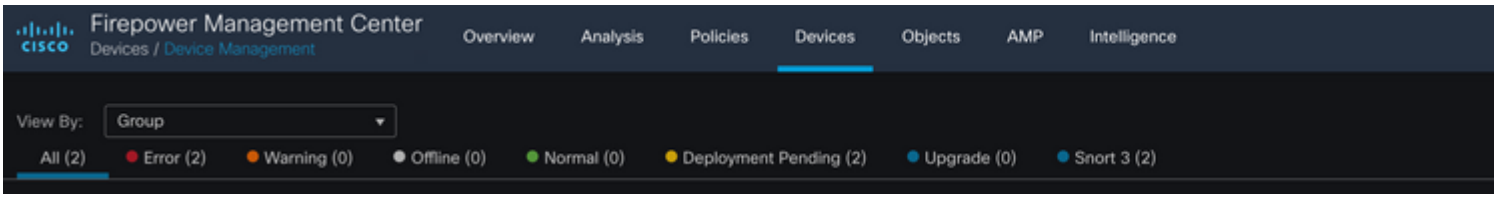
Paso 12.

Seleccione el **checkbox** para BFD fallover y haga clic en el botón **OK** botón.



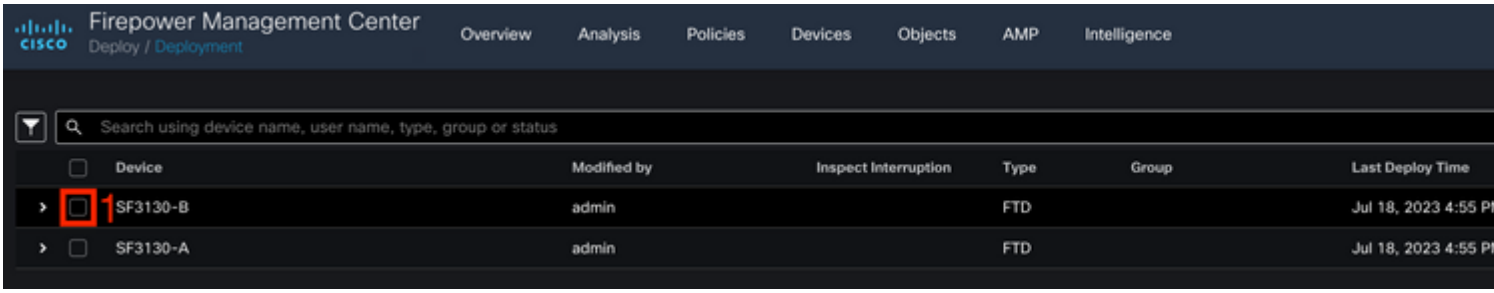
Paso 13.

Haga clic en el **Deploy** y haga clic en el botón **Deployment** botón.



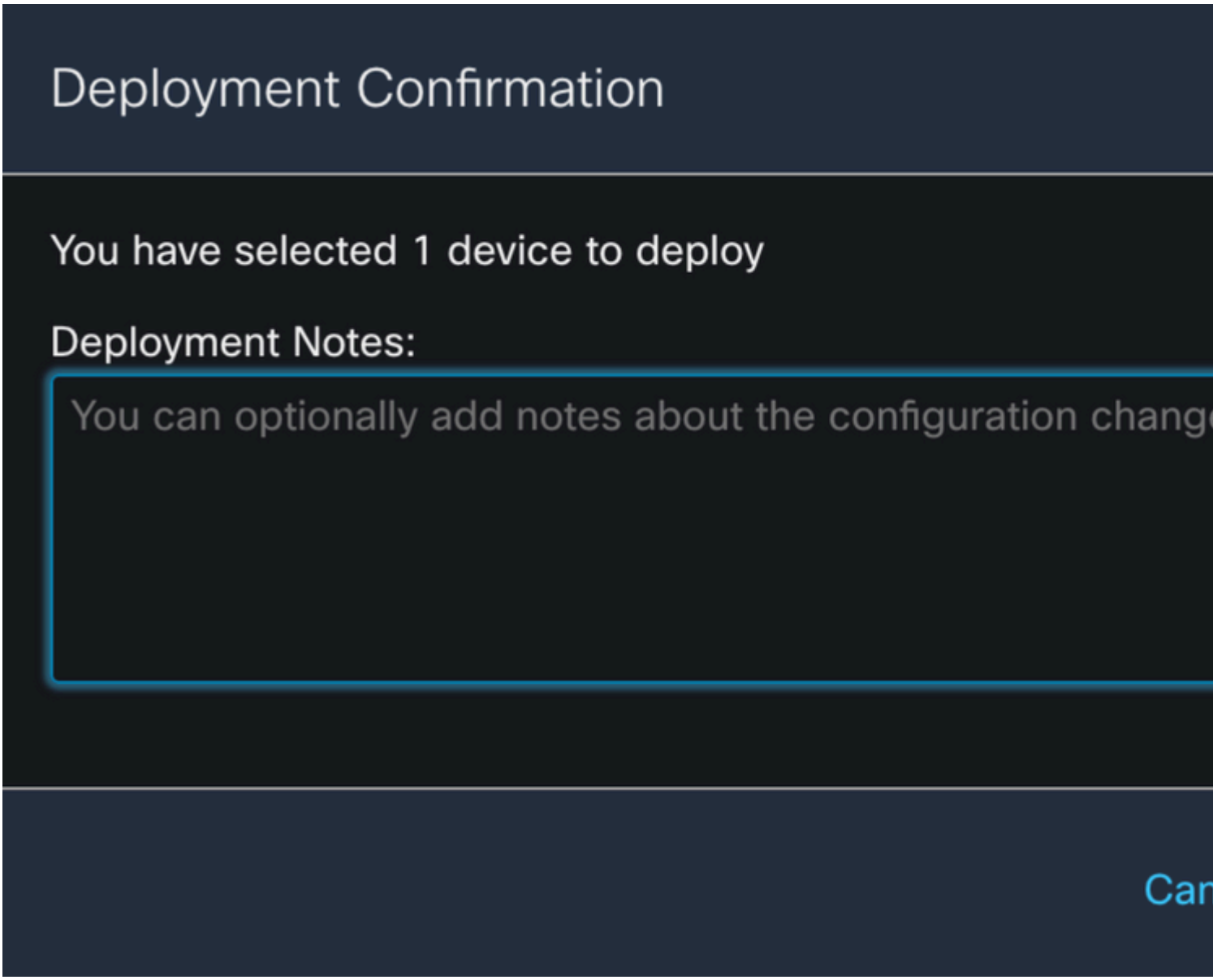
Paso 14.

Seleccione el dispositivo al que se van a asignar los cambios haciendo clic en el botón **checkbox**y, a continuación, haga clic en el**Deploy** botón.



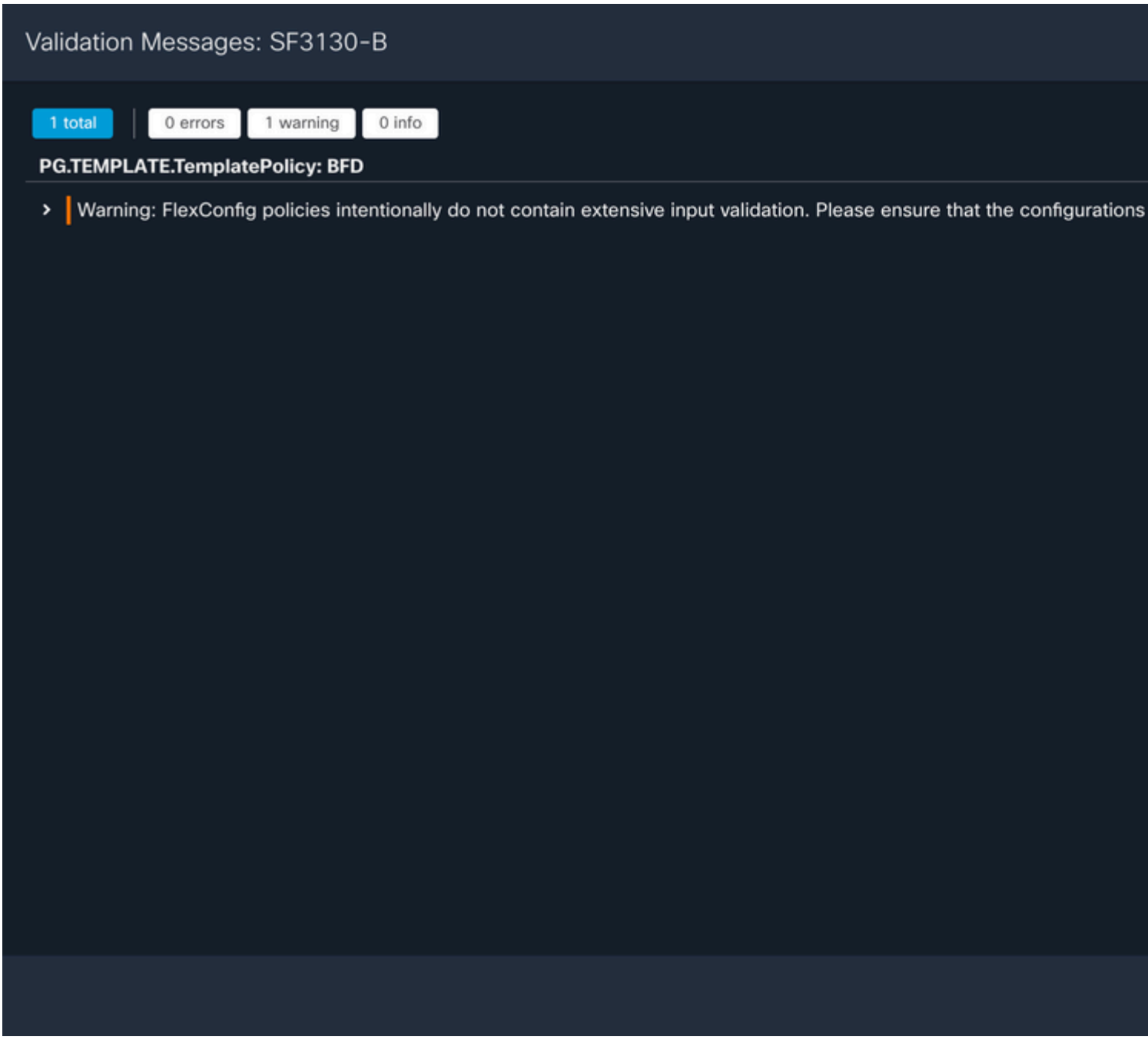
Paso 15.

Haga clic en el **Deploy** botón.



Paso 16.

Haga clic en el **Deploy** botón.



Nota: se espera la advertencia y es sólo informativa.

Verificación

Verifique la configuración BFD y el estado directamente en la sesión CLI con los siguientes comandos.

<#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-A>

enable

Password:
SF3130-A#

show running-config | inc bfd

bfd-template single-hop Template
 bfd template Template
  neighbor 172.16.10.2 fall-over bfd single-hop

SF3130-A#

show bfd summary

                    Session          Up          Down
Total               1                1           0

SF3130-A#

show bfd neighbors


IPv4 Sessions
NeighAddr                                      LD/RD         RH/RS       State   Int
172.16.10.2                                     1/1          Up
```

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

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).