

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

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

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

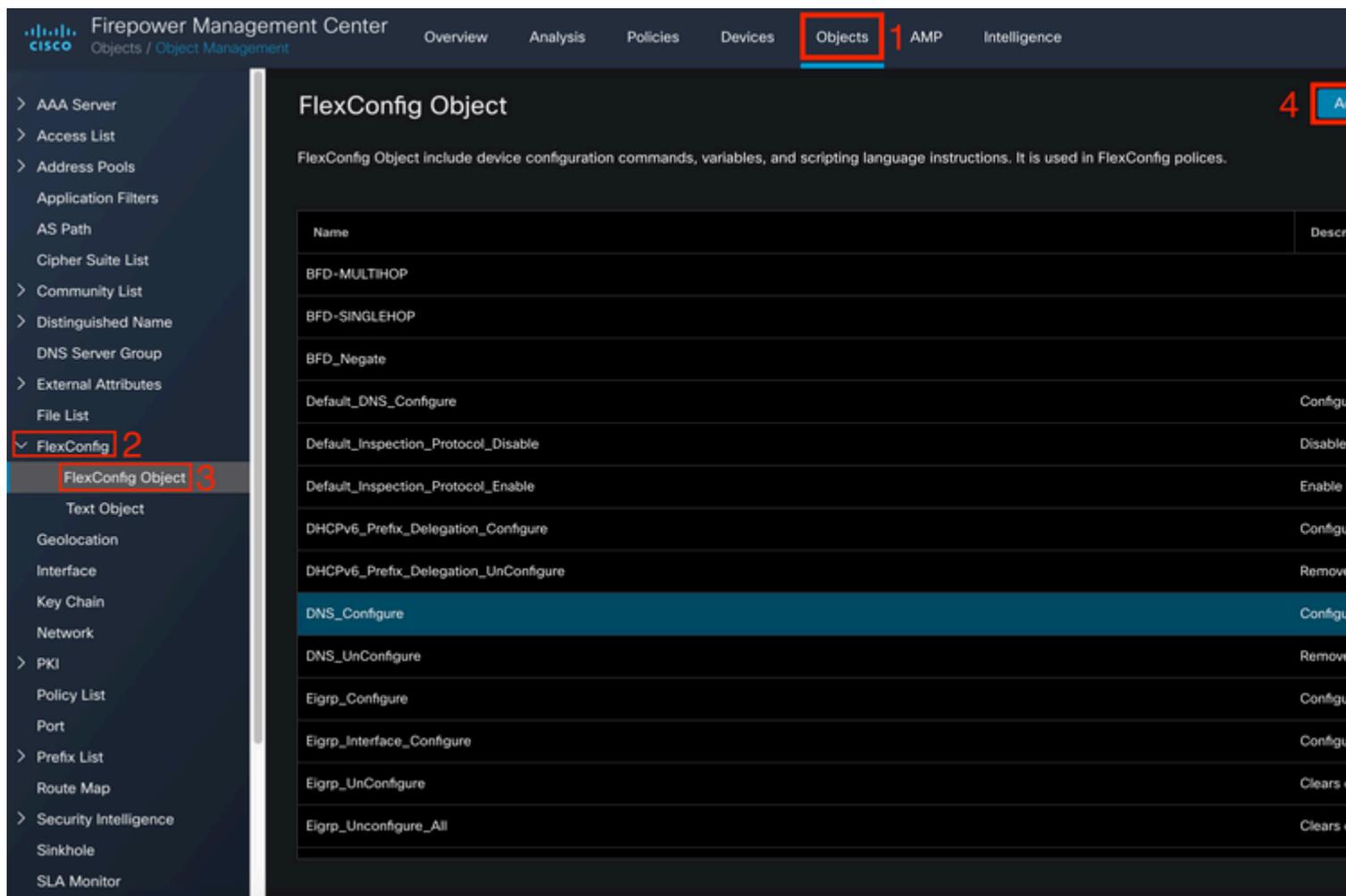
Las configuraciones BFD en FMC que ejecutan versiones 7.2 y anteriores deben configurarse con objetos y políticas Flex-Config.

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-md5 | 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|8 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.

Edit FlexConfig Object

Name:

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert Deployment: Type:

```
bfd-template single-hop TEMPLATE1
echo
interval both 50
authentication sha-1 0 cisco key-id 10
```

▼ Variables

Name	Dimension	Default Value	Property (Type:Name)	Override
No records to display				

Paso 3.

Asocie la plantilla BFD a la interfaz.

Edit FlexConfig Object

Name:

BFD-SINGLEHOP

Description:



Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▾



Deployment:

Once ▾

Type:

Append

```
bfd-template single-hop TEMPLATE1
echo
interval both 50
authentication sha-1 0 cisco key-id 10

interface Ethernet1/7
bfd template TEMPLATE1
```

▾ Variables

Name	Dimension	Default Value	Property (Type:Name)	Override
No records to display				

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.

Edit FlexConfig Object

Name:

BFD-MULTIHOP

Description:



Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▾



Deployment:

Once ▾

Type:

Append

```
bfd-template multi-hop MULTI-TEMPLATE1
  interval both 50

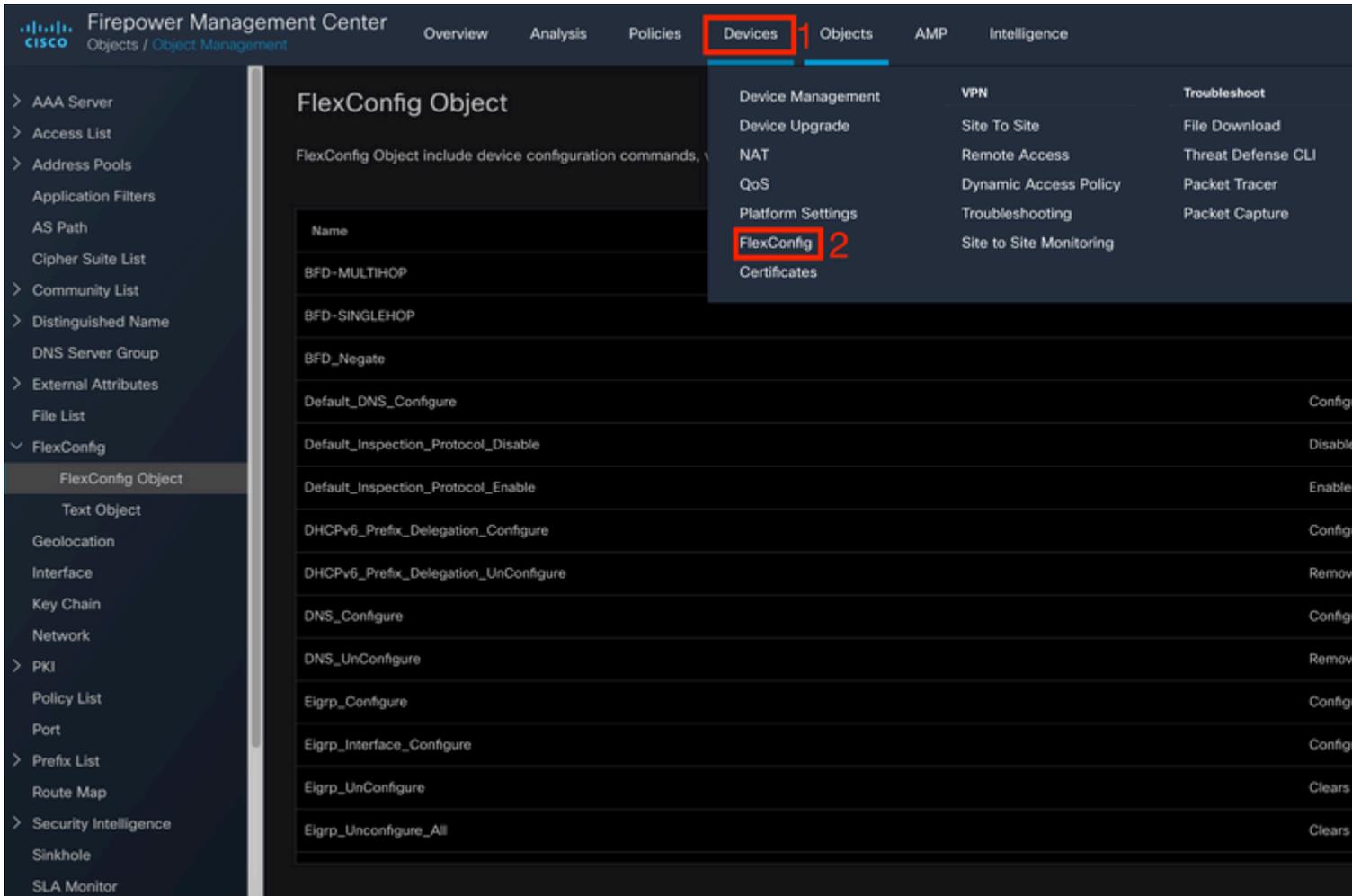
bfd map ipv4 10.11.11.0/24 10.36.42.5/32 MULTI-TEMPLATE1
```

▾ Variables

Name	Dimension	Default Value	Property (Type:Name)	Override
No records to display				

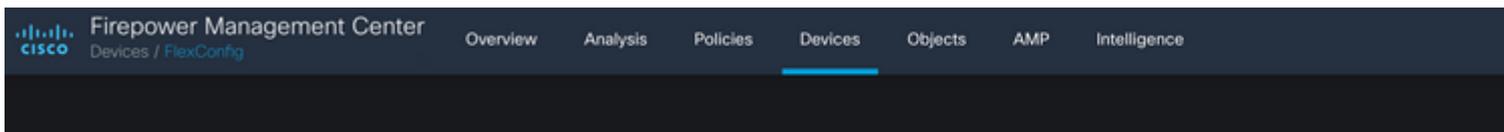
Paso 5.

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.

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

New Policy

Name:

BFD

1

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

🔍 Search by name or value

SF3130-A

SF3130-B

2

Add to Policy

Selected Devices

SF3130-A

SF3130-B

3

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.

Firepower Management Center
Devices / Flexconfig Policy Editor

Overview Analysis Policies **Devices** Objects AMP Intelligence

BFD

Enter Description

Available FlexConfig FlexConfig Object

- User Defined
 - BFD-MULTIHOP** 1
 - BFD-SINGLEHOP
 - BFD_Negate
- System Defined
 - Default_DNS_Configure
 - Default_Inspection_Protocol_Disable
 - Default_Inspection_Protocol_Enable
 - DHCPv6_Prefix_Delegation_Configure
 - DHCPv6_Prefix_Delegation_UnConfigure
 - DNS_Configure
 - DNS_UnConfigure
 - Eigrp_Configure
 - Eigrp_Interface_Configure
 - Eigrp_UnConfigure
 - Eigrp_Unconfigure_All
 - Inspect_IPv6_Configure
 - Inspect_IPv6_UnConfigure

Selected Prepend FlexConfigs

#	Name	Description
---	------	-------------

Selected Append FlexConfigs

#	Name	Description
1	BFD-MULTIHOP	

Paso 9.

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

Firepower Management Center
Devices / Flexconfig Policy Editor

Overview Analysis Policies **Devices** 1 Objects AMP Intelligence

BFD
Enter Description

Available FlexConfig X

- User Defined
 - BFD-MULTIHOP**
 - BFD-SINGLEHOP
 - BFD_Negate
- System Defined
 - Default_DNS_Configure
 - Default_Inspection_Protocol_Disable
 - Default_Inspection_Protocol_Enable
 - DHCPv6_Prefix_Delegation_Configure
 - DHCPv6_Prefix_Delegation_UnConfigure
 - DNS_Configure
 - DNS_UnConfigure
 - Eigrp_Configure
 - Eigrp_Interface_Configure
 - Eigrp_UnConfigure
 - Eigrp_Unconfigure_All
 - Inspect_IPv6_Configure
 - Inspect_IPv6_UnConfigure

Selected Prepend FlexConfigs

#	Name

Selected Append FlexConfigs

#	Name	Description
1	BFD-MULTIHOP	

Paso 10.

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

Firepower Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects AMP Intelligence

View By: Group

All (2) Error (2) Warning (0) Offline (0) Normal (0) Deployment Pending (2) Upgrade (0) Snort 3 (2)

Collapse All

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses
<input type="checkbox"/>	Ungrouped (2)				
<input type="checkbox"/>	SF3130-A Snort 3 10.88.146.203 - Routed	Firewall 3130 Threat Defense	7.1.0	Manage	Base, Threat (2 mor
<input type="checkbox"/>	SF3130-B Snort 3 10.88.146.205 - Routed	Firewall 3130 Threat Defense	7.1.0	Manage	Base, Threat (2 mor

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.

Firepower Management Center
Devices / NGFW Routing

Overview Analysis Policies **Devices** Objects AMP Intelligence

SF3130-A

Cisco Secure Firewall 3130 Threat Defense

Device **Routing** 1 Interfaces Inline Sets DHCP

Manage Virtual Routers

Global

- Virtual Router Properties
- ECMP
- OSPF
- OSPFv3
- RIP
- Policy Based Routing
- BGP
 - IPv4** 2
 - IPv6
 - Static Route
- Multicast Routing
 - IGMP
 - PIM
 - Multicast Routes
 - Multicast Boundary Filter

Enable IPv4:

AS Number 65000

General **Neighbor** 3 Add Aggregate Address Filtering Networks Redistribution Route Injection

Address	Remote AS Number	Address Family	Remote Private AS Number
172.16.10.2	65001	Enabled	

Paso 12.

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

Edit Neighbor

IP Address*

172.16.10.2

Enabled address

Shutdown administratively

Remote AS*

65001

(1-4294967295 or 1.0-65535.65535)

Configure graceful restart

Graceful restart(failover/spanned mode)

Description

BFD Fallover ⓘ

Configuring BFD support for BGP for multi-hop, ensure that the BFD map is already created for the source destination pair through flex-config.

Filtering Routes

Routes

Timers

Advanced

Migration

Incoming

Outgoing

Access List

Access List

+

+

Route Map

Route Map

+

+

Prefix List

Prefix List

+

+

AS path filter

AS path filter

+

+

Limit the number of prefixes allowed from the neighbor

Maximum Prefixes*

(1-2147483647)

Paso 13.

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

Firepower Management Center
Devices / Device Management

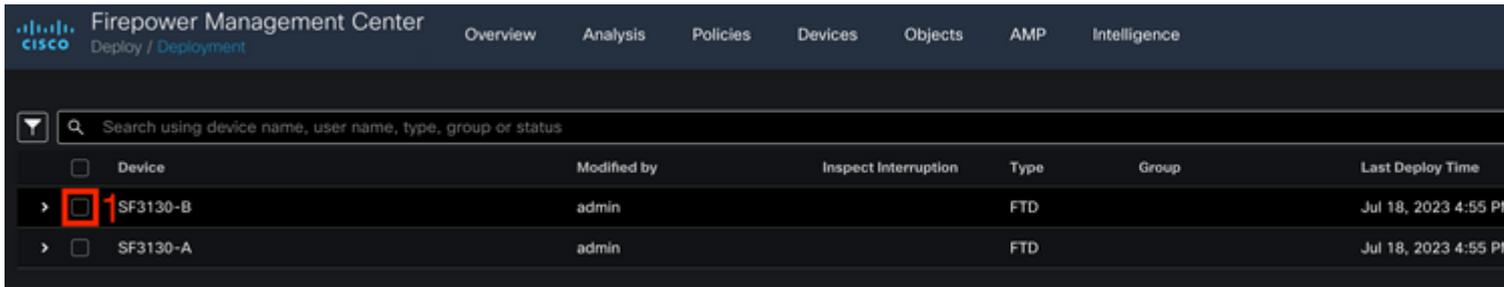
Overview Analysis Policies **Devices** Objects AMP Intelligence

View By: Group

All (2) Error (2) Warning (0) Offline (0) Normal (0) Deployment Pending (2) Upgrade (0) Snort 3 (2)

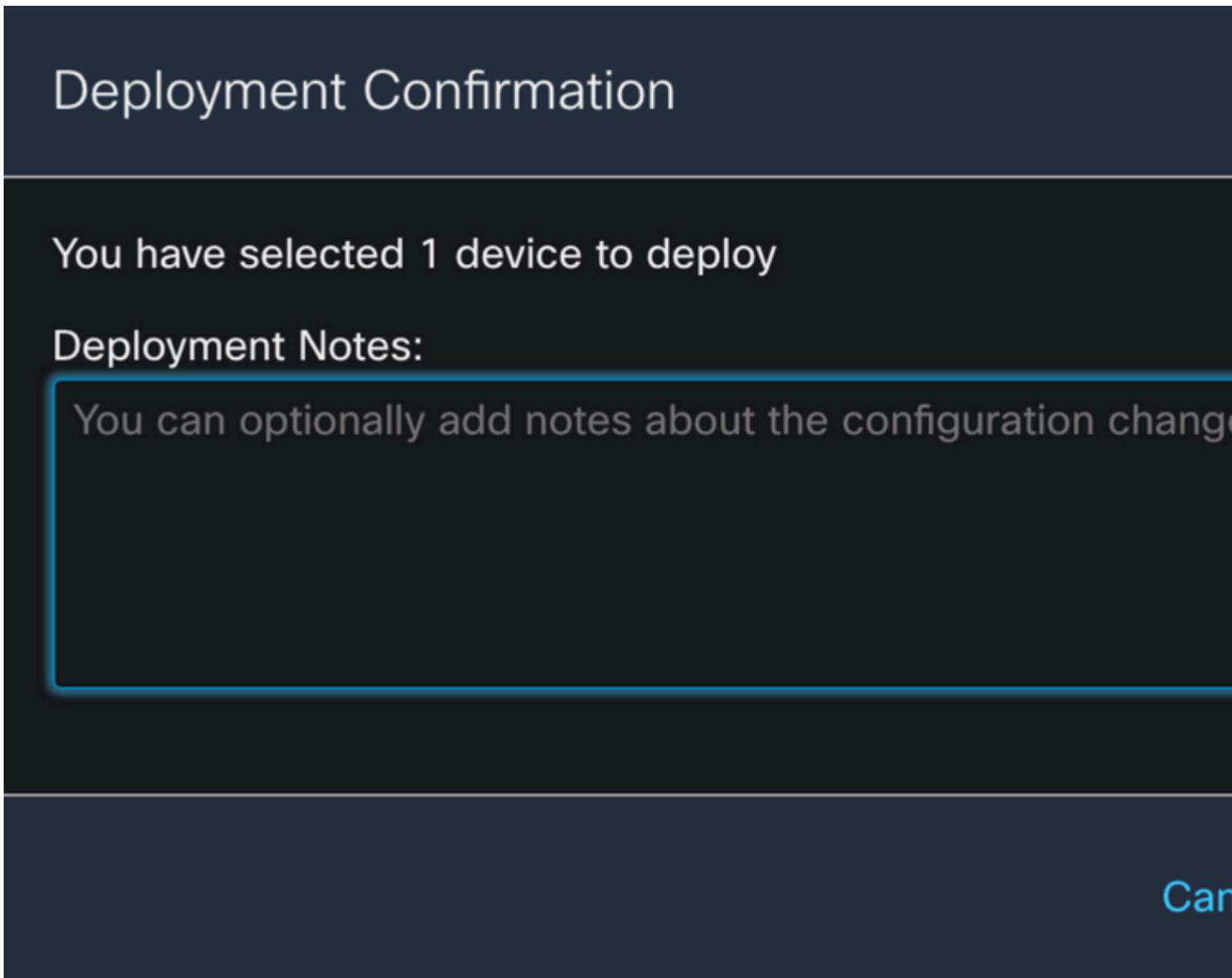
Paso 14.

Seleccione el dispositivo al que se van a asignar los cambios haciendo clic en el botón checkboxy, a continuación, haga clic en elDeploy botón.



Paso 15.

Haga clic en el **Deploy** botón.



Paso 16.

Haga clic en el **Deploy** botón.

Validation Messages: SF3130-B

1 total

0 errors

1 warning

0 info

PG.TEMPLATE.TemplatePolicy: BFD

> | Warning: FlexConfig policies intentionally do not contain extensive input validation. Please ensure that the configurations

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).