

# Configure o BFD no Secure Firewall Threat Defense com Flex-Config

## Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Verificar](#)

[Troubleshooting](#)

## Introdução

Este documento descreve como configurar o protocolo BFD no Secure Firewall Management Center executando a versão 7.2 e anterior com o Flex-Config.

## Pré-requisitos

Border Gateway Protocol (BGP) configurado no Cisco Secure Firewall Threat Defense (FTD) com o Cisco Secure Firewall Management Center (FMC).

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- protocolo BGP
- Conceitos de BFD

## Componentes Utilizados

-Cisco Secure Firewall Management Center executando a versão 7.2 ou anterior.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

A Detecção de Encaminhamento Bidirecional (BFD) é um protocolo de detecção projetado para fornecer tempos de detecção de falha de caminho de encaminhamento rápido para todos os tipos de mídia, encapsulamentos, topologias e protocolos de roteamento.

## Configurar

As configurações de BFD no FMC executando versões 7.2 e anteriores devem ser configuradas com políticas e objetos Flex-Config.

Etapa 1.

Crie o modelo BFD por meio do Objeto Flexconfig.

O modelo BFD especifica um conjunto de valores de intervalo BFD. Os valores do intervalo BFD configurados no modelo BFD não são específicos de uma única interface. Você também pode configurar a autenticação para sessões de salto único e multi-salto.

Para criar o objeto Flex-Config, selecione a opção **Objects Tab** na parte superior, clique no botão **FlexConfig** na coluna esquerda e clique no botão **FlexConfig Object** e clique em **Add FlexConfig Object**.

The screenshot shows the Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects' (1), 'AMP', and 'Intelligence'. The left sidebar shows a tree view of configuration objects, with 'FlexConfig' (2) and 'FlexConfig Object' (3) highlighted. The main content area displays a table of FlexConfig Objects. The 'DNS\_Configure' object is selected (4).

Name	Description
BFD-MULTIHOP	
BFD-SINGLEHOP	
BFD_Negate	
Default_DNS_Configure	Configure
Default_Inspection_Protocol_Disable	Disable
Default_Inspection_Protocol_Enable	Enable
DHCPv6_Prefix_Delegation_Configure	Configure
DHCPv6_Prefix_Delegation_UnConfigure	Remove
<b>DNS_Configure</b>	<b>Configure</b>
DNS_UnConfigure	Remove
Eigrp_Configure	Configure
Eigrp_Interface_Configure	Configure
Eigrp_UnConfigure	Clear
Eigrp_Unconfigure_All	Clear

Etapa 2.

Adicione os parâmetros necessários para o protocolo BFD:

O modelo BFD especifica um conjunto de valores de intervalo BFD. Os valores do intervalo BFD configurados no modelo BFD não são específicos de uma única interface. Você também pode configurar a autenticação para sessões de salto único e multi-salto.

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

- salto único - Especifica um modelo de BFD de salto único.
- multi-hop - Especifica um modelo de BFD multi-hop.
- nome\_do\_modelo - Especifica o nome do modelo. O nome do modelo não pode conter espaços.
- (Opcional) Configure o Echo em um modelo BFD de salto único.

---

**Observação:** você só pode ativar o modo de eco em um modelo de salto único.

---

Configure os intervalos no modelo BFD:

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

- both - Capacidade mínima de intervalo de transmissão e recepção.
- O intervalo em milissegundos. O intervalo é 50 a 999.
- microssegundos - Especifica o intervalo BFD em microssegundos para both e min-tx.
- microssegundos - O intervalo é de 50.000 a 999.000.
- min-tx - O recurso de intervalo mínimo de transmissão.

Configure a autenticação no modelo BFD:

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

- authentication - Especifica o tipo de autenticação.
- md5 - Autenticação Message Digest 5 (MD5).
- meticulous-md5 - Autenticação MD5 com chave meticulosa.
- meticulous-sha-1 - Autenticação SHA-1 com chave meticulosa.
- sha-1 - Autenticação SHA-1 com chave.
- 0|8 - 0 especifica que uma senha NÃO CRIPTOGRAFADA será exibida em seguida. 8 especifica que uma senha CRIPTOGRAFADA será exibida em seguida.
- word - A senha (chave) BFD, que é uma senha/chave de um único dígito com até 29 caracteres. Não há suporte para senhas que comecem com um dígito seguido por um espaço em branco; por exemplo, 0 passagem e 1 não são válidos.
- key-id - O ID da chave de autenticação.
- id - O ID da chave compartilhada que corresponde à string da chave. O intervalo é de 0 a 255 caracteres.

## 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
```

▾ Variables

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

Etapa 3.

Associe o modelo BFD à interface.

## 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				

---

**Observação:** associe o modelo de multi-hop BFD a um mapa de destinos.

---

Etapa 4 (opcional).

Crie um mapa BFD contendo destinos que você pode associar a um modelo multi-hop. Você deve ter um modelo de BFD de vários saltos já configurado.

Associe o modelo multi-hop BFD a um mapa de destinos:

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

- ipv4 “ Configura um endereço IPv4.
- ipv6 “ Configura um endereço IPv6.
- destination/cdir “ Especifica o prefixo/comprimento de destino. O formato é A.B.C.D/<0-32>.
- source/cdir “ Especifica o prefixo/comprimento de destino. O formato é X:X:X;X::X/<0-128>.
- nome-do-modelo “ Especifica o nome do modelo multi-hop associado a este mapa BFD.

Clique no botão **Save** para salvar o 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

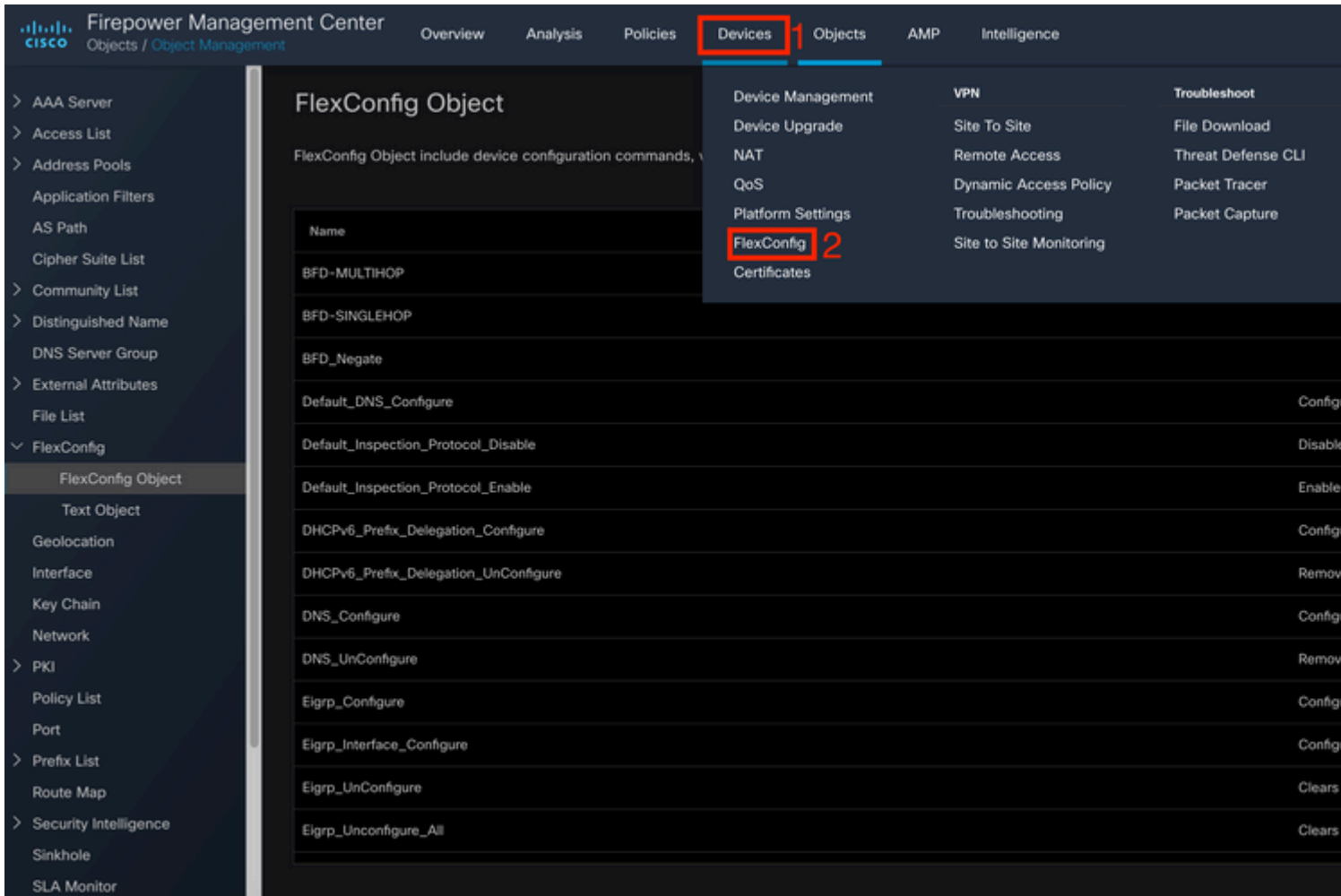
bfd map ipv4 10.11.11.0/24 10.36.42.5/32 MULTI-TEMPLATE1
```

▾ Variables

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

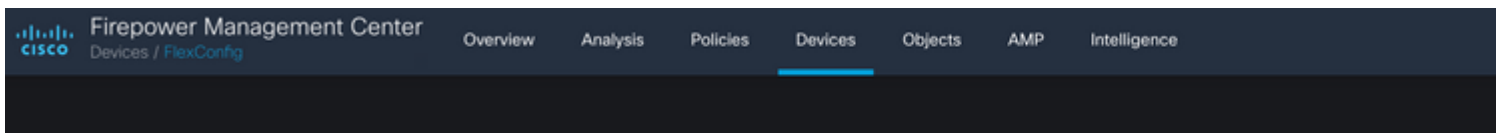
Etapa 5.

Clique no botão **Devices** na parte superior e selecione a guia **FlexConfig** opção.



Etapa 6.

Para criar uma nova Política FlexConfig, clique no botão **New Policy** botão.



Passo 7.

Nome a regra e selecione os dispositivos atribuídos à regra. Clique no botão **Add to Policy** e clique no botão **Save** botão.



## 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

Etapa 8.

Selecione o Objeto FlexConfig na coluna esquerda e clique no botão > para adicionar o objeto à Política FlexConfig e clique no botão Save botão.

Firepower Management Center  
Devices / Flexconfig Policy Editor

Overview Analysis Policies **Devices** Objects AMP Intelligence

### BFD

Enter Description

Available FlexConfig **FlexConfig Object**

**1**

- 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

**2**

Selected Prepend FlexConfigs

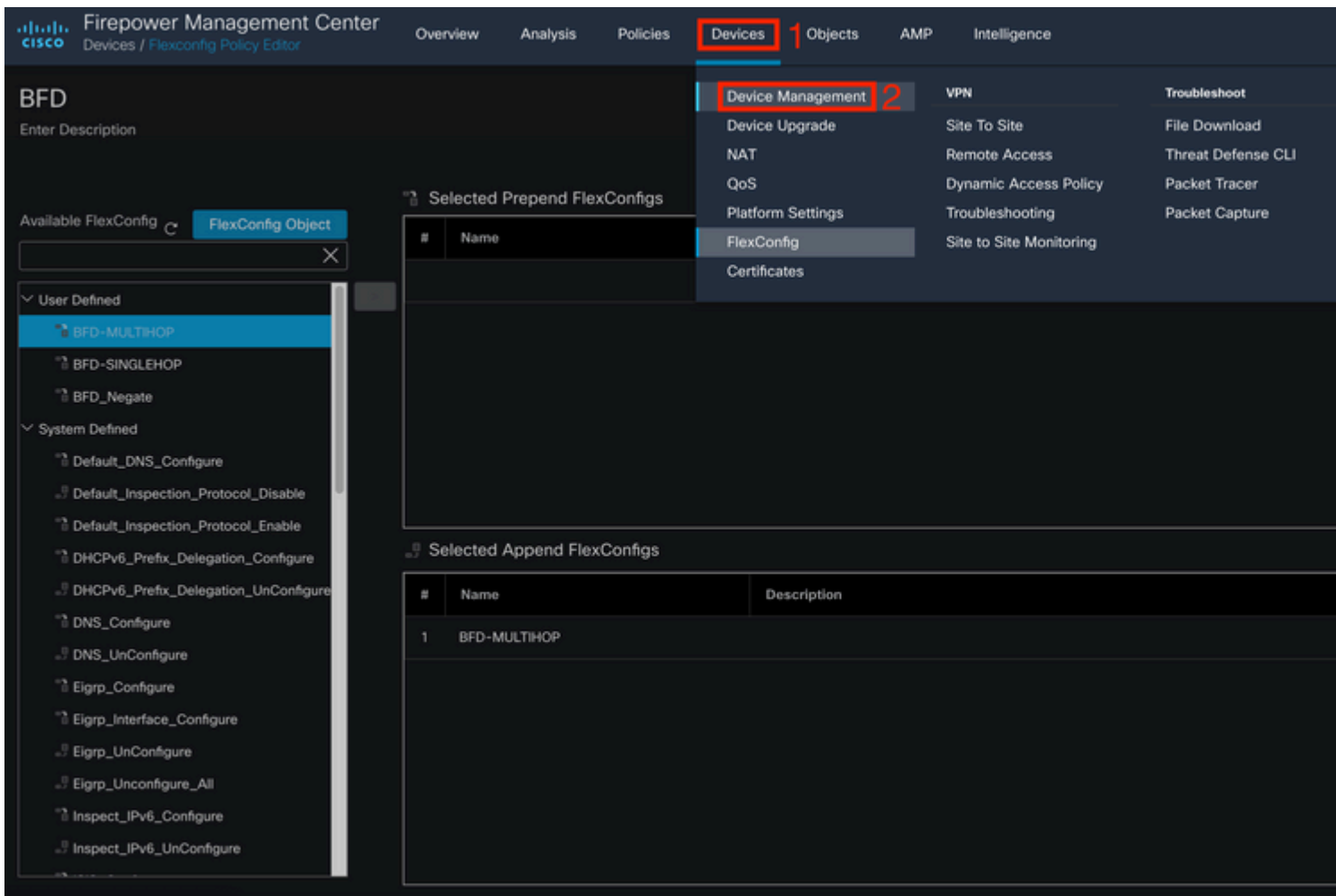
#	Name	Description
---	------	-------------

Selected Append FlexConfigs

#	Name	Description
1	BFD-MULTIHOP	

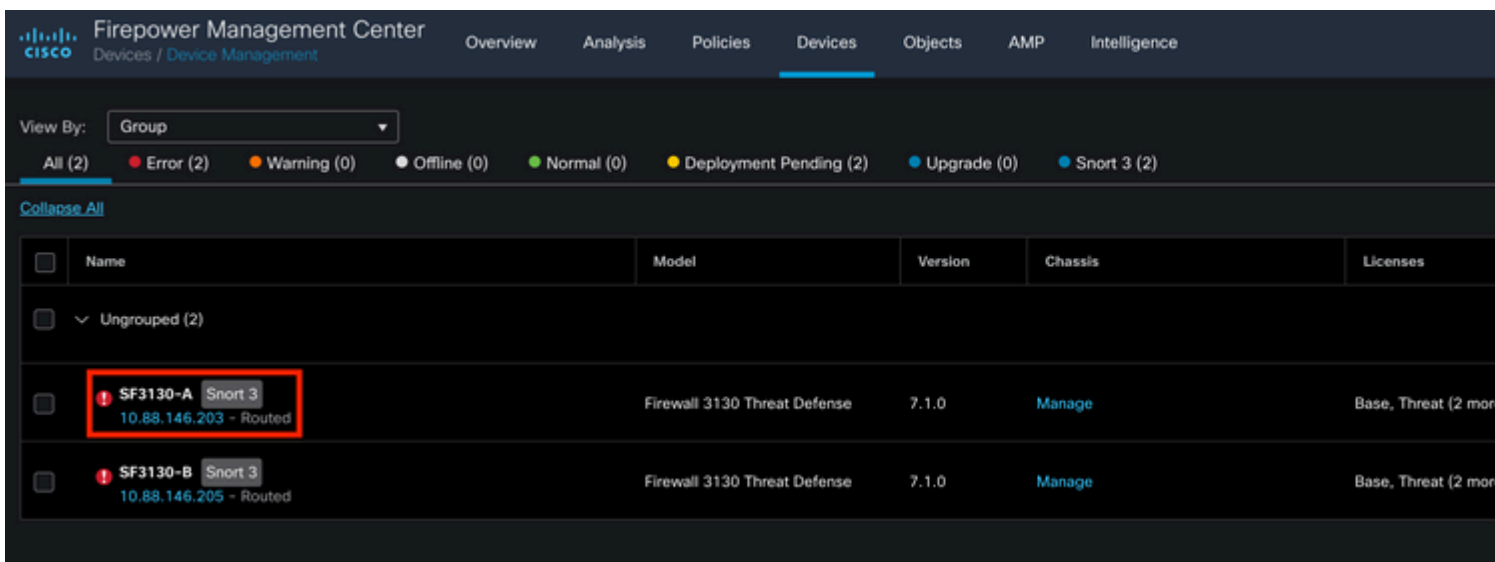
Etapa 9.

Clique no botão **Devices** na parte superior e clique no botão **Device Management** opção.



Etapa 10.

Selecione o dispositivo ao qual a configuração BFD será atribuída.



Etapa 11.

Clique no botão Routing e clique no botão IPv4 or IPv6, dependendo da sua configuração na seção BGP na coluna esquerda, em seguida, clique no Neighbor e clique no botão editar lápis para editá-lo.

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	

Etapa 12.

Selecione a opção **checkbox** para failover de BFD e clique no botão **OK** botão.

## 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)

Etapa 13.

Clique no botão **Deploy** e, em seguida, clique no botão **Deployment** botão.

Firepower Management Center  
Devices / Device Management

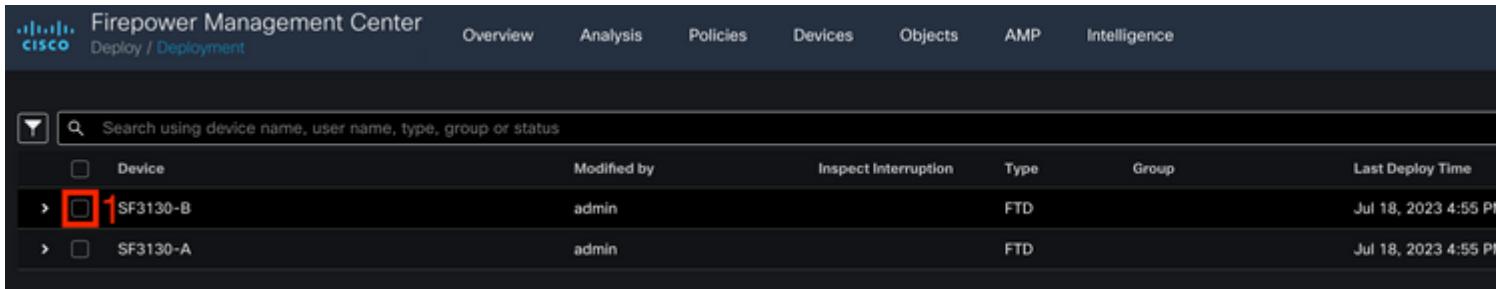
Overview Analysis Policies **Devices** Objects AMP Intelligence

View By: Group

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

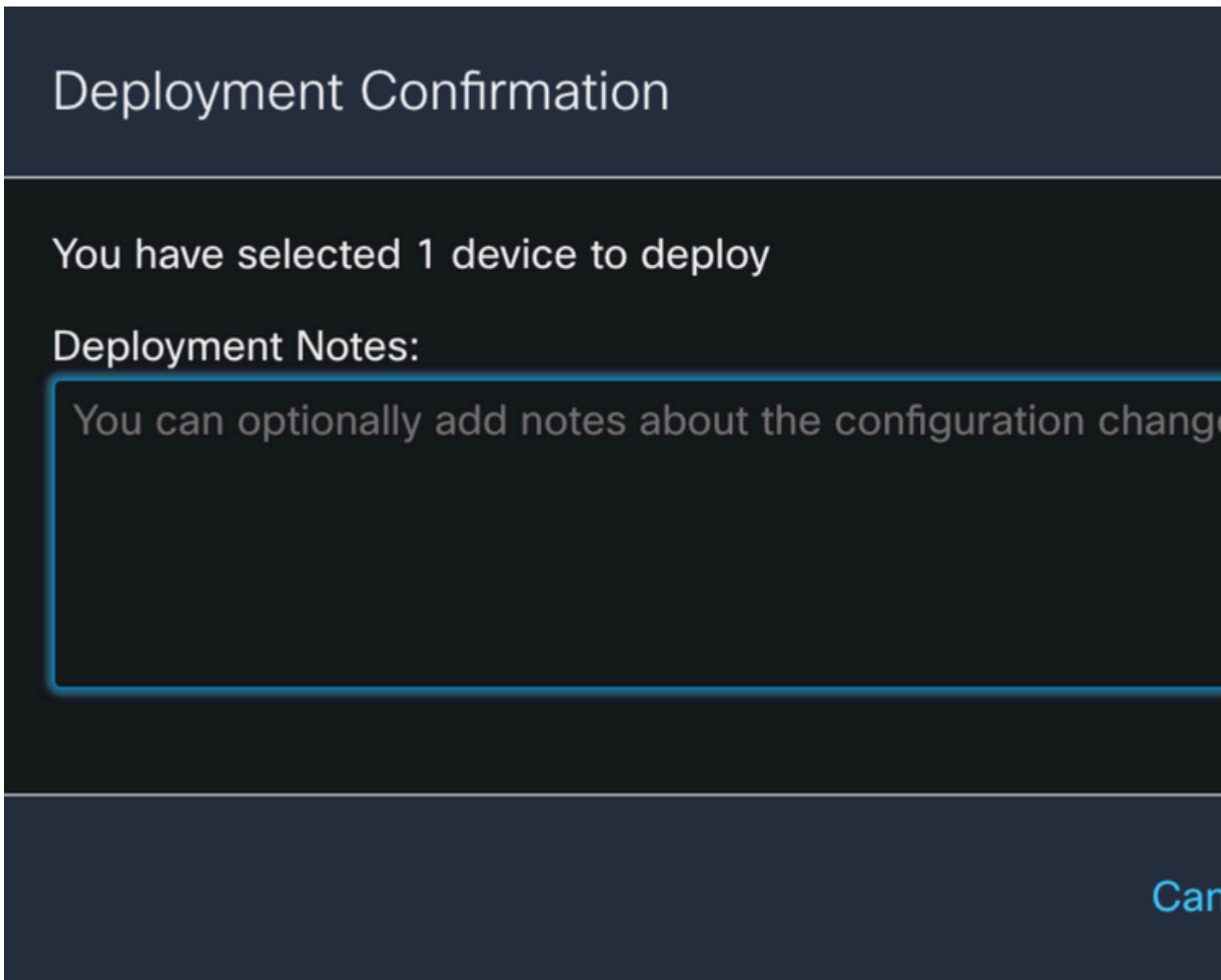
Etapa 14.

Selecione o dispositivo ao qual as alterações serão atribuídas clicando no **checkbox**, em seguida, clique no botão **Deploy** botão.



Etapa 15.

Clique no botão **Deploy** botão.



Etapa 16.

Clique no botão **Deploy** botão.

## 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

---

**Observação:** o aviso é esperado e é apenas informativo.

---

## Verificar

Verifique a configuração do BFD e o status diretamente na sessão CLI com os próximos 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		

## Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.



## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.