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

Contents

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

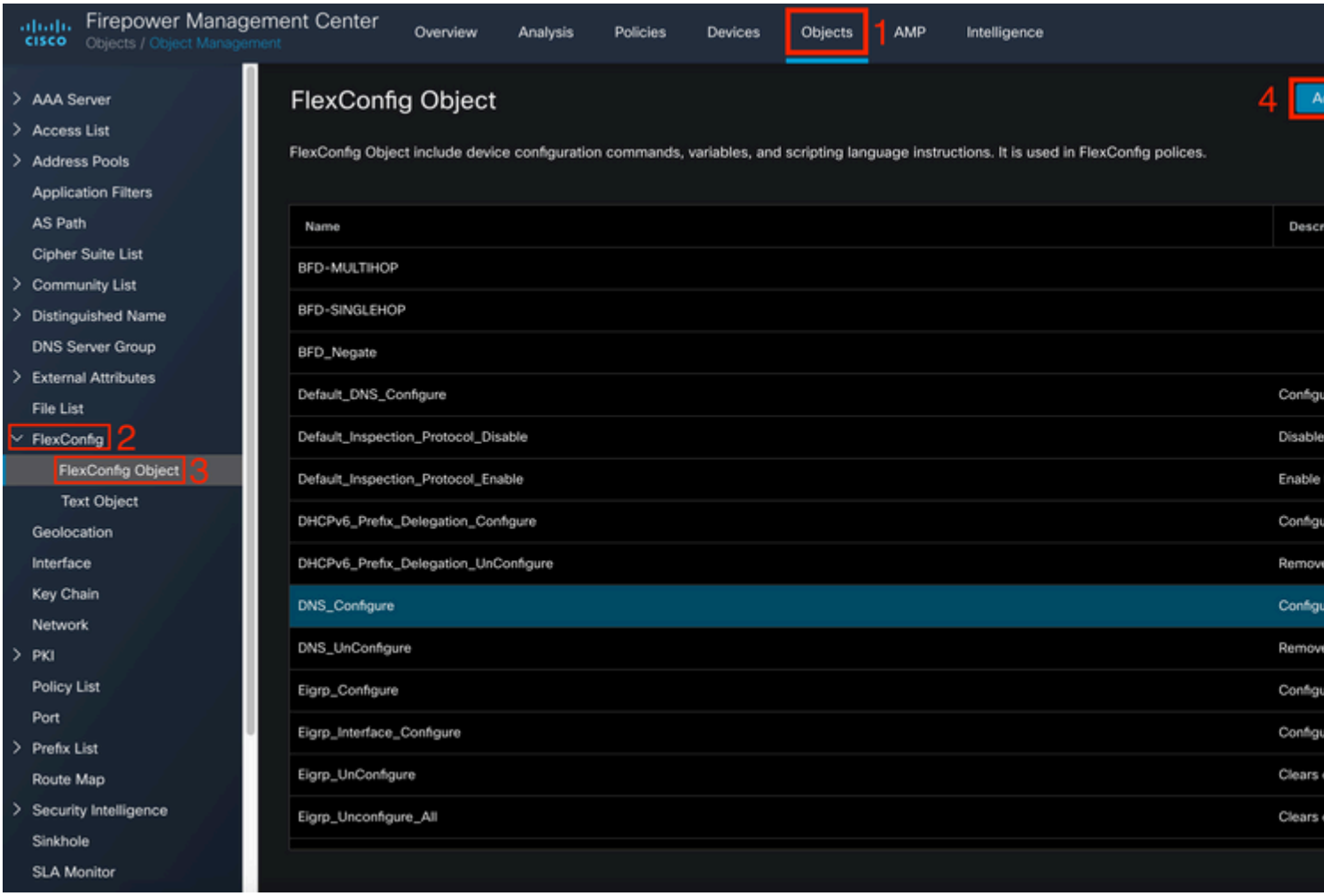
As configurações de BFD no FMC executando versões 7.2 e anteriores devem ser configuradas com políticas e objetos Flex-Config.

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**.



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 â€” Especifica um modelo de BFD multi-hop.
- nome_do_modelo â€” 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:

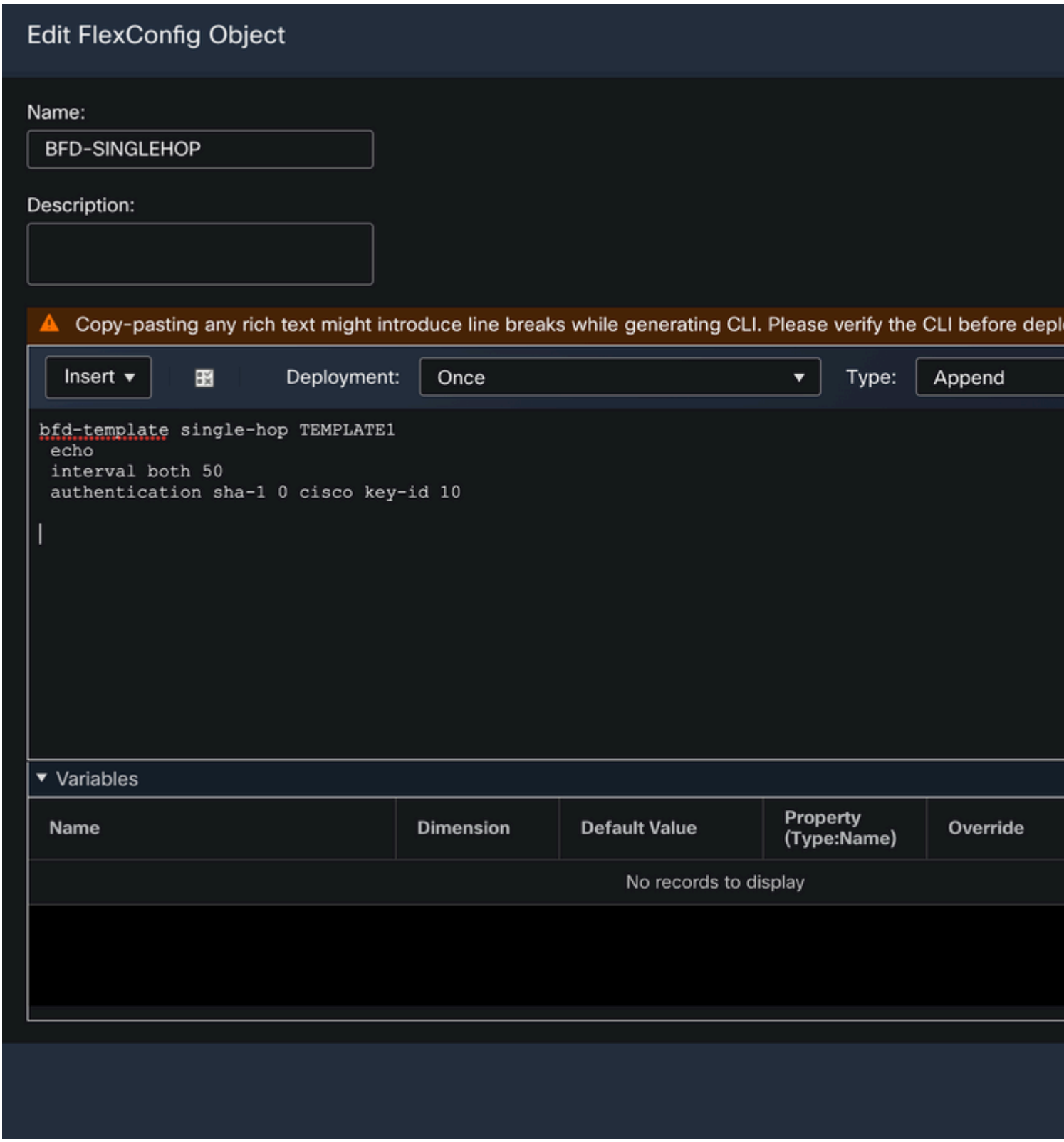
```
interval both milliseconds | microseconds {both | min-tx} microseconds | min-tx milliseconds echo
```

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

Configure a autenticação no modelo BFD:

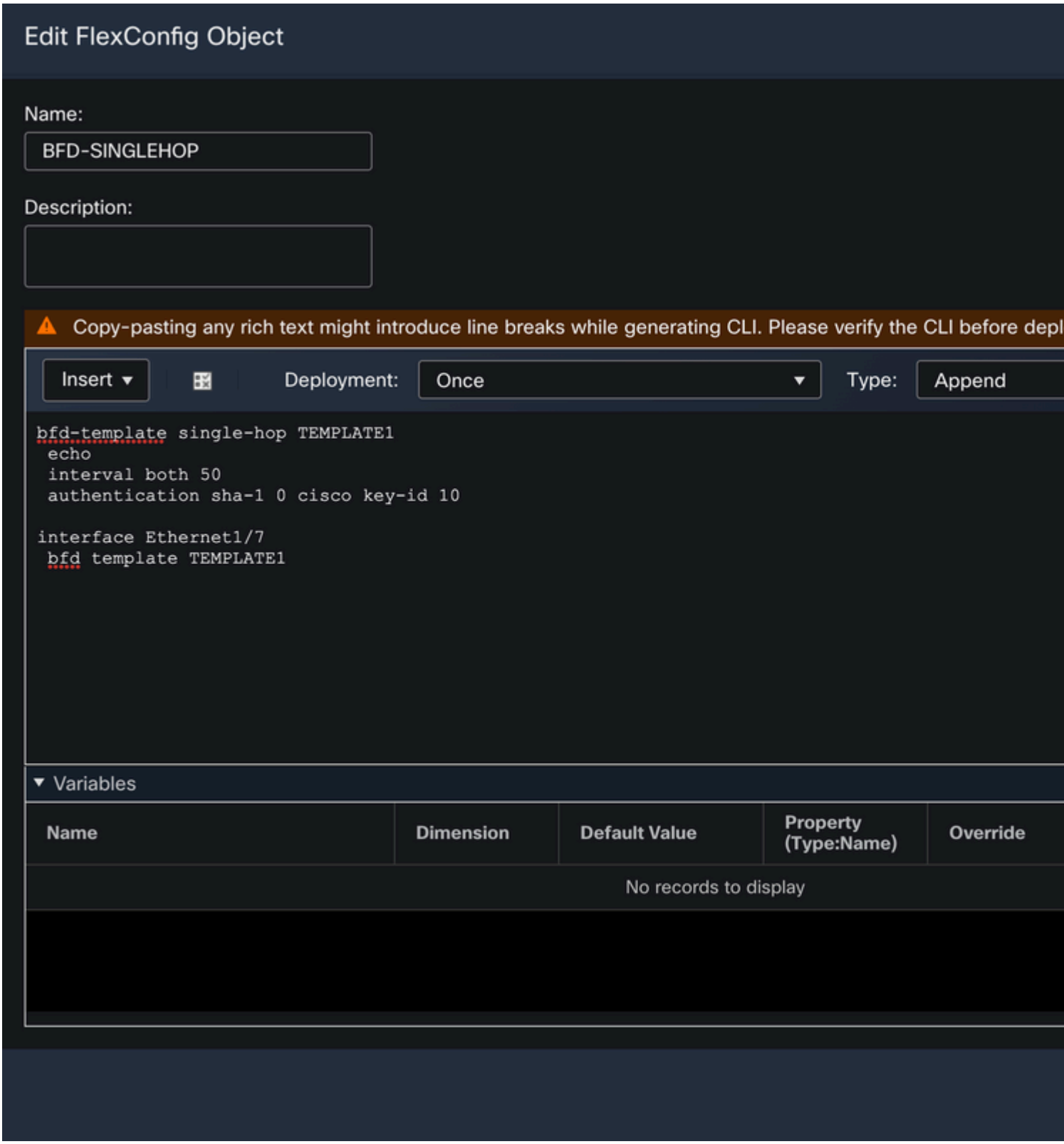
```
authentication {md5 | meticulous-mds | meticulous-sha-1 | sha-1}[0|8] wordkey-id id
```

- authentication â€” Especifica o tipo de autenticação.
- md5â€” Autenticação Message Digest 5 (MD5).
- meticulous-md5 â€” Autenticação MD5 com chave meticulosa.
- meticulous-sha-1â€” Autenticação SHA-1 com chave meticulosa.
- sha-1â€” Autenticação SHA-1 com chave.
- 0|8 â€” 0 especifica que uma senha NÃO CRIPTOGRAFADA será exibida em seguida. 8 especifica que uma senha CRIPTOGRAFADA será exibida em seguida.
- word â€” 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 â€” O ID da chave de autenticação.
- id â€” O ID da chave compartilhada que corresponde à string da chave. O intervalo é de 0 a 255 caracteres.



Etapa 3.

Associe o modelo BFD à interface.



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

Etapa 4 (opcional).

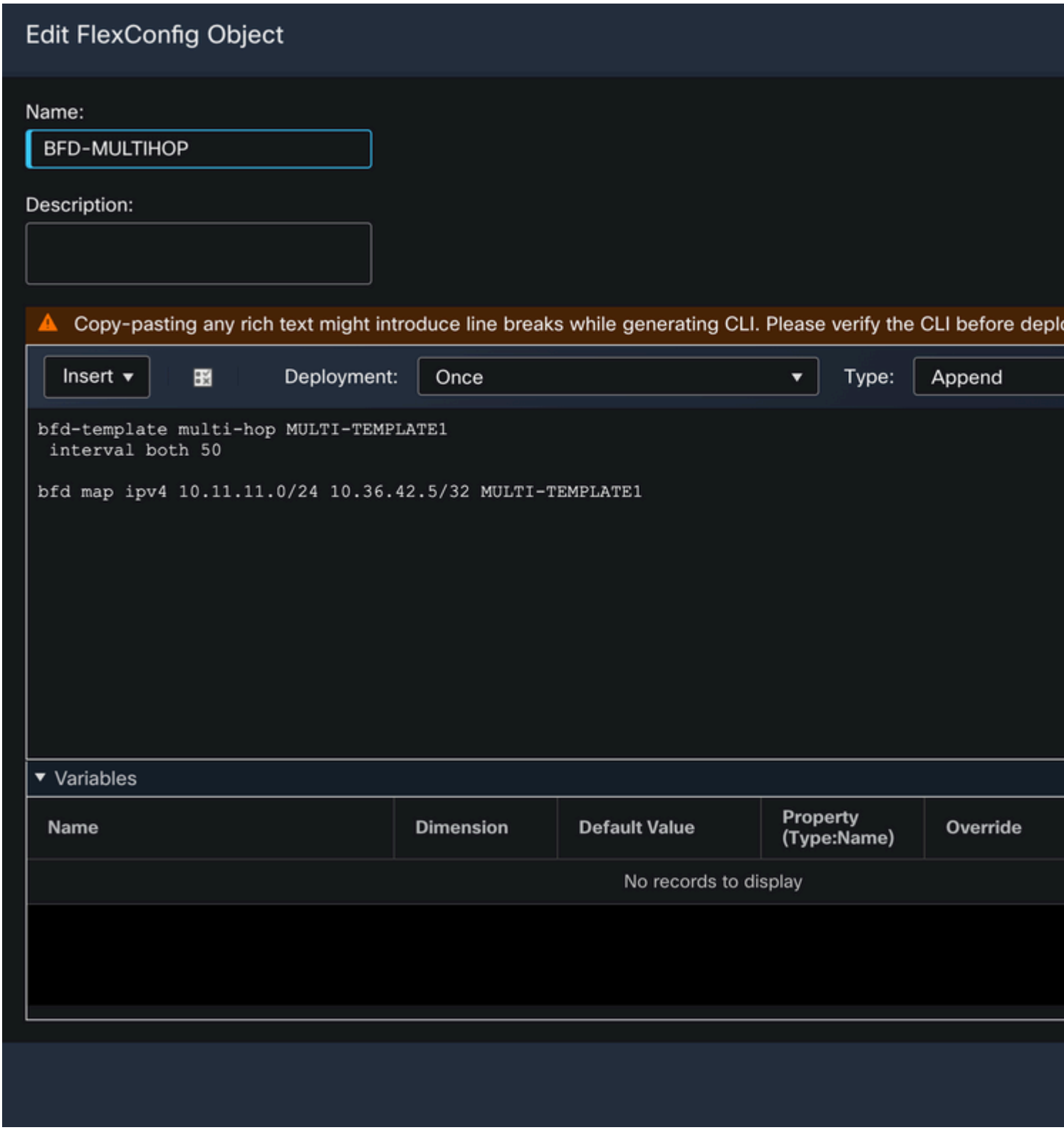
Crie um mapa BFD contendo destinos que você pode associar a um modelo multi-hop. Você deve ter um modelo de BFD de vários saltos já configurado.

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

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

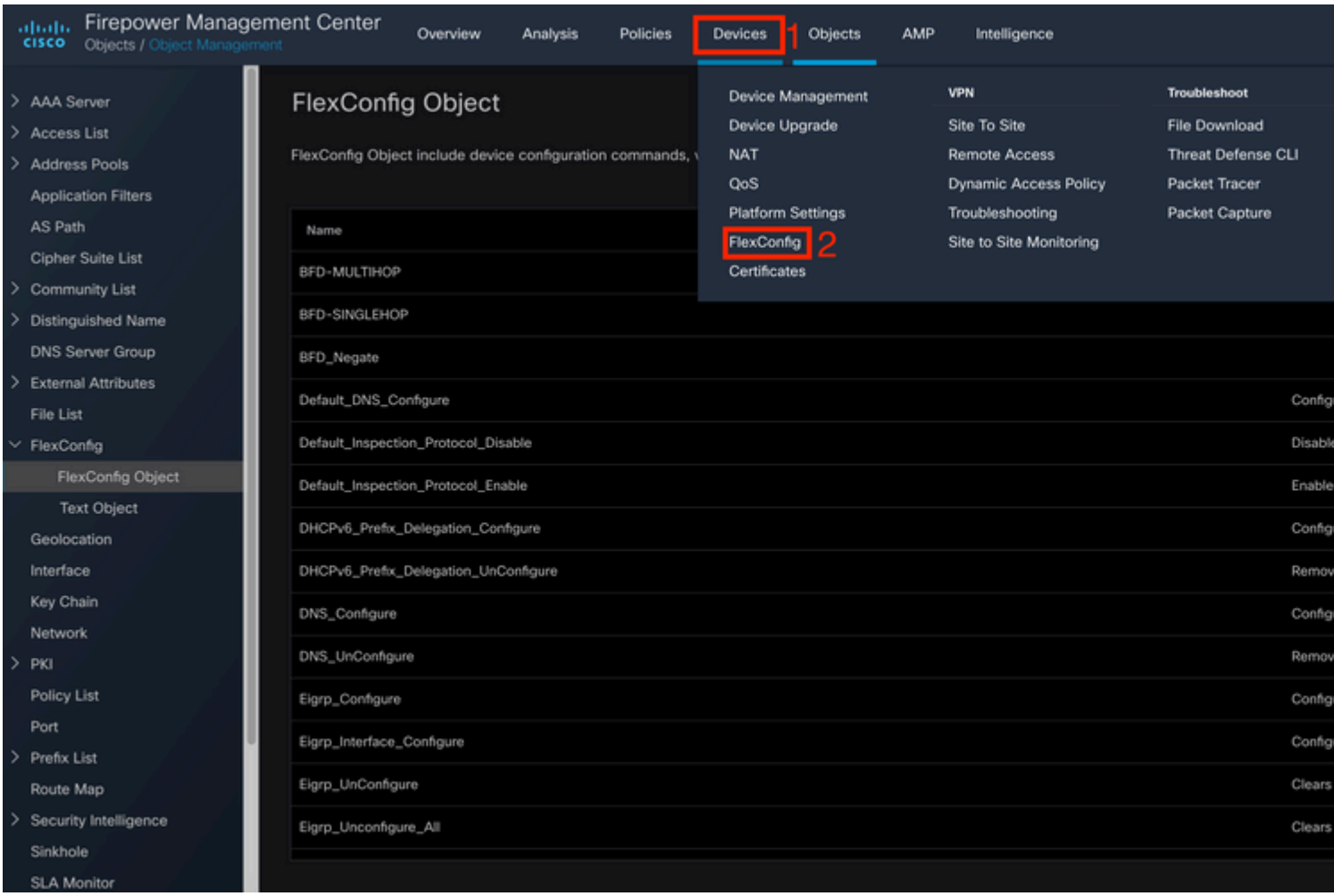
- ipv4 â€” Configura um endereço IPv4.
- ipv6 â€” Configura um endereço IPv6.
- destination/cdir â€” Especifica o prefixo/comprimento de destino. O formato é A.B.C.D/<0-32>.
- source/cdirâ€ — Especifica o prefixo/comprimento de destino. O formato é X:X:X;X::X/<0-128>.
- nome-do-modelo â€” Especifica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

Clique no botão **Save** para salvar o objeto.



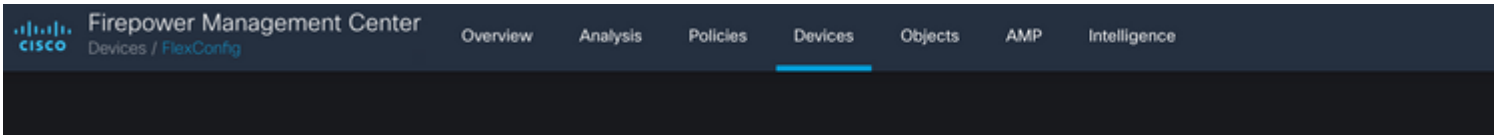
Etapa 5.

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



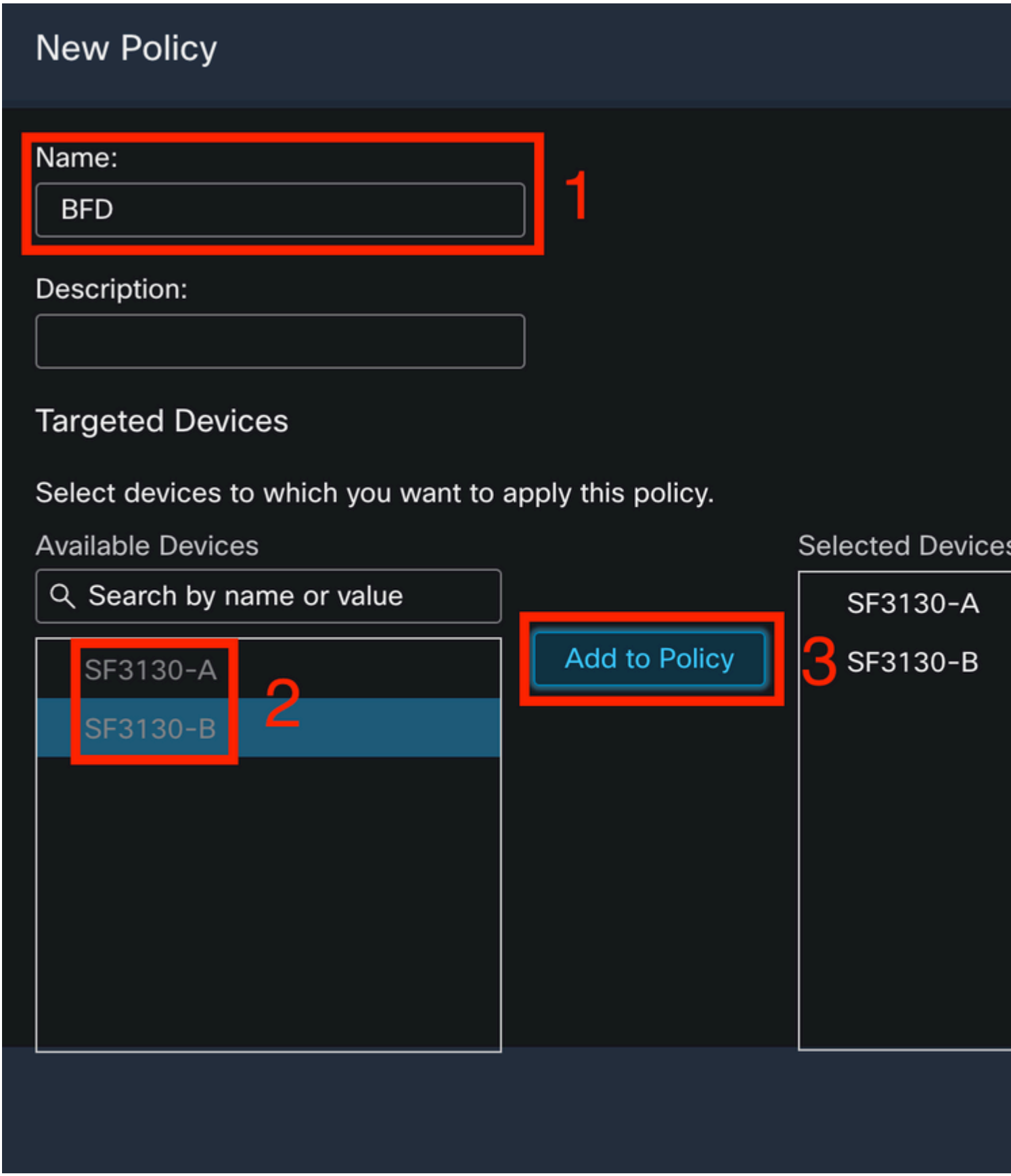
Etapa 6.

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



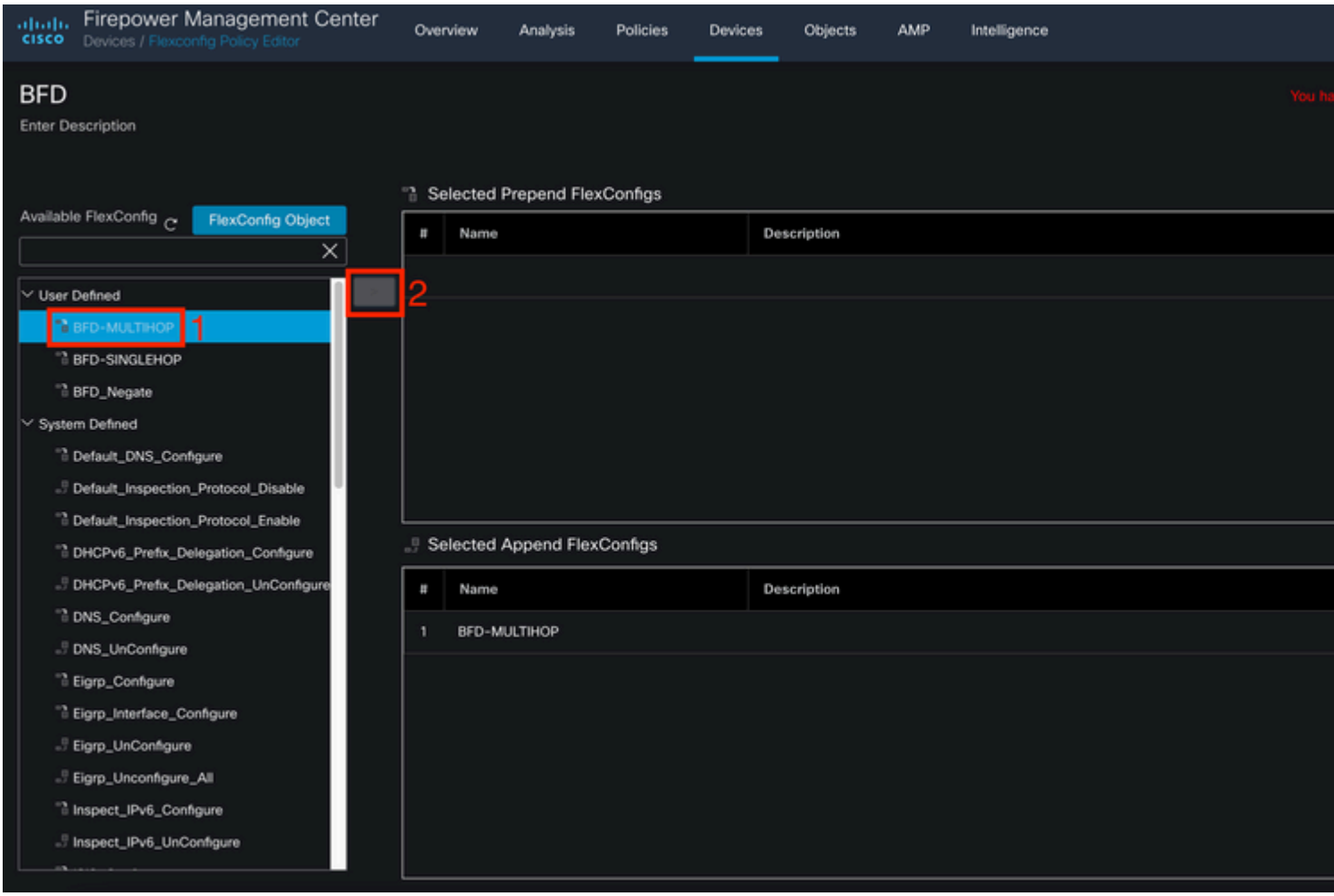
Passo 7.

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



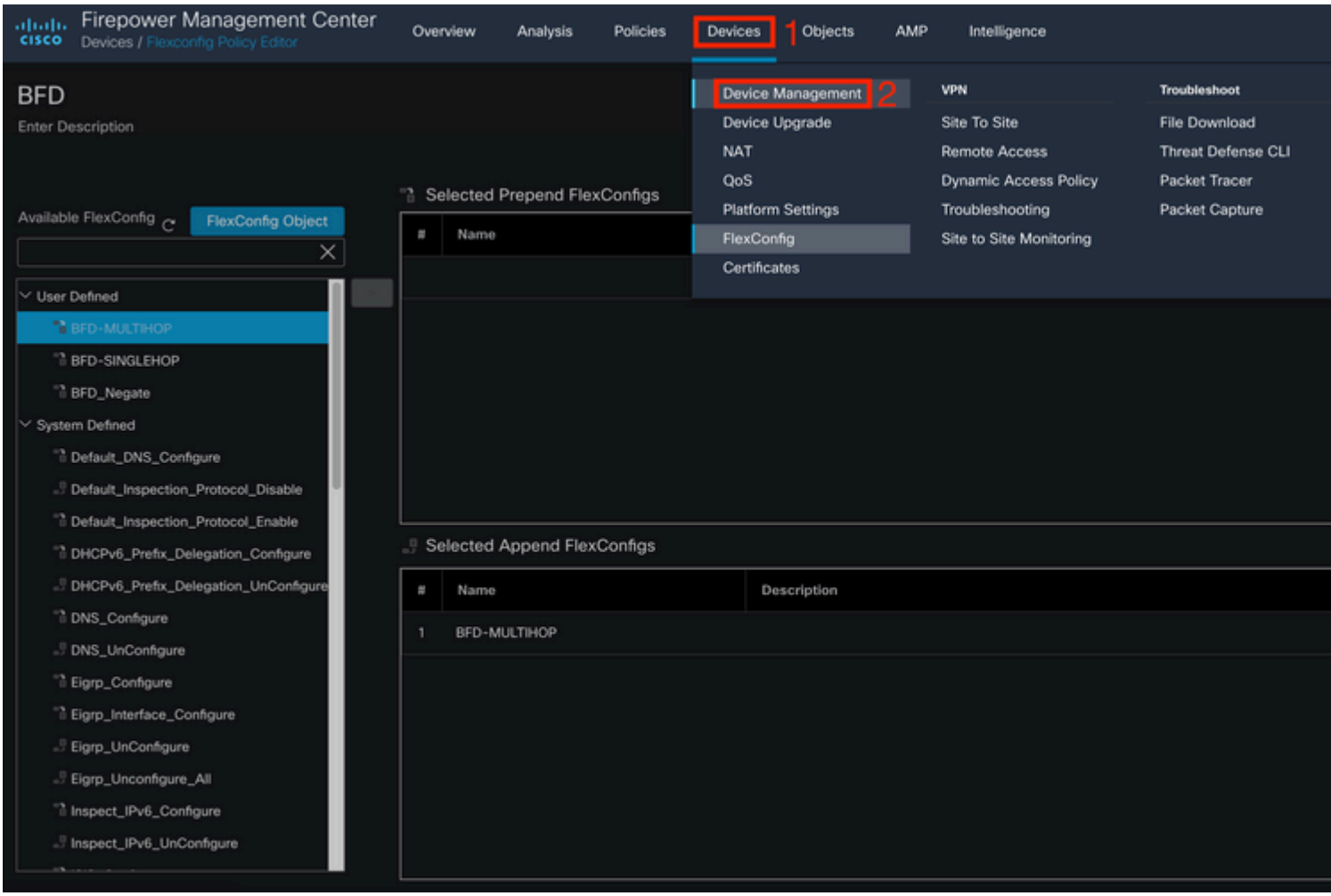
Etapa 8.

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



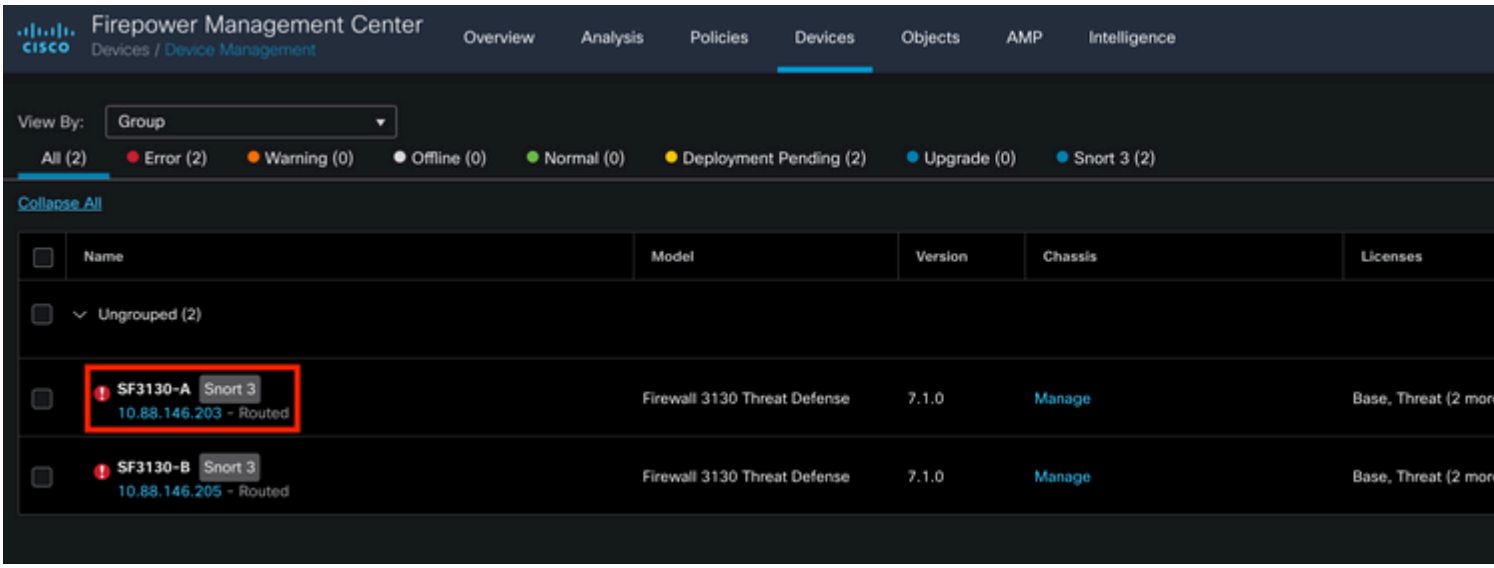
Etapa 9.

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



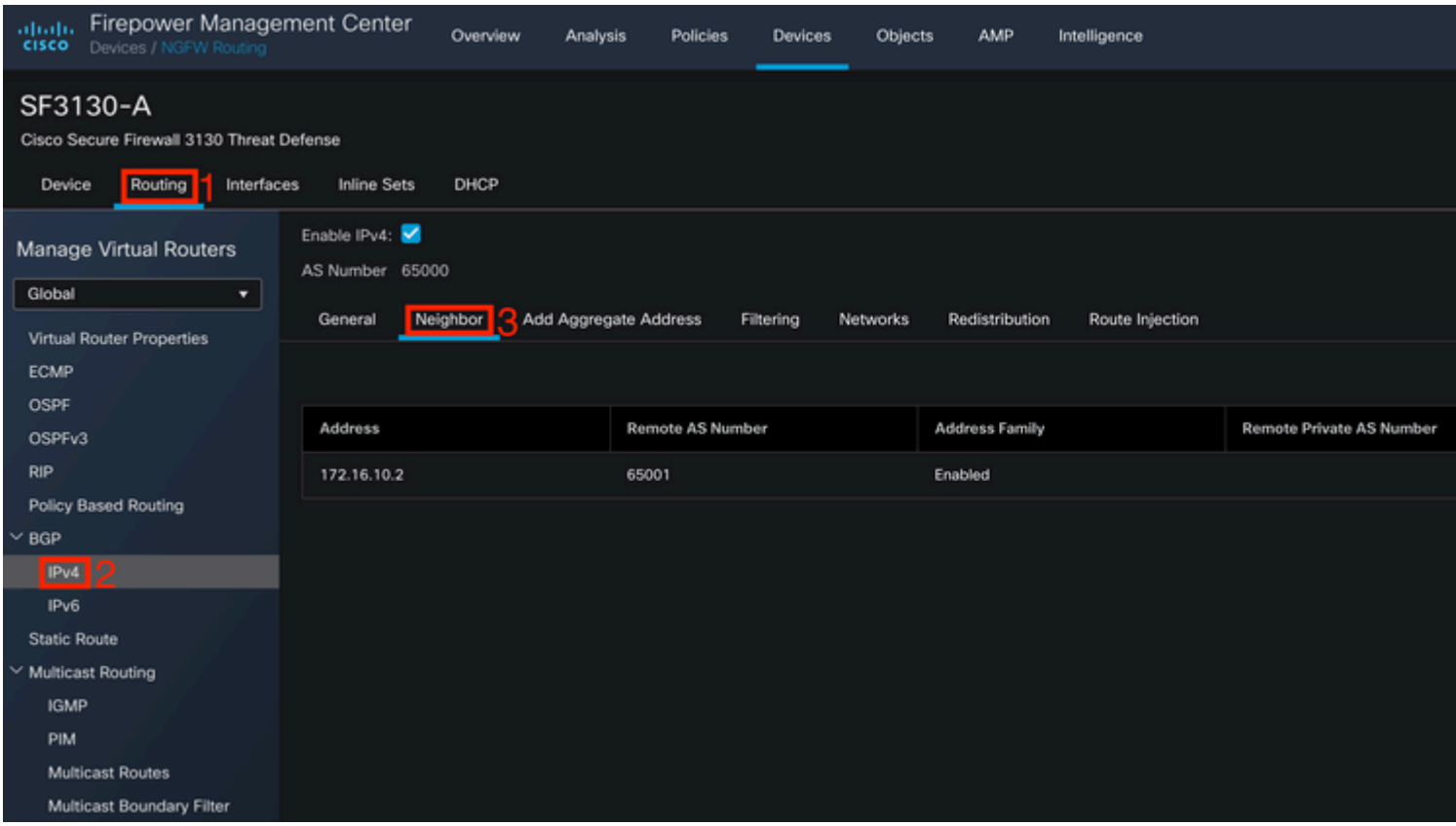
Etapa 10.

Selecione o dispositivo ao qual a configuração BFD será atribuída.



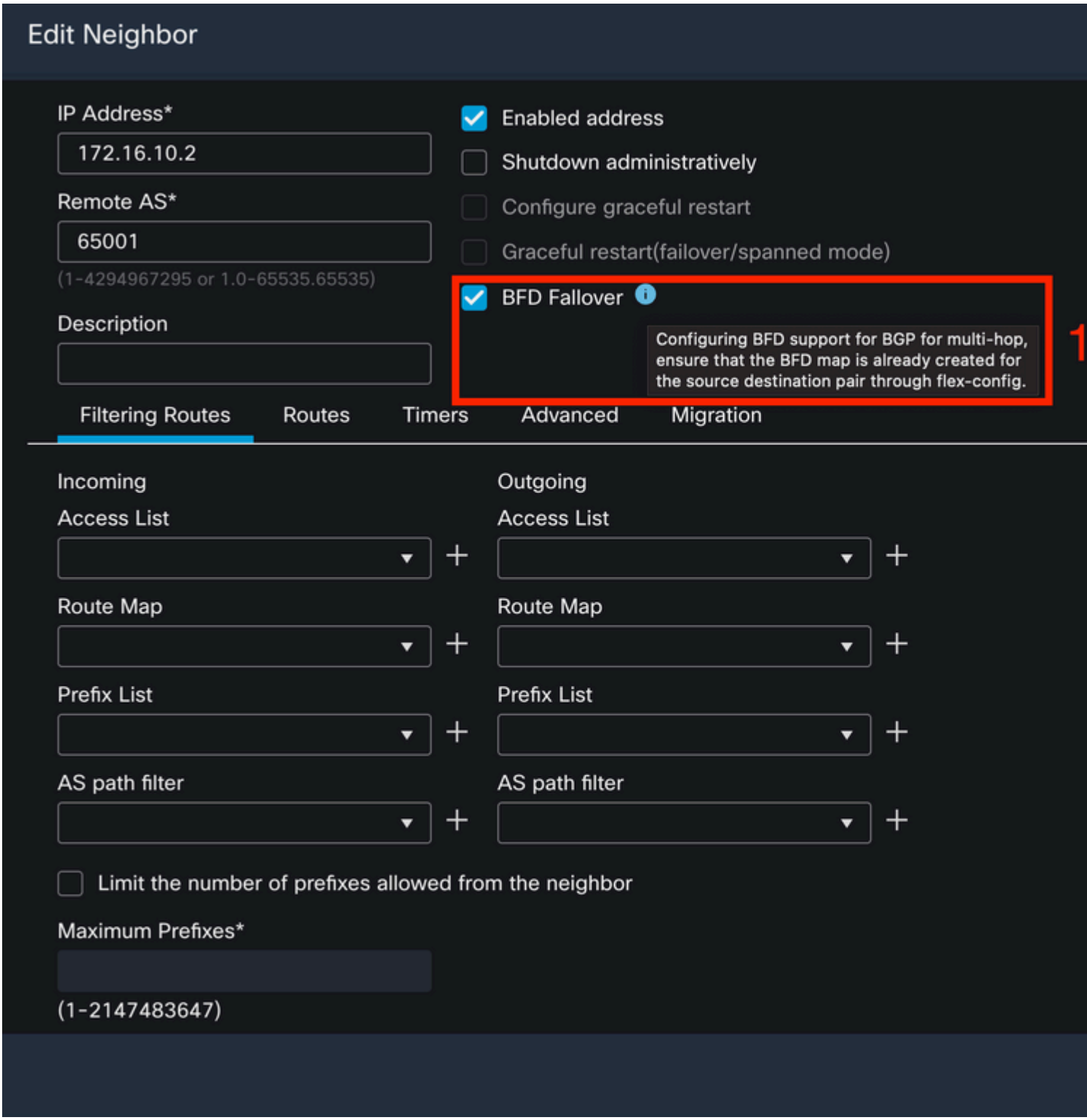
Etapa 11.

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.



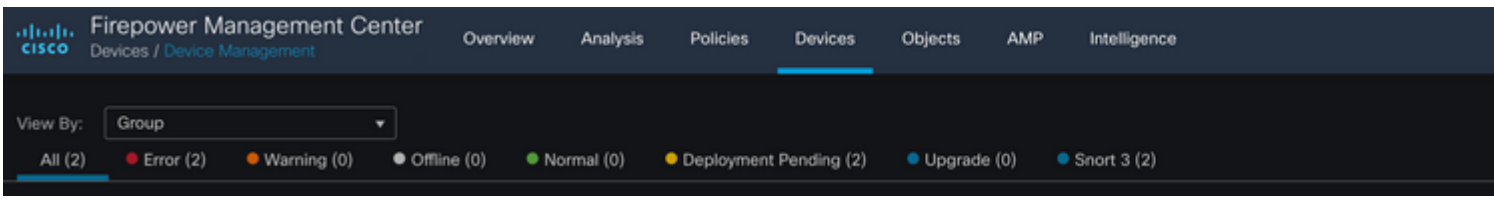
Etapa 12.

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



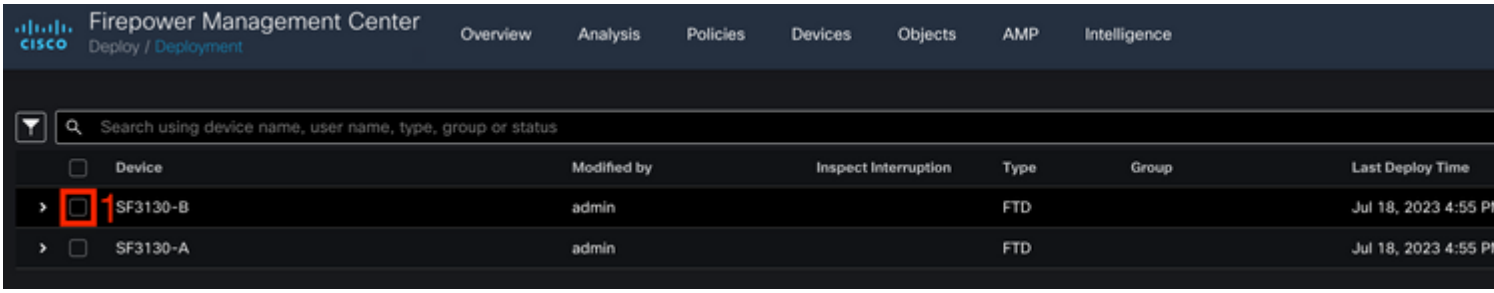
Etapa 13.

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



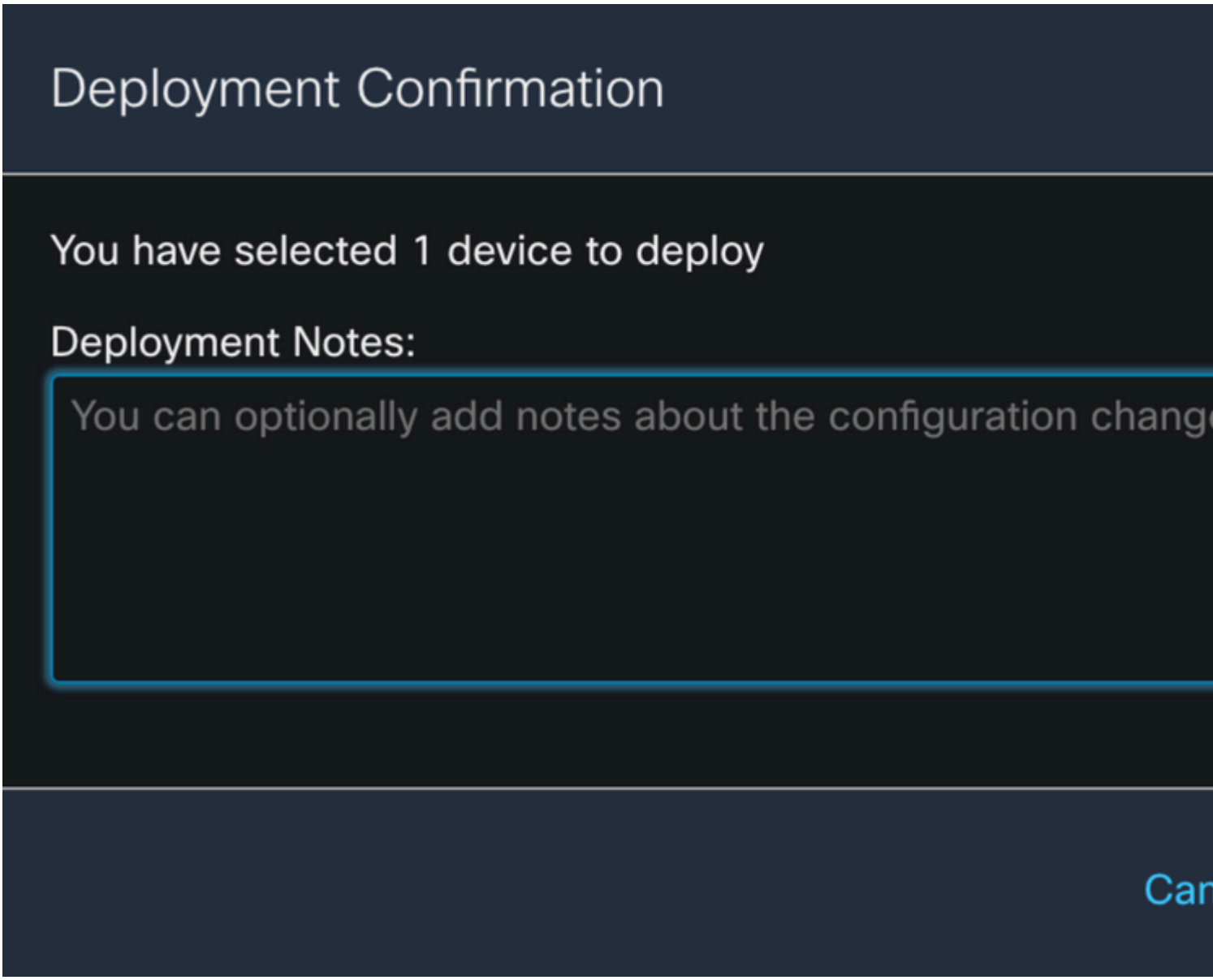
Etapa 14.

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



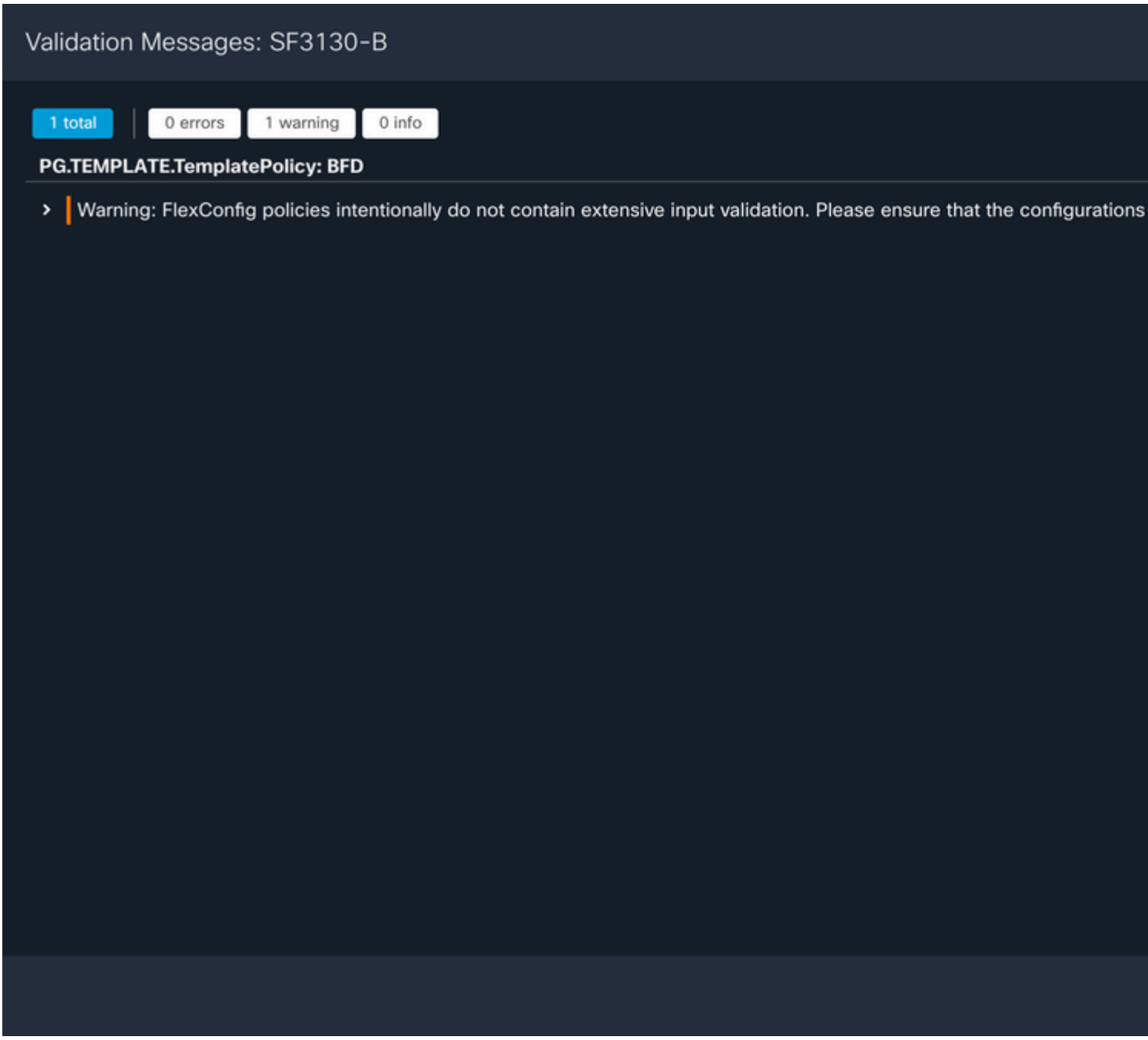
Etapa 15.

Clique no botão **Deploy** botão.



Etapa 16.

Clique no botão **Deploy** botão.



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.