Configuration de BFD dans Secure Firewall Threat Defense avec Flex-Config

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

Vérifier

Dépannage

Introduction

Ce document décrit comment configurer le protocole BFD dans Secure Firewall Management Center exécutant 7.2 et les versions antérieures avec Flex-Config.

Conditions préalables

Protocole BGP (Border Gateway Protocol) configuré dans Cisco Secure Firewall Threat Defense (FTD) avec Cisco Secure Firewall Management Center (FMC).

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

-Protocole BGP
-Concepts BFD

Composants utilisés

-Cisco Secure Firewall Management Center exécutant la version 7.2 ou les versions antérieures.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le protocole BFD (Bidirectional Forwarding Detection) est un protocole de détection conçu pour

fournir des temps de détection de défaillance de chemin de transfert rapide pour tous les types de supports, encapsulations, topologies et protocoles de routage.

Configurer

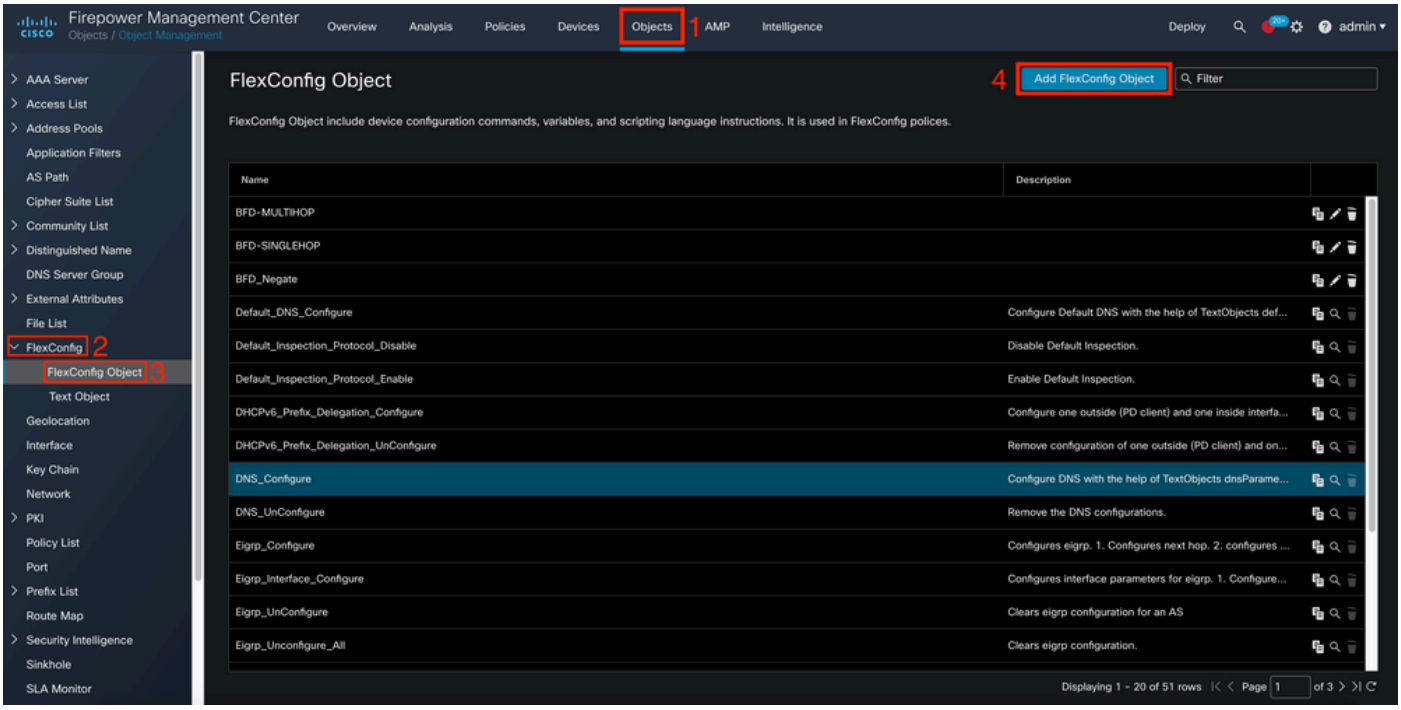
Les configurations BFD dans FMC exécutant les versions 7.2 et antérieures doivent être configurées avec des politiques et des objets Flex-Config.

Étape 1.

Créez le modèle BFD via l'objet Flexconfig.

Le modèle BFD spécifie un ensemble de valeurs d'intervalle BFD. Les valeurs d'intervalle BFD configurées dans le modèle BFD ne sont pas spécifiques à une seule interface. Vous pouvez également configurer l'authentification pour les sessions à saut unique et à saut multiple.

Pour créer l'objet Flex-Config, sélectionnez l' **Objects Tab**option en haut, cliquez sur l' **FlexConfig**option dans la colonne de gauche, puis cliquez sur l' **FlexConfig Object**option, puis cliquez sur **Add FlexConfig Object**.



Étape 2.

Ajoutez les paramètres requis pour le protocole BFD :

Le modèle BFD spécifie un ensemble de valeurs d'intervalle BFD. Les valeurs d'intervalle BFD configurées dans le modèle BFD ne sont pas spécifiques à une seule interface. Vous pouvez également configurer l'authentification pour les sessions à saut unique et à saut multiple.

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

- single-hop - Spécifie un modèle BFD à saut unique.
- multi-hop : spécifie un modèle BFD à sauts multiples.
- template_name — Spécifie le nom du modèle. Le nom du modèle ne peut pas contenir d'espaces.
- (Facultatif) Configurez Echo sur un modèle BFD à saut unique.

Remarque : vous ne pouvez activer le mode Écho que sur un modèle à saut unique.

Configurez les intervalles dans le modèle BFD :

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

- both : intervalle minimal de transmission et de réception.
- Intervalle en millisecondes. La plage est comprise entre 50 et 999.
- microsecondes : spécifie l'intervalle BFD en microsecondes pour la commande andmin-tx.
- microsecondes : la plage est comprise entre 50 000 et 999 000.
- min-tx : capacité d'intervalle de transmission minimum.

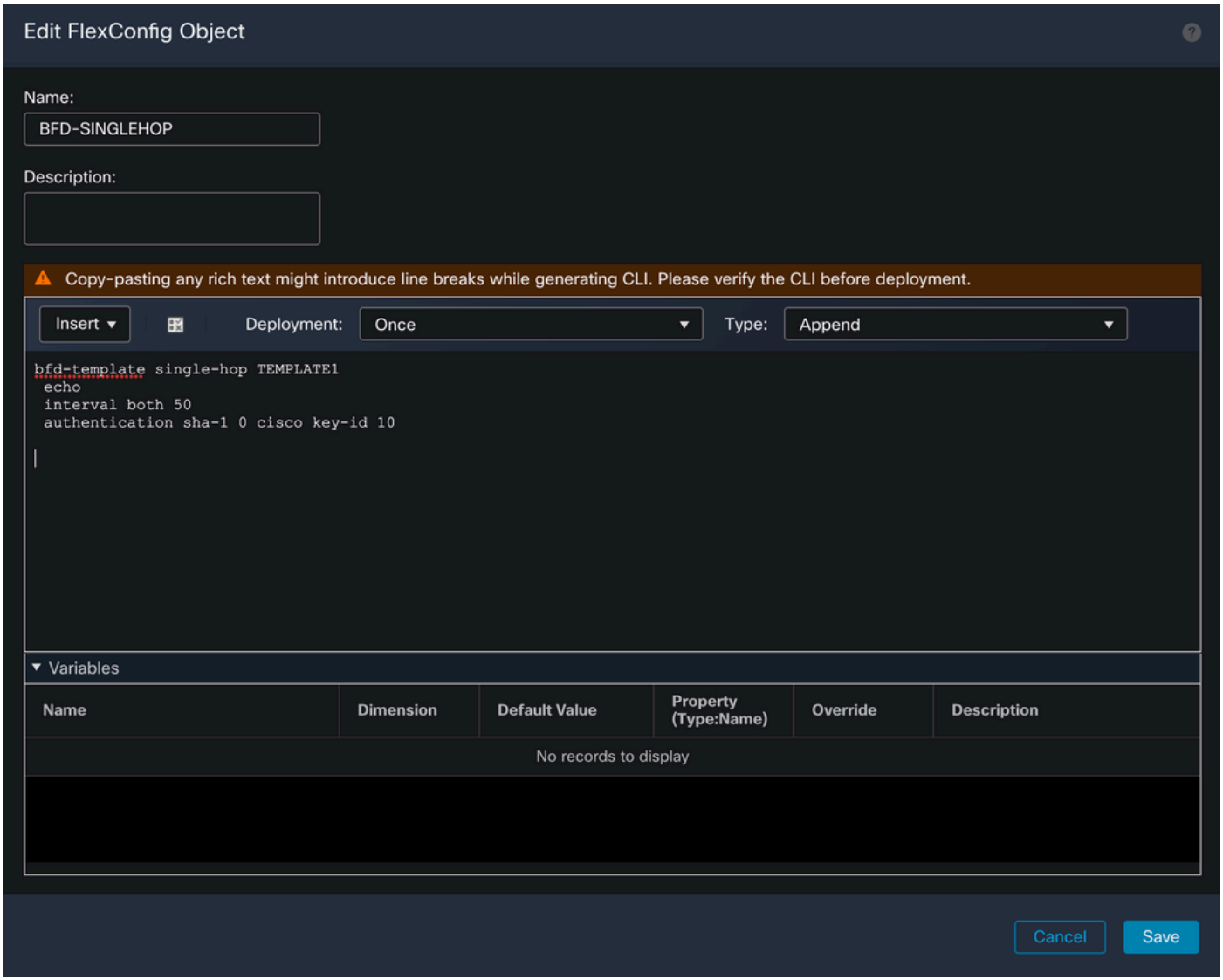
Configurez l'authentification dans le modèle BFD :

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

- authentication : spécifie le type d'authentification.
- md5 : authentification MD5 (Message Digest 5).
- meticulous-md5 — Authentification MD5 à clés méticuleuses.
- meticulous-sha-1 — Authentification SHA-1 à clés méticuleuses.
- sha-1 : authentification SHA-1 par clé.
- 0|8 : 0 indique qu'un mot de passe NON CHIFFRÉ suit. La figure 8 indique qu'un mot de passe ENCRYPTED suit.
- word : mot de passe BFD (clé), qui est un mot de passe/clé à un chiffre comprenant jusqu'à

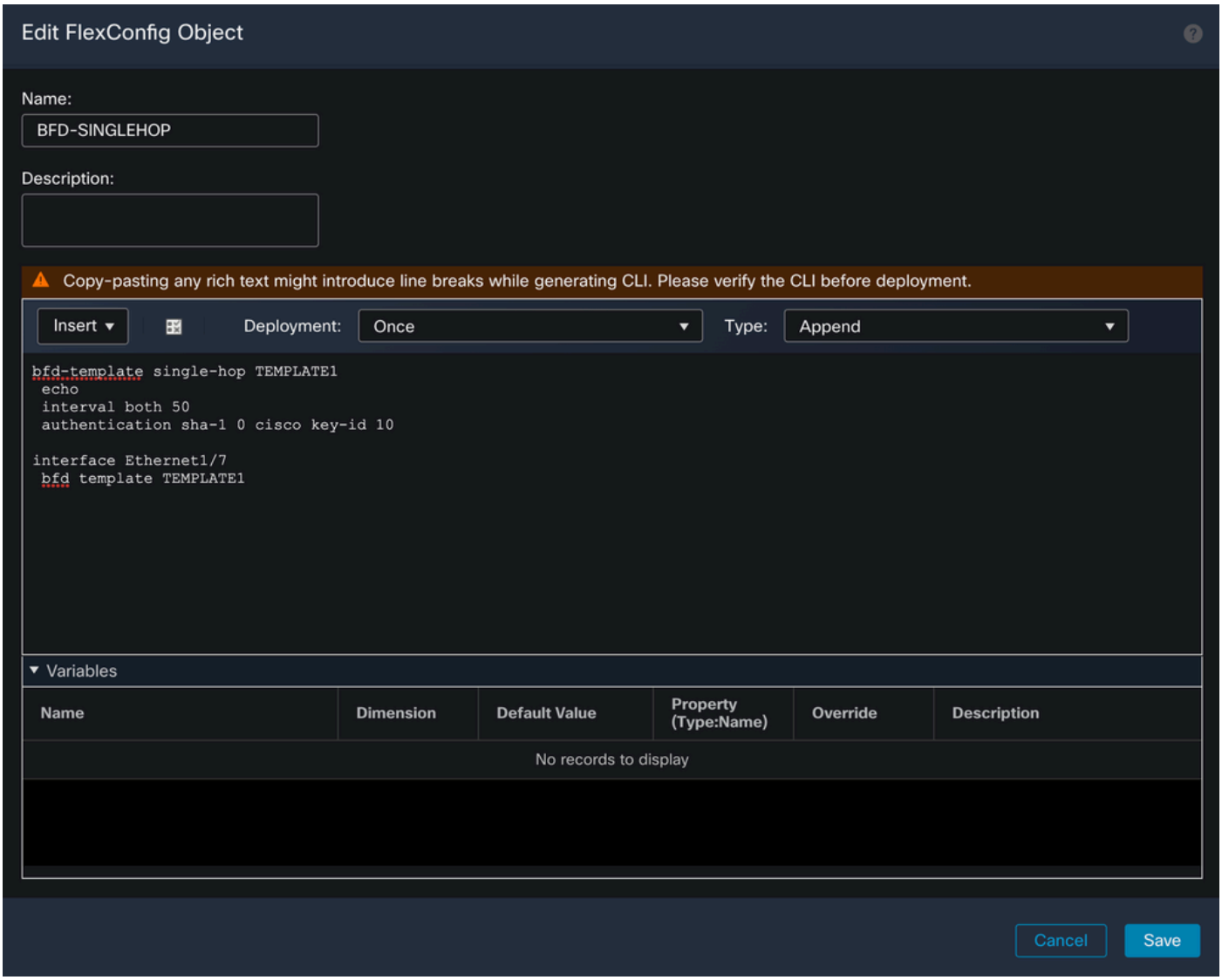
29 caractères. Les mots de passe commençant par un chiffre suivi d'un espace ne sont pas pris en charge. Par exemple, 0 passe et 1 ne sont pas valides.

- key-id : ID de la clé d'authentification.
- id : ID de clé partagée correspondant à la chaîne de clé. La plage est comprise entre 0 et 255 caractères.



Étape 3.

Associez le modèle BFD à l'interface.



Remarque : associez le modèle BFD à sauts multiples à une carte de destinations.

Étape 4 (facultatif).

Créez un mappage BFD contenant des destinations que vous pouvez associer à un modèle à sauts multiples. Vous devez avoir déjà configuré un modèle BFD à sauts multiples.

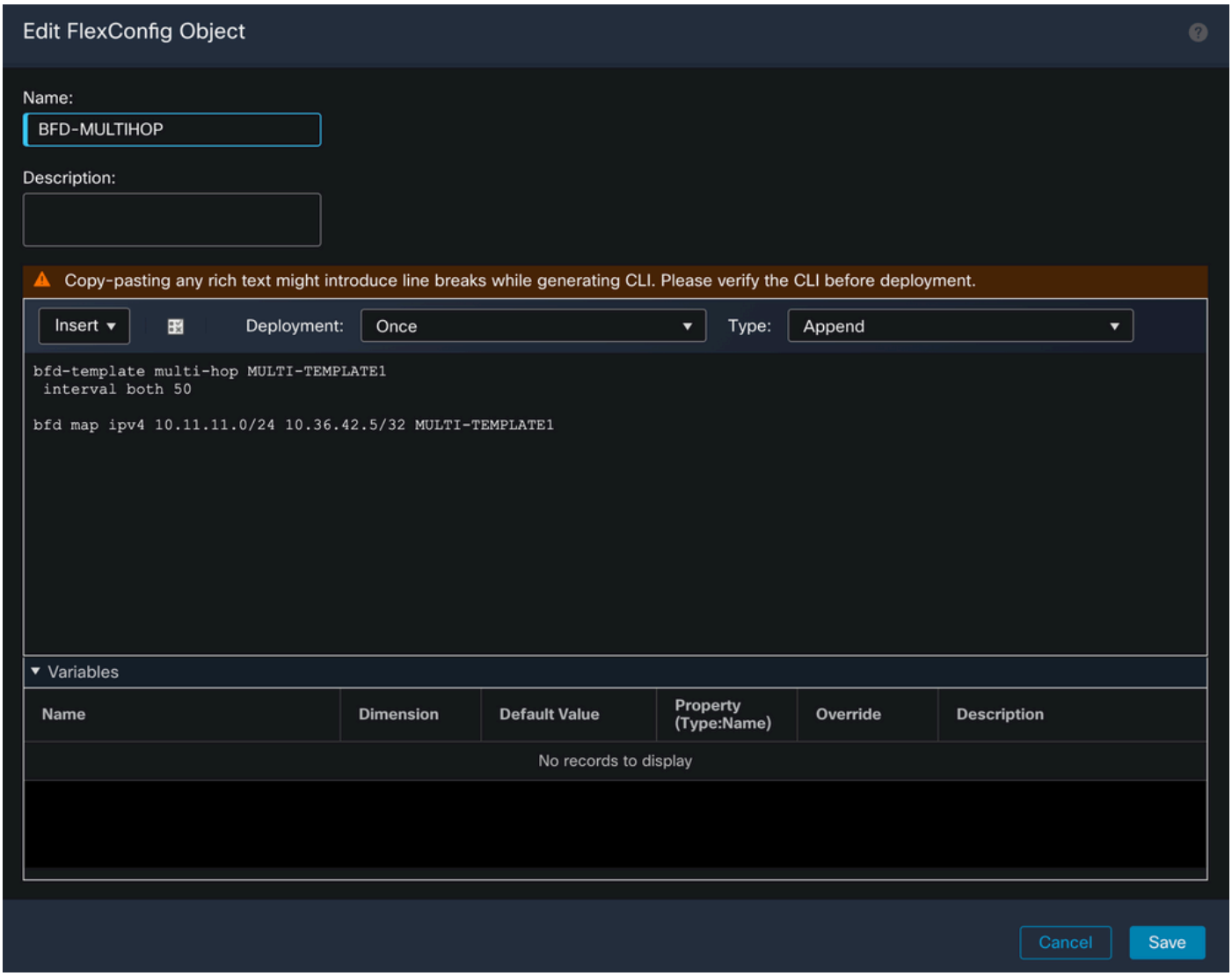
Associez le modèle à sauts multiples BFD à une carte des destinations :

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

- ipv4 : configure une adresse IPv4.
- ipv6 : configure une adresse IPv6.
- destination/cdir — Spécifie le préfixe/la longueur de destination. Le format est A.B.C.D/<0-32>.

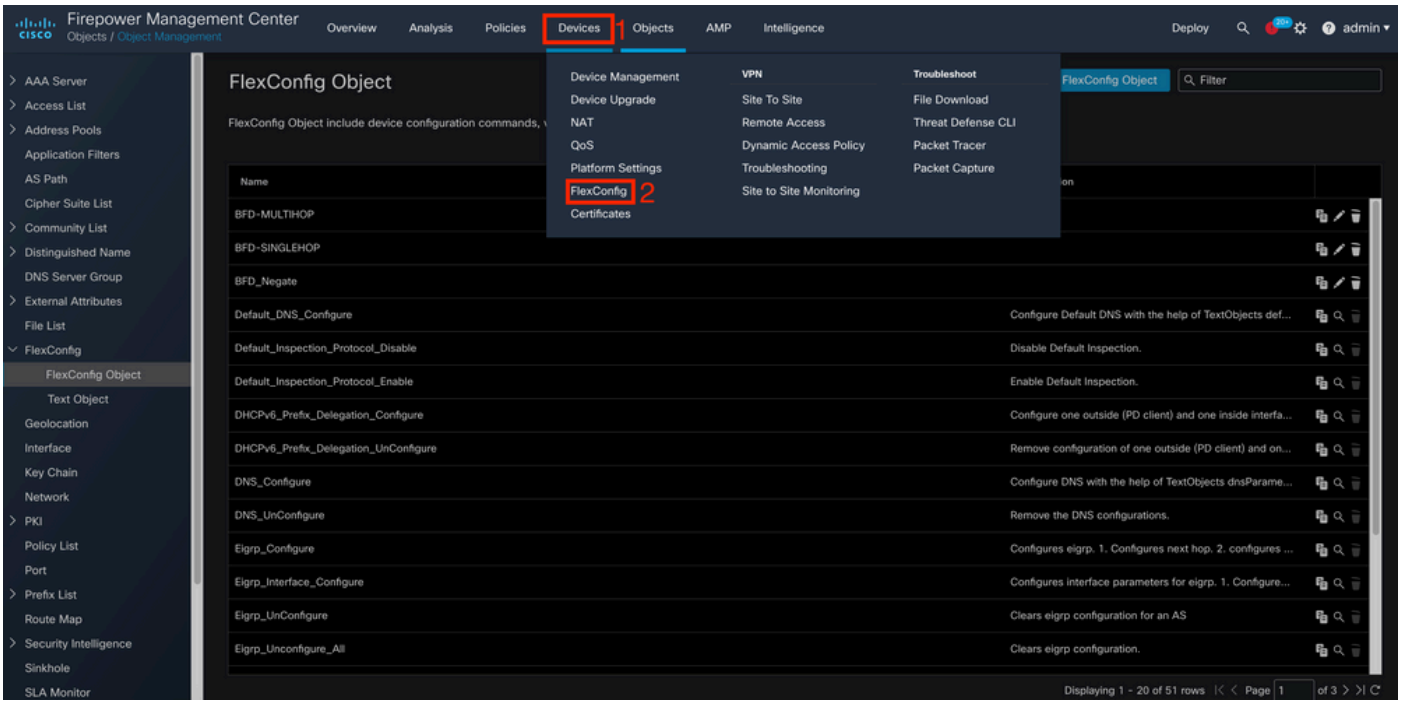
- source/cdir : spécifie le préfixe/la longueur de destination. Le format est X:X:X;X::X/<0-128>.
- template-name — Spécifie le nom du modèle à sauts multiples associé à ce mappage BFD.

Cliquez sur le **Save** bouton pour enregistrer l'objet.



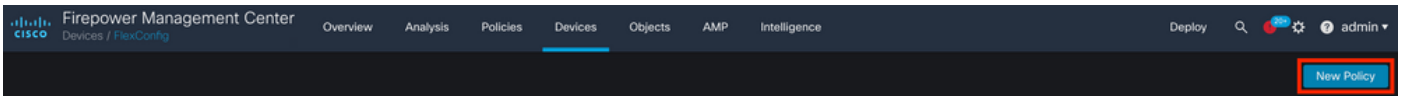
Étape 5.

Cliquez sur l' **Devices**onglet en haut et sélectionnez l' **FlexConfig**option.



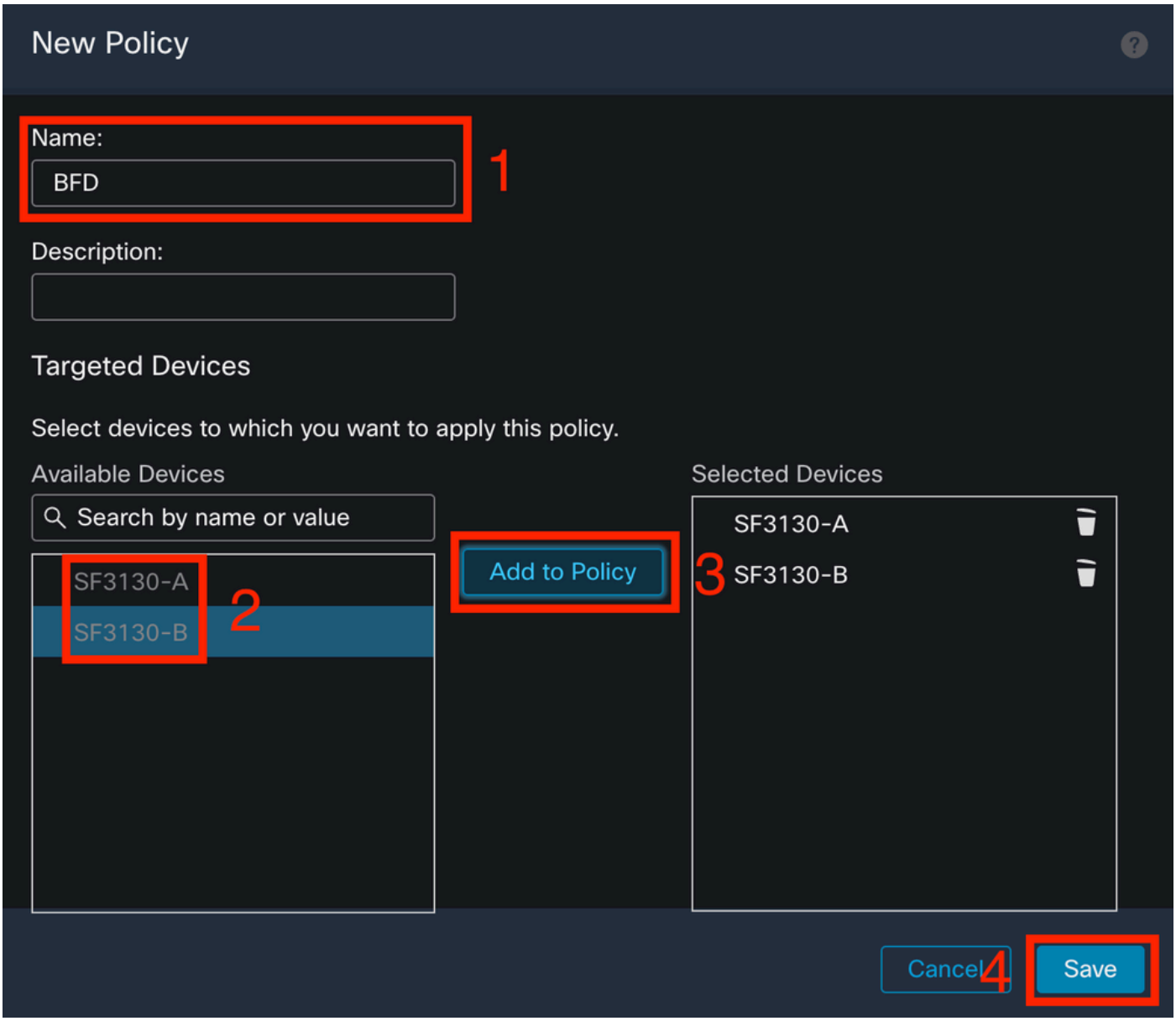
Étape 6.

Pour créer une nouvelle stratégie FlexConfig, cliquez sur le **New Policy** bouton.



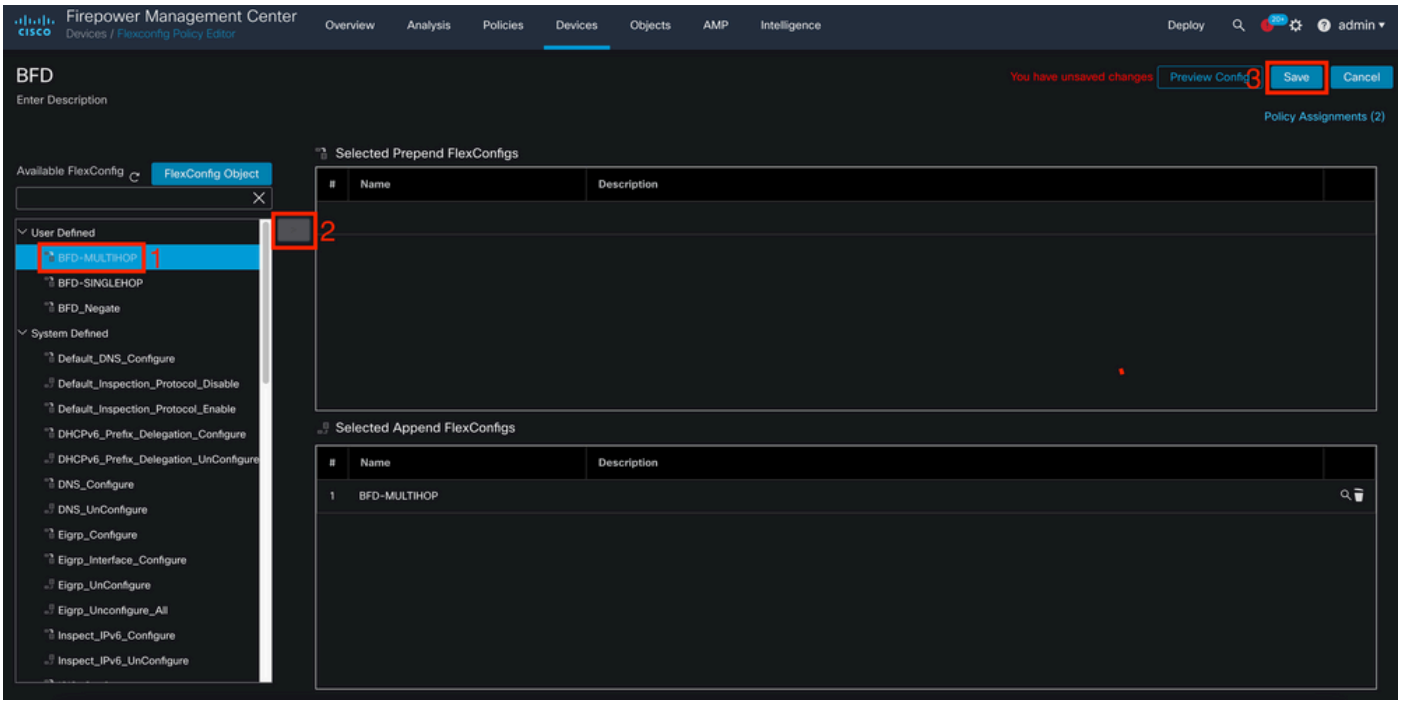
Étape 7.

Name la stratégie et sélectionnez les périphériques affectés à la stratégie. Cliquez sur le **Add to Policy** , puis sur le **Save**bouton.



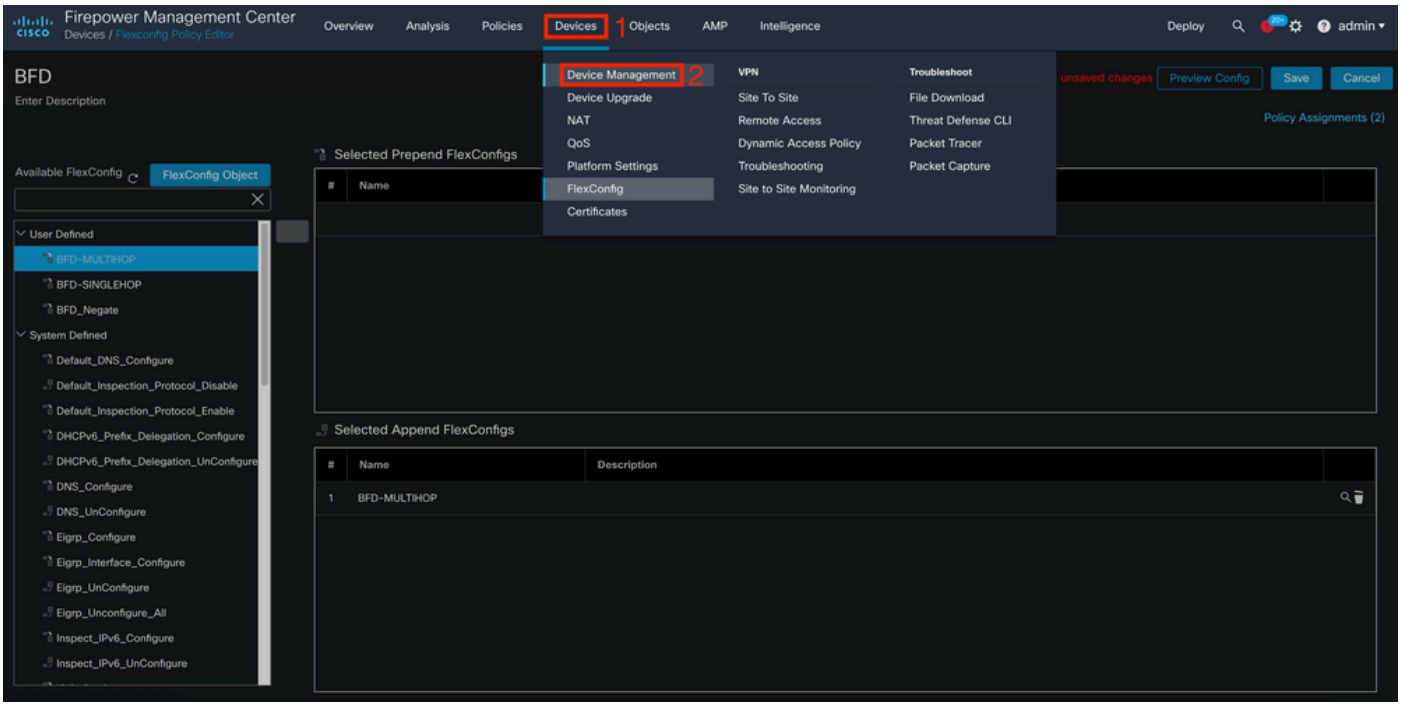
Étape 8.

Sélectionnez l'objet FlexConfig dans la colonne de gauche, cliquez sur le > bouton pour ajouter l'objet à la stratégie FlexConfig, puis cliquez sur le **Save** bouton.



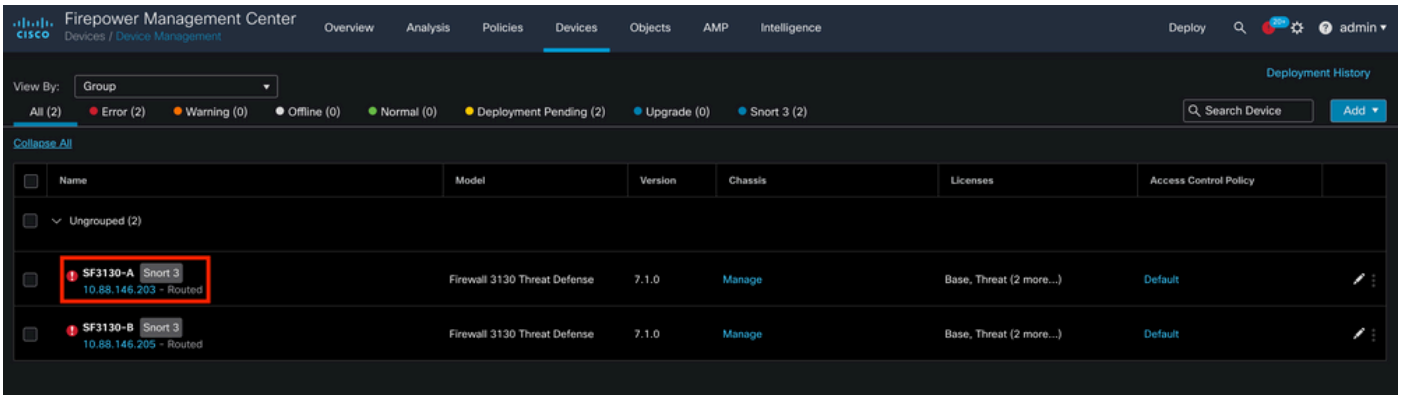
Étape 9.

Cliquez sur l' **Devices**onglet en haut et cliquez sur l' **Device Management**option.



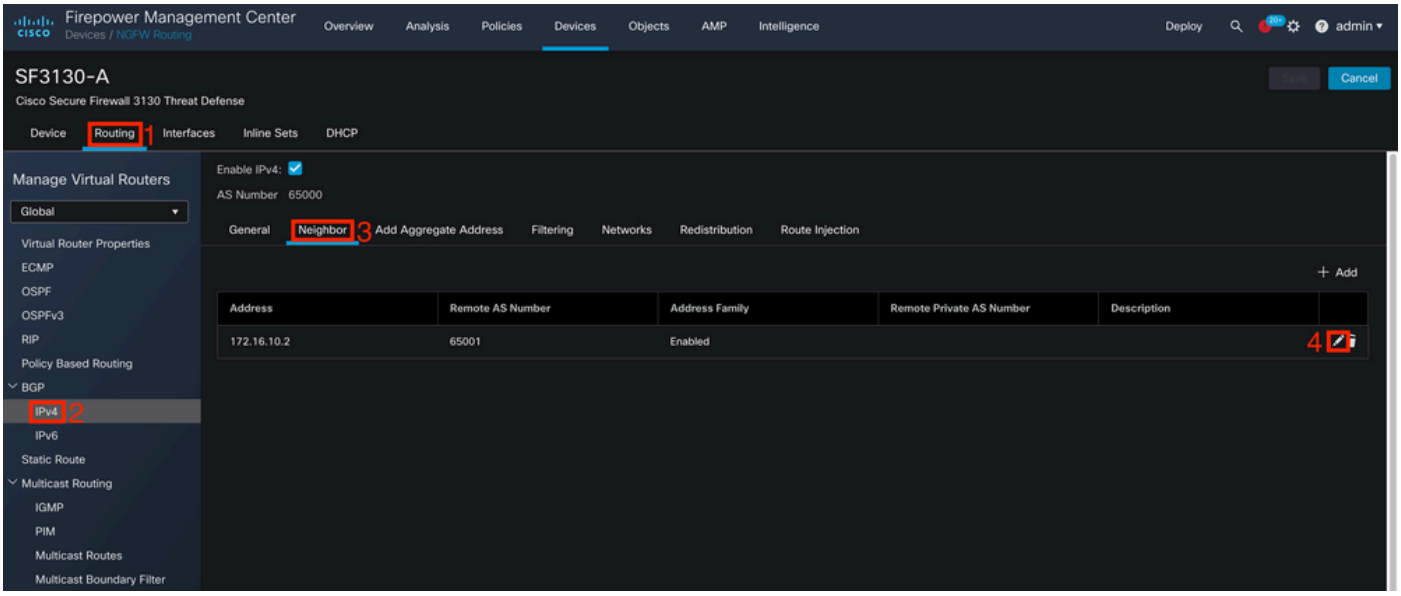
Étape 10.

Sélectionnez le périphérique auquel la configuration BFD sera attribuée.



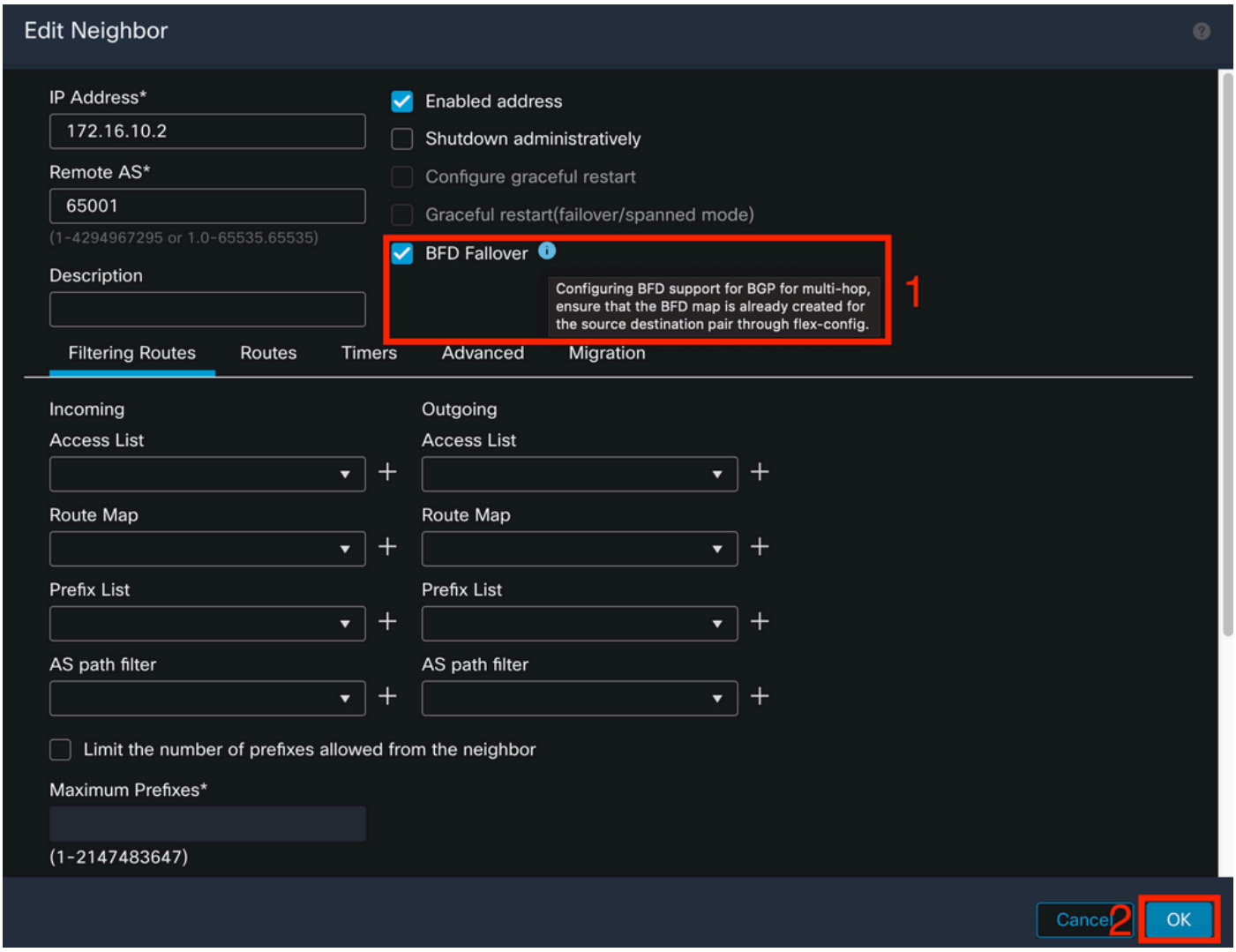
Étape 11.

Cliquez sur l' Routing onglet, puis sur les**IPv4** ou, **IPv6,** selon votre configuration dans la section BGP sur la colonne de gauche, puis cliquez sur l'**Neighbor**onglet, et cliquez sur le bouton de crayon de modification pour le modifier.



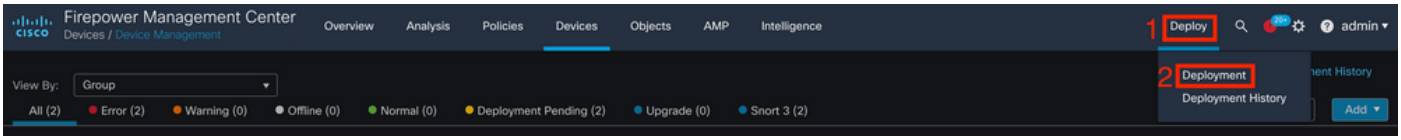
Étape 12.

Sélectionnez la **checkbox** pour le basculement BFD et cliquez sur le **OK** bouton.



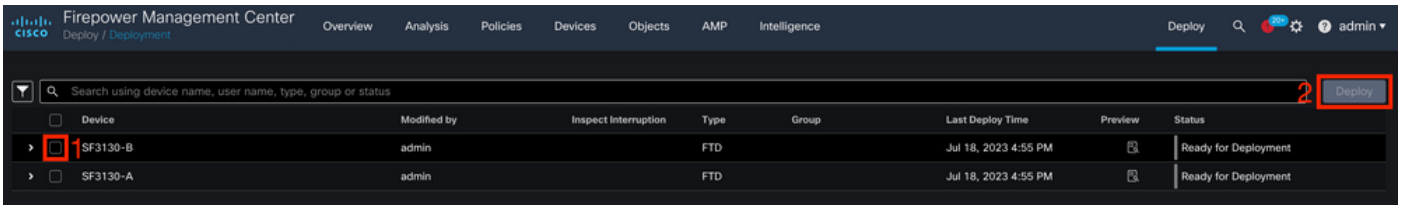
Étape 13.

Cliquez sur le **Deploy** bouton, puis sur le **Deployment** bouton.



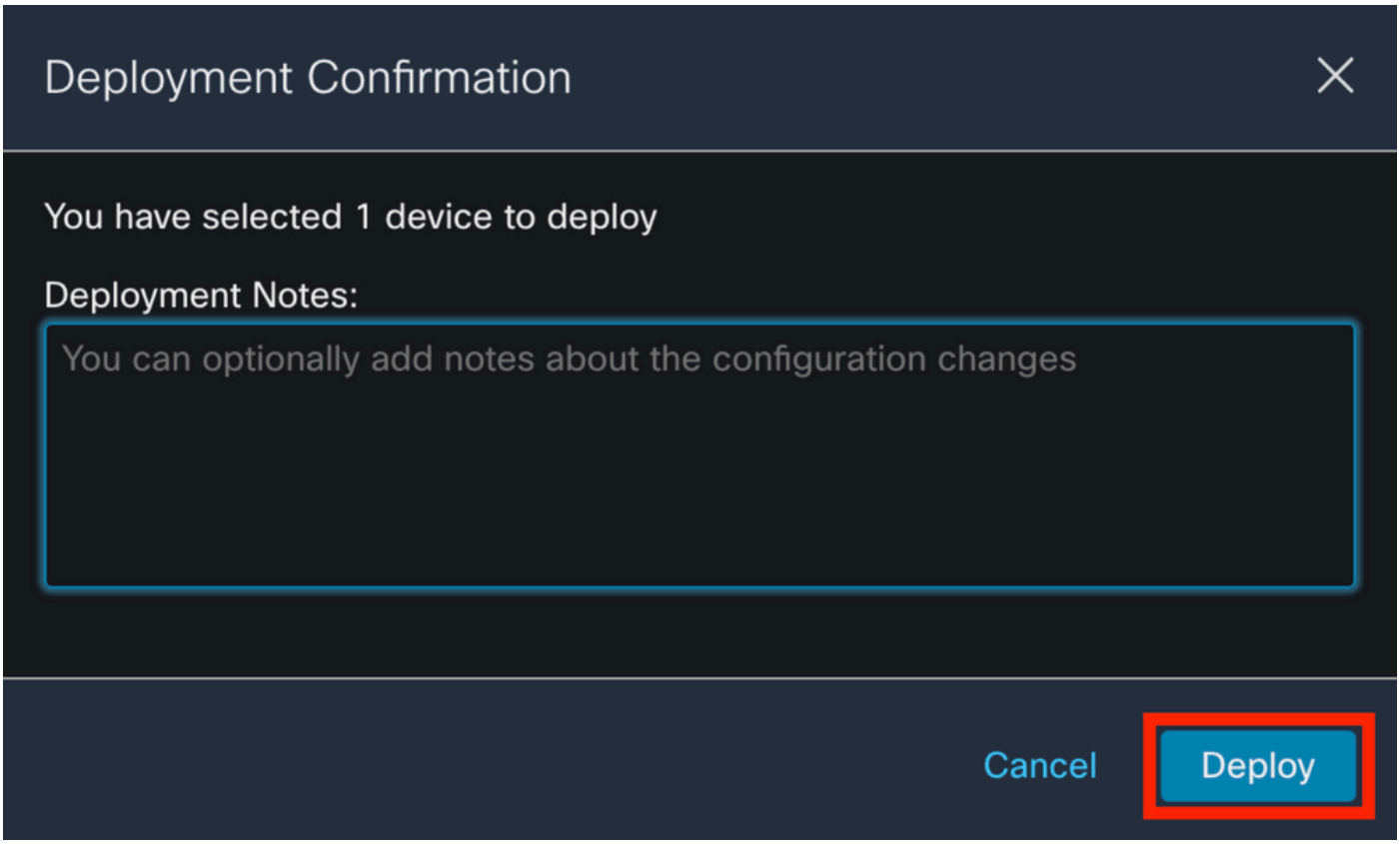
Étape 14.

Sélectionnez le périphérique auquel les modifications vont être attribuées en cliquant sur le bouton **checkbox**, puis sur**Deploy** le bouton.



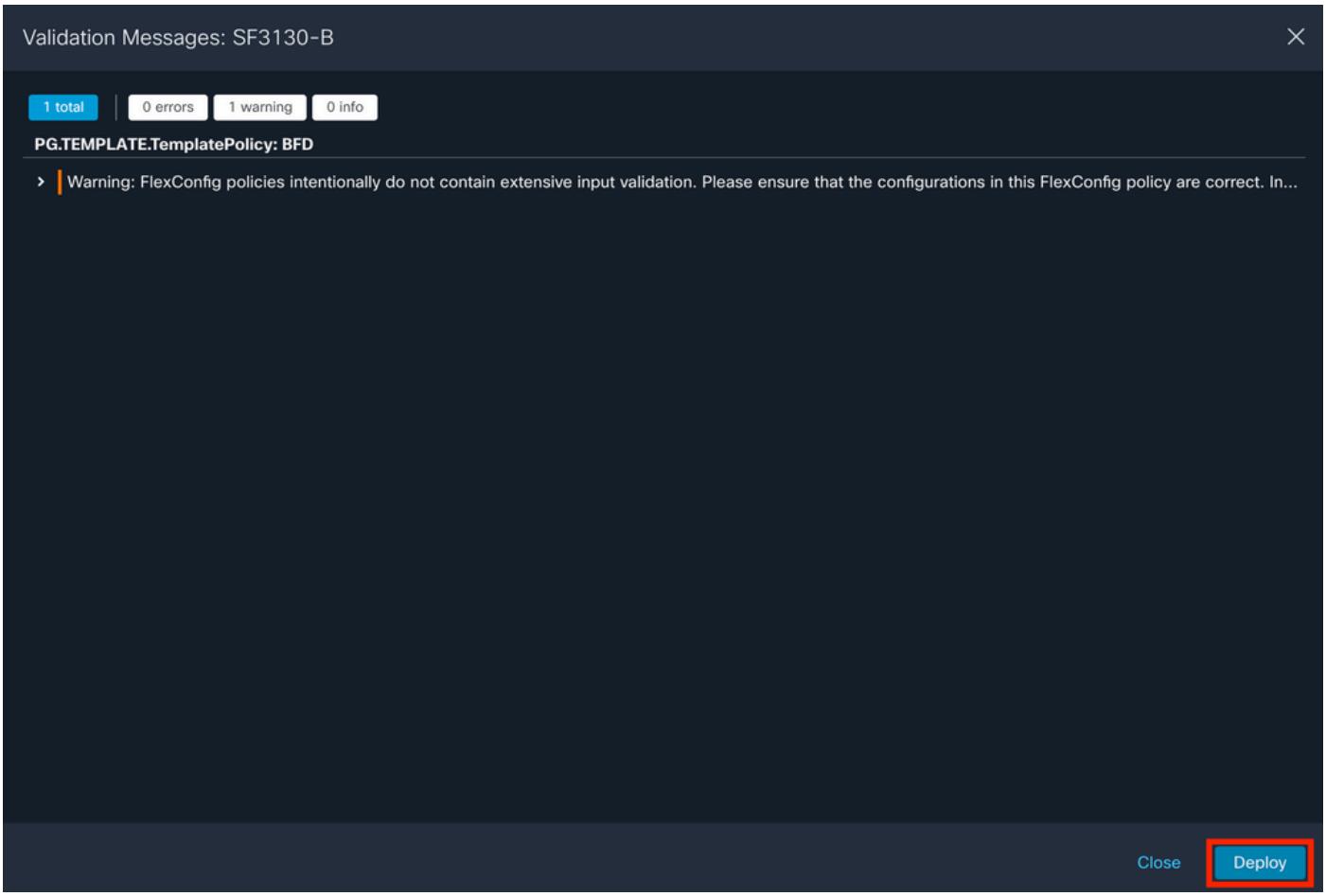
Étape 15.

Cliquez sur le **Deploy** bouton.



Étape 16.

Cliquez sur le **Deploy** bouton.



Remarque : L'avertissement est attendu et n'a qu'un caractère informatif.

Vérifier

Vérifiez la configuration BFD et l'état directement sur la session CLI à l'aide des commandes suivantes.

```
<#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
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.