Configurazione di BFD in Secure Firewall Threat Defense con Flex-Config

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Configurazione](#)
[Verifica](#)
[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive come configurare il protocollo BFD in Secure Firewall Management Center con versione 7.2 e precedenti con Flex-Config.

Prerequisiti

Border Gateway Protocol (BGP) configurato in Cisco Secure Firewall Threat Defense (FTD) con Cisco Secure Firewall Management Center (FMC).

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

-protocollo BGP
-Concetti di BFD

Componenti usati

-Cisco Secure Firewall Management Center con versione 7.2 o precedenti.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

BFD (Bidirectional Forwarding Detection) è un protocollo di rilevamento progettato per fornire tempi di rilevamento rapido degli errori dei percorsi di inoltro per tutti i tipi di supporti, incapsulamenti, topologie e protocolli di routing.

Configurazione

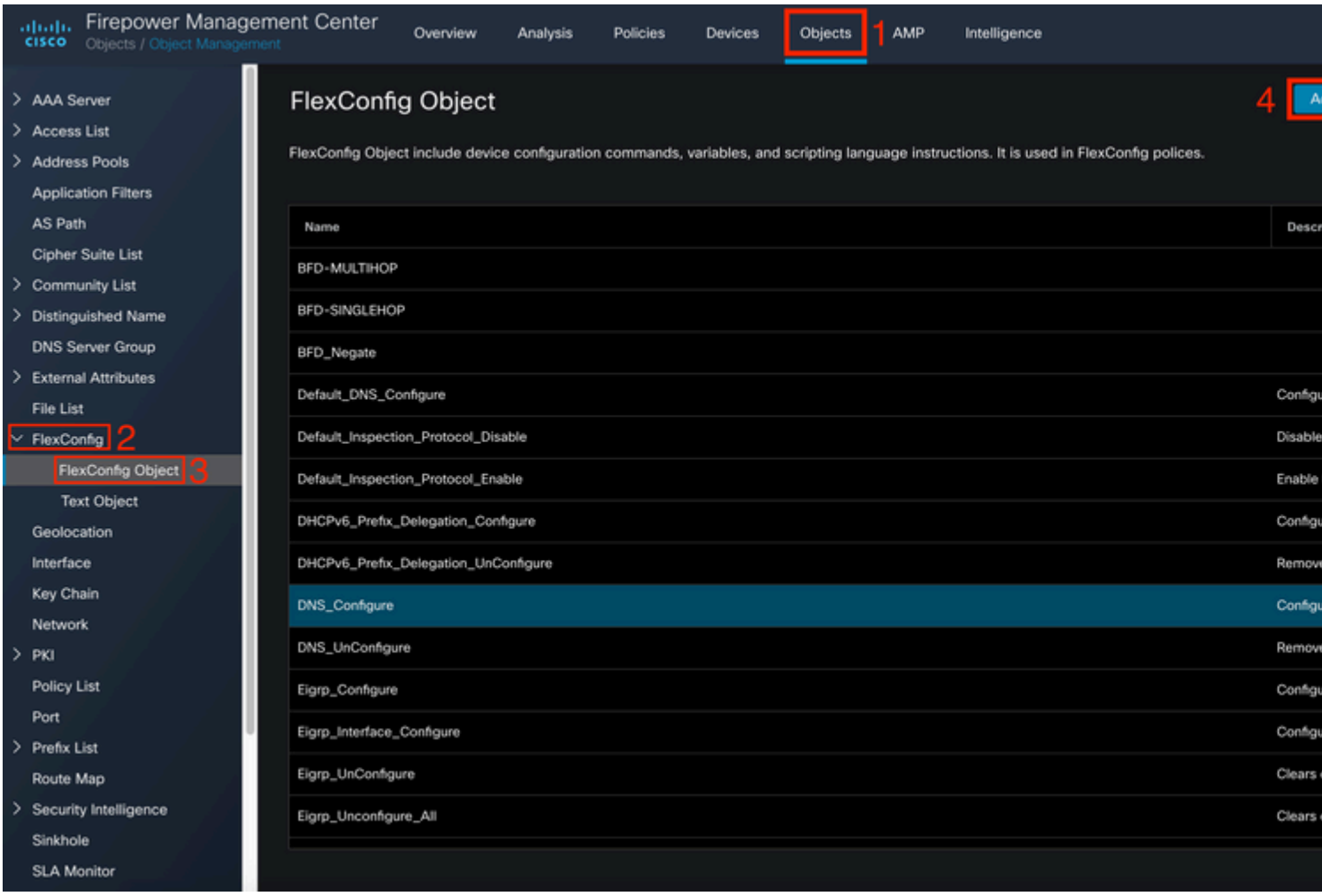
Le configurazioni BFD in FMC che eseguono le versioni 7.2 e precedenti devono essere configurate con oggetti e criteri di configurazione flessibile.

Passaggio 1.

Creare il modello BFD tramite l'oggetto Flexconfig.

Il modello BFD specifica un insieme di valori di intervallo BFD. I valori di intervallo BFD configurati nel modello BFD non sono specifici di una singola interfaccia. È inoltre possibile configurare l'autenticazione per le sessioni single-hop e multi-hop.

Per creare l'oggetto Flex-Config, selezionare **Objects Tab** nella parte superiore, fare clic sul pulsante **FlexConfig** nella colonna sinistra, quindi fare clic sull'opzione **FlexConfig Object** , quindi fare clic su **Add FlexConfig Object**.



Passaggio 2.

Aggiungere i parametri necessari per il protocollo BFD:

Il modello BFD specifica un insieme di valori di intervallo BFD. I valori di intervallo BFD configurati nel modello BFD non sono specifici di una singola interfaccia. È inoltre possibile configurare l'autenticazione per le sessioni single-hop e multi-hop.

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

- single-hop: specifica un modello BFD single-hop.
- multi-hop: specifica un modello BFD multi-hop.
- nome_modello - Specifica il nome del modello. Il nome del modello non può contenere spazi.
- (Facoltativo) Configurare Echo su un modello BFD a hop singolo.

Nota: è possibile attivare la modalità Eco solo in un modello a hop singolo.

Configurare gli intervalli nel modello BFD:

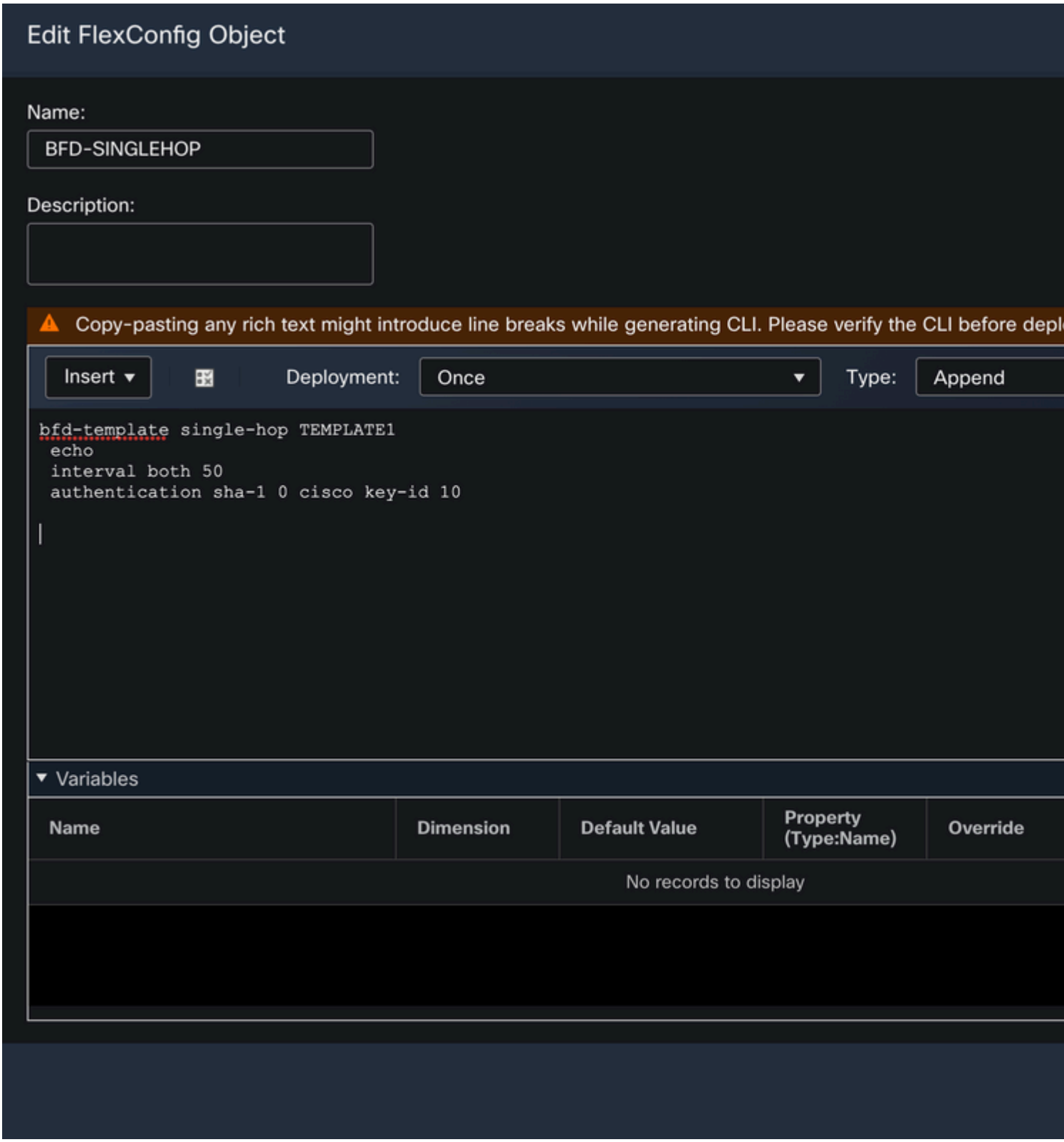
```
interval both milliseconds | microseconds {both | min-tx} microseconds | min-tx milliseconds echo
```

- both - Intervallo minimo di trasmissione e ricezione.
- Intervallo in millisecondi. L'intervallo è compreso tra 50 e 999.
- microsecondi: specifica l'intervallo BFD in microsecondi per bothandmin-tx.
- microsecondi: l'intervallo è compreso tra 50.000 e 999.000.
- min-tx - La capacità dell'intervallo di trasmissione minimo.

Configurare l'autenticazione nel modello BFD:

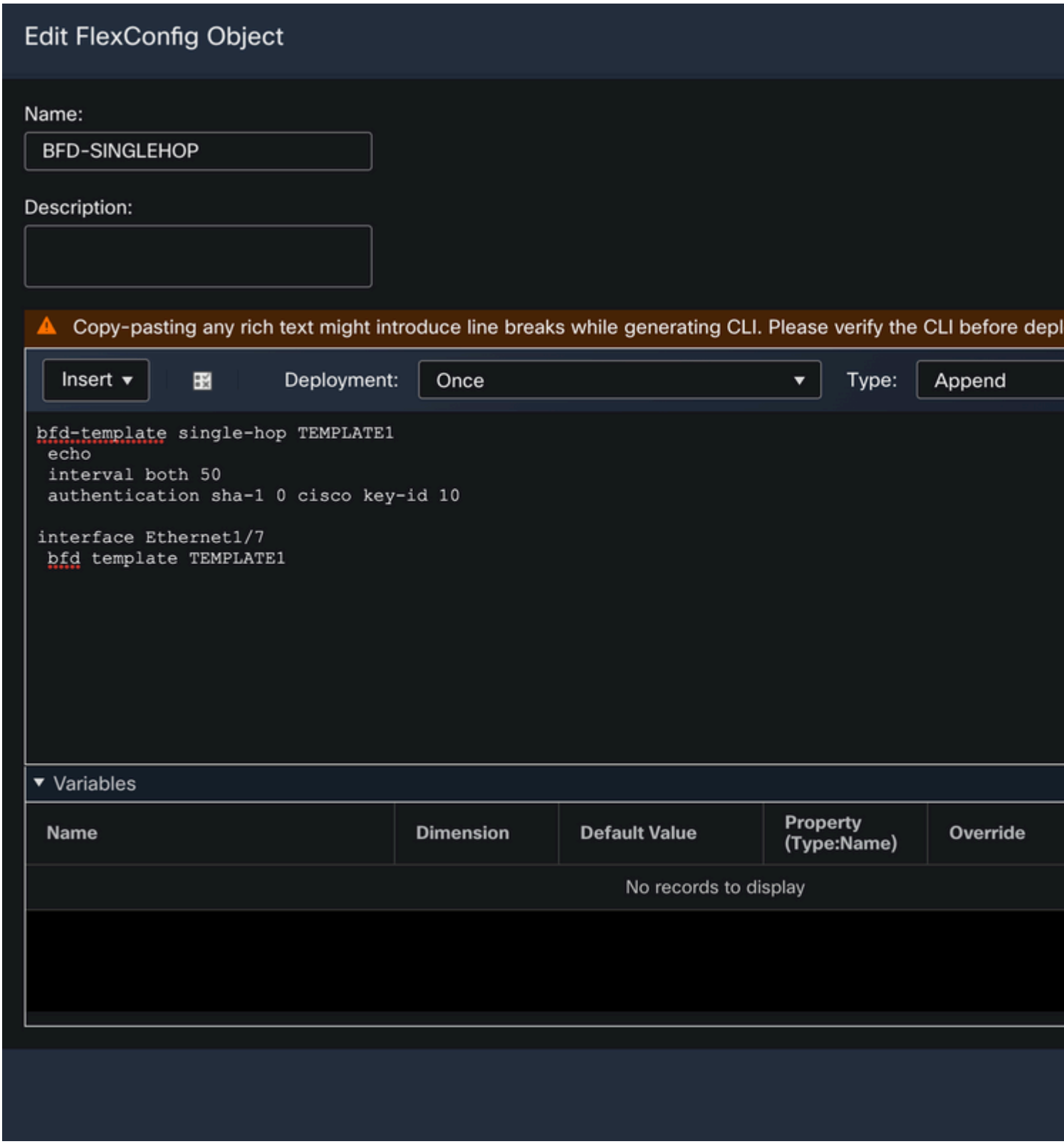
```
authentication {md5 | meticulous-mds | meticulous-sha-1 | sha-1}[0|8] wordkey-id id
```

- authentication: specifica il tipo di autenticazione.
- md5: autenticazione MD5 (Message Digest 5).
- meticulous-md5: autenticazione MD5 con chiave meticolosa.
- meticulous-sha-1: autenticazione SHA-1 con chiave meticolosa.
- sha-1: autenticazione con chiave SHA-1.
- 0|8â€”0 specifica che segue una password NON CRITTOGRAFATA. 8 specifica che segue una password CRIPTATA.
- word - La password BFD (chiave), ovvero una password/chiave a una cifra composta da un massimo di 29 caratteri. Le password che iniziano con una cifra seguita da uno spazio non sono supportate, ad esempio 0 e 1 non sono valide.
- key-id: ID della chiave di autenticazione.
- id - ID della chiave condivisa corrispondente alla stringa della chiave. L'intervallo è compreso tra 0 e 255 caratteri.



Passaggio 3.

Associare il modello BFD all'interfaccia.



Nota: associare il modello multi-hop BFD a una mappa di destinazioni.

Passaggio 4 (facoltativo).

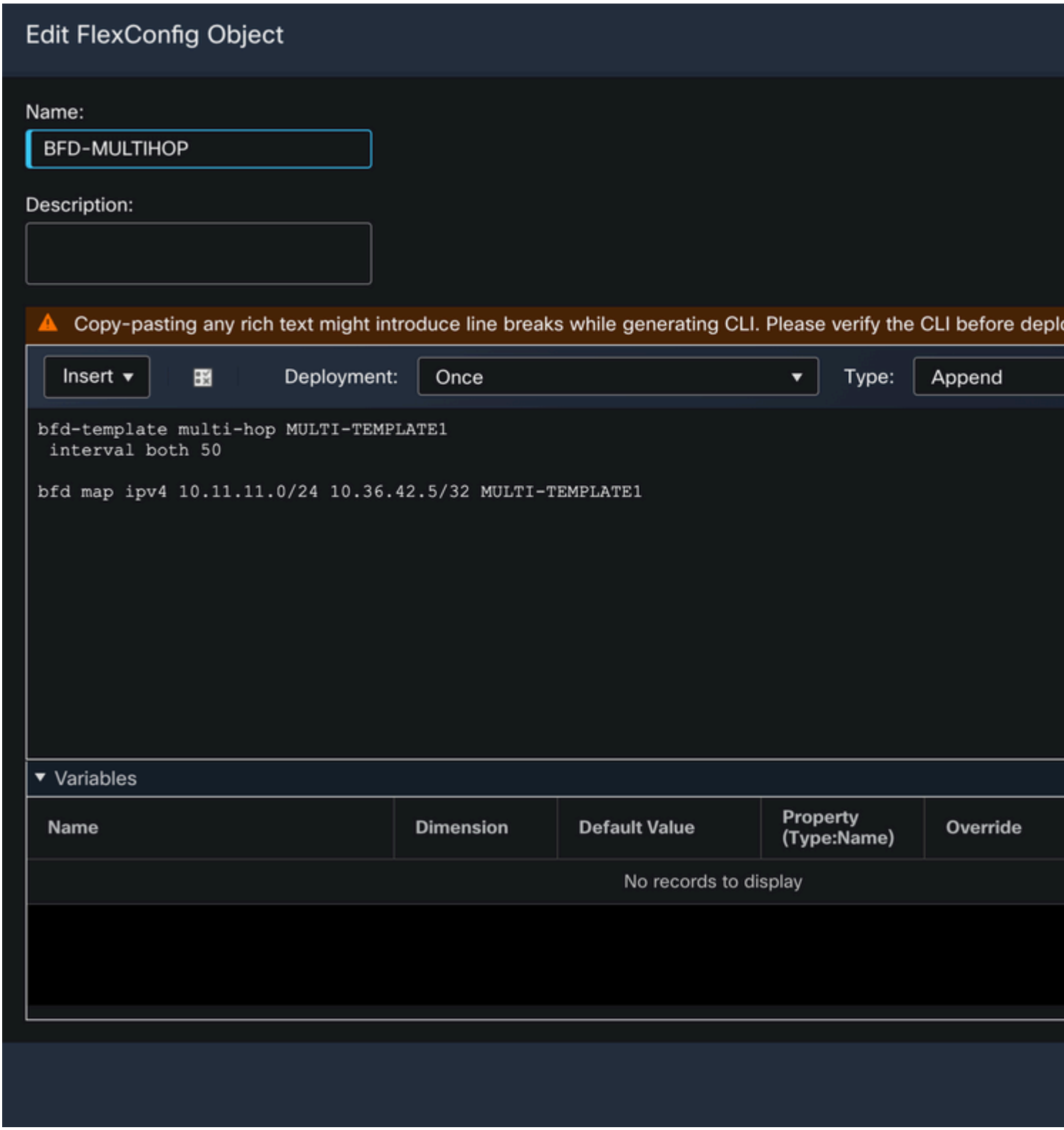
Creare una mappa BFD contenente le destinazioni che è possibile associare a un modello multi-hop. È necessario avere già configurato un modello BFD multi-hop.

Associare il modello multi-hop BFD a una mappa di destinazioni:

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

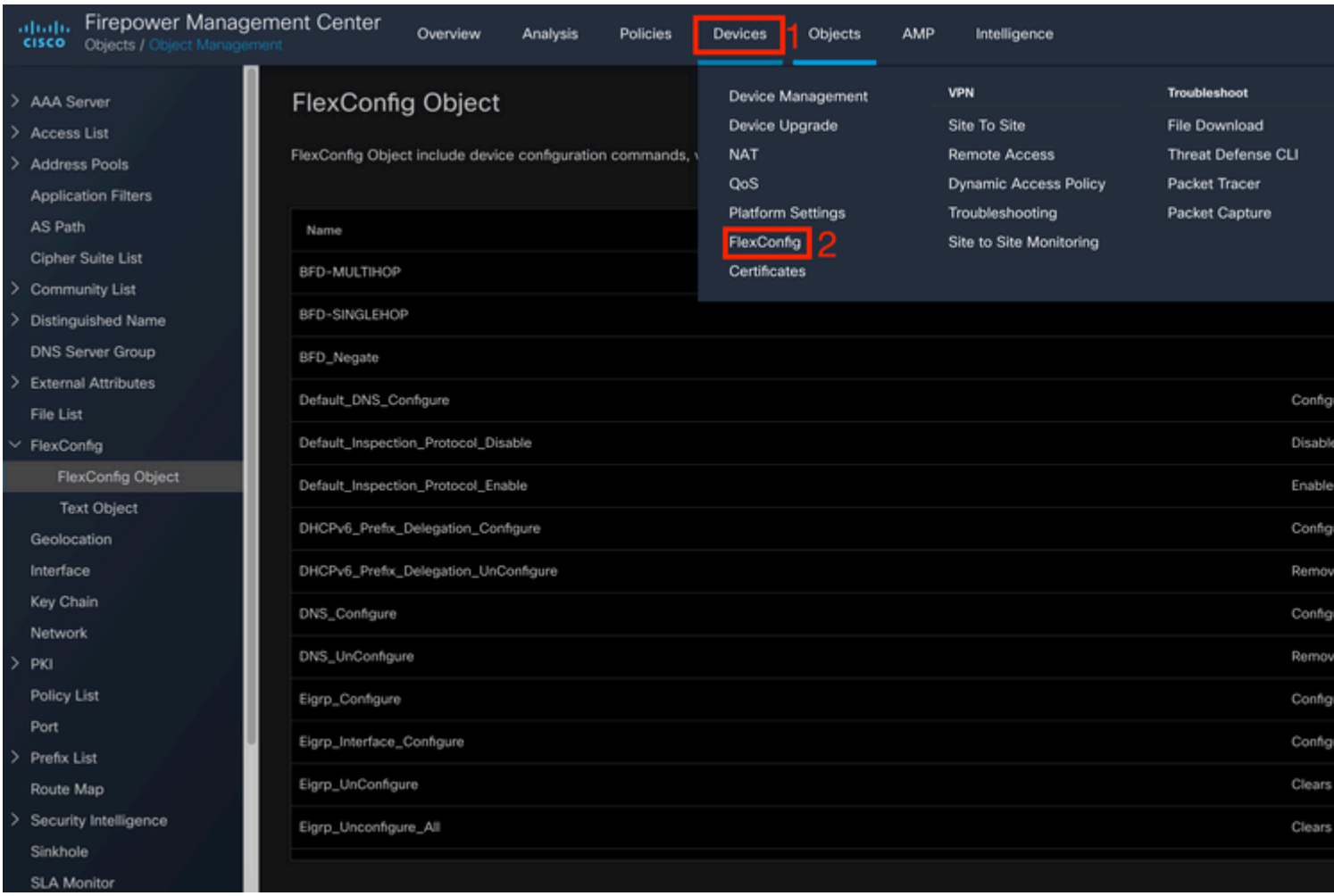
- ipv4: configura un indirizzo IPv4.
- ipv6: configura un indirizzo IPv6.
- destination/cdir: specifica il prefisso/la lunghezza della destinazione. Il formato è A.B.C.D/<0-32>.
- source/cdir: per specificare il prefisso/la lunghezza di destinazione. Il formato è X:X:X;X::X/<0-128>.
- template-name: specifica il nome del modello multi-hop associato a questa mappa BFD.

Fare clic sul pulsante **Save** per salvare l'oggetto.



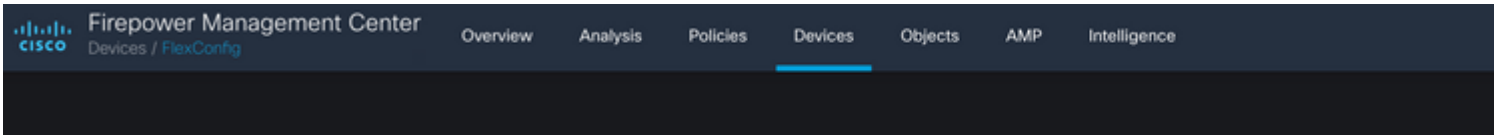
Passaggio 5.

Fare clic sul pulsante **Devices** nella parte superiore e selezionare la scheda **FlexConfig** opzione.



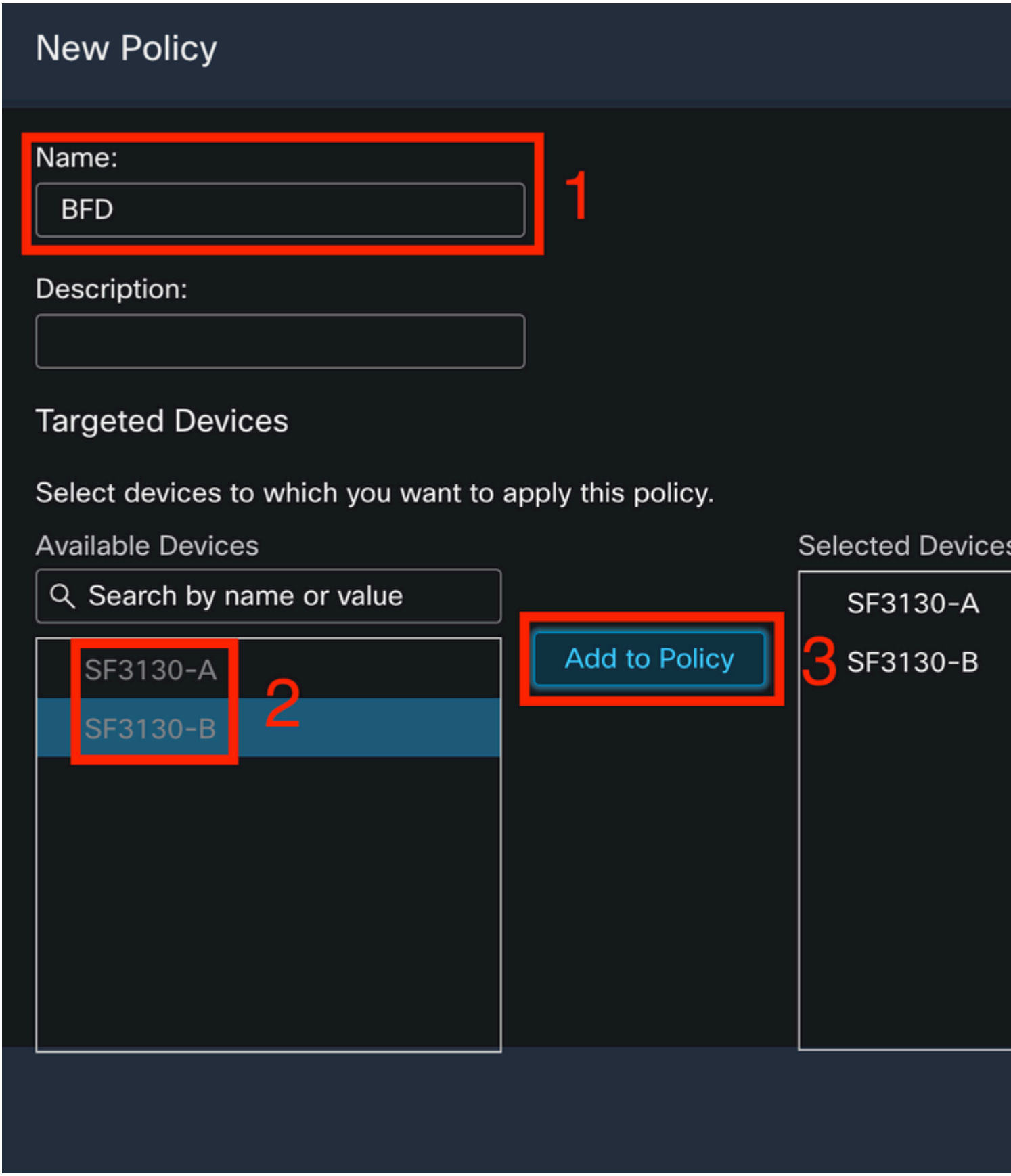
Passaggio 6.

Per creare un nuovo criterio FlexConfig, fare clic sul pulsante **New Policy** pulsante.



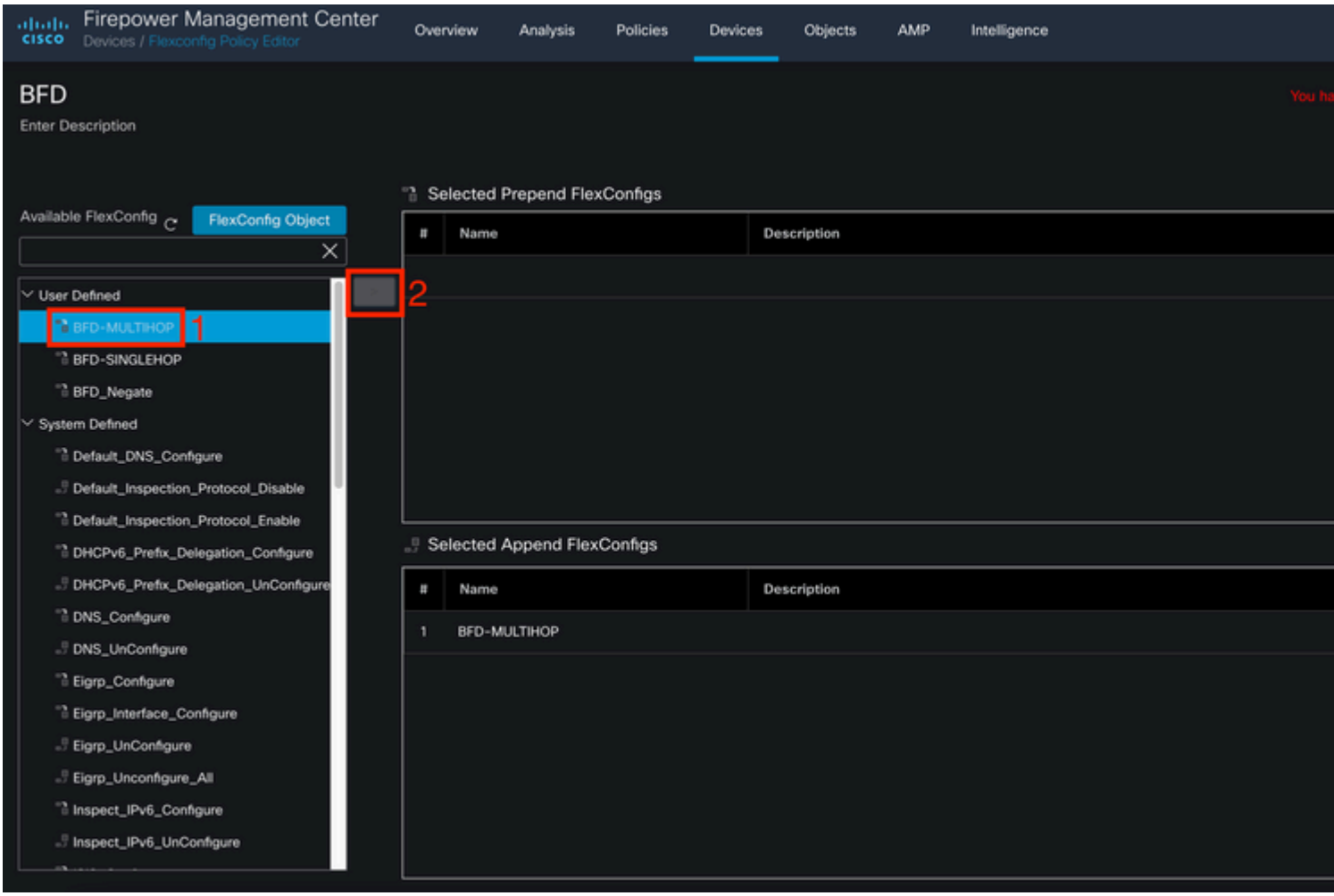
Passaggio 7.

Name il criterio e selezionare i dispositivi assegnati al criterio. Fare clic sul pulsante **Add to Policy** quindi fare clic sul pulsante **Save**pulsante.



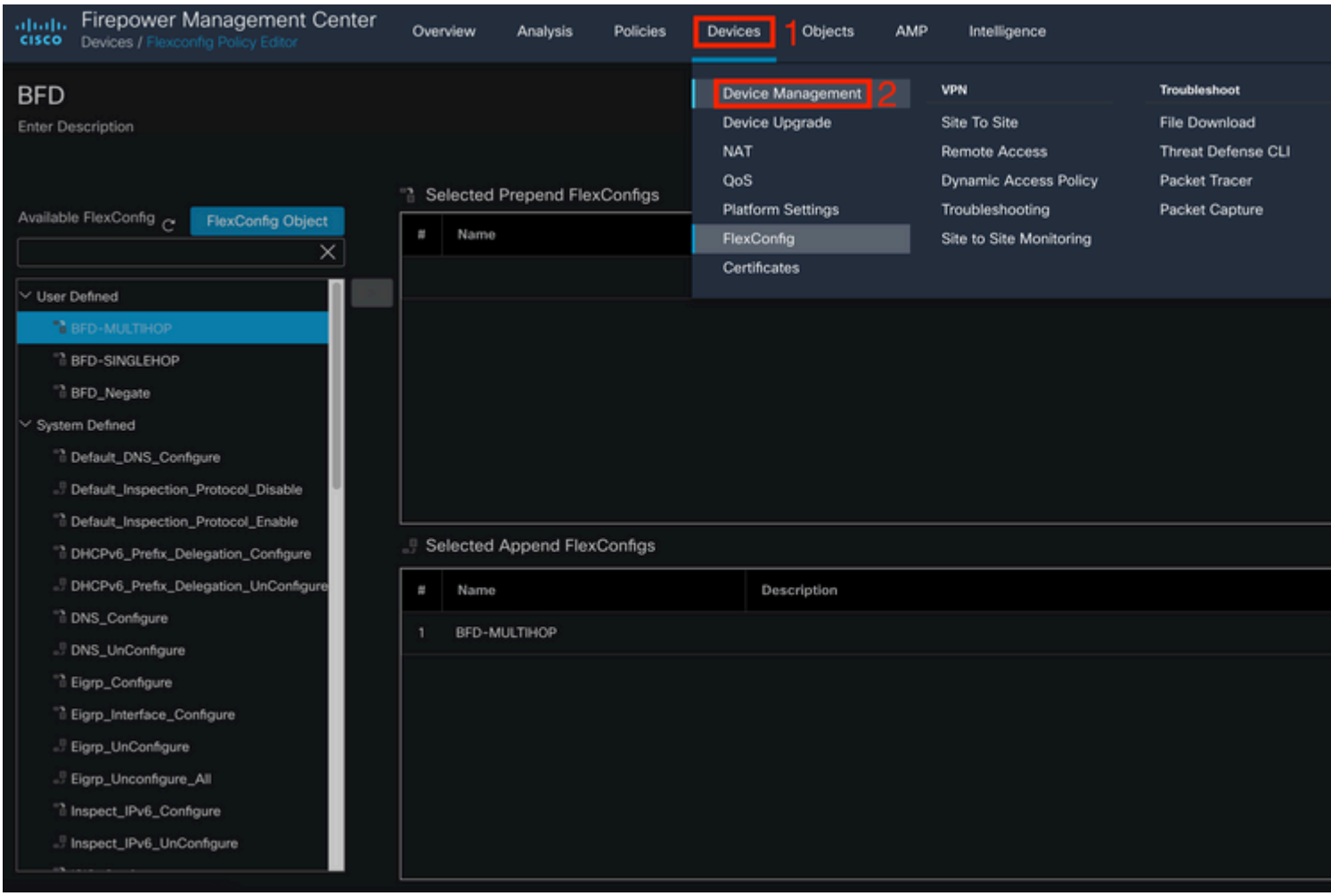
Passaggio 8.

Selezionare l'oggetto FlexConfig nella colonna sinistra e fare clic sul pulsante > per aggiungere l'oggetto al criterio FlexConfig, quindi fare clic sul pulsante **Save** pulsante.



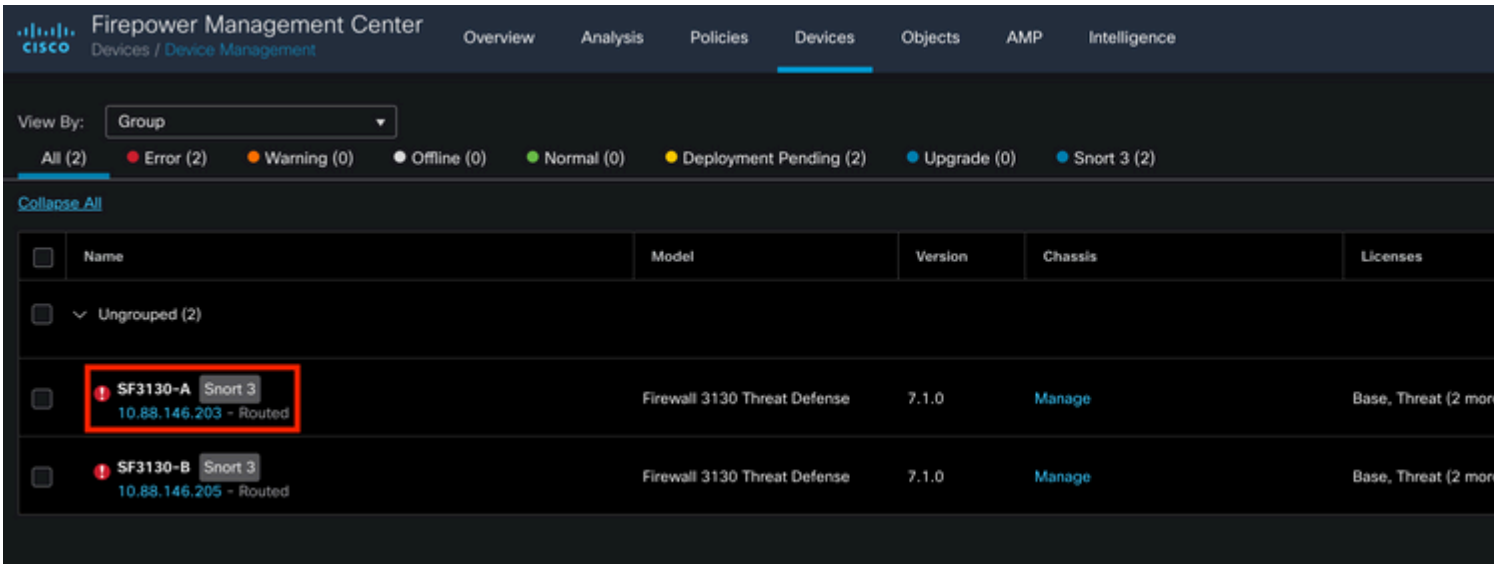
Passaggio 9.

Fare clic sul pulsante **Devices** nella parte superiore e fare clic sulla scheda **Device Management** opzione.



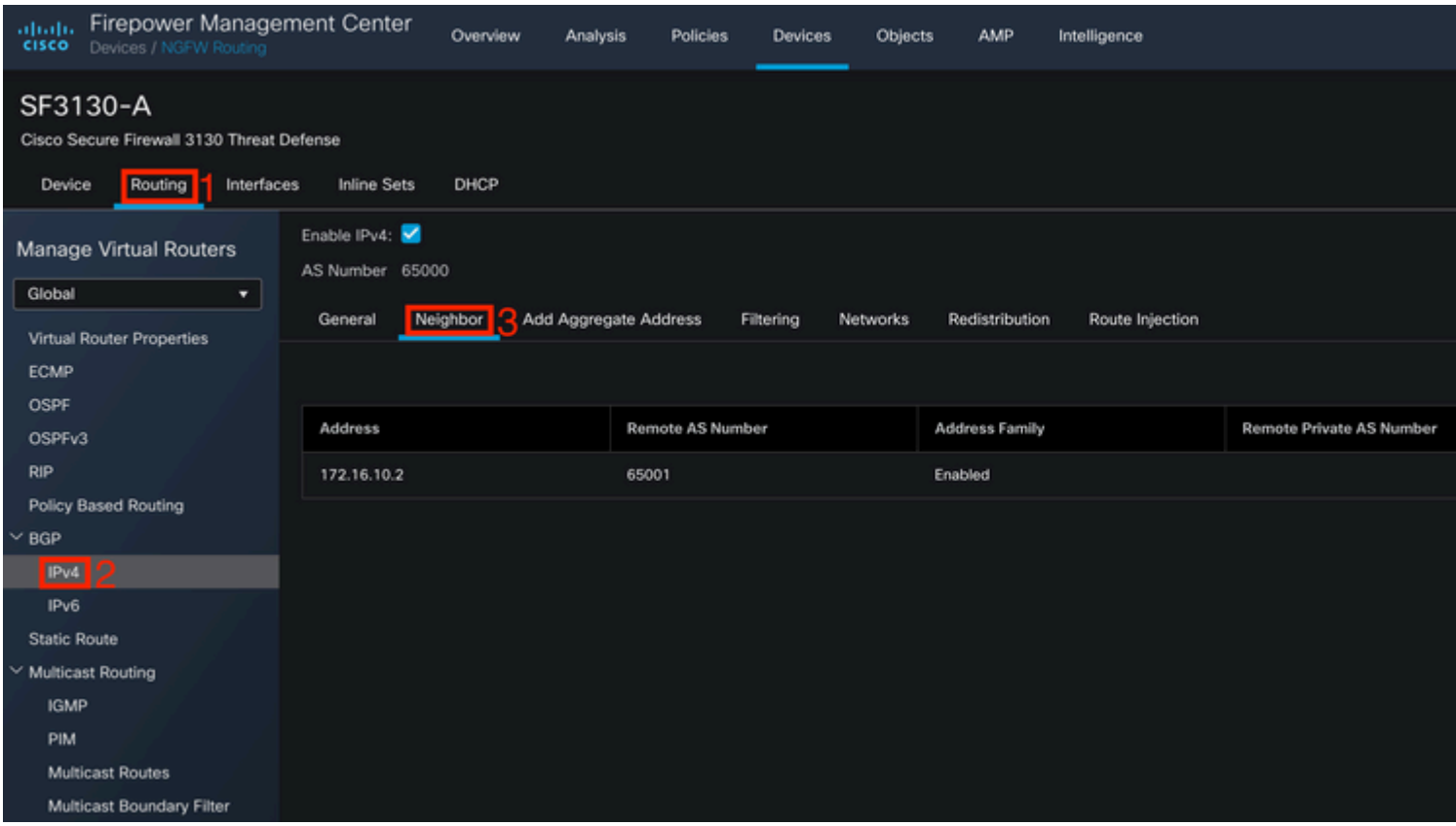
Passaggio 10.

Selezionare il dispositivo a cui assegnare la configurazione BFD.



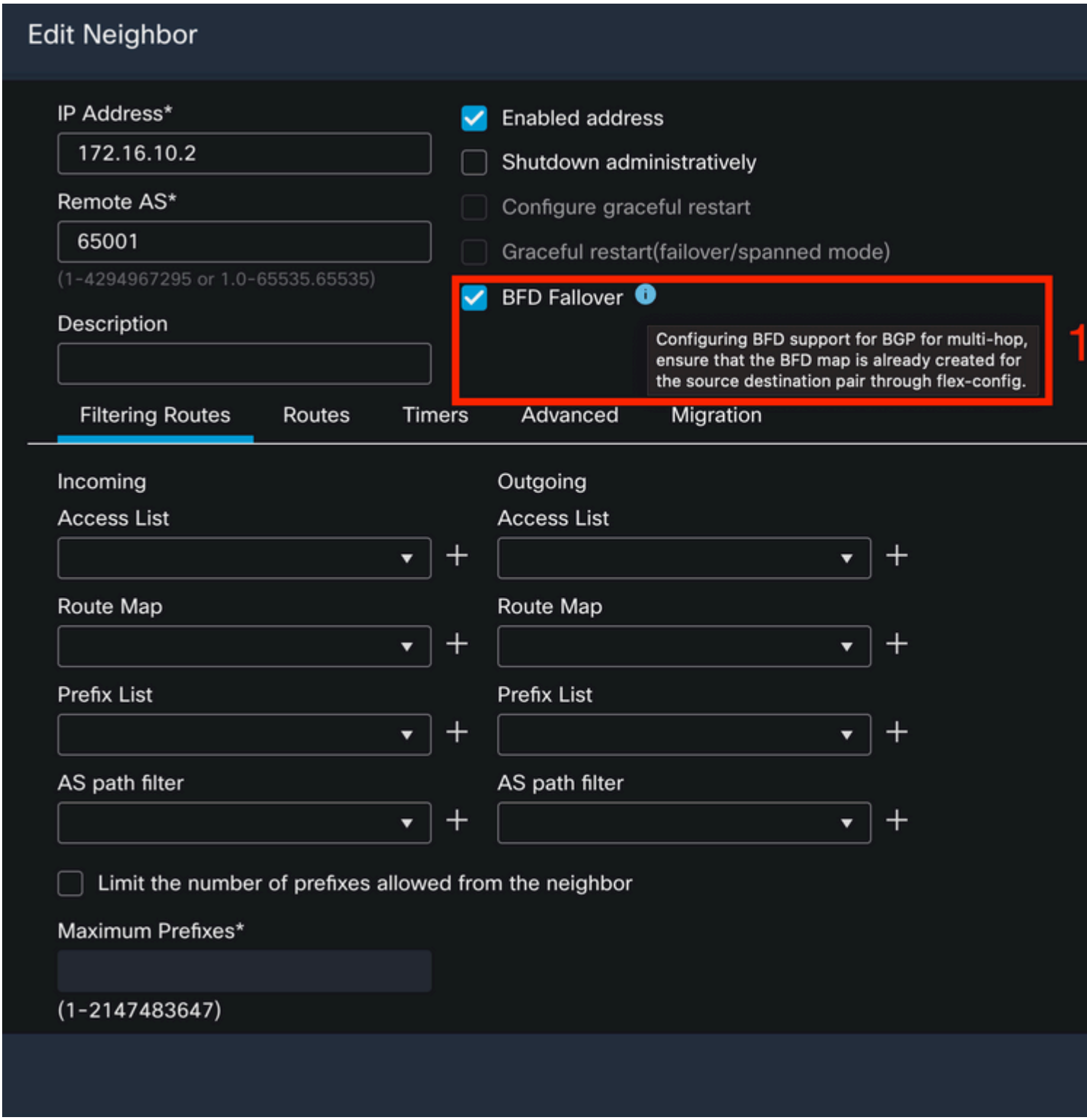
Passaggio 11.

Fare clic sul pulsante Routing , quindi fare clic sulla scheda**IPv4** o **IPv6**, a seconda della configurazione nella sezione BGP della colonna sinistra, quindi fare clic sul pulsante **Neighbor** e fare clic sul pulsante modifica matita per modificarla.



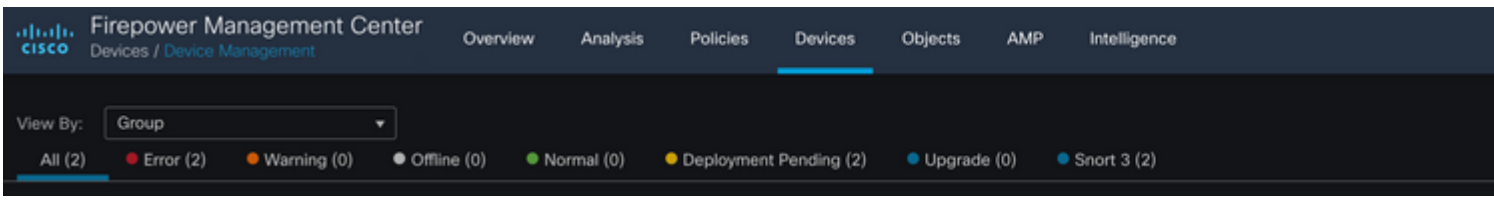
Passaggio 12.

Selezionare il **checkbox** per il failover BFD e fare clic sul pulsante **OK** pulsante.



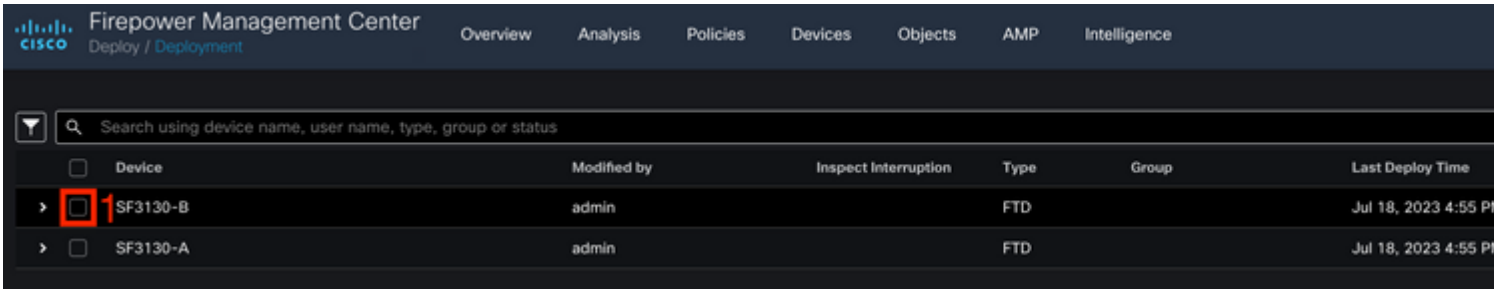
Passaggio 13.

Fare clic sul pulsante **Deploy** , quindi fare clic sul pulsante **Deployment** pulsante.



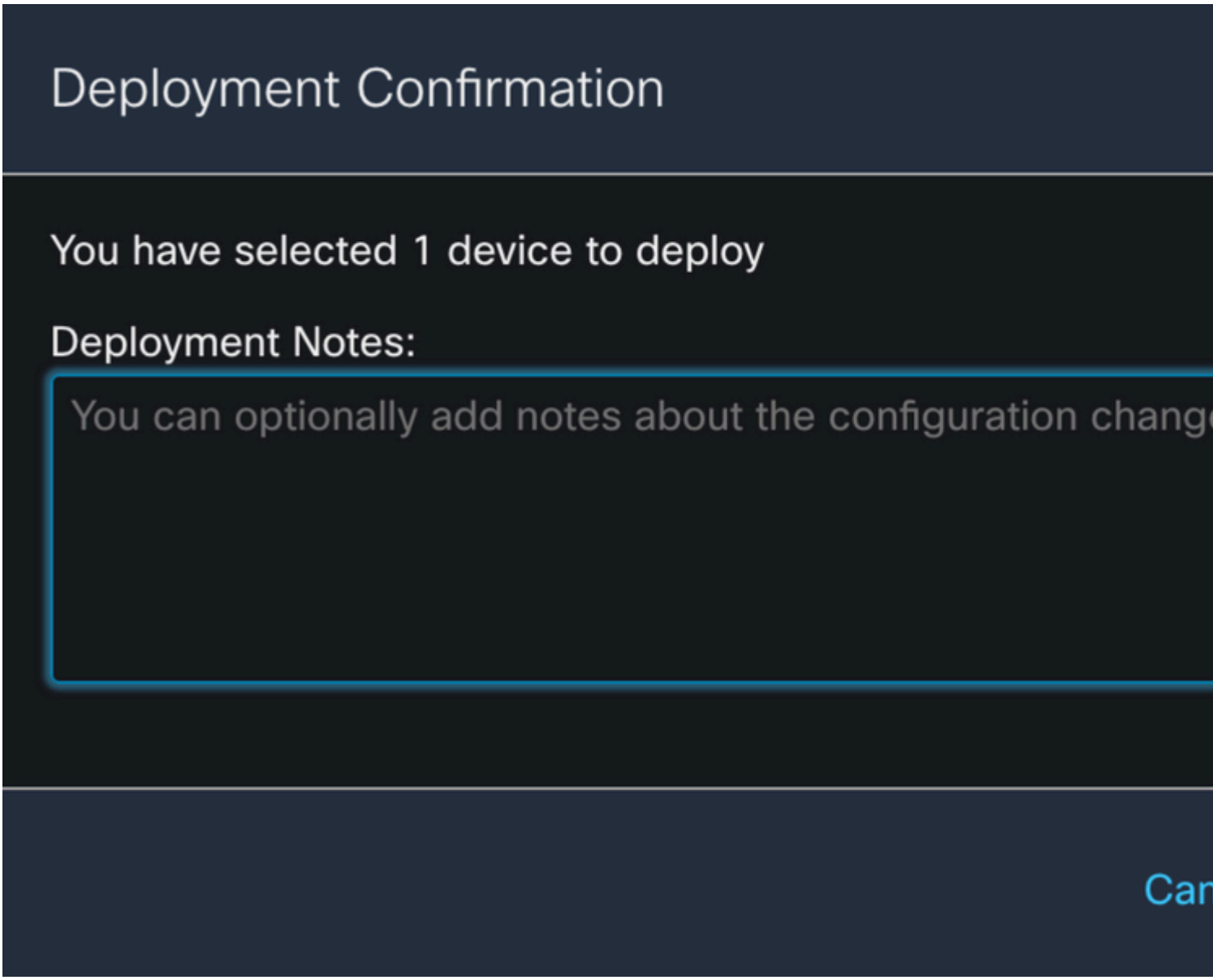
Passaggio 14.

Selezionare il dispositivo a cui verranno assegnate le modifiche facendo clic sul pulsante **checkbox**e quindi fare clic sul pulsante**Deploy** pulsante.



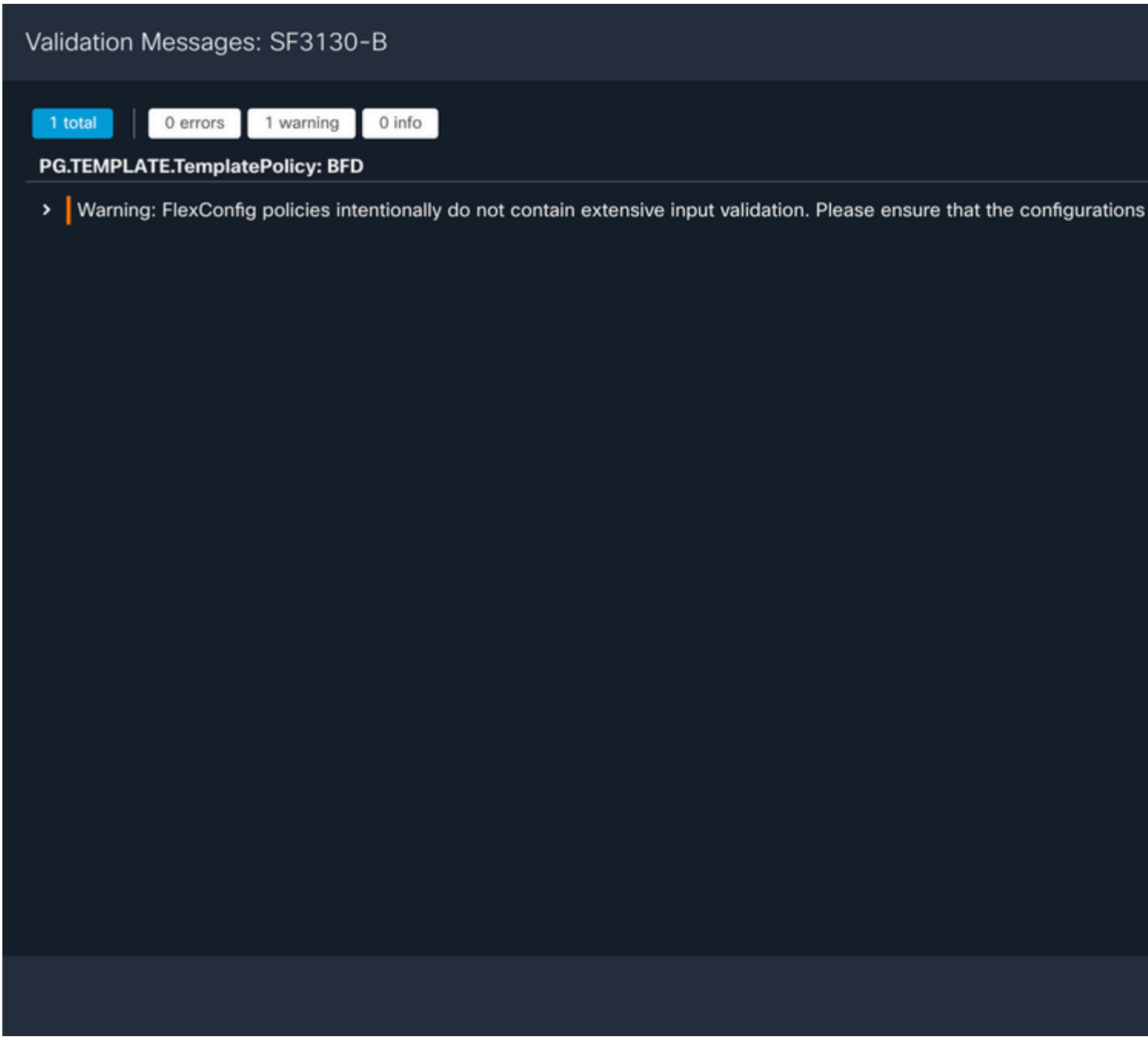
Passaggio 15.

Fare clic sul pulsante **Deploy** pulsante.



Passaggio 16.

Fare clic sul pulsante **Deploy** pulsante.



Nota: l'avviso è previsto ed è puramente informativo.

Verifica

Verificare la configurazione BFD e lo stato direttamente nella sessione CLI con i comandi successivi.

<#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
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).