Konfigurieren von BFD in Secure Firewall Threat Defense mit Flex-Config

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration des BFD-Protokolls in Secure Firewall Management Center mit Version 7.2 und früheren Versionen mit Flex-Config beschrieben.

Voraussetzungen

Border Gateway Protocol (BGP) wird in Cisco Secure Firewall Threat Defense (FTD) mit Cisco Secure Firewall Management Center (FMC) konfiguriert.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

-BGP-Protokoll
- BFD-Konzepte

Verwendete Komponenten

- Cisco Secure Firewall Management Center mit Version 7.2 oder früheren Versionen

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

BFD (Bidirectional Forwarding Detection) ist ein Erkennungsprotokoll, das entwickelt wurde, um eine schnelle Erkennung von Pfadausfällen für alle Medientypen, Kapselungen, Topologien und Routing-Protokolle zu ermöglichen.

Konfigurieren

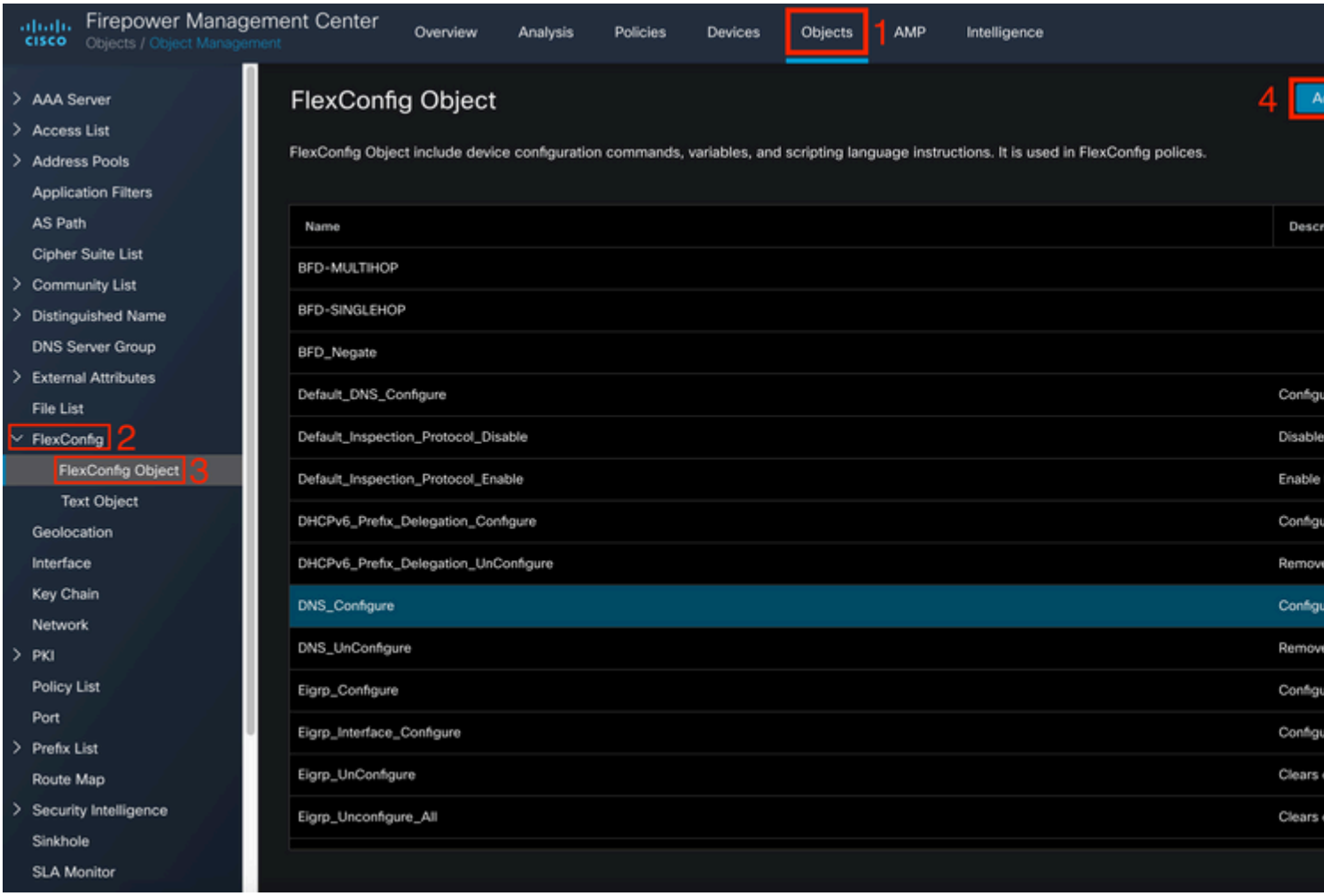
BFD-Konfigurationen in FMC mit Version 7.2 und früheren Versionen müssen mit Flex-Config-Richtlinien und -Objekten konfiguriert werden.

Schritt 1:

Erstellen Sie die BFD-Vorlage über Flexconfig-Objekt.

Die BFD-Vorlage legt eine Reihe von BFD-Intervallwerten fest. Die in der BFD-Vorlage konfigurierten BFD-Intervallwerte sind nicht spezifisch für eine einzelne Schnittstelle. Sie können auch die Authentifizierung für Single-Hop- und Multi-Hop-Sitzungen konfigurieren.

Um das Flex-Config-Objekt zu erstellen, wählen Sie **Objects Tab** Klicken Sie oben auf das **FlexConfig** in der linken Spalte ein, und klicken Sie dann auf **FlexConfig Object** und klicke anschließend auf **Add FlexConfig Object**.



Schritt 2:

Fügen Sie die für das BFD-Protokoll erforderlichen Parameter hinzu:

Die BFD-Vorlage legt eine Reihe von BFD-Intervallwerten fest. Die in der BFD-Vorlage konfigurierten BFD-Intervallwerte sind nicht spezifisch für eine einzelne Schnittstelle. Sie können auch die Authentifizierung für Single-Hop- und Multi-Hop-Sitzungen konfigurieren.

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

- single-hop - Gibt eine single-hop BFD-Vorlage an.
- multi-hop - Gibt eine Multi-Hop-BFD-Vorlage an.
- template_name - Gibt den Vorlagennamen an. Der Vorlagenname darf keine Leerzeichen enthalten.
- (Optional) Konfigurieren Sie Echo auf einer Single-Hop-BFD-Vorlage.

Hinweis: Sie können den Echo-Modus nur für eine Single-Hop-Vorlage aktivieren.

Konfigurieren Sie die Intervalle in der BFD-Vorlage:

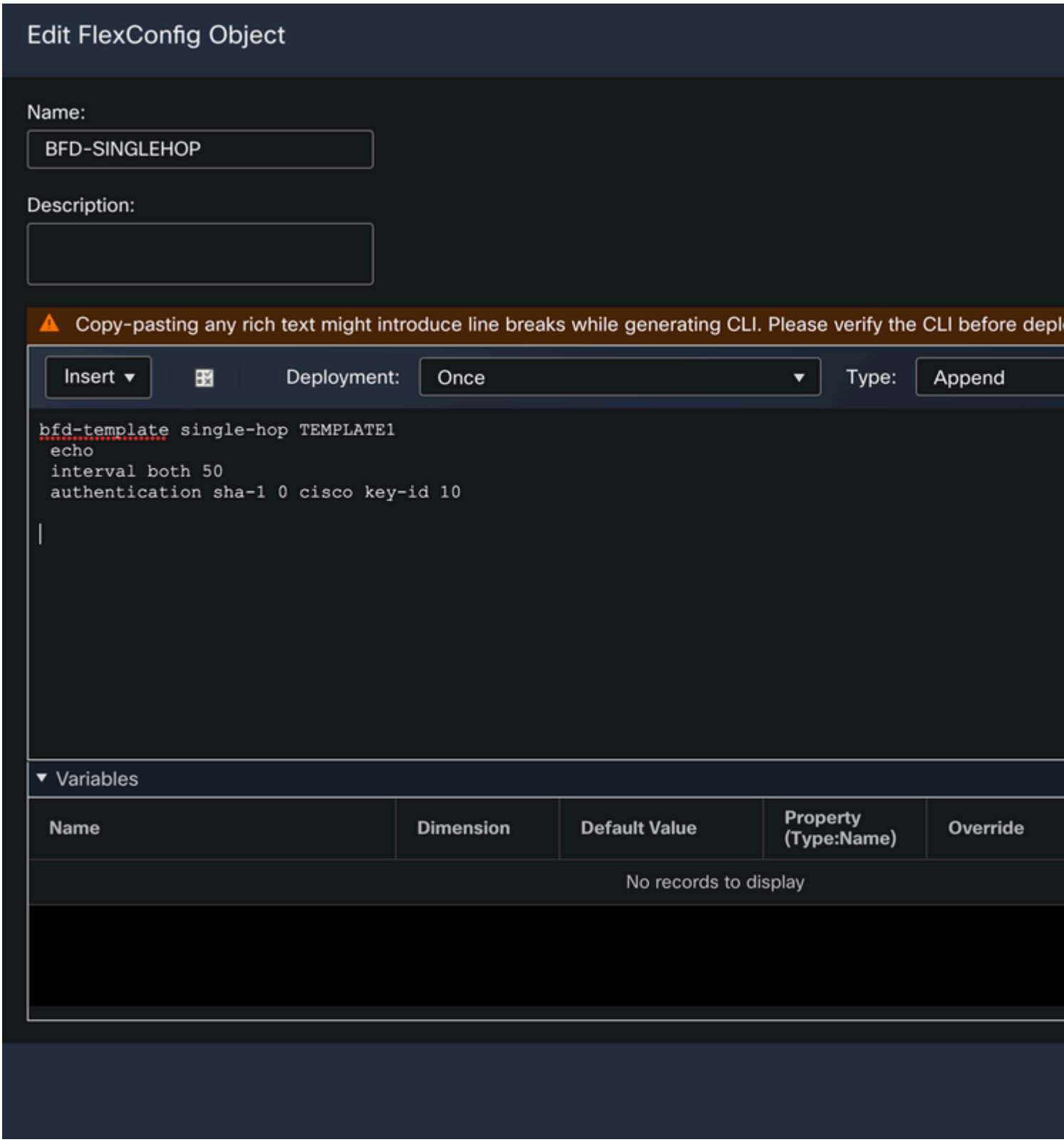
```
interval both milliseconds | microseconds {both | min-tx} microseconds | min-tx milliseconds echo
```

- both - Mindestkapazität für Übertragungs- und Empfangsintervall.
- Das Intervall in Millisekunden. Der Bereich liegt zwischen 50 und 999.
- microseconds (Mikrosekunden): Gibt das BFD-Intervall in Mikrosekunden für "forbothandmin-tx" an.
- Mikrosekunden - Der Bereich liegt zwischen 50.000 und 999.000.
- min-tx: Die Funktion für das minimale Übertragungsintervall.

Konfigurieren Sie die Authentifizierung in der BFD-Vorlage:

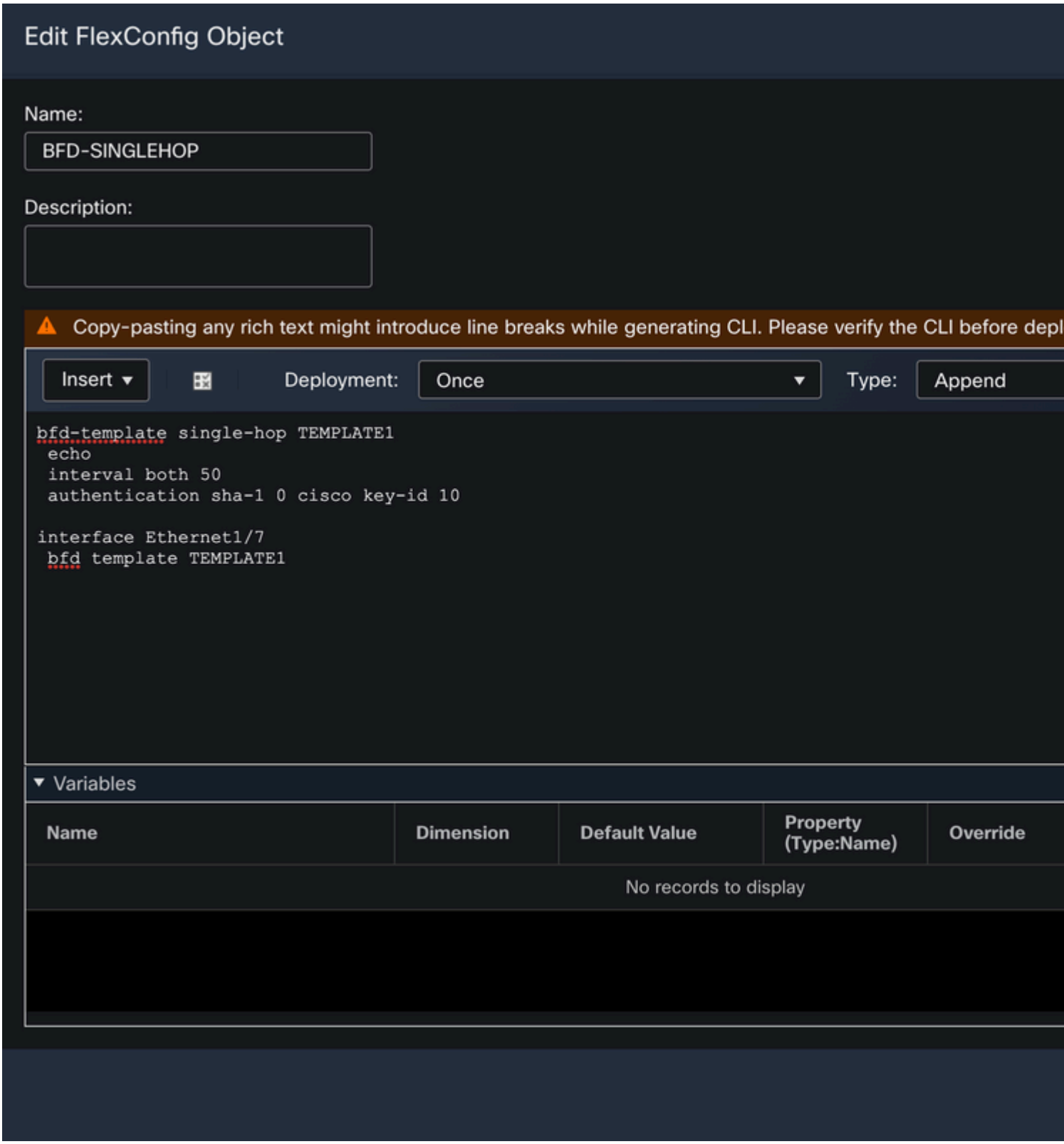
```
authentication {md5 | meticulous-mds | meticulous-sha-1 | sha-1}[0|8] wordkey-id id
```

- authentication - Gibt den Authentifizierungstyp an.
- md5 - MD5-Authentifizierung (Message Digest 5).
- meticulous-md5 - Präzise verschlüsselte MD5-Authentifizierung.
- akribisch-sha-1 - Akribisch verschlüsselte SHA-1-Authentifizierung.
- sha-1 - Schlüsselbasierte SHA-1-Authentifizierung.
- 0|8-0 gibt an, dass ein UNVERSCHLÜSSELTES Kennwort folgt. 8 gibt an, dass ein VERSCHLÜSSELTES Kennwort folgt.
- word - Das BFD-Kennwort (Schlüssel), d. h. ein einstelliges Kennwort bzw. ein Schlüssel mit bis zu 29 Zeichen. Kennwörter, die mit einer Ziffer gefolgt von einem Leerzeichen beginnen, werden nicht unterstützt, z. B. 0 pass und 1 sind ungültig.
- key-id: Die Authentifizierungsschlüssel-ID.
- id: Die ID des freigegebenen Schlüssels, die der Schlüsselzeichenfolge entspricht. Der Bereich umfasst 0 bis 255 Zeichen.



Schritt 3:

Ordnen Sie die BFD-Vorlage der Schnittstelle zu.



Hinweis: Ordnen Sie die BFD-Multi-Hop-Vorlage einer Zielzuordnung zu.

Schritt 4 (optional).

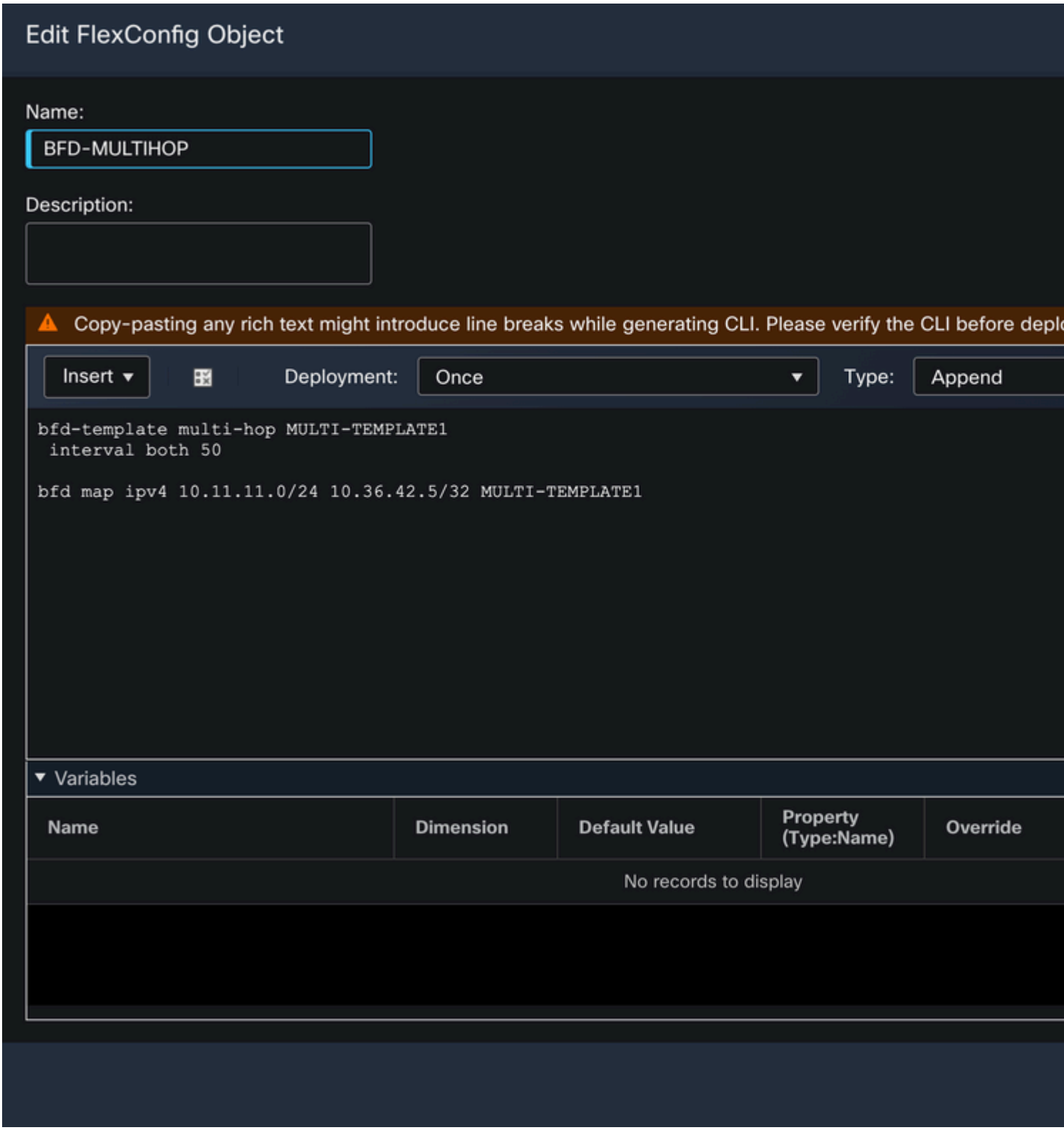
Erstellen Sie eine BFD-Zuordnung mit Zielen, die Sie einer Multi-Hop-Vorlage zuordnen können. Es muss bereits eine Multi-Hop-BFD-Vorlage konfiguriert sein.

Ordnen Sie die BFD-Multi-Hop-Vorlage einer Zielzuordnung zu:

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

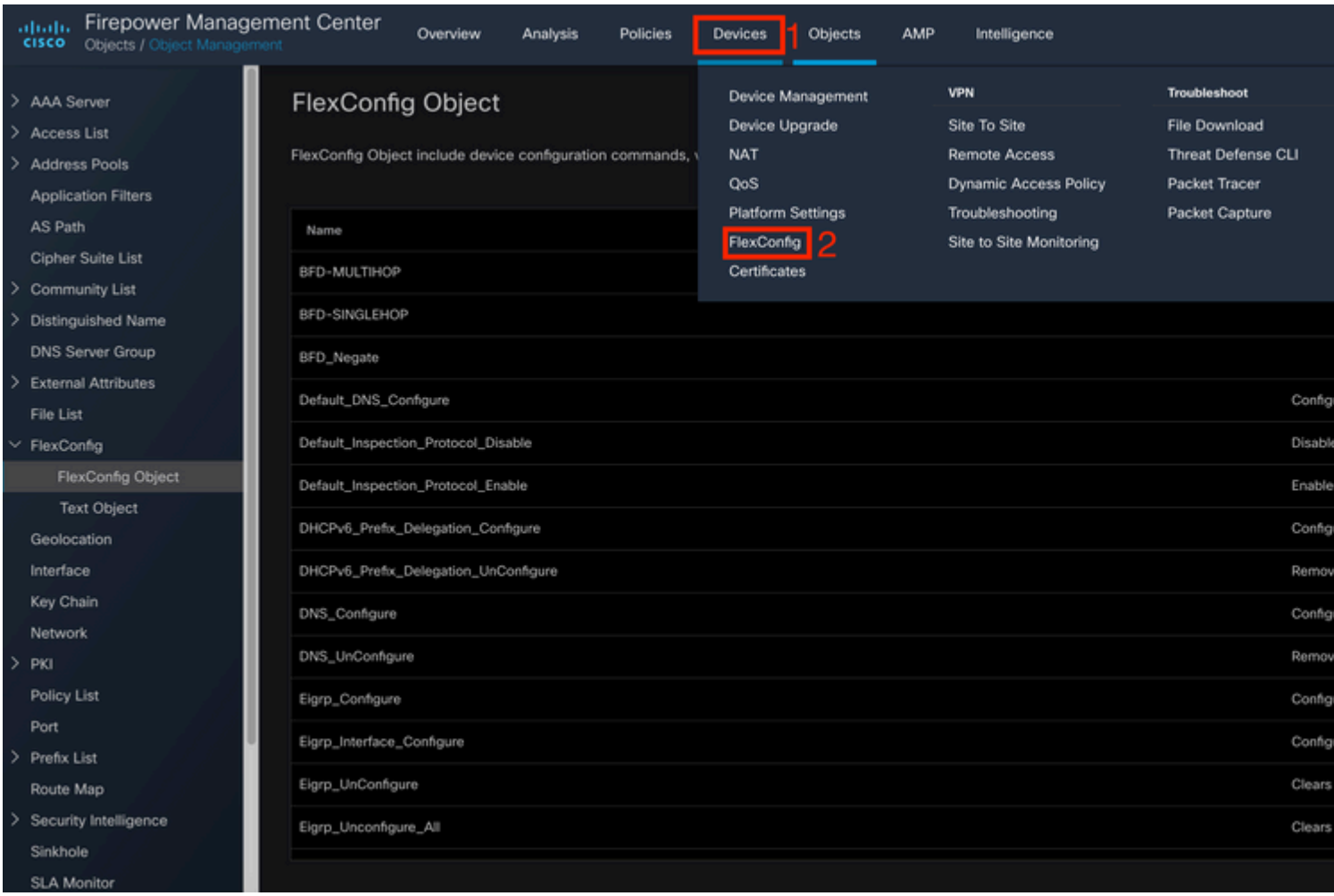
- ipv4 - Konfiguriert eine IPv4-Adresse.
- ipv6 - Konfiguriert eine IPv6-Adresse.
- destination/cdir - Gibt das/die Zielpräfix/Länge an. Das Format ist A.B.C.D/<0-32>.
- source/cdir - Gibt das/die Zielpräfix/Länge an. Das Format ist X:X:X;X::X/<0-128>.
- template-name - Gibt den Namen der Multi-Hop-Vorlage an, die dieser BFD-Zuordnung zugeordnet ist.

Klicken Sie auf **Save** um das Objekt zu speichern.



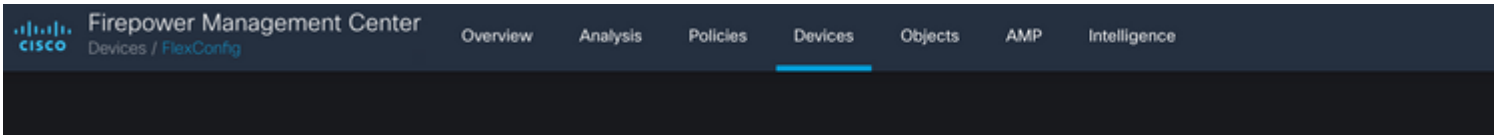
Schritt 5:

Klicken Sie auf **Devices** und wählen Sie die **FlexConfig** Option.



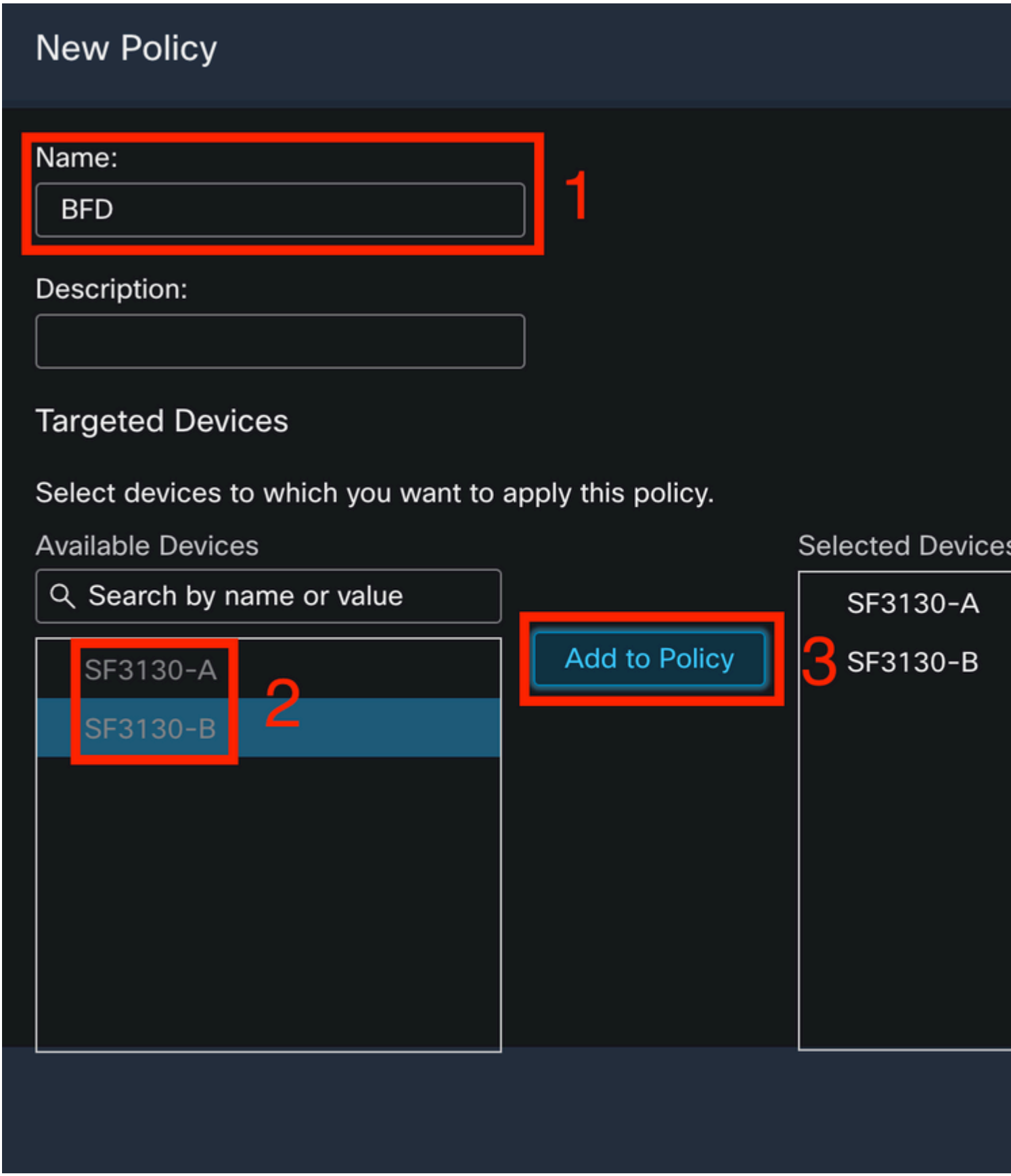
Schritt 6:

Um eine neue FlexConfig-Richtlinie zu erstellen, klicken Sie auf **New Policy** -Taste.



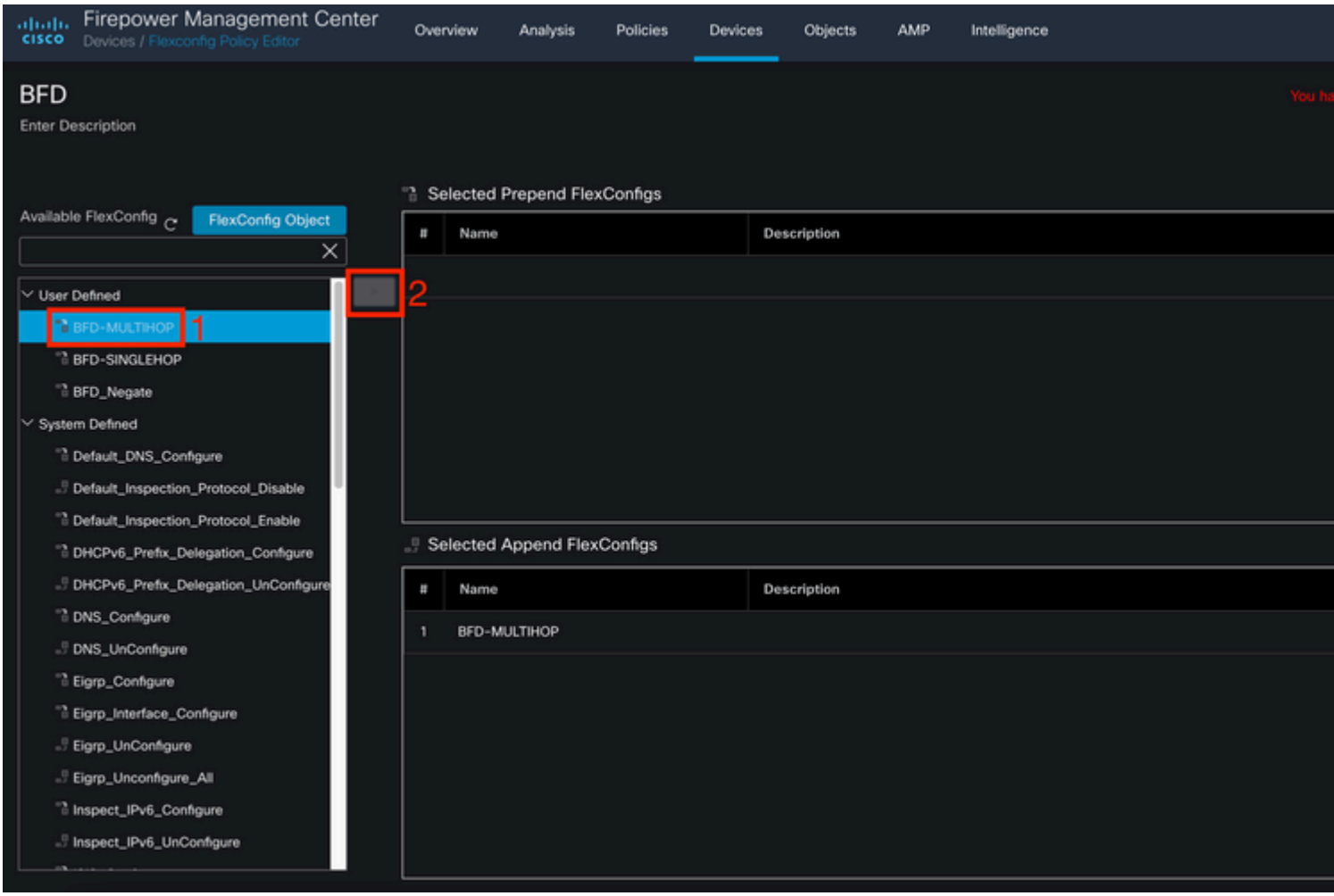
Schritt 7.

Name die Richtlinie und wählen Sie die der Richtlinie zugewiesenen Geräte aus. Klicken Sie auf **Add to Policy** klicken Sie dann auf **Save**-Taste.



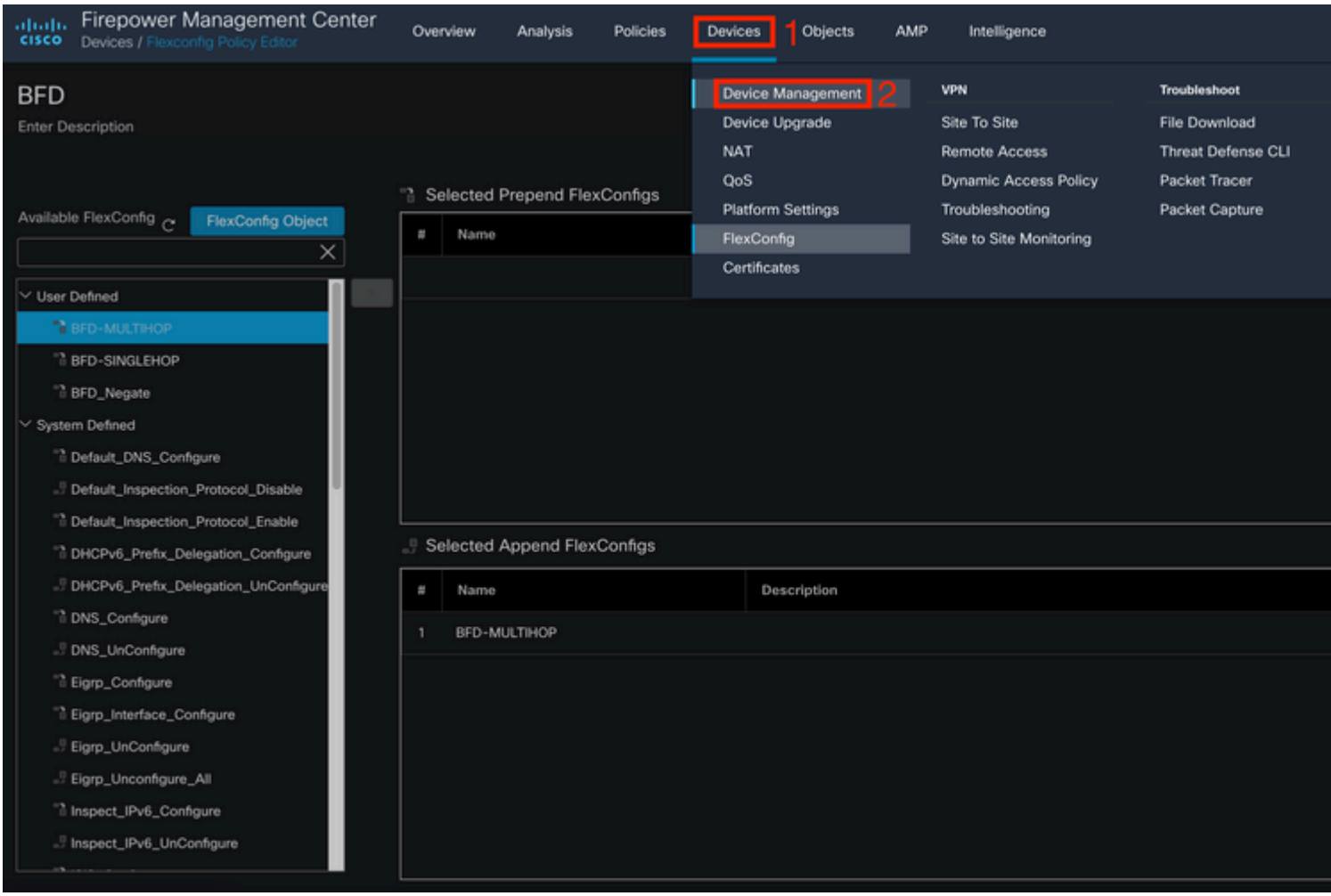
Schritt 8:

Wählen Sie in der linken Spalte das FlexConfig-Objekt aus, und klicken Sie auf > um das Objekt der FlexConfig-Richtlinie hinzuzufügen, und klicken Sie auf **Save** -Taste.



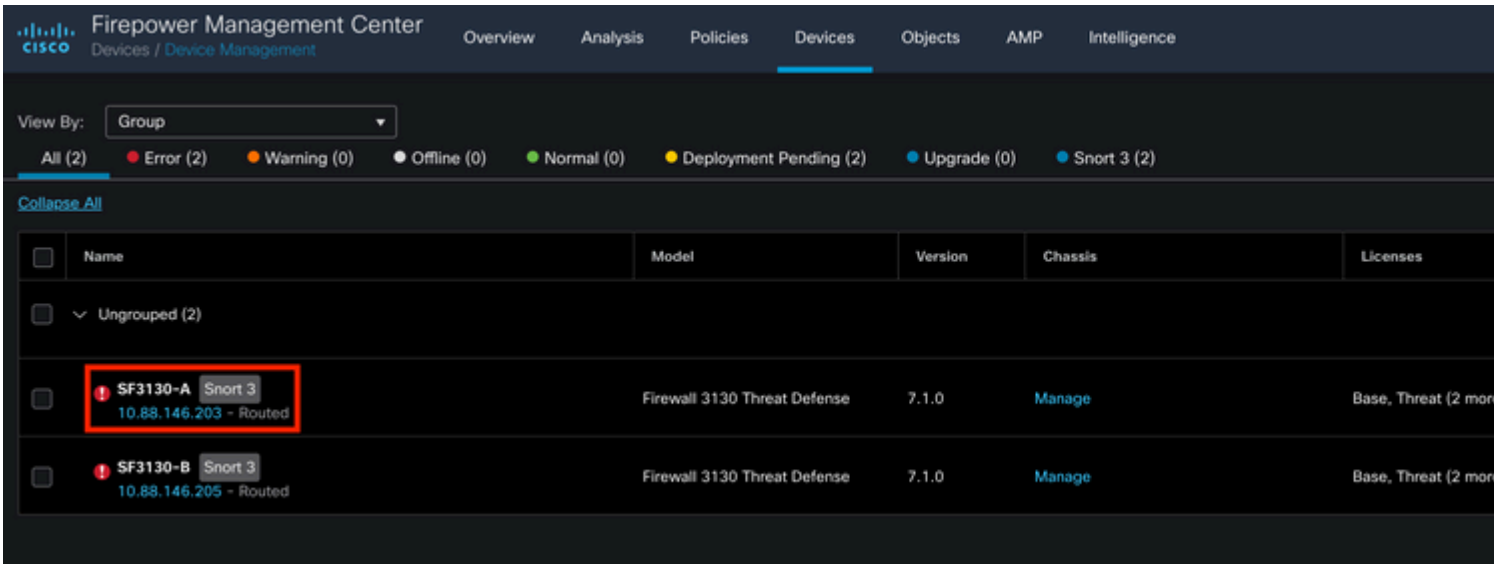
Schritt 9.

Klicken Sie auf **Devices** und klicke auf die Schaltfläche **Device Management** Option.



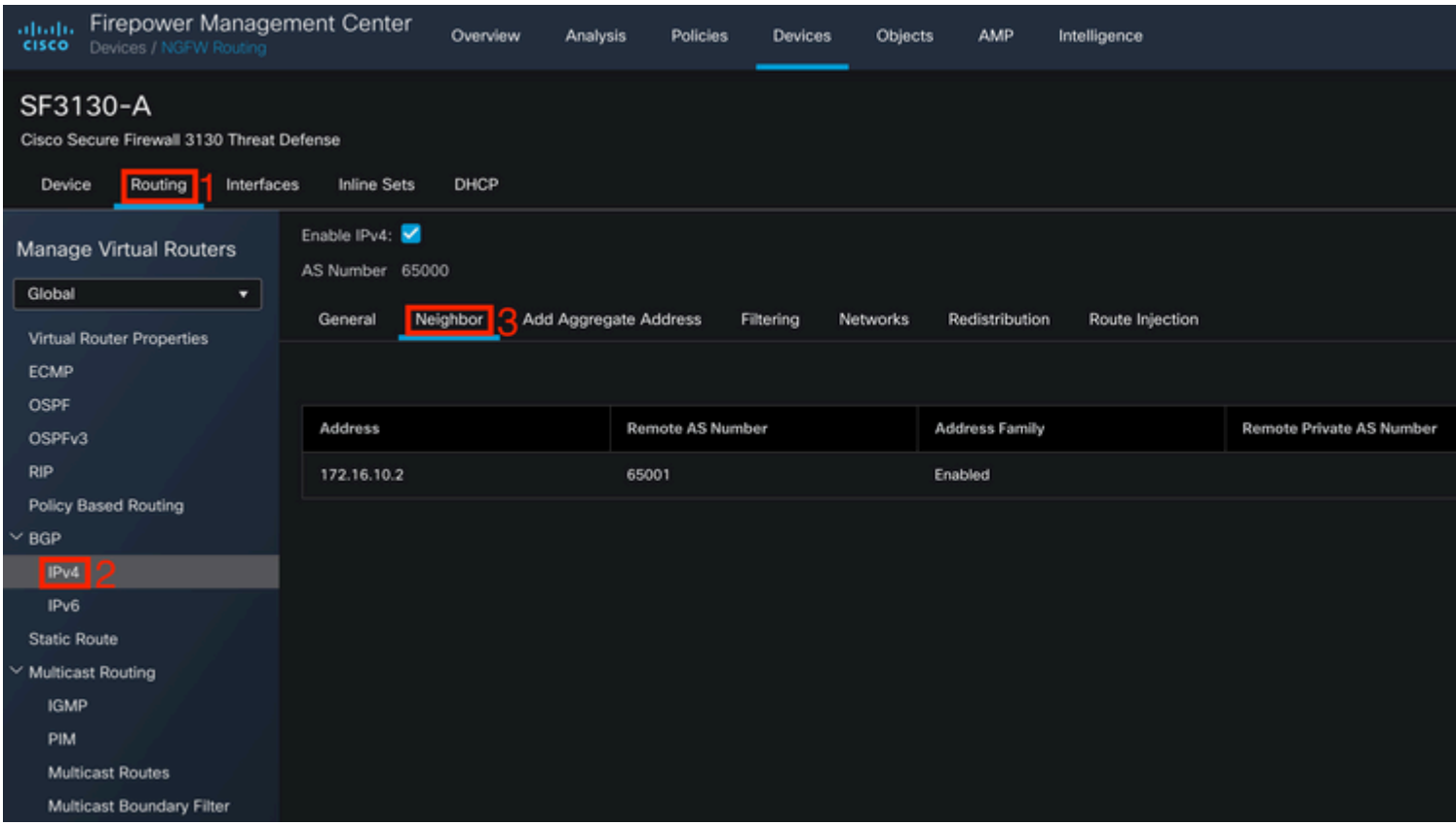
Schritt 10.

Wählen Sie das Gerät aus, dem die BFD-Konfiguration zugewiesen werden soll.



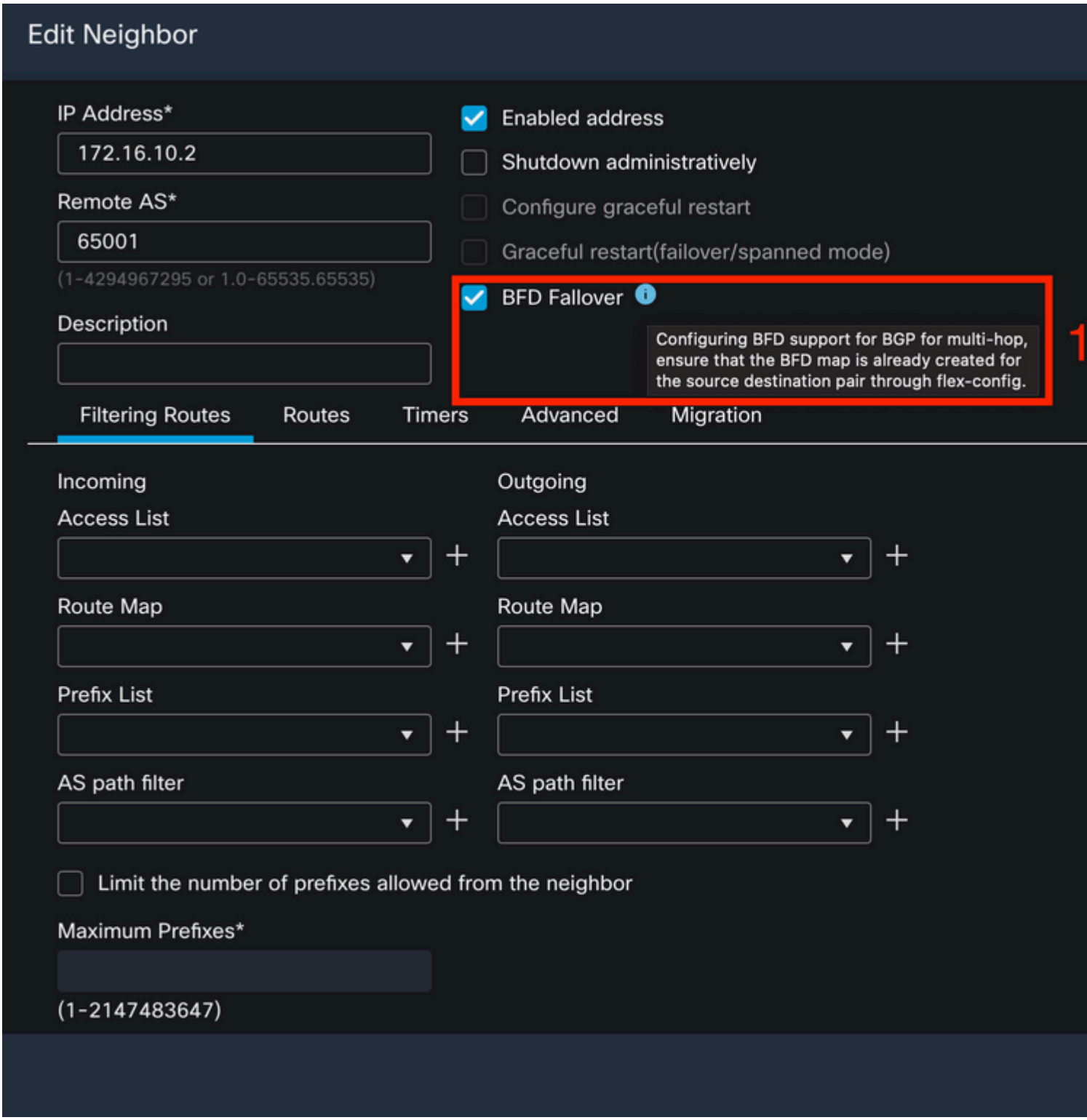
Schritt 11.

Klicken Sie auf Routing auf, und klicken Sie dann auf**IPv4** Oder **IPv6,** je nach Konfiguration im Abschnitt "BGP" in der linken Spalte. Klicken Sie dann auf **Neighbor** und klicke auf die Bleistiftschaltfläche, um sie zu bearbeiten.



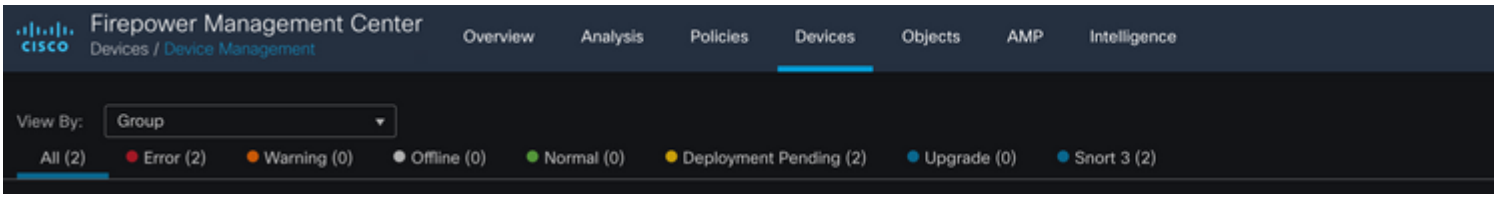
Schritt 12:

Wählen Sie **checkbox** für den BFD-Failover, und klicken Sie auf **OK** -Taste.



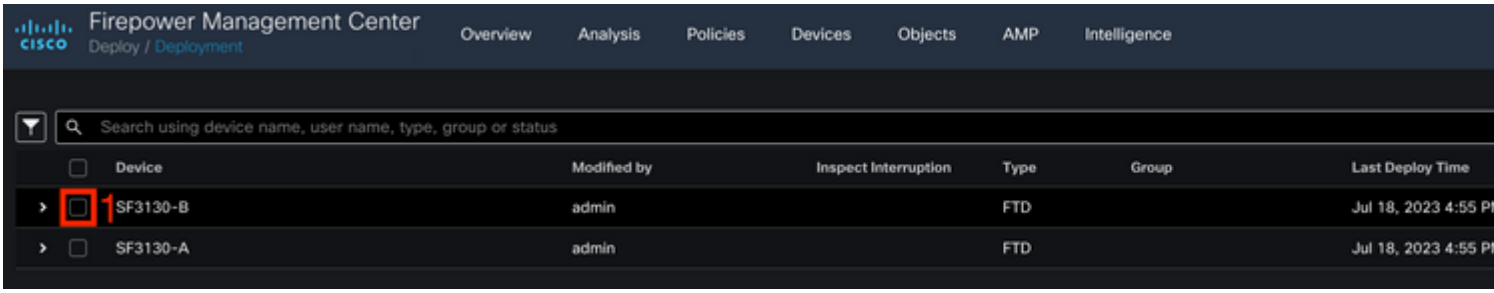
Schritt 13:

Klicken Sie auf **Deploy** klicken Sie auf die Schaltfläche **Deployment** -Taste.



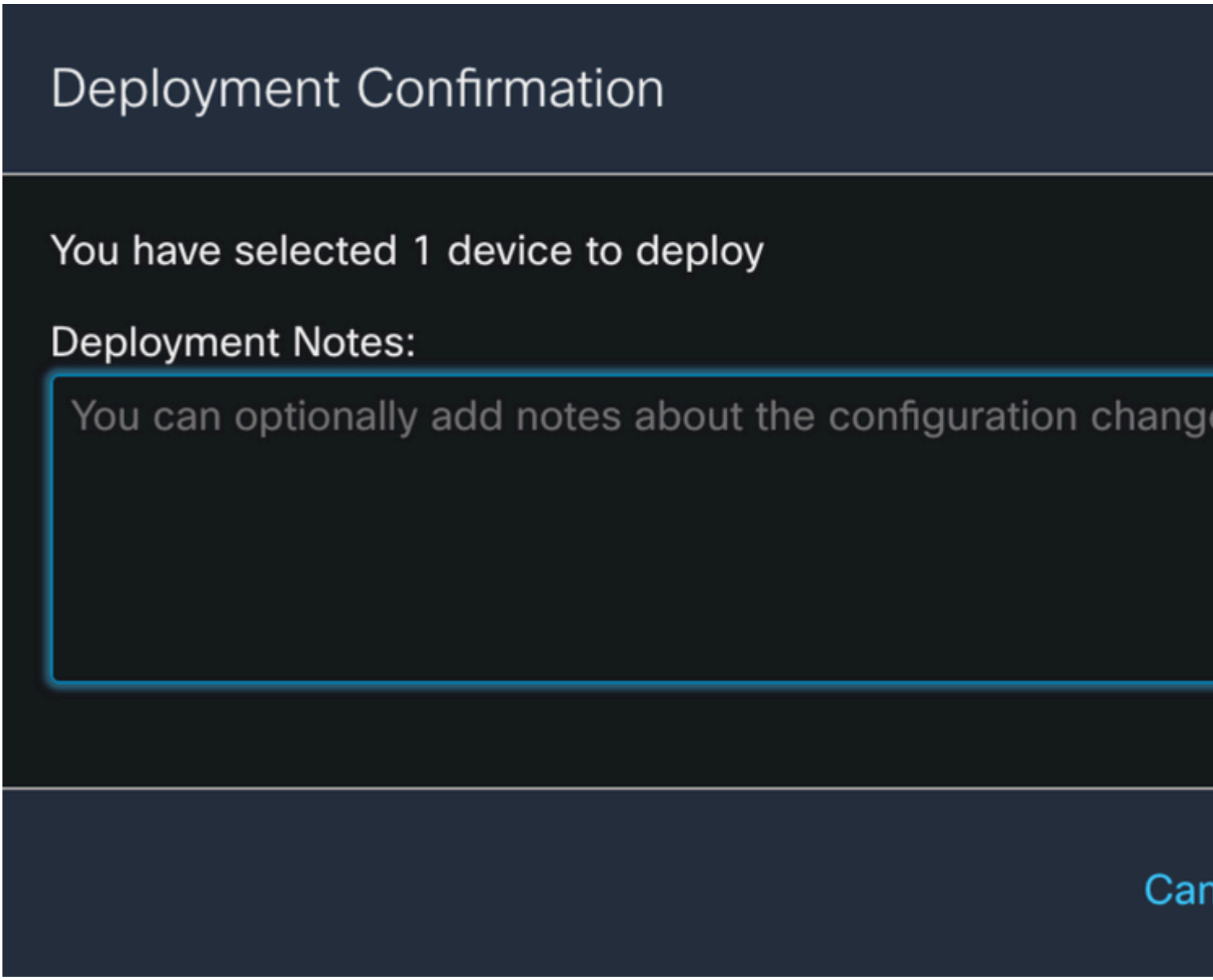
Schritt 14:

Wählen Sie das Gerät aus, dem die Änderungen zugewiesen werden sollen, indem Sie auf das **checkbox**, und klicken Sie dann auf**Deploy** -Taste.



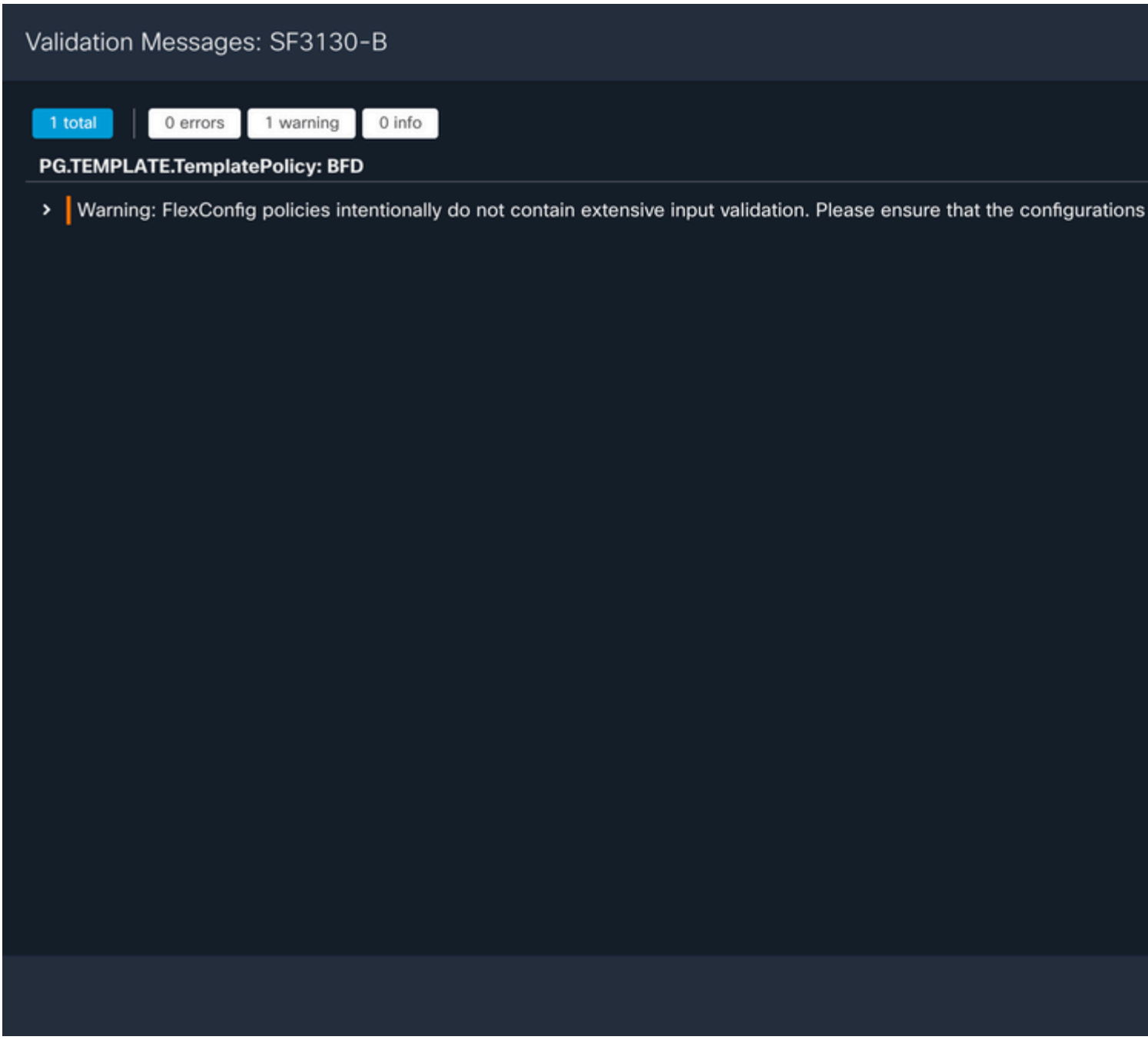
Schritt 15:

Klicken Sie auf **Deploy** -Taste.



Schritt 16:

Klicken Sie auf **Deploy** -Taste.



Hinweis: Die Warnung wird erwartet und ist nur informativ.

Überprüfung

Überprüfen Sie mit den nächsten Befehlen die BFD-Konfiguration und den Status direkt in der CLI-Sitzung.

<#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
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.