Déployer une interface de données redondante dans Azure FTD gérée par CD-FMC

Table des matières

Introduction

Ce document décrit les étapes pour configurer un FTD virtuel géré par cdFMC pour utiliser la fonctionnalité d'interface de données d'accès au gestionnaire redondant.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Firewall Management Center
- Cisco Defense Orchestrator

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Centre de gestion des pare-feu cloud
- Virtual Secure Firewall Threat Defense version 7.3.1 hébergé dans le cloud Azure.

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.

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Tout appareil physique capable d'exécuter Firepower Threat Defense version 7.3.0 ou ultérieure.

Informations générales

Ce document montre les étapes pour configurer et vérifier un vFTD géré par cdFMC pour utiliser deux interfaces de données à des fins de gestion. Cette fonctionnalité est souvent utile lorsque les clients ont besoin d'une seconde interface de données pour gérer leur FTD sur Internet, à l'aide d'un second FAI. Par défaut, le FTD effectue un équilibrage de charge par permutation circulaire pour le trafic de gestion entre les deux interfaces ; il peut être modifié en déploiement actif/sauvegarde comme décrit dans ce document.

La fonctionnalité d'interface de données redondante pour la gestion a été introduite dans la version 7.3.0 de Secure Firewall Threat Defense. On suppose que le vFTD est accessible à un serveur de noms qui peut résoudre les URL pour l'accès CDO.

Configuration

Diagramme du réseau

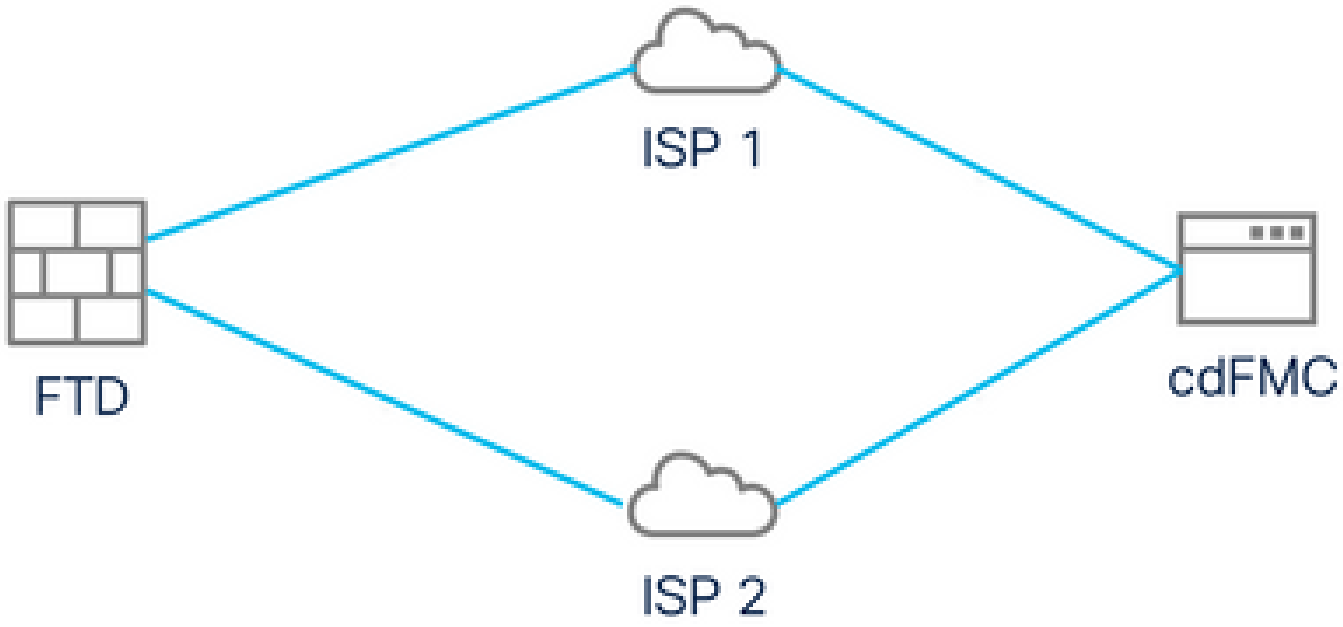


Diagramme du réseau

Configurer une interface de données pour l'accès à la gestion

Connectez-vous au périphérique via la console et configurez l'une des interfaces de données pour l'accès à la gestion avec la commande configure network management-data-interface :

<#root>

>

configure network management-data-interface

**Note: The Management default route will be changed to route through the data interfaces. If you are conn
interface with SSH, your connection may drop. You must reconnect using the console port.**

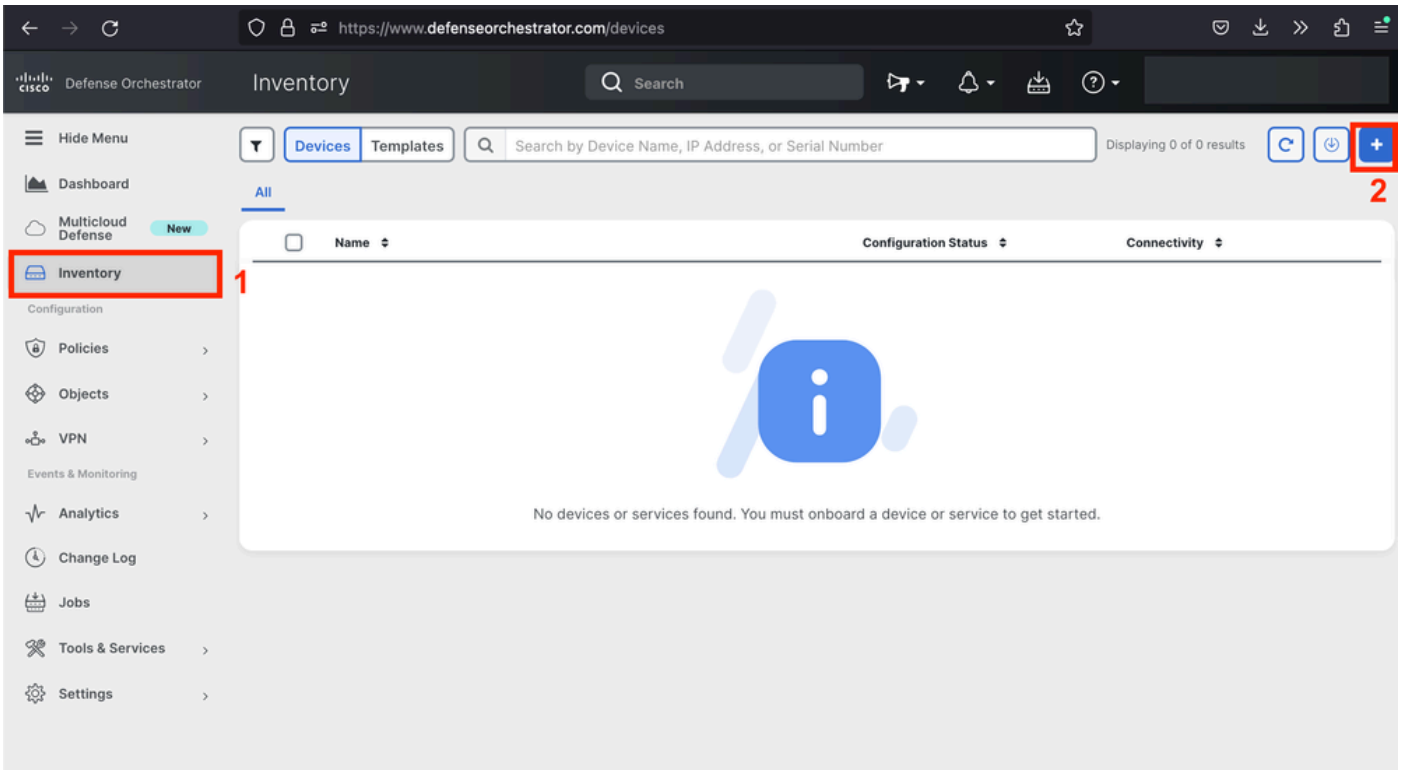
```
Data interface to use for management:

GigabitEthernet0/0

Specify a name for the interface [outside]:

outside-1

IP address (manual / dhcp) [dhcp]:

manual

IPv4/IPv6 address:

10.6.2.4

Netmask/IPv6 Prefix:

 255.255.255.0

Default Gateway:

10.6.2.1
```

Gardez à l'esprit que l'interface de gestion d'origine ne peut pas être configurée pour utiliser DHCP. Vous pouvez utiliser la commande show network pour vérifier ceci.

Intégration du FTD avec CDO

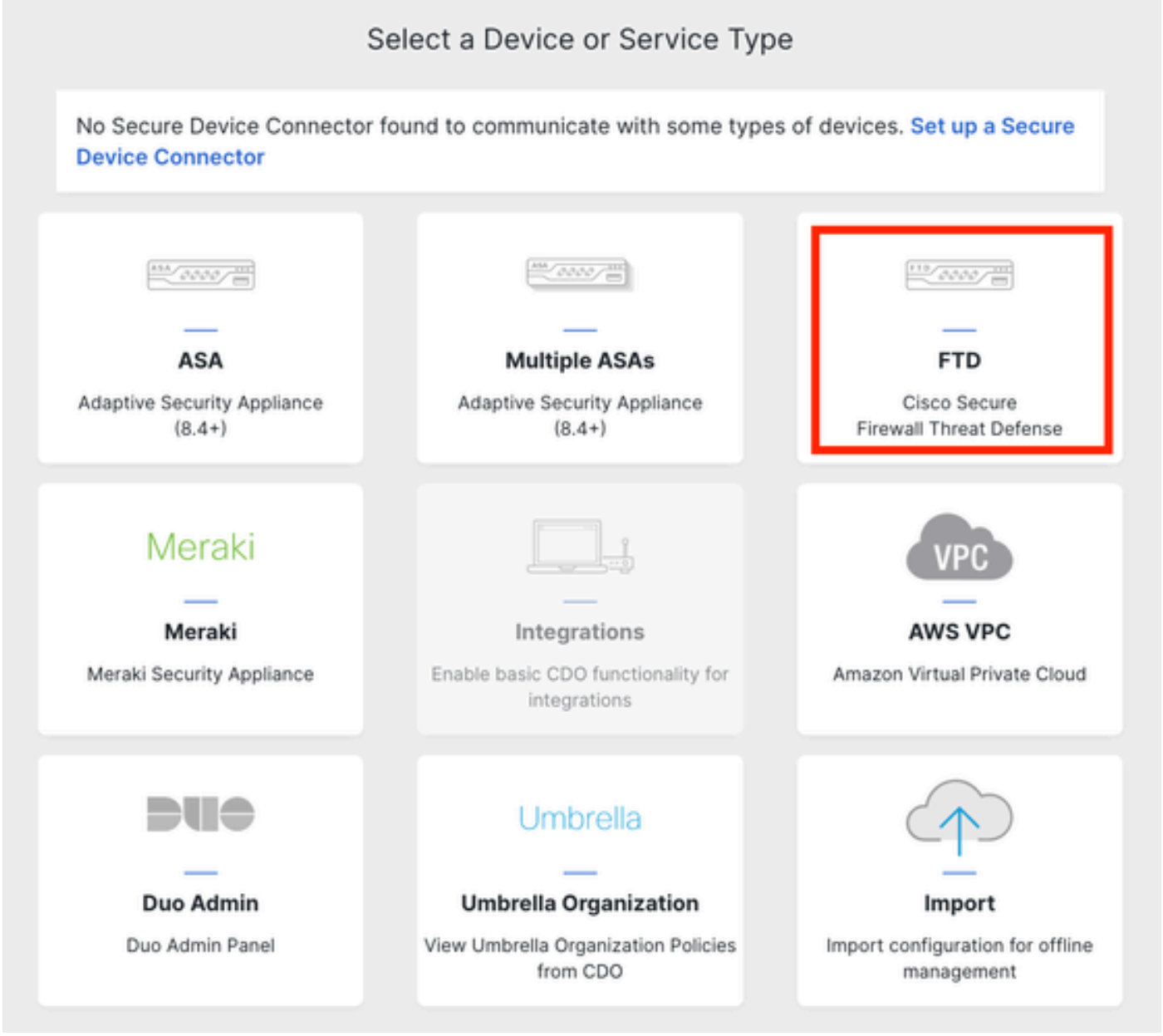
Ce processus est intégré au FTD Azure avec CDO afin qu'il puisse être géré par un FMC fourni dans le cloud. Le processus utilise une clé d'enregistrement CLI, ce qui est utile si votre périphérique dispose d'une adresse IP attribuée via DHCP. Les autres méthodes d'intégration, telles que la mise en service log-touch et le numéro de série, sont uniquement prises en charge sur les plates-formes Firepower 1000, Firepower 2100 ou Secure Firewall 3100.

Étape 1. Dans le portail CDO, naviguez jusqu'à Inventory et cliquez ensuite sur Onboard option :



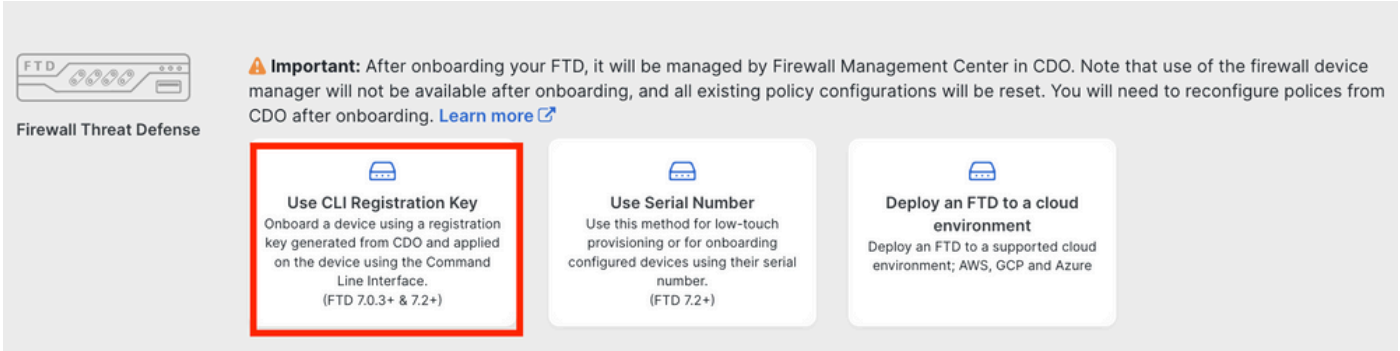
Page Inventaire

Étape 2. Cliquez sur la vignette FTD :



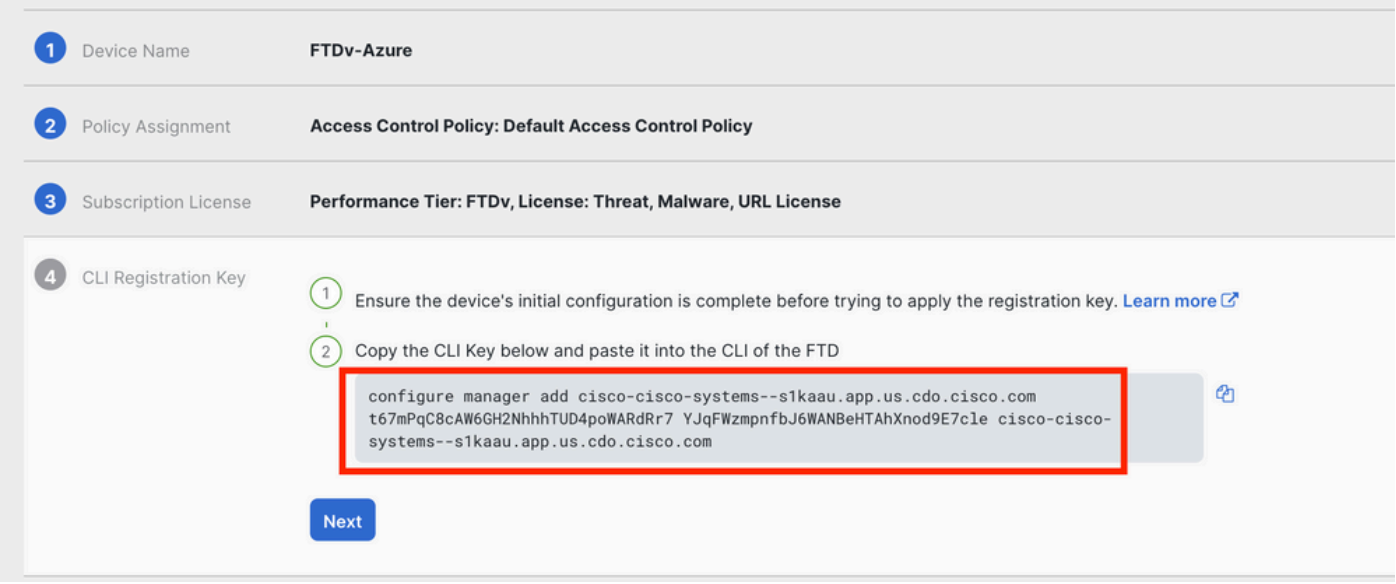
Intégration du FTD

Étape 3. Choisissez l'option Utiliser la clé d'enregistrement CLI :

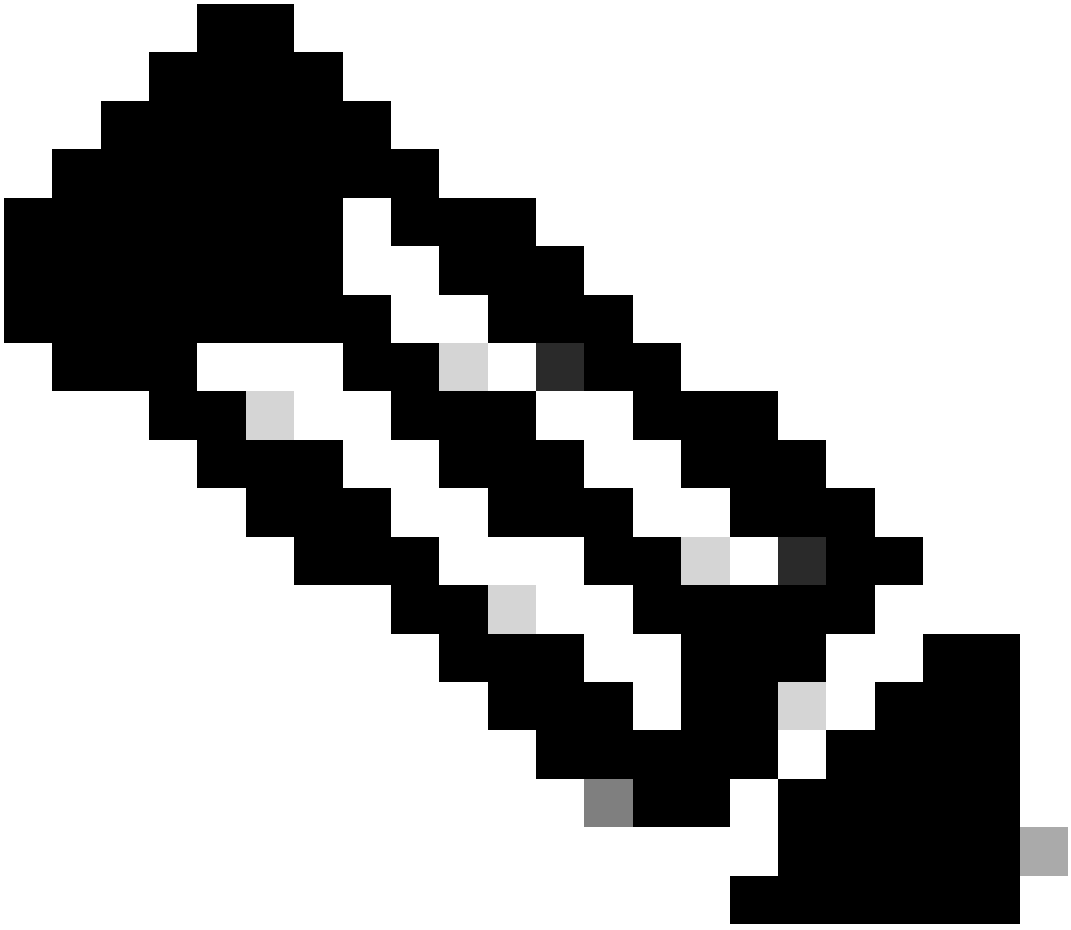


Utiliser la clé d'enregistrement CLI

Étape 4. Copiez la clé CLI à partir de la commande configure manager :



Copier la commande Configure Manager



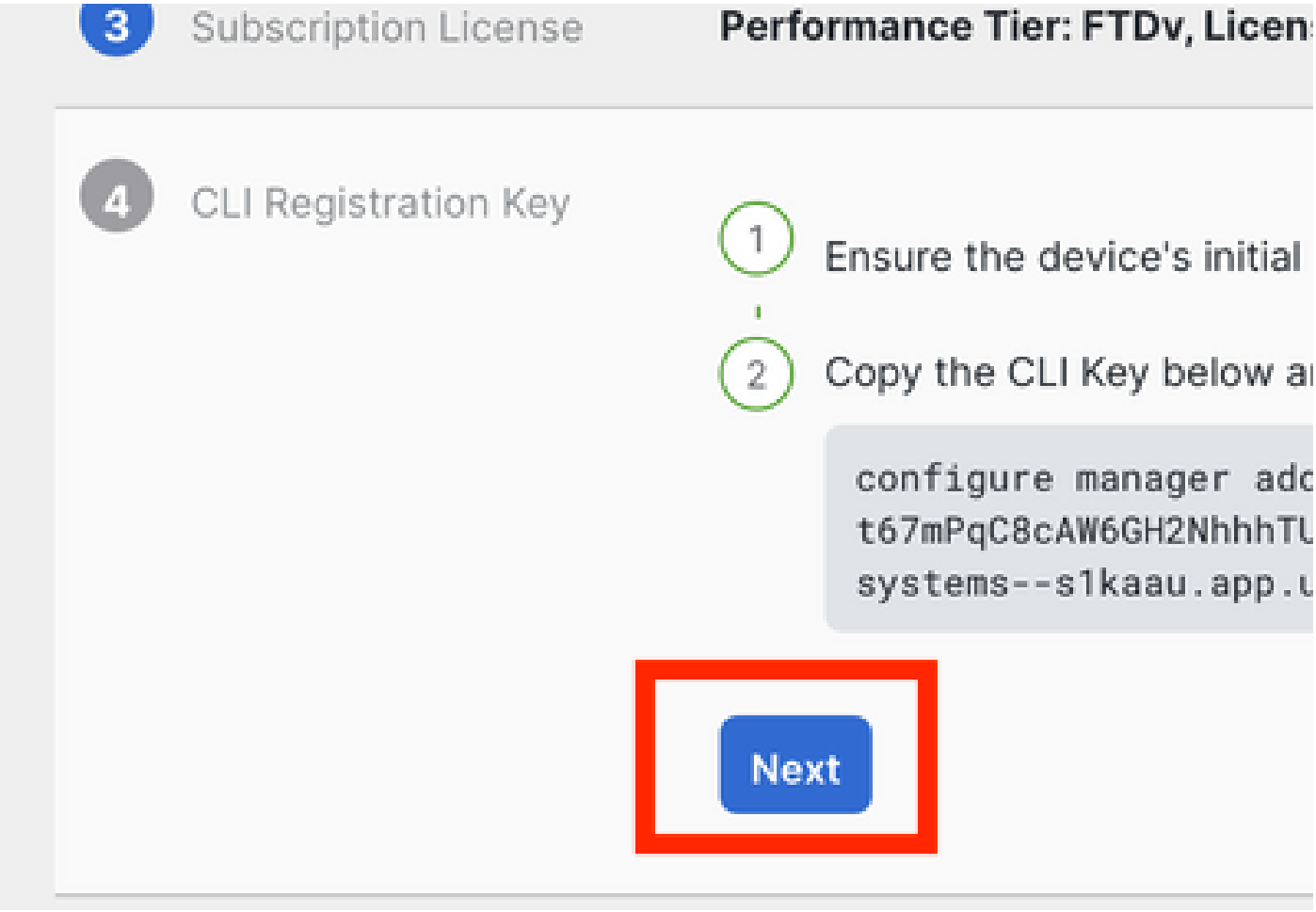
Remarque : la clé CLI correspond au format utilisé dans les enregistrements de FTD avec

les FMC sur site, où vous pouvez configurer un NAT-ID pour autoriser l'enregistrement lorsque votre périphérique géré est derrière un périphérique NAT : configure manager add <fmc-hostname-or-ipv4> <registration-key> <nat-id> <display-name>

Étape 5. Collez la commande dans l'interface de ligne de commande FTD. Vous devez recevoir ce message si la communication a réussi :

```
Manager cisco-cisco-systems--s1kaau.app.us.cdo.cisco.com successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

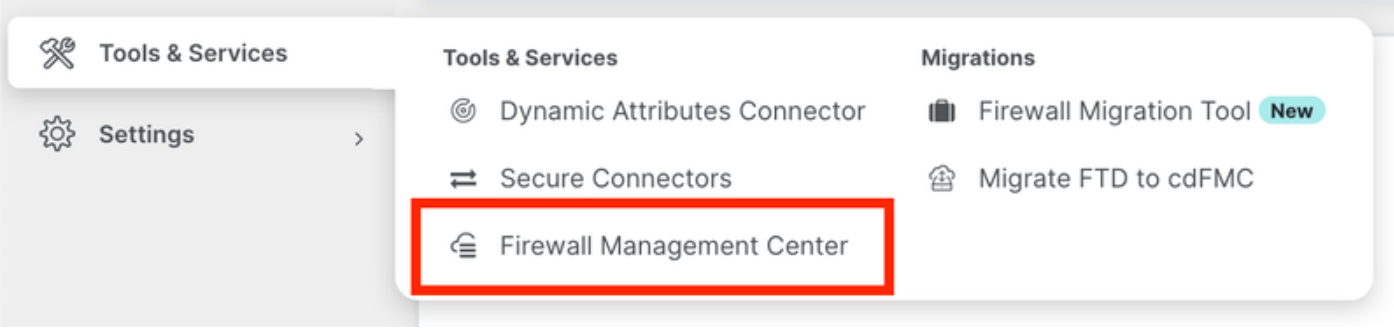
Étape 6. Retournez à l'outil CDO et cliquez sur Next :



Cliquez sur Next (suivant).

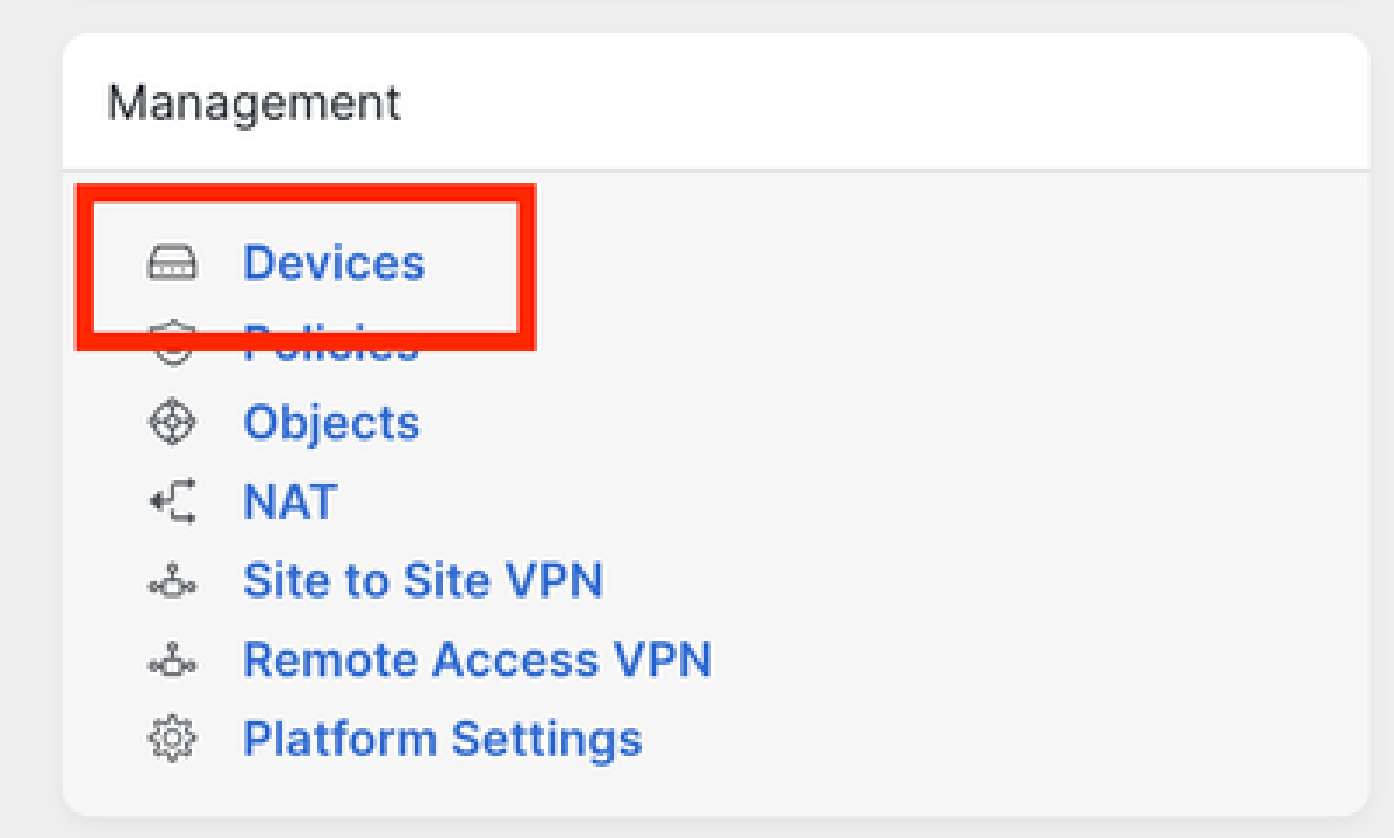
CDO poursuit le processus d'inscription et un message s'affiche indiquant que le processus va prendre beaucoup de temps. Vous pouvez vérifier l'état du processus d'inscription en cliquant sur le lien Périphériques dans la page Services.

Étape 7. Accédez à votre FMC via la page Outils et services.



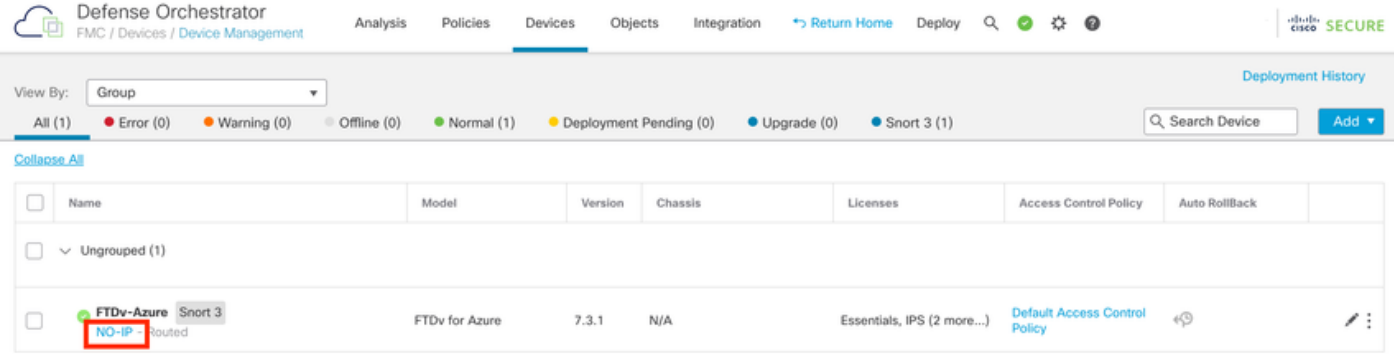
Accès au cdFMC

Cliquez sur le lien Périphériques.



Cliquez sur Périphériques

Votre FTD est désormais intégré dans CDO et peut être géré par le FMC fourni dans le cloud. Notez dans l'image suivante qu'une adresse IP non autorisée est répertoriée sous le nom du périphérique. Ceci est prévu dans un processus d'intégration utilisant la clé d'enregistrement CLI.

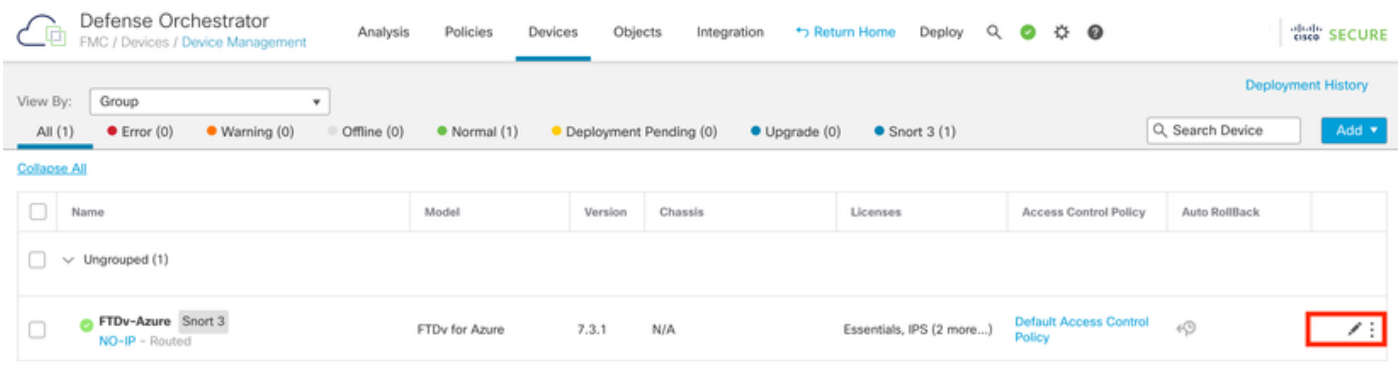


FTD géré

Configurer une interface de données redondante pour l'accès au gestionnaire

Ce processus attribue une deuxième interface de données pour l'accès à la gestion.

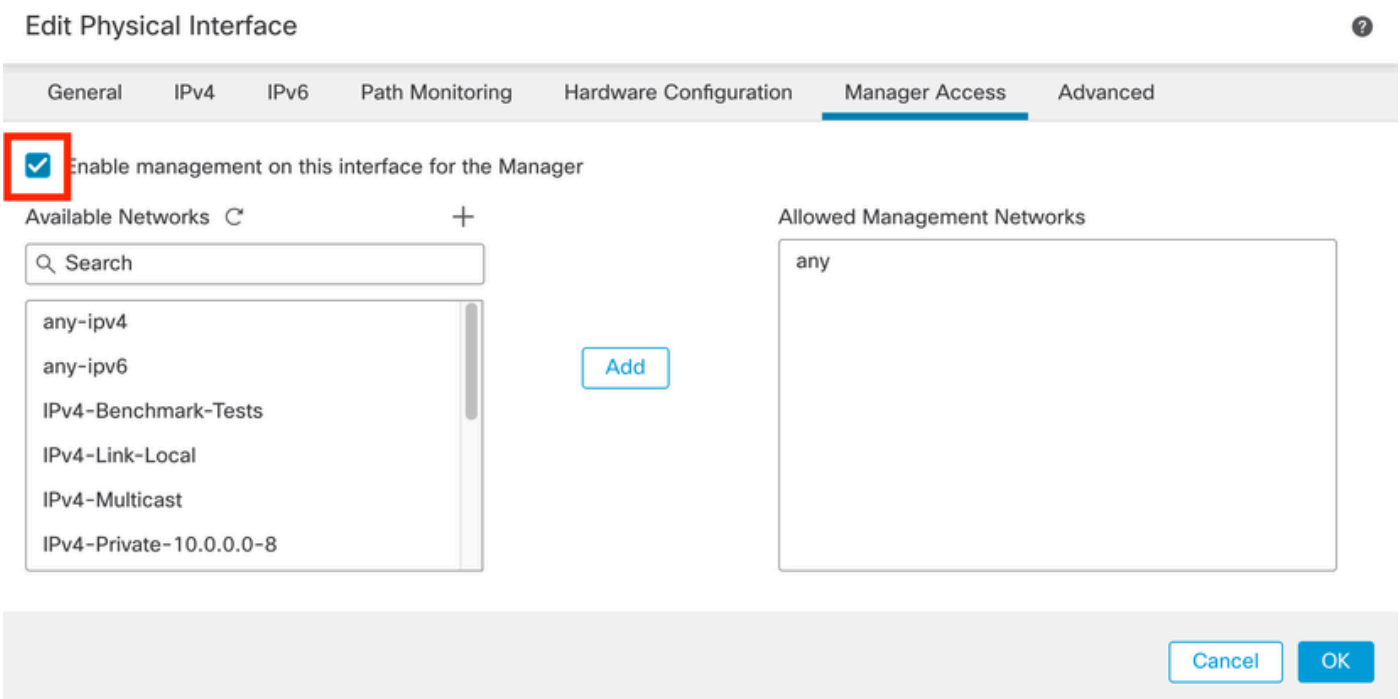
Étape 1. Dans l'onglet Devices, cliquez sur l'icône du crayon pour accéder au mode d'édition FTD :



Modifier le FTD

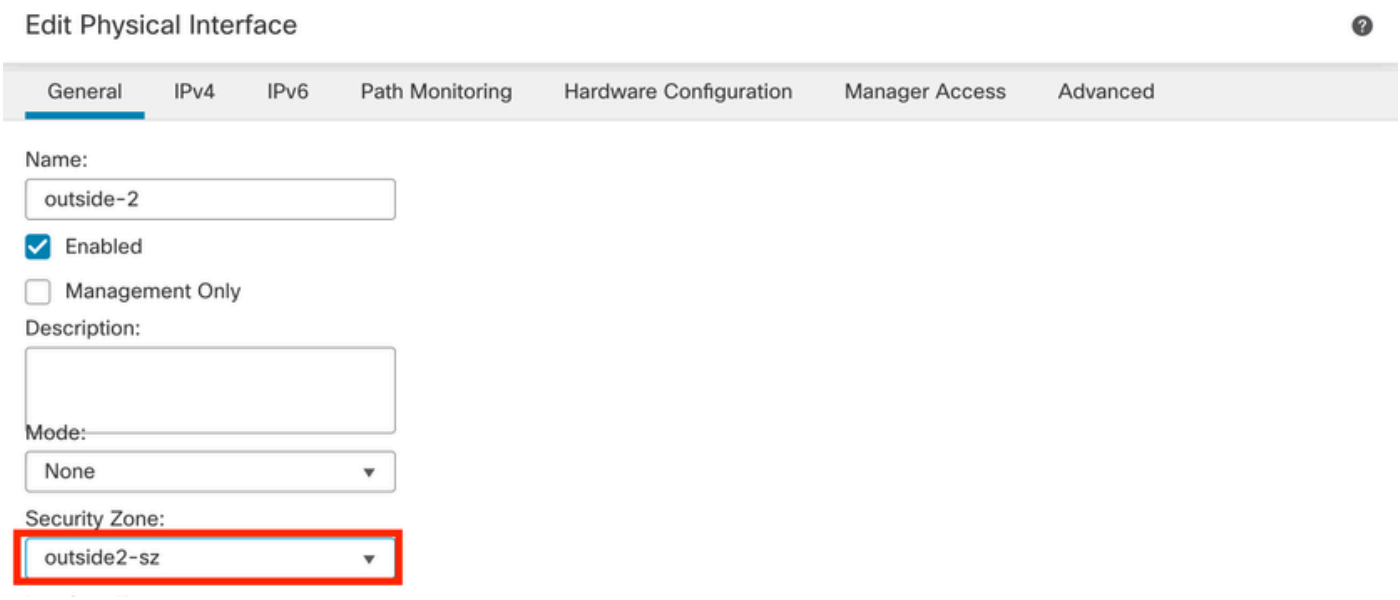
Étape 2. Dans l'onglet Interface, modifiez l'interface qui va être attribuée comme interface de gestion redondante. Si cela n'a pas été fait précédemment, configurez un nom d'interface et une adresse IP.

Étape 3. Dans l'onglet Accès au manager activez la case à cocher Activer la gestion sur cette interface pour le manager :



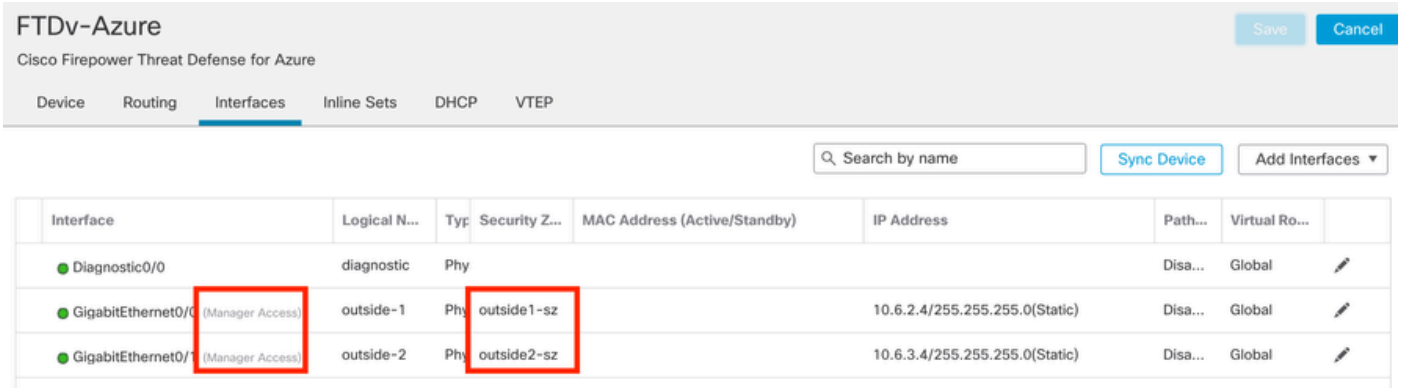
Activation de l'accès Manager

Étape 4. Dans l'onglet General, vérifiez que l'interface est affectée à une zone de sécurité et cliquez sur OK :



Zone de sécurité pour interface de données redondante

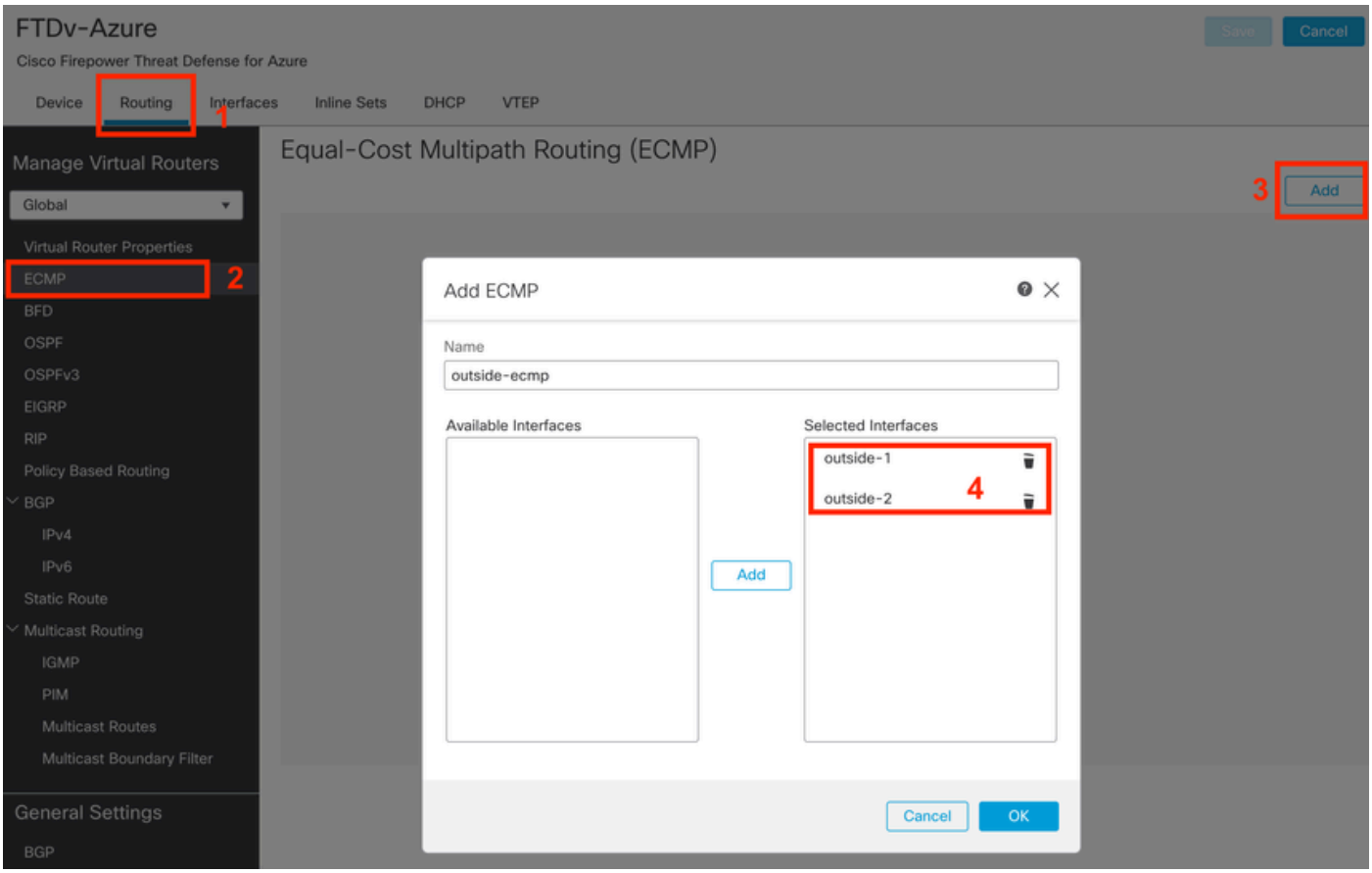
Étape 5. Notez que maintenant les deux interfaces ont la balise Manager Access. Assurez-vous également que l'interface de données principale a été attribuée à une autre zone de sécurité :



Révision de la configuration des interfaces

Dans la section suivante, les étapes 6 à 10 visent à configurer deux routes par défaut à coût égal pour atteindre le CDO, chacune étant surveillée par un processus de suivi SLA indépendant. Le suivi SLA garantit qu'il existe un chemin fonctionnel pour communiquer avec le cdFMC à l'aide de l'interface surveillée.

Étape 6. Accédez à l'onglet Routing et sous le menu ECMP créez une nouvelle zone ECMP avec les deux interfaces dans celle-ci :

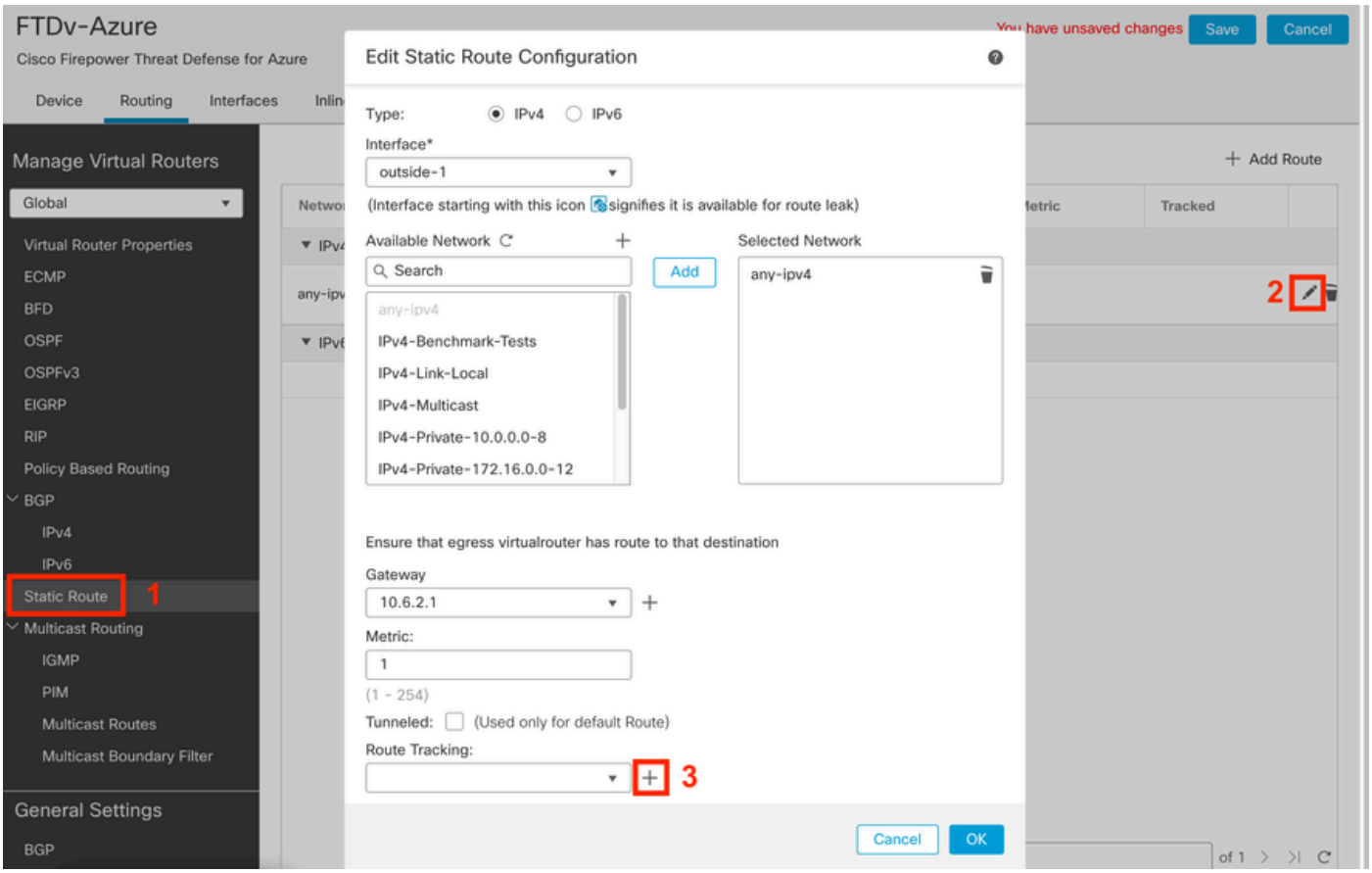


Configurer une zone ECMP

Cliquez sur OK et sur Save.

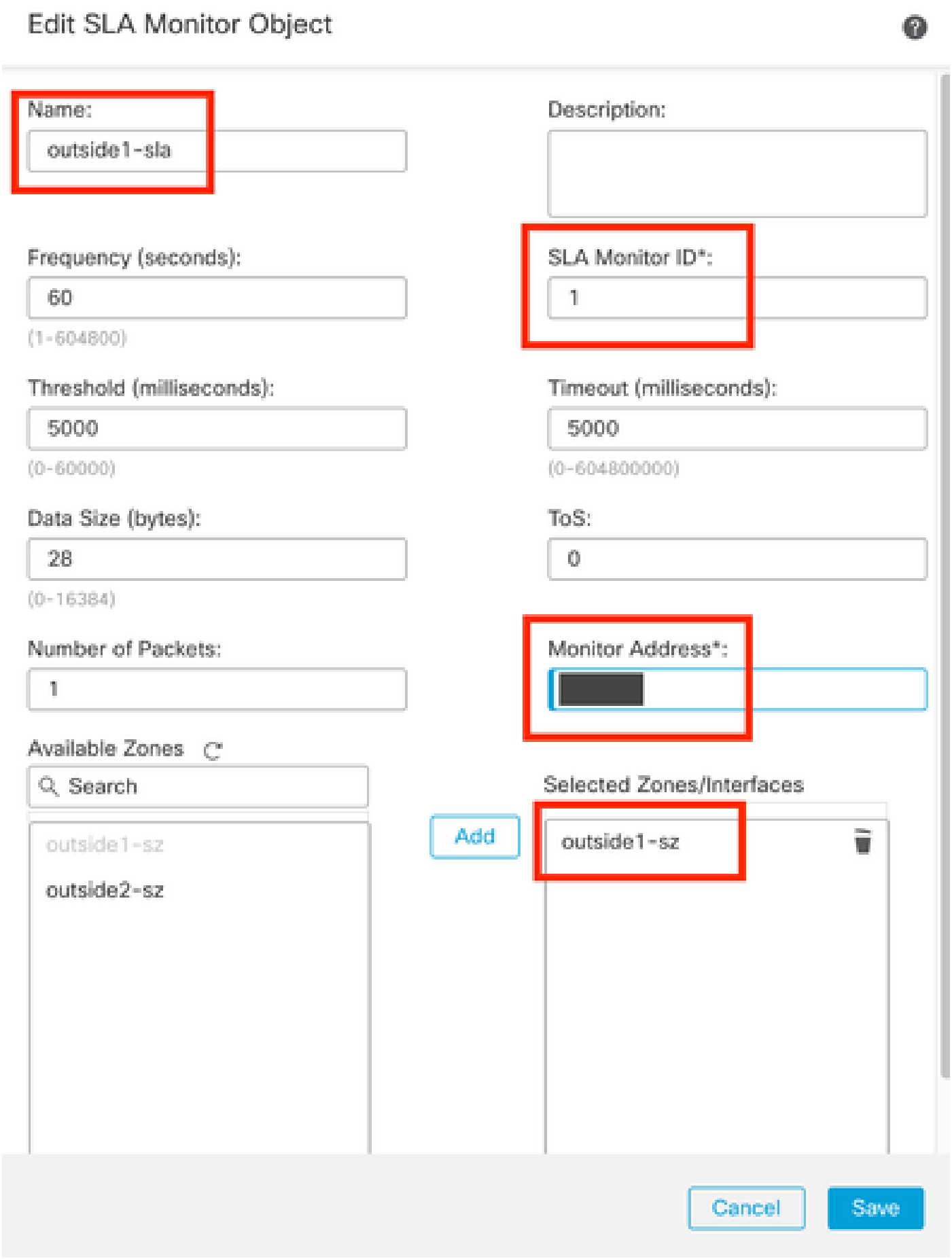
Étape 7. Dans l'onglet Routing, accédez à Static Routes.

Cliquez sur l'icône représentant un crayon pour modifier votre route principale. Cliquez ensuite sur le signe plus pour ajouter un nouvel objet de suivi SLA :



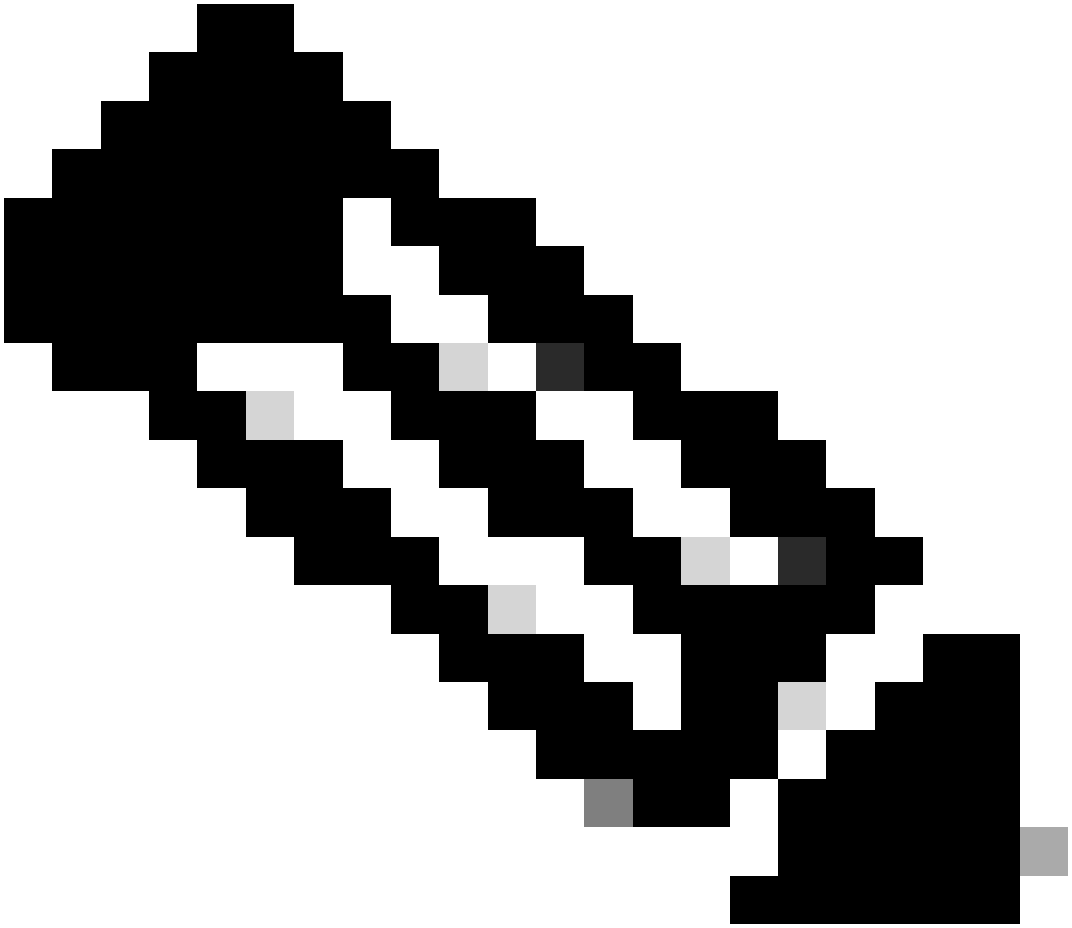
Modifier la route principale pour ajouter le suivi SLA

Étape 8. Les paramètres requis pour un suivi SLA fonctionnel sont mis en surbrillance dans l'image suivante. Vous pouvez éventuellement régler d'autres paramètres tels que Nombre de paquets, Délai d'attente et Fréquence.



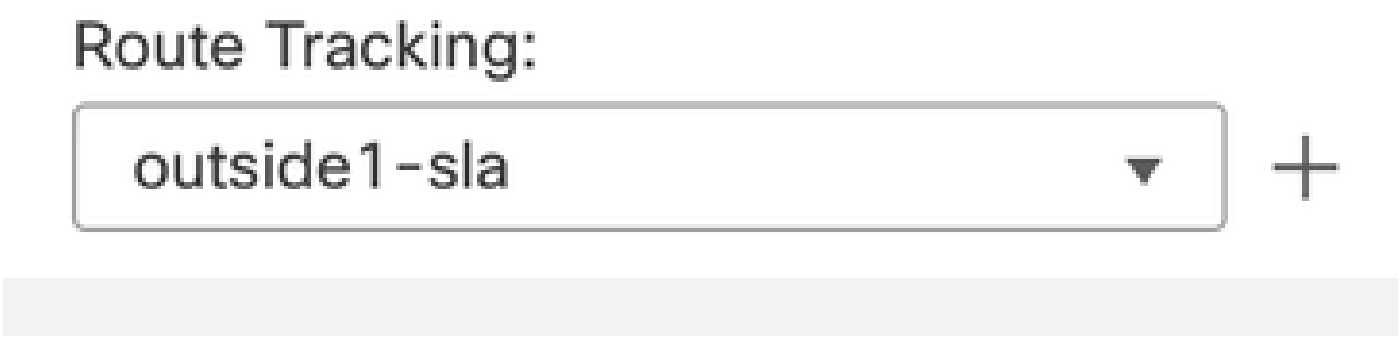
Configurer le suivi SLA pour ISP 1

Dans cet exemple, Google DNS IP a été utilisé pour surveiller les capacités FTD pour atteindre Internet (et CDO) via l'interface outside1. Cliquez sur ok quand vous êtes prêt.



> Remarque : assurez-vous que vous suivez une adresse IP qui a déjà été vérifiée comme accessible depuis votre interface externe FTD. La configuration d'une piste avec une adresse IP inaccessible peut faire baisser la route par défaut dans ce FTD, puis empêcher sa capacité à communiquer avec CDO.

Étape 9. Cliquez sur Save et assurez-vous que le nouveau suivi SLA est attribué à la route pointant vers l'interface principale :

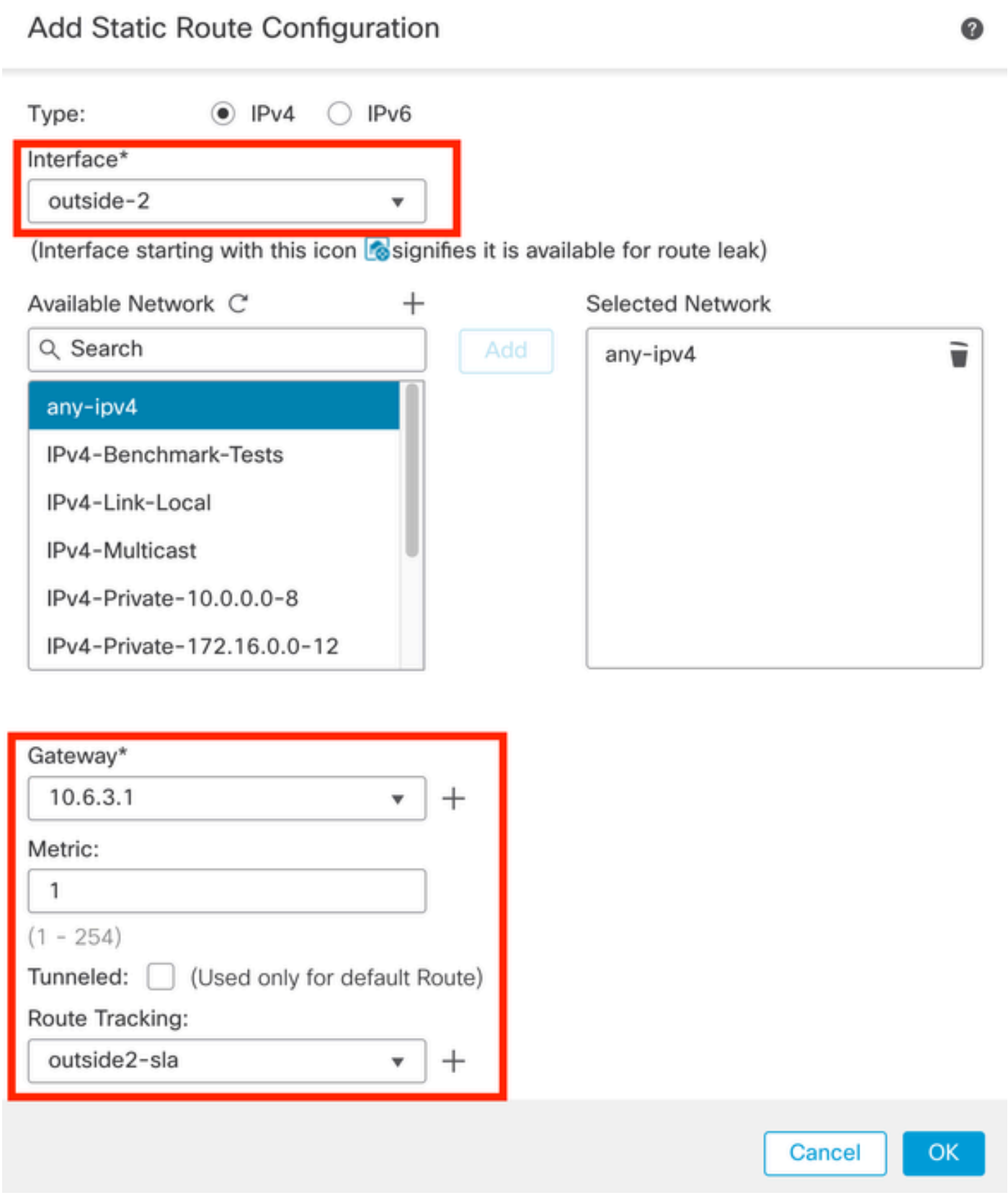


Suivi 1 SLA externe

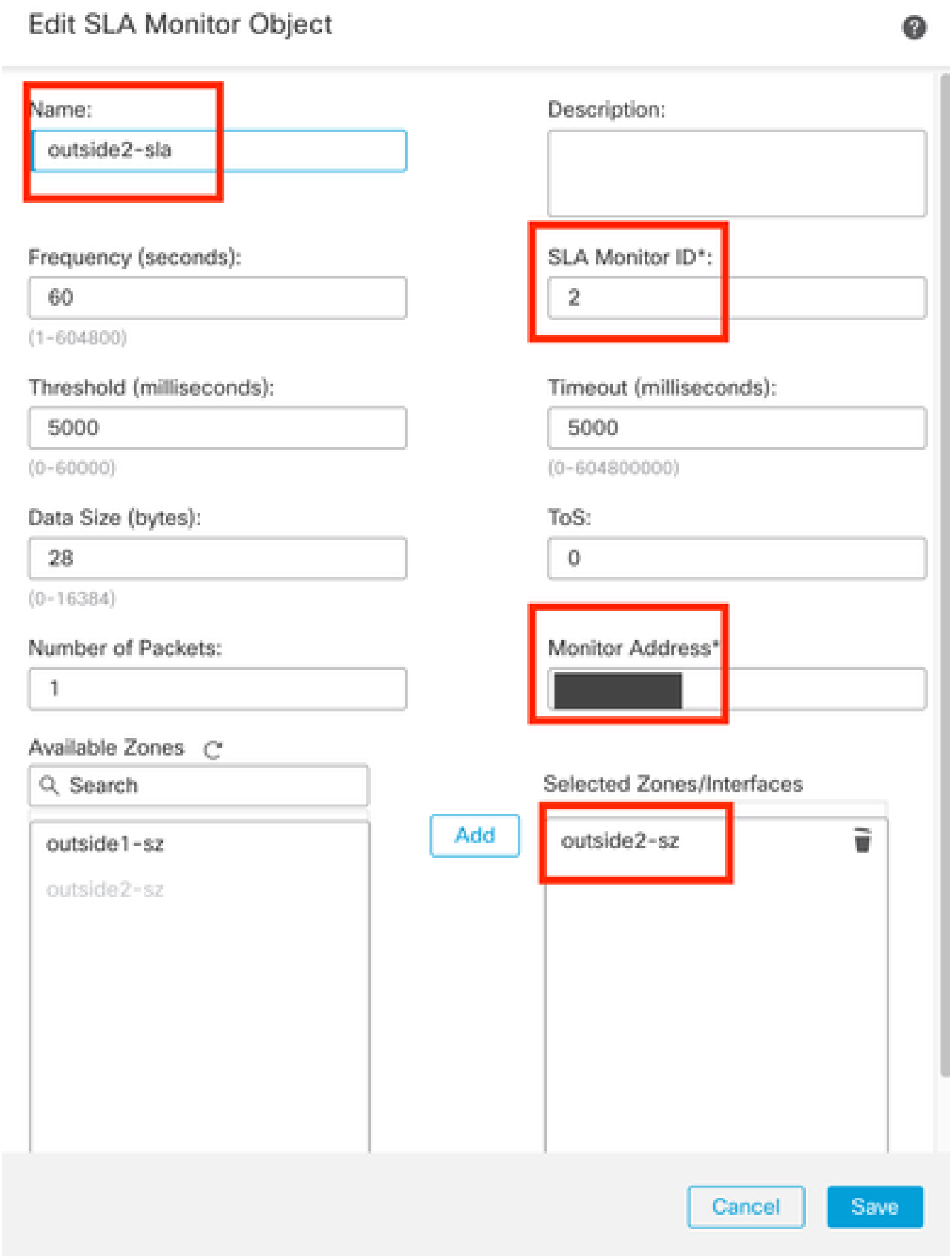
Une fois que vous cliquez sur OK, une fenêtre contextuelle s'affiche avec le message d'AVERTISSEMENT suivant :

Avertissement de configuration

Étape 10. Cliquez sur Add Route option pour ajouter une nouvelle route pour l'interface de données redondante. Notez dans l'image suivante que la valeur Metric pour la route est la même ; en outre, le suivi SLA a un ID différent :



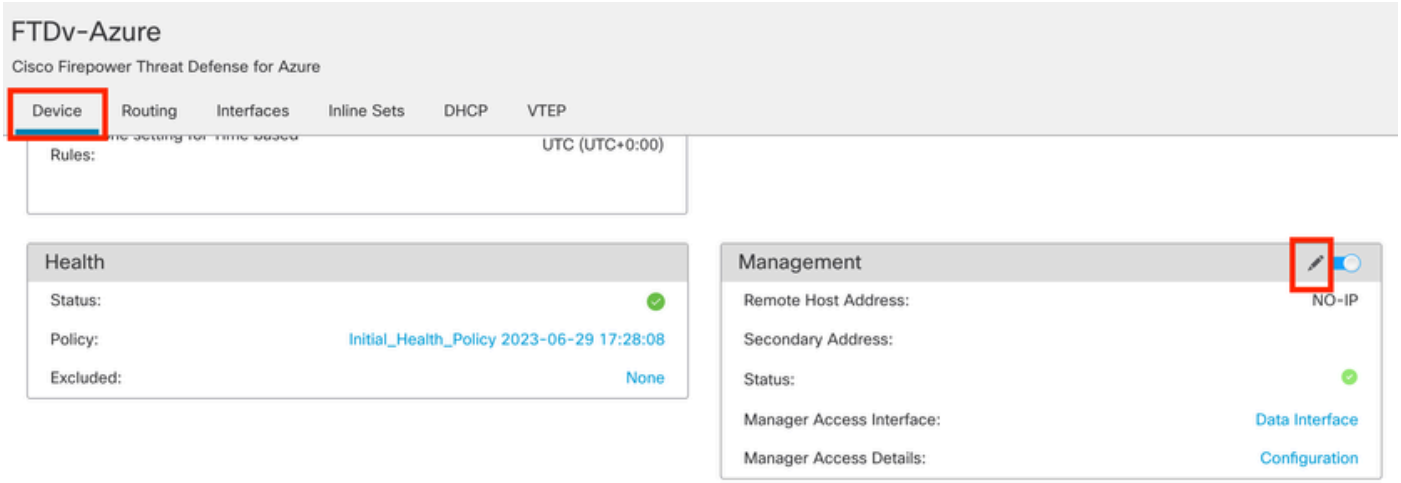
Configuration de la route statique redondante



Configurer le suivi pour l'interface de données redondante

Cliquez sur Save.

Étape 11. Vous pouvez éventuellement spécifier l'adresse IP de l'interface de données secondaire sous Device > Management. Toutefois, cette opération n'est pas obligatoire, car la méthode d'intégration actuelle utilise le processus de clé d'enregistrement CLI :



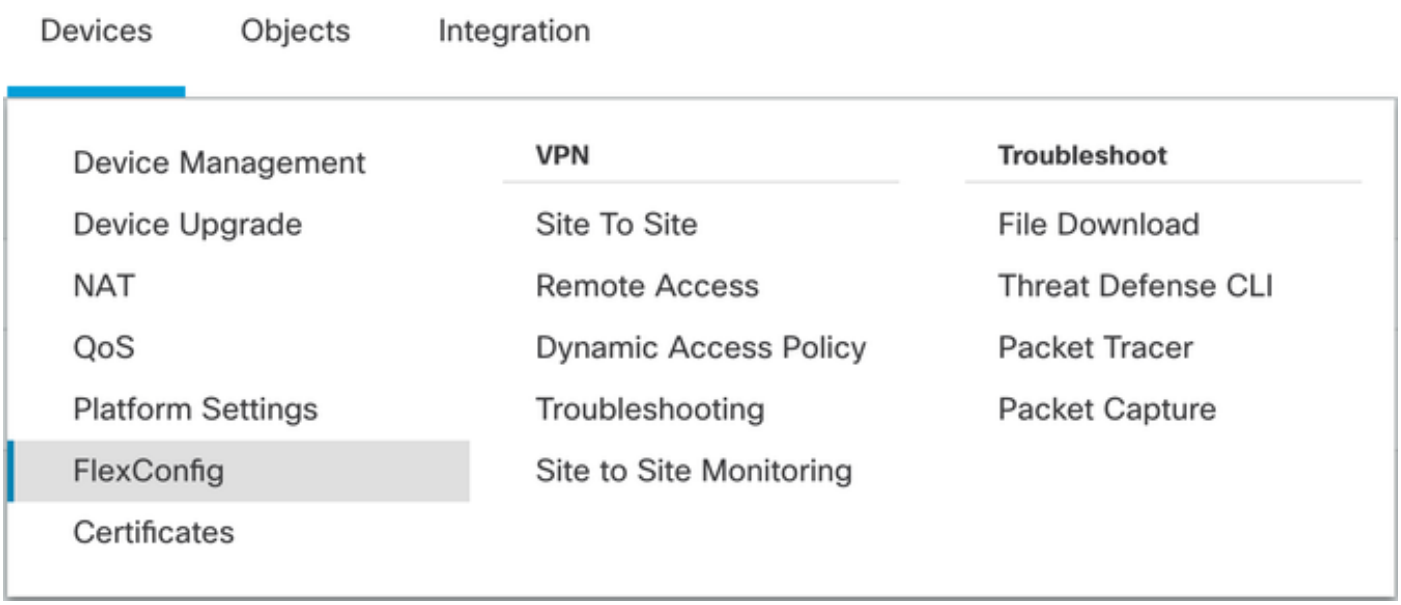
(Facultatif) Spécifiez une adresse IP pour l'interface de données redondante dans le champ Management

Étape 12. Déployez les modifications.

(Facultatif) Définissez un coût d'interface pour un mode d'interface actif/de sauvegarde :

Par défaut, la gestion redondante sur l'interface de données utilise le round robin pour distribuer le trafic de gestion entre les deux interfaces. Par ailleurs, si une liaison WAN a une bande passante plus élevée que l'autre et que vous préférez qu'elle soit la liaison de gestion principale alors que l'autre reste en tant que liaison de secours, vous pouvez attribuer à la liaison principale un coût de 1 et à la liaison de secours un coût de 2. Dans l'exemple suivant, l'interface GigabitEthernet0/0 est conservée en tant que liaison WAN principale tandis que GigabitEthernet0/1 sert de liaison de gestion de sauvegarde :

1. Accédez au lien Devices > FlexConfig et créez une stratégie flexConfig. Si une stratégie flexConfig est déjà configurée et attribuée à votre FTD, modifiez-la :

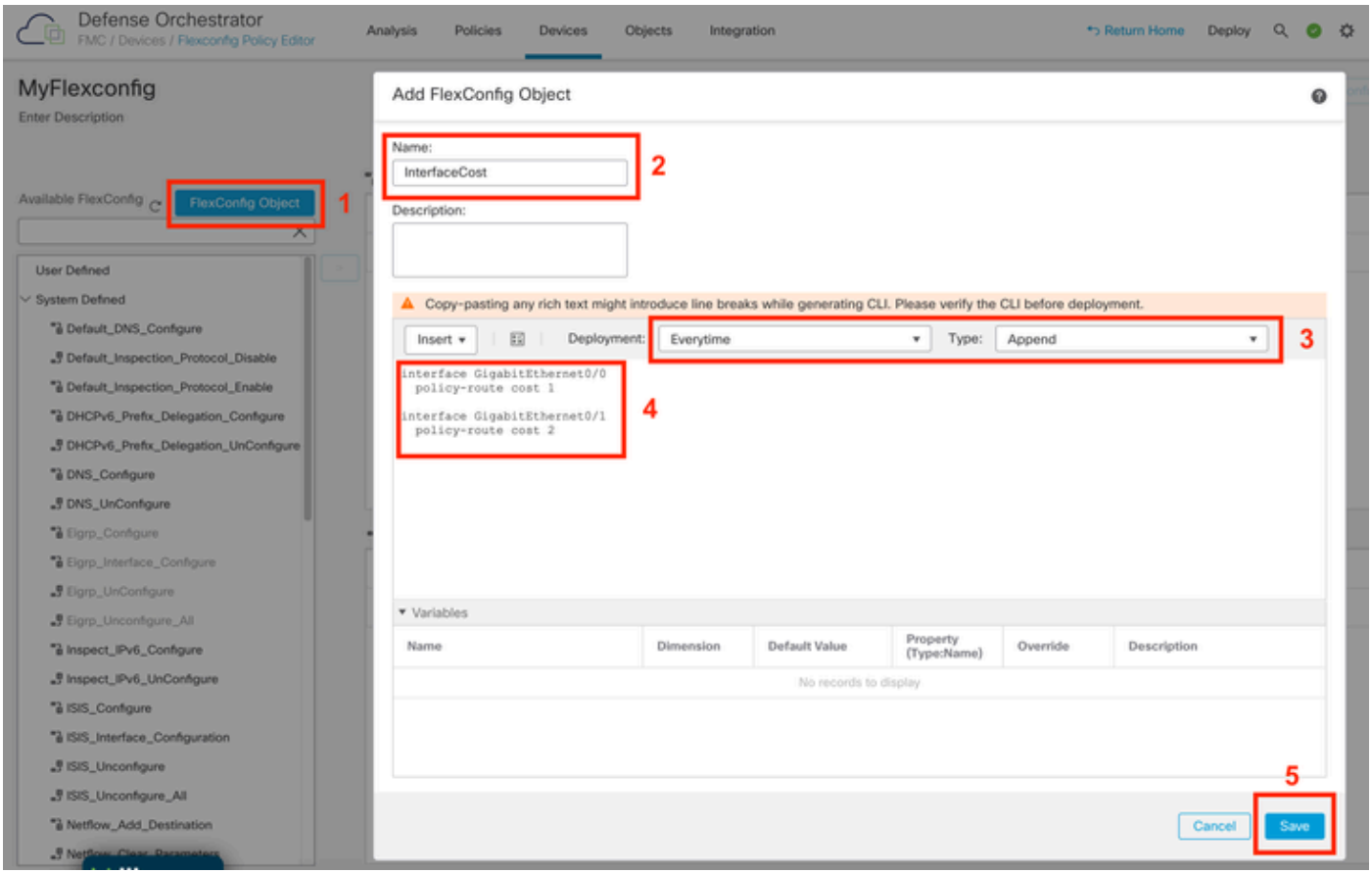


Accès au menu FlexConfig

2. Créez un nouvel objet FlexConfig :

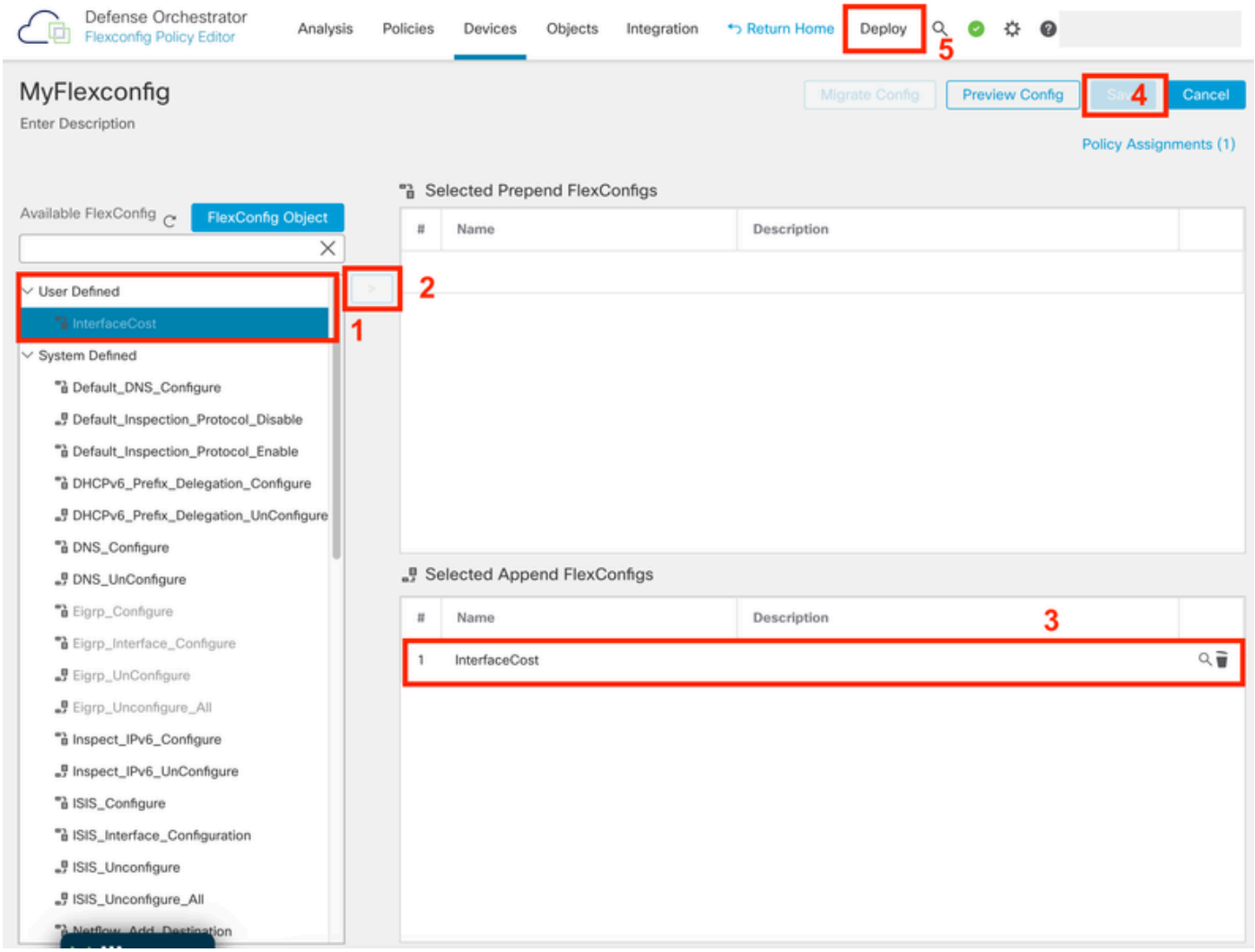
- Attribuez un nom à l'objet FlexConfig.
- Choisissez Everytime et Append respectivement dans les sections Deployment et Type.
- Définissez le coût des interfaces à l’aide des commandes suivantes, comme illustré dans l’image 22.
- Cliquez sur Save.

```
<#root>
interface GigabitEthernet0/0

  policy-route cost 1

<=== A cost of 1 means this will be the primary interface for management communication with CDO tenant.
interface GigabitEthernet0/1

  policy-route cost 2

<=== Cost 2 sets this interface as a backup interface.
```



Ajout d'un objet Flexconfig

3. Choisissez l'objet récemment créé et ajoutez-le à la section Selected Append FlexConfigs comme illustré dans l'image. Enregistrez les modifications et déployez votre configuration.



Affectation de l'objet à la stratégie Flexconfig

4. Déployez les modifications.

Vérifier

1. Pour vérifier, utilisez la commande show network. Une nouvelle instance de l'interface de gestion redondante est formée :

```
> show network

<<---------- output omitted for brevity ---------->>

======================[ eth0 ]======================
State : Enabled
Link : Up
Channels : Management & Events
Mode : Non-Autonegotiation
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 60:45:BD:D8:62:D7
----------------------[ IPv4 ]----------------------
Configuration : Manual
```

```
Address : 10.6.0.4
Netmask : 255.255.255.0
----------------------[ IPv6 ]----------------------
Configuration : Disabled

================[ Proxy Information ]================
State : Disabled
Authentication : Disabled
. . .

===============[ GigabitEthernet0/0 ]===============
State : Enabled
Link : Up
Name : outside-1
MTU : 1500
MAC Address : 60:45:BD:D8:6F:5C
----------------------[ IPv4 ]----------------------
Configuration : Manual
Address : 10.6.2.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
----------------------[ IPv6 ]----------------------
Configuration : Disabled

===============[ GigabitEthernet0/1 ]===============
State : Enabled
Link : Up
Name : outside-2
MTU : 1500
MAC Address : 60:45:BD:D8:67:CA
----------------------[ IPv4 ]----------------------
Configuration : Manual
Address : 10.6.3.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
----------------------[ IPv6 ]----------------------
Configuration : Disabled
```

2. L'interface fait maintenant partie du domaine sftunnel. Vous pouvez le confirmer avec les commandes show sftunnel interfaces et show running-config sftunnel :

<#root>

```
>

show sftunnel interfaces


Physical Interface Name of the Interface
GigabitEthernet0/0 outside-1
GigabitEthernet0/1 outside-2

>

show running-config sftunnel


sftunnel interface outside-2
sftunnel interface outside-1
```

```
sftunnel port 8305
sftunnel route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346
```

3. Une route basée sur des règles est automatiquement définie. Si vous n'avez pas spécifié de coût d'interface, l'option adaptive-interface définit le traitement round robin pour équilibrer la charge du trafic de gestion entre les deux interfaces :

```
<#root>

>

show running-config route-map


!
route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346 permit 5
 match ip address FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392
 set adaptive-interface cost outside-1 outside-2

>

show access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392


access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392; 1 elements; name hash: 0x8e8cb508
access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392 line 1 extended permit tcp any any eq 8305 (hi
```

4. Utilisez la commande show running-config interface <interface> pour vérifier les paramètres d'interface :

```
<#root>

>

 show running-config interface GigabitEthernet 0/0


!
interface GigabitEthernet0/0
nameif outside-1
security-level 0
zone-member outside-ecmp
ip address 10.6.2.4 255.255.255.0
policy-route cost 1

>

show running-config interface GigabitEthernet 0/1


!
interface GigabitEthernet0/1
nameif outside-2
security-level 0
zone-member outside-ecmp
ip address 10.6.3.4 255.255.255.0
```

```
policy-route cost 2
```

Certaines commandes supplémentaires peuvent être utilisées pour vérifier le suivi des routes configurées :

```
<#root>

>

show track


Track 1
Response Time Reporter 2 reachability
Reachability is Up                    <============== Ensure reachability is up for the monitored interf
2 changes, last change 09:45:00
Latest operation return code: OK
Latest RTT (millisecs) 10
Tracked by:
STATIC-IP-ROUTING 0
Track 2
Response Time Reporter 1 reachability
Reachability is Up                    <============== Ensure reachability is up for the monitored interf
2 changes, last change 09:45:00
Latest operation return code: OK
Latest RTT (millisecs) 1
Tracked by:
STATIC-IP-ROUTING 0


>

show route



Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.6.3.1 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.6.3.1, outside-2
                   [1/0] via 10.6.2.1, outside-1
C 10.6.2.0 255.255.255.0 is directly connected, outside-1
L 10.6.2.4 255.255.255.255 is directly connected, outside-1
C 10.6.3.0 255.255.255.0 is directly connected, outside-2
L 10.6.3.4 255.255.255.255 is directly connected, outside-2
```

Informations connexes

- Assistance technique de Cisco et téléchargements
- Gestion de la défense pare-feu avec le centre de gestion des pare-feu cloud de Cisco Defense Orchestrator

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.