Modifier l'adresse IP de l'interface de gestion sur FTD géré par FMC

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

- Configurations

Vérifier

Dépannage

Informations connexes

Introduction

Ce document décrit comment modifier l'adresse IP de gestion du périphérique Firewall Threat Defense géré par le Centre de gestion du pare-feu sécurisé.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

Composants utilisés

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

- Secure Firewall Management Center Virtual version 7.2.6
- Cisco Secure Firewall Threat Defense Virtual version 7.2.4

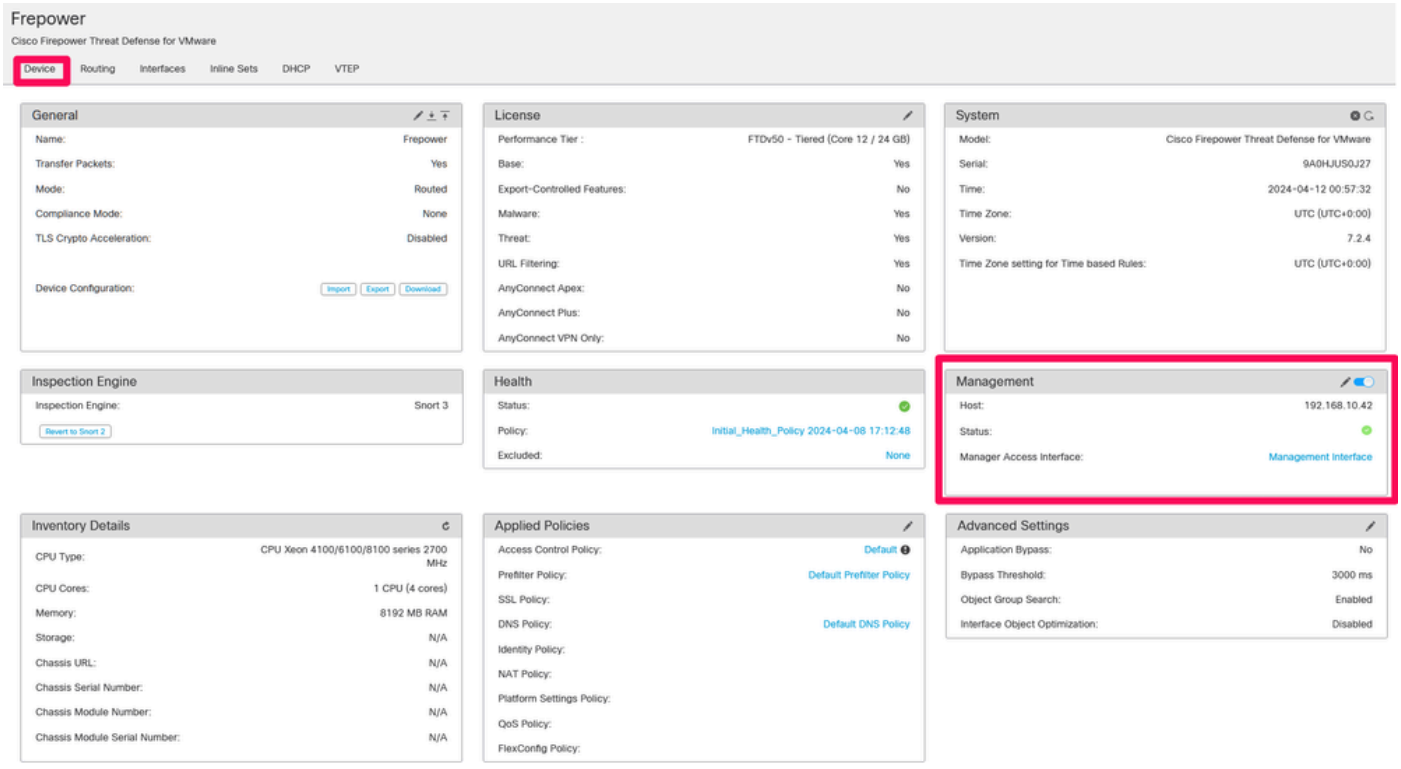
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

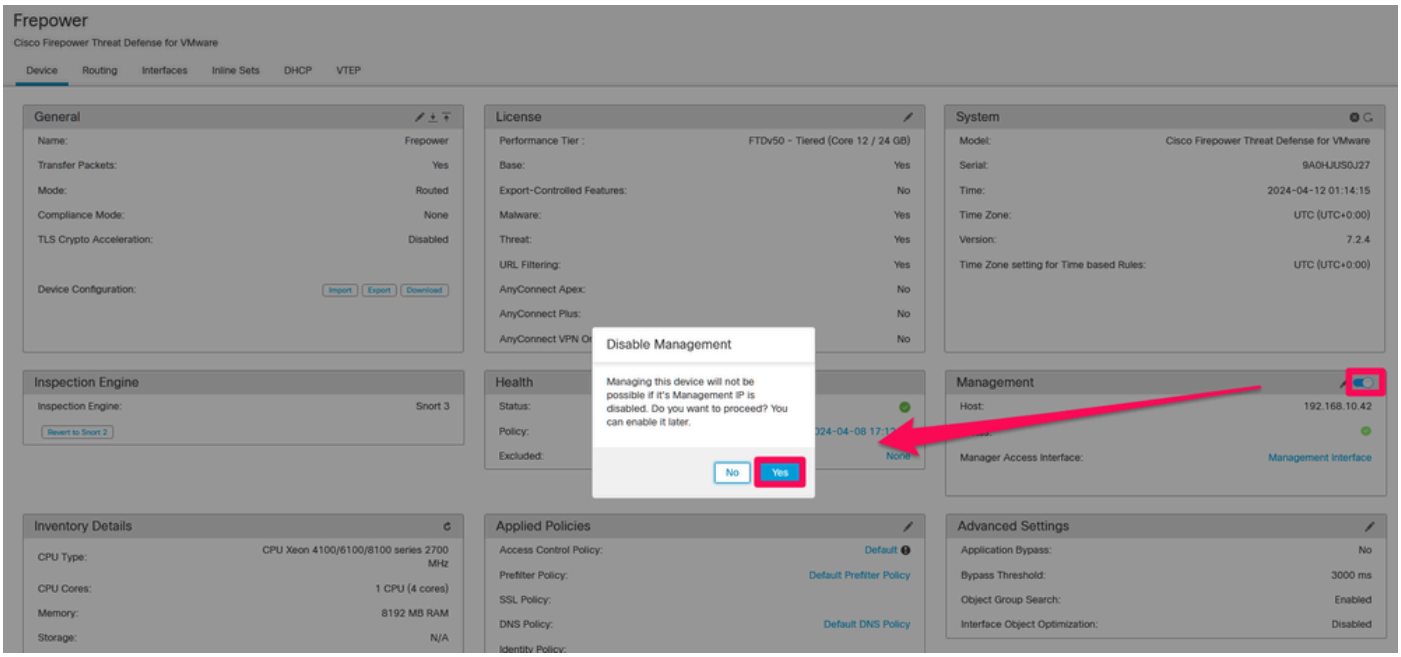
Configurations

Étape 1. Accédez à l'interface utilisateur graphique de FMC et passez à Device > Device Management.

Étape 2. Sélectionnez Device et recherchez la section Management.



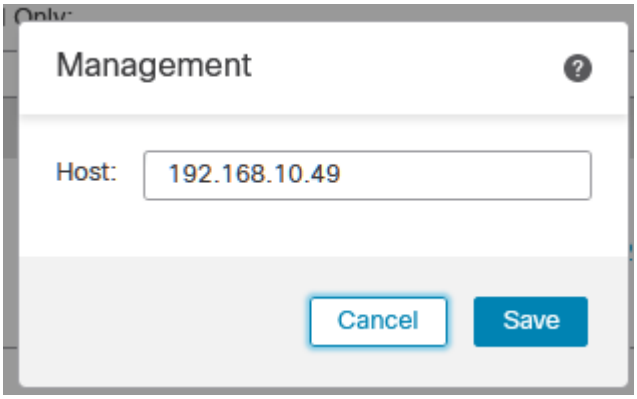
Étape 3. Désactivez la gestion en cliquant sur le curseur et confirmez l'action en sélectionnant Oui.



Remarque : La désactivation de la gestion interrompt la connexion entre le centre de gestion et le périphérique, mais conserve le périphérique au sein du centre de gestion.

Étape 4. Lorsque la gestion est désactivée, modifiez la connexion de gestion en sélectionnant Modifier.

Étape 5. Dans la boîte de dialogue Management, modifiez l'adresse IP dans le champ d'adresse de l'hôte distant, puis sélectionnez Save.



Remarque : Dans le cas d'un déploiement FMC en haute disponibilité, cette modification doit être effectuée à la fois sur les appliances FMC primaires et secondaires, car elle n'est pas répliquée.

Étape 6. Connexion à la console FTD pour modifier l’adresse IP de gestion

---

Avertissement : La modification de l'adresse IP de gestion peut entraîner la perte de la connectivité SSH au périphérique si la session est établie via l'adresse IP de gestion. Par conséquent, il est recommandé d'effectuer cette modification via l'accès à la console, comme suggéré par Cisco.

Étape 7. En mode Chic, modifiez l’adresse IP de gestion à l’aide de la commande suivante :

```
> configure network ipv4 manual 192.168.10.49 255.255.0.0 192.168.255.254
```

Remarque : Cette configuration est appliquée à l'interface de gestion par défaut.

Étape 8. Revenez à l’interface graphique utilisateur du FMC et réactivez Management en plaçant le curseur en position On (Activé).



Étape 9. Sachez que le rétablissement de la connexion de gestion peut prendre un certain temps ; une reconnexion réussie est indiquée comme illustré dans cette image :



Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement. Vous pouvez vérifier la connectivité de gestion via l'interface de ligne de commande FTD. Pour ce faire, connectez-vous à l'interface de ligne de commande, en mode Clish, en exécutant la commande suivante :

```
> sftunnel-status

SFTUNNEL Start Time: Fri Apr 12 01:27:55 2024
------OUTPUT OMITTED------
**********************

**RPC STATUS****192.168.10.40*************
'last_changed' => 'Fri Apr 12 01:09:19 2024',
'active' => 1,
'ipv6' => 'IPv6 is not configured for management',
'uuid_gw' => '',
'uuid' => '4a6e43f6-f5c7-11ee-97d5-a1dcfaf53393',
'name' => '192.168.10.40',
'ip' => '192.168.10.40'

Check routes:
No peers to check
```

Dépannage

Cette section fournit des informations pour dépanner votre configuration.

- Pour vérifier l'état de la connexion de gestion au niveau de l'interface de ligne de commande FTD, exécutez la commande show sftunnel status brief. Observez la sortie d'une connexion qui est inactive, indiquée par l'absence de détails connectés au canal homologue et par des informations de pulsation manquantes.

```
> sftunnel-status-brief

PEER:192.168.10.40
Registration: Completed.
Connection to peer '192.168.10.40' Attempted at Fri Apr 19 21:14:23 2024 UTC
Last disconnect time : Fri Apr 19 21:14:23 2024 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

Une connexion saine entre les périphériques est confirmée lorsque la commande sftunnel-status-brief au niveau de l'interface de ligne de commande FTD produit une sortie qui inclut un canal homologue connecté aux informations et aux données de pulsation.

```
> sftunnel-status-brief

PEER:192.168.10.40
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '192.168.10.40' via '192.168
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '192.168.10.40' via '192.168.1
Registration: Completed.
IPv4 Connection to peer '192.168.10.40' Start Time: Fri Apr 19 21:12:59 2024 UTC
Heartbeat Send Time: Fri Apr 19 21:13:00 2024 UTC
Heartbeat Received Time: Fri Apr 19 21:13:23 2024 UTC
Last disconnect time : Fri Apr 19 21:12:57 2024 UTC
Last disconnect reason : Process shutdown due to stop request from PM
```

- Pour vérifier la connectivité du réseau, envoyez une requête ping au centre de gestion à partir de l'interface de gestion et entrez ping system fmc_ip dans l'interface de ligne de commande FTD.

Informations connexes

- Notions de base sur la gestion des périphériques
- Assistance technique de Cisco et téléchargements

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.